Symantec™ Security Gateways Reference Guide

Supported Products:

Symantec Gateway Security 2.0 5400 Series (Models 5420, 5440, 5441, 5460, and 5461)
Symantec Enterprise Firewall 8.0

Symantec™ Enterprise Firewall Reference Guide

Documentation version 8.0

Copyright notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

This product requires a license file. The fastest and easiest way to register your service is to access the Symantec licensing and registration site at https://licensing.symantec.com.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at https://www-secure.symantec.com/platinum. When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 9 Preventing attacks

Chapter 10 Ensuring availability

Appendix A Log messages

Appendix B IDS events

Chapter 1

Introducing Symantec security gateways

This chapter includes the following topics:

About this guide

This guide provides conceptual information about Symantec security gateways, which include the Symantec Enterprise Firewall and Symantec Gateway Security 5400 Series appliances. This guide offers further insight into how the features of these products work, and suggests guidelines on when or when not to use specific functionality. Unless stated otherwise, the information in this book applies to all supported security gateways.

This guide does not offer installation or configuration information. For installation issues, consult the appropriate installation guide for your product. Consult your product's administrator guide for detailed step-by-step instructions to configure product features. You can find information on integrating and managing this product from SESA in your product's implementation guide.

Intended audience

This manual is intended for system managers or administrators responsible for maintaining Symantec security gateways. This guide assumes that readers have a solid understanding of networking concepts, familiarity with the product and the management interface, and knowledge of the company's network topology.

Documentation updates

Consult the release notes for platform-specific information on any issues related to feature support or any corrections to the supplied documentation. Always check the Symantec Web site at http://www.symantec.com for the latest information on any Symantec products.

License information

You should consult the licensing appendix in your product's installation guide for license information.

About Symantec security gateways

Symantec security gateways are software and hardware solutions that employ a multi-layered security approach, integrating core Symantec technologies to effectively prevent security breaches at the perimeter. Each product incorporates an industry-tested firewall, virtual private networking, content filtering, and high availability and load balancing, all easily configurable through a platform-independent management interface. The appliance products also offer antivirus and intrusion detection and prevention components.

Symantec security gateways are designed for small and medium size companies that may not have a dedicated security staff and equipment for a full security architecture but need protection against the most common types of threats, to the largest companies that demand the strongest levels of enterprise protection.

Industry-tested firewall

The foundation of the security gateway is the firewall component. With an impeccable security record, the mature Symantec Enterprise Firewall-based component protects at the network layer with a custom driver that scrutinizes every packet, and at the application layer with full application inspection proxies that provide protection against a variety of application-based attacks.

The core of the firewall component is the Symantec driver. The driver incorporates several security features including fragment reassembly, header and datagram validation, and SYN flood protection. You can view the driver as a security guard that checks the credentials and integrity of both incoming packets (packets originating from any source other than the security gateway) and outgoing packets (packets originating from the security gateway), and determines whether or not those packets go on to more sophisticated checks.

Similar to standard proxies, Symantec's application proxies reduce overhead, create access to services that may not exist on the security gateway, and provide security by creating a virtual air gap between the client and the server. However, Symantec's application proxies also prevent attacks by scanning and filtering for them within the data stream. Working at this level, Symantec's application proxies analyze the entire data stream of every connection attempt. This provides a considerable advantage over other approaches that only work at lower levels of the protocol stack.

Virtual private networking

The security gateway incorporates a robust VPN component, letting organizations securely extend their network. The VPN component is a standards-based solution, that establishes encrypted connections from remote locations. The security gateway uses IPsec tunnels to send encrypted and encapsulated traffic across public networks to other IPsec-compliant endpoints.

A central piece of any VPN implementation is the algorithms used to provide encryption and integrity checks. The security gateway supports the Advanced Encryption Standard (AES) algorithm for stronger security and improved performance over Triple DES and DES implementations. Triple DES and DES are also supported, as well as MD5 and SHA1 for packet integrity.

Content filtering

Symantec security gateways include a strong content filtering component that lets administrators simply and efficiently deny access to Web sites and Web site content. Content filtering is supported through an internal, categorized URL database of Web sites. When you purchase a subscription, the internal database is periodically updated to reflect new Web sites. You can make manual entries to the Web site database. When content filtering is used with rules that prevent access to sites that may fall outside a company's acceptable use policy, attempted access is logged, and the browser displays a "Forbidden by ratings check" to the end user.

High availability/load balancing

The security gateway includes support for high availability and load balancing (HA/LB). HA/LB combines multiple security gateways into a single security solution, and then narrows the point of access to a virtual IP address (VIP) on each network the cluster faces. Users no longer direct requests at a specific machine. Rather, connection requests are pointed at the cluster VIP. Connections are no longer dependent on the state of a specific machine; if one cluster node fails, another is there to continue with the connection, transparent to the end user.

The integrated HA/LB technology is based on a share nothing model. Other HA/LB solutions commonly use disk sharing or MAC address sharing to achieve failover. Symantec's implementation is network-based, where the network provides the means of communication between all nodes in a cluster. Every node in the cluster shares responsibility in maintaining the state of the cluster over a controlled network.

Anti-spam support

The number of unsolicited emails sent daily is staggering. Unsolicited electronic messages are commonly referred to as spam, and are intrusive, aggravating, and sometimes offensive. Many email clients try to address the issue by filtering email messages, but filters are usually only effective when the sending source or information in the header remains constant. Spammers understand the tools available to users, and in many cases they simply spoof or change the source email address, or change the subject, circumventing the filter.

If your company operates an internal mail server that receives email from external sources, Symantec's security gateways offer some additional methods to reduce the vast amount of unsolicited received email. By default, the SMTP proxy checks for protocol anomalies, and you can configure the the SMTP proxy to prevent the security gateway from functioning as an SMTP relay. You can impose hard and soft limits on the number of recipients in an email. Additionally, you can check email sources can, and if they don't resolve, block them. Optionally, you can elect to use one of the public real-time blackhole lists (RBL) when deciding to accept or reject an email.

Antivirus

Symantec security gateways feature award-winning antivirus technologies that make Symantec the industry leader in virus protection software. Symantec antivirus technology is one of the fastest and most effective solutions available today for detecting and preventing malicious virus attacks. As new threats emerge, Symantec's LiveUpdate technology updates both virus definitions and the engine without service interruption, keeping you fully protected now and in the future. Although the antivirus component is an appliance-only feature, software versions of the security gateway can leverage the appliance's antivirus feature by using the appliance as an off-box antivirus solution.

The antivirus component incorporates bloodhound technology for heuristic detection of known and unknown viruses, and Symantec Striker™ technology to detect and identify polymorphic viruses. The antivirus component detects malicious viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats. Additionally, the antivirus component lets you decide what to do with infected files; you can block or clean files containing malicious code.

Intrusion detection and prevention

Symantec security gateways monitor network traffic for suspicious behavior and respond to detected intrusion in real-time. The intrusion detection component's signatures help detect and prevent against numerous attacks including Teardrop, Whisker, Girlfriend, NOOP, buffer overflows and many others. Symantec's LiveUpdate ensures that new atomic signatures are downloaded to address new threats well before they become security issues. Intrusion detection and prevention is an appliance-only feature.

Traditionally, network intrusion detection systems (NIDS) consist of one or more sensors deployed across an enterprise and a console to aggregate and analyze the collected data. The majority of commercial IDS products are based on a system that examines network traffic for special patterns of attack. This method of detection is called signature-based detection. Some NIDS miss attacks because they cannot keep pace with the high traffic volumes, or generate unmanageable numbers of alerts due to false positives.

Symantec's intrusion detection and prevention component provides a common, highly coordinated approach to detect attacks at very high speeds within the network environment. Using an array of detection methodologies to enhance attack identification, the intrusion detection and prevention component collects evidence of malicious activity with a combination of protocol anomaly detection (PAD), traffic rate monitoring, protocol state tracking, and IP packet reassembly. The intrusion detection and prevention component does not rely on signatures to detect attack, giving administrators hours, if not days, to respond to the threat and helping to close the window of vulnerability inherent in other detection solutions.

Where to get more information

You can find additional information concerning this product in:

- *Symantec Gateway Security 5400 Series Installation Guide*
- *Symantec Gateway Security 5400 Series Administrator's Guide*
- *Symantec Gateway Security 5400 Series Release Notes*
- *Symantec Enterprise Firewall Installation Guide*
- *Symantec Enterprise Firewall Administrator's Guide*
- *Symantec Enterprise Firewall Release Notes*
- *Symantec Advanced Manager for Security Gateways (Group 1), Symantec Event Manager for Security Gateways (Group 1) Integration Guide*
- *Symantec Advanced Manager for Security Gateways (Group 1), Symantec Event Manager for Security Gateways (Group 1) Administrator's Guide*
- *Symantec Advanced Manager for Security Gateways (Group 1), Symantec Event Manager for Security Gateways (Group 1) Release Notes*
- *Symantec Client VPN User's Guide*
- *Symantec Client VPN Quick Start Card*
- *Symantec Client VPN Release Notes*

You can find additional information on TCP/IP, networking, and Internet security in:

- *DNS and Bind*, Paul Albitz and Cricket Liu. 3rd ed. Sebastopol, California: O'Reilly & Associates, Inc., 1998. ISBN 1-56592-512-2.
- *Internetworking with TCP/IP,* Vol. 1*, Principles, Protocols, and Architecture*, Douglas E. Comer. 4th ed. Upper Saddle River, New Jersey: Prentice Hall, 1995. ISBN 0-130-18380-6.
- *Firewalls and Internet Security: Repelling the Wiley Hacker*, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. 2nd ed. Boston, Massachusetts: Pearson Education, Inc., 2003. ISBN 0-201-63466-X
- *TCP/IP Illustrated.* Vol. 1*, The Protocols*, W. Richard Stevens. Reading, Massachusetts: Addison Wesley Publishing Co., 1994. ISBN 0-201-63346-9

Chapter 2

Network security overview

This chapter includes the following topics:

About network security

The success of a corporation's network and information infrastructure depends on its adaptability to evolving communications needs. A well-designed network enables a business to easily handle the varied and competing needs of a mobile workforce, inter-enterprise computing, virtual work teams, and the increasing dependence on the Internet. The benefits offered by a well-designed network include increased channels for customer interaction and feedback, access to network resources of information, and the ability to securely extend the boundaries of the local office to include all remote locations.

However, these benefits are not without risks; the Internet was not designed with security in mind. With potentially unlimited access to the Internet, there is a real chance that someone will try to gain access to your network resources. Therefore, the boundary between the enterprise's private and public network segments, known as the perimeter, is an extremely important security focal point. You should use the information in this chapter as a starting point to understand the different points of access to your network, and what you must consider when developing a secure network policy.

Security considerations

While it is becoming increasingly important to develop a secure, well-designed network that supports multiple access methods, the risks associated with this strategy have also increased. You must address the issue of security first before tackling any other issue. After considering security first, you can then look at balancing the safety of your network with access.

When developing a secure network, you should consider four access areas to ensure that you get the maximum benefit with minimal risk. These areas include:

- Internal access
- Perimeter protection
- Internet access
- Remote access

Internal access

One of the most important areas to consider is the access granted to employees. The majority of security breeches originate internally, whether they are accidental or intentional. A strong internal security policy prevents almost all accidental security breaches, and helps hamper many intentional ones. When developing your internal access security policy, you must account for the confidentiality, integrity, and availability of all company data.

Data confidentiality

Company data ranges from public information, such as product brochures or marketing materials, to personal or private information, such as an employee paycheck or company trade secrets. Obviously, not every piece of company data should be viewable to everyone. For example, you wouldn't want to make public what your customers paid for your product or service. With this information, a competitor could underbid you, and steal this customer.

When considering data confidentiality, you must decide how to classify, or separate your company information, the roles or permissions users are given when they connect to the network, and the type of access each user has. For example, if you separated your company information into the categories of private, internal, and public, regular employees that logon to the network might only have access to internal and public information. You might reserve access to private information to managers.

Data integrity

The access you grant to a network user determines the integrity of your company data. If you grant a general employee modification privileges to private information, your upper management, who might normally use this information to make management decisions, can no longer depend on the accuracy of the data; the employee may have accidentally or purposely modified this data.

When planning for data integrity, you must consider who has access to the different types of data, and the ramifications of their actions on that data. You should also consider having checks and balances in place to thwart intentional attempts to corrupt data by authorized personnel. For example, you may consider having more than one individual write and review material before release. Having two or more people responsible for the integrity of data significantly reduces the likelihood of data corruption.

Data availability

The concept of data availability guarantees that authorized individuals are granted uninterrupted access to required information in a timely manner. Ensuring data availability requires that you have controls in place that properly authorize users, provide an acceptable level of performance, quickly handle interruptions, and prevent data loss or destruction. Poorly thought out or insufficient access controls may create a situation where data is compromised, making it unavailable for authorized personnel at a later date. A security policy that takes into account data availability helps insure that your network performs optimally and that authenticated users can access the information they need to perform their jobs.

There are several approaches that ensure data availability. Some of these approaches include designing data delivery systems properly, using controls to prevent unauthorized access, monitoring network performance, using routers and firewalls to prevent attacks, and maintaining and testing backup systems.

Perimeter protection

A strong security product at the perimeter of your network is an absolute necessity. The router supplied by your Internet service provider (ISP) can provide some security for a network in the form of packet filtering, but once bypassed, if there are no other security measures in place, your internal systems are wide open to compromise. If you elect not to install a perimeter security device, the burden for protection falls on each individual system. You must configure each system to repel the strongest attack that an attacker might use. You must also continuously monitor each system, looking for successful attack attempts. Because many companies have a mixture of computers with different operating systems, and a mixture of users with different levels of computer experience, perimeter security is an absolute must.

Most companies address the perimeter security issue by installing some form of security gateway that includes, at a minimum, firewall capabilities. A security gateway is a system or group of systems that act as a secure barrier, separating two or more networks. You can use a security gateway to impose access controls on the connections between all connected networks. For example, a security gateway can accept traffic on one interface and drop packets that arrive on another, or drop all packets that originate from a defined range of IP addresses.

A security gateway is a vital first line of defense against attacks directed at a company's internal network. However, a security gateway is a perimeter defense only. When properly configured, it prevents access to the internal network from the outside, but does nothing to restrict access within the network. A security gateway cannot protect you from:

- Propagation of viruses by physical or electronic medium
- Theft of passwords by trusted users for use in future attacks
- Attacks led by trusted users behind the security gateway
- Intentional corruption or destruction of company data or property by a trusted individual

Types of security gateways

There are several different types of security gateways, including:

- Simple packet filter
- Stateful packet filter
- Circuit-level
- Application-level

Simple packet filter

Packet filtering has long been a feature of routers, and still serves as the foundation for many security gateways on the market today. Packet filters work by distinguishing packets based on IP addresses or specific bit patterns. However, simple packet filters cannot protect against application-level attacks because packets are processed at the lower levels of the stack, and not in application space.

Simple packet filters have drawbacks that include:

- They are inherently more complex, making them difficult to set up and administer.
- They are by nature less secure than application-level proxy security gateways.
- They do not automatically hide network and system addresses from public view.

Stateful packet filter

Stateful packet filtering security gateways build on the functionality of simple packet filtering security gateways by extracting certain well-known bit patterns in the protocol headers of TCP and UDP connections. They create and maintain a table of established, open TCP and UDP connections, and then examine and compare header information of each packet that passes through the security gateway. This state information is used to track open, valid connections without having to process the rule set for each packet. Only the first packet of a connection is approved; subsequent connection packets are recognized and allowed unchecked.

Stateful packet filters have a number of weaknesses, including:

- Inability to protect against application-level attacks
- Susceptibility to sophisticated IP fragmentation and IP source routing attacks
- No control of application-specific operations, such as read/write or put/get
- Configuration in the proper order to work as intended
- Inability to automatically perform address hiding
- Susceptibility to routing-based attacks or to failing open
- Complex configuration

Circuit-level

Unlike Symantec security gateways, which look for application-level data before allowing a connection, circuit-level security gateways operate at the session level. They typically rely on a state table containing a list of valid connections. Subsequent TCP and UDP connections are allowed based on comparison with the information in the state table.

The downside to this approach is that it works at the session layer only. Once a session is established, the security gateway might allow any type of traffic to pass through. This is inherently less secure than proxying connections at the application level, and might leave the protected network open to attacks that exploit the security gateway's lack of contextual information. This lack of contextual information also makes it difficult to distinguish between different types of traffic for the same protocol, like FTP gets and FTP puts.

Application-proxy firewall

Many consider application-proxy firewalls offer the most robust inspection of packets. Not only can you review the source IP address, destination IP address, and ports to determine whether to allow or deny the packet, but you can also perform a full inspection of the data. Because application proxies get information about a packet at any layer of the network stack, they are capable of detecting many attacks that other firewall types miss. For example, an application proxy for HTTP can block the traffic based on an illegal or malformed HTTP command, where firewall types like packet filter or circuit-level have no knowledge of the data in the packets.

One major drawback to application-proxy firewalls is that they generally perform most of the work in application space. This makes them inherently slower than other types of firewalls as packets must travel to the uppermost layers of the network stack for processing.

Symantec hybrid security gateway

Symantec's security gateways are hybrid firewalls that offers the following advantages:

- True packet filter.
- Optional stateful packet inspection and the ability to speed up traffic throughput with its fast path mechanism.
- Application proxies that are RFC-compliant and protect against well-known attacks through protocol anomaly detection (PAD).

- URL pattern matching and content filtering.
- Secure failure. The design of the Symantec security gateway ensures that if the security gateway fails, packets are not routed. Packets can only pass once they are verified through the security gateway's rule checking mechanism.
- VPN support that is normally shipped as a separate product with other solutions.
- For the appliance models only, additional features such as antivirus, intrusion detection and intrusion prevention.

Protection provided by your Symantec security gateway

Some of the most common attacks are routing based. To protect against this type of attack, the security gateway does not route IP traffic at the network layer. Instead, the security gateway acts as a virtual brick wall that provides a physical and logical separation of internal (secured) from external (public) networks. This refusal to route is important, because it makes it impossible for packets to pass through the security gateway at the routing layer, even if a failure occurs. The security gateway simply does not provide a network-level path, or route, for packets to take. Instead, packets are forced to travel to the security gateway's application layer where the content of a request is thoroughly examined.

In addition to its refusal to route traffic at the network layer, the Symantec security gateway provides protection in the following areas:

- Security driver
- Intrusion detection component (appliance only)
- Application proxies

Security driver

Your security gateway was designed with security as its number one objective. Incoming packets are first exposed to the security gateway at the lowest levels of the network stack by a security driver that performs the following checks:

Host blacklisting	The security gateway provides a feature called a blacklist that tracks IP addresses the security gateway should block. If an IP address appears in this list, the driver immediately drops all incoming packets from this source, preventing any further processing by the security gateway. IP addresses are normally added to the list by an intrusion detection system agent registered with the security gateway. Addresses are eventually removed from the blacklist after a configurable predetermined period of time.
IP address spoof checking	Address spoofing makes a packet appear to come from a different source address than where it actually originated. Spoof protection associates network ranges with an interface. If a packet has a source address that falls within the associated network, the security gateway examines the packet to see if it arrived at the correct interface. Packets within the network range, but arriving at an incorrect interface, are dropped. The security gateway checks for spoofing by performing a thorough check of the source and destination addresses. Address checks include ensuring that the source or destination for the packet is not the loopback address, and the source address is not one of the security gateway's addresses, is not an ICMP redirect, and is not a broadcast or multicast address.

Detailed packet inspection	IP packet processing monitors the packet type and certain types are disallowed for security reasons; ICMP redirects and source routed packets are two examples. The security gateway also checks the reserved bit, and discards any packets with the reserved bit set. IP datagram validation is similar to IP packet processing; however, this is done with fully re-assembled IP datagrams. This inspection examines datagrams for TCP length, TCP flags, and UDP length. IP headers, checksums, lengths, options, and addresses are scrutinized to prevent attacks against the local machine's IP stack. For example, by creating a bad IP header length, an attacker could attempt to overrun a data buffer. To protect against this, packets with an incorrect header length are discarded.
IP fragment protection	The Symantec driver provides its own IP fragmentation and re-assembly routines. This is done to ensure that the reassembly of packets is consistent among platforms, and to help guard against IP fragmentation attacks. Packets that do not reassemble correctly are immediately dropped.
SYN flood protection	SYN flood protection is interface specific and, when enabled, tracks incoming packets. If multiple connection attempts are made from the same source within a defined period of time, additional connections from that source are denied. Additionally, the driver logs an entry to show that the driver blocked the source IP address. SYN flood protection for outgoing traffic works in conjunction with the check done on incoming packets. The driver ensures that a SYN received entry appears in the state table, and replaces this entry with a SYN ACK.
Interface packet filter	An interface packet filter lets you block specific traffic on each interface basis. With one or more input or output filters in place, incoming and outgoing packets are screened. The driver drops packets not matching any filter.
MTU check	This check determines the media type and ensures that the outgoing packet is the correct number of bytes in size when the don't fragment bit is set.
Address transparency	This check looks for a transparency record that matches the packet. If a matching record is found, the record is updated appropriately, and the packet's destination is modified according to the information in the record. Address transparency for TCP occurs during this check. For incoming traffic only, if this is an authorized connection, and no record exists, a new transparency record is created.

Intrusion detection and intrusion prevention (appliance only)

As part of the security process on security gateways with integrated intrusion detection and prevention, the driver communicates with the intrusion detection and prevention component to analyze packets and ensure that they do not match known attack types. All driver security checks and calls to the intrusion detection and prevention component are handled in the kernel prior to sending packets up the stack, making the process quick and efficient.

Application proxies

A set of application-specific security proxies evaluates all attempts to pass data into or out of the protected network. While attackers may try a variety of ways to invade a targeted system, most attacks try to exploit application services and their data streams. For example, attackers often use well-known Simple Mail Transfer Protocol (SMTP) holes to break into internal mail systems. Other application-level attacks are designed to exploit services like the File Transfer Protocol (FTP) or the Hypertext Transfer Protocol (HTTP).

The security gateway's application-level access controls prevent attacks by scanning for and filtering them within the connection's data stream. Working at this level, the security gateway uses dedicated security proxies to examine the entire data stream for every connection attempt. This provides a significant advantage over other approaches that only operate at the lower levels of the stack, and typically evaluate connections in to and out of the protected network on a packet-by-packet basis, rather than as a whole.

When a new connection arrives, the appropriate security proxy (determined by connection protocol) first validates that the connection is allowed, and then creates a new connection with the true destination. The security proxy rewrites the source and destination information of the connection to keep information about your network secret. Therefore, with any connection that passes through a security proxy, there are actually two connections: one between the source and the security gateway, and another between the security gateway and the destination.

Internet access

Any company that is serious about being in business must address the issue of plugging into and interacting with the Internet. The Internet has grown into one of the most popular mediums for business communication, from email and Web browsing, to full-blown online meetings. When used securely, the Internet is an indispensable business tool.

The Internet was developed to facilitate the exchange of information, with security as an afterthought. The Internet places the burden of security on the user. New users may not be aware of the dangers imposed by an unsecured Internet connection. Experienced users rationalize that because the Internet is so large, it is unlikely that anything will happen to them. The fact is, if you're unprotected, it's only a matter of time before your system is discovered and compromised. With the tools available today, attackers can scan vast numbers of IP addresses far quicker than ever before.

Profile of an attacker

An attacker (sometimes referred to as a hacker) is anyone who intentionally tries to compromise your network. Understand that there is no typical profile for an attacker. Anyone, at any time, can try to compromise your network. Therefore, you must plan your network security around the fact that everyone is a potential attacker.

As the security gateway administrator, when it comes to access privileges, you have to assume a don't trust attitude towards everyone. To reiterate, there is no stereotype for an attacker, so it's impossible to look at someone and decide whether or not to grant them access. Additionally, access should never be granted as an all or nothing approach. Your network security approach should include varying levels of access, based on job responsibility.

Common attacks

Some of the most common Internet-based attacks include:

IP address spoofing	IP packet headers show a trusted IP address as the source of the packet, but the packet actually originated elsewhere.
SMTP attacks	Mail spamming, mail spoofing, and email-based viruses fall into this category.
TCP session hijacking	An active session is taken over by an unfriendly user.
Port scanning	All ports are checked, looking for potential services to attack.
DNS attacks	Used to gather information, overwrite correct information, or hijack connections.
Man-in-the-Middle attacks	A third-party location (the attacker) acts as an intermediary between two ends of a connection. This lets the attacker gather the information from both ends of the connection, which normally includes user names and passwords.

Stealing information

Once into your network, it is more difficult to prevent an attacker from stealing sensitive information. However, assuming that your perimeter defense has not been compromised, an attacker may look at alternative methods to gain access. Information about your network is very useful to attackers desiring access. You should keep names of computers, accounts, IP addresses, and other similar information confidential. Give extra attention to guarding passwords, as there are several ways to compromise them:

Sniffing	Networks are monitored for users entering their passwords as they log on. Although passwords are sometimes encrypted over public networks, it is possible to obtain the original password by running large numbers of candidate passwords through the same encryption function and comparing the outputs to the actual encrypted passwords. This is done by trying every possible combination of characters or by using a large dictionary of common words in expectation that users often choose common passwords. You can defend against this type of attack by choosing strong passwords that contain eight or more characters and contain mixed case, numbers, and punctuation. If you have to choose words, try to string together two or more unrelated words.
Trojan horse	In security terms, a Trojan horse is a rogue program that takes the identity of a trusted application to collect information or avoid detection. For example, in a common Trojan horse attack, the user is presented with a logon screen that appears to be genuine. The user enters their user name and password, and are either logged on, or presented with an error message that they have to type their logon credentials again. Often, the rogue logon application exits after the first request passing the user on to the real logon. Users are easily fooled into thinking that they probably typed the wrong password and must re-enter the information again, never suspecting that their logon credentials are compromised. This type of attack is difficult to detect. A strong network security policy with no unauthorized downloads is usually the best way to defend against Trojan horses. If you have the time and resources, perform random file comparisons of key binaries on hosts to known, good binaries, confirming that key binaries haven't been compromised.
Social engineering	A social engineering attack is a name given to any attack that tricks an individual into revealing private information. For instance, a user might get a piece of mail that appears to be from that user's ISP. The mail could explain to the user that the ISP is investigating a potential attack on certain accounts, and is asking that the user change their password for security. The mail asks that the user send in their old account information, and what they would like the new account information to be. An unsuspecting user, disarmed by the fact the ISP really seems to be concerned about his or her privacy, can unwittingly return the old and new credentials. Obviously, the only credentials the attacker is interested in is the old ones. The new credentials are never set up, and the attacker has successfully gained access. People identifying themselves over the phone as representatives of a service provider can also trick users out of passwords. A convincing line from someone just doing their job is often hard to resist. Once an attacker obtains the password, he or she often attempts to add privileges to or access information of interest in the account, and then moves on to the next account. Some attackers actually use private information obtained from one account to gain access to a related account. Employees, especially those not affiliated with network security or an IT group, are not always as aware of potential security threats. This makes them a more likely target for a social engineering attack. A strong network security policy and proper education of all company personnel about potential social engineering attacks and preferred responses can significantly reduce or eliminate this threat.

Information theft is not limited to passwords. In addition to passwords, attackers also look for system information, including IP addresses, host names, operating system, and so forth. If a system is unprotected, pertinent information is very easy to obtain through utilities like ping and finger. There is also a wide variety of network scanners like nmap or nessus available to determine the operating system used, and any potential ports to direct an attack.

Viruses

Viruses are self-replicating computer code that are generally harmful to the host in which they reside, and focus on infecting as many hosts as possible. Viruses may just display a message on your screen, change your computer's configuration, lock up you computer, corrupt your files, or erase the hard drive. Some viruses, such as the Nimda virus, attempt to exploit security holes in standard applications or services. Other viruses, such as worms, use up all available resources on a host or network by continually replicating themselves.

Viruses are transmitted in several ways, including downloading infected files from a public Web or FTP site, copying an infected file from floppy disk or other portable storage medium, receiving and opening an infected email, or even across the network from another infected host. Antivirus software for all hosts is required for any good network security plan. Antivirus software helps contain a virus if a host becomes infected, and prevents new viruses from infecting the system in the future.

Denial-of-Service

Sometimes an attacker is not interested in gaining access. Instead, the attacker only wants to prevent legitimate users from gaining access to network services. Any attack that is designed to deny access to computing or network resources is called a denial-of-service (DoS) attack. In general, a DoS attack works by overwhelming your system or network with some sort of false requests. Some denial-of-service attacks include:

Ping attack	In a brute force ping attack, an attacker sends as many ICMP packets within as short a time as possible, overwhelming a system. An attacker may also try sending an unusually large ICMP packet, hopefully exploiting a weakness in the system, and causing the system to freeze.
SYN flood	A SYN flood is a DoS attack where an attacker tries to disrupt service by using up all of the security gateway's available resources. The attacker sends a TCP connection request with the SYN bit on. The security gateway acknowledges and responds to the TCP connection request by sending a TCP response packet with both the SYN and ACK bits set. If this were a normal connection request, the attacker would acknowledge the security gateway's TCP response packet with his own TCP response packet that has the ACK bit set, and the three-way handshake would be complete. However, the attacker never responds. This leaves the process open on the security gateway until the TCP timeout period has expired. An attacker repeats this process, opening as many new connections as possible, as quickly as possible. If enough of these false requests are sent, the security gateway can run out of memory or CPU cycles, preventing legitimate connections from getting through.

Remote access

Many companies today support telecommuter positions where employees do not need to physically be at the office to perform their job. With the advances in Internet speed, video and audio conferencing, and VPNs, the logical boundaries of the company have blurred, and employees can now work outside of the main office. To adequately perform their jobs, remote employees may require access to the office network. However, the number of hackers and curious parties outside the network door has also increased, so access in and out of the network must be properly controlled.

When developing your security policy, take into consideration if or how you plan to grant access to remote employees. You need to think about how that access is granted, who makes the decision to grant access, and what access level is given. Just as one size fits all normally does not apply to a large group of people, one defined access level probably does not apply to every remote employee. Consider segmenting employees by responsibility level, and creating multiple access levels, one for each group.

Management scenarios

The type of network deployment you choose determines the security issues you need to address. The most common types of network deployments include the following:

- Managed security gateway

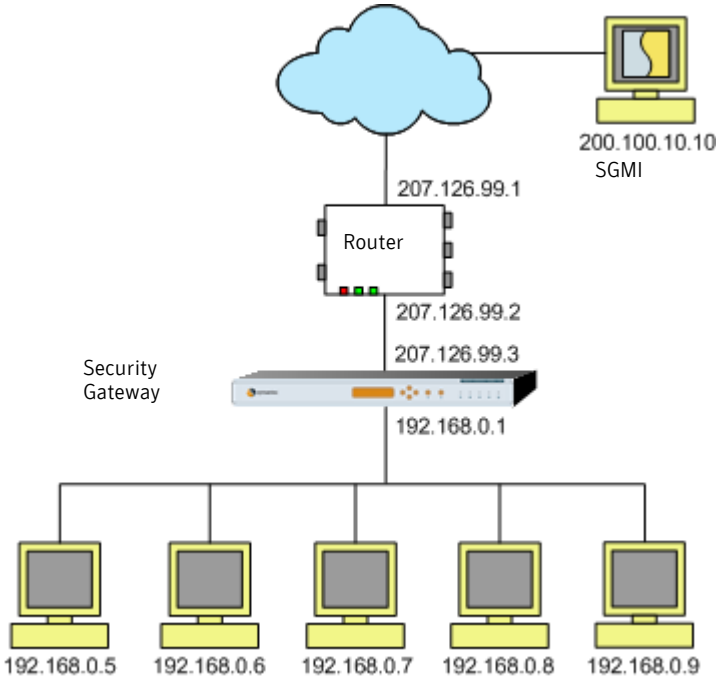
- Managed security gateway (fault tolerant)
- Managed security gateway (advanced)
- Managed security gateway (enclave)
- Managed security gateway (through another security gateway)

Obviously, there are many variations of these scenarios, and your systems may not match exactly. The scenarios presented give you models to consider for your own network deployment, and highlight any potential security issues you may face.

Managed security gateway

Figure 2-1 shows that the simplest deployment scenario requires the security gateway to have two interfaces, each on a different LAN segment. The Security Gateway Management System (SGMI) that manages the security gateway is normally located on the public Internet. A security gateway in this configuration is typically reserved for one-way traffic, especially if one of the interfaces has direct access to a public network. Connection requests are usually initiated from the protected network and destined for external services. If inbound access is enabled, it is not possible to completely secure the protected network. Administrators are advised not to place mail or Web servers on the protected network.

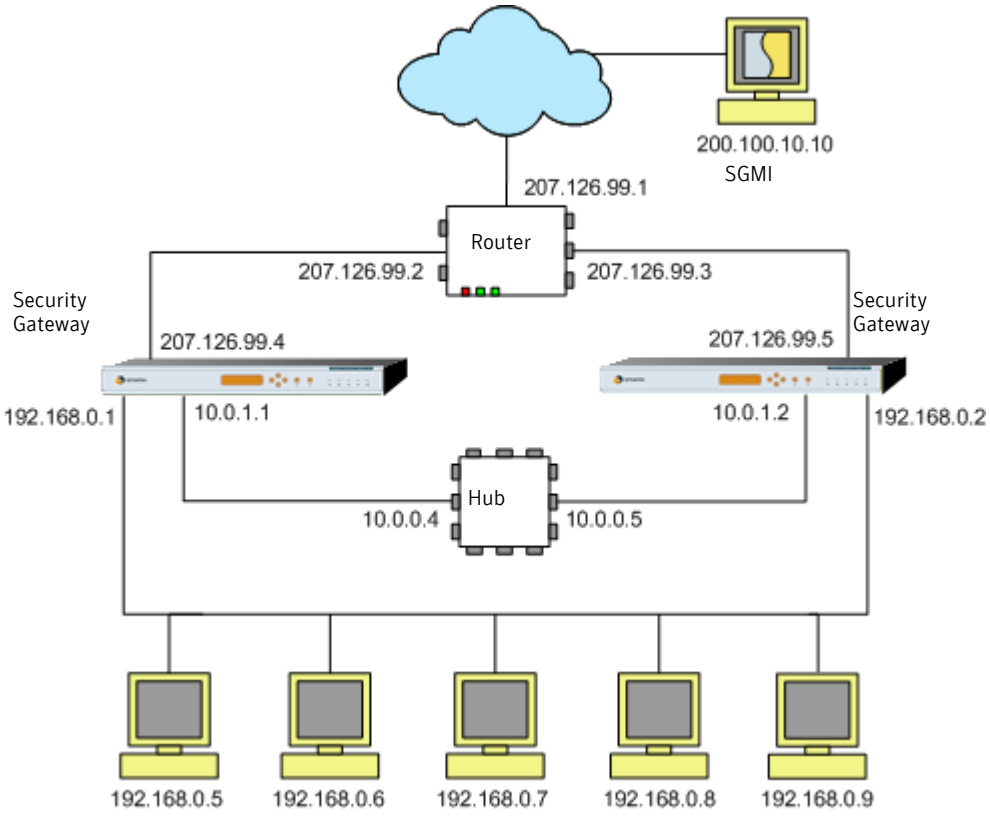
Figure 2-1 Basic network scenario



Managed security gateway (fault tolerant)

Customers often extend the basic deployment by adding one or more security gateways. This configuration, shown in Figure 2-2, can provide redundant and load balanced processing power in the event of a catastrophic failure of a security gateway. Again, connection requests are usually initiated from the protected network and destined for external services. A cluster configuration adds a third, heartbeat network, which is used to monitor the status of each member of the cluster and to pass cluster configuration information.

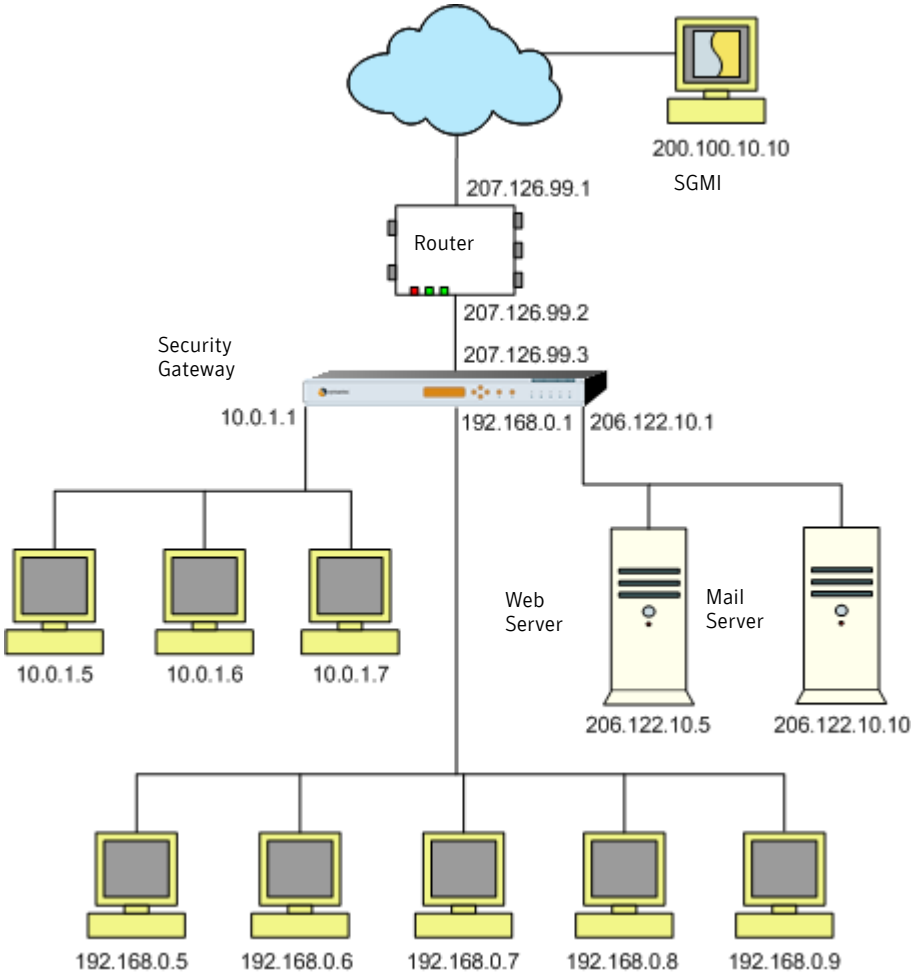
Figure 2-2 Fault tolerant network scenario



Managed security gateway (advanced)

Customers offering e-commerce solutions, or those offering access to services by untrusted users often have additional, directly-connected network segments. These networks are protected LAN segments, but are not given the level of trust that a true internal network enjoys. For example, one of these networks might be used for customer-facing applications such as Web and mail servers, or for connections to partner companies. This scenario might look like the topology shown in Figure 2-3.

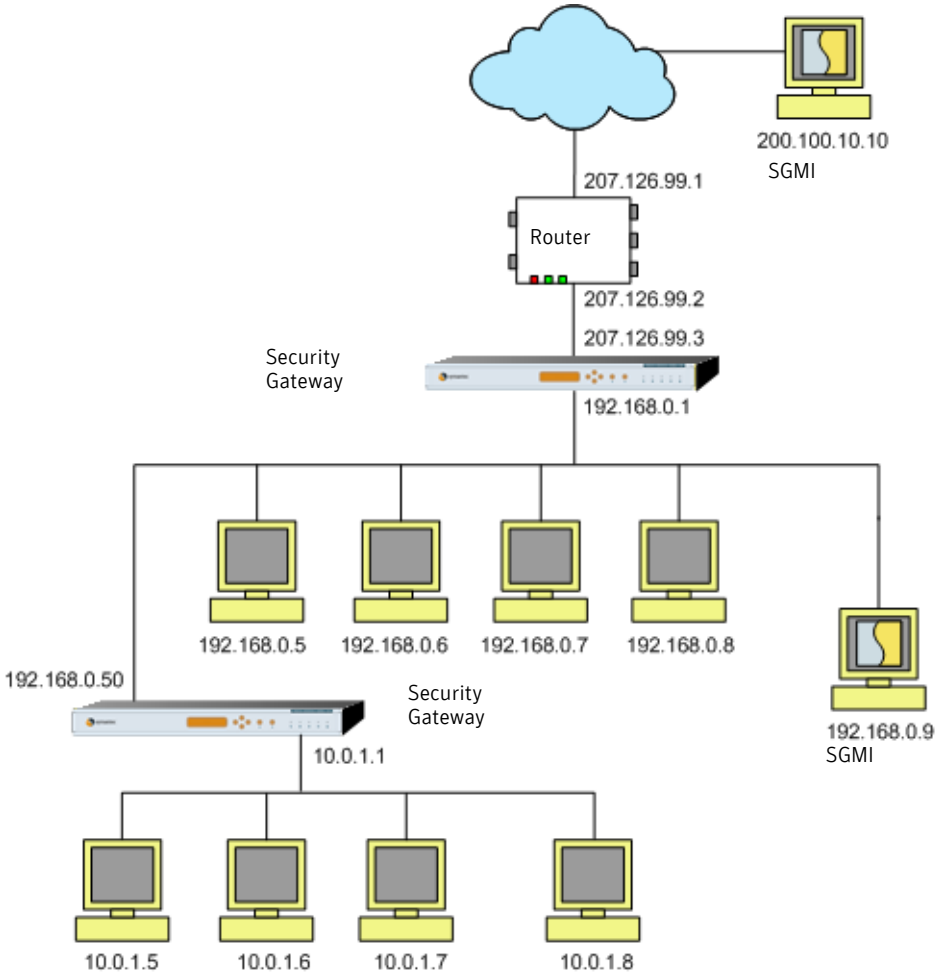
Figure 2-3 Advanced network scenario



Managed security gateway (enclave)

Figure 2-4 shows an enclave security gateway protects sensitive machines or data from access by unauthorized internal users. An enclave security gateway may offer outbound access, but often requires extended user authentication for inbound access, or provides no inbound access at all. Essentially, an enclave security gateway is installed to further segment a network.

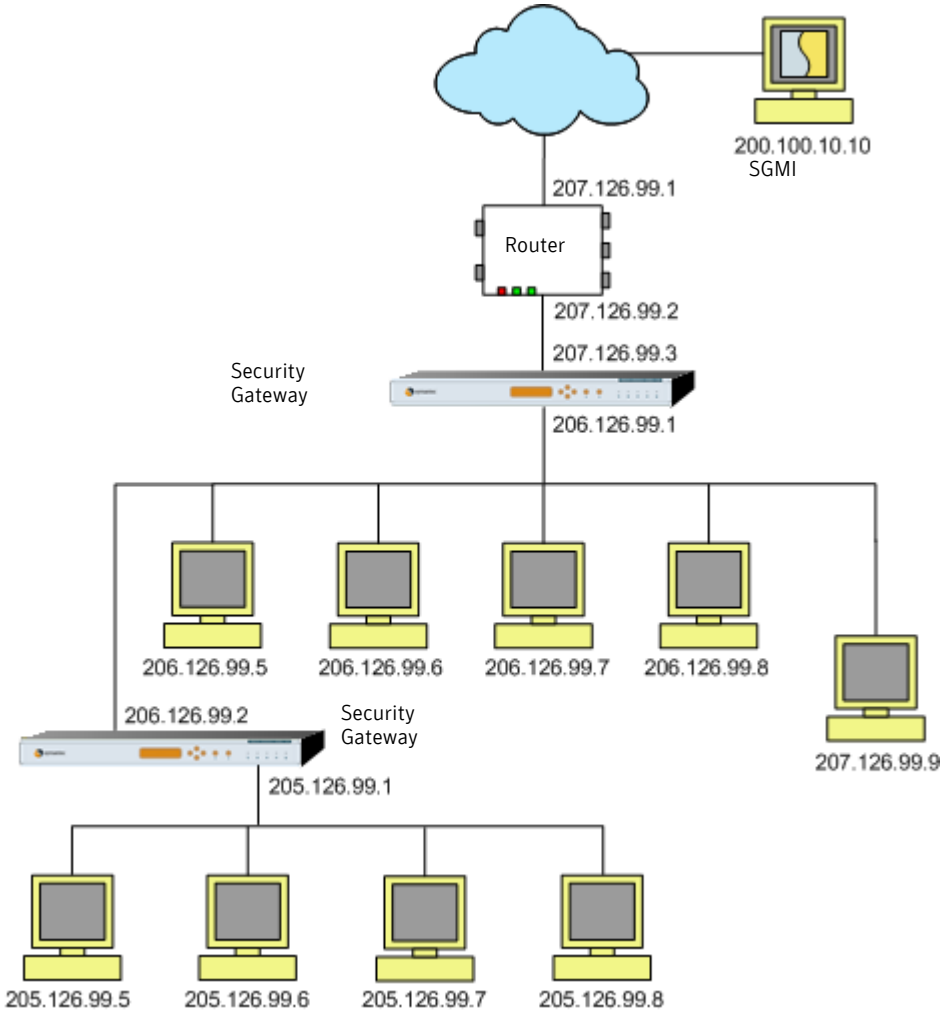
Figure 2-4 Enclave network scenario



Managed security gateway (through another security gateway)

In some situations, it may be necessary to manage a security gateway that is protected by another security gateway. This final scenario presents a unique challenge; each security gateway listens for management requests and must understand whether the request was truly directed to itself, or another security gateway on the protected network. Figure 2-5 shows an external SGMI that manages both security gateways.

Figure 2-5 Managed security gateway through another security gateway



The problem this scenario presents is a function of how the security gateway handles requests. Regardless of the destination, all requests that go through the security gateway initially have their destination address changed to that of the security gateway to force them up the stack for processing. If the request is for another system, and the connection request meets all requirements, a new connection is created to the destination address.

For management connections, however, the security gateway sees that the destination address is the security gateway and the destination port is 2456, and intercepts the packet as a request to manage locally. Management requests are caught by the management server prior to when the security gateway creates the new connection, so without modification, any management request sent to or through the security gateway is processed by the first security gateway encountered.

There are two different approaches to resolving this issue, depending on whether or not the IP address of the second security gateway is routable.

If the address of the second security gateway is routable, you should do the following:

- Create a TCP GSP that allows traffic on 2456.
- Edit the SGMI protocol. You can find this under Policy > Advanced > Network Protocols. Check the box labeled Use Native Service. This should automatically fill in the Native Service Port field with the value 2457.

Enabling the use native service option instructs the security gateway to change the destination port of the packet to 2457 before sending it up the stack. This lets the packet pass through without being captured as a management connection. When the new connection is created to the true destination, both the real destination address and port are substituted back, and the connection proceeds normally.

Warning: When working with the SGMI protocol, make sure that you do not disable both the protocol and the GSP without first creating a new SGMI GSP. Disabling both without having a new SGMI GSP to replace the original SGMI protocol and applying the changes blocks new management requests and prevents you from using the SGMI to manage your system. Consult your product's Administrator's Guide for the steps to properly create an SGMI GSP.

If the address of the second security gateway is non-routable, you should do the following:

- Clone the SGMI protocol and edit the cloned copy. Change the Destination Low Port field to be an unused port other than 2456.
- Create a rule to allow the cloned protocol.
- Create a service redirect to send all incoming management requests that are directed to the new port to the non-routable security gateway.

Chapter 3

Security gateway fundamentals

This chapter includes the following topics:

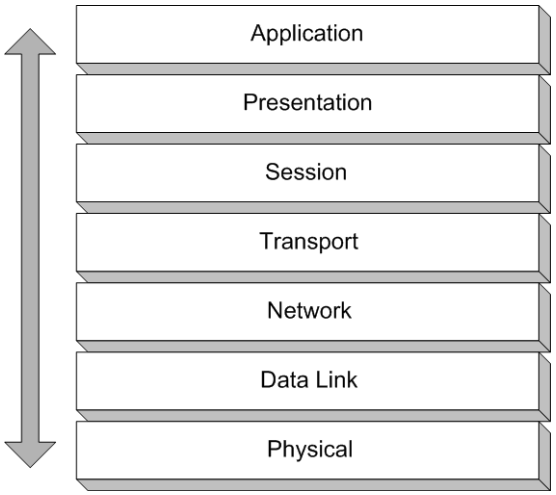
Routes

Routing is the process of choosing a path over which to send packets of information. For the security gateway to function properly, you must define specific routes. Administrators set default routes according to instructions specific to their platforms. Almost all discussions on routing and data communications require an understanding of the publicly accepted terms and technology involved. This section presents some of that underlying technology behind data communications and how it works.

The Open Systems Interconnect Reference Model

Symantec security gateways adhere to the Open System Interconnection (OSI) reference model developed by the International Standards Organization (ISO). This model, shown in Figure 3-1, provides a common reference for discussing data communications, and consists of seven layers, with each layer providing a specific type of service.

Figure 3-1 The OSI reference model network stack



Looking at Figure 3-1, the protocols are almost always presented in this format, like a pile of building blocks stacked upon one another. Because of this appearance, the structure is often referred to as a stack or protocol stack. All hosts desiring to communicate using TCP/IP map to this type of network stack. Table 3-1 describes the functions performed at each layer of the OSI reference model network stack.

Table 3-1 OSI reference model layer functions

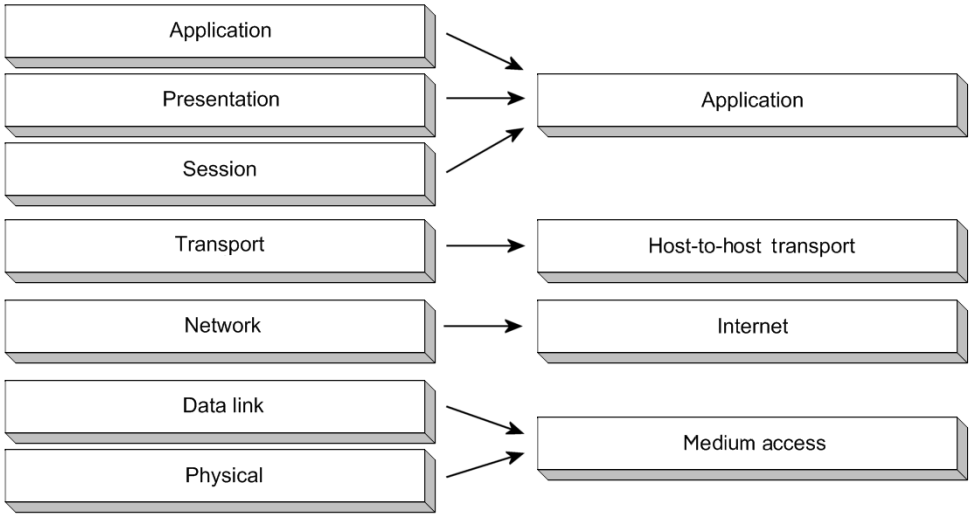
Layer	Function
Physical	Defines the physical characteristics of the hardware needed to carry the data transmission signal. This layer encompasses features such as voltage levels, and the number and location of interface pins. Some established standards for this layer include RS232C, V.35, and IEEE 802.3.
Data link	Responsible for handling the reliable delivery of data across the underlying physical network.
Network	Manages connections across the network, and isolates the upper layer protocols from the details of the underlying network.
Transport	Guarantees that the receiver gets the data exactly as it was sent.
Session	Manages the sessions between cooperating applications.
Presentation	Provides standard data presentation routines.
Application	The layer where user-accessed network processes reside. This includes all of the processes (applications) that users directly interact with, as well as other processes at this level that the user is unaware of.

Each layer of the stack is concerned only with communicating to its peer, the same layer or protocol implemented on another host, and does not concern itself with what happens in the layers above or below. Each layer understands how to work with data it receives, and also understands that the packet is passed up or down to the next layer after it is finished.

TCP/IP basics

The most widely used protocols for transmitting data from one host to another are grouped into a protocol suite called TCP/IP. This suite is a combination of different protocols at various layers with each layer responsible for a different facet of communications. The TCP/IP protocol suite is normally grouped into four functional areas, with some areas incorporating more than one layer of the stack. Figure 3-2 shows how the network stack layers from the OSI reference model are grouped under the TCP/IP suite.

Figure 3-2 Comparison of the OSI reference model to the TCP/IP suite



Medium access layer

This layer normally includes any network interface cards in the security gateway and their corresponding system drivers. Additionally, it comprises the medium used to physically transport data from one host to another. This medium is normally Ethernet, Token ring, fiber optic, or a serial connection.

Internet layer

This is the layer where routing takes place. This is sometimes referred to as the IP layer, and resides in the kernel. Packets passing through routers never go above this layer.

The Internet layer maintains a routing table in memory that it searches each time an IP packet arrives. Each entry in the routing table contains the following:

Destination IP address	This is either a complete host address or a network address. A host address refers to one machine and has 32-bit netmask (255.255.255.255). A network address appears similar to a host address, but has a netmask less than 32 bits. The most common netmasks are 8-bit, 16-bit, and 24-bit, representing the old classification method of class A, class B, and class C respectively, but you can use any value from 1 to 31.
Next-hop router IP address	The next-hop router may or may not be on the intended destination network. If the next-hop router is not the final destination, the next-hop router forwards the packet on to its respective next-hop router. This process continues until the packet reaches its intended destination.
Flags	These specify options about the entry in the routing table. For example, one flag would specify whether the destination IP address is a host or a network, while another flag would specify whether the destination is up or down.

IP routing is done on a hop-by-hop basis. If the IP layer doesn't see the specific IP address matching one of its network interfaces, it sends it to the next-hop router, assuming the next-hop router gets it closer to the packet's intended destination.

Host-to-host transport layer

Both TCP and UDP reside in this layer. Both protocols, although significantly different in the way they operate, provide a flow of data between two hosts. TCP provides a reliable flow of data, concerning itself with things like the size of the packet sent, checksum values, and correct arrival order of packets. On the other hand, UDP uses a simple send and receive operation, without all of the intermediate checks being done. There are specific uses and reasons for each protocol.

Like the network layer, the transport layer resides in the kernel.

Application layer

The application layer is the user interface to the TCP/IP stack. The Web browser you open or FTP application you start up run at this level. The application layer handles all of the details of an application and its interaction with the other layers.

Regardless of their function and responsibilities, each layer typically communicates only with the layers directly above and below it.

Routing TCP/IP packets

Conceptually, IP routing is straightforward. Packets follow a logical and ordered approach to move from one host to another. Listed below are the steps that all protocol stacks follow when routing packets using the TCP/IP protocol suite.

- The application layer creates a packet, beginning with the application header (information about the packet) and ending with the data from the original packet. The new packet is then sent down the stack to the host-to-host transport layer.
- The host-to-host transport layer follows what the previous layer did, and creates a new TCP packet, having its own header information first, and then the application packet information. The host-to-host transport layer then pushes the packet down to the Internet layer.
- The Internet layer determines what to do next with the packet by:
  - Searching the internal routing table for an entry that matches the complete destination IP address. If found, the packet is sent to the next-hop router, or to the directly connected network interface.
  - Next, searching the internal routing table for an entry that just matches the destination network ID. If found, the packet is sent to the indicated next-hop router, or to the directly connected interface.
  - Lastly, searching the routing table for an entry marked “default.” If found, the packet is sent to the next hop-router.
- Once the host-to-host transport layer determines where the packet goes next, an IP header is added and the packet is pushed down the stack to the network access layer.
- At the Network Access layer, a header and footer are added, and the entire frame is now pushed along the physical layer (network connection) until the frame hits the destination machine. Each machine on the network checks the header to determine if the frame belongs to their machine. If not, the frame is quietly ignored. If the frame is intended for a machine, however, that machine pulls the frame off of the network connection, strips off the header and footer, and pushes it up its own protocol stack to the Internet layer.
- The Internet layer follows the same three steps it did in step 3 on the prior host to determine what needs to happen to the packet. If this is the last machine (our intended destination), then the packet IP header is stripped off and sent up to the host-to-host transport layer. If this was not the intended machine, step 4 would be called again, and the packet would continue on its way.
- The host-to-host transport layer checks the packet for accuracy and proper checksum, and if the packet’s information is correct, strips off the TCP header and sends the packet to the application layer.
- The application layer then directs the packet to an application or process operating on the machine.

This process occurs for each packet, until all the necessary information is transferred in both directions. This process also depends on all of the machines involved in the entire delivery path being correctly configured, and with their routing tables properly set up.

Static routes

If your network consists of a series of smaller networks, it is considered a routed network, as opposed to a flat network which consists of only one subnet. Because the security gateway follows the process for routing TCP/IP packets outlined earlier, if one of your internal subnets is not connected directly to the security gateway, any packets hitting the security gateway go out through the default gateway. In most cases, the default gateway is the router or connection you have to your ISP.

A problem arises, however, if a packet comes in to the security gateway, destined for a machine on one of your internal subnets, but not directly visible to the security gateway. The packet is rejected and never reaches its intended destination. To correct this problem, you must define static routes to tell the security gateway about other hosts or networks, not directly visible to the security gateway, but to which the security gateway should route traffic.

Explicit static routes identify a specific network or subnet destination. The routing table holds currently configured static routes. Each entry in the table contains:

Destination IP address	Network, subnet, or host.
Netmask	This is generally an 8-bit, 16-bit, 24-bit, or 32-bit value depending on the destination. For example, 255.0.0.0 is used as an 8-bit mask for a class A network, and 255.255.255.255 is used as a 32-bit mask for a host.
Gateway address	The next hop IP address.

Static routes are used for network or subnet designations only. IP hosts automatically generate a direct route to the network or subnet based on the interface's assigned IP address.

Non-routable networks

It is often the case that a company's internal network is already in place, and the security gateway administrator does not have the luxury of planning this out before adding the security gateway to the network. The problem this presents is that if there are a lot of networks and subnets with no real organization, you need to set up static routes on the security gateway for each of these networks to permit access.

RFC 1918 lists several networks designed for internal use only. These IP addresses do not route across regular Internet routers, and offer a wide range of configuration options, whether a company has a small network, or one consisting of many subnets. The range of addresses specified in the RFC are:

- 10.0.0.0 through 10.255.255.255
- 192.168.0.0 through 192.168.255.255
- 172.16.0.0 through 172.31.255.255

One way to reduce the number of required static routes is to use a hierarchical approach to network addressing. What this means is that all of your subnets stem from a larger main network, and individual routers handle the task of breaking things down further. For example, if you chose to use the 10.0.0.0 network internally, the only static route you would need to set up on the security gateway would be one that says to point any 10.0.0.0 traffic to an internally configured router.

Dynamic routing

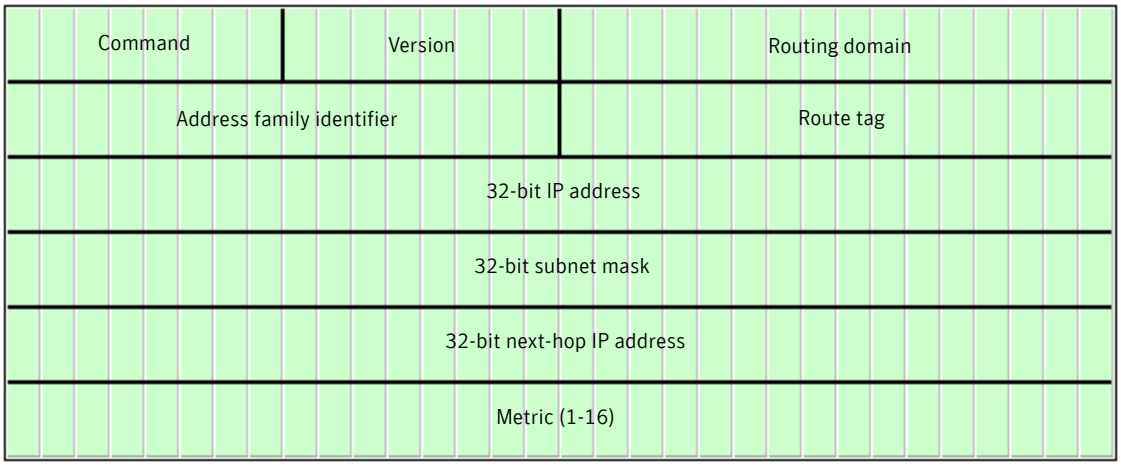
Dynamic routing automatically changes and updates routing information to adjust to changes in network topology or traffic. One of the limitations of a static routing environment is that you must manually configure routing information. In smaller networks, manual configuration is not a major administrative task and is an acceptable alternative to configuring a more complex routing environment. However, as networks increase in size, manual configuration is time-consuming, error-prone, and not the most productive use of resources. To overcome the limitations of static route configuration, administrators use dynamic routing. Dynamic routing significantly reduces the likelihood of an errant entry in a routing table by letting the routing daemon add the entry electronically. It also removes some of the responsibility of monitoring the network, freeing up valuable administrator time.

Dynamic routing is achieved by configuring all of your network routers to speak the same protocol. On corporate networks, it is common to find an Interior Gateway Protocol (IGP) deployed as a practical means of dynamic route discovery. This section discusses two possible protocol choices: Routing Information Protocol Version 2 (RIP-2) and Open Shortest Path First (OSPF) Version 2.

Routing Information Protocol Version 2 (RIP-2)

As defined in RFC 2453, RIP-2 is a UDP-based protocol based on the Bellman-Ford (distance vector) algorithm and is an enhancement to the RIP protocol discussed in RFC 1058. The term distance vector means that messages sent by RIP-2 contain a vector of distances (hop counts). The cost assigned to a route between two networks is calculated by counting the number of hops between the two networks. If there are multiple routes to the same destination, RIP-2 chooses the route with the smallest hop count, and ignores the other paths.

Figure 3-3 RIP-2 packet



As shown in Figure 3-3, the structure of a RIP-2 packet consists of a command (1 byte), version (1 byte), routing domain (2 bytes), and one or more (up to 25) 20-byte groupings that include an address family identifier, route tag, 32-bit IP address, 32-bit subnet mask, 32-bit next hop IP address, and a metric. Table 3-2 describes the information found in each of the fields in a RIP-2 packet.

Table 3-2 Explanation of the fields in a RIP-2 packet

Field	Description
Command	Typically set to one (1) or two (2). A value of 1 indicates that this packet is a request for the responding system to send all or part of its routing table. A value of 2 means that this packet is a response to a RIP-2 request and contains all or part of the sender's routing table.
Version	Defines the version of the RIP protocol being used. For RIP-2 packets, this field is set to 2.
Routing domain	An identifier of the routing daemon to which this packet belongs. RIP-2 supports running multiple instances of the routing daemon, with each instance assigned to its own domain.
Address family identifier	The address family identifier value indicates the type of address in the grouping. For example, an IP address equates to a field value of two (2).
Route tag	This system's Autonomous System (AS) number. This is usually only required when this router is a border router using an exterior gateway protocol, such as EGP or BGP, for communication between two ASes.
32-bit IP address	The IP address of the host or network.
32-bit subnet mask	The mask of the 32-bit IP address. This field was added to RIP-2 to overcome one of the limitations of original RIP packets.
32-bit next hop address	The immediate next hop IP address to which to route packets. Generally used when not all routers in a system use RIP-2.
Metric	A number between 1 and 15 that denotes the cost to get to the declared IP address. If this field is set to 16, it means the destination is unreachable.

RIP-2 communicates using UDP port 520 and was designed to work with moderate-size networks using the same or similar technology. RIP-2 has very little bandwidth overhead when compared to OSPF. RIP-2 supports multicasting in addition to broadcasting, which can reduce the load on hosts that are not listening for RIP-2 messages. However, the protocol is limited to networks whose longest path is 15 hops and uses fixed metrics to compare alternative routes. Because the metrics are fixed, this protocol is not appropriate for situations where routes need to be chosen based on real-time parameters such as load or reliability.

Note: By default, the security gateway does not allow traffic through on UDP port 520 and must be configured to do so. You can open this port by adding or modifying the advanced option portcontrol.enable_udp_ports.

Open Shortest Path First (OSPF) Version 2

Defined in RFC 2328, OSPF is a link-state routing protocol. Unlike RIP-2, which measures the number of hops between networks, each router in an OSPF environment actively tests the status of the link to each of its neighbors, and then sends this information to each of its neighbors. Each router then uses the reported link-state information to build a routing table. Additionally, unlike many other routing protocols, OSPF uses IP (protocol 89) directly.

OSPF is considered to be superior to RIP-2 in many respects. Some of the major advantages to using OSPF over RIP-2 include:

- OSPF networks almost always converge (stabilize) faster than RIP-2 networks in the event of a change to the network topology.
- OSPF can calculate a separate set of routes for each IP type-of-service, which means for any destination, there can be multiple routing tables entries, one for each entry.
- You can base the cost for each interface on various parameters, including throughput, round-trip time, or reliability. A separate cost can be assigned for each IP service.
- Because there is no dependency on the number of hops,as is the case with RIP-2, network paths are not limited to 15 hops.
- When several equal-cost routes to a destination exist, OSPF distributes traffic equally among the routes (load balancing).

Network entities

A network entity is a host or group of hosts that reside locally on the protected network, or on the public network external to the security gateway. A network entity is defined by an IP address, a group of IP addresses, or a domain name. You must define network entities to describe the hosts that pass data through the security gateway. Once the appropriate network entities are defined, you can construct rules and VPN tunnels.

Network entities should be thought of as building blocks, each providing a single endpoint or network definition. Network entities also provide flexibility to your configuration by letting you change host attributes (the IP address of the mail server, for example) without having to change associated rules. All applicable rules are updated automatically.

Network entities include host, subnet, domain, security gateway, group, and VPN security entity.

Host entity

A host entity is a single computer that serves as either a client or server. It resides on the protected network, or on the public network. You define a host using its IP address in fully-qualified, dotted-quad format (for instance, 192.168.0.1 or 10.0.12.5), or by its DNS-resolvable name.

Subnet entity

A subnet entity is a grouping of hosts defined by a network and subnet mask. This grouping of hosts sit either on the protected network, or on the public network. Subnet entities are normally created to define a range of IP addresses that are permitted by a rule. Defining a subnet removes the requirement to create a separate rule for each host to grant access.

By default, the security gateway ships with a subnet entity called Universe. The Universe subnet entity has an IP address of 0.0.0.0 and a subnet mask of /0. The Universe subnet entity is similar to a wildcard that defines the set of all valid IP addresses. You can use this entity in rules that apply to any IP address, but you should only use it in these rules when any host can have access; do not use this entity in a rule when you want to restrict access to only a defined set of hosts.

Domain entity

A domain entity is a group of hosts that share the network portion of their DNS-resolvable host names. For example, www.symantec.com and ftp.symantec.com are both members of the symantec.com domain.

Security gateway entity

By definition any host that acts as a secure entry or exit point for a network is a security gateway. Most often, this term is assigned to firewalls or VPN servers that form an endpoint for secure connections to and from protected networks. Defining a security gateway entity lets the administrator set up some basic characteristics of one of these endpoints. The IP address assigned to this entity is usually the publicly accessible address of the endpoint being defined. To establish Gateway-to-Gateway VPN tunnels, you must define security gateway entities for both local and remote systems that serve as the tunnel endpoints.

Group entity

A group entity is a collection of other network entities. This reduces the number of similar rules by letting the administrator create one rule and apply it to the group instead of creating separate rule for each network entity. For instance, a host entity (single machine) and a subnet entity (several machines) could be combined into a group entity. Only one rule would then be needed to grant access to both entities the host and the subnet.

VPN security entity

A VPN security entity lets you combine a series of subnets and security gateways into a single entity. This single entity can then be used to establish multiple tunnels simultaneously. The advantage to this is that only one tunnel definition has to be described on the security gateway.

Domain Name Service (DNS)

The security gateway includes support for the domain name service (DNS). The security gateway's DNS implementation supports many of the features of standard DNS implementations, including full name resolution and reverse name resolution. DNS configuration on the security gateway may seem a bit more challenging than a standard DNS implementations because the security gateway supports security-conscious DNS configurations only.

There are three primary functions of DNS:

Name resolution	The most common use of DNS is to resolve or translate a given domain name to its equivalent IP address. Computers communicate through numbers, where humans prefer a spoken and written word. DNS lets humans type the alphabetic name of a host, and then translates that name into its numerical equivalent.

Reverse name resolution	The counterpart to name resolution. Instead of typing in an alphabetic name, and figuring out the associated IP address, the DNS system is given the IP address and asked to return the alphabetic name. This is commonly seen with Web servers logging traffic by both host name and IP address.
Mail exchange information	Mail servers use DNS to determine the next machine to forward your email. If your organization has a mail server, email you send is directed at that server first. That mail server then checks to see if the email was addressed to any domain it handles. If the email was addressed elsewhere, that mail server resolves the IP address of the email's destination server. This gives your mail server the information it needs to get the email to its intended recipient.

The security gateway's DNS system consists of different types of records that work together to provide full name and reverse name resolution. Each record type handles different information, from defining a single name server or mail server, to defining entire subnets.

Authority record

An authoritative record defines the name server that is responsible for a given domain. This name server has the physical zone records for the domain, and responds to all DNS requests for zone information. For any given domain, there is only one name server delegated as the authority for a domain.

One common message displayed when an nslookup is performed is that the response is non-authoritative. What this means is that the DNS reply did not come directly from the authoritative name server. Instead, the local or intermediate DNS systems contacted (if applicable) returned a cached version of the record.

Forwarder record

A forwarder record points to an external server used to redirect DNS requests. If you decide that you'd rather not have the security gateway perform DNS lookups, but instead offload this work to another DNS server, configuring a forwarder is the way this is achieved. The DNS proxy still handles the exchange of information between the requesting client and the DNS server the request was forwarded to, passing the original DNS request to the destination DNS server, and then sending the reply back to the client.

If you do not configure any forwarders, the DNS system performs its own lookups, querying a root name server for the domain's authoritative DNS server. Not configuring a forwarder is the recommended approach, unless there is something blocking access to the root servers or other public name servers. For example, if you want to use a public DNS server to answer DNS requests instead of having the security gateway answer them, create a forwarder on the security gateway that points to the external DNS servers.

Host record

A host record identifies either a name or IP address of a host in a given domain. This type of record serves a dual purpose, acting as either an A (address) record, which resolves names to addresses, or a PTR (pointer) record, which resolves addresses to names. You can also assign an alias, or short name, to a host, but these aliases are only resolvable for access requests originating from the security gateway itself. DNS requests originating external to the security gateway must use the fully-qualified host name.

Mail server record

A mail server record identifies the name or IP address of mail servers responsible for handling email addressed to this domain, typically the outside interface of the security gateway. External mail servers use this information when directing email to internal users. You can also configure the DNS system to spool (hold temporarily) your email on an external server until it can delivered. This assures that mail destined for your internal systems eventually gets delivered, even if your internal mail server is down for a short period of time.

Name server record

The DNS system supports defining name servers for a domain. The name server entry marks the authoritative or secondary name servers to consult when performing DNS lookups for a host in that domain. Authoritative and secondary name servers maintain an internal record, called a host record, for each domain they administer.

There are three different types of name servers:

Primary	A primary name server retrieves DNS information from files local to the system after determining that it is authoritative for the requested domain. For domain requests that do not have corresponding records on the local machine, the information is retrieved from other primary and secondary name servers hosting the information. Retrieved information is cached, improving performance for identical lookups later.
Secondary	Secondary name servers are used as backups for primary name servers. A secondary name server can perform the same duties as the primary name server, such as pulling zone information from a primary or another secondary name server. When initialized, the secondary name server copies over all records from the primary name server, and continuously performs incremental checks to stay synchronized with the primary name server. The secondary name server can answer requests for zone information for files it knows about, and cache information for zones it does not directly administer.
Caching only	Caching-only name servers improve DNS performance by caching DNS lookups. A caching-only name server does not administer zone records for any domain; a caching-only name server only caches zone records from previous DNS lookups. For busy name servers, this is a significant improvement in speed. DNS requests that use either a primary or secondary name require the name server to determine who is authoritative for a requested domain, contact that name server, transfer the zone information, and then present the information to the requester. DNS requests that use a caching-only name server actually incur a slight penalty for the first lookup, but are much faster on subsequent lookups for the same zone information. A caching-only name server first looks at its internal cache to see if it already has a copy of the zone information. If a zone record exists, the caching-only name server checks the record expiration time. Expired records are dropped, and the request is handled the same as a new zone request. Records that are still valid let the caching-only name server immediately return the lookup information to the requester. For all new requests, the caching-only name server acts in similar fashion to a primary or secondary name server. The caching-only name server determines who is authoritative for the zone, contacts that name server, and transfers the zone record. However, prior to presenting this information to the requester, the caching-only name server caches a copy of the zone record locally.

Note: You can only configure the security gateway to act as a primary name server.

Recursion record

It is never advisable to permit the use of the security gateway as a public DNS server. In some locations, however, hosts or servers may reside external to the security gateway, and require the use of the security gateway's DNS system. For example, a Web Server sitting in an external DMZ may have a public address, and may need to use the security gateway as its primary name server. Because the interface the Web server connects through is public, the default behavior of the security gateway is to drop any DNS request received that the security gateway is not authoritative for; that is, the security gateway does not recurse (use another server) for the information.

Configuring a recursion record instructs the security gateway to perform recursion for requests received from a subnet and directed at a public interface. For the Web server in our example, the subnet defined would be a single host. Now, DNS requests submitted by the Web server would be answered regardless of who is authoritative for the domain, and all other public hosts are still prevented from using the security gateway as a public DNS server.

Root server record

The root name servers are a group of special name servers that are either authoritative for a top-level domain, or clearly know which server is authoritative. DNS lookups begin with the root servers, which send back either the DNS information requested or the name server that can get the requester closer to the DNS information they seek. The root servers are critical to DNS functioning properly. If all of the root servers were unavailable for an extended period of time, Internet DNS resolution would fail.

To reduce lookup time, the security gateway has the current list of root servers hard coded. You can add a root server record if you wish to change the list of servers that DNS uses to find top-level domain information. Adding a new record instructs the security gateway to ignore the hard-coded servers, and use only the defined entry. If the DNS server pointed to in the newly added root server record is unavailable, DNS lookups fail; they do not fall back to the hard-coded list.

Table 3-3 lists all of the current root servers with their respective IP addresses. This list is subject to change. The most current version of this list is found at ftp://ftp.internic.net/domain/named.cache.

Table 3-3 Current root name servers

Fully-qualified domain name	IP address
A.ROOT-SERVERS.NET.	198.41.0.4
B.ROOT-SERVERS.NET.	128.9.0.107
C.ROOT-SERVERS.NET.	192.33.4.12
D.ROOT-SERVERS.NET.	128.8.10.90
E.ROOT-SERVERS.NET.	192.203.230.10
F.ROOT-SERVERS.NET.	192.5.5.241
G.ROOT-SERVERS.NET.	192.112.36.4
H.ROOT-SERVERS.NET.	128.63.2.53
I.ROOT-SERVERS.NET.	192.36.148.17
J.ROOT-SERVERS.NET.	192.58.128.30
K.ROOT-SERVERS.NET.	193.0.14.129
L.ROOT-SERVERS.NET.	198.32.64.12
M.ROOT-SERVERS.NET.	202.12.27.33

Subnet record

A subnet record is used to define a range of IP addresses applicable to a given domain. For example, if an ISP allocated 64 IP addresses for the raptor.com domain, a subnet record could be used to define the range of addresses. Assuming the ISP gave a block of 64 IP addresses, there are four possible starting points at 0, 64, 128, and 192. If we were given the 10.0.5.128 through 10.0.5.191 range of addresses, we would define the IP address as 10.0.5.128 (the beginning of the network) and define the subnet as 255.255.255.192. Defining 192 in the fourth octet masks off the first two bits, yielding only 64 possible different IP addresses. Subnet records are also sometimes referred to as subnet maps.

Note: Your security gateway responds to reverse lookup requests only used when your ISP has delegated the reverse domain to you and you have configured your security gateway as the reverse domain authority for the subnet.

Chapter 4

Understanding access

This chapter includes the following topics:

Network protocols

A protocol is a formal set of rules used when two parties wish to communicate or exchange information. Similarly, a network protocol is a set of communication rules agreed upon by endpoints (computers) for the purpose of transacting a data exchange. Without protocols, it is significantly harder, if not impossible, for different computers to communicate with one another.

The security gateway predefines the most commonly used protocols, including their respective ports and the expected packet type (TCP, UDP, IP, or ICMP). These predefined protocols are used singly or in combination in a rule, but you cannot change or delete them. You can define additional custom protocols which may be necessary for custom applications.

Protocols with a proxy

These protocols represent services commonly used in an IP network. Each standard protocol is predefined in the security gateway software, and has an individual application-specific proxy associated with it. Examples include DNS, FTP, HTTP, and Telnet. Table 4-1 shows a complete list of supplied protocols and their associated application proxy.

Table 4-1 Supplied protocols with their associated application proxy

Protocol name	Type	Port	Associated proxy
cifs	TCP/UDP-based	139	CIFS
dns_tcp	TCP/UDP-based	53	DNS
dns_udp	TCP/UDP-based	53	DNS
dns_udp_s2s	TCP/UDP-based	53	DNS
exec	TCP/UDP-based	512	RCMD
ftp	TCP/UDP-based	21	FTP
h323	TCP/UDP-based	1720 (UDP 20000 - 30000)	H323
http	TCP/UDP-based	80	HTTP
ICMP	IP-based	---	Ping

Table 4-1 Supplied protocols with their associated application proxy (Continued)

Protocol name	Type	Port	Associated proxy
icmp_dest_unreachable	ICMP-based	---	Ping
icmp_echo_reply	ICMP-based	---	Ping
icmp_echo_request	ICMP-based	---	Ping
icmp_src_quench	ICMP-based	---	Ping
icmp_time_exceeded	ICMP-based	---	Ping
login	TCP/UDP-based	513	RCMD
netbios_138_udp	TCP/UDP-based	138	NBDGRAM
netbios_139_tcp	TCP/UDP-based	139	CIFS
nntp	TCP/UDP-based	119	NNTP
ntp	TCP/UDP-based	123	NTP
ping	IP-based	---	Ping
realaudio	TCP/UDP-based	7070	RealAudio
realaudio_proxy	TCP/UDP-based	1090	RealAudio
realaudio_udp	TCP/UDP-based	6970	RealAudio
rtsp	TCP/UDP-based	554	RTSP
shell	TCP/UDP-based	514	RCMD
smb	TCP/UDP-based	445	CIFS
smtp	TCP/UDP-based	25	SMTP
telnet	TCP/UDP-based	23	Telnet

Protocols without a proxy

These protocols represent services less commonly used in an IP network. Each standard protocol is defined, but is not associated with an application-specific proxy. Table 4-2 shows a complete list of supplied protocols that have no associated application proxy.

Table 4-2 Supplied protocols with no associated application proxy

Protocol name	Type	Port
AH	IP-based	---
AIM	TCP/UDP-based	5190
auth	TCP/UDP-based	113
bftp	TCP/UDP-based	152
bgp	TCP/UDP-based	179
biff	TCP/UDP-based	512
biff_rev	TCP/UDP-based	1024
chargen_tcp	TCP/UDP-based	19
chargen_udp	TCP/UDP-based	19

Table 4-2 Supplied protocols with no associated application proxy (Continued)

Protocol name	Type	Port
chargen_dup_rev	TCP/UDP-based	1024
daytime_tcp	TCP/UDP-based	13
daytime_udp	TCP/UDP-based	13
daytime_udp_rev	TCP/UDP-based	1024
discard_tcp	TCP/UDP-based	9
discard_udp	TCP/UDP-based	9
dns_udp_rev	TCP/UDP-based	1024
echo_tcp	TCP/UDP-based	7
echo_udp	TCP/UDP-based	7
echo_udp_rev	TCP/UDP-based	1024
EGP	IP-based	---
EON	IP-based	---
esm_agent	TCP/UDP-based	5601
esm_mgr	TCP/UDP-based	5600
esm_rem_install	TCP/UDP-based	5599
esm_rev_install	TCP/UDP-based	1025
ESP	IP-based	---
finger	TCP/UDP-based	79
gopher	TCP/UDP-based	70
gwproxy	TCP/UDP-based	416
hawk	TCP/UDP-based	418
HELLO	IP-based	---
hsrp	TCP/UDP-based	1985
IGMP	IP-based	---
imap	TCP/UDP-based	143
IPinIP	IP-based	---
IPIP	IP-based	---
irc_6665	TCP/UDP-based	6665
irc_6666	TCP/UDP-based	6666
irc_6667	TCP/UDP-based	6667
irc_6668	TCP/UDP-based	6668
irc_6669	TCP/UDP-based	6669
irc_7000	TCP/UDP-based	7000
isakmp	TCP/UDP-based	500
iso_tsap	TCP/UDP-based	102

Table 4-2 Supplied protocols with no associated application proxy (Continued)

Protocol name	Type	Port
ita_admin	TCP/UDP-based	3833
ita_agent	TCP/UDP-based	5052
ita_mgr	TCP/UDP-based	5051
ita_view	TCP/UDP-based	3834
kerberos_auth_88	TCP/UDP-based	88
kerberos_tcp	TCP/UDP-based	750
kerberos_udp	TCP/UDP-based	750
kerberos_udp_rev	TCP/UDP-based	1024
ldap	TCP/UDP-based	389
lockd_tcp	TCP/UDP-based	4045
lockd_udp	TCP/UDP-based	4045
lockd_udp_rev	TCP/UDP-based	1024
netbios_137_tcp	TCP/UDP-based	137
netbios_137_udp	TCP/UDP-based	137
netbios_138_tcp	TCP/UDP-based	138
netbios_139_udp	TCP/UDP-based	139
netmeeting_audio_control	TCP/UDP-based	1731
netstat	TCP/UDP-based	15
nfsd_tcp	TCP/UDP-based	2049
nfsd_udp	TCP/UDP-based	2049
nfsd_udp_rev	TCP/UDP-based	1024
nsetupd	TCP/UDP-based	420
pcserver	TCP/UDP-based	600
pop-2	TCP/UDP-based	109
pop-3	TCP/UDP-based	110
printer	TCP/UDP-based	515
PUP	IP-based	---
RAW	IP-based	---
readeagle	TCP/UDP-based	414
readhawk	TCP/UDP-based	418
realaudio	TCP/UDP-based	7070
realaudio_proxy	TCP/UDP-based	1090
realaudio_udp	TCP/UDP-based	6970
rip	TCP/UDP-based	520
SGMI	TCP/UDP-based	2456

Table 4-2 Supplied protocols with no associated application proxy (Continued)

Protocol name	Type	Port
sip	TCP/UDP-based	5060
sip_udp	TCP/UDP-based	5060
snmp	TCP/UDP-based	161
snmptrap	TCP/UDP-based	162
socks	TCP/UDP-based	1080
srl	TCP/UDP-based	423
sunrpc_tcp	TCP/UDP-based	111
sunrpc_udp	TCP/UDP-based	111
syslog	TCP/UDP-based	514
systat	TCP/UDP-based	11
t120	TCP/UDP-based	1503
tacacs	TCP/UDP-based	49
TCP	IP-based	---
tftp	TCP/UDP-based	69
UDP	IP-based	---
udp_encap	TCP/UDP-based	786
uucp	TCP/UDP-based	540
visualizer	TCP/UDP-based	417
wapdgram	TCP/UDP-based	9200
who	TCP/UDP-based	513
whois	TCP/UDP-based	43
x-server0	TCP/UDP-based	6000
x-server1	TCP/UDP-based	6001

Custom protocols

A custom protocol is any generic protocol defined to manage traffic flow through the security gateway. Once you define custom protocols, you can use them in authorization rules along with the standard services the security gateway supports. To use a protocol with authorization rules, you must associate it with a proxy. The associated proxy may be one of the individual built-in proxies, or one of the generic server proxies (GSPs).

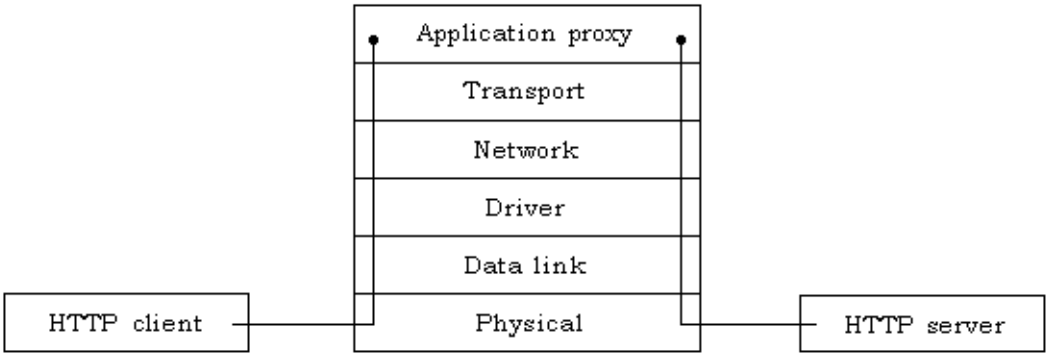
Note: You can use any protocol, whether it is predefined or custom, in filters.

Proxies

The security gateway includes several stack-based application proxies that act as both a server and a client, accepting connections from a client and making requests on behalf of the client to the destination server. Application proxies provide protocol-specific security checks that normally are not implemented in the client or server software. Some proxies can also be configured to scan content for viruses and inconsistencies.

To illustrate how a proxy acts as both a client and server, Figure 4-1 shows a sample HTTP connection using the HTTP proxy. Notice that having a proxy intervene actually causes two connections, even though the appearance to the client and server is one connection. When the application proxy receives a new connection request, it answers, making itself the server for the connection. The application proxy then initiates the same request to the true destination server. The proxy interprets replies received from the server, and retransmits those replies to the client.

Figure 4-1 An application proxy creating two separate connections



Application data scanning

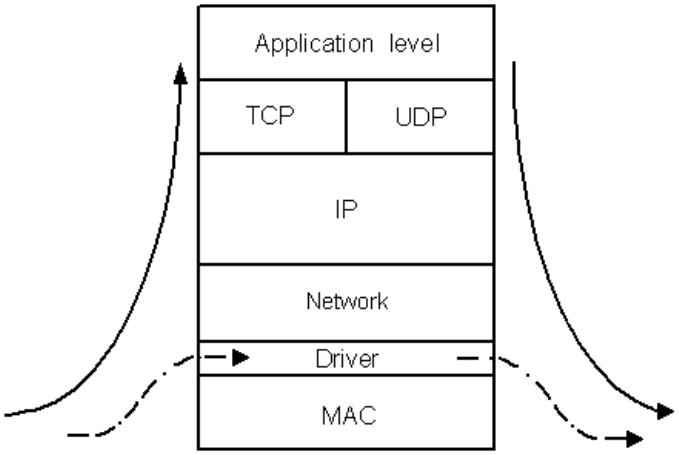
Normally, traffic passed to the HTTP proxy undergoes a rigorous examination, ensuring that data complies with defined RFCs. For performance reasons, though, it may sometimes be advantageous to eliminate some of the packet examination performed by the HTTP proxy, especially if the packets are believed to originate from a trusted source. Disabling application data scanning does exactly this.

HTTP connections are generally short-lived, consecutive connections that originate from the same source. A Web client sends a page request (through their Web browser) and the server responds with the page. In the source HTML for the Web page, there may be multiple image requests for graphics that appear on the Web page. Each one of these requests creates another short-lived connection to the Web server while the graphic is downloaded and displayed on the client. For pages with many graphics, there could be as many as 20 or more requests all originating from the same host.

Disabling application data scanning instructs the HTTP proxy to examine and record the first full connection. Information recorded for the connection includes the source address, the destination address, the destination port, and the protocol. Subsequent connections matching this collected information are not sent up the stack for processing by the HTTP proxy, but instead pass through directly after being processed by the Symantec driver. The security gateway retains this connection information for approximately 60 seconds after the last matching connection, and then removes the record. If a new connection matching the same parameters comes in after the expiration time, the first full connection is once again checked, and a new record created.

Figure 4-2 illustrates what happens when application data scanning is disabled. The first full connection (solid arrow) continues up to the application level to be evaluated. Once verified, subsequent matching connections (dotted arrow) pass through the Symantec driver.

Figure 4-2 Application data scanning disabled



Note: If you disable application data scanning, you cannot take advantage of antivirus protection as the entire data stream does not pass up to the application layer.

HTTP proxy considerations

HTTP page requests make an ideal candidate for disabling application data scanning if performance is slow due to heavy traffic. However, poor HTTP performance could be hardware related. Your interfaces or network connection may be saturated or your ISP may be slow. DNS may not be set up correctly, or timing out on name requests. If your bottleneck is anywhere besides the security gateway, disabling application data scanning weakens your security with no benefit.

Note: If the security gateway has idle CPU time, or plenty of free memory, the performance problem is not the security gateway.

For HTTP connections, you can disable application data scanning only in rules that meet all of the following conditions:

- Does not use rating profiles.
- Does not use MIME type filtering.
- Does not limit by URL or file extensions.
- Is not for a connection that uses an external proxy.
- Does not have antivirus scanning enabled.

The CIFS (SMB) proxy

The Common Internet File System (CIFS) protocol and its predecessor, System Message Block (SMB) protocol, are the network foundation for many Microsoft applications. These applications include file and print sharing, named pipes, network browsing, remote management, NT Domain, DCE RPC, and DCOM. The CIFS/SMB proxy integrates Microsoft networking support into the security gateway environment in a way that makes setup as easy and flexible as possible.

Examples of traffic that the CIFS proxy supports include:

- External users trying to access internal SMB servers from home or the road to read mail, access databases, or access documents. For this type of access, you configure the security gateway to disable write access to the servers. These users connect non-transparently and use service redirection to let the CIFS proxy hide the details about the real SMB servers.
- Internal users trying to access external SMB servers. These types of users only need to connect transparently to the server.

The CIFS proxy does not support authentication of the CIFS/SMB client except through Out of Band Authentication. Additionally, you can create rules that include CIFS just as is done with HTTP, FTP, Telnet, SMTP, NNTP, and other protocols. Table 4-3 lists the configurable options for CIFS.

Table 4-3 Configurable CIFS services

Service	Description
File Reading Allowed	Lets users read files or query attributes of files on an SMB server. This is useful for setting up public directories for download purposes only.
File Printing Allowed	Lets users perform print operations or connect to print shares on an SMB server. (May not work for Windows 2000 clients)
File Renaming Allowed	Lets users and applications rename or move files on an SMB server.
File Writing Allowed	Lets users write or copy files, or create directories on an SMB server. This is useful in setting up public directories for upload purposes only.
File Deleting Allowed	Lets users or applications delete files and directories from the SMB server.
File Access Allowed	Lets users connect to file shares on an SMB server. (May not work for Windows 2000 clients)
File Permission Change Allowed	Lets users and applications change modal attributes of any file on an SMB server.
File Generic Access Allowed	Lets users connect to any shared resource not covered by: ■ File Printing Allowed ■ Pipe Use Allowed ■ File Access Allowed ■ COM Port Access Allowed Some CIFS clients use generic access to connect to CIFS servers for administrative purposes. In general, they connect to server-namePC$ with a target of "$$$$" (the generic device). The connection to the IPC$ share on the server lets the server validate the client as existing in the domain. If you want to prevent this type of traffic from passing through the security gateway, uncheck this option. However, if you disable this option, and the client and server are in different domains, file and print sharing between client and server will not work.
File Directory Access Allowed	Lets users and applications obtain directory listings.
Pipe Use Allowed	Lets applications use named pipes over an SMB connection. Name pipes are used for a variety of applications, such as remote management, network printer sharing, and SQL server (using default transport). If you uncheck Pipe Use Allowed, you cannot pass traffic from these applications through the security gateway. If you do not want your inside servers remotely managed from the outside, and you have CIFS enabled, uncheck this option.
COM Port Access Allowed	Lets users connect to shared communication devices (such as serial ports).
SMB Operation Logged	Causes the CIFS daemon to perform an audit log of all SMB operations attempted. This causes performance degradation under heavy loads, but lets you see what files are being read, modified, or deleted on each SMB server. This can be used to supplement the audit logs on Microsoft Windows server platforms. This option also increases the size of the security gateway log file.

Table 4-3 Configurable CIFS services (Continued)

Service	Description
Kerberos Authentication Allowed	Microsoft Windows 2000 uses Kerberos as an authentication method for any connecting systems. You should enable this option should if you are granting CIFS access in a rule, and the destination is a Microsoft Windows 2000 network.

Transparent connections

The CIFS proxy supports transparent connections through the security gateway. With transparent connections, it is the target SMB server's responsibility to perform any required user authentication. The client must know the name of the SMB server and the name of its shares, because browsing through the security gateway is disabled.

Non-transparent connections

For non-transparent connections, a user connects to the security gateway, and the security gateway acts as the SMB server. The SMB protocol does not support connection redirection so you must configure the security gateway to perform service redirection for CIFS.

The CIFS proxy uses network address translation (NAT) for non-transparent connections. Because the share name is of the form firewallxx, the name is changed to the form redirected-host-namexx before being forwarded to the real SMB server.

Despite the NAT functionality, however, internal share names like xxx are exposed to the outside. To avoid exposure, go to each SMB server and create alias share names for the same directory but create different permissions for the shares that are to be exposed. These new permissions are set up to give less control to outside users, if so desired.

Restrictions

Restrictions that relate to the security gateway CIFS proxy include the following:

- The CIFS proxy is not an integrated SMB server and SMB proxy. Do not use in conjunction with a real SMB server running on the security gateway.
- The CIFS proxy does not support UDP port 137, which is used by the NetBIOS naming service. This means that users cannot browse for any SMB servers behind the security gateway. Therefore, users must use other naming services to access the security gateway and the SMB servers inside.
  SMB clients can enable DNS for Windows name resolution. To use DNS for transparent access to SMB servers inside the security gateway, the administrator can use the Security Gateway Management Interface (SGMI) to add entries for the SMB servers to the public hosts file.
- The CIFS proxy does not support UDP port 138 (NetBIOS datagram service). This service is used by some Microsoft applications, most notably NT Domain Controllers, to locate certain types of servers. If you want to communicate with domain controllers through a security gateway, you should use the NetBIOS datagram proxy when creating your rule for this type of access.

You may also have to enable client side transparency on the inside interface for the inside domain controller and enable it on the outside interface for the outside domain controller.

The DNS proxy

By default, the security gateway responds to DNS queries received on the loopback adapter (127.0.0.1) and any internal interfaces defined during setup. This means that clients on the protected network should never point directly to a public DNS server. If an internal DNS configuration is already present, clients on the protected network should point to the internal DNS server for all DNS requests. Similarly, internal DNS servers should not point directly to a public system for resolution. Instead, they should configure forwarders that point to the security gateway. If there is no internal DNS system, clients on the protected network should point directly at the inside interface of the security gateway.

Note: A check of the DNS settings should show that 127.0.0.1 is listed as the first name server. It is recommended that you have 127.0.0.1 as the only entry in the list so failed DNS lookups immediately signal a problem with the DNS proxy.

Private and public zone files

Public hosts are defined as any host that connects to the security gateway through a public interface (any interface not marked as private). For example, hosts on the Internet or on a service network are considered public hosts. Private hosts are defined as any host that connects to the security gateway through a private interface. A common example of a private host is an employee's workstation.

The DNS proxy can host both public and private DNS records. Private host records are intended for internal use, and are never broadcast to public hosts. Public records are seen by both public hosts and private hosts. Therefore, access to these records depends on whether the requesting host is public or private.

Public and private DNS requests arriving at an interface marked as private are honored. Public DNS requests arriving at a public interface are answered only if the security gateway has a matching public host record. By default, any requesting host not connected to a private interface can only issue public DNS requests; they cannot have access to private DNS information. A public interface can be configured to expose private DNS information, but this is not commonly done.

Note: Inside and private do not mean the same thing. You can define an inside interface as public. For example, you may wish to define the inside interface facing a service network as public. However, before changing an inside interface, consider your licensing level. Each new connection from the security gateway to the network connected to that inside interface counts against your available licenses.

Using internal name servers

If you configured internal name servers to act as backups for the DNS proxy, do not point the security gateway's resolver to the internal name servers. Instead, the resolver should always point to 127.0.0.1 (localhost) either solely or as the first entry. The DNS proxy should always try to look at the security gateway first when performing a DNS lookup. The only time that the internal name servers are used is when the DNS proxy is unable to handle the request.

Note: The DNS proxy cannot serve as a secondary name server. The DNS proxy can only serve as a primary name server.

The proper way to configure the DNS proxy to use internal name servers is to delegate through the DNS proxy's zone files. For example, let's define 192.168.1.10 and 192.168.1.20 as our internal name servers, and let's say that they are authoritative for three zones:

myco.org	Forward zone for myco.org
1.168.192.in-addr.arpa	Inverse lookup table for zone 192.168.1.0/24
16.172.in-addr.arpa	Inverse lookup table for 172.16.0.0/16

You set up the DNS proxy's private zone file to delegate to the internal name servers for any of the above. You start with six entries:

- 192.168.1.10 ns1.myco.org #nsfor myco.org
- 192.168.1.10 ns1.myco.org #nsfor 1.168.192.in-addr.arpa
- 192.168.1.10 ns1.myco.org #nsfor 16.172.in-addr.arpa
- 192.168.1.20 ns2.myco.org #nsfor myco.org
- 192.168.1.20 ns2.myco.org #nsfor 1.168.192.in-addr.arpa
- 192.168.1.20 ns2.myco.org #nsfor 16.172.in-addr.arpa

This pre-populates DNSd's cache with the following information:

; delegation NS records	
myco.org.	IN NS ns1.myco.org.
	IN NS ns2.myco.org.
1.168.192.in-addr.arpa.	IN NS ns1.myco.org.
	IN NS ns2.myco.org.
16.172.in-addr.arpa.	IN NS ns1.myco.org.
	IN NS ns2.myco.org.

Now, when a name in any of the three zones is sought, the resolver queries the DNS proxy cache. The DNS proxy then does one of the following:

- If the DNS proxy has resolved the query once before, it doesn't have to burden the internal name servers with a redundant query. The current information is pulled from the DNS proxy's cache.
- If there is no record in cache, the DNS proxy looks up the authoritative name servers for the zone. From the records above, the DNS proxy knows where to send the request. Unlike a resolver, though, the DNS proxy is a bit smarter. It first checks round-trip times (RTT) of queries to the name servers, and uses the one with the best response. This contributes to name lookup efficiency and load balancing.

The FTP proxy

The file transfer protocol (FTP) is commonly used to transfer files from one location to another. FTP normally works through a pair of connections between a client and a server. The FTP proxy supports the FTP protocol, and lets the administrator refine connections to allow both PUT and GET commands (default), PUT commands only, or GET commands only.

The FTP proxy is configurable to block connections based on length of user names and passwords. The default is 32 characters for both user name and password, with the maximum being 256 characters. This feature provides protection against user name/password buffer overflow attacks. The default logon banner, Secure Gateway FTP Server, can also be changed to minimize the risk of identifying the security gateway's presence.

By default, the FTP proxy protects against bounce attacks. The FTP proxy logs and disconnects the control and data connections from an offending client if the client tries to send a PORT command for an address that does not match the client's address. The FTP proxy does not overwrite the PORT command with its own address if the address on the PORT command is not the client's address.

The H.323 proxy

H.323 is a standard for Internet audio, video, and data communications. Programs using the H.323 standard can communicate and inter-operate with other compliant systems in a peer-to-peer network. You can configure the security gateway to act as a virtual peer accepting requests for this type of traffic, and then passing them on to the H.323 endpoint located behind the security gateway.

The security gateway does not support all elements of the H.323 standard. The following features are not supported:

Multicast addressing	The security gateway supports only unicast addressing (several point-to-point transmissions).
LDAP	Online Directory Lookup uses the LDAP protocol to look up addresses at an LDAP server.

You can maintain an inside directory server for your site. You can populate this server with addresses from a public server or with your inside addresses and addresses of business partners and associates. Have your users set this server as their default directory server.

The HTTP proxy

The HTTP proxy operates as a non-caching proxy between Web clients and servers. The HTTP proxy supports all major features of HTTP 1.1, and also acts as a local Web server with its own document set. The server primarily fulfills requests for the security gateway's home page and icons used in the protocol converters, but the administrator can place any files desired into the document area.

HTTP proxy authorization

No request is fulfilled until that request is authorized. The security gateway evaluates the source IP address, source interface, destination IP address, and destination interface. The result indicates whether the request can proceed, whether authentication is required, and what other limits apply, such as content restrictions or the proxy server to use for the rule.

The HTTP proxy does not solely rely on gwcontrol to make its authorization decisions. It looks at other factors in the request such as whether or not the request is protocol-compliant. The HTTP proxy also restricts requests from contacting servers on many low numbered ports. A request is allowed only after all authorization checks are complete, including authentication and content filtering.

HTTP proxy authentication

Client connections may require authentication. The HTTP proxy determines whether to use proxy authentication or HTTP authentication. If the HTTP proxy selects and the client's browser supports proxy authentication, the HTTP proxy issues a challenge to the client's browser indicating that proxy authentication should be used. You need to enter the required user name and password combination needs to be entered only once for each browser session.

Secure sockets layer

The security gateway HTTP proxy passes secure HTTP traffic using secure sockets layer (SSL) transparently or by what Netscape refers to as SSL tunneling. Requests are authorized in the same way as standard HTTP requests except that the proxy cannot see the full URL. This means that content filtering is limited to a ratings check based on the destination IP and host name, if available. User authentication cannot be performed on transparent SSL connections because the entire session is encrypted and user information is not available to the HTTP proxy.

Transparent SSL connections are normally received on port 443. Additional ports are defined in the properties window for the HTTP proxy.

Note: Entering an SSL port in the service group Parameters for HTTP dialog only will not open the desired port on the security gateway. Ports defined there are for authorization purposes only. You must also define the SSL port in HTTP proxy.

Persistent HTTP connections

A persistent HTTP connection uses a single connection between a Web client and a Web server to fulfill multiple HTTP requests. It reduces network load by reducing the number of packets that need to pass through the network for a number of HTTP requests. Most Web pages require additional HTTP objects from the same site for inline image support. Also, more than one HTML page is usually downloaded from a single site during a visit Netscape introduced in HTTP 1.1 the concept known as HTTP keep-alive to efficiently deal with this situation.

Persistent HTTP connections and pipelining of requests are supported and used by default. Pipelining lets the client send multiple requests as it would over a standard persistent connection without waiting for responses. This enhances HTTP performance considerably, unless application data scanning has been disabled.

WebDAV support

The HTTP proxy supports Web Distributed Authoring and Versioning (WebDAV). WebDAV is a set of additional methods that support version control for URLs, enabling distributed source control applications to be built using HTTP as the wire protocol.

RFC 2518 defines the set of extensions to the HTTP protocol to support WebDAV. The HTTP proxy fully supports the following three extensions:

Overwrite prevention	Provides the ability to let only one person work on a document at a time. This prevents the lost update problem in which modifications are lost as first one author makes changes, and then another author makes changes before merging in the first author's changes.
Properties	Also referred to as metadata, this extension provides the ability to create, remove, and query information about a Web page, such as its author, or creation date. This feature also enables the user to link pages of any media type to related pages.
Name space management	Provides the ability to copy and move Web pages, and to receive a listing of pages at a particular hierarchy level, much like a directory listing in a file system.

WebDAV support is integrated into several authoring tools, such as Microsoft Word, Excel, and PowerPoint from the Microsoft Office 2000 suite, Adobe Acrobat, Photoshop, Go Live, and Macromedia Dreamweaver. Microsoft Internet Explorer, Microsoft Outlook and Microsoft Windows 2000 use WebDAV extensions, called Web folders, to support viewing a Web server as a network disk.

The NBDGRAM proxy

The NetBIOS Datagram proxy transports NetBIOS traffic over UDP port 138. The proxy modifies the NetBIOS header to contain the correct source IP address and port number as seen by the recipient of the packet. This solves the problem of NetBIOS being unable to respond to received packets because the specified source in the NetBIOS header is not the actual source of the UDP packet.

This proxy is useful in cases where NetBIOS services need to pass through the security gateway, but some sort of non-standard routing or address hiding is in effect.

The NNTP proxy

Network news transfer protocol (NNTP) has existed since 1986, and NNTP news servers have long been the targets of attacks. Much of this is because the management of news servers has, until recently, been unauthenticated. Anyone with access to a Telnet utility can connect to a news server and type in news articles or commands in an attempt to corrupt the USENET newsgroups.

The NNTP proxy lets the administrator regulate what articles are sent and received from news servers.

Usage scenarios

There are several possible traffic patterns that the NNTP proxy can accommodate:

- Users on the protected network accessing public news servers. You may want to filter the newsgroups users can access (by newsgroup name or by IP address). You may want to disable posting of new articles. You may want to authenticate users or restrict the time of day they can access newsgroups.
- Users on the protected network accessing internal news servers. Internal news servers get feeds from external news servers. You may want to control which newsgroups are downloaded between servers and what time of day the downloads can occur. You may want to authenticate the external news server or allow only external news servers with specific IP addresses to feed the internal news server.
- Users outside of the protected network accessing internal news servers. You want to authenticate the users because they are likely employees at home or on the road trying to access the internal news server.

Note: The following commands are not supported by the NNTP proxy: CHECK, TAKETHIS, XINDEX, XPATH, XROVER, XTHREAD.

NNTP proxy authentication

The NNTP proxy supports only those authentication systems that do not require the proxy to interact with the user. For example, the NNTP proxy supports gateway password and RSA SecurID authentication schemes, but Bellcore S/Key is not supported.

When news readers prompt users for names and passwords, they normally do not indicate what kind of password is being requested (although the NNTP protocol gives them enough information to do so). However, it is possible to type challenge-less one-time passwords as the clear-text password, as long as the user knows ahead of time what kind of scheme is being used. The NNTP proxy simply passes the user name and password into whatever authentication scheme is enabled for the rule.

It is also possible for both the security gateway and the news server to require authentication. The security gateway also requires a news server to authenticate before allowing a news feed.

The NTP proxy

The network time protocol (NTP) synchronizes the time of a computer client or server to another server or reference time source. The NTP proxy provides client accuracies typically within a millisecond on LANs and up to tens of milliseconds on WANs relative to a primary server synchronized to coordinated universal time (CUT) by means of a global positioning service (GPS) receiver, or some similar mechanism.

The ping proxy

By default, ICMP packets hitting the security gateway are dropped, as the security stance of an unmodified system is to appear invisible on the network. However, it is often advantageous to have the security gateway respond to ICMP requests, especially when testing or troubleshooting. The ping proxy provides a mechanism for the security gateway to respond to ICMP requests

The ping proxy does not pass the actual ICMP packets through the security gateway; like all other proxies, the security gateway pings the ultimate destination itself. The security gateway does not include the original client data payload in the echo request to the real destination. Instead, the ping proxy constructs a new echo request with a new sequence number, time-to-live (affecting traceroute), and new optional data so that other protocols cannot be tunneled on top of the ICMP echo. If the security gateway receives an ICMP echo request through a tunnel, and that tunnel is not forcing traffic through the proxies, the packets are permitted to pass unmodified. If the security gateway is the target of the ICMP echo request, the ping proxy responds to the client normally.

Some ping clients (traceroute, for example) have an option to specify a source route or to record the route taken. By default, the ping proxy has these features turned off for security reasons, since they could compromise information about your inside networks. A ping request using one of these features is dropped and logged. Support for this is re-enabled by adding the variable ping.preserve.ttl to the Advanced Services tab.

The RCMD proxy

RCMD provides a greater level of security for the rsh, rlogin, and rexec protocols than is obtained by using a GSP. Proxying these connections through RCMD, as opposed to a GSP, offers tighter port usage control and facilitates interactive strong authentication, which would not otherwise be available. For example, by using the proxy, you can configure S/Key authentication for the connection.

RCMD supports three services commonly used by UNIX users:

rexec Use in a rule when you want to let a user execute commands on a UNIX system. The commands are entered from a remote machine, but executed on the UNIX system.

rlogin Used to let a user remotely log on to another UNIX system. The logon credentials reside on and should be applicable to the remote machine, not the machine from which the user is executing the command.

rsh Lets a user open a remote shell on another machine from their host system, and interact with that remote machine. All commands entered in the remote shell are executed on the remote machine.

The RTSP proxy

The Real-Time Streaming Protocol (RTSP) proxy handles real-time data such as the audio and video produced by RealPlayer and QuickTime. Sources of data can include both live data feeds and stored clips. The RTSP specification (RFC 2326) establishes and controls either single or several time-synchronized streams of continuous media such as audio and video. It does not typically deliver the continuous streams itself. Rather, RTSP acts as a network remote control for multimedia servers.

There is no notion of an RTSP connection; instead, a server maintains a session labeled by an identifier. An RTSP session is in no way tied to a transport-level connection such as a TCP connection. During an RTSP session, an RTSP client may open and close many reliable transport connections to the server to issue RTSP requests. Alternatively, it may use a connectionless transport protocol such as UDP.

While the RTSP protocol is intentionally similar in syntax and operation to HTTP, an RTSP server needs to maintain state by default in almost all cases, as opposed to the stateless nature of HTTP.

The SMTP proxy

The SMTP proxy supports transparent, bi-directional access for email connections through the security gateway. Like other security gateway proxies, the SMTP proxy accepts or rejects delivery of email on a connection-by-connection basis, subject to the existence of authorization rules. You can configure the SMTP proxy to check each email connection and scan for known email-based forms of attack.

The SMTP proxy, however, is not a full-fledged mail system and does not store email. If you operate an internal SMTP server, it is recommended that you configure this internal server to resolve external SMTP servers through DNS, and that you set its default route to pass through the security gateway. All that is required then is to create a rule to allow the traffic, letting the internal SMTP server access any SMTP servers. If you are unable to set your internal SMTP server's default gateway to the nearest security gateway interface, possibly due to an internal routing situation, be careful not to point to the security gateway for any store-and-forward operations.

You can also redirect internal requests to an external server by pointing the internal SMTP server to the nearest interface of the security gateway, creating a service redirect on the security gateway, and creating a rule to allow the traffic. However, this approach has the drawback that if the external SMTP server fails, mail is not delivered, and more importantly, is not spooled.

Note: Because the SMTP proxy does not store email, the security gateway itself is not vulnerable to email-based attacks.

Supported commands

Most mail servers use a series of four-letter commands to send and receive email. Table 4-4 shows the supported SMTP and ESMTP commands by the Symantec SMTP proxy.

Table 4-4 Supported SMTP commands

Command	Description
HELO	Identifies the SMTP client to the SMTP server. The argument field contains the fully-qualified domain name, if one is available. This command announces that the SMTP client supports the regular SMTP command set.
MAIL	Initiates a mail transaction in which mail is delivered from the SMTP client to the SMTP server. The argument field contains a reverse path and may contain optional parameters if ESMTP is supported.
RCPT	Identifies an individual recipient's data; multiple recipients in a mail header are addressed with multiple uses of this command. The argument field contains a forward path and may contain optional parameters.
DATA	Tells the SMTP recipient that what follows is data or the message body. The recipient looks for a line with only a period on it as the signal that the data has ended.
RSET	Aborts the current mail transaction. There are no arguments for this command.
NOOP	Specifies no action other than that the receiver should send an OK reply. Does not affect any parameters or previously entered commands.
VRFY	Asks the receiver to confirm that the argument identifies a user or mailbox. This command has no affect on the reverse-path buffer, forward-path buffer, or the mail-data buffer.
EXPN	Asks the receiver to confirm that the argument identifies a mailing list, and if so, to return membership of that list. This command has no affect on the reverse-path buffer, forward-path buffer, or the mail-data buffer.
QUIT	Specifies that the receiver must send an OK reply, and then close the transmission channel.

Extended SMTP

The SMTP proxy also supports extended SMTP (ESMTP) commands, by this support must be enabled. Defined in RFC 2821, ESMTP is a set of extensions to SMTP. Table 4-5 lists the SMTP extensions the Symantec SMTP proxy supports.

Table 4-5 Supported ESMTP commands

Command	Description
EHLO	Identifies the SMTP client to the SMTP server. The argument field contains the fully-qualified domain name, if one is available. This command announces that the SMTP client supports the Extended SMTP command set, and is inquiring if the SMTP server does the same.
ESMTP	Provides access to the Extended Simple Mail Transfer Protocol. ESMTP is enabled by default. When it is enabled, the other service extensions on this tab are enabled.
AUTH	Lets the client send user name and password to authenticate with the server. Authentication is enabled by default.
ATRN	Permits an on-demand mail relay from the server to the client by turning the existing connection around. ATRN is disabled by default. Note that the security gateway does not support authentication mechanisms that result in the connection being encrypted.
ETRN	Lets the client access mail. In this case, the server is requested to initiate a separate connection to the client for the purpose of mail relay from the server to the client. ETRN is disabled by default.
EXPN	Allows for the expansion of mailing lists. EXPN is disabled by default. Enabling this option exposes information about your internal network to untrusted sites and is therefore not recommended.
VRFY	Allows verification of mail addresses. VRFY is disabled by default. Enabling this option exposes information about your internal network to untrusted sites and is therefore not recommended.

SMTP proxy communication

When interacting with your mail exchange server, whether it be connecting, performing various mail related functions, or closing a connection, the server responds with a code. These codes tell other mail servers and mail clients how to behave. Table 4-6 provides a brief description of the codes that might be returned by an SMTP server.

Table 4-6 SMTP return codes

Code	Description
211	A system status message.
214	A help message for a human reader follows.
220	Service ready.
221	Service closing.
250	Requested action taken and completed.
251	The recipient is not local to the server, but the server accepts and forwards the message.
252	The recipient cannot be verified, but the server accepts the message and attempts delivery.
354	Start message input and end with ".". This indicates that the server is ready to accept the message itself.
421	Service is not available and the connection will be closed.
450	The requested command failed because the user's mailbox was unavailable.
451	The command was aborted due to server error.

Table 4-6 SMTP return codes (Continued)

Code	Description
452	The command was aborted due to insufficient system storage.
500	The server could not recognize the command due to syntax error.
501	A syntax error was encountered in command arguments.
502	This command is not implemented.
503	The server has encountered a bad sequence of commands.
504	A command parameter is not implemented.
550	The requested command failed because the user's mailbox was unavailable.
551	The recipient is not local to the server.
552	The action was aborted due to exceeded storage allocation.
553	The command was aborted because the mailbox name is invalid.
554	The transaction failed.

Hard and soft limits

The SMTP proxy lets the administrator set hard and soft limits for recipients in email messages. This feature is used to help the proxy prevent against mail spamming.

A soft limit sets the maximum number of recipients in an email header that are accepted at one time. If the number of recipients exceeds the soft limit, the first group of recipients, equal to the soft limit, is sent out. The SMTP proxy then sends a 452 error back to the SMTP server. It is up to the server how it deals with the error. Generally, the SMTP server resends the email with a modified list of recipients that no longer includes the addresses that were already successfully sent. The effect a soft limit has is to throttle the SMTP proxy, sending emails out in small batches of recipients instead of flooding a large number of recipients all at once.

A hard limit defines a maximum number of recipients permitted in an email message header. An email sent with a number of recipients larger than this hard limit is blocked, and a corresponding code is sent back telling the SMTP server that the SMTP proxy denied the message. Again, it is up to the SMTP server how it handles the response from the SMTP proxy. Hard limits should be used to prevent spamming or to limit the size of company mailings. The soft limit takes precedence when both the soft limit and hard limits are set.

Note: An SMTP server may not define the number of recipients in the header, but instead, embed the number in the message. You should enforce hard limits at the SMTP server.

The Telnet proxy

Similar to most of the other proxies, the Telnet proxy performs forward and reverse lookups on the source IP address of the connection attempt. If the results of the lookups are not consistent, the proxy suspects DNS contamination and drops the connection.

If the Telnet proxy accepts the lookup information and the connection is non-transparent, the Telnet proxy prompts the client for the destination host name and (optionally) the destination port. For transparent connections, the destination is already known. When this information is provided, gwcontrol:

- Denies the connection if the destination host name does not exist or is invalid
- Allows the connection without restrictions
- Allows the connection with user, group, or authentication restrictions

If the connection is allowed, but with restrictions, and depending on the authentication method, the Telnet proxy may prompt for a user name and password. If the user name and password are valid, the Telnet proxy then negotiates with the destination machine and begins proxying packets.

When the Telnet proxy authenticates a user using standard gateway passwords, gwcontrol performs the authentication. For other forms of authentication, such as S/Key, the Telnet proxy makes the call itself. If no authentication method is specified for the rule, but users or groups are specified, the Telnet proxy performs multiple authentication, as follows:

- For connections external to the protected network, and destined for the protected network, the Telnet proxy tries S/Key authentication first.
- If the user does not have an S/Key account set up and presses Enter at the S/Key challenge, the Telnet proxy attempts to authenticate using gateway password.
- If the user has an S/Key account, but provides an incorrect password, the connection is refused.

Generic Server Proxy (GSP)

A generic server proxy (GSP) is a mechanism that creates a custom listener for services that are otherwise turned away. A GSP is most commonly used when the security gateway needs to allow requests through for services running on other machines for which there is no supplied application proxy. For example, external requests to an internal Internet Relay Chat (IRC) server would be stopped at the external interface of the security gateway unless a GSP were created to allow that protocol.

Note: GSPs do not provide packet inspection. If an application proxy exists, you should use the application proxy instead of creating a GSP.

Configuration of a GSP involves defining the protocol (which includes both the port and packet type) the service uses. A rule is then created to allow the service through. Once a GSP is created, a record is loaded into the driver with information about the new GSP. If the driver hasn't been notified about a specific port listening for traffic, the packet is normally dropped. Pushing the GSP record into the driver instructs the driver to send the traffic up to the GSP. You can use generic services in authorization rules just as you would any of the services that have a native application proxy.

Note: By default, a GSP handles all requests transparently. These requests are proxied to their destinations as if the requester were directly connected to the destination machine.

Because a GSP is a general purpose proxy, the security gateway does not know in advance for which services it is used. Therefore, no known protocol set is adhered to. As a result of this, if authentication is required for the connection, Out of Band Authentication (OOBA) is the only authentication method permitted.

A GSP is classified by the type of protocol selected. The four choices include IP, TCP, TCPAP (multiple TCP ports), and UDP.

Note: FTP is not supported by TCP GSP as TCP GSP has no intelligence of control and data ports.

Third-party proxies (appliance only)

There are times when you may want to use the security gateway in an environment that supports one or more network technologies for which there is no default application proxy and for which a GSP is insufficient. Examples of this include dynamic routing, dynamic network address assignement through the Dynamic Host Control Protocol (DHCP), or connecting to a standards-based server, such as an Oracle

server. To extend its capabilities, the current Symantec Gateway Security 2.0 release includes support for the following third-party proxies:

- DHCP
- RIP and OSPF
- SQL*Net traffic

When configured, these third-party proxies work seamlessly with the security gateway. The security gateway does not process or handle traffic associated with these proxies. Instead, the security gateway is configured to open the appropriate port for the service, and the listening proxy handles the connection from there.

DHCP relay

By default a security gateway that separates a DHCP client and DHCP server on a DHCP network blocks communication between the DHCP client and the DHCP server. This occurs because the security gateway does not have a standard proxy that listens on port 67 (DHCP) for requests and replies, and is not capable of being a DHCP server itself. The security gateway drops packets for which there is no proxy or service listening.

With the inclusion of the the DHCP relay proxy, you can configure the security gateway to allow DHCP traffic. You can find complete step-by-step instructions to enable support for DHCP in the *Symantec Gateway Security 5400 Series Administrator's Guide*.

GNU Zebra (RIP-2 and OSPF)

In larger envrionments, administrators may use dynamic routing protocols for route propogation and discovery. The two most common dynamic routing protocols are RIP-2 and OSPF. As is the case with the DHCP Relay proxy and the Oracle Connection Manager, the security gateway normally blocks this type of traffic. To support dynamic routing environments using either of these protocols, the security gateway includes the GNU Zebra suite of daemons.

For a complete discussion on the RIP-2 and OSPF protocols, see "Dynamic routing" on page 35.

For step-by-step instructions to enable support for these protocols, consult the *Symantec Gateway Security 5400 Series Administrator's Guide*.

Oracle Connection Manager (SQL*Net)

To support the growing number of business that require secure, public-access to protected Oracle servers using the SQL*Net (Net8) protocol, the security gateway includes a product called the Oracle Connection Manager. The Oracle Connection Manager interacts with the security gateway in a manner similar to the other included third-party applications. You configure the security gateway to open up the correct port, and then configure the Oracle Connection Manager to point to the Oracle server. Once configured, the Oracle Connection Manager listens for incoming SQL*Net connections, and processes them appropriately.

You can find complete step-by-step instructions to enable support for SQL*Net traffic in the *Symantec Gateway Security 5400 Series Administrator's Guide*.

Service groups

A service group is a definition of network traffic that includes one or more protocols. Service groups are used in rules to define the type of traffic to allow or deny, and offer a simple way to group multiple protocols into a single entity. Service groups also let an administrator organize access rights. For example, one service group might have only FTP enabled, another may have FTP, Telnet, and HTTP access, and a third might have full access. Rules can then be created that allow varying degrees of access as appropriate.

A service group consists of the service group name, an assigned ratings profile (if appropriate), both a short and long description, assigned protocols, and any additional parameters. Some of the included protocols assigned to a service group allow additional options to be defined by highlighting the protocol in the Included Protocols window and clicking on Configure. For example, HTTP lets you configure antivirus scanning.

Rules

When the security gateway receives a connection request, it searches for rules that match the time window and definition of the connection request. From this list of possible matches, the security gateway then selects the rule that most closely matches the source address, destination address, protocol, and interface or VPN tunnel. The rule that best fits is then applied; the connection is either allowed or denied. If there are no rules either within the time window or that match to allow the connection, and the connection is not part of a VPN tunnel, the connection is denied.

Note: You should not add a second, return-traffic rule when creating rules. Returning traffic is automatically allowed for connections that match existing rules. Adding a return-traffic rule may open unnecessary holes in the security gateway.

Additionally, there is an implicit rule that lets an administrator initiate a connection from the security gateway. You do not have to create a rule for this, or for the return traffic.

Rule definitions

Rule definitions consist of several editable fields that define such things as the name or number of the rule, whether the rule is active or not, source, destination, description, and so forth. Rules are granular, and rule behavior is modified by changing the appropriate field. Table 4-7 lists each configurable entry, along with its description.

Table 4-7 Rule components

Component	Description
Rule name	Alphanumeric name for the rule. Acceptable characters include letters and numbers only, with no spaces.
Enable	Check box to enable or disable a rule.
Number	Generated number for a rule that shows up in log entries.
Arriving through	Connection point on the security gateway where traffic arrives. This is a selectable list that shows all potential connection points. Selectable options include <ANY> (traffic from anywhere), <ANY VPN> (traffic from any VPN connection), all defined network interfaces, and any Gateway-to-Gateway or Client-to-Gateway VPN tunnels.
Source	Denotes the network entity where traffic should originate. This is a host, subnet, user, group, security gateway, or universe.
Destination	Denotes the network entity where traffic is destined.
Leaving through	Connection point on the security gateway where traffic leaves. This is a selectable list that shows all potential connection points. Selectable options include <ANY> (traffic to anywhere), <ANY VPN> (traffic to any VPN connection), all defined network interfaces, and any Gateway-to-Gateway or Client-to-Gateway VPN tunnels.
Service group	Connections matching this rule are granted access to the services or protocols defined in this group.

Table 4-7 Rule components (Continued)

Component	Description
Action	Determines the action taken by the security gateway when a packet matching this rule arrives. This action is either let the connection continue (allow) or drop the connection (deny). The security gateway denies connections by default, so actions in rules are usually allow.
Caption	Shortened description for the rule. It's recommended that you fill out this field to reduce confusion. This field appears in the main rule window, and offers you a quick way to determine what a rule is for without having to view the properties of each rule.
Time range	Time or date range for which that rule is active. A rule defaults to <ANYTIME> if no time range is specified.
Alert Thresholds	Option that determines if a notification is sent when a certain threshold is reached. Helps you to see if traffic has increased above a certain threshold. Checking this box activates the fields below, letting you modify the defaults for five different time ranges.
Log normal activity	By default, this flag is enabled. This instructs the security gateway to log all traffic, including statistics messages, for this rule. Disabling this option instructs the security gateway to only log warning and error conditions for this rule. You may consider disabling this flag to reduce the number of log messages produced, especially if your log files grow quickly and exceed available disk space.
Application data scanning	Option to scan entire connection for information, or to allow subsequent packets through automatically once initial packets have been verified and the connection deemed valid. Disabling this also disables any configured antivirus scanning.
Stateful failover	Setting this tells the connection for which this rule applies to take advantage of stateful failover. State information for this connection is maintained throughout all nodes on the cluster, and if the node currently handling the connection fails, another node takes charge of the connection, continuing transparent to the user. Stateful failover applies only to HTTP, FTP, Telnet, TCP GSP, and TCPAP GSP connections.
Advanced Services	This screens lets you enter optional parameters to modify the behavior of this rule.
Authentication	Defines the method for authenticating the connection. Checking out-of-band authentication deactivates the authentication drop-down menu.
Description	Optional field that holds more text than the caption field. It's recommended that you fill out this field to reduce confusion. You should use it to keep track of any changes made.

Rule priority

The security gateway performs rule scanning in two passes. In the first pass, the security gateway examines the source address, destination address, destination port, the incoming interface, and the time of day the requested arrived. Gwcontrol then reviews the list of rules to see which match all of these parameters. If there is only one rule that matches, and that rule has no user or authentication configured, it is picked and the appropriate action (allow or deny) taken. For a matching rule that has users or authentication defined, the requesting user is first prompted to enter the appropriate credentials and authenticated before any action is taken.

Gwcontrol will make a second pass only when it finds more than one rule that matches. When gwcontrol finds more than one rule, the first matching rule is chosen. In this case only, how you added the rule to the security gateway determines the rule picked. Therefore, if rule two and five were almost identical and match all of the incoming connection request parameters, rule two is picked.

Note: The order in which rules are added is only a factor when creating many similar rules. In almost every case, this can be avoided by creating rules that do not overlap.

Similar to rules themselves, the rule parameters also have a priority as to which takes precedence. For similarly configured rules, the following order is checked:

- Rules that define a time period (WorkingHours, for example) take precedence over those with no defined time period (<ANYTIME>) when the connection request arrives during that time period. If the connection request arrives outside of the defined time period (trying to access the network on the weekend when WorkingHours is defined, for example), then the rule with <ANYTIME> takes precedence.
- Rules with more source network bits defined rank higher than those with fewer. Therefore, a rule specific to a host is picked before a rule that defines a subnet, and both of these are chosen before a rule that uses the *universe entity. In cases where there is no difference between the number of network bits, entity names are used, with longer names taking priority over shorter ones.
- Rules with source interface restrictions (eth0, eth1, and so forth) have a higher priority than those with no interface restrictions.
- Rules with more destination network bits defined rank higher than those with fewer. Therefore, a rule specific to a host is picked before a rule that defines a subnet, and both of these are selected before a rule that uses the *universe entity. In cases where there is no difference between the number of network bits, entity names are used, with longer names taking priority over shorter ones.
- Rules with destination interface restrictions (eth0, eth1, and so forth) are higher in priority than those with no interface restrictions.
- Rules that explicitly deny traffic supersede matching rules.
- Rules with user restrictions overrule those with no restrictions.
- Rules with authentication override those with no authentication.

This order also defines top-down priority. That is, a rule with a time period takes precedence over a similar rule with authentication.

Rules with groups

The security gateway treats rules with groups as a concatenation of rules using the members of the group. If you have a group with a host entity and a subnet entity and another rule with the same host entity, the two rules have the same priority when evaluating a connection attempt with respect to the host entity. The first rule to appear in the list is the one the security gateway uses. In the case of equivalent rules, the security gateway logs a message indicating the rule it applied. In this case, the order of the rules in the configuration file is significant. You should periodically review your group entities to ensure that there are no conflicts.

Note: Unless you desire to build all rules with the Universe entity (all addresses) as both the source and destination (not advisable), you must create network entities for the specific host or hosts you wish to allow.

Rule authentication

Unless it's the Universe entity, it is not advisable to create an allow rule based only on where the request originates. Rules should have some authentication or extended authentication requirement in addition to matching the source and destination addresses. You can spoof source addresses, and without verifying the user's credentials, you have no guarantee that the user connecting is really who they say they are. Adding an authentication requirement to a rule lets the administrator instruct the connecting user to identify themselves and prove they should have access.

When a connection request matches a rule, the security gateway determines whether or not authentication on that rule is required. If the rule requires authentication and the connecting user identifies themself properly, the connection is permitted. If the user fails to identify themself, the connection is denied, and a message is logged.

Configuration and modification information for rules is found in your product's administrator guide.

Chapter 5

Controlling service access

This chapter includes the following topics:

Filters

Filters let the administrator discard packets that should not be forwarded or serviced locally. A well-constructed filter can reduce a significant portion of undesired traffic, freeing up valuable resources to address legitimate connections. Packet filtering is a versatile security gateway feature that is sometimes considered complicated because packet filters are order-dependent and use different logic from authorization rules, which are based on best fit. Make sure you understand how packet filters work and how to use them before creating any filters.

Understanding filters

A filter is a criteria list and action pairing that consists of the following information:

- The IP address and netmask of the source.
- The IP address and netmask of the destination.
- The type of protocol.
- The lower bound of the source port (if applicable).
- The upper bound of the source port (if applicable).
- The lower bound of the destination port (if applicable).
- The upper bound of the destination port (if applicable).
- Any protocol-related flags (such as TCP ACK).

Each packet is checked against the criteria list to see if there is a match. If the packet matches, the paired action takes place; the action either allows or denies the packet. An allow filter sends the packet up the stack to be processed by the proxies. If the packet does not match, or it matches but the action is deny, the packet is dropped.

A filter is processed sequentially until a match is found. It is important to understand that the filtering mechanism only looks for the first matching entry and takes that action; the order of deny and allow actions is significant. Filters are not like rules, where all rules are considered when making a decision to allow or deny. In general, put the most specific filter elements first and more general elements last.

Note: With no filter list in place, all packets are allowed by default. If a filter is added to the list, the default policy changes to deny anything not specifically allowed by the filter. Any packet that fails to match is dropped. For this reason, filters must be constructed with care.

Types of filters

The security gateway supports the following types of filters:

- Input
- Output
- Forwarding
- VPN
- Filter groups

Input filter

Input filters apply to traffic arriving at a network interface or traffic coming out of a VPN tunnel. An input filter is one of the first incoming packet checks performed. Packets that do not satisfy the filter are dropped before being seen by the proxies or any local applications. The security gateway logs all packets dropped by input filters.

The steps necessary to create an input filter are found in your product's administrator guide.

Output filter

Output filters apply to traffic leaving from a network interface or traffic going into a VPN tunnel. An output filter is one of the last outgoing packet checks performed. Packets that do not satisfy the filter are dropped. Unlike packets dropped by an input filter, packets dropped by an output filter are not logged.

The steps necessary to create an output filter are found in your product's administrator guide.

Forwarding filter

A forwarding filter forwards all allowed packets through the security gateway without first passing the packets to the application layer. Packets not allowed through the forwarding filter continue up the stack to be inspected by the proxies. The behavior of a forwarding filter approaches that of a simple packet-filtering router, but is applied simultaneously to all packets at all interfaces; the filter is applied to both incoming or outgoing packets. Unlike input and output filters which apply at a single interface, forwarding filters apply to all interfaces simultaneously.

Note: A network interface can have separate input and output filters, whereas a forwarding filter has a single filter for both input and output.

A forwarding filter should be a last resort for letting packets through the security gateway. A forwarding filter provides minimal security for allowed packets because packets matching the chosen forwarding filter bypass application-level checks. Forwarding filters are useful under some specific cases, but you should try using a custom protocol instead.

Note: When using a forwarding filter, it is vitally important to understand the security implications. If you create a broad filter (one that allows protocols other than those you require), you are creating a hole in your security gateway. This may seriously undermine the security of your network.

You might consider configuring a forwarding filter to support a point-to-point tunneling protocol (PPTP) server behind the security gateway. The security gateway does not include a PPTP proxy (which involves both GRE and TCP protocols). If you want external entities to access the PPTP server, you need to configure the security gateway to pass PPTP.

However, because a forwarding filter is basically an open window to the Internet with no security checks applied to packets, setting up a GSP and writing a rule allowing this service to pass between the PPTP Server and the Universe gives you security over the connection that a forwarding filter does not.

Note: Forwarding filters do not support network address translation (NAT). If a forwarding filter lies between an external client and an internal server, the internal server must have a routable address. If possible, use a GSP rather than a forwarding filter. Using a GSP lets you NAT and log packets, where forwarding filters do not.

You can find the steps necessary to create a forwarding filter in your product's administrator guide.

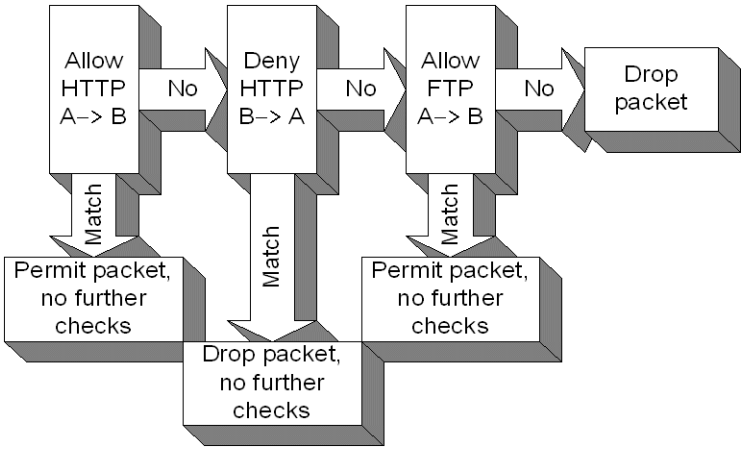
VPN filter

A VPN filter limits the types of permitted traffic allowed through a VPN tunnel. You can view a VPN filter as the opposite of a forwarding filter. A forwarding filter's purpose is to increase the number of permitted services through a secure entry point. By default, a VPN connection allows all services. When you apply a VPN filter to a VPN connection, the behavior of that connection is changed to restrict the types of services permitted.

Filter groups

You can couple filters to form groups (a collection of filters), letting you create more complex filters from a series of simpler ones. Packets are checked against each filter in the filter group in sequence as shown in Figure 5-1. If a packet matches a filter group at any point, that action is immediately taken, and no further checks performed. You should use deny filters only as part of a filter group because filters deny all traffic by default. A standalone deny filter disallows traffic that is not permitted in the first place.

Figure 5-1 Evaluating packets with filter groups



You can find the steps necessary to create a filter group in your product's administrator guide.

How filters are used

Filters are used in several ways:

- At a security gateway interface to allow or deny packets that pass through that interface.
- As a property of a VPN tunnel to control the protocols that the tunnel supports. For example, a packet filter could be designed that limits tunnel traffic to email (SMTP) only.
- As a property of all of the security gateway's interfaces (a forwarding filter*)* that permits otherwise unregulated traffic to pass through the system in cases where the proxies would not permit.

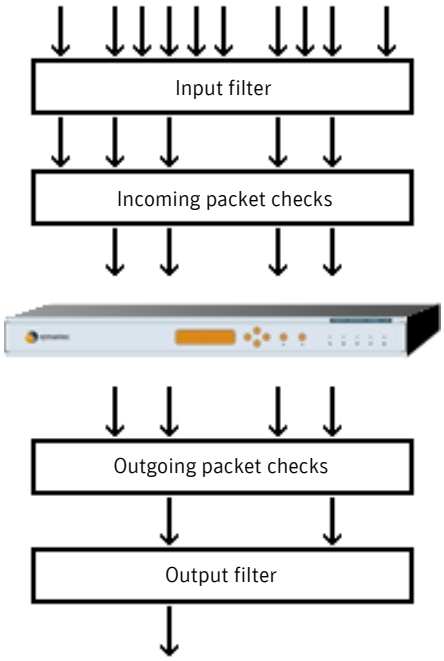
- To protect non-security gateway related services from attacks. For example, a packet filter could prevent the security gateway from forwarding RIP packets, which contain information about the protected network, to the Internet.

You should not run any general services on the security gateway. If this is unavoidable, packet filters placed on the security gateway interface provide a measure of protection.

Filter processing

As shown in Figure 5-2, packet filters, if they exist, are applied before the driver examines incoming packets, and after the Symantec driver has reviewed outgoing packets.

Figure 5-2 Position of interface filters



Incoming packets are filtered in the following order:

- If no filter is present, packets continue on to the incoming packet checks.
- If a filter is present, but the filter contains no criteria/action pairings, the packet is dropped.
- If a filter is present, and criteria/action pairings exist, each pairing is examined, in the order they were added, until a match is found. Once a match is found, the defined action (allow or deny) is applied, and no further examination takes place. If no match is found, the packet is dropped.

Outgoing packets are filtered in the following order:

- If no filter is present, packets continue on to their destination.
- If a filter is present, but the filter contains no criteria/action pairings, the packet is dropped.
- If a filter is present, and criteria/action pairings exist, each pairing is examined, in the order they were added, until a match is found. Once a match is found, the defined action (allow or deny) is applied, and no further examination takes place. If no match is found, the packet is dropped.

Note: If an input filter causes a packet to be dropped, a log entry is written to the log file that includes the interface, source address, destination address, and protocol.

Packet flow

One important aspect of a filter is the direction of the packet flow between the source and destination. For example, an output filter allowing FTP packets between source A and destination B (A -> B) means destination B can only respond to FTP packets sent from source A. Destination B cannot send a new FTP packet to source A.

The security gateway checks that the TCP ACK bit is set, indicating it is a response, for any packet it receives from destination B addressed to source A. If the TCP ACK bit is not set, the packet is dropped. To grant permission to both A and B to initiate FTP sessions, create an output filter that allows (A -> B) for FTP and an input filter that allows (B -> A) for FTP.

Content filtering

Content filtering lets an administrator prevent access to objectionable material, or allow access to specific sites. The security gateway can allow or deny access to content through the following types of content filtering:

- Rating profiles
- URL list
- URL pattern matching
- MIME types
- File Extensions
- Newsgroup profiles

Rating Profiles

Many organizations want to enforce acceptable use policies at the security gateway. These policies limit user browsing to Web sites that do not fit within acceptable use criteria. For example, allowing access to pornography or other objectionable material may be undesirable. To help address this issue, the HTTP proxy allows for content scanning with restrictions to certain types of sites. If a Web request is to a questionable site, and the appropriate rating has been applied, the request is denied.

Rating categories

Each Web site in the URL database is listed in one or more categories. Rating profiles are then constructed using these categories, not individual Web sites. A rating profile only looks at the category level, and denies access to all Web sites that fall into that category. You can add more than one category to a profile if you require restriction to multiple types of sites. For service groups with an applied rating profile, the HTTP proxy searches through all URL entries in the categories defined by the rating profile. If a match occurs, the request is denied.

The URL database is categorized into 13 groups, with Web sites assigned to one or more groups. These 13 categories include the following:

Gambling	Drugs/Non-medical	Racism/Ethnic Impropriety
Sex/Nudity	Gross Depictions	Sex/Acts
Alcohol-Tobacco	Violence/Profanity	Militant/Extremist
Sex/Attire	Occult/New Age	
E/Sports	SexEd	

For instructions on configuring and applying a ratings profile, consult your product's administrator guide.

Rating modifications

Web sites, especially newer ones, may not yet be categorized in the URL database. Using a rating profile to block access to the type of site does not work because the site is not in the database. Rating modifications lets the administrator manually add a Web site to a category, blocking access to the Web site when the appropriate rating profile is in use. Web sites added manually are stored in a local database separate from the URL database. When ratings are applied to rules, both databases are parsed. Entries in both databases have the same level of precedence and common entries in both databases are inclusive; if an entry exists in both databases, but is assigned to different categories in each, ratings created using any of the categories deny access.

There is also a search option that lets you search the URL database for a specific site. If you search for a site, and it is in the database, it appears in the upper window. You can then modify the ratings for this particular URL.

URL List

The URL list lets you define Web sites that are allowed when you enable restrict by URLs in the HTTP parameters for a service group that contains HTTP. When this service group is used in a rule, users can retrieve the URLs listed; access to all other URLs is denied. For example, this might let an administrator restrict access to company-approved sites only.

The IP address of defined Web sites must reverse map to their Web URL. For example, you may have two different Web sites such as http://www.somesite.com and http://www.somesite2.com that are hosted on the same server. Both of theses sites return an IP address of 207.53.87.2 to a DNS request. However, only one of these sites can appear in the DNS records for a reverse map of the IP address 207.53.87.2. If http://www.somesite.com is matched with the IP address 207.53.87.2 in the reverse lookup record, requests to access http://www.somesite2.com fail because the reverse lookup of the returned IP address matches http://www.somesite.com; the entered URL does not match the URL returned for the reverse lookup of the IP address.

Configuration information for restricting by URL lists is found in your product's administrator guide.

URL pattern matching

URL pattern matching using regular expression syntax is a security method available to the HTTP proxy. Regular expression syntax is a series of characters put together to form a pattern. Table 5-1 lists the supported characters that are used in regular expressions. When you use the advanced services command http.urlpattern in a rule, this file is examined and each URL request that comes in is parsed against this file.

Table 5-1 Supported regular expression symbols

Symbol	Description
\	Indicates that the next character should be interpreted literally if it normally isn't, and should not be interpreted literally if it normally is.
.	Matches anything except the NULL character
*	A suffix which signifies that the preceding pattern is repeated zero or more times.
+	Similar to * except that at least one instance of the previous pattern is required for a match.
?	Similar to * except that it allows zero or one match only for the preceding pattern.
[	Designates the beginning of a character set.
[>	Designates the beginning of a complement character set (that is a pattern that matches any characters except the ones included in the set).
]	Designates the end of a character set. If you wish to make this character one of the matchable characters in a set, it must appear immediately after the opening bracket.

Table 5-1 Supported regular expression symbols (Continued)

Symbol	Description
-	Specifies a range of characters in a set. If you wish to make this character one of the matchable characters in a set, it must be used in a context where it cannot possibly indicate a range. This can either be at the beginning of the set, or immediately after a range.
>	Beginning anchor character and matches the blank space at the beginning of a line. It must be placed before the pattern that you want to match. It matches if that pattern appears at the beginning of the line.
$	End anchor character and matches the blank space at the end of a line. You must place it immediately after the pattern that you are looking to match. It matches if that pattern appears at the end of the line.
|	This is the Boolean OR character and requires two patterns, one preceding the | and one following it. It matches either the preceding pattern or the following pattern.
/	Requires two patterns, one preceding the / and one following it. This character says to match the preceding pattern only if it is followed by the second pattern.
“...”	Tells the parser to interpret literally everything inside of the “ ”.
()	Used to group a series of regular expressions to form a new, single expression.
{}	Used to specify exactly how many occurrences of the preceding pattern should be matched. If just a single number is type (such as {2}), the number of occurrences of the pattern must match exactly (2 times in this case). If a comma is used (such as {1,3}), it specifies an upper and lower bound, with the pattern occurring at least as many occurrences as the first number, but no more than the second number. Leaving off the first number designates no minimum occurrence for the pattern, and leaving off the last number designates no maximum occurrence.
\b	Matches a word boundary.
\B	Matches a non-word boundary.
\n	Matches a newline character.
\w	Matches any alphanumeric character, including the underscore (same as [A-Za-z0-9_]).
\W	Matches any non-word character (same as [>A-Za-z0-9_]).
\<	Anchors the pattern to the beginning of a word.
\>	Anchors the pattern to the end of a word.
‘	Marks the beginning of a buffer.
\’	You must use this character combination to terminate a buffer. If a single quote is used again, everything in between the two single quotes is interpreted literally.

For example, let’s say that you want to prevent employees from browsing Web sites with adult material. One common combination of letters to see in a adult Web site URL might be “xxx.” To restrict URLs with this three letter combination, you could put together an expression that looks like

xxx

This expression tells the security gateway to look for the combination of three lowercase xs in a URL, and if found, deny the request. This rather simplistic expression is fine if the URL does not use uppercase letters, and if the URL has a minimum of 3 xs in it.

It may be impossible to match the patterns of all sites you want to exclude with one expression, so it is common to add additional expressions. For example,

XXX

Now, with these two entries, the URLs containing three uppercase Xs or three lowercase Xs were blocked, but nothing else. What if the URL has mixed case? A more elegant solution to solve all three cases is to use character set variables. To combine and look for three uppercase Xs, three lowercase Xs or any combination of three consecutive uppercase and lowercase Xs, use

[Xx][Xx][Xx]

As shown in Table 5-1, the [and] characters denote a range of characters that should be matched. Because you are looking specifically for three consecutive letters, you need to set up three sets of brackets.

Note: One common mistake is to use the * character as a global wild card character thinking that it solves multiple cases. For example, the expression

[Xx]*

achieves the same results in blocking access to the desired sites previously mentioned; however, it also blocks access to every other site. The * says zero or more occurrences, so, regardless of whether or not the URL has the letter x in it, it is blocked.

The strength of URL pattern matching is immediately apparent. Instead of having to list exactly the URLs you want to allow, you can define patterns to deny any URLs that contain specific words or phrases. This is further extended to recognition of buffer overflow attacks.

For example, examine the URL http://www.website.com/index.htm/?%2%c0x5at. The last part of the URL appears to be gibberish, but is actually an attack and an attempt to overrun the Web server, or cause it to behave in a way it normally wouldn't. Through the use of pattern matching, once you know what the signature for the attack looks like, you can add the appropriate line to prevent this request from going through.

Configuration information for creating and using URL pattern matching with the HTTP proxy is found in your product's administrator guide.

MIME Types

The HTTP proxy can restrict access according to a list of MIME types. Each URL received is scanned to see if its content-type matches a restricted MIME type. When a match is found, the Web page still downloads, but those components matching blocked MIME types do not. Unlike other restrictions, MIME restrictions are global, affecting all HTTP connections. For additional information including a list of common MIME types, see RFC 1521.

Configuration information for restricting by MIME types is found in your product's administrator guide.

File Extensions

The file extensions list lets you define filename extensions that are allowed when you enable restrict by File Extensions in the HTTP parameters for a service group that contains HTTP. When this service group is used in a rule, users can only retrieve URLs with the extensions listed; access to all other URLs is denied. This provides a way of allowing, for example, only text or HTML files, while restricting binary executables. Files with no extension are assumed by default to have .html extensions.

Note: If you create this list, only the extensions you include in this list are allowed. Once this list is created and applied to a rule, the default policy is to deny everything not on the list.

Configuration information for restricting by file extensions is found in your product's administrator's guide.

Newsgroups

The newsgroups list lets you define newsgroups to be used in newsgroup profiles. Once you create a newsgroup, you can add it to a newsgroup profile. Newsgroup entries are entered with the complete newsgroup name, or can make use of wildcards to denote one or more newsgroups. For example, the enter newsgroup alt.science.nasa to grant access to just this group, or alt.science.* to grant access to all groups in the alt.science forum.

Configuration information for creating newsgroups is found in your product's administrator's guide.

Newsgroup Profiles

Newsgroups are a popular medium to exchange thoughts and ideas, and collect answers to questions on specific topics. However, because some groups are unmoderated, articles posted can contain offensive or objectionable material. Creating a newsgroup profile lets an administrator decide which newsgroups to allow access to. For example, a newsgroup is useful when internal users desire news access, and a company wishes to limit exposure to certain types of articles.

Configuration information for creating newsgroups profiles is found in your product's administrator's guide.

Chapter 6

Controlling user access

This chapter includes the following topics:

Users

A user represents an individual with rights to access your protected network resources, and must be defined for rules and tunnels to limit access to authorized connections only. Users are also required for most types of authentication. Users are defined by creating a user account consisting of a unique user name and authentication method.

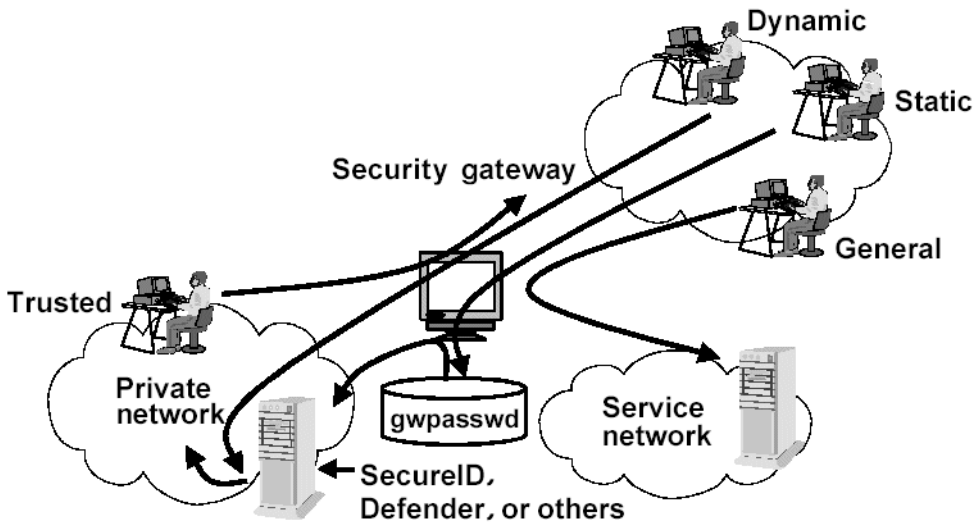
Types of users

There are several different types of end-users that might try to access your network:

General	Any person outside of the protected network. You may want all general users to access a few services, like a Web or news server. General users are unknown to you, and should be viewed as a security risk.
Trusted	Any user your company has a relationship with, including employees, contractors, subscribers, and employees of companies with business relationships with your company. Such a user is not, in principle, anonymous to you because you can attach a name to this user. Many of your rules allow the trusted users at your site to access the Internet using one protocol or another. Trusted users may pose greater security risks than general users. Remember, these people are often in the building and behind the security gateway.
Gateway or static	A gateway user is any end-user with a user account on the security gateway. These user accounts are established through the security gateway management interface and maintained in a local database file named gwpasswd. Gateway users are authenticated with the gateway password authentication system, Bellcore S/Key, or with an external authentication server.
Dynamic	A dynamic user is an end-user who is authenticated with one of the authentication systems available to the security gateway, but has no record on the security gateway. Instead, the user account is on the authentication server. The security gateway offers several types of authentication methods that use authentication servers, such as RSA SecurID and PassGo Defender.
Default IKE user	The default IKE user is not a physical user that accesses the security gateway, but is instead a pre-defined user type. The default IKE user lets an administrator grant access to anyone that has the proper shared secret without having to create a user for the individual on the security gateway. The default IKE user should be used in a user group that requires an extended authentication method, such as Defender or RADIUS, for access.

Figure 6-1 shows the different types of users and their location with respect to the security gateway.

Figure 6-1 Types of users



Should you create a user account for everyone who works at your company? No. In a private network, trusted users typically do not interface with the security gateway when accessing protected network resources and services. But, external users, both static and dynamic, do pass through the security gateway and require authentication.

Depending on the type of user, user accounts are created in different locations. For static users, the administrator defines the user on the security gateway. Static users are then authenticated by the security gateway. For dynamic users, the administrator links the users to the authentication server. The authentication server contains the actual user account.

Authentication

Authentication creates an additional layer of security by requiring connecting users to verify their identity. Authentication is used to enhance access control for other aspects of the security gateway configuration, such as proxy rules. Generally, records are entered into a database and these records are used to verify identities and establish a security context for the connection.

Authentication in rules

To support authentication methods that require them, the security gateway prompts for a user name and password. If the security gateway recognizes the user name, that user must be a gateway user. The security gateway authenticates the user as defined in the rule. If the security gateway does not recognize the user name, the security gateway assumes the user is dynamic and contacts the authentication server or servers defined in the rule. Normally, dynamic authentication requires additional configuration settings, and is not set up simply by creating a rule.

Authentication methods

The security gateway supports several distinct authentication methods. Each has its own database and protocol for establishing a security context. Some supported methods are third-party products managed external to the security gateway. The security gateway makes use of them as it would any application. More than one mechanism is queried in the course of an authentication decision.

The security gateway supports the following methods for authenticating users:

- Bellcore S/Key
- Entrust
- Gateway password
- Lightweight Directory Access Protocol (LDAP)
- NT Domain (Microsoft Windows only)
- PassGo Defender
- Remote Authentication Dial In User Service (RADIUS)
- RSA Security SecurID
- TACACS+

Administrators can create custom templates that apply one or several of these authentication methods in a definable order. In addition to these methods, which are protocol-dependent, the security gateway supports an Out of Band Authentication (OOBA) scheme incorporating any of the above methods. The security gateway can also be configured to set up simple user authentication based on static users.

Weak and strong authentication systems

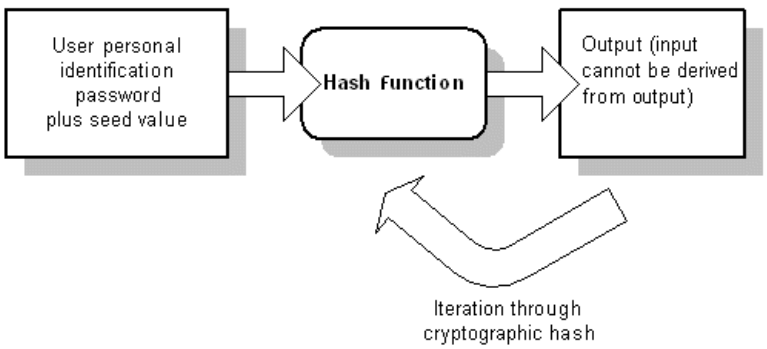
Authentication systems are defined as weak or strong based on how many times the same password is used. Authentication systems that use the same password continuously (multi-use) are weak. Multi-use passwords offer a potential attacker time to figure out the password, something strong systems do not. Authentication systems that require a different password for each session for each use (single-use) are strong. Strong authentication systems are inherently more secure than weak ones since they are not as vulnerable to password sniffing.

Note: Although the security gateway supports both weak and strong authentication methods, you should use a strong authentication system for anyone requesting access.

Bellcore S/Key authentication

Bellcore S/Key is a software-based strong authentication system. The Bellcore S/Key server is integrated within the security gateway. Bellcore S/Key generators for PC and UNIX clients are included. Figure 6-2 shows that Bellcore S/Key works by running a user password and seed value through a cryptographic hash function a fixed number of times. A cryptographic hash function takes an input and creates an output. The input is not recoverable from the output.

Figure 6-2 S/Key hash iteration



Bellcore S/Key runs the password and seed value though the hash function a pre-determined number of times for the first logon, then the original value less 1 for the second log on, and so forth until the number reaches 1. At this point, the seed value must be reset.

To connect to the security gateway, Bellcore S/Key users must provide the correct password and seed value to a local Bellcore S/Key password generator. Upon supplying them, the Bellcore S/Key software on the user's client system generates a one-time password in the form of six short words.

The user enters this string when prompted by the security gateway. With each subsequent connection, the Bellcore S/Key software generates a new password string and decrements the user's iteration count. When the user's count decrements to zero, no further connections are permitted.

Each password is unique and cannot be predicted from any password with a higher numbered iteration. However, you can predict Bellcore S/Key passwords from a lower numbered iteration. If a user enters a password, seed value and an iteration count of 78, all passwords numbered 79 and above are generated using the hash function.

Warning: There is a possible Trojan horse attack available with Bellcore S/Key. You can trick a user into entering a password numbered a few iterations ahead of the current number. For example, if the end-user was supposed to be on iteration 74, but gets prompted by a hacker for iteration 73, you can generate 74. Users should be aware of this possible attack. If they are asked to authenticate with Bellcore S/Key and enter an iteration number and then try again and enter a higher number, they should contact the security gateway administrator immediately.

Configuration information for Bellcore S/Key authentication is found in your product's administrator's guide.

Entrust authentication

The security gateway supports the use of Entrust Certificates to authenticate Symantec Client VPNs. The Entrust authentication method requires a configuration setup, both on the client and the security gateway. You must define an entrust user at the security gateway to log on to the Entrust Server and an entrust user for each Symantec Client VPN that needs to authenticate.

An entrust user is defined by the following:

- An initialization file (*.ini)
- A client profile (*.epf)
- A client password

The client profile is a file containing the various Entrust certificates for the user. The client password is used to encrypt the private certificates within the profile. The initialization file, client profile, and client password are used by the user to log on to the Entrust Server and use its API to encrypt, decrypt, and sign messages.

Configuration information for Entrust certificate authentication on the Symantec Client VPN is found in the *Symantec Client VPN User's Guide*. Configuration information for Entrust certificate authentication on the security gateway is found in the your product's administrator's guide.

Gateway password authentication

Gateway password authentication is a multi-use password maintained within the security gateway database for each gateway user. Users and their passwords are entered and maintained by the administrator. Gateway password authentication is a weak form of authentication. Both the challenge and the response are passed as clear text.

Configuration information for gateway password authentication is found in your product's administrator's guide.

LDAP authentication

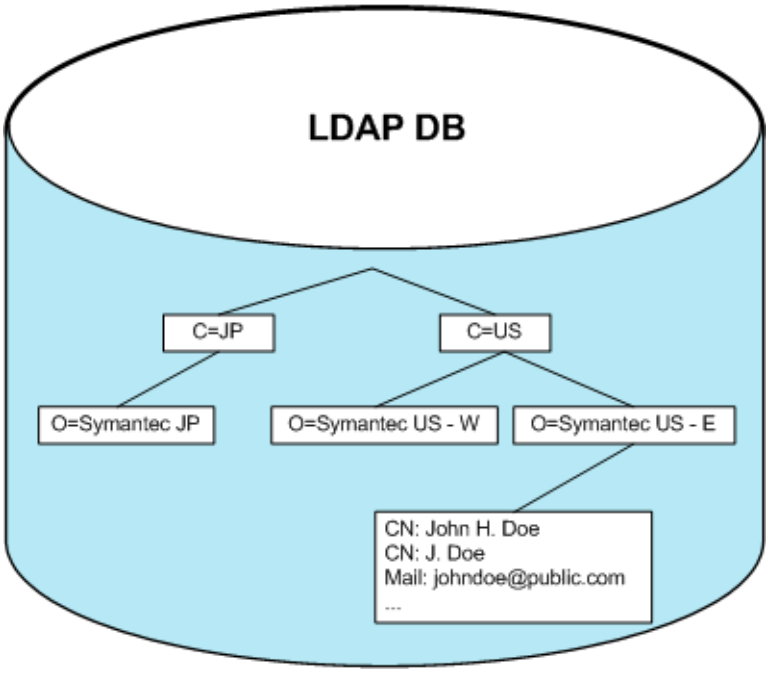
Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. LDAP was originally developed as a front end to X.500, the OSI directory service. X.500 defined the Directory Access Protocol (DAP) for clients to use when contacting directory servers. DAP uses the entire network stack and requires significant computer resources to operate. In contrast, the LDAP protocol operates through a single TCP connection, and provides most of the functionality of DAP, but at reduced costs.

How LDAP works

LDAP uses a client-server model, with one or more LDAP servers maintaining the data that comprises the LDAP directory tree. The LDAP directory tree consists of data structures called entries. Each entry is a collection of named attributes, called a distinguished name (DN). Each distinguished name has a type and one or more values. Types are generally set up to be intuitive, and the value is dependent upon the type configured. For example, email might be set up as a type to refer to an email address, and the value in this entry might be joe@public.com.

Entries are most often configured in a tree structure based on political, geographical and organizational boundaries. Upper entries normally begin with geographical location, and then move down into state or organizational layouts. Below the state or organizational entries, more granular entries are placed, such as people, smaller organizational units, or documents. Entries can also contain a pointer to another directory tree where the information is found. Figure 6-3 is an example of one possible directory tree.

Figure 6-3 Sample LDAP directory tree



A client initiates a connection to the server to request information. The server parses the entry, and either returns the information in the record, or redirects the request to where the pointer states the information is found (typically another LDAP server). Because the directory structure is the same regardless of the LDAP server connected to by the client, pointers are used as substitutes for the actual information. Each entry in the directory tree is in the same location on each LDAP server.

The security gateway supports LDAP-based authentication for LDAP version 3.

How LDAP authentication works

LDAP is considered to be a weak authentication method. Authentication is performed by binding a DN on the LDAP server to a user ID. The user ID is used to lookup the DN from the directory tree, and then the password is used to bind to the entry, completing authentication.

A group list is looked up by searching for groups where the user's DN (or other specified unique attribute) is a member specified in the configuration. If no primary group attribute is specified, the first one of the group list is returned as the primary group. Access is denied if multiple users exist with the same UID attribute, and the denial is logged.

Configuration information for LDAP authentication is found in your product's administrator's guide. Additional information on LDAP protocol and LDAP authentication is found in the RFCs listed in Table 6-1.

Table 6-1 RFCs that define the LDAP protocol

RFC	Title
1777	Lightweight Directory Access Protocol
1778	The String Representation of Standard Attribute Syntaxes
1779	A String representation of Distinguished Names
1960	A String Representation of LDAP Search Filters
2251	Lightweight Directory Access Protocol (v3)
2252	LDAPv3: Attribute Syntax Definitions
2253	LDAPv3: UTF-8 String Representation of Distinguished Names
2254	The String Representation of LDAP Search Filters
2255	The LDAP URL Format
2256	A Summary of the X.500 (96) User Schema for Use with LDAPv3
2829	Authentication Methods for LDAP
2830	LDAPv3: Extension for Transport Layer Security
3377	Lightweight Directory Access Protocol (v3): Technical Specification

Configuration information for LDAP authentication is found in your product's administrator's guide.

Microsoft Windows NT Domain

Microsoft Windows NT Domain authentication provides access to the user names and passwords stored on the primary domain controller (PDC). This enables administrators to store user names and passwords using the operating system, rather than the security gateway database.

When using Microsoft Windows NT Domain authentication, keep in mind that:

- Microsoft Windows NT Domain authentication is not a strong method of authentication. Both the challenge and the response are passed as clear text.
- The security gateway must be a member of the PDC's domain before the security gateway software is installed. The PDC must be behind the security gateway, that is, on the protected network.

Microsoft Windows-based Symantec Enterprise Firewalls that want to use Microsoft Windows NT Domain authentication can either join the domain prior to the installation of the software and then use the authentication natively, or configure the security gateway to connect remotely through RADIUS. All other security gateways are limited to using the RADIUS method.

Out Of Band Authentication (OOBA)

Out of Band Authentication (OOBA) is Symantec's customizable form of authentication. OOBA lets the administrator define any currently configured authentication or extended authentication method as the authentication method that OOBA uses. Not all proxies support authentication. OOBA was designed specifically for those proxies that do not support authentication, or support a limited set of authentication types (like HTTP). The most common use for OOBA is to enable authentication on a GSP, which does not have authentication by default.

Understanding OOBA

The administrator configures the OOBA daemon by selecting the authentication method to use and port to listen on. A user desiring access to services behind the security gateway directs their Web browser to the security gateway on the defined port. Once authenticated, the user is prompted to select the services they want access to. OOBA then issues a cookie to the user's machine that defines how long the current session may last, and what services are allowed.

OOBA is most often used on connections originating from an internal network destined for an external network because text passed during OOBA authentication is in clear-text. OOBA authentication is used by remote users. However, because OOBA passes traffic in clear-text, it is not advised that you use OOBA for this purpose.

Non-HTTP connections

Users that need to be authenticated by OOBA and connecting to any proxy other than the HTTP proxy must first use their Web browser to connect to the OOBA daemon and authenticate themselves. Users must open the Web browser, enter the IP address and OOBA port of the security gateway, and connect. Through a series of Web pages, OOBA guides the user through the authentication process. When finished with the authentication process, the user must leave the Web page open for the duration of the connection.

For the user that successfully authenticates, the OOBA daemon creates a ticket and sends that ticket back to the user's browser in the form of a cookie. The cookie is sent back to the security gateway each time the user accesses an OOBA-protected service, so the user need not authenticate again until the ticket expires. The expiration time of the ticket is determined by the administrator and is set globally for every OOBA connection.

HTTP connections

Users connecting to the HTTP proxy do not need to connect to OOBA on a specific port. When accessing the HTTP proxy, it recognizes that the rule requires OOBA, and redirect the connection to the OOBA authentication process automatically. Authentication proceeds exactly as non-HTTP connections and, if successful, returns to the HTTP proxy and connects the user to the URL originally requested.

Note: The HTTP proxy cannot support true challenge/response passwords for authentication. Acceptable forms of authentication include RSA SecurID, S/Key, or Defender in synchronous mode. Administrators should set the password reuse on authentication methods for HTTP connections.

Configuration information for Out of Band authentication is found in your product's administrator's guide.

PASSGO Defender authentication

Often, static passwords are easily guessed, shared, cracked by others, or in some way compromised. Longer passwords help, but still don't prevent all problems when authenticating a user with a password. In environments where users are forced to change their passwords on a regular basis, users often pick something easy to remember, or use a single password for all applications. If the password is unfamiliar, the user may write the new password down. All of these make the user more vulnerable to compromise and highlight why static passwords are inadequate for uniquely authenticating users.

Defender solves the password problem by providing two-factor authentication that uniquely authenticates users without forcing them to remember another password. Defender is an industry standard, and uses a challenge/response mechanism to create a one-time password that is far more secure than static passwords. For an attacker to correctly compute the response for a challenge, they need not only the user's PIN, but also the unique client software. Without both pieces, potential intruders cannot calculate the required response. Even if the response is viewed when entered, it serves no purpose, as the response is only valid for that session.

Defender also supports a synchronous password method similar to RSA SecurID. When the token is synchronized with the Defender Security Server (DSS), an internal clock generates an unpredictable string that changes every minute. The DSS also uses an event counter and increments this counter each time a new challenge is generated. This event counter is used in conjunction with the unpredictable string, a user-specific secret key, and an encryption algorithm to generate the challenge to be issued. Because the event counter always rolls forward, the one-time password is truly only valid one time, and not susceptible to replay attacks like some other time-based synchronous password methods are.

Note: Defender supports static passwords, but you should not use them. One of the strengths of the Defender authentication method is its single-use passwords.

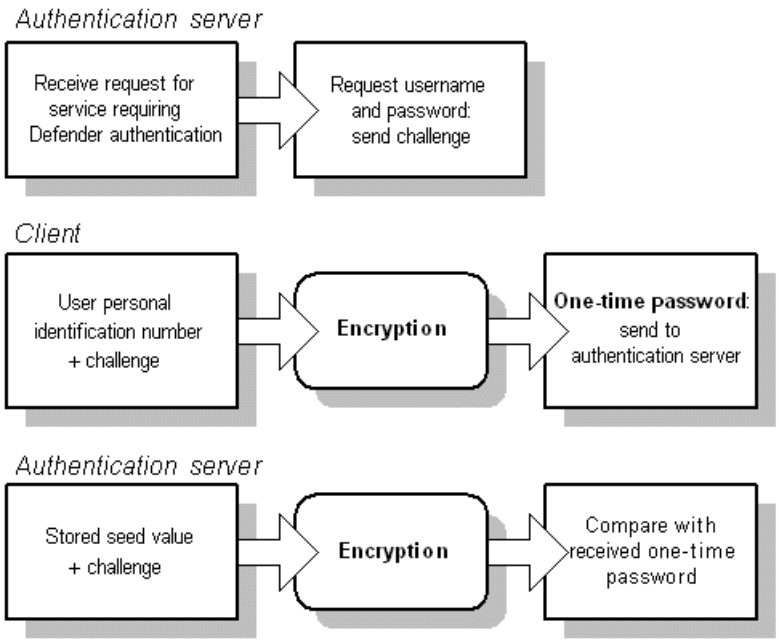
How Defender authentication works

Defender, a strong authentication system, is commonly used as extended authentication for VPN connections. Defender authentication uses the following components:

Defender Security Server (DSS)	Maintains a database of Defender users and their information pertinent to their token. Requests are compared against information contained in the DSS user record.
Defender Management Console (DMC)	Used by the administrator to create and synchronize new tokens, or update existing user information.
Token	Takes the form of either a client disk, a hand-held token, or SmartCard. Each token is unique.
Personal Identification Number (PIN)	Normally known only to the user, and must be entered each time the token is used for authentication.

Figure 6-4 shows the Defender challenge/response authentication process.

Figure 6-4 Challenge/response authentication



During authentication, the DSS sends a generated series of numbers known as a a challenge. If the user has a hardware token, the user activates the token, enters both their PIN and the challenge, and then generates a response. The response must be typed in and the DSS then verifies the response. For users with the software token, they are prompted to enter their PIN only; the challenge phrase is passed seamlessly to the token response generator, requiring no user interaction.

The one-time response generated by the token has the following attributes:

- It cannot be reused, since the authentication server issues a different challenge each time.
- It is not subject to Trojan horse attacks, which are used on static passwords and S/Key, since you cannot guess a password from any other password.
- In practical terms, it cannot reveal the private password entered into the token generator.

You can also configure Defender to accept a user name and password without a challenge/response. However, using Defender this way makes it a weak authentication method.

Configuration information for Defender authentication is found in your product's administrator's guide.

RADIUS authentication

Remote Access Dial In User Service (RADIUS) is a UDP-based authentication method. RADIUS normally uses a simple user ID and password method, but you can configure it to use one-time password smart cards. The administrator must configure the RADIUS server details on the security gateway to use RADIUS authentication.

Configuration information for RADIUS authentication is found in your product's administrator's guide.

RSA SecurID authentication

RSA SecurID is a time-based, strong authentication scheme that uses smart card technology. The RSA SecurID card produces a new 6-digit password at 60-second intervals. Sniffed passwords are useless.

To use this authentication method, users must have installed the RSA SecurID software on a separate system behind the security gateway. The security gateway then sends and receives RSA SecurID authentication requests to that system for validation. For more information on RSA SecurID, see their Web page at www.rsa.com.

Configuration information for RSA SecurID authentication is found in your product's administrator's guide.

TACACS+ authentication

TACACS+ is a TCP-based authentication method. The administrator must provide the IP address of the TACACS+ server to use TACACS+ authentication. In addition, the administrator must enable the daemon, and set up a template for the authentication method.

Note: The configuration of the TACACS+ server is beyond the scope of this book.

Configuration information for TACAS+ authentication is found in your product's administrator's guide.

Time Periods

Another method to control user access is the time periods feature. This feature lets the administrator limit the time period that someone can gain access to the protected network. This time window usually mirrors when a company is open for business, or when the administrator is around to troubleshoot a problem.

Time range template

A time range template is a starting and ending time or date combination, such as July 1, 2003-July 31, 2003, Monday-Wednesday, or 4 PM-6 PM. Templates also support both days and times such as 4 PM-6 PM during July 1, 2003-July 31, 2003 or 4 PM-6 PM during Monday-Wednesday.

There are a number of time range templates already created. You have the ability to edit the templates to refine them to your unique requirements, or you can simply create new time range templates. The pre-configured time range templates include:

Everyday	Sunday through Saturday, 24 hours a day. This is also the time range used when no template is active.
Weekdays	Monday through Friday, 24 hours a day.
Weekend	Saturday and Sunday, 24 hours a day.
WorkingHours	8:00 AM to 5:00 PM.

When creating a new rule, if no time period is selected, <ANYTIME> appears in the rule definition to signify that the rule has no time restriction.

Time range sequence

A time range sequence is a group of time range templates joined together in an inclusive OR relationship. Each sequence is a group of time range templates combined in a uniquely named group. Once created, the sequence appears in the time range pull-down, and you can select it for a rule or notification.

Chapter 7

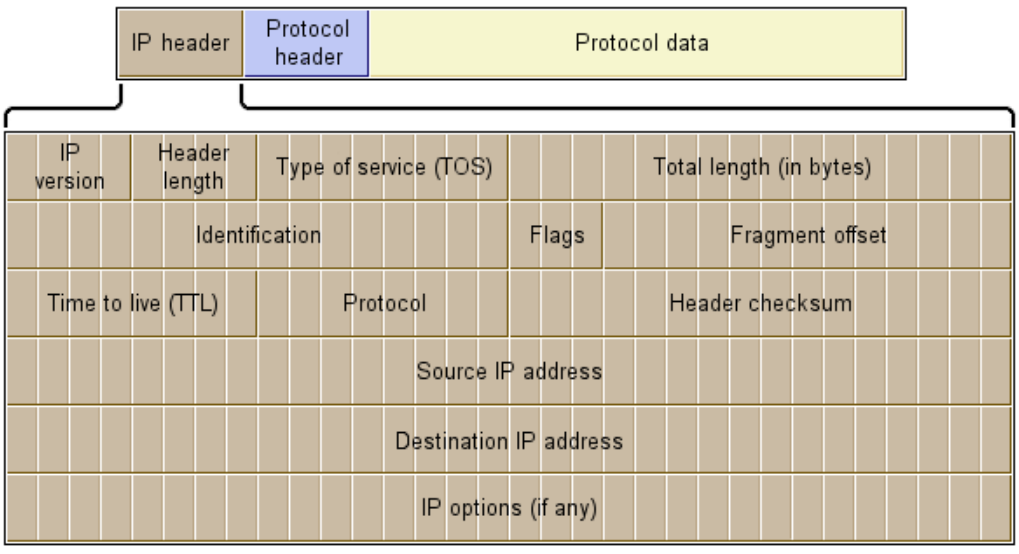
Understanding VPN tunnels

This chapter includes the following topics:

Introduction to IP security

Standard IP datagrams have no inherent authentication or encryption features. IP packets travel in clear text on public networks, and anyone with the knowledge, time, and access can intercept and capture this data. Packets contain sensitive information such as user names, passwords, or proprietary information, and exposure to this information can have devastating results. To understand how vulnerable IP packets are, Figure 7-1 shows a typical IP datagram consisting of an IP header, a higher level protocol (such as TCP or UDP), and the payload or data.

Figure 7-1 Standard IP datagram with expanded packet header



From the IP header, an attacker can obtain the source and destination IP addresses, giving them a potential target to direct a denial-of-service (DoS) attack. Access to the header lets an attacker modify the header checksum and total length fields if his or her choice of attack is a buffer overflow. He or she can pull sensitive information, such as a user name or password, from the protocol data. An attacker doesn't need to use a brute force method to gain access when they can use a trusted user's credentials.

Tunnels

Early networking pioneers originally created tunneling to pass data of one protocol type (IPX, for example) over a network using a different protocol (IP, for example). These virtual tunnels let packets travel over foreign networks without modifying their contents. Virtual private networks evolved by adding encryption and authentication checks to the tunnels, which let encrypted packets propagate securely over the network.

Tunnel endpoints

Tunnel endpoints perform encryption, decryption, encapsulation, decapsulation, and authentication operations on tunnel packets. Tunnel endpoints are typically two security gateways (Gateway-to-Gateway VPN tunnel) or a Client VPN and security gateway (Client-to-Gateway VPN tunnel).

Tunnel endpoints do not have to be outside your protected network. You might use a VPN tunnel completely within the protected network to keep sensitive information safe from casual access by your inside users. The principle is the same; connections are encrypted between the two endpoints, not behind them.

Note: You cannot select domain entities to be an endpoint of a secure tunnel. All tunnel endpoints must have resolvable IP addresses.

Network entities assigned to a tunnel determine the source or destination of packets permitted to use the tunnel. Tunnels support using user groups, hosts, subnets, and VPN security entities as scope markers. Tunnels also support users and user groups to define who may use the tunnel. Users and user groups are most commonly used with Symantec Client VPN tunnels.

When creating a tunnel using group, host, and subnet network entities, you must define the entry and exit endpoints. The local endpoint must be an interface of the security gateway protecting the local entity, and is often the outside interface of the security gateway because the outside address is routable from other public endpoints. VPN security entities do not require a remote endpoint when defining the tunnel, as they already contain the endpoints for each tunnel to create.

Note: Symantec Client VPN users with a home router using network address translation (NAT) may conflict with each other by assigning the same non-routable network for their home networks. Because the security gateway uses both the source IP address and source port to uniquely define a tunnel, a non-unique IP address condition can occur if both connecting sources happen to use the same source IP address and same unprivileged source port when connecting.

The security gateway's VPN component was enhanced to work around non-unique client IP addresses when you enable the option to pass traffic to the proxies in the VPN policy. If the security gateway cannot resolve an address conflict, it notifies you of this condition. Upon failure, the security gateway generates a non-unique client address warning message in the log file. The offending request is discarded as non-routable. In addition, an ICMP Parameter Problem message is sent back to the client. The best solution to this symptom is to ask the end user to modify the default home subnet assigned by their home router.

Tunnel indexes

The security gateway uses tunnel indexes, also called security parameter indexes (SPIs), to handle VPN packets it receives from another security gateway or Symantec Client VPN. The index is a number agreed upon by each encryption device, and is unique for each destination address. The receiving security gateway uses the index to get the pointer to the packet's security characteristics. The security characteristics contain information on how to authenticate, decapsulate, and decrypt the packet.

Tunnel communication

Tunnel packets are handled at the IP layer of the protocol stack. The receiving security gateway uses the tunnel index to remove the encapsulation and encryption from the original packet. With the protective outer shell removed, the security gateway then forwards the original packets to their intended destination.

Traffic is only encrypted in the tunnel, between the tunnel endpoints. Traffic outside the tunnel is in its original form with no protection.

Note: Incoming tunnel traffic uses the original client IP address by default. Therefore, your internal hosts need to ensure that they have a valid route back to the client or network. If your internal hosts do not have a valid route back to the client or network, the security gateway must have network address translation (NAT) enabled, and specify that the return packet use the security gateway address.

Tunnel security

VPN tunnels pass data through the security gateway without any additional security checks. You can modify this default behavior so that VPN packets are subject to the same scrutiny as other traffic. You can subject tunnel traffic to authorization rules, input and output filters, and application proxies.

Authorization rules for tunnel traffic

Unlike packets handled by Telnet, FTP, and other server applications, VPN packets are not sent up the protocol stack for processing. Tunnel traffic is not necessarily subject to authorization rules. Connections not subject to authorization rules are not logged. By definition, VPN connections are established between trusted end systems. Moreover, all packets exchanged are encapsulated and encrypted between the two security gateways.

Limiting tunnel traffic with filters

Filters provide additional security to tunnel traffic by restricting the type of traffic passed through a tunnel. For example, it is appropriate for some VPN users to use the protocols FTP, HTTP, and POP3, but not Telnet. A deny Telnet filter applied to a VPN tunnel can enforce such a policy.

For information on configuring filters to restrict traffic passing through a VPN tunnel, see your administrator's guide.

Passing tunnel traffic to a proxy

A check is performed to see if the tunnel traffic should pass through the proxies. If so, the packets are sent up the stack for further processing instead of passing directly through. If there is no proxy requirement, the packets move on to their destination.

Proxying tunnel traffic lets the administrator control the type of traffic allowed through a tunnel. Even between trusted systems, you may not want to allow all services. For example, you may want to permit mail and file transfers, only.

Using the proxies with VPN traffic lets you:

- Restrict source and destination addresses and protocols (as filters do)

- Take advantage of NAT
- Restrict traffic by time of day
- Restrict specific commands within connections (like FTP gets or puts)

Whenever possible, choose VPN with proxies over VPN with filters, for a higher degree of security. Passing VPN traffic through the proxies has the following advantages:

- The proxies log connections. By default, VPN tunnel traffic with no proxy interaction is not logged.
- Proxies provide fine control over services, like restricting URLs or CIFS services.

Types of tunnels

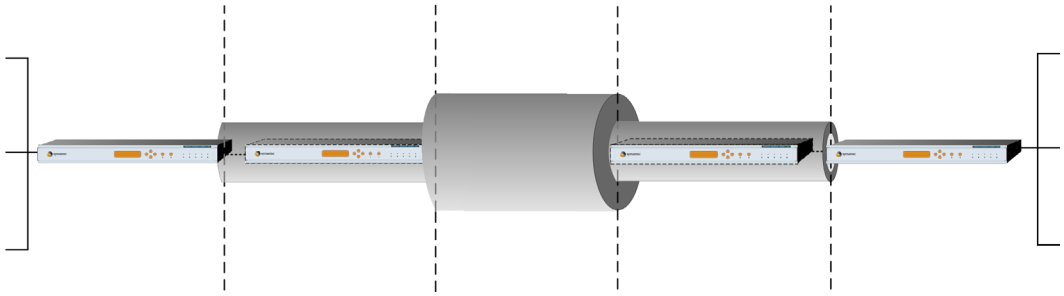
In additional to supporting tunnels between two endpoints, the security gateway also supports two additional types of tunnels: nested and cascaded.

Nested tunnels

A nested tunnel configuration has one secure tunnel passing through another. A nested tunnel configuration normally occurs when a second security gateway encrypts and encapsulates VPN tunnel traffic. When the packets arrive at the first destination security gateway, they are decrypted and decapsulated from the most recent encryption and encapsulation. Because the packets are still encrypted and encapsulated from the original source security gateway, at the final security gateway, they are once again decrypted and decapsulated.

You might use a nested tunnel configuration, shown in Figure 7-2, if you have an existing VPN between two compartmentalized sites and wish to use a second tunnel to protect the transfer of sensitive information between sites. For example, you may have two distinct branch offices connected by a primary VPN tunnel, with each internal department further segmented with their own network and security gateway. This topology lets a department in each location establish a second tunnel between the two offices to protect sensitive data from other departments.

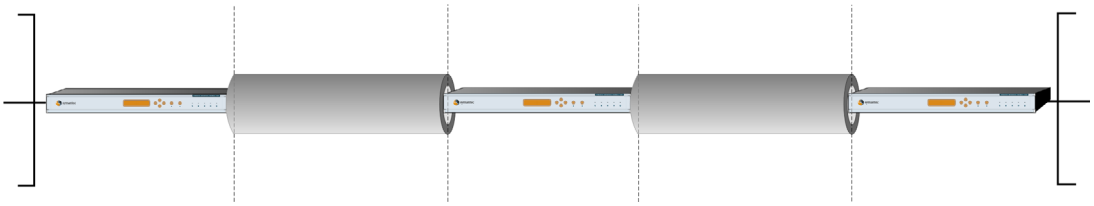
Figure 7-2 Nested VPN tunnels



Cascaded tunnels

In a cascaded tunnel configuration, an intermediate security gateway acts as a bridge between two distinct tunnels. A cascaded configuration is used if you have an existing VPN between two sites and you want to forward traffic that is already part of a VPN to the other site. When a packet reaches the end of one tunnel, it is decrypted and decapsulated and then encrypted and encapsulated for the second tunnel. The decision to make two VPNs cascaded may reflect different levels of security on your private network and the Internet.

Figure 7-3 Cascaded VPN tunnels



Groups

When granting VPN access, you usually create a separate tunnel for each remote user, especially if there is only a handful of users to be created. For large numbers of users, however, this can get quite cumbersome. Maintaining a large list of users with their corresponding tunnels is time consuming, especially if maintenance frequently requires additions and deletions.

User groups let you create a layer of abstraction that simplifies the tunnel creation process. Instead of creating a tunnel for each user, you create a user group and define a single tunnel for that user group with the appropriate access level. Users only need to be added to the group to have the access that all other members of the group share; no additional tunnels are necessary. Denying access is as simple as removing the user from the User Group. Additionally, user groups also let you define DNS, WINS, and the primary PDC for Windows-based networks, and this information is downloaded to Symantec Client VPN connections.

User groups should be created based on access level. Remember that all users in a user group share the same access privileges.

IPsec standard

IPsec, the IETF IP security standard created to address the security limitations of IP packets, is a set of IP packet security protocols that work at the network layer providing authentication, integrity, privacy, and replay protection. The overall architecture for IPsec is described in RFC 2401, with additional information provided in RFC 2402 and 2406.

The functional areas of IPsec include the following:

- Encapsulation modes
- Data integrity protocol
- Data integrity preference
- Data privacy preference
- Data compression preference

Encapsulation modes

Packets that are encapsulated have their contents hidden from public view, and are restored to their original state only when the packet arrives at its intended destination. IPsec supports the encapsulation, or protection, of packets through either transport mode or tunnel mode. The encapsulation mode you select determines the rest of the policy information you must enter.

Transport mode

Transport mode is designed for host-to-host connections only, where the destination address is an end node, and not a gateway that encrypts and decrypts on behalf of an end node. This restriction is present because there is no inner IP header in a transport mode packet. Once the destination system receives the packet, and strips off the IPsec header, only the original (outer) header is present, and its destination address is the system it's on.

Transport mode is not very flexible; tunnel mode is often used instead.

Tunnel mode

Tunnel mode is designed for gateway-to-gateway or host-to-gateway connections where the destination address is the decryption engine, but not necessarily the packet's final destination. Tunnel mode also works with host-to-host connections, but using tunnel mode for host-to-host connections does not offer an advantage over transport mode. In fact, transport mode is better because it does not add an extra IP header to the packet.

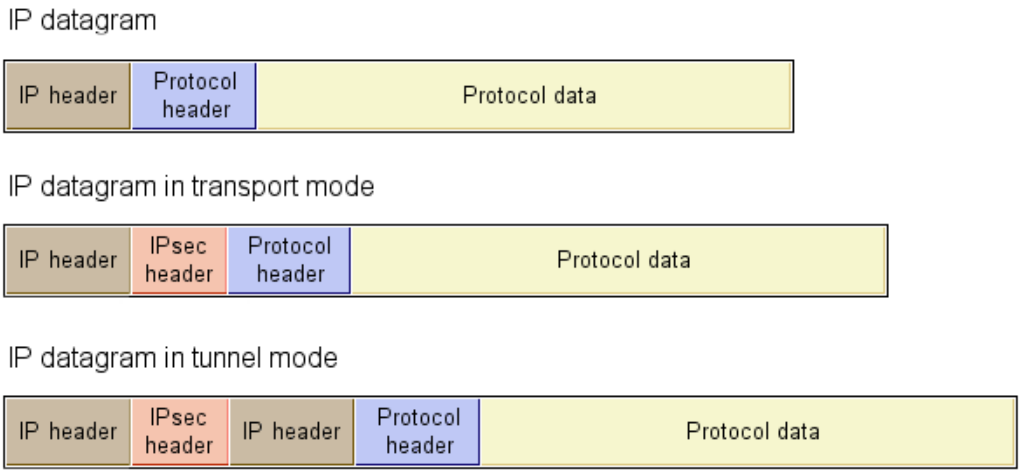
An IPsec tunnel mode packet is encapsulated with an authentication header (AH) or encapsulating security protocol (ESP) header and an additional IP header. This creates two IP headers, an inside or protected header that was created by the source host and an outside or clear-text header created by the host providing the packet security services (encryption). The IP addresses in the outer IP header define the endpoints of the tunnel, and the IP addresses in the inner IP header mark the true source and final destination for the packet.

A common use of tunnel mode is to support VPN networks where connections are secured by means of IPsec.

Note: IPsec tunnel mode does not work directly with a gateway that employs network address port translation (NAPT), unless that gateway can parse the security parameter index (SPI) for the port information. Symantec security gateways work properly with NAPT, but third-party security gateways may not.

Figure 7-4 shows the difference in structure between a standard IP datagram, an IP datagram in transport mode, and an IP datagram in tunnel mode.

Figure 7-4 Transport and tunnel modes



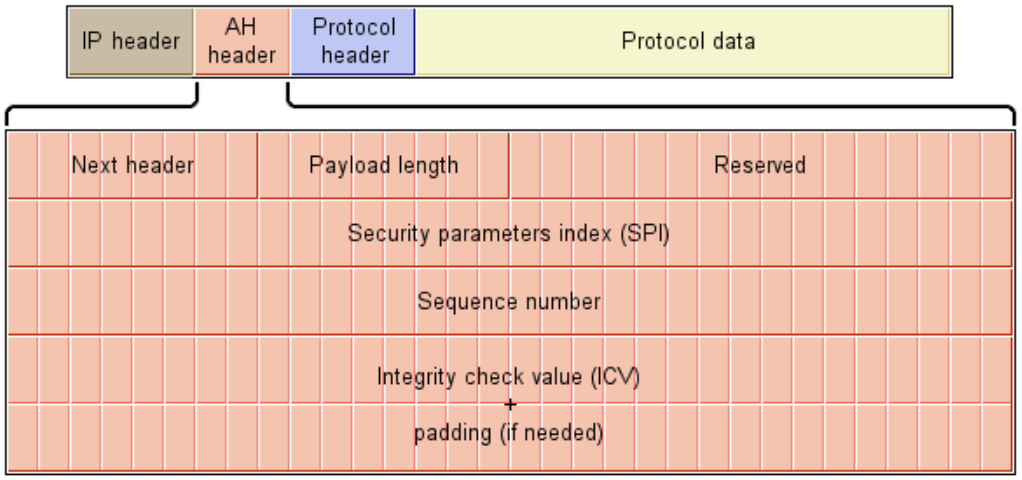
Data integrity protocol

The data integrity protocol defines what portion of the IP datagram to use when calculating and verifying its authenticity. The security gateway supports two different protocols, AH and ESP, to protect either the entire IP datagram, or just the upper-layer portion.

Authentication header (AH)

AH provides authentication, integrity, and replay protection to the entire IP datagram. AH achieves this by calculating an integrity check value (ICV) based on content that should not change during transit. AH then positions its own header between the packet's IP header and payload, announcing to the remote system that AH is in use. When the packet arrives at the remote system, the ICV is again recalculated, and compared to the original ICV. If the values do not match, the packet is discarded. Figure 7-5 shows an expanded view of the AH header.

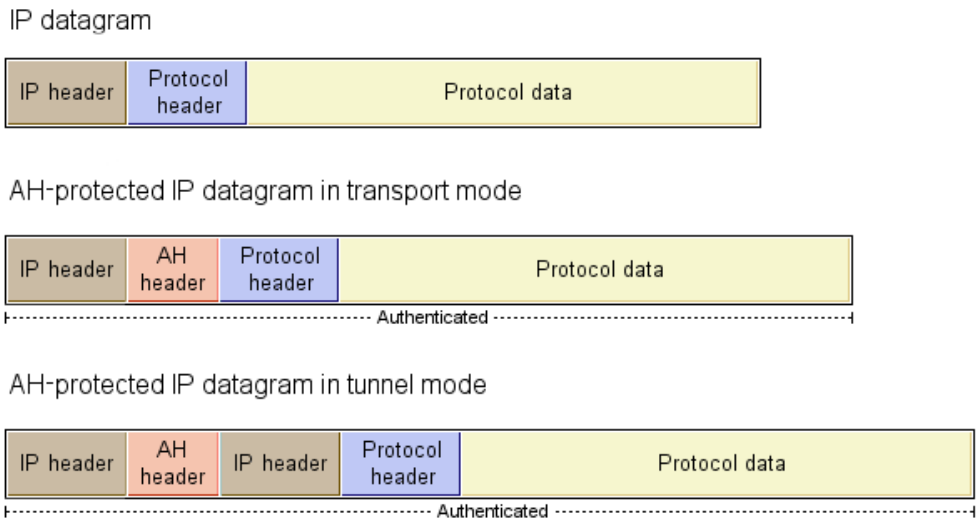
Figure 7-5 AH-protected IP datagram with expanded AH header



Although AH guarantees that the data has not changed, it does not hide or encrypt the data. Additionally, the AH header is calculated based on all packet information. The IP header, protocol header and protocol data are all sampled, and the ICV is built from this information. Because AH uses this method, it can only be used when connections do not use network address translation (NAT). Regardless of the transportation mode used, with NAT, the IP header would have one of its addresses changed. When the packet reaches its destination, the computed ICV does not match the original ICV, and the packet is discarded.

Figure 7-6 shows packets using the AH protection mechanism in both transport and tunnel modes, and what portion of the packet is protected.

Figure 7-6 AH-protected IP datagram in transport and tunnel modes



Encapsulating security payload (ESP)

ESP provides confidentiality, data integrity, data source authentication, and replay protection to most of the IP datagram by inserting an ESP header after the IP header and any IP options, and appending an ESP trailer. The IP datagram payload is an upper-layer protocol with its respective data, or another entire IP datagram. The ESP header is not encrypted but a portion of the ESP trailer is. Enough of the ESP trailer (the authentication portion) is in clear text to allow the decrypting system to process the packet.

Note: ESP is the most commonly used data integrity method.

Figure 7-7 shows an expanded view of the ESP header, and Figure 7-8 shows an expanded view of the ESP trailer.

Figure 7-7 ESP-protected IP datagram with expanded ESP header

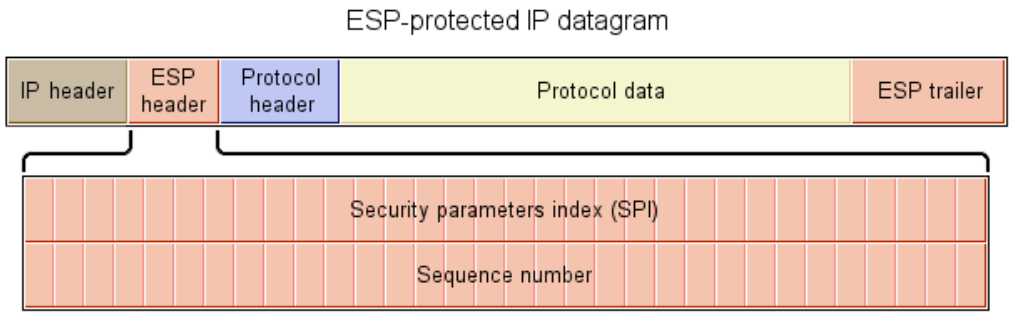


Figure 7-8 ESP-protected IP datagram with expanded ESP trailer

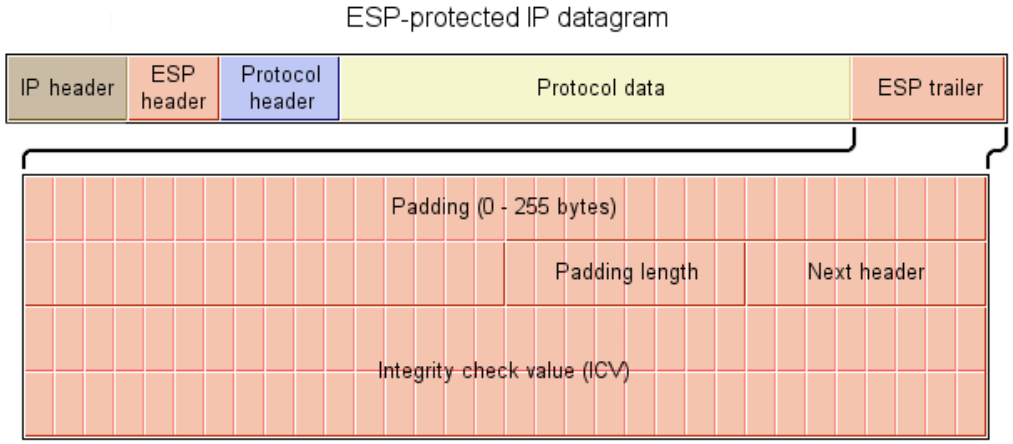
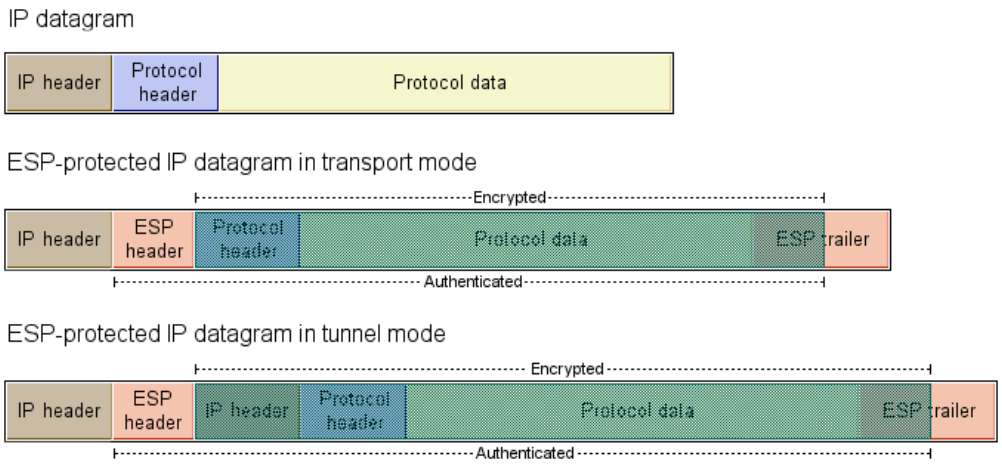


Figure 7-9 shows IP datagrams using the ESP protection mechanism in both transport and tunnel modes, and what portion of the packet is protected.

Figure 7-9 ESP-protected IP datagram in transport and tunnel modes



Note: If you use AH in your VPN policy and you also use a data privacy algorithm (AES, Triple DES, DES), both ESP and AH are applied to the packet.

Data privacy preference

Data privacy is provided by encryption algorithms which convert plaintext (readable form) into an unintelligible form called ciphertext. Decrypting the ciphertext converts the data back to its original form (plain text). Encryption methods are either asymmetric or symmetric.

Asymmetric ciphers

Asymmetric encryption is a form of encryption that uses two different keys, called key pairs, with one key for one for encryption and one for decryption. Asymmetric encryption is most often seen in use where users want to assure that the recipient is the true intended target. For example, User A wants to send a personal email to user B, but wants to make sure that no one else can read the email, even if they get the message by mistake. User B maintains his own key pair, one public and one private, and makes available his public key. User A encrypts the email with user B's public key, and then sends the email to user B. Because user B is the only one with the key pair's private key, user B is the only one that can decrypt the message.

Symmetric ciphers

Symmetric encryption methods only require one key for both encryption and decryption. Symmetric ciphers that act on blocks of data are called block ciphers. The size of the block used for a given block cipher is dependent on the algorithm. In contrast, stream ciphers operate on data one byte at a time. Block ciphers are used exclusively with IPsec. Some common examples of symmetric ciphers include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric block cipher that is used to protect electronic data. The AES algorithm is capable of using cryptographic keys of 128 bits (AES with 16-byte key), 192 bits (AES with 24-byte key), and 256 bits (AES with 32-byte key) to encrypt and decrypt data in blocks of 128 bits. The Security Gateway Management Interface configuration window uses the byte notation, instead of bit notation, with one byte being equivalent to eight bits.

Data Encryption Standard (DES)

The Data Encryption Standard (DES) was originally developed in 1974 by IBM, and adopted as a standard in 1977. DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key. However, only 56 bits are actually used. The least significant bit (right-most) bit in each 8-byte block is a parity bit, and is unused. This results in only 7 of every 8 bits being used, yielding 56 bits. DES takes a 64-bit block of plaintext as input, and then executes its algorithm on the plaintext 16 times, producing a 64-bit block of ciphertext.

Triple DES

DES was effective for its time, but is now easy to break with today's rapidly advancing technology. Most institutions serious about security bypass DES and move on to either Triple DES or AES. Triple DES is, in effect, the DES algorithm applied three different times. Therefore, its understandable that it takes three times as long to encrypt or decrypt with Triple DES as compared to DES. However, the level of security improvement varies depending on how the implementation is carried out. The Symantec implementation of Triple DES uses three different keys, encrypting with the first key, decrypting with the second key, and then encrypting with the third key. Like the DES algorithm, only 168 bits (3 times 56) are actually used for the entire encryption process instead of all 192 bits.

Data integrity preference

Encapsulation and encryption are important aspects of VPNs, but one of the most important pieces is to ensure that the original data sent is also the data received. Data integrity ensures that this takes place. Typically, a checksum or digest is calculated on the sending end, based on the data being sent. The receiving end then recalculates using the same algorithm on the received data. If the calculated values at both ends match, the data has not been tampered with.

MD5

The MD5 algorithm takes as input a message or datagram of arbitrary length, and produces a 128-bit message digest (fingerprint) of that data. This digest is then recomputed on the receiving end to verify that the data has not changed in transit. The MD5 algorithm was developed by MIT Professor Ronald L. Rivest and is discussed in more detail in RFC 1321.

SHA1

The Secure Hash Algorithm, Version 1.0 (SHA1), is a cryptographic message digest algorithm similar to the MD4 family of hash algorithms produced by MIT Professor Ronald L. Rivest. SHA1 takes a message less than 2^{64} bits in size and creates a 160-bit message digest. SHA1 was also designed to make it difficult to find another message which matches the hashed result. SHA1 is slower but considered to be more secure than MD5.

Data compression preference

Compression algorithms work by detecting duplicate patterns in data, and then minimizing the representation of the duplicate data. The larger the number of duplicate patterns, the better the compression is. For example, if the pattern the appears many times in a long document, the compression algorithm could create a new, compressed file that lists the string once at the beginning, and then includes a pointer back to this string at every other location that string the would normally appear. The benefit of this is that the pointer would require less space to store than the original string, essentially reducing the size of the compressed file.

Because there is some minor overhead included with compression, files with no duplicate patterns, or very few duplicate patterns, may actually end up being larger in size when compressed than the original. This is also the key reason why compression is performed prior to encrypting data, as a good encryption algorithm leaves almost no duplicate data.

The security gateway supports both the DEFLATE and LZS compression algorithms. Additional information on the DEFLATE compression algorithm is found in RFC 1951 and additional information on the LZS compression algorithm is found in RFC 1974.

Warning: Turning on compression is highly CPU intensive, and degrades the security gateway's performance with tunnel traffic.

Tunnel encryption keys

The encryption method used to keep tunnel traffic private requires tunnel encryption keys. These keys must either be manually defined or generated dynamically. While it is more common to have keys generated dynamically, the security gateway both static and dynamic tunnel encryption keys.

Static keys

VPN tunnels support static configurations, where tunnel parameters are created at each security gateway. Both ends have to have the same parameters, including secret keys, security parameter indexes (SPIs), authentication schemes, encryption methods, and so forth. However, this system is cumbersome for several reasons:

- Administrators can enter the wrong information by mistake.
- Administrators have to select SPIs from a list of unused SPIs.
- Administrators have to negotiate what encryption and authentication schemes to use.
- There is no way to implement key expiration except manually.

Dynamic keys

The Internet Key Exchange (IKE) protocol allows for the negotiation and dynamic creation of IPsec tunnels. The Internet Security Association and Key Management Protocol (ISAKMP) defines the procedure to negotiate keys, establish SPIs, negotiate transforms, and provide key expiration for greater security and flexibility in VPN setup. Key negotiation, security parameter indices, and transform negotiations are all done dynamically, and for this reason, there is no field for key generation when an IPsec/IKE policy is selected. The security gateway's IKE component negotiates with its peer IKE application on the other device to determine the encryption algorithm keys and authentication algorithm keys and SPIs of the IPsec protocol (AH, ESP) for a specific VPN.

The negotiation occurs in two phases. In Phase I, the IKE application creates an IKE security association with its peer to protect Phase II of the negotiation, which determines the protocol security association for the tunnel. For Gateway-to-Gateway VPN tunnel connections, either system can initiate Phase I or Phase II renegotiation at any time. Both specify intervals after which to renegotiate. For Client-to-Gateway VPN tunnel connections, only the client can initiate Phase I or Phase II renegotiation. Phase II renegotiation is referred to as quick mode renegotiation, because no Phase I renegotiation is performed.

VPN Policies

Rather than configuring data privacy, data integrity, and data compression algorithms for every tunnel you create, the security gateway lets you configure standard, reusable VPN policies and then later apply them to multiple secure tunnels. VPN policies group together common characteristics for tunnels, and allow for rapid setup of additional tunnels with the same characteristics. The security gateway also includes a handful of commonly used VPN policies, for both static and dynamic tunnels.

Note: You can create more than one policy, varying the components you select for each one. Ensure that your naming conventions let you distinguish between policies that use the same encapsulation mode. When you are ready to create your secure tunnels, clearly defined naming conventions make selecting the correct VPN policy easier.

Global IKE Policy

The security gateway comes with a predefined global IKE policy that automatically applies to your IKE Phase 1 negotiations. This global IKE policy works in conjunction with the IPsec/IKE VPN policy you configure, providing the parameters for Phase 1 negotiations for your IKE tunnel, while the VPN policy you configure and select provides the parameters for Phase 2 negotiations.

The configurable elements included in the global IKE policy shipped with the security gateway are as follows:

Policy Name	Name for the policy.
Data Privacy Preferences	Encryption algorithm used for packet data. Assigning more than one algorithm defines that the first one is tried, and if unsuccessful, the next algorithm is tried. Available encryption algorithms include DES and Triple DES.
Data Integrity Preferences	Hash algorithms used for packet authentication. Assigning more than one algorithm defines that the first one is tried, and if unsuccessful, the next algorithm is tried. Available hash algorithms include SHA1 and MD5.
Diffie-Hellman Groups	Diffie-Hellman is the standard IKE method of establishing shared keys. Group 1 and group 2 are the Diffie-Hellman group numbers available for establishing these IKE session keys. Group 1 is 768 bits long and group 2 is 1024 bits long. Using group 2 is more secure but it also uses more CPU power.
Connection Timeout	Indicates the timeout limit (in seconds) for establishing a connection. If you are using slower authentication or encryption methods, and your connection requests are timing out, you might want to increase this time limit.

Chapter 8

Monitoring security gateway traffic

This chapter includes the following topics:

Active connections

Current and recently finished connections are monitored through the Active Connections window. This window provides general information on all active connections, including the type of connection, the source and destination IP address, the time the connection started, the time the connection finished (if applicable), and the rule that allowed the connection. This window also shows all blacklisted hosts. Viewing the properties of a connection shows the source and destination ports, and the source and destination interfaces.

In addition to viewing connections, the Active Connections window lets you kill undesired connections. Killing a normal session immediately terminates that connection. Killing a blacklisted host entry lets that IP address once again attempt to connect to the security gateway.

Note: Killing a connection does not prevent that connection from coming back. To effectively prevent a connection from reestablishing, you should first create a new or modify an existing rule to deny the connection before killing it.

View logs

Log files maintain a record of all activity to or through the security gateway. You can search and filter log files to display only pertinent information, or leave unfiltered to display all activity. The View Logs window provides detailed information on all connections and connection attempts made.

The log file messages format has changed. A log message now consists of a message code, message text, and a parameter list. For example, a message that once appeared like this:

"Jun 27 14:45:16.864 felix rtspd[590]: 120 rtspd Info: Daemon Started"

now looks like this:

> "Jun 27, 2003 14:45:16.864 felix rtspd[590] 117 INFORMATIONAL: Daemon starting, Program Name=rtspd, Operation=Initialize, Resource=rtspd, Status=Success, State=Starting"

This new format consolidates similar messages, and improves on the information presented in a message. For example, it should now be clear whether or not a service or daemon started successfully. This new format is also compatible with the format used by the Symantec Enterprise Security Architecture (SESA) environment.

Additionally, if you are familiar with text format log files, notice that log files are now stored in binary. The logging engine writes log files in binary format, and offers some significant advantages over their text counterparts; identical log messages are now consolidated and the binary log format lets log files be parsed by a translator service and localized.

Because log files are stored in binary by default, third-party utilities like tail or text editors can no longer be used to view them without changing the default logging method. Enabling text logging instructs the security gateway to write out two separate versions of the log file, one in binary, and the other in text. However, there is a performance impact as the security gateway now has to write two log files instead of just one. Alternatively, the flatten8 utility is used to convert a binary log file into a text log file. The flatten8 utility also lets you tail the log file (view the last n lines, where n is any positive number), and follow the log file (view the last n lines that dynamically update when new entries arrive).

Collecting statistics on connections

The security gateway produces many different types of messages in response to system and network activity. Each message consists of a message number, the message text, and a list of parameters that generated the message. For example, if you want to collect specific information on individual connections, you might look for log message 121, which indicates a statistics message. Log messages categorized as 121 provide information on the duration, type of service, source, and destination for every connection through the security gateway. If your company billed for the time active connections use, 121 messages give a complete record of usage. The information captured by 121 messages depends upon the type of connection and the data passed through the security gateway on the connection.

Most connections lasting longer than two minutes are logged after two minutes and every hour thereafter. Telnet connections are not subject to this rule, since Telnet sessions frequently last for hours. The security gateway logs a message for Telnet immediately. If a Telnet connection lasts longer than an hour (3600 seconds), the security gateway logs a message at every hour mark and another message when the connection is closed.

Changelog

The security gateway uses a program called changelog to backup the current log file and start a new one. After running changelog, the old file is stored in a folder for that day, sorted first by year and then month. Clicking Browse in the View Logs window brings up the list of old log files. A second changelog operation the same day adds the suffix (1) to the log file name; a third adds (2), and so forth.

Note: If you run the changelog binary from the command-line while the SGMI is still open, the log file will change correctly, but the log file shown in the SGMI log file view will not update. Closing the SGMI and reconnecting will update the view to the correct log file.

Managing the log file size

If left unchecked, log files can grow very large in size. It is critical that you are aware of the amount of space taken up by both the current log file, and any back up files. Files that grow in size, using up all available space on the disk, cause performance problems.

When a log file exceeds 200 Mb, or the amount of disk space available for logging drops below 5 MB, action is taken to increase the amount of space available. The security gateway either switches to a new log file by running changelog, or deletes an old log file. The security gateway deletes a log file only if it has not been modified within the last 24 hours. If the security gateway cannot get space for logging by running changelog or deleting an old log file, the system stops.

Flatten utility

The flatten8 utility is shipped on the included CD and lets you perform simple log file management from the command-line. The flatten8 utility reads in the log message information from the system's XML files, and then parses in real-time the binary log file, substituting the actual error text message for its binary counterpart.

Most often, this utility is used to convert the binary log file to a more usable format for a third party utility, such as an ASCII text editor. This utility is also used to review the most recent messages, or directed to show just statistics messages.

usage: flatten8 [-h] [-r|-s|-D] [-f] [-u seconds] [-t n] [-x xmlpath] log file ...

Where:

-h Print this message and exit.

-r Only has an effect when -s is used. Do reverse lookups on IP addresses.

-s Output stats only.

-D Do not print out error information.

-f Follow output. (Binary files, default interval 2 seconds).

-u Follow update interval in seconds. (Implies -f).

-t Tail the last 'n' log messages.

-x Next argument specifies path to XML dictionary files. This argument should not need to be used, as the XML files are placed in the default location during installation.

SESA event gating

One of the strengths of the Symantec security gateways is that they are capable of reporting events to Symantec's SESA architecture. By doing so, you can correlate events from many security gateways into a single report. The SESA event gating option appears in the local SGMI because you configure the messages to report to SESA prior to joining the security gateway to the SESA environment. The SESA architecture is beyond the scope of this book. Additional information on the SESA architecture, and its advantages can be found in the *Symantec Enterprise Security Architecture Administrator's Guide* and the *Symantec Advanced Manager for Security Gateways, Symantec Event Manager for Security Gateways Administrator's Guide*.

All security gateway log messages have been classified into SESA event classes and subclasses. Additionally, each log message has been tagged with one of three possible values, which include always, sometimes, or never being logged to SESA. Events marked as always being logged to SESA are always logged, regardless of whether or not their associated class or subclass has been selected under the SESA Gating option. Similarly, messages marked as never being logged to SESA are never logged. Messages marked as never being logged to SESA are low-level messages that are only of interest to a local administrator. The SESA Gating option focuses on only those messages that are marked as sometimes being logged to SESA. If selected, they are logged to SESA.

Messages logged to SESA may not always appear identical to what is seen in the local log file. The majority of log messages sent to SESA appear very similar to their local counterparts, but there is some minor variations from time to time.

Note: If you join a security gateway to SESA, the default configuration sends only a small subset of events to SESA. Turning on all events incurs additional overhead, and may slow system performance. Carefully consider your selections when determining the events to send to SESA.

The major SESA classes and subclasses that log messages are assigned are listed in Table 8-1.

Table 8-1 SESA event classes and subclasses

Class or subclass	Description
Statistics	Provides statistical information about each connection.
Security Gateway	Provides for possible attack, process killed, and remote management connection events.
Authentication Failures	Any log message indicating that a user has been denied access to a service due to an authentication failure.
Network	Logs detailed network errors between two endpoints of communication, a range of addresses for filtering, or a specific network client request.
Configuration	Reports configuration information about a network driver or network service.
Authentication	Reports network events at the driver level normally generated by the filter driver or VPN services.
IDS/IPS	Intrusion events found by the intrusion detection and prevention component.
Duplicate	Notifies SESA that the local logging service (logserviced) has consolidated messages.
Management	Logs detailed information on entity management, configuration issues, and system reconfiguration.
Reconfiguration	Reports to a global administrator when a severe configuration problem has been found, and a reconfiguration of the component is necessary. These messages are normally about the DNS configuration or configuration files.
Antivirus	Viruses found by the antivirus scan engine. The proxies may also log a virus found message.
General	Provides general logging of information. This class would be used when log messages do not fall into any other class or subclass.
Connection	Lower-level, connection-oriented messages.
Rule	Reports any action that was denied by an explicit rule, or implicit rule (those that violate security gateway acceptable behavior).
State	Reports state change information about a component or hardware feature of the security gateway. Included in this subclass are start and stop messages, as well as hardware CPU temperature.
Version	Reports the version number of the security gateway and its components.
Component	Includes errors related to process interaction.
Violation	Reports component interactions that violate policies.
Core	Reports errors occurring within components that result from fundamental system or communication errors.
License	Includes errors related to licensing.

Four of the event classes, IDS/IPS, Duplicate, Antivirus, and License are greyed out and marked as unmodifiable. These event classes are always sent to SESA and cannot be changed.

Reports setup

The reports setup section defines how configuration reports should be saved and displayed to the administrator. Reports saved in HTML are displayed in the window to the right of the report selection list. To view PDF reports, the management host must have Adobe Acrobat Reader installed. The security gateway displays reports generated in PDF in a separate window. From this window, you can save the report.

To print reports, you must configure and attach a printer to the management host. You can configure reports to print in many of the standard sizes and formats, including letter, legal, executive, A4, and A3.

Configuration reports

The security gateway management interface provides a series of system configuration reports. Generated in real-time when selected, these reports are stored locally and are viewed with any standard Web browser if generated in HTML format, or Acrobat reader if generated in PDF. All reports begin with a cover page that shows when the report was last generated. Table 8-2 shows a complete list of the supplied reports, including what each report covers.

Table 8-2 Available configuration reports

Report	Description
Antivirus	Summarizes the current configuration of the antivirus scan server, and all scanning options. (appliance only)
Authentication Method	Reports the methods of authentication and extended authentication available. Covered information includes the security gateway ID for this protocol, the description, and, if applicable, a primary server, alternate server, and shared key.
Address Transform	Details all address transforms including the default address transforms VPNTunnelEntryTransform and VPNTunnelExitTransform. Covered information includes associated NAT pools, interfaces the connection arrives and leaves through, the description, the type of connection entering and leaving, and the type of address transform.
Advanced Option	Summarizes configured advanced options including the name of each variable, its description, and its value.
Content Filtering	Shows the current state of content filtering on the security gateway.
DNS Record	Details configured DNS records. Information displayed is dependent on the type of record. Fields include record type, access level (public or private), network address, aliases, and description.
Filters	Lists the filters currently configured, including the policy they are granting (allow or deny), the description, packet direction, packet protocols, and network endpoints.
H.323 Alias	Shows if the security gateway has been configured with an H.323 alias and the actual server to which it is sending requests.
IDS/IPS	Displays the current state of IDS/IPS on the security gateway. (appliance only)
IP Route	Presents a table of all configured routes.
License Features	Shows the current license state for all security gateway features.
LiveUpdate	Lists the current LiveUpdate configuration for antivirus, content filtering, and IDS/IPS.
Local Administrators	Shows all of the administrator accounts for the security gateway.

Table 8-2 Available configuration reports (Continued)

Report	Description
Logical Network Interface	Shows all defined logical network interfaces.
Machine Account	Lists all configured systems, and the functions they can perform.
NAT Pool	Details any configured network address translation (NAT) pools, including the starting and ending addresses in the pool, the addresses being modified, and the description.
Network Entity	Lists all configured network entities. Information reported is dependent on the type of entity, and can include the network address, MAC address, and description.
Network Interface	Displays information on all of the hardware adapters in the machine. It includes information on the IP address assigned to each interface, whether or not spoof protection is enabled, and whether or not the interface allows multicast traffic. In addition, it also shows if one or more filters are assigned.
Network Protocol	Lists all of the protocols either in use or available, including any custom protocols.
Notification	Displays all configured notifications. You can set notifications to alert administrators of noteworthy security gateway conditions.
Proxy Services	Lists the current state, enabled or disabled, or each of the proxies. Information displayed is dependent upon the section viewed, and includes default and customized field parameters.
Redirected Service	Lists any configured service redirects, including the requested address, requested address netmask, redirected address, redirected port, and description.
Rule	Lists configured definitions to allow or deny traffic based on network entities. There are several fields of information displayed including the applicable entry and exit points, the source and destination, protocol, authentication method, and description.
VPN Tunnel	Displays all configured Gateway-to-Gateway and Client-to-Gateway VPN tunnels. Information displayed includes the VPN policy, local and remote endpoints, local and remote gateways, and description.
VPN Tunnel Policy	Lists all of the VPN policies currently configured, including the respective parameters of each. It also covers the Global IKE policy.
Service Group	Displays all configured service groups. Covered information includes the group's description, protocols, applied ratings, and any additional parameters.
System Parameters for Location	Shows the minimum password length for gateway and Bellcore S/Key passwords.
System Parameters for Policy	Reports on the assigned forward filter (if any), if reverse lookups are enabled and the time to wait for them, and whether or not the host name is used in the log file in place of the IP address.
System information	Details the current system state, licensed options, and SESA Agent status, for SESA-enabled security gateways.
Time Period	Shows any defined time restrictions available for use. Fields include the starting and ending time, day, and year.
User Account	Shows configured static users. Fields include the name, authentication type, and description.
User Group	Details any user groups currently configured.
Services	Shows the current status of key daemons and services. Gateway services interact with other security gateway processes. Information reported is specific to the service described. For example, the LDAP window section lists the primary and alternate LDAP servers, and the OOBA section covers timeout periods and whether or not to use SSL.

Table 8-2 Available configuration reports (Continued)

Report	Description
Virtual Private Network	Summary report that combines both the Secure Tunnel Policy report and Secure Tunnel report. Lets the administrator see an overall view VPN configuration.
Master Configuration	Generates a report with all security gateway configurations. When run, this report runs all of the other reports and collects them in one file.

Notifications

Notifications free up valuable time, letting administrators focus on other responsibilities while ensuring that security gateway issues do not go unnoticed. Notifications are configured to alert administrators by email, pager, or SNMP message when events requiring attention occur. You can also configure the security gateway to invoke an application, potentially resolving an issue without administrator intervention.

Each notification method the security gateway generates is built from a common template. All notifications consists of one or more message severity levels and a time frame to watch. The differences for these methods lie in the action taken when the security gateway should invoke the notification.

Audio

Audio notifications play an audio file on the security gateway and alert anyone present that a defined event has taken place. When configuring an audio notification, ensure that the selected audio file is present and is a .WAV file. Audio notifications are specific to the Symantec Enterprise Firewall (software).

Information on configuring or modifying audio notifications is found in your product's administrator's guide.

Email

Email notifications send the text of the log message that generated the notification to an administrator or other intended recipient through email. When configuring a mail notification, ensure that the email address is valid and resolvable.

Information on configuring or modifying mail notifications is found in your product's administrator's guide.

Pager

Pager notifications transmit the text of the log message generating the notification to a designated paging device. Pager notifications require that you enter the telephone number of the pager to call. To support paging notifications, if the security gateway is a Symantec Gateway Security 5400 Series appliance, you must have a connected and supported USB modem. The software-based Symantec Enterprise Firewall supports only serial modems.

Information on configuring or modifying pager notifications is found in your product's administrator's guide.

Client

Sometimes, a message sent by email or pager is not enough. Action may be needed immediately. The security gateway supports invoking a client application or script as a notification method. For example, you may decide to shutdown a machine entirely, preventing all access until the administrator can fully assess the situation, when a critical or emergency situation arises. For other situations, you may call a script to email several people, instead of just one. If a client notification is configured, the security gateway calls the named program as it appears in the definition of the notification, and appends the date and contents of the message text (including parameters) to the end of the command line.

Information on configuring or modifying client notifications is found in your product's administrator's guide.

SNMP notifications

The Simple Network Management Protocol (SNMP) is a request/response protocol that communicates management information between applications and agents. SNMP provides support for traps, or notifications, to advise an administration application when one or more conditions exist. Traps are network packets that contain data about the host sending the trap.

For SNMP managers to understand traps, the names of any device-specific variables to be exchanged must be agreed upon. These variable names are stored in the Management Information Base (MIB) of the agent and manager software. Although the appropriate MIB values for security gateway SNMP alerts are pre-configured, SNMP management stations that receive alerts from the security gateway must have this information incorporated into their MIBs.

The security gateway distribution CD-ROM includes MIB files for SNMPv1 and SNMPv2 alerts. Besides configuring the MIB, the agent and manager must also agree upon how to verify that the traps are generated by the security gateway. The differences between SNMPv1 and SNMPv2 alerts are explained in the following sections.

SNMPv1 traps

SNMPv1 traps contain a community field, which is a text string holding a value agreed upon between a manager and the agents that it manages. The security gateway and any SNMPv1 managers with which it communicates must both be configured to accept the same community string. The administrator of the SNMP management station can assign a community value for the security gateway to use.

Consult the SNMP management documentation for its configuration information. Configuration and modification information for SNMPv1 traps is found in your product's administrator's guide.

SNMPv2 traps

SNMPv2 traps contain object identifier (OID) values that represent the source and destination parties and trap context. An OID is a sequence of integers separated by periods, such as 1.3.1.6.1.4. You can use different privacy methods to hide the information in the trap as it crosses the network, and different authentication methods to ensure the identity of the trap originator.

The security gateway supports only unauthenticated, non-private traps. However, the manager and security gateway must still agree upon values for the source and destination parties and the trap context. The administrator can assign an OID to represent the security gateway (the source party) and tell you the OID that represents the management station (the destination party).

The administrator should also assign an OID value for the trap context. The trap context must include both Internet-defined MIB variables and security gateway-defined MIB variables. The snmpv2.mib file provides the administrator with enough information to do this.

Configuration and modification information for SNMPv2 traps is found in your product's administrator's guide.

Advanced options

Occasionally, the default state of the security gateway must be fine-tuned to run at peak performance. This fine-tuning is accomplished through parameters whose values can change. These variables are only modified under specific circumstances.

Warning: Before modifying any security gateway advanced option, you should first contact Symantec Technical Support to determine if the change is necessary.

Table 8-3 lists security gateway modifiable parameters.

Table 8-3 Advanced options

Parameter	Description
antivirus.inf.content_blocked_notice	Definable message to send when a virus is detected and blocked. The default is, “The message being sent to you had a virus and was blocked by Symantec’s AntiVirus Scan Engine.”
antivirus.liveupdate.protocol	Network protocol used by LiveUpdate when retrieving antivirus updates. The default is HTTP.
antivirus.liveupdate.workdir	Working directory for the LiveUpdate engine when processing antivirus updates. This defaults to /Symantec/LiveUpdate.
cluster.dbglevel	Level of debug messages for HA/LB. The default value is 1 and can range from 1 (minimal) to 5 (verbose).
cluster.fotimeout	Time in seconds to wait before creating a failover record for a connection. Failover records are costly, so setting this value below 30 seconds has no affect. The default is 60 seconds. If this parameter is set to any value less than 30, that value is ignored, and 30 seconds is used instead.
cluster.hashlb	Determines whether or not the cluster uses the hash algorithm to direct packets. The default value is 0 (off). Acceptable values for this parameter are 1 (on) and 0 (off).
cluster.hbtimeout	Time in seconds that nodes wait before pinging each other to ensure other nodes are reachable. The default value is 4 seconds. Acceptable values include any number of seconds, but the value chosen should be reasonable.
cluster.lprotect	Enables and disables load protection. When load protection is on, strained nodes drop random packets to alleviate load. The default value is 0 (off). Acceptable values for this parameter are 1 (on) and 0 (off).
cluster.lprotectpcnt	Percentage of random packets to drop if cluster.lprotect is set to 1 (on). The default value is 7. Acceptable values include any positive integer between 1 and 100 inclusive.
cluster.symroute	Symmetric routing. The default is 1 (on). Acceptable values for this parameter are 1 (on) and 0 (off).
cluster.useport	Use 5-tuple (source, source port, destination, destination port, protocol) as one session. The default is 1 (on). Acceptable values for this parameter are 1 (on) and 0 (off).
cluster.viplb	Load balancing for the VIP incident node assignment. The default value is 0 (off). Acceptable values for this parameter are 1 (on) and 0 (off).
contentfilter.liveupdate.protocol	Network protocol used by LiveUpdate when retrieving content filtering updates. The default is HTTP.

Table 8-3 Advanced options (Continued)

Parameter	Description
contentfiltering.liveupdate.workdir	Working directory for the LiveUpdate engine when processing content filtering updates. This defaults to /Symantec/LiveUpdate.
entrust.client_ini_file	Name of the client initialization file used with Entrust user authentication. The default is isakmp.ini.
entrust.client_password_file	Name of the client password file used with Entrust user authentication.
entrust.client_profile_file	Name of the client profile used with Entrust user authentication. The default is isakmp.epf.
http.browser.capabilities.allow_all	Enable/disable all other browsers that support proxy authentication. The default is enable.
http.browser.capabilities.ie.version	Defines the minimum version of Microsoft Internet Explorer that supports proxy authentication. The default is 3.0.
http.browser.capabilities.java.version	Defines the minimum Java version of a Java-based browser that supports proxy authentication.
http.browser.capabilities.ne.version	Defines the minimum version of the Netscape Web browser that supports proxy authentication. The default is 1.1.
http.browser.capabilities.thirdparty	Defines third-party browser that supports proxy authentication.
http.denied_url_patterns.add	Defines new patterns to be added to the URL list.
http.denied_url_patterns.remove	Defines new patterns to be removed from the URL list.
http.external_proxies	Defines external Web proxies that would be used by internal user's Web browsers. Proxy servers are defined using either their DNS-resolvable fully-qualified domain name (FQDN) or IP address with netmask (for example, 10.10.10.10 & 255.255.255.255).
log.level.<message ID>.newlevel	Used to map a log message to a different message level. <message ID> should be replaced with the original message ID. For example, log.level.120.newlevel=150.
log.level.<message ID>.pattern	Message pattern to be matched. <message ID> should be replaced with the original message ID. For example, log.level.120.pattern. The value should be a regular expression pattern.
log.stats.<protocol>.firstmessage	Elapsed time after a connection using the defined protocol that statsd waits before sending a statistics message to the log file. The field <protocol> should be replaced with the protocol name. For example, log.stats.telnet.firstmessage.
log.stats.<protocol>.interval	Time that statsd waits to log the next statistics message to the log file for the defined protocol. The field <protocol> should be replaced with the protocol name. For example, log.stats.telnet.interval.
log.stats.default.firstmessage	Default time in seconds to for statsd to start logging messages. The default is 120 seconds.
log.stats.default.interval	Default time in seconds for statsd to wait before logging another message. The default is 3600 seconds (1 hour).
misc.httpd.extensionblacklist	Option to modify the default behavior of the file extensions filter for HTTP traffic. By default, this option is set to False and any file extensions added to the list designate allowed file extensions. All others are blocked. IF this option is changed to True, all file extensions added to the list are now blocked, and all others are allowed.

Table 8-3 Advanced options (Continued)

Parameter	Description
misc.httpd.mimeblacklist	Option to modify the default behavior of the blocked MIME types for HTTP traffic. By default, this option is set to True and any MIME types listed are blocked. Anything not listed is allowed. IF this option is changed to False, all MIME types listed are now allowed, and all others are blocked.
misc.httpd.urlblacklist	Option to modify the default behavior of the URL list for HTTP traffic. By default, this option is set to False and any URLs added to the list designate allowed sites. All others are blocked. IF this option is changed to True, all URLs added to the list are now blocked, and all others are allowed.
misc.logServiced.logsesa	Determines whether or not logging to SESA takes place. The default is false. You must join SESA to begin sending messages. This flag does not have an affect until you send log messages to SESA.
ooba.mime_types.add	Defines new MIME types to be added to the OOBA server.
ooba.mime_types.remove	Defines new MIME types to be removed from the OOBA server.
portcontrol.enable_tcp_ports	TCP ports to enable. The default is 2456. **Note:** 2456 is the default used by the Security Gateway Management Interface when managing the security gateway. Unless the default has changed, this variable should always include 2456. If the default port has changed, this parameter should always have that new value defined. If not, you can no longer manage the security gateway from a remote Web browser.
portcontrol.enable_udp_ports	UDP ports to enable.
tacacs.auth_key	Secret key used for authentication with the TACACS+ server.
tacacs.auth_method	Method for authentication with the TACACS+ server.
tacacs.server_ip	TACACS+ server IP address. Acceptable arguments include any valid IP address.
ui.inactivity_timeout	Period of time in minutes of inactivity before re-authentication is required. The default is 15 minutes.
ui.status_poll_interval	Period of time in seconds between system status calls. The default is 30 seconds.
vultured.elapsetime	Time in seconds between vulture scans. The default is 60 seconds. Setting this value to -1 disables the vulture process.
vultured.users	System users permitted to run processes and services. The default is root, daemon, and bin for the Symantec Gateway Security 5400 Series and Administrator for the Symantec Enterprise Firewall.

Chapter 9

Preventing attacks

This chapter includes the following topics:

Antivirus (appliance only)

Viruses are a leading cause of concern to the enterprise. Viruses can easily spread and pose major threats to critical business operations and financial investment. Implementing antivirus protection at the security gateway is a critical step in protecting your network against viruses and other related threats. The security gateway provides comprehensive virus protection and lets you control scanning by individual services so you can configure virus protection specific to your needs.

Understanding antivirus

The security gateway implements Symantec antivirus technology using a scan engine that detects viruses, worms, and Trojan horses in all major file types. The scan engine also detects mobile code, such as Java, ActiveX, and standalone script-based threats. The security gateway uses Symantec's key antivirus engine technologies, including Bloodhound for heuristic detection of new or unknown viruses and Symantec's Norton AntiVirus Extension (NAVEX), which provides protection from new classes of viruses automatically by means of LiveUpdate.

The security gateway's antivirus component includes a decomposer that handles compressed file formats and nested levels of files. For embedded files, scanning is limited to certain file types based on extension. The scan server handles the following archival and encoded file types:

.amg	.arj	.cab	.exe	.gz	.hqx
.lha	.lz	MIME	.rar	.rtf	.ss
.tar	.txt	.tnef	/uue	.z	.zip

Symantec antivirus technology is fully supported by the Symantec Security Response Team. Symantec's Security Response engineers work 24 hours per day, 7 days per week, tracking new virus outbreaks and identifying new virus threats.

Antivirus scanning has a client/server relationship. The SMTP, HTTP, and FTP proxies act as clients that pass files to the antivirus scan server. The antivirus scan server can either be a licensed component of the local security gateway, or a licensed component of a remote security gateway. When you specify antivirus scanning for one of these proxies, files are passed by that proxy to the antivirus scan server. The antivirus scan server then scans the files for viruses and mail and container policy violations. Files that have unrepairable infections or that violate the established policy are blocked, while clean files and infected files that are repaired are allowed to pass through.

Virus detection

When Symantec engineers identify a new virus, information about the virus (a virus signature) is stored in a virus definitions file. Virus definitions files are updated periodically by means of Symantec's automated LiveUpdate feature. When the scan engine scans for viruses, it is searching for these virus signatures. To supplement detection of virus infections by virus signature, the scan engine includes Symantec's patented Bloodhound technology, which heuristically detects new or unknown viruses based on the general characteristics exhibited by known viruses.

Bloodhound heuristic technology

Researchers at Symantec have developed two types of heuristics for Symantec AntiVirus. The first, Bloodhound, is capable of detecting upwards of 80 percent of new and unknown executable file viruses. The second, Bloodhound-Macro, detects and repairs over 90 percent of new and unknown macro viruses. These statistics are staggering considering the growth rate of computer viruses. Bloodhound requires minimal overhead since it examines only programs and documents that meet stringent prerequisites. In most cases, Bloodhound can determine in microseconds whether a file or document is likely to be infected by a virus. If it determines that a file cannot be infected, it immediately goes on to the next file.

Bloodhound and executable viruses

Bloodhound uses artificial intelligence (AI) to isolate and locate the various logical regions of each program it is told to scan. It analyzes the program logic in each of these components for virus-like behavior and simulates this behavior to determine whether the program is a virus.

Bloodhound and macro viruses

Symantec Bloodhound-Macro technology uses a hybrid heuristic scheme to detect and repair more than 90 percent of all new and unknown macro viruses automatically. For example, every time the scan engine scans a Microsoft Word document, Bloodhound-Macro sets up a complete virtual Microsoft Word environment into which it loads the document. The macros contained in the document are run as they would be in the word processing application. Bloodhound-Macro monitors the macros as they run and watches for them to copy themselves from the host document to another virtual document. Bloodhound-Macro also stimulates the copied macros and verifies that they can further propagate.

Norton AntiVirus Extension (NAVEX) technology

NAVEX is a technology that lets Symantec update the scan engine during routine virus definitions updates. That means no inline revisions or time-consuming upgrades are necessary to ensure that antivirus protection stays current, regardless of platform, even against new virus threats.

The scan engine is made up of dozens of complex search algorithms, CPU emulators, and other program logic. The scan engine examines a file to determine whether the file contains viruses. The scan engine scans files and disks for virus fingerprints (unique sequences of bytes known to be contained in viruses). These fingerprints are stored in the virus definitions files downloaded each week. The scanning engine also repairs infected files.

Occasionally, a new virus or class of viruses emerges that is not detected by existing scan engines. These viruses require new algorithms for detection—and consequently a new scan engine. With the NAVEX technology, Symantec engineers can quickly upgrade the fundamental scan engines, with no extra cost or effort required on the part of the customer.

Symantec Striker technology

Symantec Striker technology identifies polymorphic computer viruses, which are the most complex and difficult viruses to detect. Like an encrypted virus, a polymorphic virus includes a scrambled virus body and a decryption routine that first gains control of the computer, and then decrypts the virus body. However, a polymorphic virus also adds a mutation engine that generates randomized decryption routines that change each time a virus infects a new program. As a result, no two polymorphic viruses are the same.

Each time Symantec Striker scans a new program file, it loads the file into a self-contained virtual computer. The program executes in this virtual computer as if it were running on a real computer. Inside this virtual computer, the polymorphic virus runs and decrypts itself. Symantec Striker then scans, detects, and repairs the virus.

Antivirus scanning

Antivirus scanning is implemented as a client/server relationship between the supported application proxies (FTP, HTTP, and SMTP) and the antivirus component. The appliance is most often configured to issue scan requests to its local scan engine, however you can configure the appliance or another software-based security gateway to direct antivirus scan requests to another appliance. Directing requests to another appliance is referred to as off-box scanning.

Antivirus scanning is enabled when a rule is created that allows FTP, HTTP, or SMTP traffic, and the respective proxy has antivirus scanning enabled. Both uploaded and downloaded files are scanned. Prior to scanning a new file, the configured scan policies and exclude list (if selected) is checked. The options include scan all but exclude, or scan all files not on the excluded extension list. Actions taken include scan and repair infected files and delete files that cannot be repaired, or scan and delete all infected files. This lets the administrator set scanning policies per protocol instead of having just one global policy, and provides the infrastructure to support off-box scanning.

Using the scan policies requested by the proxies and configured mail policies, the antivirus component scans files for viruses and mail policy violations. Normally, files that have unrepairable infections, or that violate the established mail policy are blocked; clean files and repairable infected files are allowed through. To comply with European Union (EU) privacy laws, which state that virus-infected eamils cannot be modified or repaired, you can configure the security gateway to add an x-virus header to the email, which prevents the email from being repaired or deleted. For a complete list of directions to configure x-virus support, consult the *Symantec Gateway Security 5400 Series Administrator's Guide*.

When the proxy determines that scanning is necessary for a particular file, it passes the entire message, including the file to be scanned, to the antivirus component. Once the entire message is received, the antivirus component begins the scan. After scanning is complete, the antivirus component returns one of three things to the proxy:

- The original message and file
- The original message and a cleaned file
- An error code and possibly a message indicating that file contained a virus and could not be cleaned

Messages are sent to client processes (FTP client, mail client, or Web Browser) which inform the user when viruses are found and cleaned, or when files are found to be unrepairable; The proxies also send virus detected messages to the log file.

Client comforting

In some instances, clients that wait for a response from the proxy, especially when scanning a large file from a download manager, can exceed their default timeout values. If the client does not see data transferred within a default length of time, the client resets or terminates the connection. In addition, when scanning FTP or HTTP connections, the client's user may get concerned when they do not see any evidence of the requested file. The user may attempt to restart the transfer several times, or attempt to abort the connection completely.

You can enable client comforting, also known as antivirus comforting, on files to alleviate application timeouts and user confusion. SGMI lets you define both a file size and buffer size for use with client comforting. By default, the buffer is set at 256 KB and the file length is set at 15000 KB. The value defined for each of these determines when the security gateway uses client comforting. Client comforting operates at a minimum of the buffer size, even if the file size is defined to be smaller. You should use the file size to define values larger than the standard buffer size.

For files smaller than the defined file size (or buffer size if it is larger than the file size), the normal scanning process takes place, and should finish well before any timeout period kicks in. If client comforting is configured, files larger than the defined file size are partially sent, indicating to the client that activity is taking place. If the antivirus component detects a virus in the file, the proxy attempts to remove the partial file, and aborts the connection. The user sees that the connection aborted, and for FTP sessions, is told why over the control connection. The proxy also logs the fact that a virus was detected.

If the antivirus component determines that the file is clean, the connection continues as normal. This keeps a steady flow of data going between the client and server, keeping the connection alive and the user aware. It also improves the speed of the file transfer when scanning is on in a rule.

There are two limitations to proxy comforting:

- The antivirus component cannot delete a partial file on the client once the file leaves the security gateway.
- When client comforting is active, the proxy cannot take advantage of the scan and repair option because part of the file is already at the destination.

Container policy

Attachments in email messages are a common method that attackers use to send viruses. Sometimes, these attachments are compressed files that hide the virus nested inside. Symantec's antivirus component can scan these compressed files for viruses. However, there is overhead introduced because the entire attachment must be read in, expanded in a protected environment, scanned, and then either approved or denied. If the file is within another compressed file inside the original compressed file (called nesting), the process again adds some additional overhead to process.

SGMI lets you determine exactly how many layers deep that you would like the scan engine to process. The default value is 10 layers, and you can configure this number to be as large as 50. You can also set the maximum attachment size, with the default being 100 MB. Carefully consider maximum values, bearing in mind that the larger the values are set, the more time it may take to process mail. If an attachment exceeds any of the defined limits, the attachment is not scanned, and the email is blocked.

Intrusion detection and prevention (appliance only)

The intrusion detection and prevention (IDS/IPS) component works with the driver, analyzing packets, and sending alerts back to the driver for any suspicious traffic it detects. The driver calls the IDS/IPS component just after checking for any blacklisted addresses or interface filters. If the IDS/IPS component detects something suspicious, an event is sent back to the driver. The driver then determines the next course of action for the packet.

The IDS/IPS component consists of two major pieces:

- State machines
- Signature engine

State machines

One piece of the IDS/IPS component is the state machines. State machines are faster than signature-based attack detection mechanisms, as each state machine focuses on only one protocol, and generally requires fewer updates. State machines are updated when the agreed upon behavior of a protocol is changed (a new RFC, for example), or if a well-known signature-based method is to be incorporated into the state engine.

The core detection methodology used by the state machines is protocol anomaly detection (PAD). The state machines perform attack detection at the application layer, focusing on the structure and the content of the communications. The state machines then compare observed behavior during network protocol exchange and note deviations from expected behavior; deviations are considered in context, and potentially with data from other sources. Unlike misuse detection which searches for patterns of known behavior, PAD can detect zero-day attacks of unknown patterns because of the deny all approach to protocol irregularity; if a connection doesn't adhere exactly to definition in the state machine, it's flagged as suspicious.

Signature engine

The signature engine provides a detection mechanism for non-anomalous attacks. As robust as the state machines are for detecting attacks, there are some attacks that are dealt with more effectively through a signature engine. The signatures included with the appliance are not modifiable. The IDS/IPS component compares events to its included signatures, and responds if it finds a match. Because the signatures are hard-coded and unmodifiable, the comparison is done at a high rate of speed.

Global gating

The global gating switch decides if the security gateway is going to wait for an answer from the IDS/IPS component before sending a packet up the stack. If global gating is on, the driver does not process the packet until it hears back from the intrusion detection component. If global gating is off, the call is still made to the IDS/IPS component, but the packet is not held waiting for a response; if an event is triggered because of the packet, it is logged only. Global gating is off by default. Gating is applied on a per event basis.

Table 9-1 shows the effects of enabling or disabling the various gating options.

Table 9-1 Event filtering

Global gating	Event enabled	Event gated	Passed up the stack	Reported	Comments
Off	Yes	No	Yes	Yes	When global gating is off, you cannot selectively gate attacks.
Off	No	No	Yes	No	When global gating is off, you cannot selectively gate attacks.
On	Yes	Yes	No	Yes	None.
On	No	No	Yes	No	If an attack is disabled when global gating is on, it is automatically ungated.
On	Yes	No	Yes	Yes	You can selectively ungate attacks.

Logical network interfaces

Logical network interfaces are an abstraction of the system's network interfaces. Logical network interfaces let an administrator apply the same general configuration to multiple security gateways, even if those security gateways have different physical hardware adapters installed. The benefit of logical network interfaces becomes clear when you understand that you can create rules that apply to a logical network interface instead of a specific interface with a static IP address.

When you run the System Setup Wizard on each security gateway, the name defined for each network interface creates a corresponding logical network interface. If you configure each security gateway to use the same logical network interface naming convention when you configure the network adapters in the System Setup Wizard, you can apply the same rules that use those logical network interface names to each security gateway.

The Logical Network Interfaces window lets you turn on and off several of the security features associated with the logical network interface.

Allow multicast (UDP-based) traffic

Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information. Multicast, which uses the Internet Group Management Protocol (IGMP), is based on the concept of a group, which is defined as an arbitrary number of receivers that have expressed an interest in receiving a particular data stream. Using a multicast router, packets sent from a single source are reviewed, replicated, and then sent only to the members in the multicast group. Systems not part of the multicast group do not receive unecessary traffic.

Multicast packets can also traverse networks, assuming that the router between the two networks is multicast enabled. This is another distinct advantage over using the broadcast address on a network, as routers do not forward broadcast packets.

Enabling this option configures the security gateway to allow multicast traffic.

Note: You cannot configure the security gateway to act like a multicast router and rebroadcast multicast packets to protected hosts. Allowing multicast traffic only instructs the security gateway not to filter and drop multicast packets it receives.

SYN flood protection

A standard TCP connection consists of three phases. In the first phase, the client sends a TCP request to the server with the SYN bit turned on. When the server receives the packet, it responds with its own packet that has both the SYN and ACK bits enabled. Finally, the client acknowledges the receipt of the server's packet by sending a response with the ACK bit enabled. At this point, a socket is created, and both systems can communicate with one another.

Attackers may try to overwhelm a server by initiating a SYN flood attack. In a SYN flood attack, the first and second phases of the three-way handshake take place. However, the client never responds to the server's SYNACK packet. Often, the original client address is spoofed, so the response goes to an invalid IP address. This leaves an open, pending connection on the server, and consumes some of the server's resources. In normal situations, the server is capable of handling these pending connections. However, when the server is repeatedly flooded with requests, and the requests are never closed, the server can be quickly overburdened.

The security gateway offers three methods of SYN flood protection. One method, the adaptive SYN flood handling algorithm, is active all of the time and offers continuous, low-overhead protection. The other two methods, algorithm 1 and algorithm 2, employ different methods to handle large numbers of SYN packets. Each has its own purpose.

Adaptive SYN flood handling algorithm (always on)

The security gateway's driver, as well as the TCP layer, maintains the state of all connections through the security gateway. To protect itself, the security gateway continuously monitors and tracks the number of unestablished connections in the driver. Every minute, the driver reviews the number of unestablished connections to see if any have exceeded the default establishment period of 60 seconds. Any connections that have exceeded the 60 second timeout period are terminated by sending a RST to the TCP layer. This terminates the connection in both the driver and the stack, and immediately frees up the memory.

The adaptive SYN flood algorithm also acts as a throttle when the security gateway is under attack. In addition to terminating unestablished connections every minute, this algorithm also keeps track of how many connections were terminated during each interval. If the number of terminated connections in a given cycle (one minute) exceeds 100, the security gateway confirms that the system is under attack, and cuts the establishment time in half to 30 seconds.

Algorithm 1

Algorithm 1 instructs the driver to first check the trusted client list for each new SYN it receives. If the connection is not in the trusted client list, the driver adds the connection information, along with a time stamp, to one of 16 lists determined by the destination port. Each list holds a maximum of 32 pending connections.

If the driver sees that a selected list has reached the 32 record maximum, the driver examines that list, beginning with the first record, for a connection that has exceeded the 60 second time limit. The driver drops the first expired connection record it finds and appends the new connection record to the end of the list. The algorithm does not assume that the first connection record in the list is the oldest. Times on each connection record are adjusted if the security gateway receives a SYN resend.

Connection records are removed from the lists when the final phase of the three-way handshake is completed (the security gateway receives the corresponding ACK from the client). If the three-way handshake is successful, the security gateway adds the connection record to the trusted client list.

Algorithm 2

Algorithm 2 relies on the fact that many SYN flood attacks originate from a spoofed IP address. For each new connection, algorithm 2 begins by checking the security gateway's trusted client list. If the connection is not in the trusted client list, algorithm 2 instructs the driver to hold the connection's source address and sequence number, create a bogus ACK, send this packet to the connection's source IP address, and wait for a response. If the source IP address is legitimate, the security gateway should receive a RST (reset) back from the source address as the source address would not have a pending connection for the bogus ACK's sequence number. When this happens, the security gateway considers the original connection valid, and adds the source address to its trusted client list.

Algorithm 2 is a lightweight, low-overhead method to detect SYN flood attempts, but is reliant on the client using a normal network stack. Some special breed stacks may not automatically send out a RST, and using algorithm 2 would prevent those systems from connecting. There is also the highly unlikely probability that an initial connection arrives and begins the verification process, and before it completes, a new connection arrives with an identical sequence number. In this case, the second connection overwrites the pending information for the first, forcing the first connection to connect again.

Enable port scan detection

A port scanning attack is an attempt to connect to one or more ports to identify compromisable services. Port scanning detection is an optional feature that the security gateway administrator can configure. When port scanning is enabled, it is enabled for reserved ports under 1024. Port scan detection does not prevent the security gateway from being scanned; it is a notification only. If the driver suspects port scanning, it logs the interface on which the packet arrived, the source IP address, the IP header, and the total length of the IP packet. Once the driver has collected and logged this information it passes the packets.

Enable spoof protection

The spoof protection flag governs whether or not spoof protection database entries are generated for this logical network interface. Database entries are produced by compiling a list of user-defined network entities associated with an interface. Once available, the database is loaded into the security gateway's driver, where it is used to verify that packets sourced from a defined entity are actually arriving on the correct interface of the security gateway.

Provide recursion and expose private DNS information

This logical network interface option alters the behavior of the security gateway's DNS daemon, instructing it to search both the private and public DNS databases stored on the system before replying. With this flag enabled, all otherwise-private host names are available for both forward and reverse lookups to queries on this interface. For example, a common use of this option would be to allow resolution of internal names and addresses by servers in the service network.

Enabling this options also instructs the network interface to support external recursion. This means that this interface can now be used as a public DNS server. For example, if this option is enabled on a security gateway's external interface, any host external to the security gateway can send a DNS request to the external interface, and the security gateway performs the lookup and responds to the host.

Suppress reset and ICMP error messages

This flag instructs the security gateway driver to conceal its presence in response to unauthorized communication attempts. To the traffic initiator, it appears as if the target host does not exist, or is offline. This happens because the driver no longer sends a reset or ICMP error notification back to the requesting host.

This feature is useful in the situations where only a handful of ports are open on the untrusted sides of the security gateway. In this scenario, this feature would reduce the likelihood of detection through network scanning, thus reducing the possibility of a directed attack. If there are a significant number of open ports on the untrusted sides, the likelihood of an attacker detecting the presence of the security gateway increases, and minimizes the benefit of this option.

Note: The effects of enabling this option are contrary to the accepted standards of polite network communication. Additionally, suppressing resets and ICMP error responses can cause problems, such as interfering with path MTU discovery or concealing the root cause of service unavailability. Carefully review your network topology to determine if enabling this option is warranted.

Address transforms

Some administrators believe that if they use reserved network addresses, specifically those defined in RFC 1918, they do not have to concern themselves with hiding a host's real IP address. On the surface, this security approach seems sound. RFC 1918 addresses do not route publicly, so an attacker external to the company perimeter cannot direct an attack at an internal host, even if the attacker know's that host's IP address. However, some administrator's forget to consider the attacker that breaches the perimeter and gains access to a host on the protected network. Once inside, that attacker, armed with the real IP addresses of hosts on the network, can direct intelligent attacks to compromise other systems. For example, if an attacker knows that a company Web server is at IP address 192.168.1.5, that attacker can focus the types of attacks to Web-based attacks only and not waste time trying other types.

Understanding address transforms

To protect the real source or destination IP address, the security gateway uses address transforms to modify source and destination IP addresses in packet headers as packets pass through. An address transform instructs the security gateway to change the source IP address, source port, destination IP address, destination port, or any combination of these just before the packet leaves the security gateway. Address transparency, redirected services, and network address translation (NAT) all employ some type of address transform, and each has its own reason for being used.

Packet headers hold the source IP address, source port, destination IP address, and destination port. To better understand how each type of address transform differs, this section assigns names to these four fields both before and after the packet passes through the security gateway. These names are used in the following sections on address transparency, redirected services, and network address translation to show before and after header values.

Table 9-2 shows the four header fields before passing through the security gateway.

Table 9-2 Header information from the original source packet

Name	Description
src	Real source IP address.
srcport	Real source port.
dst	Perceived destination IP address.
dstport	Perceived destination port.

Table 9-3 shows the same fields in the packet after the packet leaves the security gateway. However, the names have been altered slightly because there is a possibility that the security gateway changed one or more of the fields.

Table 9-3 Modified header information after packet exits the security gateway

Name	Description
src’	Perceived source IP address.
srcport’	Perceived source port.
dst’	Real destination IP address.
dstport’	Real destination port.

Address transparency

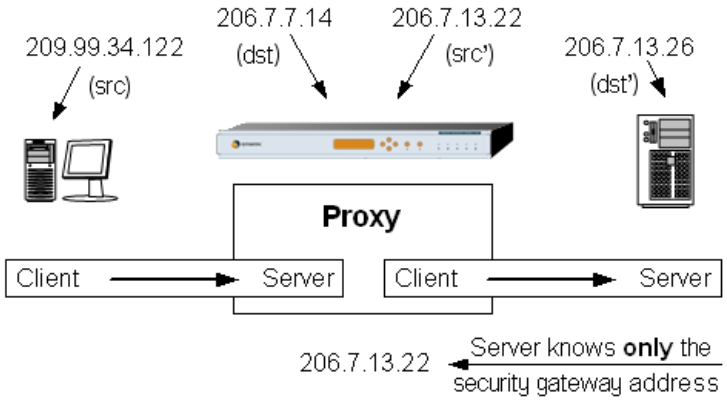
Address transparency determines whether or not one side of a proxied connection (either the client or the server) is permitted to see the real IP address of the other side. Depending on the type of transparency (client-side or server-side), the security gateway modifies either the source or destination IP addresses in the packet header. If enabled, this modification takes place on the outbound connection.

However, you should not use the terms inbound and outbound to describe address transparency. The security gateway treats all traffic that originates outside of the security gateway as an inbound connection and all traffic that originates from an interface on the security gateway as an outbound connection. Every connection that passes through the security gateway incorporates both of these. The connection originates from a host, enters the security gateway through one interface as an inbound connection, is processed by the security gateway, and then handed to another interface as an outbound connection for exit. Instead, think about transparency in terms of client and server.

Client non-transparency

With client non-transparency, the security gateway hides the real IP address of a client from the server by changing the source IP address in a packet's header to the IP address of the security gateway's outside interface (src != src'). By doing this, the server believes that the connection request originated from the security gateway. Responses from the server are directed back through the security gateway. Before forwarding these responses to the client, the security gateway changes the destination address in the packet header from the security gateway's IP address to the client's real IP address. This looks like Figure 9-1.

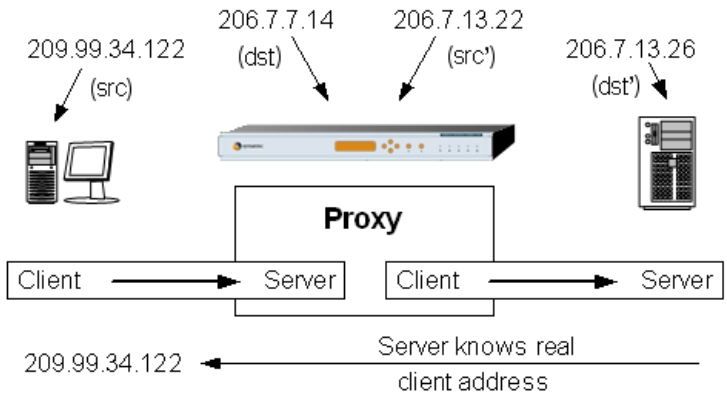
Figure 9-1 Client non-transparency



Client transparency

You can also configure the security gateway to leave the source IP address unchanged (src = src'). The connection still goes through the security gateway, with all appropriate checks enforced, but the server understands the real source of the request, and its responses are sent back to the real IP address, not the security gateway. This is known as client transparency because the security gateway is said to be transparent (invisible) in the connection from the server to the client. This is shown in Figure 9-2.

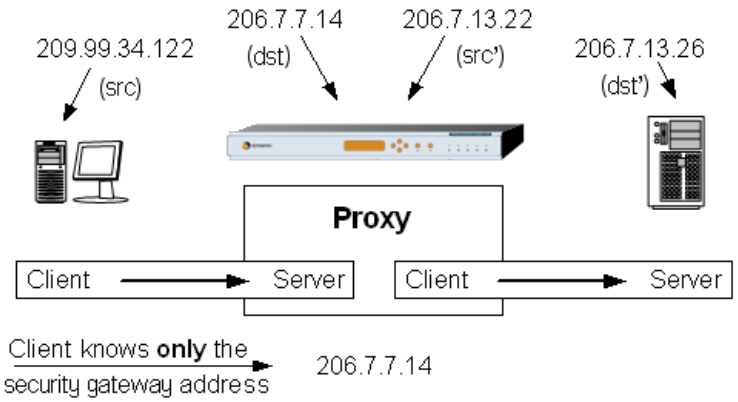
Figure 9-2 Client transparency



Server non-transparency

It is usually a good idea to hide the IP address of servers that sit on a service network. Clients external to the service network direct their connection requests to the security gateway to gain access to the desired service. For anyone external to the service network, it appears that the security gateway itself is providing all services. The security gateway replaces its address in the header's destination IP address field with the server's real IP address (dst != dst') and forwards the packet on to the server. Responses from the server travel back through the security gateway, even if the server knows the client's real IP address, and the security gateway replaces the header's source IP address with its own IP address. The client believes that it is only dealing with the security gateway. Figure 9-3 shows this address hiding.

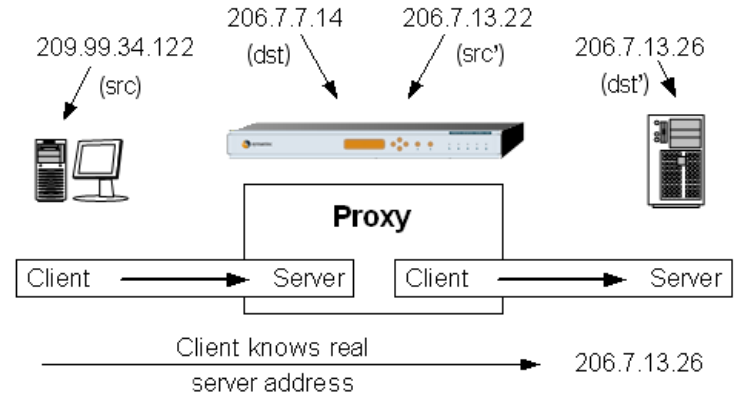
Figure 9-3 Server non-transparency



Server transparency

You can configure the security gateway to accept connections for a service hosted by an external server. When the security gateway accepts these connections, it still acts as a proxy, with the same level of security. Assuming that you created the appropriate rule, the connection is allowed through, and the header left unchanged (dst = dst'). Because the client uses the real server address, you can describe the security gateway as transparent in the connection from the client to the server. This is shown in Figure 9-4.

Figure 9-4 Server transparency



Transparency guidelines

When considering address transparency, keep the following guidelines in mind:

- By default, the security gateway uses client non-transparency (changing the source IP address) and server transparency (leaving the destination IP addresses unchanged) for packets that originate from an inside host and are destined to an outside host.
- By default, the security gateway uses client transparency (leaving the source IP address unchanged) and server non-transparency (changing the destination IP address) for packets that originate from an outside host and are destined to an inside host.
- Client transparency is useful for hosts that need to track the real source of the request. For example, Web servers might use logging facilities to track the location of the hits on the server and some news servers require clients to provide actual IP addresses. For servers outside your security gateway, you can identify inside clients, but at the cost of revealing their IP addresses.
- Server transparency is useful when you host publicly accessible servers on one of your protected networks. Consider server transparency for an internal server with a routable address that is intended for public use, such as a news or Web server.

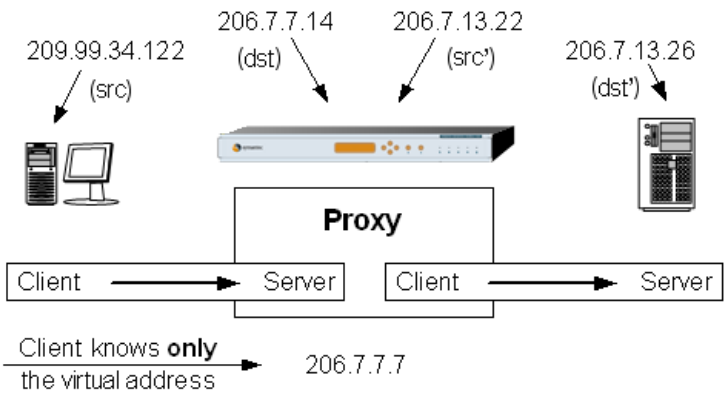
Redirected services

To support hidden addresses (non-transparency), the security gateway uses service redirection to tell the proxy where to direct incoming requests. A service redirect changes a packet's destination IP address (dst != dst') or destination port (dstport != dstport'). Through service redirection, you can configure the security gateway to redirect a connection request to some other system behind the security gateway.

Another benefit of service redirection is having the security gateway answer service requests for virtual IP addresses. Essentially, a service redirect creates a record that instructs the driver to forward packets matching the requested service and destination IP address to another, hidden machine. As long as the proper network routing to the security gateway is set up, the security gateway can answer for addresses that are not physically assigned to any adapter. This feature lets you publish an address different than the security gateway's real address, but still have the security gateway process the request.

Notice in Figure 9-5 that the client directs the connection request at 206.7.7.7 because this is the only published address to send connection requests. None of the physical interfaces have the IP address 206.7.7.7. However, ISP routing has established that all packets on the 206.7.7.x network be directed to the security gateway. This practice is common as it provides a single point of protected network access, and lets the security gateway examine each connection attempt. Because the driver has a record to answer for 206.7.7.7, packets sent to this address are handled appropriately.

Figure 9-5 Service redirection



Network address translation

Network Address Translation (NAT) establishes a relationship between the real IP address of a packet, and a translated IP address. This is commonly done to translate packets on non-routable networks into routable packets for travel across public networks, or to mask externally-sourced packets and make them appear as internally-sourced. NAT provides a method of guaranteeing that return traffic is routed back to the appropriate security gateway.

Understanding NAT

NAT is most often used for true address hiding and to alleviate the IPv4 address shortage. NAT partitions and controls network traffic. NAT is also used when connections to protected resources must originate from a specific network. For example, a secure Telnet server on a protected network may only allow connections that originate from that protected network; the connection is denied for anyone else attempting to use the service. Using NAT, the security gateway changes the source address of an external request to a protected network IP address. The internal server allows the translated connection, believing the connection originated internally.

NAT pools establish a range of one or more IP addresses used in address translation. Typically, addresses in these pools are part of the existing protected network. For example, if the protected network was 192.168.1.x, and the first 50 addresses were in use by hosts on that network, a NAT pool could be created that starts at 192.168.1.51. This pool could be as large as the remaining number unused addresses.

Warning: Never assign addresses to a NAT pool if they are already in use by a host. This causes network failure.

The security gateway can translate source addresses for transmitted packets and destination addresses for received packets. NAT substitutes the source IP address (src != src') of incoming packets with one from the assigned pool. The security gateway maintains a table of the pairings so that return traffic is switched back to the original IP address. As return packets arrive, the security gateway consults the table and switches the destination address (dst != dst') to match the original incoming source address.

NAT addresses do not time-out. As long as the connection is active, the client owns the allocated address. VPN connections are handled the same way; the NAT address supplied to the VPN connection does not time out. However, tunnels themselves can time-out due to inactivity or maximum connection time limits. When this happens, the connection is dropped, and the NAT address is released back to the pool.

Note: You must pass traffic to the proxies to NAT.

NAT is applied statically on a client-by-client basis. Individual addresses are always assigned when a specific connection request arrives. This is commonly used when routing requires the use of NAT and clients that connect need to be distinguished from other similar clients.

For example, assume you have a Web server on a protected network that only accepts connections from other hosts on the same network. Let's also say that you want to grant access to the Web server to several partner companies. You could create several NAT address transforms, one for each company. Whenever anyone from a company connects, they're always assigned the same IP address. By doing this, you could look locally to see which addresses are in use, and understand what companies are currently connected.

Anti-spam measures

The security gateway includes several features that help control the receipt of unsolicited email, often referred to as spam. Spam email generally arrives in the form of bulk email, improperly formatted SMTP traffic, emails with specific subjects, or from locations known to facilitate spam (open relays). For organizations, dealing with spam is expensive because it places an undue burden on network resources and eats into your employee's productive work hours.

You can use several security gateway features to limit types of email permitted into your organization. These features include:

- Checking whether or not the email comes from a server known to facilitate spam by making use of one of the several free open relay lists.
- Restricting inbound email to only mail destined for the organization by specifying a recipient domain.
- Using hard or soft recipient limits to control the number of emails received and limit bulk emailings.
- Filtering for patterns in mail headers to block messages with commonly used spam subject lines.
- Making use of DNS lookups on sending mail servers to confirm that they are correctly identified.
- Sending all email through the SMTP proxy with virus scanning enabled for full application inspection, as well as virus checking.

You can find configuration information for all anti-spam options in your product's administrator's guide.

Chapter 10

Ensuring availability

This chapter includes the following topics:

Limitations of non-clustered solutions

Security gateway uptime is critical. It is important to ensure that all personnel that make use of your company's network can perform their jobs, and are not hampered by loss of network connectivity. At a minimum, loss of the security gateway is a major inconvenience. What's worse is that it can result in lost productivity or revenue.

There are problems that can occur with any security gateway. Often, these problems concern allocation of machine resources (CPU time and memory) and redundancy. Companies of all sizes can encounter these problems.

Single-machine drawbacks

Companies with smaller network budgets often look for a single machine solution to address the issue of network security. However, a single machine is susceptible in several areas.

Single point of failure

If the security gateway is down, external users no longer have access to internal resources, and internal users are cut off from the rest of the world. Because of the importance of the security gateway, everything else must be dropped to resolve the issue.

Possible bottleneck

Especially in smaller companies, the security gateway is often tasked to perform additional roles over and above the role of network protection. As companies grow and the demand for bandwidth and processing power increases, a strong security gateway now may not be adequate to do the job in the future.

Dedicated administration

Because the security gateway plays such a critical role in your company environment, it may require a dedicated administrator.

Multi-machine concerns

Adding additional machines may address some single-machine issues. Multiple machines offer several access points for both internal and remote hosts. Multiple machines can also be assigned different tasks to break up the jobs that need to be performed.

However, using multiple machines present its own unique set of issues. Setting up several machines is more complex than setting up one. Instead of integrating one machine into the existing network infrastructure, multiple machines need to be added. Internal and external interfaces on each machine must be configured properly, and the networks that each machine is connected to must also be configured.

Each security gateway commonly has one of the IP addresses from your public company network (provided by your Internet service provider), and one from your private network. All machines that access your network usually point to the security gateway as a next-hop router; internal hosts point to the security gateway to gain Internet access, and remote users use the security gateway as a tunnel endpoint to connect to the protected network. To distribute the load, you may elect to point some hosts to the first gateway, some to the second, and so forth. However, if one of those security gateways fails, you have to quickly reconfigure all of the hosts that pointed at the failed system to point at a different security gateway.

Although adding additional resources begins to address the problems of a single-machine setup, it is really a trade-off. You have alleviated some problems, but created new ones.

Symantec's clustered approach

Symantec uses a cluster to resolve the high availability and load balancing issues faced by single and multi-machine environments. A cluster is a group of machines, called nodes, that ensure continued connectivity (high availability) and leverage their processing power (load balancing), even if one or more nodes fail. Symantec offers a complete, integrated solution that alleviates both single-machine and multi-machine concerns. In a cluster, multiple machines are grouped together and instructed to work as a single entity. All nodes in the cluster share the state information of all other nodes, and any node can immediately assume and support a connection for a failed node. Additionally, you can distribute work evenly among all node members, letting the cluster handle significantly more load than a single machine can.

Cluster components

The Symantec clustering solution uses the following components:

- Synchawk daemon
- Bullfrog daemon
- Virtual IP addresses (VIPs)
- Incident node
- Authoritative node
- Dedicated heartbeat network

Synchawk daemon

Synchawk is the daemon responsible for negotiating and coordinating cluster configuration information between nodes. Until a node has joined a cluster, synchawk lies dormant. Once the node has joined the cluster, synchawk broadcasts information about its revision number, cluster name, and unique cluster ID to other nodes in the cluster.

Periodically, each node in the cluster announces the revision it currently has, including that node's cluster ID and revision timestamp. The most current revision is chosen, and the node with that revision becomes the reference node. The synchawk daemon on each other node then pulls down the configuration from the reference node. Synchronization algorithms ensure that even if the system time on each node is different, the most current configuration is always selected.

Bullfrog daemon

The bullfrog daemon provides state sharing among nodes in the cluster, and continuously updates driver state information received from other nodes. Bullfrog also periodically pings other cluster nodes and maintains a table of which nodes are still active and can receive packets.

Virtual IP addresses

All configured network adapters have a unique physical IP address. Routing protocols prohibit two network adapters on a connected network from sharing the same IP address. In fact, most operating systems announce when two separate adapters sharing the same IP address are detected.

Each node maintains an ARP table that is used to map the IP addresses of other interfaces to their respective MAC addresses. As soon as an interface is configured, an entry containing the MAC address and IP address for the interface is placed in the ARP table. When ARPs and RARPs are broadcast on the network, each node looks at the information in its ARP table, and if the adapter information matches the request, that node answers. This is how each node on a network understands where to route packets to.

Symantec's cluster implementation uses virtual addresses to direct traffic. When a VIP is created, an adapter entry is placed in the routing table of each node in the cluster. Unlike physical network adapter records, the virtual adapter record on each node can and does contain the same IP address.

Each machine in the cluster shares the same virtual IP address for a given subnet, and is viewed as a potential candidate to receive packets. If one security gateway goes down, another security gateway can assume control and handle any new requests, providing continued connectivity to your network. All of this is done without having to change or reassign default gateways on any hosts. All hosts point to the VIP, and not the real IP address of a given node.

Because the VIP is assigned to a subnet, all of the nodes in the cluster on that subnet have the same virtual adapter. With load balancing configured, the cluster spreads out the connections more evenly over several different machines instead of always sending requests to one machine. This makes more efficient use of your network resources.

Incident node

Even though each node in the cluster has the same virtual adapter information, only one node can physically own the VIP at any given time. If this didn't happen, packets wouldn't understand to which security gateway they were supposed to go. When the VIP is established, internally, a node is chosen to answer ARP requests. This node is referred to as the incident node.

The incident node is responsible for maintaining a handle on the current condition of each of the nodes in the cluster, which includes tracking the nodes that need to be updated with state information. The incident node also bears the responsibility of directing incoming packets to the authoritative node. If a failure occurs on the incident node, another node in the cluster is automatically assigned control of the VIP and becomes the incident node.

When a packet arrives at the incident node, it is checked against the known connection list in the symmetric routing table. If an entry exists, the packet is processed on that node. If there is no entry, the incident node employs a hash algorithm to determine which node is authoritative for the connection. The hash algorithm assigns the numbers 0 - 31 as evenly as possible to all nodes in the cluster. With only two nodes, for example, the first machine is assigned the numbers 0 - 15, and the second node receives 16 - 31. The assignment pools grow smaller for each additional node added. Once the target node is determined, a new entry is placed in the symmetric routing table, and the packet is then directed to that node.

Authoritative node

The authoritative node is the decision maker for which node handles the packet. This node employs the defined algorithm to determine which machine should get the packet. Possible algorithms include round-robin and least load. If the selected node is able to handle the packet, that node becomes the owner for all packets in that connection. If the selected node is unable to handle a new connection, possibly due to high load, the packet is assigned to another node until accepted.

Heartbeat network

The heartbeat network is the subnet the cluster uses to share state information. This is also the network the incident node uses to keep track of which machines are still up and viable candidates for packets.

If licensed for HA/LB, the System Setup Wizard requires that you define the heartbeat network. Traffic on the heartbeat network is not encrypted. You should choose a private network as the heartbeat, and separate the heartbeat network from any other protected network to keep traffic to a minimum.

The heartbeat network uses five ports for clustering. When configuring the cluster, the wizard asks for a starting port, and then chooses the next four consecutive ports for the five used. Ensure that you have not picked a starting port that overlaps another port in use. There is no enforcement of the picked port, and if another service is operating on the port picked or derived, there may be conflicts.

Warning: Do not enable IDS on the heartbeat network. This degrades the performance of both the cluster and the security gateway.

Stateful failover

Stateful failover is set up with a rule and is a best effort approach. The stateful failover routines use a UDP connection to transmit information to other nodes in the cluster. Because there is no acknowledgement from the other nodes, there is no guarantee that each node in the cluster received the latest information. To help address this, the cluster sends updates every minute, reducing the likelihood that one node may be required to take over a connection without the correct information.

Using a rule-based method to enable stateful failover lets an administrator configure failover for one type of service, but not have failover for another. Tunnel connections employ stateful failover by default, and are the only connections that do not require a rule to enable stateful failover. In addition to tunnel connections, stateful failover is applied to HTTP, FTP, Telnet, TCP GSP, and TCPAP GSP connections; these connection types have stateful failover disabled by default, and require a rule to enable.

There is a penalty incurred when using stateful failover. With stateful failover enabled, new connections require a record in the state table, which is approximately 200 bytes in size. Because each state table is unique to its node initially, each state table must be propagated to all other nodes. Therefore, each node's state table grows by 200 bytes for each additional node in the cluster.

Carefully consider the types of service to set for failover, and the types to let fail. For example, HTTP connections are usually short-lived and numerous. For a large number of nodes in a cluster protecting the Web server, enabling stateful failover causes each node to trigger broadcast traffic to disperse the state information for each new connection. On very busy sites, this could significantly impact response time.

For longer-lived connections, such as FTP or VPN tunnels, it makes sense to enable stateful failover. In fact, stateful failover is automatically enabled for VPN tunnels because the only state information shared is the Phase 1 ID, which produces minimal state traffic. In the event of a failover, the new node performs a Phase 2 negotiation, transparent to the user. This may be seen as a small moment of unresponsiveness, but the connection should come back and resume normally.

To help reduce potential congestion, the clustering routines monitor all connections that have been assigned for failover. The security gateway sets an internal timer for these connections when established. If the connection does not last for at least 60 seconds, no state information is passed between nodes. This means that short-lived connections that live less than 60 seconds do not fail over, even if failover is selected. This retired time is reduced by setting the appropriate advanced parameter, but always defaults to minimum of 30 seconds.

Load balancing

A load balancing implementation that uses only the source and destination IP address to define a connection employs a 2-tuple (two distinct items) algorithm. There is a disadvantage to using this type of load balancing algorithm. Power users might connect to the same machine many times throughout the day. Because the source and destination IP address doesn't change, their connections are always handled by the same node because the algorithm always derives the same result.

The Symantec approach uses a 5-tuple (five distinct items) algorithm based on the source and destination IP addresses, the source and destination ports, and the protocol to determine which node to send packets. This more granular approach improves the cluster's load balancing effectiveness. Notice that even for a power user, the user is no longer locked into one node. Even though the source and destination IP address, the destination port, and the protocol would most likely stay the same, the source port is random. This means that for every new connection, the algorithm recalculates with at least one new parameter.

Cluster administration

Creating a cluster, adding nodes to a cluster, and deleting nodes from a cluster are all handled through the Cluster Wizard. Once a cluster has been created and defined, the status of the cluster is viewed using the monitoring page or through report generation. Cluster functionality is only available on systems licensed for cluster support.

Creating a new cluster and adding nodes

When creating a new cluster, you can choose any free node to set up the cluster, and that node becomes the reference node. The hardware and network configuration of the reference node becomes the basis for all other nodes. The reference node is implicitly added to the cluster, since it is the node from which the cluster creation sequence was initiated.

Once connected to the reference node, the user runs the cluster wizard. To build the cluster, new nodes are added. A cluster has to have two machines at a minimum.

When you choose to add a new node to the cluster, the reference node opens a secure management connection on port 2456 to the candidate node. The reference node then qualifies the candidate node, ensuring that the candidate node has the proper hardware configuration, has connections to the same networks as the reference node, is not a member of any other cluster, and has the proper cluster license.

If the candidate node passes the qualification stage, the reference node notifies the candidate node that it may join the cluster, and passes a small record to the candidate node. This record includes the cluster name, cluster ID, IP address of the reference node, and fingerprint of the reference node certificate. With this information, the new node is now able to communicate on the heartbeat network with the reference node. The secure connection between the reference node and the new node is closed as soon as the reference node executes a successful activate changes.

The new node is only aware of the reference node at this point because the small record passed by the reference node contained only the IP address of the reference node. The new node does not have a cluster configuration yet, so the new node listens to messages from the reference system. Once the new node determines that the reference system has the most current configuration, synchawk on the new node retrieves the configuration from the reference node. The new node now has the complete cluster configuration record, including information on any other nodes in the cluster. An activate changes is done on the new node automatically as part of the retrieval process, and the new node is now in sync with the cluster.

Configuration information for creating a cluster and adding nodes to a cluster is found in your product's administrator's guide.

Deleting nodes from a cluster

The node being deleted is left in one of two possible states after being removed from the cluster. The node either maintains the current configuration, minus the cluster attributes, or reverts back to its original state before joining the cluster. If you elect to keep the current configuration, the cluster configuration information is deleted, but the location and policy information is preserved and used as the active configuration. Choosing to revert back to the original configuration removes all configuration changes that took place after joining the cluster.

Warning: You cannot delete a cluster node from the node to be deleted; you must be on another node.

Configuration information for deleting nodes from a cluster is found in your product's administrator's guide.

Appendix A

Log messages

This chapter includes the following topics:

About log messages

This appendix describes all the messages that can appear in the security gateway log file. Each message has an identification number. The first digit of the message number identifies the severity of the message. The lower the number, the lower the severity. For example, messages numbered from 100 to 199 contain routine information whereas messages 700-799 are marked as emergency messages. Also associated with each message is one or more parameters. These parameters provide further details about the log message. Log messages take the format <date>, <component>, <message text>, where the message text includes the additional parameters if they exist.

Informational messages (100-199)

Informational log messages fall into the range 100-199. They are normally standard messages that indicate the security gateway is operating properly.

101 - Logging to file

Description: The program is logging the output to the file specified in the parameter.

101 - Precision

Description: Indicates the local clock precision in microseconds.

101 - Successfully installed hotfix

Description: The hotfix utility successfully installed the specified hotfix.

101 - Successfully installed hotfix bundle

Description: The hotfix utility successfully installed all hotfixes in the specified hotfix bundle.

101 - Successfully listed active hotfixes

Description: The hotfix utility successfully retrieved the active hotfix list.

101 - Successfully listed all hotfixes

Description: The hotfix utility successfully retrieved the list of all installed hotfixes.

101 - Successfully listed recent hotfixes

Description: The hotfix utility successfully retrieved the list of hotfixes installed with the most recent hotfix bundle.

101 - Successfully processed module

Description: The hotfix utility successfully processed the specified module as defined in the hotfix control file.

101 - Successfully uninstalled all hotfixes

Description: The hotfix utility successfully uninstalled all previously installed hotfixes.

101 - Successfully uninstalled hotfix

Description: The hotfix utility successfully uninstalled the specified hotfix.

101 - Successfully uninstalled recent hotfixes

Description: The hotfix utility successfully uninstalled the hotfixes that were installed with the most recent hotfix bundle.

101 - Symantec Network Security Management System starting up

Description: The security gateway proxies are starting up.

101 - Synchronization lost

Description: The security gateway lost synchronization with the peer. This occurs at system startup, and also when you are unable to communicate with the peer.

101 - Synchronized

Description: An appropriate peer is identified, and the clocks are synchronized accordingly.

101 - Time reset

Description: The clock and its peer were not synchronized, so the time was reset to rectify this problem.

102 - Shutdown command received, service exiting

Description: Each service is receiving a normal shut down command, initiated by the administrator.

103 - Closing connection

Description: The security gateway or proxy is closing a connection. A subsequent message provides the reason for the closing action.

103 - Closing connection (killed by operator)

Description: The operator requests the security gateway to close the connection. This message should have a matching connection message (105).

103 - Start bullfrogd process

Description: The bullfrog daemon is starting, cluster support commencing.

103 - Terminate bullfrogd process

Description: The bullfrog daemon is terminating.

104 - Feature is not enabled

Description: A security gateway feature is disabled because either an administrator disabled the feature using the GUI or a license does not exist for this feature. An administrator can enable this feature by obtaining the appropriate license.

104 - Re-read of new configuration file successful

Description: The configuration file has changed. A new configuration setting resulted in changed behavior as indicated by the parameters.

105 - Connection for service

Description: A connection has been made from the incoming host to the outgoing host for the service.

106 - Set debug level to <variable 1>

Description: This message displays the current debug level (defaults to the lowest value of 1). The user can set the debug level to a higher number to get more debug information.

107 - Closing log file

Description: The log file changes on a daily basis. At midnight, the changelog service renames the old log file to oldlogs/logfile.YYMMDD, in the location where the logs are stored. This message is an indicator that the old log file has been closed. This message is normally followed by an 108 message.

108 - Starting new log file, UTC offset used

Description: The new log file is now created and the Universal Time Coordinates (UTC) offset is at 0400.

109 - Re-reading configuration file

Description: A service is repeating the read of a specified configuration file. This is usually the result of an administrator reconfiguring the security gateway.

112 - Rule expired, re-scanning rules

Description: The time range associated with a rule has expired, so the connection has to be reauthorized.

115 - Successful authentication from remote management client

Description: A user has remotely connected to the security gateway through the GUI. The parameters indicate the identity and location of the remote connection.

116 - Remote management completed

Description: Remote management sessions include connecting to the security gateway from another host by means of the SGMI, secure remote login (SRL), or the remlogsuite of utilities (remotelogdir and remotelogfile). This message indicates that one of these remote management sessions terminated normally.

117 - Daemon starting

Description: A proxy or a security gateway service is starting normally.

117 - The Scan Engine has just started up

Description: The specified daemon (ftpd, dnsd or httpd) can use the antivirus scan server.

118 - Daemon exiting

Description: A proxy or security gateway service is exiting normally.

118 - Daemon exiting and disabled

Description: A security gateway server application exits, and is disabled because of problems.

118 - Daemon exiting. Attempting to use Symantec Client VPN on security gateway

Description: The client version of the component is not able to run on the server, so the daemon exits. Use the server version of the component.

119 - Read of HTTP request failed due to overly long header

Description: The HTTP daemon has a header that is suspiciously long.

119 - Read of HTTP request failed due to too many header lines

Description: The HTTP daemon has a header with numerous lines.

119 - Read of HTTP response failed due to overly long header

Description: The HTTP response failed because of a long header. The connection is dropped.

119 - Read of realaudio request failed

Description: While reading from the RealAudio server, an error was encountered. The connection may remain alive, but may fail. Reestablish the connection.

119 - Realaudio read request timed out

Description: The proxy does not get a response when it talks to the RealAudio server. The connection remains alive, but may fail. Reestablish the connection.

120 - A service controller is already running on this machine

Description: This message indicates that a service controller is already running on the machine.

120 - Access denied

Description: The system does not permit access because there is no rule specified.

120 - Added IP address to blacklist, timeout set

Description: IDS detects an intruder entering the security gateway and blacklists the IP address for a set time period.

120 - Anonymous bind to LDAP server using null password is not allowed

Description: An anonymous bind to the LDAP server using a null password is not allowed.

120 - Asked host about name and received response

Description: The received response to a host/address lookup did not match the query. The parameter provides information on the query, the request, and the response. If the server that it is querying is under your control, you should check the DNS configuration for the host. If it is an external query, monitor the logs for any suspicious activity originating from this host. This is an attempt to obscure the source.

120 - Bind with DN and supplied password failed

Description: The bind action has failed. The cause of this failure is available in the log message.

120 - Cannot determine ESP type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Cannot determine tunnel type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Cannot find entrust configuration file, will use default configuration

Description: The default configuration file is used, as the authentication configuration file is not found.

120 - Cannot find security policy for user or its primary group or its extended authentication usergroup list

Description: The user attempts to connect and failed. This may occur because of a misconfiguration, or if the user is unauthorized to make the connection.

120 - Cannot process configuration mode without a valid ISAKMP security association

Description: The Symantec Client VPN failed to establish the connection because a valid ISAKMP security association (SA) does not exist.

120 - Cannot recognize keyword

Description: The configuration file is corrupted.

120 - Cannot resolve name to an IP address

Description: This message is from the SDI. The SDI library is unable to resolve the name of the RSA SecurID server.

120 - Cannot use entrust for extended authentication

Description: The Entrust authentication method is not an extended user authentication method, it is used to authenticate Symantec Client VPNs. There are other extended user authentication methods available.

120 - Checking user protocol

Description: This is a check to test if the user can use Out of Band Authentication (OOBA) for a given protocol.

120 - Configuration file has not changed, skipping

Description: The configuration file has not changed.

120 - Configuration file not present

Description: The process searches for a configuration file that is not available. The name of the file is indicated in the parameters.

120 - Consolidated connection statistics

Description: If the dnsd.log_connection_info is set to 1, DNS connection statistics are logged periodically. This includes the number of bytes sent/received per source or destination IP.

120 - Detected adapter IP address change, rebinding to new sockets

Description: The software has to be reconfigured because of a change in the adapter.

120 - Disconnected Symantec Client VPN

Description: The Symantec Client VPN has been disconnected from the server.

120 - Dropping request from host because it arrived on an unknown interface. Reloading interfaces

Description: The DNS query is dropped as it has arrived from an unknown destination. The interface table is reloaded to ensure that it is current version available.

120 - Error adding attribute tunnel mode to list

Description: This message indicates a software failure.

120 - Error adding attributes to transform list

Description: This message indicates a software failure.

120 - Error adding proposal to request list for protocol AH

Description: This message indicates a software failure.

120 - Error adding proposal to request list for protocol ESP

Description: This message indicates a software failure.

120 - Error adding proposal to request list for protocol IPComp

Description: This message indicates a software failure.

120 - Error during creation of neg proposal list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Error during creation of peer list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Error during IPSec security association negotiation with peer

Description: There is an error in the Phase II negotiation. This is not a software error, but may be a configuration or an operational error. The log message displays the error code, which is used by the administrator to identify and correct the problem.

120 - Error during ISAKMP security association negotiation with peer

Description: There is an error in the Phase I negotiation. This is not a software error but is a configuration or an operational error. The log message displays the error code, which is used by the administrator to identify and correct the problem.

120 - Error while initiating protocol negotiation

Description: This message indicates an error in the negotiation process. This is usually due to a a configuration error.

120 - Error while processing data received from peer

Description: There exists a problem in the interpretation of the negotiation message from the peer. This is a configuration problem.

120 - Established IPsec security association

Description: The Phase II negotiation, which determines the protocol security association for the tunnel, is established.

120 - Established ISAKMP security association

Description: The Phase 1 negotiation for your IKE tunnel is established. In Phase 1, the IKE application creates an IKE security association with its peer to protect the Phase II negotiation.

120 - Failed downloading tunnels with peer

Description: This is a VPN client tunnel negotiation failure. The VPN client failed to get proper configuration from the server side. Check the configuration.

120 - Failed extended user authentication with peer

Description: Extended authentications occurs between Phase I and Phase II IKE negotiations. For extended user authentication, you enter the required user name and password. In this case, either the user name or the password is invalid.

120 - Failed to add tunnel

Description: This message indicates a software failure.

120 - Failed to add tunnel mode attribute to the attributes list

Description: This message indicates a software failure.

120 - Failed to allocate active ISAKMP security association

Description: A shortage of memory is the cause of this failure.

120 - Failed to allocate dynamic ISAKMP security association

Description: A shortage of memory is the cause of this failure.

120 - Failed to allocate dynamic protocol security association

Description: A shortage of memory is the cause of this failure.

120 - Failed to allocate dynamic VPN policy

Description: In this case, this process fails because of a shortage of memory.

120 - Failed to allocate list for downloading filters

Description: This message indicates a memory failure problem.

120 - Failed to allocate list for downloading tunnels

Description: This message indicates a memory failure problem.

120 - Failed to allocate lists

Description: This message indicates a memory failure problem.

120 - Failed to allocate NAT mapping from pool, entries in use

Description: The security gateway software failed to allocate an address from the NAT pool. All the addresses in the NAT pool are exhausted. To avoid such a situation, set up a larger NAT pool.

120 - Failed to connect to service

Description: The component attempts to connect to a service, and it fails to connect.

120 - Failed to create notify message

Description: This is an operational error, which is identified using the error code.

120 - Failed to establish IPSec security association with peer

Description: The Phase II negotiation has failed. This failure is caused because of a mismatch between the security gateway configuration on both sides. Check the global IKE policy for configuration problems.

120 - Failed to establish ISAKMP security association with peer

Description: The Phase II negotiation has failed. This is caused because of a configuration error but could also be caused by a software error.

120 - Failed to extract authentication method

Description: When you connect to the Symantec security gateway, you provide the IP address and the authentication method for your security gateway. In this case, the authentication method could not be extracted.

120 - Failed to extract hash algorithm

Description: Unable to extract the encrypted data, which is in hash algorithm format.

120 - Failed to extract libauth mechanism

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Failed to extract number of peer proposals

Description: The proposal in the negotiation is incorrect, so it cannot be extracted.

120 - Failed to find suitable source address

Description: A component fails to find a suitable source address for the given domain.

120 - Failed to get a handle to authentication subsystem for authentication mechanism

Description: This is a configuration error. The server requires certain users to authenticate but these users are unable to do so, because they do not have access to the authentication server.

120 - Failed to get user response to prompt

Description: The user authorization process for a tunnel failed because of no user response.

120 - Failed to get VPN message handle

Description: This message indicates a shortage of memory.

120 - Failed to handle request from host because fail-safe timeout period expired

Description: A DNS query from the host, for an address or name, failed. The DNS server that the query was forwarded to, failed to answer within the set time frame.

120 - Failed to handle request from host. No progress possible

Description: A DNS query from host, for an address or name, failed, probably because the DNS server that the query was forwarded to, failed to answer. This might occur if the server is down, overloaded, or network connectivity to the server has been lost.

120 - Failed to handle request from host. Possible lame delegation

Description: A name server (NS) record is misconfigured. As a result, the DNS proxy was unable to resolve a name or an address. If the name server is within your control, check your DNS configuration on that server.

120 - Failed to handle request from host. Probable lame delegation as we have forwarded same request to that address

Description: A name server (NS) record is misconfigured. As a result, the DNS proxy was unable to resolve a name or an address. If the name server is within your control, check your DNS configuration on that server.

120 - Failed to load network parameters to user

Description: The VPN server can force a client to have a certain network configuration setting. In this case, the client is unable to load the network configuration setting enforced by the VPN server, resulting in a client configuration error.

120 - Failed to malloc libauth buffer

Description: This message indicates a shortage in memory.

120 - Failed to malloc while saving group list for user

Description: This message indicates a shortage in memory.

120 - Failed to open dispatcher for NAT keep-alive message

Description: If this message appears every few hours it does not indicate a problem. However, if this message appears in greater frequency (every 10 minutes or sooner), it indicates a possible internal problem. Customers with a current support agreement may contact Technical Support by phone or online at http://www.symantec.com/techsupp/.

120 - Failed to open file

Description: The daemon was unable to open the file specified in the log message. In the HTTP daemon, this may indicate a problem accessing a local Web server or problems decompressing the ratings file.

120 - Failed to parse line in file

Description: The configuration file is erroneous. This is not a common occurrence.

120 - Failed to send NAT keep-alive message

Description: If this message appears every few hours it does not indicate a problem. However, if this message appears in greater frequency (every 10 minutes or sooner), it indicates a possible internal problem. Customers with a current support agreement may contact Technical Support by phone or online at http://www.symantec.com/techsupp/.

120 - Found invalid configuration attribute of basic type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Found matching information

Description: The component has found the information for which it was searching and this information is listed in the parameters.

120 - Incomplete query

Description: Received an incorrectly formatted DNS query. It has been dropped. The sender of the query needs to send a valid query.

120 - Installed new file

Description: The HTTP daemon has successfully installed the latest httpratings.db file.

120 - Interface list contains only loopback address. Please check your TCP/IP configuration

Description: Unable to find an IP address that is operative. A misconfiguration has occurred.

120 - Invalid configuration mode identifier, expected

Description: A failure occurs during client tunnel negotiation. This does not happen frequently, but if it does, try to reconnect.

120 - Invalid identifier

Description: The security gateway Phase I ID, also called the remote Phase I ID, is the identifier that lets Phase I negotiations proceed. In this case, the security gateway Phase I ID is invalid.

120 - Invalid number of transforms

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Invalid operation

Description: This message indicates a problem in one of the software components.

120 - Invalid peer certificate (does not contain peer ID)

Description: To configure the Symantec Client VPN to use a certificate, you must have a profile, password and the security gateway Phase1ID. In this case, the peer Phase 1 ID is invalid. Contact your system administrator to ensure connectivity using certificate authorization.

120 - Invalid Phase 2 (QuickMode) ID type, it must be ID_IPV4_ADDR or ID_IPV4_ADDR_SUBNET

Description: The peer tries to negotiate a tunnel for an ID type that is not supported, so the connection fails. The tunnel is only supported for a host, subnet or for a range of addresses.

120 - Invalid SPI

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Invalid tunnel index

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Invalid type in configuration mode payload

Description: The Symantec Client VPN has failed to establish the negotiation.

120 - ISAKMP peer recovery completed, thread exiting

Description: The ISAKMP peer recovery has been completed.

120 - ISAKMP security association with peer expired, will renegotiate

Description: The Phase I negotiation has expired. The Symantec Client VPN needs to reestablish the connections. This is a normal operational procedure and does not indicate a problem.

120 - Joining cluster

Description: This message is part of the normal startup procedure during a cluster operation.

120 - Listening on port

Description: This message indicates that the proxies are fully functional. The port is identified from the resource parameter.

120 - Loading ISAKMP configuration files

Description: To ensure the safe transmission of data between the VPN client and the security gateway, Symantec Client VPN uses the standardized Internet Security Association and Key Management Protocol (ISAKMP). In this case, the ISAKMP configuration files are getting loaded.

120 - Loading static IPSec tunnels

Description: VPN tunnels support static configurations, where tunnel parameters have to be manually created at each security gateway. In this case, the system is loading static IPsec tunnels and the configuration information has to be entered manually.

120 - Looking for ticket

Description: The HTTP daemon is searching for a ticket, while processing tickets for Out of Band Authentication (OOBA).

120 - Looking up

Description: If the interface.debug is set to one, all DNS lookups are logged.

120 - Matching information not found

Description: The component searches for information and is unable to find a match.

120 - Maximum frame size to TCP/IP reduced

Description: Pending removal. Used for testing.

120 - Method handler returned error - access denied by rule

Description: Access is denied, security gateway administrator must review the rules.

120 - Method handler returned error - cannot connect to destination

Description: Communication error, the client needs to retry.

120 - Method handler returned error - proxy authentication required

Description: The user needs to authenticate before passing this type of traffic.

120 - Must send startup command first

Description: This message is part of the normal startup procedure.

120 - NAT enforcement fails, retrying

Description: NAT is unable to perform an address translation.

120 - No adapter changes found

Description: Symantec Client VPN did not find any adapter changes, while checking for one.

120 - No attributes were returned for entry

Description: The LDAP authentication is unable to verify a user name because no attributes were returned for the entry.

120 - No response to query

Description: This message appears when a DNS query from the host for an address or name, or a query to gwcontrol for connection information does not produce a response.

120 - No valid file descriptor

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Node garbage collector deleted <variable 1> rrs and <variable 2> nodes, <variable 3> nodes remaining

Description: If dnsd.report_cleanup is set to 1, the DNS proxy reports when it cleans up old cached information.

120 - Non-matching or unsupported Diffie-Hellman group

Description: Diffie-Hellman is the standard IKE method for establishing shared keys. Group 1 and Group 2 are the Diffie-Hellman group numbers for establishing these IKE session keys. In this case, the group entered is invalid.

120 - Not able to determine the authentication type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Not aggressive mode, cannot extract Phase 1 ID

Description: There is an error in the Phase I negotiation.

120 - Not enough memory to perform distinguished name conversion

Description: This is caused by an incorrect or corrupted configuration file.

120 - Not sending ICMP unreachable in response to non-informational ICMP (<variable 1>) received on interface <variable 2>

Description: An ICMP message was received indicating an error condition. The security gateway did not respond to this error.

120 - Not waiting for Symantec Client VPN

Description: This message appears when you start the Symantec Client VPN.

120 - Notified, removing stale tunnels to/from security gateway

Description: Received notification to remove the old tunnels to and from the security gateway, and therefore, removing these tunnels.

120 - Notify payload from peer incorrectly formatted

Description: The notify message from peer is incorrectly formatted.

120 - NS garbage collector deleted <variable 1> NS entries, <variable 2> entries remaining

Description: If dnsd.report_cleanup is set to 1, the DNS proxy reports when it cleans up old cached information.

120 - Packet received

Description: The option “log all receive packets” was enabled, for either test or diagnostic purposes, so every packet that is not blacklisted is logged. The performance is adversely affected.

120 - Packet transmitted

Description: The option “log all transmit packets” was enabled, for either test or diagnostic purposes, so every packet not blacklisted is logged. The performance is adversely affected.

120 - Performing ISAKMP peer recovery on tunnel

Description: This is a normal feature. When you restart the security gateway, this message appears, indicating that all the old tunnels are retrieved.

120 - Process was automatically restarted

Description: The bullfrog daemon (HA/LB) received a command to restart itself.

120 - Processor

Description: The “count” indicates the number of physical processors on the system. If Hyper Threading is turned on, the “count” indicates the number of logical processors.

120 - Protocol disabled for user from host

Description: Various proxies have been set up for Out of Band Authentication (OOBA). This message provides the status of the OOBA session.

120 - Protocol enabled for user from host

Description: Various proxies have been set up for Out of Band Authentication (OOBA). This message provides the status of the OOBA session.

120 - Query

Description: A query to made to gwcontrol, requesting connection information, authentication information, or configuration information.

120 - Query read error

Description: A query to gwcontrol, for information, has failed.

120 - Query response too long

Description: A gwcontrol query, receives a response that is long.

120 - Queue full, dropping new packet

Description: The new packets are dropped as a large number of packets arrive. This is a software protection feature.

120 - Ratings file is up to date

Description: The HTTP daemon ratings file has been updated with the most current version.

120 - Reached maximum capacity, cannot open session with peer

Description: You can only have a particular number of IKE negotiations, at a given time, because of resource limitation. This message indicates that this limit has been reached.

120 - Read select failed on ISAKMP sockets

Description: This message appears when you connect to a remote machine that is not alive, or does not have the requested service running.

120 - Read select file descriptor was not selected

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Read select timed out on file descriptor

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Received control message

Description: Received a control header line in the news article.

120 - Received disconnect message from security gateway

Description: The Symantec Client VPN has received a message to disconnect from the server.

120 - Received empty response, not accepted

Description: The user authentication process failed because the user name or password field is empty. Enter a valid user name or password.

120 - Received notification from peer that ISAKMP security association was negotiated

Description: The ISAKMP software on peer informs that the Phase 1 negotiation is complete.

120 - Received notification from peer that PROTOCOL security association was negotiated

Description: The local software on peer informs that the Phase 1 negotiation is complete.

120 - Received Phase 1 ID differs from configured one

Description: During tunnel negotiation, the Phase 1 ID from the peer differs from the Phase 1 ID entered during configuration.

120 - Received quick mode while performing extended authentication, drop it and continue with extended authentication

Description: The VPN server receives a quick mode while performing an extended authentication, so it drops the quick mode and continues to perform an extended authentication.

120 - Received unknown command

Description: This indicates a software error.

120 - Reconfiguring ISAKMP tunnels

Description: Loading new configuration for the IKE tunnels.

120 - Reconfiguring static IPSec tunnels

Description: The configuration information for the static IPsec tunnels has changed, so the configuration must be loaded again.

120 - Refusing request from host because the host is not authoritative and not recursing for this request

Description: The security gateway rejects the request to look up a domain name for security reasons.

120 - Reloading tunnels

Description: The tunnels are reloading.

120 - Removed blacklist entry for IP address due to user request/timeout. Packets discarded

Description: The blacklist entry for the IP address is removed, either in response to a request from an administrator or if it exceeds the set time period.

120 - Repeated:

Description: Messages that have occurred multiple times have been consolidated, indicating a possibility of an occurrence of a more serious problem.

120 - Request headers are too long, will not comfort

Description: The proxy changed the headers (usually to remove hop to hop headers), so no comforting is required.

120 - Restarting

Description: Restarting a process on the security gateway.

120 - rlimit_nofile now current

Description: The rlimit_nofile is the updated value specified.

120 - Rule IDs sorted by priority

Description: This notice states that the security gateway rules are sorted by priority.

120 - Search for group information failed. Looked under <variable 1> for <variable 2>

Description: Unable to find group information. The reason for this failure is available in the log message.

120 - Search for user record failed. Looking under <variable 1> for <variable 2>

Description: Unable to find the LDAP user record. The reason for this failure is available in the log message.

120 - Security gateway is not IKE enabled and will not be loaded

Description: This problem arises because of a misconfiguration.

120 - Service exited

Description: (Microsoft Windows only) The service has exited and terminated.

120 - Shared key is not defined for user

Description: This is a configuration error. An attempt to connect to the tunnel has failed as the shared key is not configured on the security gateway.

120 - Some adapter IP address has changed, will reconfigure VPN services

Description: The IP address of the remote user who connects to a private network using the Symantec Client VPN has changed. The VPN service is reconfigured when there is a change in the IP address.

120 - Spawning new process

Description: A process is starting a new instance.

120 - Stale rule cache host-to-address mapping detected. Reloading rule cache

Description: If the variable gwcontrol.rule_cache_reload_timer is set, periodic reloading of the cache ensures that a host entity which is defined with a fully-qualified domain name in a rule, but whose address is assigned by DHCP, is still found in the rule. Without rule cache reloading, the old address persists in the cache, even after DHCP has assigned a new address.

120 - Starting

Description: Individual proxy sessions are starting.

120 - Successfully logged into the ISAKMP engine with a customized profile with certificate support

Description: The Symantec Client VPN has successfully logged into the ISAKMP engine. The administrator has created the Entrust certificate profile for the user, enabling the VPN Client to use the digital certificate method for authentication.

120 - Successfully logged into the ISAKMP engine with a default profile which has no certificate support

Description: This is a standard operational feature. The Symantec Client VPN has successfully logged into the ISAKMP engine with a default profile, and operates without using the Digital Certificate method of authentication.

120 - Switched to lite mode, cannot access CA directory

Description: This is a standard operational feature. The Symantec Client VPN is switched to lite mode, so it operates without using the Digital Certificate method of authentication.

120 - Symantec Client VPN does not respond to Phase 1 requests

Description: The Symantec Client VPN does not respond to Phase 1 negotiation.

120 - Symantec Client VPN has exited

Description: This message notifies that the Symantec Client VPN has exited.

120 - Symantec Client VPN has started

Description: This message notifies that the Symantec Client VPN has started.

120 - Symantec Client VPN internal version 1

Description: This message is part of the normal Symantec Client VPN startup procedure.

120 - Symantec Client VPN must send a STARTUP command first

Description: The Symantec Client VPN needs to send a STARTUP command first.

120 - Symantec Enterprise Firewall management processes started

Description: The security gateway proxies have started successfully.

120 - Template ID does not fit in one longword

Description: If this message appears, it is caused because of a configuration error or an incorrect file related to the static tunnel.

120 - Terminating

Description: Individual proxies are terminating normally (for example, as a result of operator action).

120 - The encrypted password did not match the supplied user password

Description: The LDAP authentication has failed.

120 - The license does not specify VPN

Description: An attempt is being made to use a VPN client, without a valid licence, on the security gateway. The user needs to obtain a license for the VPN client.

120 - The Scan Engine has been manually shut down

Description: The antivirus scan server engine has been shut down gracefully.

120 - There are more tunnels for user, we download only

Description: Each user is allowed to create not more than 500 tunnels. If you exceed this number, then this message appears.

120 - Third-party intrusion detection system from host/port has authenticated and is issuing a request to blacklist a host

Description: The intrusion detection system from a host or port has found an invalid host, therefore, issues a request to blacklist the host.

120 - Timed out, failed to send data

Description: If this message is sent from the Notify daemon, it indicates that the daemon was unable to get a response from the modem.

120 - To enforce Phase 1 ID to be included in peer certificate, set configuration variable 'isakmpd.enforce_id_in_cert=0'

Description: To use the digital certificate authorization, you must configure the Symantec Client VPN to use the certificate. To perform the configuration, you must have a profile, password, and the security gateway Phase1 ID. In this case, the message provides details on how the Phase 1 ID is included in the peer certificate.

120 - Unable to connect to port. Attempting retry

Description: If the communication issue persists for a long period, it indicates a problem.

120 - Unable to create UDP socket for isakmpd

Description: This is a case of software failure. The software is unable to create a UDP socket for the ISAKMP daemon.

120 - Unable to fit ID of bytes length

Description: This is a configuration problem. The Phase I ID exceeds the set length limit.

120 - Unable to send data to peer

Description: Sending data to peer has failed. Check system resources, such as, memory and network connectivity to peer.

120 - Unknown AH transform type for tunnel

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Unknown ESP transform type for tunnel

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Unknown ESP type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Unknown tunnel type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Unsupported AAAA query

Description: The DNS daemon does not currently support AAAA queries (IPV6). The security gateway dropped the query.

120 - Unsupported configuration attribute type

Description: The VPN server can force a client to have a certain network configuration setting. In this case, the software does not support one of the network configuration settings enforced by the VPN server, resulting in a configuration error.

120 - Unsupported VPN command

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

120 - Updated blacklist timeout for IP address, timeout set

Description: This warning informs the blacklisted host about the updated timeout. This occurs when the blacklisted host attempts to access the network before the completion of the timeout period.

120 - User failed to authenticate

Description: The VPN client user failed to authenticate.

120 - User name given during extended authentication is not a substring of Phase I ID

Description: The client Phase I ID should be a substring of your user name for extended authentication.

120 - User name given during extended authentication is not the same as Phase 1 ID

Description: The client Phase I ID should be the same as your user name for extended authentication.

120 - Waiting for other sessions to complete

Description: This message is part of the normal operation.

120 - Waiting two seconds for adapter changes

Description: This message is part of normal operation.

120 - Waiting until reload is complete

Description: If reconfiguration is in progress when you attempt to negotiate (generate a tunnel) then this message appears, requesting you to wait until the configuration is complete.

120 - Will retry to bind to sockets

Description: An attempt is made to bind to the UDP socket again.

121 - Connected to SESA agent

Description: The notify daemon has successfully connected to the SESA Agent, and will begin sending messages to the SESA Manager.

121 - Statistics

Description: This is a statistics log message. The parameters provide information about each connection.

122 - Daemon listening on port(s)

Description: The proxies are fully functional. The ports are identified in the resource parameter. Ensure that they are not used by any other service.

122 - Daemon listening on TCP port(s)

Description: The proxies are fully functional. The TCP ports are identified in the resources parameter. Ensure that they are not used by any other service.

122 - Daemon listening on UDP port(s)

Description: This is a startup message. The UDP proxy is fully functional and is identified in the resource parameter.

123 - Allocating mapping from pool

Description: This message identifies the range of IP addresses that were added to the NAT pool.

124 - Freeing mapping from pool

Description: This messages identifies the range of IP addresses that were freed from the NAT pool.

124 - Parameters and filters set for interfaces

Description: The parameters and the filters have been set for the interfaces.

131 - Remote management connection request

Description: The secure remote login (SRL) daemon has received a request for a remote connection. This call provides audit information.

143 - Sending file to antivirus scan server

Description: This message is from FTP, SMTP or HTTP proxy. The proxy that generated this message is sending a file to the antivirus scan server for processing.

144 - Files with no extension = <variable 1>, fixed extensions = <variable 2>, redirects skipped = <variable 3>, no ContentType = <variable 4>, found < HTML > = <variable 5>, scanned = <variable 6> (total files scanned = <variable 7>

Description: A file with no extensions is being sent to the antivirus scanner. The actual setting is substituted into this message.

144 - No Content-Type: <variable 1>, response: <variable 2>

Description: If httpd.log_missing_type is set to 1, this log message displays when a file with no extension or a content type is encountered.

151 - Configuration edit

Description: The settings and key parameters indicate the file or setting associated with the configuration edit action. The user parameter identifies the administrator, and the operation parameter indicates which action was performed.

151 - Exported configuration to SESA Manager

Description: The local configuration gateway was exported to the SESA Manager. This configuration (which is a policy or a location setting) can now be managed on the SESA Manager. The user parameter identifies the administrator who performed the export, and the revision parameter indicates the configuration.

151 - LiveUpdate successful

Description: A LiveUpdate process has successfully obtained the latest definitions or URL lists from the LiveUpdate site.

151 - Local override: SESA Manager configurations are now disabled

Description: All configurations achieved through SESA are overridden locally, and ignored, until they are rejoined to SESA.

151 - SESA Management enabled. SESA Manager configurations are now enabled.

Description: The security gateway has joined SESA and configurations are now managed on the SESA Manager. The user parameter identifies the administrator, who joined the security gateway to SESA.

151 - Use of configurations received from SESA Manager disabled

Description: The administrator, who is identified from the user parameter, configures the security gateway to use local management. The security gateway ignores any configurations received during this configuration process.

151 - Use of configurations received from SESA Manager enabled

Description: The administrator, who is identified from the user parameter, configures the security gateway to use Local Management. The security gateway will resume using configurations received from the SESA Manager.

152 - LiveUpdate found files up-to-date

Description: A LiveUpdate was requested but the requested items are found to be updated.

152 - Remote management operation performed

Description: An operation was requested through the remote GUI and has been performed on the security gateway. The operation parameter identifies the operation, and the user parameter identifies the administrator. The filename parameter optionally indicates the file that is involved with this operation.

153 - Received configuration from the SESA Manager

Description: The security gateway has received a configuration from the SESA Manager. The key parameter indicates the name of the policy or location settings that was received. The revision parameter indicates the revision of the policy or the location settings.

154 - Configuration pulled successfully from node IP address

Description: In a cluster environment, synchronization occurs between nodes, and the configuration data remains on the same nodes.

154 - No license found to execute LiveUpdate

Description: The antivirus scan engine was preparing to update its virus definitions but a valid license for this feature was not found.

154 - Node has a newer configuration, attempting to synchronize

Description: This message indicates that in a cluster environment, the security gateway is updating configurations from another node in the cluster.

155 - Configuration discarded

Description: Any configuration edits that have been made since the last activation have been deleted. The user parameter identifies the administrator, and the revision parameter identifies the revision.

155 - The Scan Engine has updated its virus definitions

Description: The Scan Engine has updated its virus definitions to reflect the current list.

164 - NDIS descriptor allocation scale factor set and number per direction is 512 times value

Description: The Microsoft Windows driver has set the scale factor according to the ScaleFactor registry value. The number of buffers statically allocated is two times 512 times the value in the ScaleFactor registry entry. An additional number equal to this result is dynamically allocated and freed.

For example, if the ScaleFactor value is 6, 3072 receive buffers and 3072 transmit buffers are pre-allocated. In addition, another 3072 receive buffers and 3072 transmit buffers are dynamically allocated as necessary. These numbers indicate the number of packets concurrently being processed within the driver.

164 - Received command to reload filter configuration

Description: A command is received to reload the filter configuration.

170 - Attempting to re-synchronize modem for retry count

Description: Notify daemon makes count attempts to synchronize the modem.

170 - Dialing phone number

Description: This is a pager notification, stating the progress of the connection to the modem.

170 - Hanging up the modem

Description: This is a pager notification, stating the progress of the pager transmission.

170 - Modem is now synchronized

Description: This is a pager notification, stating the progress of the pager transmission.

170 - Waiting for a specific string using a retry count or timeout

Description: Notify daemon is waiting for a particular modem response.

171 - Driver log messages at this level suppressed

Description: Logging of driver log messages is suppressed until the volume of messages decreases.

171 - SESA Agent installed

Description: The software that lets the security gateway communicate with the SESA Manager has been installed and configured.

171 - SESA Agent removed

Description: The software that lets the security gateway communicate with the SESA Manager is no longer required and is deleted.

171 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve, so that the log services do not load the CPU.

172 - Successfully activated security gateway configuration

Description: A new configuration has been activated on the security gateway. This is the result of a local administrator activating a set of configuration edits, or the security gateway receiving a configuration from the SESA Manager. The user parameter indicates the administrator (or SESA administrator if managed by SESA) and the revision parameter contains the policy and location settings revision information.

175 - Perform graceful shutdown of the system

Description: The security gateway system is shutting down normally.

190 - Remote management timed out

Description: The security gateway remote management session was logged out after it was left up and running with no interaction.

190 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.

Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

199 - Bad protocol passed

Description: The H.323 voice over IP protocol is bad, so it is passed.

Notice messages (200-299)

Log messages in the range 200-299 are notices that indicate a situation requiring minor attention.

201 - Access denied

Description: The system does not permit access as no rule that allows this connection exists. To pass this traffic, create an appropriate rule.

201 - Adjust time server <variable 1> offset <variable 2> second(s)

Description: The time is being adjusted by the number specified.

201 - Already authenticated

Description: The user attempts to authenticate.

201 - Command received while waiting for data connection

Description: While waiting to establish an FTP connection, an unexpected command was received by the FTP proxy.

201 - Connection closed before connected to last destination

Description: A connection was terminated before the connection process was complete.

201 - Data transfer timed out waiting to send data to client

Description: The FTP daemon does not receive a response from the client.

201 - Data transfer timed out waiting to send data to server

Description: Data comforting has been enabled for the virus scanning session but the session has timed out.

201 - Denied due to MIME type restrictions

Description: The HTTP daemon logs that this particular type of file is not allowed because the security gateway is configured to disallow this type of file.

201 - Duplicate sender specified

Description: This is the case of an unexpected SMTP protocol. A duplicate sender is specified.

201 - Found AUTH command inside transaction

Description: This is the case of an unexpected SMTP protocol. The message provides details on the type of error.

201 - Leap second occurred, slewed time back one second

Description: Leap second occurred, slewed time back one second.

201 - Leap second occurred, slewed time forward one second

Description: Leap second occurred, slewed time forward one second.

201 - Leap second occurred, stepped time back one second

Description: Leap second occurred, stepped time back one second.

201 - Leap second occurred, stepped time forward one second

Description: Leap second occurred, stepped time forward one second.

201 - Mail with no transaction

Description: This is the case of an unexpected SMTP protocol.

201 - Originator validation failure on command <variable 1>

Description: This is the case where a command like MAIL contains one or more illegal characters. The Loose sender check option should be enabled to avoid this failure.

201 - Received ATRN command without authentication

Description: This is the case of an unexpected SMTP protocol. Received an ATRN command without authentication.

201 - Received RCPT command without MAIL command

Description: This is the case of an unexpected SMTP protocol. An RCPT command is received without receiving any prior MAIL command.

201 - Recipient validation failure on command

Description: This is the case where a command like RCPT contains one or more illegal characters. The Loose sender check option should be enabled to avoid this failure.

201 - Repeated

Description: Messages that have occurred multiple times have been consolidated, indicating the possibility of an occurrence of a more serious problem.

201 - Resetting blacklist sequence number

Description: While communicating with the blacklist daemon, notify daemon finds a mismatch sequence number, so the specified IP is not blacklisted.

201 - Step time server <variable 1> offset <variable 2> second(s)

Description: This is an informational message informing how large the time slew is.

201 - Timed out waiting for data connection

Description: The FTP client or server did not send a timely response to the FTP proxy. The session is terminated.

201 - Unable to create, bind, or listen to local socket

Description: The FTP daemon received a TCP error, and has terminated the session. If the problem persists, check the TCP configuration settings.

201 - Unable to enter PASV mode

Description: The FTP daemon is configured only for the PASSIVE sessions. In this case, an active connection was attempted.

201 - Unable to forward command

Description: The FTP daemon was unable to forward a command to the remote server.

201 - Unable to get addressing information for data connection

Description: The FTP daemon was unable to acquire the correct destination address of an internal server.

201 - Unable to get reply from server

Description: The FTP daemon did not receive a reply from the remote server.

201 - Unable to open data connection

Description: The FTP daemon was unable to open the data channel required to complete the FTP session.

201 - Unexpected control connection termination

Description: The FTP server has unexpectedly terminated the session with the FTP proxy.

201 - Unexpected response on control connection

Description: While processing data on an FTP session, an unexpected response was received.

203 - Remote password changed in file

Description: Rempass was used to change the remote security gateway password.

204 - Password added

Description: This notification message indicates that a password has been added through rempass, which allows access to the security gateway for secure remote login (SRL), remote logging, SGMI, or IDS blacklisting.

211 - License limit exceeded

Description: The user has used the maximum number of connections available for the current license. Additional licences are required. You can access the Symantec licensing and registration site at www.symantec.com/certificate to obtain a license file.

212 - IP packet not allowed on tunnel

Description: The source and/or destination address of the encapsulated IP packet in a VPN packet is not allowed on the tunnel.

213 - IP packet not allowed in implicit tunnel

Description: The encapsulated IP packet in a VPN packet, received on an implicit tunnel, was not addressed to the host configuration daemon.

214 - IP packet addressed to X server dropped

Description: The security gateway dropped a connection attempt on the X server port.

215 - VPN packet not forwarded as it does not match any defined tunnel

Description: Security gateways only forward VPN packets addressed to other machines if they match a defined tunnel. Otherwise, the packet is dropped.

216 - Access denied (connection terminated on re-authorization, no valid rules)

Description: The user has established a connection through a proxy when the administrator was in the process of changing the authentication rules. The connection was terminated because the connection no longer meets the criteria for the rules.

216 - Access denied because dynamic users are not permitted for this connection

Description: A user lacking the allowable authentication rules is not allowed to connect to the security gateway.

216 - Access denied because the use of a remote proxy is not permitted

Description: The security gateway is configured to disallow the use of the remote proxy.

216 - Access denied because the use of the security gateway as a proxy is not permitted

Description: The security gateway is not configured to be a proxy for a client.

216 - Access denied for host. Failed name check for newsgroup - profile

Description: The user has failed the name check authorization, to connect to this particular newsgroup, so the access is denied.

216 - Access denied for host. Failed ratings check for newsgroup - profile

Description: The user has failed the ratings check authorization, to connect to this particular newsgroup, so the access is denied.

216 - Access denied, could not get IP address for ratings check

Description: A user requested a URL that is prohibited by the rating profile.

216 - Access denied, no user authentication possible

Description: A user could not be authenticated. This is caused when either the authentication information is not available or the user has failed the authentication.

216 - Access denied, URL matches the denied pattern on line

Description: Access is denied as the URL contains a pattern that is not allowed. The line number identifies the line in the pattern configuration.

216 - Approved URL file missing, access denied

Description: Ratings profiles are set up to deny access to classifications of Web sites. However, you may want to grant access to some sites that fall into a denied category. These sites are normally defined in a configuration file. This message indicates that no such configuration file exists to define the exception, so the security gateway is blocking the Web site based on the ratings profile.

216 - Attempt to fetch Java class, access denied

Description: The HTTP daemon Java classes are not allowed because of a rule.

216 - Attempted access to file extension type not allowed

Description: An attempt has been made to access a file with extensions types that are not allowed. The administrator needs to set up or modify the authentication rules to specify valid extension types.

216 - Exceeded timeout sending/receiving data

Description: H.323 is timing out a session as it has exceeded the time period while sending or receiving data.

216 - File GET not allowed, access denied

Description: A rule exists in the HTTP daemon that does not allow a GET command.

216 - File PUT not allowed, access denied

Description: A rule exists in the HTTP daemon that does not allow a PUT command.

216 - FTP method not allowed, access denied

Description: A different type of HTTP method (for example, GET or PUT) is not allowed.

216 - Ratings check failed, access denied

Description: The user provides a URL that fails the ratings profile check.

216 - Received unexpected client data

Description: This indicates an unexpected state in protocol.

216 - Request denied by gwcontrol

Description: There are no rules to allow the connection type requested. The administrator can modify the authentication rules to allow this particular type of request.

216 - Requested URL not in approved list

Description: Ratings profiles are set up to deny access to classifications of Web sites. However, you may want to grant access to some sites that fall into a denied category. These sites are normally defined in a configuration file. This message indicates that a configuration file exists, but the requested URL does not appear, so the security gateway is blocking the Web site based on the ratings profile.

216 - Server rejects SIZE command, file size cannot be determined

Description: The remote server does not support the SIZE command. The transfer continues to take place.

216 - Unable to connect

Description: RealAudio was unable to connect to a server. In the case of readhawk, the proxy was unable to connect to the process identified in the parameters.

216 - Unexpected client error on send

Description: HTTP was unable to perform a send action to a remote client, because of a remote client error.

216 - Unexpected closure of server socket

Description: The FTP or HTTP daemon received an unexpected close from the server.

216 - Unexpected server error on send

Description: HTTP was unable to perform a send action to a remote server because of a remote server error.

216 - Unknown scheme detected

Description: An unknown scheme was specified. Some valid schemes include http:, mailto:, and ftp:.

218 - Abnormal end of session

Description: This indicates the NNTP abnormal termination of the client.

218 - Article exceeds cache size

Description: The news article is too long to cache in memory.

218 - Bad authentication challenge received from server

Description: A bad authentication challenge is received from the server. The message is dropped.

218 - Bad authentication response received from server

Description: A bad authentication response is received from the server. The message is dropped.

218 - Illegal request/response received

Description: An unexpected protocol is used, or certain events are out of sequence, which signify an attack. The type of request is identified from the resource parameter. Check for other log messages related to this address.

218 - Invalid H.323 protocol. Bad version in RFC 1006 header

Description: The H.323 protocol is invalid. The message provides details on this error.

218 - Invalid H.323 protocol. Message decode failed

Description: The packet could not be decoded as a valid H.323. The log message provides information on this error.

218 - Invalid protocol (bad challenge from host)

Description: An attempt to access the security gateway readhawk process failed. Access denied.

218 - Invalid protocol (bad checksum from host)

Description: An attempt to access the security gateway readhawk process failed. Access denied.

218 - Invalid protocol (illegal message length from host)

Description: An attempt to access the security gateway readhawk process failed. Access denied.

218 - Invalid Q.931 protocol. Error in field

Description: The Q.931 protocol (Call signalling and control) is invalid. The log message provides details on this error.

218 - Invalid Q.931 protocol. Error parsing ASN

Description: The Q.931 protocol (Call signalling and control) is invalid. The log message provides details on this error.

218 - Invalid RealAudio protocol, requesting client UDP port not in range

Description: A client has attempted a RealAudio connection, over a UDP port, that is not available.

218 - Invalid real-time streaming protocol

Description: This is an invalid real-time streaming protocol.

218 - Invalid SMTP protocol

Description: The security gateway has drop the mail message because the SMTP protocol is invalid. The additional parameters in this message provide details on this error.

218 - Invalid SMTP protocol, response code is not numeric

Description: An invalid SMTP protocol is received. The response code is not numeric.

218 - Message header contains invalid characters

Description: The SMTP protocol is invalid because the message header contains invalid characters. The message is dropped.

218 - Message header contains too many 8-bit characters

Description: The SMTP protocol is invalid because the message header contains too many 8-bit characters. The message is dropped.

218 - Overly long line received

Description: The SMTP protocol is invalid because a very long line is received. The message is dropped.

218 - Overly long message header field

Description: The SMTP protocol is invalid because a very long message header is received. The message is dropped.

218 - Sending system is not 8-bit clean

Description: The SMTP protocol is invalid because the sending system is not 8-bit clean. The message is dropped. Enable the “pass non ascii” option to resolve this problem.

218 - Suspicious article received

Description: The NNTP domain received an article that did not conform to the protocol for articles.

The NNTP domain checks the header to determine if any of the header fields reference some denied newsgroups, and checks the cached article body to determine if it contains material that should be denied access.

218 - Too many short packets - possible use of Telnet by client

Description: The SMTP protocol is invalid because the client may have used Telnet. The message is dropped.

218 - Unknown response to command

Description: The NNTP protocol that is being used is not allowed.

218 - Unsupported protocol type

Description: An attempt is made to send a protocol command using an unsupported protocol type, which may signify an attack. The resource parameters provide more detail. Check for other log messages related to this particular IP address.

218 - Unsupported/inappropriate command

Description: A protocol command is sent that is either not supported or sent at an inappropriate time, which may signify an attack. The resource parameter provides information on the type of command. Check for other log messages related to this particular IP address.

218 - Validation failure on response

Description: There is a validation failure on the response. The response is either too long or contains invalid characters.

219 - Cannot parse URL

Description: The uniform resource locator (URL) string specified is illegal.

220 - Local Web server can not handle request, loop detected

Description: The security gateway's HTTP daemon, is itself, the target of an HTTP request, and is unable find the file specified in the URL.

222 - Connecting to port by means of the HTTP proxy is not allowed

Description: A connection through the HTTP daemon is not allowed.

225 - Possible spoofed IP packet dropped

Description: The IP packet is dropped because the packet has not arrived through the expected interface. If a request originates from an outside interface but has an internal address, it is considered spoofed and is dropped.

226 - IP packet dropped as this packet should have been received through a tunnel but was received as a plain IP packet

Description: An unencrypted packet was received. But, the tunnel database indicates that this packet should have been received encrypted, so the packet was dropped.

226 - IP packet dropped because it is an unsolicited ICMP packet

Description: An ICMP Echo Reply was received without requesting one. A large number of these signify an attack.

226 - IP packet dropped because it is an unusual or disallowed ICMP packet

Description: The ICMP message is not one of the allowed types, so it was discarded. Only a subset of the ICMP messages are permitted, for security reasons.

By default, the following messages are allowed up the stack: Destination Unreachable, Source Quench, Time Exceeded, and Parameter Problem.

Blocking Destination Unreachable (Type = 3) fragmentation needed (Code = 4) is not advisable as this would prevent Path MTU from working properly. Connectivity problems can result when large packets are silently dropped.

Echo Requests are only permitted, if enabled. An Echo Reply is only permitted if there is a corresponding Echo Request.

226 - IP packet dropped because it was source routed

Description: The kernel detects that the IP packet was source routed, so the packet is dropped.

226 - IP packet dropped because it was received as a broadcast or multicast packet

Description: Generally, if the multicast packet is directed to a unicast Ethernet address, it is dropped. TCP packets to broadcast addresses are not permitted.

226 - IP packet dropped because packet size < 20

Description: A TCP packet was rejected because the source port was zero or the IP header length is too small.

226 - IP packet dropped due to bad IP destination address

Description: The destination IP address of the packet failed one of the numerous checks, so the packet was dropped.

226 - IP packet dropped due to bad IP fragment offset

Description: During packet reassembly of fragmented packets, the IP fragment offset field was determined to be invalid, so the packet was dropped. A few of these are acceptable.

226 - IP packet dropped due to bad IP header

Description: Various IP protocol checks led to a packet being dropped. A few of these are acceptable.

226 - IP packet dropped due to bad IP option

Description: An IP option was determined to be invalid either during IP datagram processing or packet reassembly, so the packet was dropped.

226 - IP packet dropped due to bad source address

Description: The source IP address of the packet failed one of the numerous checks, so the packet was dropped.

226 - IP packet dropped due to ICMP redirect

Description: ICMP redirect messages are a security risk and are ignored.

226 - IP packet dropped, bad IP checksum

Description: The IP checksum for the packet did not match the IP header data, so the packet was dropped. A few of these are acceptable. A large number could indicate a hardware problem.

226 - IP packet dropped, restricted port

Description: The TCP Port 111 is always blocked when packets are received.

226 - Packet dropped because the IP header length is illegal

Description: The packet is dropped because it does not conform to the IP header length limit.

226 - Packet dropped because the IP packet length is illegal

Description: The packet is dropped because it does not conform to the IP packet length limit.

226 - Packet dropped because the IP version is not supported

Description: The security gateway received a packet with the version bit set to a number other than four. The security gateway has dropped the packet.

226 - Packet dropped because the packet is too large to be encapsulated for this tunnel

Description: The packet is dropped because the packet is too large to be encapsulated for this tunnel. This indicates a configuration error.

226 - Packet dropped because the packet size is illegal

Description: The packet is dropped because it does not conform to the packet size limit.

227 - VPN packet dropped because of an invalid SPI for tunnel

Description: The SPI value in the packet did not match the SPI value determined when the tunnel was created, so the packet is dropped. This is a security check.

227 - VPN packet dropped because authentication failed for tunnel

Description: When decrypting an incoming encrypted packet, the integrity check failed. Network hardware checksum errors or packet tampering are possible causes.

227 - VPN packet dropped because decapsulated packet does not match tunnel end points for tunnel

Description: When a packet was successfully decrypted, its source and/or destination IP address was not within the scope of the tunnel.

227 - VPN packet dropped because decapsulated packet length exceeds encapsulated size for tunnel

Description: This message is logged when a VPN packet is dropped by the security gateway, as the packet is not formed correctly.

227 - VPN packet dropped because decompressed packet is larger than the maximum allowed packet

Description: The decompression process failed for a packet, so the packet was dropped.

227 - VPN packet dropped because decompression failed for tunnel

Description: The decompression process failed for a packet, so the packet was dropped.

227 - VPN packet dropped because decryption failed. Invalid format or length for tunnel

Description: When decrypting an incoming encrypted packet, the integrity check failed. Network hardware checksum errors or packet tampering are possible causes.

227 - VPN packet dropped because expected header was missing

Description: The encrypted packets that are received have a series of headers and one of the headers was not of the type expected.

227 - VPN packet dropped because IP payload compression is not supported by this release

Description: Packets entering a tunnel undergo the encapsulation process, which includes applying a valid compression method. In this case, the IP payload compression method is not supported in the current release, so the VPN packet is dropped by the security gateway. This occurs because of a misconfiguration.

227 - VPN packet dropped because peer used incorrect compression algorithm. To accept any algorithm used by peer, set “vpnd.strict_decompression_check=False” in config.cf

Description: By default, a security gateway rejects a tunnel when the compression algorithm does not match the algorithm in the tunnel policy. You can override this behavior by setting vpnd.strict_decompression_check to False in the advanced options. A simpler method is to modify the tunnel policy to accept either one of the compression algorithm.

227 - VPN packet dropped because received IP compression packet on a tunnel that was not configured for compression

Description: This message is atypical and results from a configuration error.

227 - VPN packet dropped because the IP encapsulating protocol is not appropriate for tunnel

Description: This is sometimes a catch all error. For example, the hardware refused to decrypt a packet for an unknown reason.

227 - VPN packet dropped because the packet has incorrect encryption padding

Description: ESP packets are typically padded to a boundary. An IPsec convention defines the padding contents of an ESP packet. Normally, the padding is not checked. But, if the check is turned on, a packet is dropped when the padding does not match the constant pattern.

227 - VPN packet dropped because the packet is either too old or has been received before by tunnel (potential replay attack)

Description: Associated with each IPsec packet is an increasing sequence number.

An IPsec feature is protection against replay of the same packets. When the same encrypted packet is sent again for some reason, the packet is dropped. This is called replay attack protection.

This feature is implemented by maintaining a sliding window of packets received. The default Replay Window Size is 128. When the same packet is sent again or a packet is received outside of the window, the packet is dropped.

Getting these messages occasionally is normal, given the fluctuation of network transmission. These messages can appear more frequently when multiple data streams are traversing the same tunnel at the same time.

It is possible to increase the size of the window and it is possible to disable this security check altogether.

227 - VPN packet dropped because unknown compression algorithm

Description: This message is atypical and results from a configuration error.

228 - Cannot connect to port

Description: The proxy is unable to connect to a specific server on the given port. The resource parameter identifies the port.

228 - Cannot connect to port (local port already in use, retrying)

Description: A connection attempt failed because the requested port is already in use. The security gateway is trying again to create the connection.

229 - IP packet dropped (decapsulated)

Description: An incoming packet was dropped after decapsulation. An interface filter is associated with the tunnel and the packet did not pass the interface filter. This is because you have configured the interface filter to drop these packets.

230 - Not authorized

Description: An attempt is being made to access a security gateway service with a bad password.

232 - Sending ICMP unreachable

Description: For the packet received, we responded with an ICMP unreachable error message. For example, someone sent a packet to a closed UDP port. A very large number of these can indicate an attack or a port scan or a mis-configuration. This message is typical in low numbers.

These messages sent on the wire and recorded in the log file can often be suppressed. This is accomplished by checking “Suppress Reset and ICMP error message” in the UI options for the interface.

233 - Packet dropped by interface, input packet filter

Description: A packet did not pass the input interface filter based on your configuration instructions. If you did not intend this kind of action, refine your filter.

233 - Packet dropped by interface, output packet filter

Description: A packet did not pass the output interface filter based on your configuration instructions. If you did not intend this kind of action, refine your filter.

234 - Network error detected, aborting

Description: A network error causes the connection to terminate.

235 - NAT address allocation failed from pool

Description: The security gateway software failed to allocate an address from the NAT pool, for the particular entity.

238 - Already active sockets to different servers for this client connection; delaying connecting until existing request completes

Description: If httpd.warn_delay is set to 1, it indicates that the HTTP daemon has reached the maximum number of connections from a client to HTTP servers.

238 - An illegal character was found in the request (see RFC 2068, RFC 1738, and RFC 1808)

Description: The proxy discovered an illegal character in the HTTP request.

238 - Audio notifications not supported on this system

Description: The notify daemon is unable to create audio notification because the hardware does not support an audio device.

238 - Authentication session for user timed out

Description: This message from Out of Band Authentication (OOBA) gives the status of the session, indicating that the authentication session has timed out.

238 - Call failed

Description: Unable to get the security gateway interface list. The security gateway is seriously misconfigured.

238 - Characters not allowed in a hostname were found in the requested URL

Description: Illegal characters were found in the URL.

238 - Client disconnected unexpectedly

Description: A secure remote login (SRL) client has terminated unexpectedly.

238 - Connecting to port by means of the HTTP proxy is not allowed

Description: An attempt by the user to connect to a port through the HTTP server was disallowed.

238 - Could not determine the file requested. Ensure that your client software puts a '/' after the Web server's hostname

Description: The URL could not be parsed.

238 - Couldn't parse hostname even though ftp:// was specified in the URL

Description: The URL is illegal.

238 - Couldn't parse hostname even though gopher:// was specified in the URL

Description: The URL is illegal.

238 - Couldn't parse hostname even though http:// was specified in the URL

Description: The URL is illegal.

238 - Couldn't parse hostname even though the CONNECT method was specified

Description: The URL is illegal.

238 - Couldn't parse port number; it may have been negative or greater than 65535

Description: The port number in the URL is erroneous.

238 - Denied packet associated with mail slot

Description: NetBIOS has denied a packet arriving from a particular mail slot.

238 - Failed to forward the request to the security gateway's configured proxy. This may be due to a configuration error or DNS failure

Description: The HTTP daemon failed to forward the request. The daemon is misconfigured or is unable to locate a proxy.

238 - Failed to forward the request to the Web server. This may be due to a security gateway configuration error or DNS failure

Description: The HTTP daemon fails to forward the request to the Web server. The daemon is misconfigured or is unable to locate a proxy.

238 - Hardware encryption algorithm mismatch

Description: The tunnel is configured to use an encryption algorithm that is not supported by the hardware. For example, Triple DES is supported by the hardware but AES is not. Therefore, the encryption occurs in software.

238 - Invalid address family for peer

Description: A client has attempted a TCP connection with an invalid address, so the connection is dropped.

238 - Login session aborted

Description: This message from Out of Band Authentication (OOBA) gives the status of the session, indicating that the logon session has been aborted.

238 - Login session aborted user

Description: This message from Out of Band Authentication (OOBA) gives the status of the session, indicating that the logon session has aborted the user.

238 - No inside interfaces specified or dnsd has not been configured. To suppress this message, disable dnsd

Description: No inside interfaces exist on the security gateway. The DNS daemon responds to queries only from the internal interfaces.

238 - Possible spoof attempt

Description: While verifying a host name/address, the process concluded that the name or address it found did not match what was requested. This may indicate a possible attempt by a non-trusted host to impersonate a trusted user or host.

238 - Proxies are already running

Description: The security gateway has restarted but the proxies were already found to be running. The duplicate set of proxies are terminated.

238 - Proxies are not running

Description: A request has been received to stop the proxies, but they are actually not running.

238 - Security gateway startup complete, proxy daemons terminated

Description: The security gateway is shut down, so no further traffic is passed.

238 - Specified request method not implemented

Description: The client has requested an URL that is not supported. Valid methods include put, copywebdav and ssl_connect.

238 - Supplied port number is invalid. Gopher connections are only allowed on port 70 and ports > 1024

Description: The HTTP proxy received a gopher request on an invalid port from a host on the protected network with the security gateway set as that hosts Web proxy. The HTTP proxy will only process gopher requests on port 70, or on a port over 1024.

238 - The address is a member of a dynamic NAT pool, but is currently unassigned

Description: An inside client attempts a connection from an internal address but did not use the DHCP to get the address.

238 - The CONNECT method cannot be used to access the requested port on the server due to the current security gateway configuration

Description: A misconfigured port prevents an HTTP connection from being completed.

238 - The interface name cannot be found

Description: There exists an illegal interface name in the rules configuration.

238 - The specified scheme cannot be used through this proxy

Description: The HTTP daemon received a request from an unsupported scheme. Valid schemes include http:, telnet:, ftp:, and others.

238 - Truncating long input from user IP

Description: This Out of Band Authentication (OOBA) message gives the status of the session, indicating that the long input from the user IP has been truncated.

238 - Unable to get more disk space to continue logging

Description: The security gateway has been shut down because there is no more available disk space for logging (you can change this behavior). You may need to release some disk space to continue logging (for example, by removing existing logs or changing the configuration for the log service to decrease the minimum disk space).

238 - Unknown packet source on channel

Description: A packet was received (H.323 protocol) but did not contain source information. Monitor subsequent log messages or traffic, on this protocol.

238 - User proxy by means of an outside interface is not allowed. Use httpd.allow_external_proxy to change it

Description: Someone outside the security gateway (external gateway) attempts to use the security gateway's HTTP daemon to obtain HTTP services. Setting httpd.allow_external_proxy lets an external proxy change the usage of HTTP services.

239 - Sending TCP reset not allowed

Description: If a TCP packet is received on a port, which is not permitted, then the connection is reset. This message is logged and includes the port number and the packet information. This message may indicate that someone is probing the security gateway.

A very large number of these can indicate an attack or a port scan or a misconfiguration. This message is typical in low numbers.

These messages sent on the wire and recorded in the log file are often suppressed. This is accomplished by checking “Suppress Reset and ICMP error message” in the UI options for the interface.

240 - TCP packet dropped due to bad TCP flags combination

Description: If a TCP packet does not have a legal protocol flag combination, it is dropped. However, poorly written protocol software may employ illegal flag combinations. In this case, you can bypass this security check by adding a parameter to the “Advanced Options” page under “System.” The parameter is driver.global.Flagcheck_Enabled and the default is True. Acceptable values include True and False.

241 - Skipping module

Description: The hotfix utility is not processing the specified module. This is because the definition in the hotfix control file indicates that this module should not be processed for the current platform.

242 - Bad SSL message received

Description: The HTTP daemon received a bad HTTP-SSL protocol.

266 - Packet dropped because of incomplete ICMP

Description: An ICMP packet does not have the minimum required length.

266 - Packet dropped because packet size is illegal

Description: While examining a variety of packet types (TCP, UDP or ICMP) the length of the packet was found to be less than the header length of the TCP, UD,P or ICMP packet.

271 - Driver log messages at this level suppressed

Description: Due to increased volume, the driver log messages are no longer being logged until conditions improve.

271 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve, so that log services do not overload the CPU. This lets you allocate CPU cycles to user services, and disable the logging of incoming connections.

290 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.
Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

Warning messages (300-399)

Warning messages fall into the range 300-399. These message usually indicate an error condition that the security gateway can recover from, but require attention to prevent further occurrences.

300 - Cannot connect to client

Description: The FTP server has terminated the connection with the FTP proxy, but the proxy is unable to notify the client.

300 - Cannot open socket

Description: The FTP server has terminated the connection with the FTP proxy.

301 - A NAT device exists between local and remote gateways, so cannot use transport mode

Description: Transport mode calculates its checksum against a pseudo header that includes both the source and destination address. Because the NAT device changes the source or destination address, and there is no inner IP header that keeps track of the original source and destination addresses, the checksum fails. Therefore, you cannot use transport mode with an intermediate NAT device.

301 - A NAT device is detected between local and remote gateways, so cannot use IPsec AH protocol

Description: Because AH uses the IP addresses in the packet header to calculate the checksum for encrypted packets, you cannot use the AH protocol with NAT. NAT changes the source address, destination address, or both, which causes the comparison AH checksum to fail.

301 - Accept failed

Description: Gwcontrol logs this message if the accept call fails when attempting to accept a connect request from one of the security gateway services or proxies.

301 - Address not in the real address range

Description: The NAT component found an illegal address when trying to change the modified address back to its original address.

301 - AH was selected, so hash algorithm cannot be NONE

Description: The Authentication Header (AH) provides authentication to the IP datagram by comparing the Integrity Check Value (ICV) on the content that is transmitted and received. Therefore, it does not encrypt or hide the data.

301 - Arguments too large

Description: An incoming message at the Out of Band Authentication (OOBA) daemon is too large to be processed.

301 - ASN packet too large (maximum 64K)

Description: The Q931 packet is too large. This is a non-transparent connection, in which the setup protocol data unit (PDU) must be encoded. Connection cannot proceed.

301 - Bad address passed

Description: The address given to the Out of Band Authentication (OOBA) daemon is not a valid address.

301 - Bad authorization command

Description: A request to authorize a connection was made, but the request is unreadable.

301 - Bad epass-find command

Description: A request to validate a user was made, but the request is unreadable.

301 - Bad process ID in authorization

Description: The process ID used for authorization is invalid.

301 - Bad process ID in query

Description: The process ID used for a gwcontrol authorization query is invalid.

301 - Bad process ID in verify

Description: The process ID used to verify a connection is invalid.

301 - Bad query command

Description: A query to gwcontrol was made, but the query is invalid.

301 - Bad response to a request for group information. Expected 'S'

Description: The user failed to authenticate.

301 - Bad verify command

Description: An invalid verify request was made to gwcontrol.

301 - Broadcast forwarding was on and is now off

Description: (Microsoft Windows only) This message provides information on the status of the network check conducted.

301 - Cannot add alias because alias limit has been reached

Description: You may have to check the H.323 configuration for errors.

301 - Cannot add vulture service

Description: The vulture service watches for tasks that should not be running on the security gateway. In this case the vulture service is unable to start.

301 - Cannot complete process scan

Description: The vulture daemon is unable to complete the process scan.

301 - Cannot complete the operation of creating an IPsec security association record since assigned tunnel ID is 0

Description: The tunnel configuration is corrupt.

301 - Cannot execute user script

Description: The component was unable to run a user script. The log message identifies the component. Execute the script from the command-line to check its validity.

301 - Cannot find an interface of local IP

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Cannot find connection in authorization

Description: Connection information for the authorization request is invalid.

301 - Cannot find interface specified as internal

Description: A problem may have started in the DNS configuration files, possibly generating other log messages, indicating the advent a more serious problem. Restart the DNS proxy and if the problem persists, check the configuration files for problems.

301 - Cannot get driver statistics

Description: (Microsoft Windows only) This message provides information on the status of the network check conducted. The system is unable to provide driver level statistics. The information is missing or an irregularity exists.

301 - Cannot load VPN policy since both AH and ESP headers were selected

Description: The configuration file is corrupted. To correct the problem, reconfigure and save the information.

301 - Cannot nest workgroups within workgroups

Description: The message indicates that nesting workgroups within workgroups is not allowed. This may occur because of a bad configuration.

301 - Cannot parse cluster configuration file

Description: The cluster.cf file is corrupted. You must rebuild the cluster.

301 - Cannot send SMTP trap

Description: The notify daemon is unable to send SMTP mail notification.

301 - Cannot set number of open files

Description: Unable to increase the number of sockets used for communication with gwcontrol.

301 - Cannot start process scan

Description: The vulture daemon is unable to scan for illegal sub-processes.

301 - Cannot understand required keyword

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then save and reconfigure.

301 - Cannot understand required keyword, so group member will not be added to group

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Cannot understand required keyword, so group will not be loaded

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Cannot understand required keyword, so host will not be loaded

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Cannot understand required keyword, so IKE policy will not be loaded

Description: The configuration file is corrupted. Try reentering the information and then activating the changes.

301 - Cannot understand required keyword, so security policy (tunnel) will not be loaded

Description: The configuration file is corrupted. Try reentering the information and then activating the changes.

301 - Cannot understand required keyword, so subnet will not be loaded

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Cannot understand required keyword, so VPN policy will not be loaded

Description: The configuration file is corrupted. Try reentering the information and then activating the changes.

301 - Cannot understand required keyword, so workgroup member will not be added to workgroup

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Channel in half closed (inconsistent) state when freed

Description: An error occurred while disabling the UDP port. The connection is closed and connection information is cleared.

301 - Child exited with status

Description: The forked process has terminated with an error status. The parameters indicate the type of error.

301 - Chmod failed

Description: Fetcher was unable to set file permissions on the http.rating file.

301 - Configuration error at line

Description: There exists a configuration error, at the line, indicated in the error message. Check the particular line.

301 - Connection will be denied because there were some rules, but no best rule found

Description: The connection is denied because no valid rule was found. The administrator should check and determine if the rules that are set up for the connection are valid.

301 - Copy could not read from file (maybe locked by another process)

Description: While trying to access the http.rating file, the daemon encountered read access problems. The new ratings file is not used.

301 - Copy failed because no memory for hash table

Description: The HTTP daemon was attempting to copy the new ratings file and encountered errors. The new ratings file is used.

301 - Corrupt file found, so will rebuild

Description: The Ratings file used by HTTP, SMTP, and FTP are corrupt.

301 - Could not access TCP/IP parameters

Description: (Microsoft Windows only) This message provides information on the status of the network check.

301 - Could not listen on port(s)

Description: A port conflict was detected between the HTTP daemon and another service running on the security gateway. Valid ports are in the resource parameter.

301 - Could not send to client

Description: A communication error was encountered while the HTTP daemon was communicating with the client.

301 - Could not set destination to proxy specified in rule

Description: The HTTP server is unable to communicate with the proxy.

301 - Could not set IP routing

Description: (Microsoft Windows only) This message provides information on the status of the network check.

301 - Could not stop bcast forwarding

Description: (Microsoft Windows only) This message provides information on the status of the network check.

301 - Could not stop source routing

Description: (Microsoft Windows only) This message provides information on the status of the network check.

301 - Creating thread as none are idle and queue still has stuff on it. Going to threads for connections

Description: A service is reporting on the status of its thread. It is either creating or destroying threads based on the system load. The administrator should monitor the load.

301 - Defender user started out as one name, but authenticated as another

Description: The first user name is the name the user started with and the second is the one the user used for authentication.

301 - Disabling shared memory support

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Download is allowed only for Symantec Client VPN, so dropping message

Description: When you are establishing connection to a Symantec security gateway, you need to provide the IP address and the authentication method. When your connection is established, the VPN policy and tunnel information for the connection can automatically be downloaded only by the Symantec Client VPN.

301 - Duplicate external server

Description: This message indicates a problem in the DNS configuration files.

301 - Eliminating csvr entry

Description: This is a debug message. When a process ceases to exist, the connection entry is removed from the connection table.

301 - Errors loading file

Description: Unable to load the file.

301 - ESP NULL must have an authentication algorithm defined

Description: Encapsulating security payload (ESP) is the most commonly used data integrity method, which provides data integrity and data source authentication. Therefore, it should have an authentication algorithm defined.

301 - Excessive replays from Netprowler

Description: Requests to blacklist a specific IP address from a remote intrusion detection device are being received at an excessive rate. This could indicate a configuration error on the remote device.

301 - Excessive replays from NetProwler, so ignoring NetProwler for specified minutes

Description: Requests to blacklist a specific IP address from a remote intrusion detection device are being received at an excessive rate so the security gateway will ignore the remote device for the defined time period. This could indicate a configuration error on the remote device.

301 - Execl failed

Description: Attempts to run a process have failed. The administrator needs to check the parameters to identify the problem.

301 - Exhausted tunnel IDs

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Extended authentication can only be initiated by the security gateway, so dropping message

Description: The extended authentication method of authenticating is initiated only from the server. In this case, the client tries to initiate this process and fails.

301 - Failed

Description: The parameters provide information on what has failed.

301 - Failed for reason

Description: The Out of Band Authentication (OOBA) daemon could not get the necessary information to authenticate a user. The user is not allowed through the security gateway.

301 - Failed to add attribute ESP algorithm to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute HMAC algorithm to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute IPsec security association lifetime to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute ISAKMP security association life type to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute ISAKMP security association lifetime to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute Oakley authentication method to the attributes list for proposal 1

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute Oakley encryption algorithm DES to attributes list for proposal 1

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute Oakley group description to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute Oakley hash algorithm to the attributes list for proposal 1

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute PFS to the IPsec transform

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute security association key length to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute security association life type to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add attribute tunnel type to the IPsec transform

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add Diffie-Hellman group or PFS attribute to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add IP compression algorithm attribute to the attributes list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add item to radix_tree

Description: The most likely reason is that the system has insufficient memory.

301 - Failed to add keys for tunnel

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add the attributes list to the Oakley transform list for proposal 1

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to add tunnel

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to allocate buffer for copying shared key

Description: This indicates an out of memory situation.

301 - Failed to allocate lists

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory

Description: Unable to allocate memory.

301 - Failed to allocate memory for AH transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_3DES transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_3DES_MD5 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_3DES_SHA1 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_AES transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_AES_MD5 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_AES_SHA1 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_DES transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_DES_MD5 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for ESP_DES_SHA1 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for SHA1 transform

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory for the VPN tunnel structure

Description: This message indicates an out of memory situation.

301 - Failed to allocate memory to create a new active IPsec security association record

Description: This message indicates an out of memory situation.

301 - Failed to copy shared key to buffer

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to create attribute list for ISAKMP security association

Description: This message indicates an out of memory situation.

301 - Failed to create Oakley transform list for ISAKMP security association

Description: This message indicates an out of memory situation.

301 - Failed to create the request proposal list during the ISAKMP proposal

Description: This message indicates an out of memory situation.

301 - Failed to disable input for UDP port

Description: An error occurs while disabling the UDP port. Connection is closed and the connection information is cleared.

301 - Failed to empty the attributes list for the Oakley transform list for the ISAKMP security association proposal

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to empty the attributes list while building the IPsec security association proposal

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to find an interface for VIP on node

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to get local address

Description: A function has failed to find the local IP and port of a given socket.

301 - Failed to get lock

Description: When attempting to purge a queue, the driver was unable to lock the queue, so the purge action for the queue failed.

301 - Failed to get memory size

Description: Failed to allocate the memory required.

301 - Failed to get requesting interface request from user

Description: The Out of Band Authentication (OOBA) daemon is unable to get the information required to authenticate a user. The user is not allowed through the security gateway.

301 - Failed to locate entity name because it is an invalid type

Description: This message indicates a bad configuration file.

301 - Failed to map to Symantec ESP transform ID

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to open file

Description: Unable to open the file identified by the parameters. If called by the save configuration utility, it indicates that the configuration has not been saved. The error number identifies the problem with the file.

301 - Failed to remove keys for tunnel

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Failed to resolve to IP address

Description: The user has configured the security gateway using a DNS name for an IP address but this information could not be resolved.

301 - Failed to send rekey response

Description: There exists a communication problem between the VPN components.

301 - Failed to send reload response

Description: There exists a communication problem between the VPN components.

301 - Failed to shutdown socket

Description: Unable to disable the send or receive action on the socket. The exact text of the error is available in the log message.

301 - Failed to update tunnel

Description: Customers with a current support agreement may contact the Technical support group by phone or online at www.symantec.com/techsupp/.

301 - Failed to write the pre-shared key to file for remote security gateway

Description: This indicates an out of memory situation.

301 - Failure to allocate memory to create a peer security gateway node

Description: This indicates an out of memory situation.

301 - File required for backup is empty

Description: The file which is required to perform a backup of the configuration, exists, but does not have any information.

301 - File_uncompress failed to unlink .gz file

Description: Fetcher has successfully updated the ratings profile, but was unable to cleanup an interim file.

301 - Fork failed

Description: One of the security gateway's software services tried to fork but failed. The system has probably run out of swap space or processes. Reboot the system.

If this message is sent by the notify daemon, it may indicate a problem trying to start a client notification. Ensure that the program is executable, has valid permissions, and resides in the right directory.

301 - Further messages that packets from IP address were blocked will be suppressed

Description: The kernel will discontinue to send messages, which warn that it has been blocking packets from a particular IP address.

301 - Getrlimit (RLIMIT_NOFILE) failed

Description: A call to getrlimit from the system failed. If the user has specified a value for h323d.rlimit_nofile in config.cf, it may not be used.

301 - Got ISAKMP configuration reply with zero-length attribute

Description: A bad packet was received during negotiation. The packet needs to be dropped.

301 - Group cannot have other groups or workgroups as members

Description: User groups consist of individual users, and user groups are created based on access levels. Therefore, a group cannot have other groups or workgroup as members.

301 - Group expected members, so the partial group will be loaded

Description: This is a warning and does not indicate a problem. The User Interface ensures that this type of situation does not arise.

301 - Group has no members, so the group will not be loaded

Description: This is a warning and does not indicate a problem. The User Interface ensures that this type of a situation does not arise.

301 - H.245 request for unsupported data transfer type

Description: The open channel request was not for an audio, video or T.120 logical channel.

301 - H.245 unsupported multiplex option (expected fLCPs_mPs_h2250LCPs)

Description: The multiplex option is not supported for audio and video channels.

301 - H.245 unsupported option (OpenLogicalChannel forwardLogicalChannelParameters)

Description: The forwardLogicalChannelParameters option is not supported for audio and video channels.

301 - H.245 unsupported option (OpenLogicalChannel reverseLogicalChannelParameters)

Description: The reverseLogicalChannelParameters is not supported for audio and video channels.

301 - H.245 unsupported option (OpenLogicalChannel separateStack)

Description: The SeparateStack option is not supported for audio and video channels.

301 - H.323 ossEncode failed

Description: Encoding a H.245 MultimediaSystemControlMessage prior to writing it out has failed.

301 - Host not found for callee alias name

Description: The host mapped to the alias name could not be found.

301 - I/O error sending to client

Description: An error was encountered while sending data to the client. The connection may remain intact, but reestablishing the connection is advised.

301 - Ignoring ICMP type

Description: An incorrect ICMP message was received from VPND. This message is incorrect and is ignored.

301 - International version cannot load AES

Description: This indicates an upgrade problem. The domestic version of the security gateway supports the Advanced Encryption Standard (AES) algorithm for stronger security and improved performance over Triple DES and DES implementation. The international version does not support this encryption algorithm.

301 - International version cannot load Triple-DES

Description: This indicates an upgrade problem. The domestic version of the security gateway supports the Advanced Encryption Standard (AES) algorithm for stronger security and improved performance over Triple DES and DES implementation. The international version does not support this encryption algorithm.

301 - Invalid AH transform ID

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Invalid authentication and encryption algorithm options

Description: The authentication and the encryption options available are not supported.

301 - Invalid authentication method for security gateway

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate.

301 - Invalid entity type for member of group

Description: The entity type is invalid and is not allowed to be a member of a group. The configuration file is not generated correctly or is corrupted.

301 - Invalid entity type for member of workgroup

Description: The entity type is invalid and is not allowed to be a member of a workgroup. The configuration file is not generated correctly or is corrupted.

301 - Invalid H.323 protocol (PDU failed)

Description: This is a non-transparent connection, in which the setup protocol data unit (PDU) has to be encoded. The encoding has failed. Connection cannot proceed.

301 - Invalid H.323 Protocol. Q931 Connect/Setup Encode ASN failed

Description: Unable to encode the Q931 pdu. This is a non-transparent connection, in which the setup protocol data unit (PDU) has to be encoded. The connection cannot proceed.

301 - Invalid IP address

Description: The IP address or DNS name entered is invalid. Type a valid IP address or DNS name.

301 - Invalid IP address for remote security gateway

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate.

301 - Invalid IP address or mask for host

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Invalid IP address or mask for subnet

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Invalid IP compression transform ID

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Invalid number of transforms

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Invalid opcode received

Description: The user failed to authenticate.

301 - Invalid Phase 1 ID

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

301 - Invalid Phase 1 ID type for security gateway

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Invalid port number

Description: The port number provided to this service is not valid (non-numeric).

301 - IP routing changed

Description: (Microsoft Windows only) This message provides information on the status of the network check conducted.

301 - Line too long for MAX

Description: The lines in the Out of Band Authentication (OOBA) HTML pages are too long for the internal buffers.

301 - Local security gateway is not IKE enabled

Description: This message indicates that the tunnel is not IKE enabled. This check is usually done by the User Interface.

301 - Malformed ISAKMP configuration attributes

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - MTU reduction ignored

Description: At attempt to reduce the frame MTU to a value less than 68 was rejected. This is a configuration error.

301 - Need to authenticate

Description: The client needs to authenticate before trying to connect.

301 - Net write failed

Description: The secure remote login (SRL) daemon is awaiting the authorization challenge from the client when it received a communication error. The session is terminated.

301 - No route found to host

Description: Unable to establish connection to a remote host. You have to establish a route or check the route for the connection to function properly.

301 - No security gateway specified for workgroup member. The entity will be dropped from the group

Description: This message is a warning about a bad configuration.

301 - No statistics block for username

Description: The statistics block for this user (the name is in the resource field) cannot be found and the user is denied access.

301 - Not authorized because connection from non-reserved port

Description: This message appears when someone attempts to direct connect on a port that is not open.

301 - Out of space. Data truncated and transmission aborted

Description: The HTTP daemon has run out of memory to continue processing this request. If this condition persists, you may need to restart the security gateway.

301 - Packet from IP address was blocked

Description: The kernel has blocked a bad packet.

301 - Phase 2 ID type of ID_IPV4_ADDR_RANGE is not supported

Description: Tunnels between a host and subnet are supported, but not between a host and a range of addresses. Subnet entities are normally created to define a range of IP addresses that are permitted by a rule.

301 - Range supplied in config.cf for UDP ports is too small

Description: Check the H.323 configuration for errors. The range is less than 10. Change the values of h323d.udp_low and h323d.udp_high to valid values. The daemon exits.

301 - Remote security gateway is not IKE enabled

Description: The tunnel is not IKE enabled. This check is done by the User Interface.

301 - Repeated:

Description: Messages that have occurred multiple times have been consolidated, indicating a possibility of an occurrence of a more serious problem.

301 - Requested (RLIMIT_NOFILE) value not in valid range

Description: The rlimit_nofile value specified in config.cf is not within the range allowed by the system, and so is not used.

301 - Second pass found no valid rules

Description: Gwcontrol attempts to authorize a connection and performs two passes through the rules. Both these passes fail and the connection is not allowed.

301 - Security gateway is not IKE enabled, so security policy (tunnel) will not be loaded

Description: The configuration file is corrupted. To correct this problem, reconfigure and save the information.

301 - Security gateway is not local, so security policy (tunnel) will not be loaded

Description: The configuration file is corrupted. To correct this problem, reconfigure and save the information.

301 - Security gateway is not remote, so security policy (tunnel) will not be loaded

Description: The configuration file is corrupted. To correct this problem, reconfigure and save the information.

301 - Security gateway specified for user or user group entity. The security gateway field does not apply to these entity types

Description: This message is a warning about a bad configuration. This does not affect any operation.

301 - Security gateway will not be loaded

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate.

301 - Security policy (tunnel) template was partially loaded

Description: The configuration file is corrupted. To correct the problem, reconfigure and save the information.

301 - Security policy (tunnel) template will not be loaded as it did not generate any valid policy instances

Description: The configuration file is corrupted. To correct the problem, reconfigure and save the information.

301 - Security policy uses transport mode VPN policy. Local entity and security gateway must have the same IP address

Description: This indicates a misconfiguration.

301 - Security policy uses transport mode VPN policy. Remote entity and security gateway must have the same IP address

Description: This indicates a misconfiguration.

301 - Send bullfrog command X failed with local error Y

Description: An attempt to send a command X to the bullfrog daemon failed, with a local error Y. This error is caused by timeout while waiting for a response from the bullfrog daemon.

301 - Send bullfrog command X failed with remote error Y

Description: An attempt to send a command X to the bullfrog daemon failed, with a remote error Y. Ignore the error if the command X is 13 (Get Node Status) and remote error Y is a non-zero value.

301 - Send of local file failed

Description: Unable to send file because of communication errors.

301 - Setrlimit (RLIMIT_NOFILE) failed

Description: Setting user specified RLIMIT_NOFILE has failed. The default value is used.

301 - Setsockopt fails

Description: A device has failed during the startup procedure. This does not happen usually, but if it does, you should identify and rectify the problem.

301 - Setting path MTU to 68

Description: The Path maximum transmission unit (MTU) for a tunnel was set to 68. This message should not appear.

301 - Shared key must be at least 20 characters

Description: This is a configuration error where the user interface (UI) is not generating the configuration file correctly. Someone may have edited the configuration files by hand or a configuration file is corrupted. You should make modifications in the UI, and then activate the new configuration.

301 - Source routing was on and is now off

Description: (Microsoft Windows only) This message provides information on the status of the network check conducted.

301 - Spawn failed

Description: Attempts to run a process have failed. The administrator needs to check the parameters to identify the problem.

301 - SRL is not enabled for this client

Description: You can restrict source addresses from which a user can establish a secure remote login (SRL) session. In this case, the user has attempted to connect from an address that has not been configured, so the connection was terminated.

301 - Syntax error at line

Description: This message is from the various services indicating errors in the configuration files. The parameters should indicate the source of the error.

301 - Time function failed

Description: A previous attempt to set the system time failed, and the offset has been recorded. Another attempt is made to adjust the time.

301 - Timed out waiting for response from oobauth daemon

Description: The Out of Band Authentication (OOBA) daemon did not respond to an authentication request in a timely manner. The user is not allowed through the security gateway.

301 - Too many authentication sessions to start a new one

Description: The Out of Band Authentication (OOBA) has reached its limit for the number of authentication sessions.

301 - Too many groups for user, so they have been ignored

Description: The user is found in multiple groups, so the fact that the user belongs to a group is ignored.

301 - Tried and failed to delete DNS node

Description: This is the case of an internal DNS problem cleaning up the cache.

301 - Tried and failed to delete NS entry

Description: This is the case of an internal DNS problem cleaning up the cache.

301 - Tunnel does not exist in vpnd local database

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Two labels exist for URL by service

Description: This message is from the ratings file.

301 - Unable to copy

Description: The host was unable to copy the resource. The resource parameter provides more information on what was to be copied. For the save configuration utility, this error indicates that the backup/restore did not complete.

301 - Unable to create all threads

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Unable to create socket

Description: This is an internal error. The NNTPD process failed to create a socket.

301 - Unable to create ticket

Description: The Out of Band Authentication (OOBA) daemon was unable to create an authenticate ticket for this user, so the user is denied access.

301 - Unable to destroy ticket

Description: The authentication ticket of a user was not destroyed, so the user is allowed through the security gateway, although the access should be denied.

301 - Unable to determine interface for destination address

Description: Unable to determine the connection destination because of a security gateway misconfiguration.

301 - Unable to determine interface for destination address due to message size mismatch

Description: Unable to determine the connection destination, which is because of a security gateway misconfiguration. The size of the packet that got sent was less than what we requested.

301 - Unable to find number of free bytes for file

Description: (Microsoft Windows only) Attempts by the logservice daemon, to release disk space for logging has failed.

301 - Unable to fork to make child

Description: The secure remote login (SRL) daemon is unable to create a child process to handle new connections and is restarted. The status parameter identifies the errno variable.

301 - Unable to get endpoints for security

Description: This indicates a corrupted configuration file.

301 - Unable to get security gateway(s) for instance of security policy <variable 1> between <variable 2> and <variable 3>

Description: This indicates a corrupted configuration file.

301 - Unable to initialize NAT trees

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Unable to load security policy

Description: A component is unable to load a security policy (gwcontrol). The security policy may have a problem that could become more serious. The administrator needs to recreate the security policy and resume the process.

301 - Unable to load security policy template

Description: The configuration file is corrupted. To correct the problem, reconfigure and save the information.

301 - Unable to make socket pair

Description: The notify daemon is unable to initialize a timeout for communicating with the modem due to a communications error.

301 - Unable to move file

Description: On a Microsoft Windows version of the security gateway, the restore of the hosts and hosts.pub file is done by moving the file. This has failed, so your DNS configuration is incomplete.

301 - Unable to open

Description: The server is unable to open a resource, which is identified in the resource (or filename) parameter.

301 - Unable to open file

Description: The process is unsuccessful when it tries to open a file. The parameters provide information on the file that it was trying to open.

301 - Unable to set port control for protocol, port and mode

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

301 - Unable to write lock file

Description: The notify daemon was unable to communicate with the modem. Attempting to communicate again.

301 - Unauthorized remote connection attempt from host

Description: Unauthorized attempts to connect to the security gateway management services have failed.

301 - Unknown entity type

Description: This message indicates that the configuration file is corrupted.

301 - Unknown file descriptor is set

Description: The notify daemon is unable to communicate with the modem. Pager notifications are not sent.

301 - Unlink failed

Description: Fetcher issues this log message because the interim file, which updates the ratings profile was not cleaned up.

301 - Unsupported notification

Description: Fax notifications are not supported in this release.

301 - User already has valid ticket

Description: The user has already authenticated, and the old ticket still exists on the security gateway.

301 - User has no valid ticket

Description: The user attempts to enable HTTP by way of Out of Band Authentication (OOBA), but has no valid authentication ticket for HTTP.

301 - User not logged off

Description: (Microsoft Windows only) This message provides information on the status of the network check conducted.

301 - Workgroup expected members, so the partial workgroup will be loaded

Description: This is a warning and does not indicate a problem. The User Interface ensures that this situation does not arise.

301 - Workgroup has no members, so the group will not be loaded

Description: This is a warning and does not indicate a problem. The User Interface ensures that this situation does not arise.

301 - Write failed

Description: The daemon could not write to the file named in the resource field.

302 - PORT command referenced a destination that does not match control channel

Description: The FTP proxy received a PORT command (part of the FTP protocol), that did not match what was required by the FTP server.

303 - Cannot read config file <variable 1>

Description: Unable to read the HA/LB configuration file. The cluster.cf file is being used or exclusively accessed by another process.

303 - Gwcontrol is already running

Description: At startup, Gwcontrol checks to see if an instance exists and is running. In this case, it has found one, so it logs this message and exits.

303 - Hotfix ID already in list

Description: The hotfix utility encountered a problem while reading a list from a file. The file contains an invalid duplicate entry. Check subsequent log messages to identify the erroneous file, before contacting support.

304 - Hotfix ID list is empty

Description: The hotfix utility encountered a problem while reading a list from a file. The file does not contain any valid entries. Check subsequent log messages to identify the erroneous file, before contacting support.

304 - Hotfix ID not in list

Description: The hotfix utility did not find the specified value in the list. No user action is necessary.

304 - License will expire

Description: This message notifies the user that the license of the product has expired. The parameters in the log message identify the product. Access the Symantec licensing and registration site at www.symantec.com/certificate to acquire a license file for the product.

304 - No active hotfixes were found

Description: The hotfix utility was instructed to uninstall all hotfixes but the active hotfix list is empty. The instruction is ignored. No user action is necessary.

304 - No recent hotfixes were found

Description: The hotfix utility was instructed to uninstall recent hotfixes but the recent hotfix list is empty. The instruction is ignored. No user action is necessary.

304 - Specified hotfix is already installed or superseded

Description: The hotfix utility was instructed to install a hotfix that has already been installed or has been superseded by a newer hotfix. The instruction is ignored. No user action is necessary.

304 - Specified hotfix is not installed and active

Description: The hotfix utility was instructed to uninstall a hotfix that has not been installed or has been superseded by a newer hotfix. The instruction is ignored. No user action is necessary. If this hotfix has been superseded by a newer hotfix and the user wants to uninstall it, all superseding hotfixes must be uninstalled first.

306 - Overlapping time range

Description: The time range for an authenticated connection overlap. Check the time range in the configuration.

308 - Cannot lookup host

Description: The host name cannot be looked up to find its IP address. The system tries to continue without it. Other daemons on the security gateway may also be unable to get external name resolution. Verify that the resolver on the security gateway is correctly configured.

On UNIX systems, the resolver is set in the /etc/resolv.conf file. On Microsoft Windows NT systems, the resolver is set in the DNS tab, of the TCP/IP protocols section, of the network control panel applet. For dual-level DNS configurations, the resolver should contain the IP address of the inside DNS server and nothing else. For configurations where DNSd on the security gateway is the sole DNS server for the local domain, the security gateway's resolver should contain the loopback address 127.0.0.1, and nothing else.

Verify that the DNS server on the security gateway is correctly configured.

If you are running security gateway's DNS proxy (DNSd) on the gateway, verify that the DNS forwarders section is either empty or contains the IP address of a DNS server on the Internet (usually the ISP's DNS server).

Verify that the Internet router is not filtering packets with a source port of 53. Filtering packets with source port 53 prevents DNS forwarding, and results in no outside name resolution.

309 - Cannot compile regular expression in configuration file

Description: The HTTP daemon encountered problems while parsing the configured URL patterns.

309 - In the configuration file, the network specification and the netmask do not correspond. The network address has been changed to match the netmask

Description: Gwcontrol, identifies that the network specification and the netmask do not correspond in the configuration file. The administrator needs to verify his configuration.

309 - Non-dotted quad address found. This should be changed to a dotted quad

Description: The IP address is found in non-dotted quad format. Specify the IP address in dotted quad format (for example, 198.162.1.3).

309 - Problem in configuration file

Description: The process encountered a problem while reading the configuration file but was able to continue reading. The line that caused the problem is ignored. Check if all the IP addresses are valid.

310 - Cannot verify reverse address as lookup does not include original address

Description: The service attempts to verify an address based on the name. In this case, the service did not receive an address, and therefore, was unable to verify it. The service decides on how to deal with the connection.

310 - Cannot verify reverse address, hostname not found

Description: The proxy attempts to verify if the address and name match. In this case, they do not, so the proxy decides on how to deal with the connection.

310 - Cannot verify reverse address, so mismatched reverse lookup

Description: While performing a lookup on a domain name, it was found that the domain name did not match the name that the user provided.

310 - User name or password too long; exceeds limit set by ftpd.maxlen_user_pass

Description: A client attempted to make an FTP connection with a user name or password that exceeds the set limit for the length.

311 - Cannot verify Ethernet address

Description: The security gateway software attempts to determine the hardware Ethernet address of the host, but received no response.

311 - Command incorrectly formatted

Description: The DNS resolver file is incorrectly formatted.

311 - Invalid keyword. Valid keywords are <variable 1> <variable 2> <variable 3>

Description: The DNS resolver file is incorrectly formatted.

313 - Host user gave bad authentication information

Description: An attempt by a host user to provide authentication data failed.

314 - Search order not specified or unrecognized keyword, so host resolution will fail

Description: The order of the commands in host.conf has a syntax error.

316 - Node ID mismatch - node with IP address has an incorrect node ID

Description: An error has occurred in the cluster, a member of another cluster is communicating to this cluster.

317 - Numeric username, so ignoring

Description: The security gateway encounters problems while parsing the rules. The log message provides more information on this problem.

317 - Unknown user, so ignoring

Description: The security gateway encounters problems while parsing the rules. The log message provides more information on this problem.

321 - Resuming downloads with antivirus comforting not allowed

Description: The protocol REST command cannot be used when comforting is enabled. The command is ignored.

321 - Unable to notify process of updated configuration

Description: The SGMI attempts to send a configuration to the security gateway but the process was unable to receive it. The process currently runs with an older configuration.

324 - No login prompt from paging service

Description: The notify daemon was unable to communicate with the paging service because the paging service did not send the prompt (“ID=”) within the set time frame.

324 - No login prompt from paging service

Description: The notify daemon was unable to communicate with the paging service because the paging service did not send the prompt (“ID=”) within the set time frame.

327 - Connection request rejected because the client does not have a unique IP address

Description: More than one host has the same IP address. The software was unable to compensate since two hosts with identical addresses are making identical requests at the same time. If the protocol is TCP, the connection attempt failed. If the protocol is UDP, the packet has been dropped. This has an impact on the connectivity.

If you are running the Symantec Client VPN, change the subnet you are using behind your NAT to one unlikely to be used by someone else, if possible. Network renumbering can sometimes be employed to eliminate non-unique collisions.

If you are not running Client VPN, this could be a network configuration problem.

327 - Connection request rejected because the server does not have a unique IP address

Description: More than one host has the same IP address. The software was unable to compensate since two hosts with identical addresses are making identical requests at the same time. If the protocol is TCP, the connection attempt failed. If the protocol is UDP, the packet has been dropped. This has an impact on the connectivity.

If you are running the Symantec Client VPN, change the subnet you are using behind your NAT to one unlikely to be used by someone else, if possible. Network renumbering can sometimes be employed to eliminate non-unique collisions.

331 - No rules in configuration file

Description: The security gateway read the gateway configuration file but did not find any authorization rules.

334 - Denied access to command

Description: A user was not allowed to execute a protocol command. The administrator can allow the execution of the command. If this is received from FTP, set ftpd.log_bad_commands to 0, to disable this message.

335 - VPN packet dropped because VPN is not enabled <variable 1>

Description: When the system is booted, VPN capabilities are disabled until the configuration program enables them after verifying the license file. VPN may also be manually disabled. Any VPN packets received while VPN is disabled is dropped.

Once your VPN capability has been enabled, no action is necessary.

Some security gateways have all VPN capabilities disabled. If these security gateways receive VPN packets, for some reason, this message continues to be triggered. Fix this at the source of the VPN packets by informing the administrator to fix the bad configuration.

341 - Child process killed

Description: The security gateway software runs independent processes in the background to free gwcontrol. This message indicates that the parent process in the <component> parameter has killed a child process.

341 - Remote management operation failed

Description: The SGMI was unable to complete a remote management request. The user parameter identifies the administrator and the operation parameter identifies the action that was attempted.

341 - The scan engine queue is backing up due to a large number of requests

Description: The antivirus scan engine is overloaded with requests to scan data.

343 - A new forked daemon has failed, so it will be restarted

Description: The process was unable to start, and is restarted. The administrator may have to provide the corrective action.

343 - A rule was found with a time range restriction, but no protocols. It will be ignored

Description: The security gateway encounters problems while parsing the rules. The log message provides more information on this problem.

343 - A rule was found with no protocols, so it will be ignored

Description: The security gateway encounters problems while parsing the rules. The log message provides more information on this problem.

343 - An invalid value was read for scan options, so setting to default: Scan, Repair or Delete

Description: This message indicates a configuration problem with the antivirus scanning but continues to function.

343 - Asked about resource for domain name and name server sent Type and Response

Description: The DNS proxy received a bad response from the remote host. The parameters contain the details of this response.

343 - Attempt to call aliased host but alias is not configured in alias name file

Description: A client attempted to connect directly to the security gateway but the server was not specified.

343 - Attempted connection from port which is >= 1024

Description: The remote command daemon received an illegal connection attempt.

343 - Attempted to load a tunnel with neither end local

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Authentication failure for user from host

Description: The user tried to authenticate while accessing the service, and the authentication failed. Invalid authentication information may have caused this problem.

343 - Bad entry in file

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Bad SMTP DATA response

Description: The notify daemon is unable to send mail notification because of an unexpected protocol.

343 - Bad SMTP End-Of-Message response

Description: The notify daemon is unable to send mail notification because of an unexpected protocol.

343 - Bad SMTP greeting response

Description: The notify daemon is unable to send mail notification because of an unexpected protocol.

343 - Bad SMTP HELO response

Description: The notify daemon is unable to send mail notification because of an unexpected protocol.

343 - Bad SMTP MAIL FROM response

Description: The notify daemon is unable to send mail notification because of an unexpected protocol.

343 - Cannot find an address for root server

Description: Unable to look up the root server, which occurs because the DNS is not configured properly.

343 - Cannot get SRL password entry because no password for 'srl' user

Description: The security gateway found the user in the secure remote login (SRL) password file, but there is no password configured. All SRL users must have a password added through the SGMI.

343 - Cannot get SRL password entry because no 'srl' user in passwd file

Description: An unauthorized user failed to access secure remote login (SRL), which is a secure Telnet with specific user configurations.

343 - Cannot get SRL password entry because password blank or not set for 'srl' user

Description: The user configurations exists in the secure remote login (SRL) password file, but the password is either blank or has not been set.

343 - Cannot get terminal attributes

Description: While attempting to send an audio alert, the notify daemon was unable to set up the workstation correctly. The audio alert is not sent.

343 - Cannot negotiate dynamic ISAKMP security associations, so using authentication SHARED_KEY with main mode (only with aggressive)

Description: This is normally caused because of a configuration error. Check the Gateway-to-Gateway tunnel configuration, and the configuration of the security gateway address and the phase ID.

343 - Cannot play audio because the audio device is busy or not configured

Description: (Microsoft Windows only) Unable to play audio because the audio device is busy or not configured.

343 - Cannot resolve DNS name

Description: The user has configured the security gateway using a DNS name for an IP address but this information could not be resolved.

343 - Cannot shutdown security gateway from GUI

Description: The security gateway was unable to shut down from the user interface because of an irregularity or connection problem.

343 - Cannot start security gateway from GUI

Description: The security gateway was unable to start from the user interface because of an irregularity or connection problem.

343 - Cannot stop security gateway from GUI

Description: The security gateway was unable to stop from the user interface because of an irregularity or system problem.

343 - Cannot synchronize with modem

Description: The notify daemon was unable to synchronize with the modem. Pager notifications are not sent.

343 - Cannot validate audio device

Description: Unable to locate the audio device configuration.

343 - Cleanup of unwritten filter.cf entries failed

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Cleanup of unwritten pkfilter entries failed

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Client transparency not performed for call. Missing required source IP and destination interface address

Description: A client tries to connect directly to the security gateway, so the connection is rejected. The client should use the remote servers address to connect (through the security gateway).

343 - Could not bind to LDAP server as user

Description: Unable to connect to the LDAP server with the given user name.

343 - Could not connect to X.500 directory, so switched to lite mode

Description: There was a problem connecting to the entrust engine. The reason is available in the message parameters.

343 - Could not force connection into VPN tunnel, so connection will be aborted. Missing required source IP and destination interface address

Description: Unable to force the connection into a VPN tunnel, so the security gateway aborted the connection. The required source IP and destination address is not available.

343 - Could not restart process

Description: An attempt to start or restart a service was unsuccessful.

343 - Could not start management daemon

Description: A management daemon was unable to start because of an irregularity or connection problem. The resource parameter identifies the management daemon.

343 - Could not start proxy

Description: A proxy was unable to start because of an irregularity or connection problem. The resource parameter identifies the proxy.

343 - Deleting old log file to free up some disk space

Description: The log service rolls over files when the files reach a certain configured size. In this case, there is no space to roll over the files, so the log service is configured to delete the oldest log file. This is a warning to notify the administrator to clean-up the system.

343 - Denied because source port out of range

Description: The user attempts to connect to the security gateway, on a port that is not open, and it fails.

343 - Detected forwarding loop to

Description: Forward looping is when you are forwarding records to another name server. In this case, the name server is forwarding it back to you, causing a loop.

343 - Detected lame delegation to ourselves

Description: Lame delegation is when a name server (NS) record points to an incorrect host. The NS record is misconfigured. If the NS is within your control, check your DNS configuration on that server.

343 - Disconnecting because of possible Telnet use

Description: A client attempts to use Telnet to send SMTP protocol, which is not allowed.

343 - 'dont_secure_answers' directive found in public hosts file

Description: While loading the hosts file the “dont_secure_answers” directive is found, although the file is public.

343 - Dropping new TCP connection for query as the system is temporarily overloaded with TCP connections

Description: On a Microsoft Windows security gateway, too many DNS queries were received simultaneously at the proxy.

343 - Dump of suspicious packet

Description: If the dnsd.dump_packet is set to 1 and the DNS proxy detects a suspicious packet is displayed. The parameters provide information about the query.

343 - Duplicate configuration variable found with value

Description: The same config.cf file variable is defined twice with different values.

343 - Duplicate URL in local ratings, ignoring

Description: A duplicate URL was identified in the ratings file, and is ignored.

343 - Encrypt configuration to file failed

Description: When you backup a configuration, the resulting file is encrypted. In this case, this process has failed and the interim configuration file is deleted.

343 - Entity is not a security gateway

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Entry is not an audio device

Description: The notify daemon is unable to send the audio notification because it is unable to access a valid audio device configuration.

343 - Error in response format

Description: The HTTP proxy received an illegal response.

343 - Error parsing extension list, so restoring default: Scan All Files

Description: This message indicates a problem with the antivirus scanning, but is able to continue.

343 - Error reading from antivirus scan server socket

Description: Unable to read from the antivirus scan server socket. Check the communication between the security gateway and the antivirus scan server.

343 - Error receiving from the antivirus scan server

Description: There is a communication problem between the HTTP daemon and the antivirus server. You may have to restart the server.

343 - Error sending data to the antivirus scan server

Description: Encountering problems while communicating with the antivirus server. You may have to restart the server.

343 - Error shutting down outbound antivirus scan server socket

Description: Encountering problems terminating sessions on the antivirus server. You may have to restart the server.

343 - Error while dialing or unable to connect to remote modem

Description: The notify daemon is unable to send a notification because the phone number used for the pager is invalid.

343 - Exceeded maximum retries logging into the paging system

Description: The notify daemon is unable to send paging notifications because the pager did not respond to several retry attempts.

343 - Exceeded maximum retries sending page

Description: The notify daemon is unable to send fax notification because it has exceeded the limit for retries.

343 - Failed to add dynamic filter for peer into local database

Description: This message indicates an out of memory situation.

343 - Failed to add dynamic ISAKMP security association for peer into local database

Description: This message indicates an out of memory situation.

343 - Failed to add dynamic protocol security association for peer into local database

Description: This message indicates an out of memory situation.

343 - Failed to add ISAKMP security association for security policy into local database

Description: This message indicates an out of memory situation.

343 - Failed to add proposal to the request proposal list

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to add protocol security association for security policy into local database

Description: This message indicates an out of memory situation.

343 - Failed to bind socket for UDP tunnel

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to build Phase 1 proposal

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to build Phase 2 proposal

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to connect to server. The server may be down

Description: Unable to connect to the TACACS library.

343 - Failed to copy buffer

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to create a UDP tunnel because there were no available slots

Description: The user may have to wait until the load eases.

343 - Failed to create linear list of user's security policies

Description: This message indicates an out of memory situation.

343 - Failed to create new ISAKMP security association

Description: This message indicates an out of memory situation.

343 - Failed to create new protocol security association

Description: This message indicates an out of memory situation.

343 - Failed to create shared key directory

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to decrypt saved configuration file

Description: When you restore a configuration, the resulting file is encrypted. In this case, the restore process has failed.

343 - Failed to get data

Description: The secure remote login (SRL) daemon was unable to get the data because of communication errors.

343 - Failed to initialize key context

Description: The security gateway is unable to encrypt data going to the remote logging utility. No data is sent.

343 - Failed to load the MAPI DLL

Description: The notify daemon is unable to send mail notification because it was unable to load Windows.dll.

343 - Failed to login into the ISAKMP engine

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to open control socket

Description: The proxy was unable to connect to the antivirus scan server. The antivirus scan server is either not operational or is not listening at the address and/or port that the proxy was configured to use.

343 - Failed to open directory

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to open file

Description: The service was unable to open the IDS XML files. Ensure that these are available in the appropriate directory:

/var/lib/sg/lang/xx (UNIX)

\usr\raptor\sg\lang\xx (Microsoft Windows)

343 - Failed to open rating file

Description: The ratings file could not be located.

343 - Failed to receive data

Description: Remote access was attempted, but during the challenge/response, there was a communication error.

343 - Failed to receive response from RADIUS server when trying to authenticate. The server may be down

Description: This indicates a communication problem with the RADIUS server. The server is down.

343 - Failed to reload

Description: Failed to reload the IKE tunnel configuration. One of the components is unavailable.

343 - Failed to remove file

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Failed to restart

Description: Unable to restart a proxy, management daemon, or security gateway service.

343 - Failed to restore configuration from file

Description: An attempt to restore the configuration file has failed. The resource parameter identifies name of the restore configuration file. The interim files are deleted.

343 - Failed to send data

Description: A remote access was attempted, but failed, because of a communication error.

343 - Failed to stop

Description: Unable to restart a proxy, management daemon, or security gateway service.

343 - Filter is not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - 'forward_to' directive found in public hosts file

Description: The “forward to” directive was found in the hosts file.

343 - Forwarding on, but server refuses to do recursion

Description: Forwarding the queries to another server continues but that server is not configured correctly.

343 - Found <variable 1> users with <variable 2> = <variable 3>, so denying access

Description: Authentication for this user failed because the user attribute key for this user, was set to the value indicated in the log message.

343 - Found extra directives at end of NAT configuration

Description: The nat.cf file is corrupted.

343 - French client cannot connect to non-french security gateways

Description: Remlog sends this message when a french client is unable to connect to non-french security gateways.

343 - Group contains the following unresolvable name(s)

Description: A non-existent rule to referred to by a group.

343 - Host <variable 1> tried to send mail from <variable 2>

Description: A mail is sent to host for which the user has no authorization, and is denied access.

343 - Host sent ARP request for address that is not distinguished by the current netmask

Description: This message, which is common is a result of a host configuration error. The mask of the host does not match the mask of the security gateway. All hosts on the same network should be configured with the same mask. If you cannot correct the hosts, you can suppress this message in the Advanced Options window. The option name is logserviced.suppress.arp_wrong_mask and the value is set to one. You can ignore this message unless the security gateway itself is configured with the wrong mask.

343 - Hostname was found in the rule database with both reverse_lookup and gwcontrol.perform_forward_lookups disabled. This will not work

Description: The host name is found in the rule database with the reverse_lookup and gwcontrol.perform_forward_lookups disabled.

343 - I/O error

Description: Unable to read or write data from a connected socket. The exact error is logged in the previous log entry.

343 - ICMP fragmentation needed checksum failure

Description: The checksum for an ICMP fragmentation needed message was invalid, so no action was taken.

343 - ID buffer has never been allocated

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Ignoring overly long packet received

Description: A long DNS query was received and is dropped. An abnormal query may indicate an attack.

343 - Ignoring packet because of too many additional records (> 64)

Description: The DNS daemon drops the query because it has received an unexpected packet. If the server continues to send illegal packets, the problem should be investigated.

343 - Ignoring packet because of too many answers (> 64)

Description: The DNS daemon drops the query because it has received an unexpected packet. If the server continues to send illegal packets, the problem should be investigated.

343 - Ignoring packet because of too many NS records (> 64)

Description: The DNS daemon drops the query because it has received an unexpected packet. If the server continues to send illegal packets, the problem should be investigated.

343 - Ignoring packet because of too many questions (> 1)

Description: The DNS daemon drops the query because it has received an unexpected packet. If the server continues to send illegal packets, the problem should be investigated.

343 - Ignoring packet because the packet is too short

Description: The DNS daemon drops the query because it has received an unexpected packet. If the server continues to send illegal packets, the problem should be investigated.

343 - IKE policy is not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Incompatible version of the security gateway

Description: The remote logging tool is unable to connect to this version of the security gateway.

343 - 'inside_interface' directive found in public hosts file

Description: The “inside_interface” directive was found in a public hosts file.

343 - 'inside_vip' directive found in public hosts file

Description: The “inside_vip” directive was found in a public hosts file.

343 - Integer variable has an unrecognized value

Description: In this case, a configuration (config.cf) variable does not have an integer value assigned.

343 - Invalid authentication method

Description: A proxy or service attempts to service an authentication request using a method that is not configured.

343 - Invalid force user field. Valid values are Y|N

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Invalid gateway password information

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Invalid gwgroup entry

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Invalid item found on line

Description: The nat.cf file is corrupt.

343 - Invalid Phase 1 ID

Description: This message indicates an out of memory situation.

343 - Invalid recipient syntax

Description: The notify daemon is unable to send mail notification because of an invalid email address.

343 - Invalid S/Key

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Invalid security policy. NULL entity pointers

Description: This message indicates a bad configuration file.

343 - Invalid shared key. Shared key must be at least 20 alpha-numeric characters

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Invalid SRL protocol received

Description: The security gateway received an invalid protocol during the secure remote login (SRL) negotiation. This connection was terminated.

343 - Invalid SSL client greeting

Description: The HTTP daemon received an invalid SSL request header.

343 - Invalid SSL server greeting

Description: The HTTP daemon received an invalid SSL request header.

343 - Invalid state. Dynamic ISAKMP security associations are allowed only with a Symantec VPN server

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Invalid Symantec Client VPN flag. Valid values are Y|N|U

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Invalid user name. User name can only contain '-', '_', and alpha-numeric characters (maximum 32 in length)

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Item is not a security gateway

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Item is not a user or user group

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Item is not a workgroup

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Item is not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Kernel encryption has been disabled due to excessive errors

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Kernel log queue overflow, dropping events

Description: Under extremely heavy load, kernel log messages are dropped. If this message appears repeatedly, you may need to investigate if this is a denial of service attack.

343 - Key negotiation failure probably due to incorrect password

Description: The secure remote login (SRL) client was unable to communicate with the security gateway's SRL daemon due to an incorrect password.

343 - Key negotiation failure, so failed to send header

Description: The secure remote login (SRL) client was unable to communicate with the security gateway's SRL daemon due to an incorrect password, mismatched version or an encrypted password file.

343 - Local entity is not a host or subnet

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Local entity is not a workgroup, entity group, subnet, or host

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Local entity not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Local security gateway not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Local user is configured to use authentication method certificate, not shared key

Description: Symantec Client VPN uses either the "shared secret" or the "certificate" method of authentication. This user is configured to use only the certificate method and not the shared secret method.

343 - Local user is configured to use authentication method shared key, not certificate

Description: Symantec Client VPN uses either the "shared secret" or the "certificate" method of authentication. This user is configured to use only the shared secret method and not the certificate method.

343 - Mail rejected due to malformed MIME headers

Description: SMTP rejects a bad mail message.

343 - Make sure that tunnel local and remote entities are defined identically on both peers

Description: This is a configuration error. The log message provides information on the error.

343 - Malloc failed while creating universal security policy

Description: This message indicates an out of memory situation.

343 - MAPI cannot logon using Microsoft Exchange profile

Description: The notify daemon is unable to send mail notification because of an invalid profile in the Microsoft Exchange API configuration.

343 - MAPI cannot resolve recipient name

Description: The notify daemon is unable to send mail notification because of an invalid email address.

343 - MAPI failed to free recipient buffer

Description: The notify daemon is unable to send mail notification because it was unable to free a buffer.

343 - MAPI failed to send mail

Description: The notify daemon is unable to send mail notification because of an unexpected protocol.

343 - MAPI logged off improperly

Description: The notify daemon is unable to send mail notification because the mail API failed to logoff correctly.

343 - MAPI logon failure. MS Exchange may not be installed

Description: The notify daemon is unable to send mail notification due to a mail API logon error.

343 - Message denied by paging service

Description: The notify daemon is unable to send paging notifications because of paging protocol problems.

343 - Method handler called for incorrect object type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Missing " in local ratings file near URL

Description: An invalid URL was encountered in the ratings file. This particular URL is ignored.

343 - Modem does not have class 2 fax support

Description: Unable to send pager notification because the modem does not support Class 2 hi-resolution fax.

343 - Multiple sequences in filter entry

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Name specified may not be a root nameserver

Description: While querying for root name servers, received a response from the address in the Resource parameter, which was not a root name server. The Reason parameter provides more information.

343 - NAT rule was chosen, but client transparency is not possible as both the source and destination interfaces are the same

Description: The security gateway has been misconfigured, both the source and the destination interfaces are the same. Therefore, NAT cannot be used.

343 - No authentication key provided for server

Description: Unable to communicate with the NTP or the radius server as no authentication information is available.

343 - No message prompt from paging service

Description: The notify daemon is unable to send paging notifications because the pager failed to conform to the pager protocol standard.

343 - No name found for address when reverse_lookup_required=TRUE

Description: The security gateway is configured to perform reverse lookups. In this case, the security gateway performs a lookup for a server address but did not find a name, so the connection is rejected.

343 - No Phase 1 proposal accepted

Description: This is a configuration error. Check the global_IKE_policy on both sides of the tunnel.

343 - No Phase 2 proposal accepted

Description: This is a configuration error. Check the configuration of the VPN policy used for the tunnel.

343 - No response received from ACE server

Description: The ACE server has failed to respond to a request for authenticating a user.

343 - No response received from ACE server

Description: The ACE server has failed to respond to a request for authenticating a user.

343 - No response received from RADIUS server when trying to authenticate

Description: This indicates a communication problem with the RADIUS server.

343 - No section for the current host was found in file. This probably indicates a problem with hostnames

Description: This message indicates that the configuration file (for example, gsp.cf, arp.cf, interfaces.cf, spoof.cf) has a missing host name or the host name does not match what is currently configured in the system. This could indicate a problem in changing the security gateway system host name (for example, manually instead of through the GUI) or the configuration file host name does not match the current system host name after restore.

343 - No setup key

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - No valid tunnels found for Symantec Client VPN

Description: No valid tunnels exist for the Symantec Client VPN.

343 - Non-transparent call but no destination given in callee alias field

Description: A client attempts to connect directly to the security gateway but the server was not specified.

343 - Not caching answer response as it conflicts with configured information

Description: A response for a DNS query conflicts with the configuration information on the security gateway. Check the server, at the source address listed in the resource parameter for correct configuration, or check the security gateway configuration for this host.

343 - Not caching authority response as it conflicts with configured information received from outside

Description: A response for a DNS query conflicts with the configuration information on the external side of the security gateway. Check the server, at the source address listed in the resource parameter for correct configuration, or check the security gateway configuration for this host.

343 - Not enough buffer to copy certificate distinguished name in ASCII

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Not enough buffer to copy encrypted configuration mode message

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Out of memory

Description: This message indicates an out of memory situation.

343 - Outgoing interface not determined for connection going into a VPN tunnel, so connection will be aborted

Description: The outgoing interface has not been determined for the connection through the VPN tunnel, so the connection is aborted.

343 - Output error

Description: (Sun Solaris only) An audio notification is not sent because the notify daemon is unable to communicate with the audio device.

343 - Packet (<variable 1>) from proxy dropped because it should have gone into a tunnel but did not

Description: The security gateway dropped a packet destined for a tunnel that the security gateway couldn't find.

343 - Packet for interface was routed to interface

Description: The packet was dropped. There was an attempt to send a packet out of the wrong interface. By default, this message is sometimes suppressed because the global/LogLevel default is less than two. This check can also be disabled entirely. You should only do this for an unusual network configuration. The global driver variable controlling this message is Dont_Check_Same_Interface.

343 - Packet from proxy dropped while trying to enter tunnel <variable 2>

Description: A transmit packet was matched to an outgoing tunnel, and the packet was not subject to proxy processing, and the source address of the packet was not on the security gateway, so the packet was dropped.

343 - Page recipient name too long

Description: The pager recipient's name is too long, so the pager notification could not be sent.

343 - Paging system forced disconnect

Description: The notify daemon is unable to send paging notifications because of paging protocol problems.

343 - Parsing extension. Restoring default: Scan All Files

Description: This message indicates a problem with the antivirus scanning but the process continues to function.

343 - Please examine your certificate configuration file and restart the security gateway

Description: Isakmpd (the VPN server) could not log into the security gateway. Check the entrust.cf file in the configuration directory, to determine the cause of the problem.

343 - Process vanished

Description: A proxy, management daemon or security gateway service, which should be running are no longer running.

343 - Proposed security association lifetime exceeds the cert notValidAfter

Description: This is a configuration error. When authenticating using the Certificate method, it is found that the tunnel has a lifetime which exceeds the lifetime of the Certificate.

343 - Read operation timed out

Description: The secure remote login (SRL) session timed out because of a communications problem. Check the connectivity with the security gateway.

343 - Received peer CPI of zero, defaulting to using well-known CPI

Description: This is a warning that appears when you use the compression algorithm for authentication. This is part of the normal procedure.

343 - 'recurse_for' directive found in private hosts file

Description: The “recurse_for” directive is found in the private hosts file.

343 - Reference to destination group from filter set is not possible due to group errors. DENY rule, so treating as *Universe

Description: A reference to destination group from the filter set is not possible because of group errors. The message provides details on this error.

343 - Reference to destination group from filter set truncated due to group errors (ALLOW rule)

Description: A reference to the destination group from the filter set is truncated because of group errors.

343 - Reference to source group from filter set is not possible due to group errors. DENY rule, so treating as *Universe

Description: A reference to the source group from filter set is not possible because of group errors. The message provides details on this error.

343 - Reference to source group from filter set truncated due to group errors (ALLOW rule)

Description: A reference to source group from filter set truncated due to group errors.

343 - Rejected connection from source because it was on the Realtime Blackhole List

Description: SMTP rejects a mail message because it arrives from an illegal sender.

343 - Response packet from RADIUS server failed the authentication check. The shared key may be incorrect

Description: The response packet from the RADIUS server has failed the authentication check, which is caused by an incorrect shared key.

343 - Response packet received that has an unrecognized or deleted ID

Description: DNS receives a response to a query that it has not requested, so it drops the packet. This could be an indication of a connectivity problem on the security gateway.

343 - Response packet received that is not an address asked for

Description: DNS receives a response to a query that it has not requested. This could be an indication of a connectivity problem on the security gateway.

343 - Response received with invalid question count

Description: An invalid DNS response is received, and it is dropped.

343 - Retry limit reached for the remote security gateway

Description: The ISAKMP daemon is unable to get an answer from the peer within a set time period. This occurs if the peer machine is down, no peer exists, or if the network traffic is heavy.

343 - Returned key has the wrong parity

Description: During the backup or restore of a security gateway configuration, the encryption or decryption has failed. The backup or restore did not complete.

343 - Returned key is weak

Description: During the backup or restore of the security gateway configuration, the encryption or decryption has failed. The backup or restore process was unable to complete.

343 - 'root_server' directive found in public hosts file

Description: The “root_server” directive is found in the public hosts file.

343 - Rule database reload caused connection to be denied

Description: Gwcontrol is the process of reloading when a connection is being made, so the connection gets terminated.

343 - Rule references non-existent profile

Description: The ratings profile referenced in one of the security gateway rules, for NNTP, is not configured correctly.

343 - Running changelogfile in an attempt to make more disk space for the log file

Description: LogService daemon requires more disk space, so it performs a roll over to delete old log files.

343 - Save configuration failed

Description: The changes to the configuration file have not been saved. The filename parameter identifies the configuration file.

343 - Sender has exceeded hard recipient limit, so message will be denied

Description: This message is received when you exceed the hard-recipient limit. Adhere to the limits and send the message again.

343 - Sender has exceeded soft recipient limit, so recipients are denied

Description: This message is received when you exceed the soft-recipient limit. Adhere to the limits and send the message again.

343 - SMTP host not responding

Description: The notify daemon sends alerts when the limit for the configured level of log messages has been reached. In this case, the notify daemon is unable to communicate with the remote SMTP server. The notification has not been sent.

343 - Some filters not loaded in filter set due to earlier errors

Description: Some filters do not get loaded in the filter set because of prior errors.

343 - Some filters not loaded in group due to earlier errors

Description: Some filters do not get loaded in the group because of prior errors.

343 - Start of authority format string is not valid

Description: This message indicates a problem in the DNS configuration files. The start of authority format string is invalid. You can rectify the problem through the SMGI.

343 - Symantec Client VPN not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - TCP GSP is enabled and tcpap-gsp.handle_single_ports is set. This means that single ports will be handled by TCP GSP. You want to correct one of these settings

Description: TCP GSP is enabled and tcpap-gsp.handle_single_ports is set.

343 - tcp-gsp.handle_port_ranges is set, and TCPAP GSP is enabled. This means that TCP GSP will handle port ranges

Description: tcp-gsp.handle_port_ranges is set, and TCPAP GSP is enabled. The TCP GSP can handle port ranges.

343 - The antivirus scan server cannot be resolved as a hostname

Description: The antivirus scan server could not be located.

343 - The antivirus scan server detected a problem with a file <variable 1>. File was <variable 2>. Found <variable 3> and <variable 4>. Threat ID was <variable 5>

Description: A virus has been detected in the file. The parameters provide details on the infected file and the virus.

343 - The antivirus scan server detected a virus, so file not transferred

Description: The HTTP daemon encountered a virus in a file. This file was not transferred.

343 - The authentication interaction took seconds and returned value

Description: The client's authentication process with the security gateway lasted for a considerable time and the authentication returned a value in the parameter.

343 - The authentication scheme was not found or cannot be started

Description: Authentication information was not found or was unable to start. The reason is available in the message parameters.

343 - The authentication sequence has the same name as a built-in mechanism. The built-in version will override the sequence, which is probably not what you anticipated

Description: The authentication sequence has the same name as a built-in mechanism and the built-in version overrides the sequence.

343 - The domain name is invalid, so it has been changed

Description: The SMTP daemon requires a fully qualified domain name, but did not receive one, so it converts this name into a fully qualified name.

343 - The host has completed <variable 1> connections in the last <variable 2> seconds

Description: The user attempts to make many connections in a short period of time.

343 - The hostname for the RADIUS server cannot be resolved

Description: The domain name and the address cannot be found for the RADIUS server.

343 - The interface has multicast enabled, but no server transparency for the subnet broadcast address. This means that subnet broadcasts will not be delivered. Suppress this message with vpn.log_missing_multicast_address=FALSE

Description: The error information and the corrective action is available in the message.

343 - The LDAP server cannot be contacted

Description: The security gateway was unable to contact the LDAP server, identified in the resource field of the message.

343 - The LDAP server cannot be resolved as a hostname

Description: The LDAP server could not be located.

343 - The NAT entry mapping could not be preserved and was deleted

Description: The new NAT pool definitions disallow an existing NAT entry.

343 - The node secret file has not been downloaded from the ACE server

Description: This warning can occur when the security gateway is not a client of the RSA SecurID server (check the RSA SecurID server logs), the “sent node secret” checkbox is set on the RSA SecurID server, or the user has entered an incorrect user name/PIN/tokencode combination.

343 - The static username and password check took <variable 1> seconds

Description: The status of the check conducted is available in the parameters.

343 - The target range includes the interface address. This range will not be loaded

Description: The range of addresses specified in the configuration setting is invalid.

343 - The target range includes the interface address. This range will not be loaded as a proxy ARP range

Description: The range of addresses specified in the configuration setting is invalid.

343 - The user authenticated successfully when given a dummy password prompt. Access has been denied

Description: The user is defined on the security gateway, but is not configured to use any of the authentication methods in this sequence.

343 - The user authenticated with an invalid domain name

Description: A client, using Microsoft Windows, attempts to authenticate through a Microsoft Windows domain but the domain name used is invalid.

343 - Timed out waiting for response from paging system

Description: The paging system did not respond in a timely manner. This notification will not be sent.

343 - Timed out waiting for response from TACACS+ daemon

Description: The session is timed out while waiting for a response from the TACACS+ daemon.

343 - Timeout waiting for response from paging system

Description: The paging system did not respond in a timely manner. This notification is not sent.

343 - Tried to fetch the zone, but was disallowed

Description: A client is denied access to domain information in the gateway because the administrator disallows users to access such information.

343 - Tunnel ignored because both gateways are local

Description: An attempt to add a tunnel to the tunnel database was rejected because both end points are on the same security gateway. This is a configuration error.

343 - Tunnel ignored because it is neither a gateway or local

Description: An attempt to add a tunnel to the tunnel database was rejected because one endpoint of the tunnel does not terminate at the security gateway. This is a configuration error.

343 - Tunnel is being deleted

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Two NAT pools have overlapping NAT address ranges

Description: Conflicting NAT definition is found. Remove this conflicting information.

343 - Two security gateways have the same IP address, so neither will be loaded

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Unable to allocate NAT address for client, so connection will be denied

Description: Unable to allocate NAT address for the client as the NAT pool is small.

343 - Unable to connect to server

Description: This message is from the Notify daemon or TAC plus authentication. The parameters identify the server with which it was attempting to establish a connection. If this message is from the Notify daemon, a mail notification is not sent.

343 - Unable to create marker file

Description: Unable to create the file, which is used to maintain the state of the security gateway.

343 - Unable to determine interface for destination address. Is the system local and down? Test connectivity with ping

Description: Unable to determine the interface for the destination address, which is because the system is local and is down. Use the ping command to check if the connection is successful.

343 - Unable to get modem attributes

Description: The notify daemon is unable to get the modem attributes. Check the configuration of the paging device.

343 - Unable to kill process with process ID

Description: The vulture daemon or the raptor service (Eaglesvc on Microsoft Windows) is unable to kill this particular process.

343 - Unable to load NAT entries as the driver cannot be opened

Description: Unable to acquire NAT pool information because of communication problems with the security gateway.

343 - Unable to lock modem

Description: The notify daemon is unable to send pager notification because it cannot access the driver. Reboot the security gateway.

343 - Unable to open modem device

Description: The notification daemon was unable to open the modem to send pager notifications because the device is busy.

343 - Unable to open modem file

Description: The notify daemon sends alerts when it reaches the limit for the configured level of log messages. In this case, notify daemon attempts to dial the pager over the modem, and it fails.

343 - Unable to process item on line

Description: The nat.cf file is corrupted.

343 - Unable to read from modem

Description: Unable to read the modem configuration file. Pager notifications will not be sent.

343 - Unable to reconfigure

Description: An attempt to restore the gateway configuration has failed because of a bad configuration entry.

343 - Unable to set modem attributes

Description: The notify daemon is unable to communicate with the modem, so the pager notifications is not sent. Check the modem configuration.

343 - Unable to set non-blocking I/O

Description: The notify daemon was unable to initialize the modem into a non-blocking state (blocking state would force the daemon to wait for responses). Therefore, pager notifications are not sent.

343 - Unable to synchronize device

Description: The notify daemon is unable to send pager notification because the modem cannot be synchronized.

343 - Unable to terminate process with process ID

Description: The vulture daemon attempts to terminate a non-authorized process.

343 - Unable to write to modem

Description: (Microsoft Windows only) The notify daemon is unable to write to the modem. Check the configuration.

343 - Unexpected connection attempt. Expected connection from different host

Description: The remote command daemon received an illegal connection request.

343 - Unexpected modem response

Description: Failed to receive the “OK” protocol when synchronizing the modem. As a result, the security gateway will not send pager notifications.

343 - Unexpected network connection close while waiting for result

Description: Remotelog attempted to get a remote login and terminated abnormally.

343 - Unexpected response from paging system

Description: The notify daemon is unable to send paging notifications because of paging protocol problems. The notification is not sent.

343 - Unknown command

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Unknown error in file

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Unknown modem speed, so using 9600

Description: The Notify daemon was unable to determine the correct modem speed, so it will use the default speed.

343 - Unknown Protocol ID negotiated

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Unknown status returned from ISAKMP engine

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Unlikely domain name

Description: The domain name appears to be invalid (invalid characters/ length issues, and so forth), on diagnosis, but the security gateway will continue to query.

343 - Unsupported configuration id_type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - Unsupported id_type

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - User aborted negotiation with peer

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

343 - User has no IKE info in ikeusers.cf

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - User is a member of too many groups, so using the first <variable 1> only

Description: The user is a member of many groups, so only the first few are being used. The administrator should ensure that the user is authorized to be a member of these groups.

343 - User is not IKE enabled

Description: This indicates a configuration error. You have not actually enabled the user, after identifying the user to be IKE enabled.

343 - Using rule ID <n> because two equally good rules were found

Description: Two rules and their time range match, so rule ID <n> is being used.

343 - Version negotiation failure (failed to receive data)

Description: The versions of remlog and the security gateway do not match. Ensure that you use the version of remlog that came with the security gateway.

343 - Version negotiation failure (timed out waiting for data)

Description: The versions of remlog and the security gateway do not match. Ensure that you use the version of remlog that came with the security gateway.

343 - Virus infected file will not be transferred. Connection aborted

Description: An attempt to transfer an infected file on a HTTP, FTP or SMTP failed.

343 - VPN policy not defined

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - VPN policy type not supported

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Vpnpolicy '<variable 1>' not defined in vpnpolicy file

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Vpnpolicy naming limit reached. Create Similar policy

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Vpnpolicy not defined in pkvpnpolicy file

Description: An attempt to restore the security gateway configuration has failed because of a bad configuration entry.

343 - Will not attempt to restart process because restart threshold reached

Description: The raptor service (Eaglesvc on Microsoft Windows) has the task of keeping the process running. In this case, it has performed a restart numerous times, and will not attempt again, as the restart threshold has been reached.

343 - You can not use default certificate for RSA authentication. Must reconfigure with Non-default certificate

Description: This indicates a misconfiguration. To use the RSA method of authentication, you must reconfigure, and should not use the default certificate.

343 - You must define a user to be used as the default IKE user

Description: This is triggered by an unusual IKE connection request. You must define the default IKE user (default_ikeuser) for connections to be established.

344 - Non-transparent call

Description: A client attempts to connect to realaudio, SMTPD or TCP GSP directly. Either the security gateway has not been correctly configured to proxy SMTP/mail or the inside mail server has not been correctly configured to send outbound mail.

345 - Illegal canonical hostname

Description: The service received an illegal host name in the response from DNS domain.

345 - Illegal top level domain name in canonical hostname

Description: The service received an illegal domain name (must begin with a letter) in the response from DNS domain.

345 - Out of memory - cannot allocate comforting buffer. No scanned files will be comforted

Description: The HTTP daemon lets you buffer files that are sent to the antivirus server. In this case, the memory available to buffer is not sufficient, so the comforting or buffering process will not occur.

347 - Possible port scan detected

Description: This indicates that the security gateway rejected a connection to a reserved TCP port. A reserved port is one which is less than 1024, by default. This message occurs each time a closed reserved port is accessed. You can enable or disable this message on a per interface basis in the SGMI.

352 - A content violation has been found

Description: The antivirus scan engine has found suspicious data, and will perform the configured action on the file.

352 - File or directory already exists

Description: The process is attempting to create, copy or move a file that already exists at the target location. The file name is available in the resource parameter.

352 - File or directory does not exist

Description: The process is unable to locate the file it requires. The file name is available in the resource parameter.

352 - Unable to open shared memory containing resource strings

Description: The process was unable to open ResourceDictionary.xml, which must be located in:

/var/lib/sg/lang/xx (UNIX)

\usr\raptor\sg\lang\xx (Microsoft Windows).

352 - Unrecognized driver message code

Description: The log service daemon is unable to read the ResourceDictionary.xml. Therefore, some strings (password prompt) displayed to the user may appear unusual.

366 - The network interface card is being flooded with receive packets. Possible attack or misconfiguration

Description: Some buffers are being dynamically allocated instead of using the statically allocated ones, which impacts performance slightly. This can result from an attack against the security gateway, or that a high-volume security gateway needs more resources. Check the index for ScaleFactor, and determine if increasing the number of buffers allocated is warranted.

Every 10 minutes, this message repeats if the condition still exists. The count is the number of times the incident occurs, is cumulative, and is much larger than the number of messages that appear in the log file.

371 - A reboot is required to complete the operation

Description: The hotfix utility is requesting a reboot to complete the operation.

371 - Driver log messages at this level suppressed

Description: Due to increased volume, information log messages are not logged until conditions improve so that log services do not load the CPU.

371 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve so that log services do not load the CPU.

371 - The firewall must be stopped and restarted to complete the operation

Description: The hotfix utility is requesting a security gateway restart process to complete the operation.

390 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.
Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

392 - A infection has been found

Description: A virus has been detected, and the details are logged by the antivirus engine. The parameters provide information on the virus and the preventive action.

392 - Virus infected file was partially transferred and should be deleted

Description: A virus was found in a file during an FTP or HTTP session. Because comforting was turned on, a portion of the file was created before the virus was detected. It should be deleted.

Error messages (400-499)

Log messages in the range 400-499 are issued when normal security gateway operation cannot complete successfully. The security of your gateway is still ensured, but you should attempt to correct the error as soon as possible.

400 - Invalid adapter

Description: This occurs only on the Symantec Client VPN client because of configuration issues.

401 - <Variable 1>

Description: If this message is from gwcontrol, this indicates an error response from a daemon when gwcontrol sent a kill command.

401 - Accelerator does not support this AH algorithm

Description: The hardware accelerator does not support authentication header (AH) authentication.

401 - Accelerator does not support this ESP algorithm

Description: The hardware accelerator does not support the IPsec algorithm. If this happens more than once, try running the hardware accelerator diagnostic program.

401 - Accept failed on port

Description: A socket API accept() call failed in nntpd. The system may have run out of resources.

401 - ACK for wrong blacklist packet

Description: The Notify daemon received an invalid protocol while communicating with the blacklist daemon. If the condition persists, restart the blacklist daemon.

401 - Allocation failed (concurrent server)

Description: Memory allocation failed. The connection cannot be handled.

401 - Allocation failed (connection I/O)

Description: Failed to connect to a content scanning server (CSS) or a news server. This is an internal resource allocation issue. Try decreasing the load.

401 - Allocation failed (cryptography)

Description: This is an internal resource allocation issue. Try decreasing the load.

401 - Allocation failed (statistics)

Description: This is an internal resource allocation issue. Try decreasing the load.

401 - Allocation failed (thread)

Description: Failed to create a new thread for a new connection. This is an internal resource allocation issue. Try decreasing the load.

401 - Allocation failed (transparency)

Description: This is an internal resource allocation issue. Try decreasing the load.

401 - Argument is an inappropriate address for the fudge command, so line ignored

Description: The argument is an inappropriate address for the fudge command, so the line is ignored.

401 - Attempt to blacklist rempass-registered address. It is possible that an active denial-of-service attack is being carried out against the address

Description: This message is self-explanatory.

401 - Attempt to configure invalid address

Description: The format of the address that is attempted to be configured is invalid.

401 - Attempted to write data, but wrote less

Description: This is an internal error.

401 - Authentication failed

Description: The user attempted to connect to the server but failed to authenticate properly.

401 - Bad blacklist ACK packet

Description: The Notify daemon received an invalid protocol while communicating with the blacklist daemon. If this condition persists, restart the blacklist daemon.

401 - Bad blacklist packet type (not an ACK)

Description: The Notify daemon received an invalid protocol while communicating with the blacklist daemon. If this condition persists, restart the blacklist daemon.

401 - Bad filename provided

Description: For the remote log retrieval tool, the filename given is too long.

401 - Blacklist ACK failed authentication

Description: The Notify daemon received an invalid protocol while communicating with the blacklist daemon. If this condition persists, restart the blacklist daemon.

401 - Blacklist packet invariant snafu

Description: The Notify daemon received an invalid protocol while communicating with the blacklist daemon. If this condition persists, restart the blacklist daemon.

401 - Blacklist protocol not yet supported

Description: The Notify daemon received an invalid protocol while communicating with the blacklist daemon. If this condition persists, restart the blacklist daemon.

401 - Cannot access LCD device

Description: The LCD hardware is not functioning correctly.

401 - Cannot add multicast address as it is not class D

Description: The address supplied is not a multicast address, and cannot be added.

401 - Cannot add tunnel

Description: The driver was unable to add the tunnel to the tunnel database.

401 - Cannot adjust the time of day

Description: An attempt to adjust the time of day has failed.

401 - Cannot adjust time

Description: An attempt to adjust the time of day has failed.

401 - Cannot allocate memory for blacklist packet

Description: The Notify daemon is unable to send the protocol to the blacklist daemon, which blacklists a host. Reboot the system, if the problem persists.

401 - Cannot allocate memory for connection block

Description: This is a HTTP protocol error and it indicates a security gateway resource problem. The administrator can rectify this.

401 - Cannot allocate memory for request

Description: This is a HTTP protocol error, and it indicates a security gateway resource problem that the administrator can rectify.

401 - Cannot allocate space for incoming data

Description: This is a HTTP protocol error, and it indicates a security gateway resource problem that the administrator can rectify.

401 - Cannot contact driver

Description: Eagle service is unable to contact the driver.

401 - Cannot create request queue

Description: This is a HTTP protocol error, and it indicates a security gateway resource problem that is cleared by restarting the proxy.

401 - Cannot create server socket list

Description: This is a HTTP protocol error and it indicates a security gateway resource problem that is cleared by restarting the proxy.

401 - Cannot create thread

Description: A proxy was unable to create an additional thread for processing connections.

401 - Cannot create thread (out of memory)

Description: A process was unable to create an additional thread for processing connections. If the process continues, it will do so at a degraded level.

401 - Cannot determine source IP address. Source IP will not be blacklisted

Description: The security gateway detected a condition which causes the source address to be blacklisted. As the source address is not specified, it is not blacklisted.

401 - Cannot determine type of interface

Description: This indicates a severe Sun Solaris DLPI installation or network configuration error.

401 - Cannot determine type of interface or cannot find interface name

Description: This indicates a severe Sun Solaris DLPI installation or network configuration error.

401 - Cannot disable user

Description: (Microsoft Windows only) Vulture daemon is unable to save an illegal account.

401 - Cannot execute

Description: A component was unable to run a user script. The log message identifies the component. Execute the script from the command line to check its validity.

401 - Cannot find entry for message ID

Description: The FTP daemon attempts to load the string resources, that it requires, to create the FTP greeting, but was unable to complete. FTP will terminate. Confirm that the ResourceDictionary.xml is in the sg\lang\en directory.

401 - Cannot find file tar file

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Cannot find kill file descriptor for daemon

Description: Gwcontrol attempted to kill a connection but the connection information was invalid.

401 - Cannot generate a key schedule from the session key

Description: A secure remote login (SRL) client was unable to connect to the security gateway's SRL daemon because it could not generate a key schedule from the session key.

401 - Cannot get blacklist protocol number

Description: The notify daemon was unable to communicate with the remote blacklist daemon because of an invalid protocol. The IP address is not blacklisted.

401 - Cannot get interface list

Description: Blacklist daemon attempts to get the interface list to track the intruder, but fails.

401 - Cannot get IP address of blacklist firewall

Description: Unable to get the IP address of the blacklist daemon that runs on another security gateway. The list of blacklisted hosts are not sent.

401 - Cannot get process list

Description: Vulture daemon is unable to acquire a list of legitimate processes that are functioning.

401 - Cannot get socket for connection

Description: Unable to allocate a socket for the connection between the security gateway services and gwcontrol.

401 - Cannot get system name

Description: (Microsoft Windows only) Unable to get the name of the security gateway, which is required by Microsoft Internet Information Server.

401 - Cannot initialize rule cache

Description: The component was unable to load the security gateway rules as it does not have sufficient memory.

401 - Cannot initialize rule caches, so performance may be degraded

Description: The HTTP daemon was unable to read the rules into its cache. The HTTP daemon will continue to apply the rules, but will have to read the rule file repeatedly.

401 - Cannot kill process

Description: The process cannot be killed.

401 - Cannot lookup attached devices

Description: There were either no interfaces configured, or an error occurred while building a list of interfaces.

401 - Cannot open configuration file

Description: Gwcontrol could not open its configuration file for reading. This message comes from many locations including the bullfrog daemon, ISAKMP daemon, VPN, and filter utilities. Each attempt to open a configuration file failed. The name of the file gwcontrol requested should be in the filename parameter.

401 - Cannot open file

Description: Unable to open the specified file.

401 - Cannot read configuration file

Description: This indicates a missing cluster.cf file or corrupted file. Contact support for assistance.

401 - Cannot read etc/passwd

Description: The secure remote login (SRL) daemon is unable to access the password file. All SRL connections are denied.

401 - Cannot read file

Description: Unable to read the specified file.

401 - Cannot set all transparent ranges for interface

Description: A tunnel or cluster is unable to set up its interfaces properly. Therefore, transport connections will not function.

401 - Cannot set interface parameters

Description: Cannot set address and mask for interface.

401 - Cannot set time of day

Description: An attempt to set the time of day has failed.

401 - Cannot start HA/LB engine

Description: Unable to start the high availability/load balancing (HA/LB) engine. The system will restart the engine after waiting for 5 seconds. If the problem persist, try to reboot the whole cluster.

401 - Cannot start logoff for user

Description: (Microsoft Windows only) The vulture daemon attempts to block a user who is unauthorized to log into the system.

401 - Cannot synchronize battery time

Description: The time on the hardware clock cannot be set.

401 - Card name is too long

Description: This is an internal resource allocation issue. Try decreasing the load.

401 - Command line broadcast delay value is unlikely

Description: The value specified from the command line is not valid. To fix the problem, a different value should be used.

401 - Command line broadcast delay value undecodable

Description: The value specified from the command-line is not valid. To fix the problem, a different value should be used.

401 - Command line encryption delay value is unlikely

Description: The value specified from the command-line is not valid. To fix the problem, a different value should be used.

401 - Command line encryption delay value undecodable

Description: The value specified from the command-line is not valid. To fix the problem, a different value should be used.

401 - Command line trusted key %s is unlikely

Description: The value specified from the command-line is not valid. To fix the problem, a different value should be used.

401 - Configuration error (Minpoll > maxpoll)

Description: An inconsistency in the xntpd configuration file has been identified. To resolve the problem, the minpoll value should not be set to be greater than the maxpoll value.

401 - Could not connect to the SESA agent

Description: The notify daemon is unable to connect to the SESA agent, so the log messages are not sent to SESA. Check the connections to the SESA Manager.

401 - Could not create proxy

Description: (Microsoft Windows only) Eaglesvc was unable to start proxies.

401 - Could not list user accounts

Description: (Microsoft Windows only) The vulture daemon is unable to list the user accounts, which causes some illegal user accounts to exist that cannot be cleaned.

401 - Could not resolve name

Description: The supplied name could not be resolved. Use the dotted octet instead.

401 - Could not stop service

Description: Vulture daemon attempts to stop a service but fails. Check the parameters to identify the cause.

401 - Could not unlink file

Description: The file could not be deleted because the file is probably in use. To resolve the problem, try closing any related programs.

401 - Daemon failed to restart self

Description: A daemon has terminated without warning. It is supposed to restart itself, but has failed to do so.

401 - Destination not provided

Description: A proxy or service was unable to determine the address of the destination.

401 - Destination packet too short to contain data

Description: Allocated output packet is too short.

401 - Encrypted read failed

Description: A secure remote login (SRL) connection terminated because the encryption of the packet failed.

401 - Entrust input buffer overflow

Description: The data for a signature verification was too big to fit into a buffer. The authentication will fail.

401 - Entrust input overflow

Description: The data for a verification was too big to fit into a buffer. The authentication will fail.

401 - Error building blacklist packet

Description: The Notify daemon encountered errors while building the packet that is to be sent to the blacklist daemon. This IP address is not blacklisted.

401 - Error from blacklist

Description: The Notify daemon was unable to receive data from the blacklist daemon. The IP address is not sent.

401 - Error sending blacklist packet

Description: The Notify daemon encountered errors while sending the packet to the blacklist daemon. This IP address is not blacklisted.

401 - Execution of daemon failed

Description: An attempt to run the security gateway process has failed.

401 - Failed to allocate memory for preshared record

Description: This indicates an out of memory condition.

401 - Failed to create backup directory

Description: On a security gateway running Microsoft Windows, a temporary directory is used for backup purposes. In this case, the save config utility was unable to create this directory, so the backup process failed.

401 - Failed to create event

Description: If the logservice daemon sends this message, it indicates an error synchronizing with the kernel.

401 - Failed to create peer context

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Failed to find interface name for address

Description: A proxy or service was unable to determine the interface name, on the security gateway, for this particular address.

401 - Failed to get memory to sort rules

Description: This is an internal resource allocation issue, either decrease the load or call customer support.

401 - Failed to list active hotfixes

Description: The hotfix utility encountered a problem while attempting to retrieve the active hotfix list. Check previous log messages to determine the cause of the failure.

401 - Failed to list all hotfixes

Description: The hotfix utility encountered a problem while attempting to retrieve the list of all hotfixes installed. Check previous log messages to determine the cause of the failure.

401 - Failed to list recent hotfixes

Description: The hotfix utility encountered a problem while attempting to retrieve the list of hotfixes installed with the most recent hotfix bundle. Check previous log messages to determine the cause of the failure.

401 - Failed to login into Entrust engine

Description: The tunnel server was unable to log on to the Entrust server.

401 - Failed to open key

Description: Failed to read a registry key.

401 - Failed to open registry path

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Failed to query value for path

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Failed to register service control handler

Description: (Microsoft Windows only) Eaglesvc is unable to register with the service control manager.

401 - Failed to remove tunnel from driver

Description: Unable to clean up a tunnel. The tunnel is not operational and is only consuming resources.

401 - Failed to restart process

Description: Unable to restart the process.

401 - Failed to send bytes to peer

Description: This is a normal situation. This problem occurs when a node fails in a cluster during an interface change.

401 - Fork failed, so cannot reload

Description: One of the security gateway's software services tried to fork, but failed. The system has probably run out of swap space or processes. Reboot the system.

401 - Fork of new daemon failed

Description: Attempts to create a new process have failed.

401 - Getpeername failed, so dropping connection

Description: The secure remote login (SRL) client checks the identity of the client as part of the verification of the session. In this case, it was unable to check the credentials, so the connection is dropped. If this is a legitimate connection, check the DNS configuration and/or TCP/IP settings.

401 - Getsockname failed on file descriptor

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - High dynamic port is less than low dynamic port

Description: The datagram proxy is unable to use the port server, which is configured to check the datagram configuration.

401 - I/O error on suspicious article file

Description: The network news transfer protocol (NNTP) daemon detected an error while inspecting an article.

401 - I/O error on trace file

Description: If tracing is enabled, this indicates that the proxy is unable to open its trace file.

401 - Illegal value for clientlimit command, so line ignored

Description: The client limit is too high. Lower the client limit to prevent this message from appearing again.

401 - Insufficient space for listing interfaces

Description: This is the case of an internal resource allocation issue.

401 - Invalid blacklist message (cannot determine destination IP address)

Description: The security gateway has detected a condition which would normally cause the source address to be blacklisted. In this case, the blacklist message, is itself, invalid, so source address is not blacklisted.

401 - Invalid blacklist message (cannot determine destination port)

Description: The security gateway has detected a condition which would normally cause the source address to be blacklisted. In this case, the blacklist message, is itself, invalid, so source address is not blacklisted.

401 - Invalid blacklist message (cannot determine source or destination IP addresses)

Description: The security gateway has detected a condition which would normally cause the source address to be blacklisted. In this case, the blacklist message, is itself, invalid, so source address is not blacklisted.

401 - Kernel logging read failed

Description: The log service daemon is unable to receive log messages from the kernel. This message is evidence that an attack has been attempted.

401 - MAC address and broadcast address lengths differ

Description: This message indicates a severe Sun Solaris DLPI installation or network configuration error.

401 - Missing argument to -f rule cache option

Description: The HTTP daemon was unable to set its rule cache flush interval, which was passed into the program that was running.

401 - Missing cookie information

Description: A newly started NNTP process did not receive the connection information of its parent.

401 - Missing session structure

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Multicast address using wildcard socket

Description: A multicast address cannot use a wildcard socket.

401 - Net write failed

Description: The secure remote login (SRL) daemon was awaiting the challenge from the client, and received a communication error. This session is terminated.

401 - No address for fudge command, so line ignored

Description: You have to specify an address for the fudge command.

401 - No address for trap command, so line ignored

Description: You have to specify an address for the trap command.

401 - No address, so line ignored

Description: An address has to be specified.

401 - No applicable rules found, yet rule was still selected

Description: This is an internal error.

401 - No memory resources for accelerator

Description: Insufficient memory available for the accelerator operation.

401 - No server suitable for synchronization found

Description: A server that runs the NTP protocol is required for synchronization. Try specifying a different server.

401 - No spare minor raw packet devices

Description: There are no available slots to support proxies that contact the driver through raw packet interfaces on Sun Solaris.

401 - No value for clientlimit command, so line ignored

Description: You have to specify a value for the clientlimit.

401 - No value for setvar command, so line ignored

Description: You have to specify a value for the setvar command.

401 - Not enough MAC buffers preallocated

Description: Insufficient memory available for the accelerator operation.

401 - NTP user interface routines not configured in this kernel

Description: The NTP user interface routines are not available with the current kernel. A modified kernel may have been introduced.

401 - Open event failed

Description: This is a HTTP protocol error, and it indicates a security gateway resource problem that the administrator can rectify.

401 - Opts failed

Description: A gwcontrol setsockopt command failed.

401 - Out of memory

Description: Memory could not be allocated to perform the requested function.

401 - Process terminating with signal

Description: The process has terminated abnormally.

401 - Read from daemon failed

Description: Gwcontrol was unable to read a response from a security gateway service.

401 - ReadFile failed with code WAIT_FAIL on the VPN driver

Description: The VPN driver is not responding, the security gateway is under attack.

401 - Received non-ICMP packet from driver

Description: Pending removal. Programming error.

401 - REDTAIL_FEATURES_SET failed

Description: Unable to inform the driver on the security gateway where the features are enabled.

401 - Registry path too long

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Remote management login failed

Description: The administrator did not authenticate correctly with the SGMI or secure remote login (SRL).

401 - Repeated

Description: Messages that have occurred multiple times have been consolidated, indicating the possibility of an occurrence of a more serious problem.

401 - Restrict requires an address

Description: You have to specify an address that is to be restricted.

401 - Secure connect failed

Description: A secure remote login (SRL) client was unable to establish a connection to the security gateway's SRL daemon.

401 - Send to NTP server failed

Description: An error occurred, while attempting to send data to the NTP server.

401 - Should be 'authenticate yes|no'

Description: The argument to authenticate should be “yes” or “no”.

401 - Socket creation failed

Description: Unable to create a socket.

401 - Socket timed out

Description: A socket timed out and is no longer active.

401 - Socket timed out while waiting on socket

Description: While waiting for a socket call to complete, a timeout occurred.

401 - Source not provided

Description: A proxy or service was unable to determine the address of the source.

401 - There has been a deadlock, so must restart daemon

Description: The daemon is waiting for a resource to clear up the situation, and one daemon is being restarted.

401 - There was an error during the endpoint_complete_resolve_dest IOCTL

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Tick value is unreasonably large

Description: You have to select a smaller value for Tick.

401 - Time error is way too large (set clock manually)

Description: A gross difference in time could indicate a hardware failure of some type.

401 - Timed out waiting for blacklist ACK

Description: The Notify daemon encountered errors while receiving a response from the blacklist daemon. The IP address is not blacklisted.

401 - Tokenizing error in file

Description: This problem is caused by a corrupt file.

401 - Transform data is not a multiple of

Description: The encrypted payload length is not a multiple of the algorithm block.

401 - Trap interface requires an argument

Description: You have to specify an interface to trap.

401 - Trap port requires an argument

Description: You have to specify a port to trap.

401 - Tried to use -f command line switch. See the manual for ways to configure the rule cache

Description: Could not set rule cache flush interval through the command-line.

401 - Trying to kill process ID

Description: Gateway control (Gwcontrol) tries to kill a process and fails. Gwcontrol may have been directed by the administrator to kill the process.

401 - Two instances of default interface in hash table

Description: Only one interface is the default interface. Remove the undesired one.

401 - Unable to add IP to blacklist

Description: The security gateway identifies a particular IP address that should be blacklisted, but was unable to add it to the list. As a result, the IP address may attempt to access the security gateway. This is an internal error and could indicate a problem with the security gateway.

401 - Unable to allocate memory for arguments

Description: Unable to allocate enough memory to create the process information table in the raptor service (Microsoft Windows – eaglesvc) daemon.

401 - Unable to bind blacklist socket

Description: The Notify daemon encountered errors receiving a response from the blacklist daemon. The IP address is not blacklisted.

401 - Unable to bind to any UDP socket for listening to ISAKMP requests, so service will exit

Description: (Microsoft Windows only) To rectify this problem, disable the visual notification from the Dr. Watson utility for Microsoft Windows.

401 - Unable to bind to oobauthd port

Description: The oobauth daemon is unable to listen on its port because another process is listening on the oobauth port.

401 - Unable to bind UDP socket

Description: In the case of bullfrog daemon, unable to bind to cluster command control port (default to 6373). Ensure that no other service is using it, or configure bullfrogd to use a different port.

401 - Unable to change log file over to the new log file name

Description: The logservice daemon attempts to roll over the log file but fails. There should be a subsequent log message that indicates the next course of action.

401 - Unable to clear driver blacklist

Description: The blacklist daemon is unable to inform the driver to clear the old blacklisted IP addresses. As a result, some of the addresses continue to be denied access to the security gateway services.

401 - Unable to connect oobauthui datagram socket

Description: The Out of Band Authentication (OOBA) daemon is unable to make the connections that it requires to authenticate users. No user is able to authenticate.

401 - Unable to create datagram socket

Description: The Out of Band Authentication (OOBA) daemon is unable to create the sockets and connections it requires to authenticate users. No user is able to authenticate.

401 - Unable to create thread to handle new call

Description: A proxy was unable to accept new connections because of thread resource limitation. Excessive connections to the proxy may cause this condition.

401 - Unable to create UDP socket for writing

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Unable to determine host identity

Description: Rempass is unable to connect to the remote security gateway.

401 - Unable to generate keys

Description: While the secure remote login (SRL) connection negotiation is in progress, the client and server encode the authentication information and send these keys to complete the negotiation. If these keys cannot be encrypted/decrypted, the session is terminated. Ensure that the shared secret and passwords are properly configured.

401 - Unable to get blacklist socket

Description: The notify daemon encountered errors while receiving a response from the blacklist daemon. The IP address is not blacklisted.

401 - Unable to get listening socket port number

Description: An attempt to look up the port number for a listening socket has failed.

401 - Unable to get listening socket port number for close

Description: An attempt to look up the port number for a listening socket failed during a close operation. The socket was closed.

401 - Unable to get SMTP port

Description: SMTP is unable to listen on its port because another process is using this port to listen.

401 - Unable to map /dev/mem

Description: The process was unable to get a memory area to perform encryption.

401 - Unable to open log file

Description: The log file is missing or is corrupt.

401 - Unable to send to oobauth daemon

Description: There was a failure to communicate with the Out of Band Authentication (OOBA) daemon.

401 - Unable to timeout blacklist entry for IP address

Description: The blacklist daemon is unable to remove an IP address from the blacklist. As a result, this IP address continues to be blocked from accessing the security gateway.

401 - Unexpected Telnet state

Description: Telnet gets into an unknown state and the connection is terminated.

401 - Unknown clienttype field

Description: A security gateway service responded to gwcontrol but the response was invalid.

401 - Unknown encr_alg

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

401 - Value for statsdir too long

Description: You may have to specify a shorter value for statsdir.

401 - Vulture service scanning is disabled

Description: The vulture daemon is unable to run because the configuration file is bad.

401 - Write failed on file descriptor

Description: An attempt to write to a socket failed.

401 - Write to daemon failed

Description: An attempt to send a reconfigure event to a security gateway service failed.

402 - Error parsing header line

Description: The hotfix utility encountered a problem while attempting to read the header section of the hotfix control file. Check preceding log messages to determine the cause of the failure.

402 - Error processing module list

Description: The hotfix utility encountered a problem while attempting to process the list of modules from the hotfix control file. Check preceding log messages to determine the cause of the failure.

402 - Error validating header data

Description: The data retrieved from the header section of the hotfix control file indicates that the hotfix is not valid for the system on which it is being installed.

402 - Unable to get host by name

Description: The RSA SecurID server could not be resolved.

402 - Unable to get host name

Description: The SDI library is unable to get the host name of the interface most immediate to the RSA SecurID server.

403 - Cannot read configuration file

Description: Gwcontrol could not open its configuration file for reading. This message comes from many places including bullfrog, isakmpd, VPN, and filter utilities. Each attempt to open a configuration file failed. The name of the file it was looking for should be in the filename parameter.

404 - Error in configuration file (action not specified)

Description: There is an error in the configuration file. The component was unable to process a line in the configuration file. The parameters provide more detail on this error.

404 - Error in configuration file (ARP mask not specified)

Description: Error loading the ARP configuration information.

404 - Error in configuration file (bad ARP address)

Description: Error loading the ARP configuration information.

404 - Error in configuration file (cannot parse as an interface)

Description: The configuration settings for the interfaces are incorrect.

404 - Error in configuration file (invalid address mapping information)

Description: The configuration settings for the interfaces are incorrect.

404 - Error in configuration file (invalid interface address information)

Description: The configuration settings for the interfaces are incorrect, it has an invalid interface address information.

404 - Error in configuration file (invalid range for nbdgramd.low_unnumbered_port - nbdgramd.high_unnumbered_port, so using default range

Description: Check the configuration for port changes.

404 - Error in configuration file (line missing or invalid)

Description: Notification configurations are corrupted. Reconfigure your notifications. If it comes from the HTTP daemon, the named configuration file is corrupt.

404 - Error in configuration file. Invalid range for udp-gsp.low_unnumbered_port - udp_gsp.high_unnumbered_port, so will use default range

Description: An error has occurred in the configuration file. Check the configuration file for port ranges.

404 - Inconsistent user counts

Description: The security gateway is unable to find a valid license because the user counts of the security gateway features do not match.

404 - License does not exist

Description: An attempt was made to configure a functionality that is not licensed.

404 - License requires base feature

Description: The security gateway is unable to find a valid license because the security gateway is not licensed.

404 - The license contains an invalid host ID

Description: The security gateway is unable to find a valid license because the Symantec System ID (host ID) is invalid.

404 - The license contains an invalid version

Description: The security gateway is unable to find a valid license because the version in the license file does not match the security gateway version.

404 - The license has expired

Description: The security gateway is unable to find a valid license because the license has expired.

405 - Re-read of configuration file failed; using previous config file

Description: Gateway control (gwcontrol) or notify daemon, when it finds the configuration file it requires with errors, proceeds with an old configuration file.

407 - Cannot open lock file

Description: The traceroute service is unable to open the lock file.

408 - Entry is not a valid audio file

Description: The audio file supplied is not valid. Audio notifications are not sent.

409 - Sample rate not available

Description: (Sun Solaris only) The audio file has a rate that the audio hardware does not support. Audio notifications will not be sent.

410 - Encoding not available

Description: The notification application cannot use the specified audio file because of its format.

410 - Failed to query network adapter information

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

411 - Unable to locate ACE server host

Description: The SDI library could not contact the ACE server.

411 - Unable to open notify schedule

Description: The notification configurations are corrupt. Delete these configurations and add them again.

412 - Failed to parse module line

Description: The hotfix utility encountered a problem while attempting to read one of the module sections of the hotfix control file. Check previous log messages to determine the cause of the failure.

412 - Unrecognized transport

Description: The notify daemon is unable to send a notification with the specified transport. The transport must be one of the following: Mail, Pager, SNMP, Blacklist (Symantec Gateway Security) or Audio. Check the notification window in the SGMI.

413 - Have configuration file errors but continuing

Description: Gwcontrol determined that the current configuration file has errors. Gwcontrol is ignoring the current configuration file, and continuing with the old configuration.

414 - Cannot determine source IP address. Source IP will not be blacklisted

Description: The notify daemon has detected a condition, which normally would cause the source IP address to be blacklisted, but as the source IP address is not specified, it does not get blacklisted.

414 - Invalid blacklist message (cannot determine source port)

Description: The notify daemon has detected a condition, which normally would cause the source IP address to be blacklisted but as the source ports cannot be determined, it does not get blacklisted.

414 - Invalid blacklist message (cannot determine destination IP address)

Description: The notify daemon has detected a condition, which normally would cause the source IP address to be blacklisted but as the destination IP address cannot be determined, it does not get blacklisted.

414 - Invalid blacklist message (cannot determine destination port)

Description: The notify daemon has detected a condition, which normally would cause the source IP address to be blacklisted, but as the destination port cannot be determined, it does not get blacklisted.

414 - Invalid blacklist message (Cannot determine source or destination IP addresses)

Description: The notify daemon has detected a condition which normally would cause the source IP address to be blacklisted, but as the source or source IP address cannot be determined, it does not get blacklisted.

414 - Invalid blacklist message (Cannot determine password)

Description: The notify daemon has detected a condition which normally would cause the source IP address to be blacklisted, but as the password cannot be determined, it does not get blacklisted.

420 - Unable to send to the ACE server

Description: The SDI library could not send data to the ACE server. The server is down or inaccessible.

421 - Dropping connections because the number of process instances already at configured maximum

Description: The number of process instances is limited for most proxies. This is because the number of concurrent connections for the proxy has reached the configured maximum. This message occurs only once for each proxy per start or stop.

There are several reasons for the appearance of this message. You may not have enough security gateways to handle the number of concurrent connections at your installation, you may be under attack, or your security gateway may have the capacity to handle a larger number of concurrent connections but needs to be configured appropriately.

421 - Unable to create ACE server socket

Description: The SDI library failed to create a socket to talk to the ACE server. Someone is probably already using this socket.

422 - Bad port number range

Description: The proxy was unable to listen on a selected port range.

423 - Bad protocol at line

Description: The protocol was not UDP or TCP.

423 - Node down due to ping monitoring failure

Description: HA/LB is unable to ping a node in the cluster. The node may not be functional. Check the target of the ping, to ensure that it responds.

423 - Node down due to process monitoring failure

Description: The cluster is constantly monitoring other nodes to update the configuration data. In this case, the HA/LB process is unable to monitor the other nodes in the process. Check the list of processes being monitored.

424 - Cannot use TCP ports because it is a reserved port. Set tcp-gsp.allow_reserved_services=TRUE to permit this

Description: TCP GSP is unable to use the TCP port because it is a reserved port.

425 - Cannot lookup service at line

Description: Service is unable to look up the symbolic name service in the etc/services file.

430 - Cannot lookup hostname

Description: The GSP is unable to lookup the host name in the file GSP.cf or the SMTP is unable to lookup the server name.

432 - Bad host name

Description: The host name in the HTTP configuration is invalid. Check the HTTP configuration settings.

433 - Cannot connect to host

Description: The NNTP daemon is unable to contact the remote host.

434 - Error reading file

Description: If this message is from the DNS daemon, it indicates that the DNS daemon couldn't read the hosts file. If this message is from the notify daemon, it indicates that it was unable to open the audio file required for audio notifications.

441 - Parameter error

Description: An illegal parameter value was discovered in the VPN configuration file.

443 - Failed to process module

Description: The hotfix utility encountered a problem while attempting to process the specified module from the hotfix control file. Check preceding log messages to determine the cause of the failure.

445 - Cannot read password file

Description: The remote access service could not open its password file for reading. Reconfigure the machine accounts through the SGMI.

450 - Management failed

Description: An attempt was made to remotely manage service but failed due to an error.

451 - Error expanding file

Description: The hotfix utility encountered a problem while attempting to expand the hotfix or hotfix bundle archive file. Check previous log messages to determine the cause of the failure.

452 - Error closing file

Description: Unable to close the file.

52 - Error copying directory

Description: Unable to copy the directory.

452 - Error creating directory structure

Description: Unable to create the directory structure.

452 - Error removing directory structure

Description: The hotfix utility encountered a problem while attempting to remove a directory structure that is no longer required.

452 - LiveUpdate failed

Description: A LiveUpdate request failed. Check the LiveUpdate settings and verify that your security gateway can access the LiveUpdate servers.

452 - There was an error loading or finding the scan engine virus definitions. All scanning will be disabled

Description: The antivirus engine is unable to locate the virus definitions. Data scanning of files and email will not occur. Check to ensure connectivity to the external network.

452 - Unable to locate resource string (problem with ResourceDictionary.xml)

Description: The daemon was unable to read the resource string required to proceed appropriately. The process will attempt to continue, but at a degraded state.

456 - HTTPS service not supported

Description: Although the HTTP proxy provides support for the HTTPS protocol, it does not support HTTPS when accessing pages on the security gateway. This message is displayed if a request received through HTTPS is for one of the security gateway's own pages.

457 - A host is active with the address assigned to the security gateway

Description: A host on the network is active with same address as that of the security gateway.

457 - A host is active with the address in use for proxy ARP or NAT

Description: A duplicate IP address error. Multiple machines are claiming to have the same IP address. This is a configuration error requiring IP address changes on the security gateway or the conflicting host. For example, an IP address in a NAT pool is starting to be used by another person. Examine the ARP tables. Corrective action must be taken.

457 - Attempt to blacklist firewall interface. Either client transparency is not enabled on the interface, or an active denial-of-service attack is being carried out against the security gateway

Description: This is an attempt to blacklist the security gateway interface. It indicates that either client transparency is not enabled on the interface, or an occurrence of denial-of-service attack against the security gateway.

457 - Attempt to blacklist IP address 127.0.0.1. Either a serious network misconfiguration exists, or a denial-of-service attack is occurring

Description: This is an attempt to blacklist IP address 127.0.0.1. It indicates that either a serious network misconfiguration exists, or an occurrence of denial-of-service attack.

457 - Attempt to blacklist security gateway proxy ARP address. Either client transparency is not enabled on the interface, or an active denial-of-service attack is being carried out against the security gateway

Description: This is an attempt to blacklist security gateway proxy ARP address. It indicates that either client transparency is not enabled on the interface, or an active denial-of-service attack is being carried out against the security gateway.

457 - Bad netmask specification

Description: The netmask specified in the DNS configuration is invalid. Public recursion cannot be enabled.

457 - Bad port number

Description: The configured port number is invalid for this proxy.

457 - Did not find ourselves as a name server for an authoritative zone

Description: The security gateway is listed as the Name Server for any entry in the noauth list.

457 - Fatal gopher error

Description: This is a HTTP protocol error and this connection is aborted.

457 - Incorrect remote management checksum received

Description: Remote access to the security gateway failed. This is caused because of an incorrect password or mismatched versions.

457 - Multiple select failures

Description: The remote user had communication errors.

457 - No domain controller found for domain

Description: (Microsoft Windows only) The process is unable to look up the domain. The domain name is not part of the domain.

457 - NP notification failed authentication

Description: A request to modify the blacklist did not authenticate properly because of a mismatch in the shared passwords. This may indicate improperly configured machine accounts, or less likely, a denial of service attempt.

457 - Only one argument allowed

Description: Do not specify more than one argument.

457 - System active with address

Description: This is a duplicate IP address network configuration error. The indicated IP address is being added to the driver's ARP table as a result of a configuration change to add a NAT pool or Redirect address. But, some host on the LAN already claims the same IP address. The attempt to have the security gateway own the IP address was rejected. Use either a different address or change the address on the host which currently claims the address. Check the ARP tables for problem isolation.

457 - The file cannot be opened as the private hosts file

Description: The DNS daemon could not open the hosts file. The hosts file provides host-to-IP address mapping for systems that are designated as private.

457 - The kernel appliance driver cannot be opened. Check that the installation was successful

Description: The message describes the problem and the necessary corrective action.

457 - The line cannot be parsed as an address or bits

Description: The "subnet_map" does not appear to be valid in the hosts file.

457 - The line has a network address that includes bits not in subnet mask

Description: The “subnet_map” does not appear to be valid in the hosts file.

457 - The line has a subnet mask size out of range (25-31)

Description: The “subnet_map” does not appear to be valid in the hosts file.

457 - The root server must be specified as a name

Description: The root server in the hosts file is invalid. The resource parameter indicates the line number that is erroneous.

457 - The user authenticated without specifying a domain, and it was not possible to discover the user's domain

Description: This is a Microsoft Windows domain authentication error. The user name was not specified correctly. The authentication failed.

457 - This system is not an NT domain member

Description: This is a Microsoft Windows domain authentication error.

457 - Unable to connect

Description: A service was unable to connect to the server.

457 - Unable to load entry

Description: Unable to load the ARP table. Check the configuration settings.

457 - Unable to pass packet to IP

Description: The logservice (or another process) was unable to open a communication channel with the driver. The logservice daemon unable to record kernel log messages. Ensure that the security gateway configuration is set up correctly.

457 - Unauthorized NP notification, incorrect port

Description: A request was received to modify the blacklist but the request was received on an improper port. This could indicate improper configuration of machine accounts, or less likely, a denial of service attempt.

457 - Unauthorized NP notification, no entry in remkeys

Description: An unauthorized request was received to modify the blacklist. This could indicate improper configuration of machine accounts, or less likely, a denial of service attempt.

457 - Unspecified internal server error while connecting

Description: The HTTP daemon server is unable to connect to a remote gopher server.

463 - Failed to get node status

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

465 - Node left the cluster

Description: The node in the cluster has disappeared, either the node has been taken offline or has crashed.

469 - Node down due to NIC card failure

Description: The node is down due to failure of the network interface card (NIC).

471 - Driver log messages at this level suppressed

Description: Due to increased volume, the driver log messages are no longer being logged until conditions improve.

471 - Failed to add ARP block

Description: Failed to add cluster-wide ARP block. Check the size of ARP block, and ensure that it is smaller than the supported max ARP block size.

471 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve, so that log services do not load the CPU.

476 - Failed to install hotfix

Description: The hotfix utility encountered a problem while attempting to install the individual hotfix specified. Check previous log messages to determine the cause of the failure.

476 - Failed to install hotfix bundle

Description: The hotfix utility encountered a problem while attempting to install the hotfix bundle specified. Check preceding log messages to determine which individual hotfix installation failed and the cause of the failure.

476 - Failed to uninstall all hotfixes

Description: The hotfix utility encountered a problem while attempting to uninstall all of the previously installed hotfixes. Check preceding log messages to determine the cause of the failure.

476 - Failed to uninstall hotfix

Description: The hotfix utility encountered a problem while attempting to uninstall the individual hotfix specified. Check preceding log messages to determine the cause of the failure.

476 - Failed to uninstall recent hotfixes

Description: The hotfix utility encountered a problem while attempting to uninstall the hotfixes that were installed with the most recent hotfix bundle. Check preceding log messages to determine the cause of the failure.

490 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.
Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

499 - The scan engine has crashed

Description: The antivirus scan engine has encountered a severe error. It should be restarted automatically. In process scans, it generates additional log messages.

Alert messages (500-599)

Messages in the range 500-599 indicate that a security rule has been triggered, and could potentially be someone attempting to breach the network perimeter.

501 - Access threshold reached

Description: One of the suspicious activity thresholds has been reached. Check which rule has been triggered. Although this message may indicate an attack, it is more likely a common service, like HTTP, getting heavy use.

501 - Repeated

Description: Messages that have occurred multiple times have been consolidated, indicating the possibility of an occurrence of a more serious problem.

502 - Ethernet address mismatch (ARP returns <variable 1>)

Description: When creating a host entity, you have the option of defining the MAC address along with the IP address. Connecting to the security gateway using this host prompts the security gateway to perform both an ARP and reverse ARP (RARP) to ensure that both the IP address and MAC address returned match the configuration. If the MAC address does not match, it could be a misconfiguration, or possibly another host spoofing the address.

502 - Potential denial-of-service (DoS) attack, so blocking IP for at least <variable 1> seconds

Description: The kernel sends this alert.

502 - Reverse address does not match, so denied

Description: The security gateway resolves host names for all connecting IP addresses. As an additional security check, the security gateway performs reverse lookups on host names to ensure that they match their respective IP address. If the returned IP address does not match the original, the connection is dropped.

505 - Unauthorized process killed

Description: The vulture routine found an unauthorized user service running and killed it. Either ignore, if the service was not supposed to be running, or add that service to the vulture.runtime file.

506 - Unauthorized user logged off

Description: The vulture daemon has logged off an unauthorized user. Either ignore, if the user account was not supposed to be running, or add that user name to the vulture.runtime file.

507 - Unauthorized user account disabled

Description: (Microsoft Windows only) A user account that was not found registered with the security gateway was disabled.

508 - The Symantec Client VPN is not installed correctly

Description: The client VPN has not been installed appropriately.

508 - Unauthorized service stopped

Description: The vulture routine found an unauthorized user service running and it terminates it gracefully. Either ignore, if the service was not supposed to be running, or add that service to the vulture.runtime file.

509 - The Symantec Enterprise Firewall is not installed correctly

Description: VPN client was unable to run, as it was not installed appropriately on the security gateway.

510 - Could not refresh kernel routing table cache

Description: The security gateway uses the kernel routing table to find the appropriate router to which to send packets. In this case, the kernel routing table could not be updated.

510 - Kernel routing table cache is not loaded

Description: The security gateway uses the kernel routing table to find the appropriate router to which to send packets. In this case, the kernel routing table could not be loaded.

513 - Saved trace file

Description: This message is logged when the SMTP application (smtpd) saves a trace of a smtpd session in a file.

514 - Unauthorized HTTP protocol response

Description: An illegal protocol was sent back to the HTTP proxy. It did not begin correctly, or arrived on an illegal port.

514 - Unauthorized HTTP protocol response (headers required by rule)

Description: An illegal protocol was sent back to the HTTP proxy. It did not have expected headers in the message.

514 - Unauthorized SMTP protocol

Description: SMTP sends this message when a user attempts an illegal SMTP protocol command.

515 - User attempted to connect to

Description: The user attempts to connect to the security gateway directly and was denied access.

515 - User attempted to connect to port

Description: This message is logged when the security gateway detects an attempt to use its proxies to connect to one of the security gateway's control ports.

515 - User attempted to connect to port. Add httpd.allow_proxy_to_port_<variable 1>=1 to the config.cf file to allow this (not recommended without investigation)

Description: A user attempted to connect to an illegal port. Access was denied.

516 - CPU temperature is high

Description: The temperature of the CPU unit is higher than the satisfactory level.

516 - CPU temperature is low

Description: The temperature of the CPU unit is lower than the satisfactory level.

523 - Incorrect remote management authenticator received

Description: An attempt for remote access has failed to authenticate correctly.

523 - Incorrect remote management challenge received (possible replay attack)

Description: An attempt for remote access has failed to authenticate correctly.

523 - Resource allocation failure (could not allocate port)

Description: The GDP proxy attempts to get a free port for connection and has failed.

568 - Driver packet resources exhausted. Packets dropped. Possible attack or misconfiguration

Description: This can result from an attack against the security gateway or a high-volume security gateway just needs more resources. End-user connectivity is impacted as some messages are being dropped. Check the index for ScaleFactor, and determine if increasing the number of buffers is warranted.

Every 10 minutes, this message repeats if the condition still exists. The count is the number of times the incident occurs, is cumulative, and may be larger than the number of messages that appear in the log file.

571 - Driver log messages at this level suppressed

Description: Due to increased volume, the driver log messages are no longer being logged until conditions improve.

571 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve so that log services do not load the CPU.

572 - The intrusion detection and prevention loadable module is not responding

Description: The intrusion detection and prevention module, which analyzes packets and sends alerts to the Symantec driver is not responding.

For either gated or non-gated mode, the administrator can change the configuration settings so that an alert level log message is generated and the security gateway is not shut down.

590 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.
Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

Critical messages (600-699)

Critical log messages fall into the 600-699. These messages state that the security gateway security is still working, but one or more services have failed.

601 - Child process killed

Description: The security gateway software runs independent processes in the background to free resources required by gwcontrol. One of them has terminated unexpectedly.

601 - Could not get console output handle

Description: Unable to get handle to standard output to write data. This is not a common occurrence.

601 - Exiting because clock could not be adjusted

Description: The NTP daemon is exiting because the clock could not be set. The program will restart, but this issue may remain. To allow the NTP daemon to continue running, identify the problem.

601 - Exiting because key file could not be found

Description: NTP searches for a configuration file and fails to find it. The parameters in the message identify the file.

601 - Exiting because no servers can be used

Description: The process searches for an NTP server and is unable to find it.

601 - Repeated

Description: Messages that have occurred multiple times have been consolidated, indicating the possibility of an occurrence of a more serious problem.

602 - Child process exited

Description: An independent process of the gateway's software returned an unexpected error. Another log message appears, which describes the problem in greater detail.

603 - CreateThread failed

Description: The VPN server was unable to start as the number of threads was exceeded.

603 - CreateThread failed for dispatcher consumer

Description: This is the case of a licence issue. You can access the Symantec licensing and registration site at www.symantec.com/certificate to obtain a license file.

603 - CreateThread failed for engine login

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

603 - CreateThread failed for peer recovery

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

603 - Fork failed

Description: One of the security gateway's services attempts to fork but fails. The system may have run out of swap space or available processes. Power cycling is necessary to release system resources.

604 - Failed to install configuration

Description: The process attempts to synchronize the configuration across the cluster, but fails to install the configuration.

604 - User count limit exceeded

Description: The license limit has been reached. You may need to acquire more licenses or release some accounts.

605 - Cannot execute

Description: The component was unable to run a user script. The log message identifies the component. Execute the script from the command-line to check if the script is valid.

If this message is sent by the secure remote login (SRL) daemon, it indicates that the user was attempting to logon at the shell prompt, and the execution of the login script failed. Delete and add this to the user again.

If this message is sent by the notify daemon, it indicates that it was unable to execute a pager, mail or client program. Check the configuration parameters for these notifications.

605 - Cannot execute (child limit reached)

Description: The notify daemon has reached the limit on the number of client programs that the security gateway can start. This notification is not sent to the client program.

606 - Failed to notify transport

Description: The notify daemon failed to send a message using the transport.

606 - Failed to send notification

Description: The notify daemon was unable to send a notification for the log message because either the message is corrupted or the transport failed (in which case there should be additional messages with details prior to this message).

607 - Daemon exited on signal

Description: A security gateway server application exited because of a software signal.

608 - Daemon exiting because the blacklist port cannot be bound to

Description: Blacklist daemon is unable to listen to a blacklist address request because the blacklist port cannot be bound to it.

608 - Daemon exiting because a socket for the blacklist port cannot be created

Description: Blacklist daemon is unable to listen to a blacklist address request because a socket for the blacklist port cannot be created.

608 - Daemon exiting because the blacklist port cannot be opened

Description: Blacklist daemon is unable to listen to a blacklist address request because the blacklist port cannot be opened.

610 - Cannot bind socket to UDP port

Description: The DNS daemon is unable to establish a connection on a UDP port, so it terminates. Check if some other process is running on port 53.

610 - Cannot find Entrust .epf file

Description: The VPN server will terminate as it is unable to find the Entrust .epf file. If this message is from Libauth, it signifies that the authentication failed.

610 - Cannot find Entrust .ini file

Description: The VPN server will terminate as it is unable to find the Entrust .ini file.

610 - Cannot find Entrust configuration file

Description: The authentication configuration file is not available.

610 - Cannot initialize configuration file read lock

Description: The process attempts to read its configuration file and is unable to get exclusive rights, so it terminates.

610 - Cannot initialize database lock

Description: VPN server was unable to read the tunnel configuration data so it will terminate.

610 - Cannot initialize filter cleanup mutex

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot initialize filter mapping mutex

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot initialize node list mutex

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot initialize shared key file index mutex

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot initialize tunnel database

Description: VPN server was unable to read the tunnel configuration data so it will terminate.

610 - Cannot store ISAKMP security association reference based on cookies

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot store ISAKMP security association reference based on peer context

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot store new tunnel ID

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Cannot use default password for .epf file

Description: The VPN server is terminating as it is unable to use the default password for the .epf file.

610 - Could not find a usable winsock.dll

Description: (Microsoft Windows only) The process was unable to communicate through TCP/IP because it was not configured on the security gateway.

610 - Daemon is exiting

Description: Individual proxy services are exiting normally.

610 - Daemonize failed

Description: An attempt to appropriately initialize the security gateway service failed. The service may not run properly.

610 - Error executing

Description: An attempt to execute a process failed. This results in a failure to start or restart a security gateway process.

610 - Failed

Description: This is a general error notification, and the corrective measure usually depends on what has failed. You should monitor the rate of occurrence of this message.

610 - Failed to generate a new tunnel ID

Description: This message indicates an internal software error. Please contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report this.

610 - Failed to get a license

Description: The security gateway is unable to find a valid license.

610 - Failed to get a list of interfaces

Description: The server is unable to get a list of security gateway interfaces and IP addresses, so it is terminating.

610 - Failed to load required library

Description: A process was unable to load the specified library file, which is required to process log messages and display strings. The library should reside in:

/lib (UNIX)

\raptor\firewall\bin (Microsoft Windows).

610 - Invalid version format (expected major.minor)

Description: The VPN server configuration version is incorrect.

610 - Maximum queuing memory exceeded

Description: The end-users face the impact of this problem, and remedial action is indicated.

An attempt to add too many items to a driver queue resulted in lost packets. There are four different queues that can generate this message: forwarding, encryption, fragmentation, and side door. The exact text of the message is required, to determine which queue was exhausted.

Either an attack or high load can generate this event. If the event is the result of high load, you can increase the maximum queue. The default size is 4194304 bytes or 4 MB. To increase the value, add the following system parameter: driver.global.Max_User_Queue_Memory. Enter the value 8388608 for 8 MB. If the If you enter a high value, you will exhaust the kernel memory, resulting in a crash.

This message repeats every 10 minutes if the incident continues to occur. The count is the number of times the incident occurs, and may be larger than the number of messages. The count is cumulative.

610 - No colon in version string

Description: The VPN server configuration version is incorrect.

610 - No ‘V’ in version string

Description: The VPN server configuration version is incorrect.

610 - Number of interfaces greater than allowed

Description: The number of interfaces allowed is 256, and this number has been exceeded.

610 - Out of memory

Description: The system is out of memory, if possible, add more memory or run fewer programs.

610 - Shutting down

Description: The DNS daemon is shutting down as it has problems with the connection.

610 - Socket failed

Description: A connection could not be established, and the NTP daemon is shutting down.

610 - The security gateway is dropping packets because a driver queue has exceeded the maximum queueing memory

Description: An attempt to add too many items to a driver queue resulted in lost packets. There are four different queues that can generate this message: forwarding, encryption, fragmentation, and side door. The text of the message identifies the queue that was exhausted.

Either an attack or high load can generate this message. If this message is due to high load, you can increase the maximum queue size. The default value is 4194304 or 4 MB. To increase the value, add the following system parameter: driver.global.Max_User_Queue_Memory. Set the value to 8388608 (8 MB). Do not make this value too high, or you can exhaust the kernel memory, resulting in a crash.

If the incident continues to occur, this message reappears every ten minutes. The count is the number of times the incident occurs and may be larger than the number of messages that appear in the log file. The count is cumulative.

610 - Too many errors from select

Description: There were too many errors while trying to communicate with the TACACS+ server. The daemon is exiting.

610 - Unable to decrypt Entrust user password

Description: An attempt to decrypt the user's password failed because the password is invalid. The user failed the authentication.

610 - Unable to find list of listening ports

Description: The HTTP daemon is unable to find the list of ports in its configuration settings, which it uses to listen.

610 - Unable to open event

Description: (Microsoft Windows only) The process was unable to establish internal thread communication with eaglesvc, and therefore, is terminating.

610 - Unable to open shutdown event

Description: (Microsoft Windows only) The process was unable to establish internal thread communication with eaglesvc, and therefore, is terminating.

611 - User count limit reached

Description: An external client accessing a server on the protected network or an internal client accessing an external server was denied access because the license limit has been reached. If the security gateway has not been properly configured, you may reach the license limit, and be denied access. Failure to mark at least one network interface as internal resulting in all IP addresses using the security gateway to be counted towards the license limit.

612 - Exiting because packet buffer reuse failed (memory problem)

Description: GDP was unable to set the memory, hence it is terminated.

612 - Unable to get more disk space to continue logging

Description: The disk space has been exhausted. The gateway is shutdown if it is running (you can change this). You may need to release some disk space to continue logging (for example, by removing existing logs or changing the configuration for the logger to decrease the minimum disk space).

616 - CPU temperature too high

Description: The temperature of the CPU unit is higher than the satisfactory level.

616 - CPU temperature too low

Description: The temperature of the CPU unit is lower than the satisfactory level.

621 - Dropping connections because virtual memory is exhausted

Description: The process is unable to obtain additional memory for establishing connections.

621 - Failed connect to local security gateway

Description: Tomcat servlets are dead. Reboot the box, ensure that local connection is possible.

621 - Failed connect to remote security gateway

Description: Ensure that all necessary nodes in the cluster are up and running.

630 - Kernel memory purge will cause lost packets

Description: (Microsoft Windows only) The driver tracks memory allocation within itself. The driver is not permitted to exceed Max_Memory usage. When memory allocation reaches Max_Memory, a memory purge is executed to free memory. The end-users may notice an error at this time.

630 - The packet array size is too big

Description: (Microsoft Windows only) The TCP/IP protocol is attempting to send more than 16 packets at the same time. The request was rejected.

632 - No cluster account

Description: Unable to find a cluster account. You can try deleting the cluster, disabling HA/LB, and enabling it again to create the cluster account.

650 - An aberrant counter incremented

Description: Contact Technical Support by phone or online at http://www.symantec.com/techsupp/ to report the exact text of this message. This message was not in the original released product, but may have been inserted as the result of a hotfix.

This message repeats every 10 minutes, if the condition still exists. The count is the number of times the incident occurs, is cumulative, and may be larger than the number of messages that appear in the log file.

651 - Failed to retrieve configuration

Description: The process attempts to synchronize the configuration across the cluster but fails to retrieve the configuration.

654 - No local active configuration

Description: In this state, no local active configuration exists. Rebuild the cluster, test the local connection.

671 - Driver log messages at this level suppressed

Description: Due to increased volume, information log messages are no longer logged until conditions improve so that log services do not overload the CPU. This lets you allocate CPU cycles to continue providing user services while not logging the incoming connections.

671 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve, so that log services do not overload the CPU. This lets you allocate CPU cycles to providing user services and not to logging the incoming connections.

672 - Shutting down the security gateway because the intrusion detection and prevention loadable module is not responding

Description: The security gateway is shut down but management connections are allowed. The IDS/IPS component may not be responding because of improper loading, no buffer space, user daemon not running or some other internal error.

For either gated or non-gated mode, the administrator can change the configuration settings so that an alert level log message is generated and the security gateway is not shut down.

679 - Kernel memory usage exceeding 75 percent of maximum memory limit

Description: The driver tracks memory allocation within itself. When memory allocation exceeds 75 percent of the maximum limit, this message is issued once. When the amount of memory allocated falls below 50 percent and then exceeds 75 percent, this message is issued again.

The vpn stats global/Max_Memory command indicates the maximum memory allowed. The vpn stats global/Current_Memory command indicates the current amount of memory allocated by the driver. The vpn stats memory command gives a subsystem the breakdown of memory allocation.

The security gateway could either be under an attack or there could be a memory leak. You could increase the maximum memory limit or a reboot may be required. Remedial action is highly recommended.

690 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.
Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

690 - Remote security gateway not trusted (certificate does not match)

Description: Attempts to synchronize the configuration across the cluster results in failed authentication.

Emergency messages (700-799)

Log messages in the range 700-799 indicate an emergency; gwcontrol has failed and the system will no longer allow traffic through. Security is ensured by shutting down all network traffic through the security gateway.

701 - Cannot allocate memory

Description: Memory could not be allocated to perform the requested function.

701 - Could not create temporary directory

Description: The eaglepath process was unable to locate or access the temporary directory.

701 - Failed to extract environment variable for temporary directory

Description: The eaglepath process was unable to locate or access the temporary directory.

701 - Failed to get attributes for temporary directory

Description: The eaglepath process was unable to locate or access the temporary directory.

701 - Repeated

Description: Messages that have occurred multiple times have been consolidated, indicating a possibility of the occurrence of a more serious problem.

701 - Quitting because of unrecoverable errors while communicating with the driver

Description: The process terminated while communicating with the driver because of unrecoverable errors.

701 - Quitting because the driver could not be opened

Description: The process terminated because the driver could not be opened.

701 - Temporary directory does not exist

Description: The eaglepath process was unable to locate or access the temporary directory.

701 - The name used for the temporary directory exists, but it is not a directory

Description: The eaglepath process was unable to locate or access the temporary directory.

702 - Quitting because of configuration errors

Description: This message is generated by gwcontrol (the security gateway control daemon) after reconfiguration or a system power cycle. It indicates that one or more control files contain invalid data. This could be caused by file corruption following a system outage, but more commonly is due to illegal addresses entered for host entities.

702 - Quitting because of configuration errors (gwcontrol not running)

Description: This program requires the security gateway gwcontrol module to be installed and running.

707 - Program <variable 1> is not installed

Description: This program requires the security gateway driver to be installed and running.

708 - Quitting because the configuration file is corrupt (setup must be run)

Description: This message is generated by gwcontrol (the security gateway control daemon) or the notify daemon after reconfiguration or after system boot. It indicates that one or more of the security gateway control files contains invalid data. File system corruption following a system outage can cause this, or more commonly, illicit IP addresses entered for host entities.

771 - Driver log messages at this level suppressed

Description: Due to increased volume, the driver log messages are no longer being logged until conditions improve, so that log services do not overload the CPU. This lets you allocate CPU cycles to providing user services and not to logging the incoming connections.

771 - Temporarily suppressing messages because the security gateway has reached log limits for driver messages at this level

Description: Due to increased volume, information log messages are no longer logged until conditions improve, so that log services do not overload the CPU. This lets you allocate CPU cycles to providing user services and not to logging the incoming connections.

790 - Intrusion Event detected

Description: An intrusion event is detected and all suspicious packets from the rogue host are dropped. The log message provides information on the type of intrusion event and includes parameters that elaborate on the event. One of these parameters is a hyperlink that provides more information on the event. The parameters are listed below:

Policy Tag	A string identifying the type of event.
Vendor	This is currently Symantec.
Class	Currently all trackable events are of one sensor class “sniffer.”
Family	The family to which the event belongs.

The Legal Values are listed below:

“integrity”	Indicates a protocol anomaly event.
“availability”	Indicates a counter alert event.
“notice”	Indicates a trackable event.
Context data	Context specific data about the connection event.
Context description	Textual description of the data, a given state machine adds to the context data buffer.
Flow Cookie	A string that pseudo uniquely identifies the network flow where the event occurs. This is a conglomerate of the protocol, IPs and ports on both ends of the connection.
IP Protocol	The transport layer protocol on which the event was detected.
Level	A number between 0 and 255, which represents how severe the event is.
Reliability	A number between 0 and 255, which represents how reliable the event is.
Payload	The exact snippet of data that generated the event. This may be empty for some alerts.
Payload offset	The number of bytes into the payload data when the alerting pattern starts. This value is zero-indexed and is left/right inclusive.
Start time	The starting time of the event.
End time	The end time of the event.
Source IP	The source IP address of the attack. This is also used when blacklist notifications are configured.
Source Port	The level four network of the source of the attack traffic.
Destination IP	The destination IP address of the attack.
Destination Port	The level four network of the destination of the attack traffic.
Packet	The whole or partial IP packet triggering the event.
Interface	The string identifying the device, on which the packet was captured.
Source MAC	The source Ethernet address of the offending packet.
Destination MAC	The destination Ethernet address of the offending packet.
VLAN ID	The virtual local area network (VLAN) ID from the Ethernet header of the offending packet.
Outcome	Currently set to unknown

Appendix B

IDS events

This chapter includes the following topics:

About IDS/IPS events and descriptions

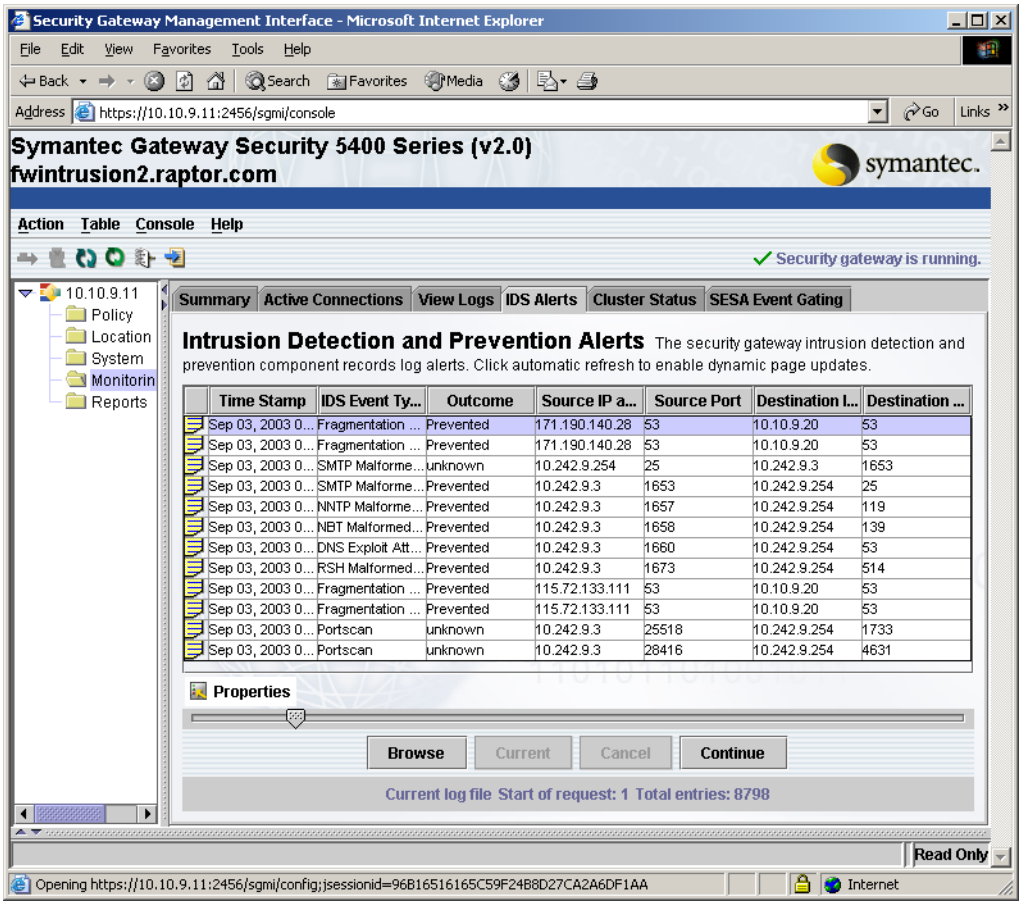
This appendix provides a complete description of all available events that the intrusion detection and prevention (IDS/IPS) component produces. This appendix explains how to view IDS alerts, and lists each event in alphabetical order for easy lookup. Full descriptions for each event follow the alphabetical table, and are categorized by IDS/IPS event type.

Note: The IDS/IPS component is a feature of the Symantec Gateway Security 5400 Series appliances only. It is not available in the software-based versions of the security gateway.

Viewing alerts

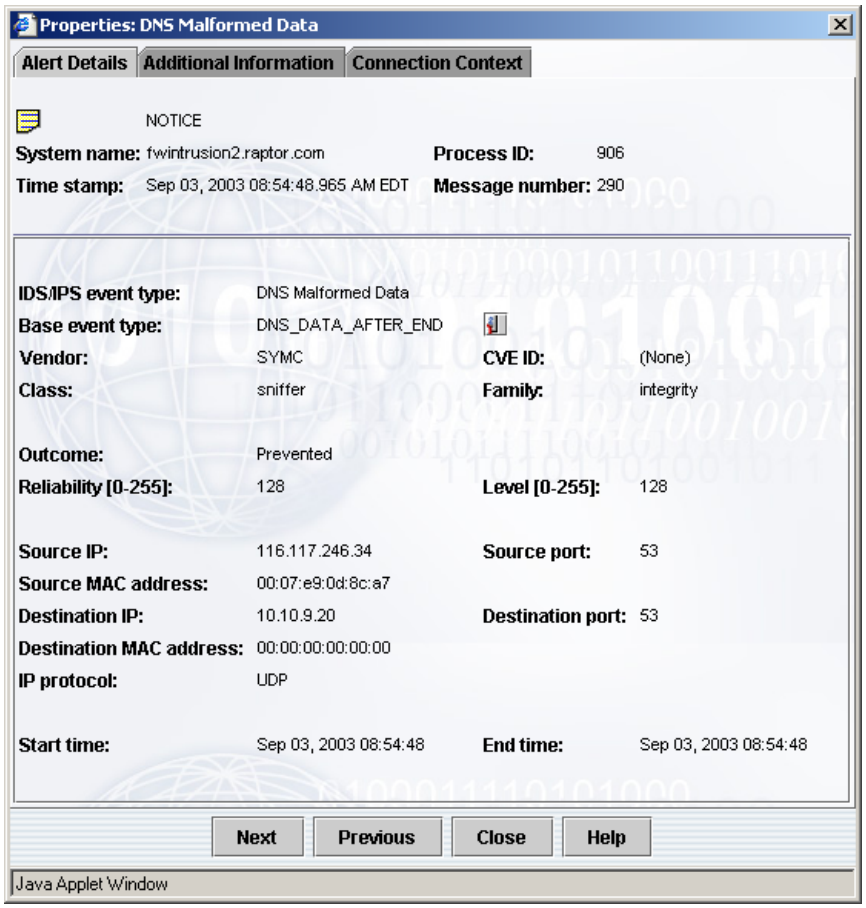
When licensed, the IDS/IPS component examines all incoming packets, looking for anomalies. All detected events are immediately logged. You can view these events (if any) through the Security Gateway Management Interface (SGMI), in the Monitoring window, on the IDS alerts tab. Figure B-1 shows an example IDS Alerts view.

Figure B-1 IDS Alerts window



Highlighting an event, and clicking **Properties** calls up that event's properties window. Figure B-2 shows an example of a properties window for a DNS Malformed Data event.

Figure B-2 DNS malformed data properties window



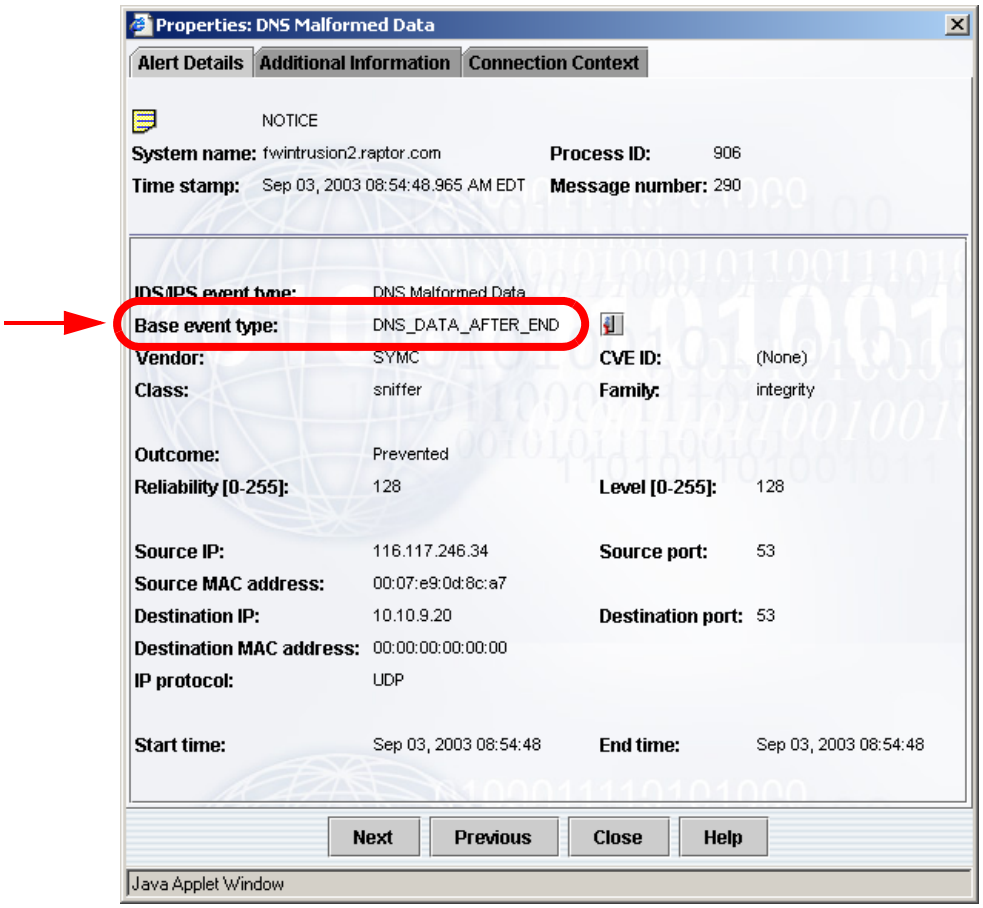
IDS/IPS event types

All security gateway IDS/IPS events are sorted into general categories, called IDS/IPS event types. An IDS/IPS event type is a short description that serves as a summarization of the type of event. IDS/IPS can apply to more than one reported event, and are not necessarily unique. For example, there may be more than one type of event classified as a DNS Malformed Data event, depending on the checks performed by the IDS/IPS component.

Base event types

To help separate and uniquely identify IDS/IPS events, each event is also assigned a unique base event type value. This is shown circled in Figure B-3.

Figure B-3 DNS malformed data event



Use the base event type with Table B-1 to quickly find the page on which the description for this event appears.

Table B-1 Alphabetical listing of base events types and their associated page

Base Event	Page
BFTP_SITE_CHOWN_BUFFER_OVERFLOW	303
BGP_AUTH_FAILURE	364
BGP_BAD_ATTRIBUTE_FLAGS	364
BGP_BAD_KEEPALIVE_MSG_LENGTH	365
BGP_BAD_MARKER	365
BGP_BAD_MSG_LENGTH	365
BGP_BAD_NOTIFICATION_MSG_LENGTH	366
BGP_BAD_OPEN_MSG_LENGTH	366
BGP_BAD_ROUTE_REFRESH_LENGTH	367
BGP_BAD_UPDATE_MSG_LENGTH	367

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
BGP_BAD_WITHDRAWN_ROUTE_LENGTH	368
BGP_GENERIC_ERROR_CONDITION	364
BGP_INVALID_HOLD_TIME	365
BGP_NONAUTH_CONNECTION	368
BGP_OPEN_CAPABILITY_LENGTH_MISMATCH	365
BGP_OPEN_INVALID_CAPABILITY_LENGTH	364
BGP_OVERLONG_OPT_PARAMS	368
BGP_PATH_ATTRIBUTE_BAD_LENGTH	367
BGP_UNKNOWN_MSG_TYPE	367
BGP_UNSUPPORTED_VERSION_NUM	368
BGP_UPDATE_AGGREGATOR_BAD_LENGTH	364
BGP_UPDATE_ASPATH_BAD_LENGTH	364
BGP_UPDATE_ASPATH_BAD_PATHSEGLEN	367
BGP_UPDATE_ASPATH_BAD_PATHSEGTYPE	367
BGP_UPDATE_COMMUNITIES_BAD_LENGTH	365
BGP_UPDATE_LOCAL_PREF_BAD_LENGTH	365
BGP_UPDATE_MULTI_EXIT_DISC_BAD_LENGTH	366
BGP_UPDATE_NETWORK_REACH_BAD_LENGTH	366
BGP_UPDATE_NEXT_HOP_BAD_LENGTH	366
BGP_UPDATE_ORIGIN_BAD_LENGTH	366
BGP_UPDATE_ORIGIN_INVALID_VALUE	366
BGP_UPDATE_ORIGINATOR_ID_BAD_LENGTH	367
BGP_UPDATE_NEG_LOCAL_PREF	368
BGP_UPDATE_NEG_MULTI_EXIT_DISC	368
CODERED_WORM	304
COUNTER_BAD_SERVICES_DOS	296
COUNTER_ICMP_HIGH	298
COUNTER_ICMP_UDPUNREACHABLE_HIGH	301
COUNTER_IPFRAG_HIGH	299
COUNTER_TCP_PORTSCAN	356
COUNTER_TCP_PORTSWEEP	357
COUNTER_UDP_HIGH	301
COUNTER_UDP_PORTSCAN	357
COUNTER_UDP_PORTSWEEP	357
COUNTER_UNACKED_SYNS_HIGH	300

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
COUNTER_UNKPROTO_HIGH	302
DNS_BAD_COMPRESSION	305
DNS_BAD_LABEL_LENGTH	305
DNS_BIND_HESIOD	354
DNS_DATA_AFTER_END	369
DNS_INVALID_ADDRLEN	369
DNS_INVALID_TTL	369
DNS_IQUERY	306
DNS_LONG_NAME	306
DNS_LONG_NXT_RDLEN	306
DNS_PACKET_OVERRUN	369
DNS_RUNT_PACKET	370
FINGER_BAD_REQUEST	370
FINGER_CDK_BACKDOOR	307
FINGER_CMD_ROOTSH_BACKDOOR	307
FINGER_EXCESS_DATA	371
FINGER_FORWARDING_ATTEMPT	296
FINGER_ILLEGAL_METACHAR	307
FINGER_ONLYNUMERIC_REQUEST	354
FINGER_ROOT_REQUEST	354
FINGER_SEARCH_REQUEST	355
FORMMAIL_COMMAND_EXEC	359
FTP_BAD_PORT_CMD_ARG	371
FTP_BAD_PORT_CMD_IPNUM	372
FTP_BAD_RANDOM_COMMAND	372
FTP_BOUNCE_ATTACK	308
FTP_CREATEDIRECTORY_BO	309
FTP_CWD_ROOT	310
FTP_INVALID_UTF8	372
FTP_INVALID_UTF8_HIGH_ASCII	371
FTP_LONG_COMMAND	373
FTP_PORT_CMD_TOO_MANY_ARGS	373
FTP_REPLYDIRNAME_BO	312
FTP_RNTO_WITHOUT_RNFR	373
FTP_TOO_MANY_GLOBS	311

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
FTP_UNRECOGNIZED_COMMAND	373
FTP_WARFTPD_MACROS	352
FTPCLI_ADMHACK_SCAN	355
FTPCLI_BUFFER_OVERFLOW	308
FTPCLI_EXPECTED_ALLORESP	374
FTPCLI_EXPECTED_CRLF	374
FTPCLI_EXPECTED_LF	374
FTPCLI_EXPECTED_RNTO	375
FTPCLI_ISS_SCAN	355
FTPCLI_LITERAL_FILE_ACCESS	313
FTPCLI_NOOP_BUFFER_OVERFLOW	308
FTPCLI_RETR_PASSWD	355
FTPCLI_RETR_USE_COMPRESS_PROGRAM	310
FTPCLI_SAINT_SCAN	356
FTPCLI_SATAN_SCAN	356
FTPCLI_SENT_CEL_COMMAND	375
FTPCLI_SITE_EXEC	310
FTPCLI_SITE_NEWER	313
FTPCLI_USER_BIN	307
FTPCLI_USER_WAREZ	308
FTPSER_AUDIOGALAXY_EXTRA_AFTER_IP	375
FTPSER_BUFFER_OVERFLOW	309
FTPSER_EXPECTED_LF	375
FTPSER_NOOP_BUFFER_OVERFLOW	309
FTPSER_NOT_LOGGED_IN	371
FTPSER_TROJAN_DEEPTHROAT	304
FTPSER_UNKNOWN_RESPONSE_FROMUNKNOWN	376
HSRP_BAD_TTL	377
HSRP_COUP	376
HSRP_HOLDTIME_GT_HELLOTIME	376
HSRP_INVALID_OPCODE	377
HSRP_INVALID_STATE	377
HSRP_INVALID_VERNUM	377
HSRP_NONACTIVE_RESIGN	377
HSRP_NONAUTH_CONNECTION	377

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
HSRP_OVERLONG_PACKET	376
HSRP_WRONG_STATE_FOR_SPEAKING	376
HTGREP_CGI_FILE_ACCESS	359
HTTP_BAD_CHUNKED_HEX	385
HTTP_BAD_CONTENT_LENGTH	383
HTTP_BAD_CONTENT_RANGE	383
HTTP_BAD_ESCAPE_SEQUENCE	303
HTTP_BAD_REQURL5_HIGH_ASCII	380
HTTP_BAD_MSGHDR_TEXT	383
HTTP_BAD_REQ_MSGHDR	384
HTTP_BAD_REQUEST	386
HTTP_BAD_REQURL0	386
HTTP_BAD_REQURL1	386
HTTP_BAD_REQURL2	386
HTTP_BAD_REQURL3	387
HTTP_BAD_REQURL4	387
HTTP_BAD_REQURL5	387
HTTP_BAD_REQURL6_0	387
HTTP_BAD_RESP_BYTE_UNIT	384
HTTP_BAD_RESP_MSGHDR	384
HTTP_BAD_STATUSTEXT	384
HTTP_BAT_FILE_PIPE	319
HTTP_BIZDB_CGI_EXPLOIT	315
HTTP_BODY_SIG0	341
HTTP_BODY_SIG1	321
HTTP_BODY_SIG2	327
HTTP_BODY_SIG3	324
HTTP_CAMPAS_ACCESS	379
HTTP_CFCACHE_MAP_ACCESS	379
HTTP_CMD_FILE_PIPE	390
HTTP_COMPUTRACE_ACTIVE	380
HTTP_DOT_DOT	378
HTTP_EARLY_UTF8_END	306
HTTP_ETC_PASSWD_ACCESS	378
HTTP_FAXSURVEY_ACCESS	370

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
HTTP_FILEEXISTS_CFM_ACCESS	380
HTTP_FPCOUNT_EXPLOIT	319
HTTP_FRONTPAGE_ADMIN_PROBE	380
HTTP_HTACCESS_PROBE	378
HTTP_HTMLSCRIPT_ACCESS	379
HTTP_HTSEARCH_FILE_ACCESS	381
HTTP_IIS_CHUNK_ENCODING_BOF	315
HTTP_IIS_CMDEXECUTION_ACCESS	316
HTTP_IIS_DATA_ACCESS	314
HTTP_IIS_OBTAIN_CODE	383
HTTP_JJ_CGI_EXPLOIT	317
HTTP_LONG_HOST_NAME	317
HTTP_MDAC_COMPONENT_QUERY	318
HTTP_MDAC_QUERY	360
HTTP_MISSING_HOST	385
HTTP_NEWDSN_EXE_ACCESS	382
HTTP_NEWLINES_IN_REQUEST_PATH	388
HTTP_NO_CRLF_AFTER_CHUNK	385
HTTP_NULL_ENCODE	378
HTTP_REQMSGHDR_SIG0	321
HTTP_REQMSGHDR_SIG1	353
HTTP_RESPMSGHDR_SIG0	321
HTTP_RESPMSGHDR_SIG1	302
HTTP_SHOWCODE_ASP_ACCESS	382
HTTP_SOURCEWINDOW_CFM	388
HTTP_TILDE_ACCESS	388
HTTP_UNKNOWN_STATUS	385
HTTP_URL_DIRECTORY_TRAVERSAL	389
HTTP_URL_OVERLONG_DOT	303
HTTP_URL_SIG0	320
HTTP_URL_SIG1	341
HTTP_URL_SIG2	326
HTTP_URL_SIG3	326
HTTP_URL_SIG4	331
HTTP_URL_SIG5	305

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
HTTP_URL_SIG6	351
HTTP_URL_SIG7	332
HTTP_URL_SIG8	326
HTTP_URL_SIG9	314
HTTP_URL_SIG10	333
HTTP_URL_SIG11	316
HTTP_URL_SIG12	352
HTTP_URL_SIG13	324
HTTP_URL_SIG14	304
HTTP_URL_SIG15	325
HTTP_URL_WPARG	327
HTTP_UTF8_LONG_CHAR	332
HTTP_VIEW_SOURCE_ACCESS	388
ICMP_UNREACH_RUNT	300
IDENT_BAD_ERROR	390
IDENT_BAD_OSNAME	390
IDENT_BAD_PORTNUMBERS	391
IDENT_BAD_REQUEST	391
IDENT_BAD_RESPONSE	391
IDENT_BAD_USERNAME	391
IDENT_BUFFER_OVERFLOW	392
IDENT_DATA_PAST_CLOSE	392
IDENT_DATA_PAST_REQUEST	392
IMAP_AUTH_BUFFOVERFLOW	319
IMAP_AUTH_TYPE_BOF	320
IMAP_CLI_ENCRYPTED_OR_INVALID_AUTH_OR_BASE64	392
IMAP_CLI_INVALID_ASTRING_CRLF	392
IMAP_CLI_INVALID_AUTH	393
IMAP_CLI_INVALID_AUTH_TYPE	393
IMAP_CLI_INVALID_COMMAND_AUTH	393
IMAP_CLI_INVALID_COMMAND_NONAUTH	393
IMAP_CLI_INVALID_COMMAND_SELECT	393
IMAP_CLI_INVALID_LIST_MAILBOX_COMMAND	393
IMAP_CLI_INVALID_SELECT	393
IMAP_CLI_INVALID_UNKNOWN	393

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
IMAP_CLI_INVALID_USERID	393
IMAP_CLI_USERID_QUOTED_TOO_LONG	320
IMAP_CLI_USERID_TOO_LONG	320
IMAP_EXPECTED_CRLF	394
IMAP_EXPECTED_LF	394
IMAP_EXPECTED_LTPAREN	394
IMAP_EXPECTED_TXT_CHAR_RTBRACKET_SPACE	394
IMAP_FAILED_LOGIN	392
IMAP_INVALID_2ASTRING_TRANS	394
IMAP_INVALID_ALL_SMART	394
IMAP_INVALID_APPEND	394
IMAP_INVALID_ASTRING_LIST	394
IMAP_INVALID_ASTRINGS_TRANS	394
IMAP_INVALID_CAPABILITY	395
IMAP_INVALID_CHAR8	395
IMAP_INVALID_ENV_BCC	395
IMAP_INVALID_ENV_CC	395
IMAP_INVALID_ENV_DATE_SUBJ	395
IMAP_INVALID_ENV_FROM	395
IMAP_INVALID_ENV_INREPLYTO	395
IMAP_INVALID_ENV_MESGID	395
IMAP_INVALID_ENV_REPLY_TO	395
IMAP_INVALID_ENV_SENDER	395
IMAP_INVALID_ENV_TO	396
IMAP_INVALID_FETCH	396
IMAP_INVALID_FLAGLIST	396
IMAP_INVALID_FLAGS	396
IMAP_INVALID_LIST_MAILBOX_COMMAND	396
IMAP_INVALID_LITERAL	396
IMAP_INVALID_MAILBOXLIST	396
IMAP_INVALID_MAILBOX_MAILBOX	396
IMAP_INVALID_MIME2_B_ENCODED_TEXT	396
IMAP_INVALID_MIME2_ENCODE	397
IMAP_INVALID_MIME2_Q_ENCODED_TEXT	397
IMAP_INVALID_NADDRESS	397

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
IMAP_INVALID_NAMESPACE	397
IMAP_INVALID_NAMESPACE_EXT	397
IMAP_INVALID_NSTRING_LIST	397
IMAP_INVALID_NZNUMBERS	397
IMAP_INVALID_PARTIAL	397
IMAP_INVALID_QUOTA_LIST	397
IMAP_INVALID_QUOTA_TR	397
IMAP_INVALID_QUOTED	398
IMAP_INVALID_QUOTED_USERID	398
IMAP_INVALID_RESP_CODE	398
IMAP_INVALID_RESP_TXT	398
IMAP_INVALID_RESP_TXT2	398
IMAP_INVALID_RESP_TXT_CODE	398
IMAP_INVALID_SEARCH	398
IMAP_INVALID_SEARCH_DATE	398
IMAP_INVALID_SEARCH_MISMATCHED_PAREN	398
IMAP_INVALID_SEARCH_SET	399
IMAP_INVALID_SECTION	399
IMAP_INVALID_SER_FLAGLIST	399
IMAP_INVALID_SER_MESG_ATTRIB	399
IMAP_INVALID_SET	399
IMAP_INVALID_SETQUOTA_LIST	399
IMAP_INVALID_SETQUOTA_PR	399
IMAP_INVALID_SPACE_TRANSITION	399
IMAP_INVALID_STATUS_ATTRB_NUM	399
IMAP_INVALID_STAT_ATTRB_NUM_PRS	399
IMAP_INVALID_STATUS_ATTRIBS	400
IMAP_INVALID_STORE_ATTRIBS	400
IMAP_INVALID_S_ASTRING_TRANS	400
IMAP_INVALID_S_MAILBOX_TRANS	400
IMAP_INVALID_STRING_LIST	400
IMAP_INVALID_TXT	400
IMAP_INVALID_URL	400
IMAP_INVALID_USERID_LITERAL	400
IMAP_MAILBOX_BOF	320

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
IMAP_SER_INVALID_ANY	400
IMAP_SER_INVALID_GREETING	400
IMAP_SER_INVALID_MSG_ATT	401
IMAP_SER_INVALID_NONAUTH	401
IMAP_SER_INVALID_TAGGED_ANY	401
IMAP_SER_INVALID_UNTAGGED_ANY	401
IMAP_URL_INVALID_LOGIN	401
IMAP_URL_TOO_LONG	320
IMAP_URL_USER_TOO_LONG	320
INFO2WWW_CGI_CMD_EXEC	362
IP_FRAG_NOMATCH	297
IP_FRAG_ODDLENGTH	297
IP_FRAG_OVERDROP1	297
IP_FRAG_OVERDROP2	297
IP_FRAG_OVERDROP3	298
IP_FRAG_TEARDROP	298
IP_HEADERLEN_OVERRUNS_PACKETLEN	299
IP_RUNT_HEADER_LENGTH	300
IP_SRC_DST_SAME_LAND	299
IPOP3_CLIENT_AUTH_ABORTED	447
IRCCLISER_AZACO_WORM	322
IRCCLISER_BAD_AFTER_NICK	401
IRCCLISER_BAD_AFTER_USER	401
IRCCLISER_CLAWFINGER_WORM	322
IRCCLISER_EL15BMP_WORM	323
IRCCLISER_EL15SPY_ANSWER	321
IRCCLISER_EL15SPY_NOTIFICATION	322
IRCCLISER_JOINED_BO_OWNED	322
IRCCLISER_LIFESTAGES_WORM	323
IRCCLISER_LOA_WORM	323
IRCCLISER_LUCKY_WORM	323
IRCCLISER_PR0N_WORM	324
IRCCLISER_SEPTIC_WORM	324
IRCSER_UNKNOWN_AFTERPASS	402
IRCSER_UNKNOWN_INIT	402

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
IRCSERSER_INVALID_CAPAB	402
IRCSERSER_UNKNOWN_AFTERPASS	402
IRCSERSER_UNKNOWN_AFTERPASSCAPABS	403
LDAP_ASN1_DATALENGTH_IMPOSSIBLE_STATE	403
LDAP_ASN1_DATALENGTH_RIDICULOUS_WIDTH	403
LDAP_ASN1_DATALENGTH_VALUE_TOO_LARGE	404
LDAP_ASN1_DATALENGTH_VALUE_TOO_SMALL	404
LDAP_ASN1_NESTEDSEQUENCE_OVERFLOW	325
LDAP_ASN1_RUNT_SEQUENCE	404
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ADDREQUEST	404
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ATTRIBUTELIST	405
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ATTRIBUTETYPEANDVALUES	405
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ATTRIBUTEVALUEASSERTION	405
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_BINDREQUEST	405
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_BINDRESPONSE	406
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_COMPAREREQUEST	406
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_CONTROL	406
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_EXTENDEDREQUEST	406
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_EXTENDEDRESPONSE	407
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_FILTER	407
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_LDAPMESSAGE	407
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_LDAPRESULT	407
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MATCHINGRULEASSERTION	408
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MODIFICATIONDIRECTIVE	408
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MODIFYDNREQUEST	408
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MODIFYREQUEST	408
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_REFERRAL	409
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ROOT	409
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SASLCREDENTIALS	409
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEARCHREQUEST	409
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEARCHRESULTENTRY	410
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQOFATTRDESC	410
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQUENCEOFCONTROL	410
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQUENCEOFMODIFICATION	410
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQUENCEOFSUBSTRINGS	411

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SETOFATTRIBUTEVALUE	411
LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SUBSTRINGFILTER	411
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ADDREQUEST	411
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ATTRIBUTELIST	412
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ATTRIBUTETYPEANDVALUES	412
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ATTRIBUTEVALUEASSERTION	412
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_BINDREQUEST	412
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_BINDRESPONSE	413
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_COMPAREREQUEST	413
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_CONTROL	413
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_EXTENDEDRESPONSE	413
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_EXTENDEDREQUEST	414
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_FILTER	414
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_LDAPMESSAGE	414
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_LDAPRESULT	414
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MATCHINGRULEASSERTION	415
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MODIFICATIONDIRECTIVE	415
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MODIFYDNREQUEST	415
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MODIFYREQUEST	415
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_REFERRAL	416
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ROOT	416
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SASLCREDENTIALS	416
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEARCHREQUEST	416
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEARCHRESULTENTRY	417
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFATTRIBUTEDESCRIPTION	417
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFCONTROL	417
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFMODIFICATION	417
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFSUBSTRINGS	418
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SETOFATTRIBUTEVALUE	418
LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SUBSTRINGFILTER	418
LDAP_ANS1_UNEXPECTED_DATA_AFTER_SEQUENCE	325
LDAP_ASN1_UNEXPECTED_TYPE_ABANDONREQ_IN_LDAPMESSAGE	418
LDAP_ASN1_UNEXPECTED_TYPE_ADDREQ_IN_LDAPMESSAGE	419
LDAP_ASN1_UNEXPECTED_TYPE_ASSERTIONFILTER_IN_SEARCHREQUEST	419
LDAP_ASN1_UNEXPECTED_TYPE_ASSERTIONFILTER_IN_FILTER	419

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
LDAP_ASN1_UNEXPECTED_TYPE_ATTRDESC_IN_ATTRTYPEANDVALUES	419
LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTEDESC_IN_MATCHINGRULEASSERTION	420
LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTEDESC_IN_SEQOFATTRDESC	420
LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTEDESC_IN_SUBSTRINGFILTER	420
LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTELIST_IN_ATTRIBUTELIST	420
LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTELIST_IN_SEARCHREQUEST	421
LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBVALUE_IN_SETOFATTRIBVALUES	421
LDAP_ASN1_UNEXPECTED_TYPE_ATTRLIST_IN_ADDREQUEST	421
LDAP_ASN1_UNEXPECTED_TYPE_ATTRVALUES_IN_ATTRTYPEANDVALUES	421
LDAP_ASN1_UNEXPECTED_TYPE_AVA_IN_COMPAREREQUEST	422
LDAP_ASN1_UNEXPECTED_TYPE_AVL_IN_SEARCHRESULTENTRY	422
LDAP_ASN1_UNEXPECTED_TYPE_BASEDN_IN_SEARCHREQUEST	422
LDAP_ASN1_UNEXPECTED_TYPE_BINDREQ_IN_LDAPMESSAGE	422
LDAP_ASN1_UNEXPECTED_TYPE_BINDRESP_IN_LDAPMESSAGE	423
LDAP_ASN1_UNEXPECTED_TYPE_BOOLEAN_IN_MATCHINGRULEASSERTION	423
LDAP_ASN1_UNEXPECTED_TYPE_BOOLEAN_IN_MODIFYDNREQUEST	423
LDAP_ASN1_UNEXPECTED_TYPE_BOOLEAN_IN_SEARCHREQUEST	423
LDAP_ASN1_UNEXPECTED_TYPE_COMPAREREQ_IN_LDAPMESSAGE	424
LDAP_ASN1_UNEXPECTED_TYPE_COMPOUNDFILTER_IN_FILTER	424
LDAP_ASN1_UNEXPECTED_TYPE_COMPOUNDFILTER_IN_SEARCHREQUEST	424
LDAP_ASN1_UNEXPECTED_TYPE_CONTROL_IN_SEQUENCEOFCONTROL	424
LDAP_ASN1_UNEXPECTED_TYPE_CONTROLS_IN_LDAPMESSAGE	425
LDAP_ASN1_UNEXPECTED_TYPE_CRITICALITY_IN_CONTROL	425
LDAP_ASN1_UNEXPECTED_TYPE_DELREQ_IN_LDAPMESSAGE	425
LDAP_ASN1_UNEXPECTED_TYPE_ENUM_IN_SEARCHREQUEST	425
LDAP_ASN1_UNEXPECTED_TYPE_EXTENDEDREQ_IN_LDAPMESSAGE	426
LDAP_ASN1_UNEXPECTED_TYPE_EXTENDEDRESP_IN_LDAPMESSAGE	426
LDAP_ASN1_UNEXPECTED_TYPE_EXTREQNAME_IN_EXTENDEDREQUEST	426
LDAP_ASN1_UNEXPECTED_TYPE_EXTREQVALUE_IN_EXTENDEDREQUEST	426
LDAP_ASN1_UNEXPECTED_TYPE_LDAPDN_IN_COMPAREREQUEST	427
LDAP_ASN1_UNEXPECTED_TYPE_LDAPDN_IN_MODIFYDNREQUEST	427
LDAP_ASN1_UNEXPECTED_TYPE_LDAPDN_IN_SEARCHRESULTENTRY	427
LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_ATTRIBUTEVALUEASSERTION	427
LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_BINDRESPONSE	428
LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_CONTROL	428

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_EXTENDEDRESPONSE	428
LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_LDAPRESULT	428
LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_SASLCREDENTIALS	429
LDAP_ASN1_UNEXPECTED_TYPE_LDAPURL_IN_REFERRAL	429
LDAP_ASN1_UNEXPECTED_TYPE_LIMIT_IN_SEARCHREQUEST	429
LDAP_ASN1_UNEXPECTED_TYPE_MATCHINGRULEVALUE_IN_MRASSERTION	429
LDAP_ASN1_UNEXPECTED_TYPE_MESSAGEID_IN_LDAPMESSAGE	430
LDAP_ASN1_UNEXPECTED_TYPE_MODIFICATION_IN_SEQUENCEOFMODIFICATION	430
LDAP_ASN1_UNEXPECTED_TYPE_MODDNREQ_IN_LDAPMESSAGE	430
LDAP_ASN1_UNEXPECTED_TYPE_MODREQ_IN_LDAPMESSAGE	430
LDAP_ASN1_UNEXPECTED_TYPE_MODSEQUENCE_IN_MODIFYREQUEST	431
LDAP_ASN1_UNEXPECTED_TYPE_MODTYPE_IN_MODDIRECTIVE	431
LDAP_ASN1_UNEXPECTED_TYPE_MODVAL_IN_MODDIRECTIVE	431
LDAP_ASN1_UNEXPECTED_TYPE_MRAFILTER_IN_FILTER	431
LDAP_ASN1_UNEXPECTED_TYPE_MRAFILTER_IN_SEARCHREQUEST	432
LDAP_ASN1_UNEXPECTED_TYPE_MRID_IN_MRASSERTION	432
LDAP_ASN1_UNEXPECTED_TYPE_NAME_IN_BINDREQUEST	432
LDAP_ASN1_UNEXPECTED_TYPE_OBJECTDN_IN_ADDREQUEST	432
LDAP_ASN1_UNEXPECTED_TYPE_OBJECTDN_IN_MODIFYREQUEST	433
LDAP_ASN1_UNEXPECTED_TYPE_PRESENTFILTER_IN_FILTER	433
LDAP_ASN1_UNEXPECTED_TYPE_PRESENTFILTER_IN_SEARCHREQUEST	433
LDAP_ASN1_UNEXPECTED_TYPE_REFERRAL_IN_BINDRESPONSE	433
LDAP_ASN1_UNEXPECTED_TYPE_REFERRAL_IN_EXTENDEDRESPONSE	434
LDAP_ASN1_UNEXPECTED_TYPE_REFERRAL_IN_LDAPRESULT	434
LDAP_ASN1_UNEXPECTED_TYPE_RESPNAME_IN_EXTENDEDRESPONSE	434
LDAP_ASN1_UNEXPECTED_TYPE_RESPVALUE_IN_EXTENDEDRESPONSE	434
LDAP_ASN1_UNEXPECTED_TYPE_RESULTCODE_IN_BINDRESPONSE	435
LDAP_ASN1_UNEXPECTED_TYPE_RESULTCODE_IN_LDAPRESULT	435
LDAP_ASN1_UNEXPECTED_TYPE_SASLAUTH_IN_BINDREQUEST	435
LDAP_ASN1_UNEXPECTED_TYPE_SEARCHREQ_IN_LDAPMESSAGE	435
LDAP_ASN1_UNEXPECTED_TYPE_SEARCHRESENTRY_IN_LDAPMESSAGE	436
LDAP_ASN1_UNEXPECTED_TYPE_SEARCHRESREF_IN_LDAPMESSAGE	436
LDAP_ASN1_UNEXPECTED_TYPE_SRVRSASLCRED_IN_BINDRESPONSE	436
LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRINGFILTER_IN_FILTER	436
LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRINGFILTER_IN_SEARCHREQUEST	437

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRING_IN_SEQUENCEOFSUBSTRINGS	437
LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRINGS_IN_SUBSTRINGFILTER	437
LDAP_ASN1_UNEXPECTED_TYPE_SIMPLEAUTH_IN_BINDREQUEST	437
LDAP_ASN1_UNEXPECTED_TYPE_UNBINDREQ_IN_LDAPMESSAGE	438
LDAP_ASN1_UNEXPECTED_TYPE_VERSION_IN_BINDREQUEST	438
LDAP_MODIFYTYPE_UNKNOWN	438
LDAP_DEREFALIASES_UNKNOWN	438
LDAP_RESULTCODE_AUTHFAILURE	439
LDAP_RESULTCODE_RESERVEDVALUEUSED	439
LDAP_RESULTCODE_UNKNOWN	439
LDAP_SEARCHSCOPE_UNKNOWN	439
LDAP_VERSION_UNKNOWN	440
MSSQL_NULL_PACKET_DOS	362
MSSQL_STACKOVERFLOW	363
NBT_INVALID_COMMAND	440
NBT_SMB_GUEST_LOGIN	455
NNTPCLI_BUFFER_OVERFLOW_ATTEMPT	331
NNTPCLI_EXPECTED_CRLF	440
NNTPCLI_FAILED_AUTHENTICATION	440
NNTPCLI_INVALID_ASCII	441
NNTPCLI_INVALID_COMMAND	441
NNTPCLI_INVALID_TEXT	441
NNTPSER_INVALID_ASCII	442
NNTPSER_INVALID_RESPONSE	441
NNTPSER_INVALID_TEXT	442
OSPF_BAD_CRYPTO_AUTH_FIELD	445
OSPF_BAD_VERSION_NUM	444
OSPF_DBDESC_INVALID_FLAGS	443
OSPF_DBDESC_INVALID_OPTS	443
OSPF_DBDESC_SHORT_PACKET	443
OSPF_HELLO_BAD_NEIGHBOR	442
OSPF_HELLO_INVALID_OPTS	442
OSPF_HELLO_SHORT_PACKET	442
OSPF_LS_UPDATE_OVERLONG_PACKET	444
OSPF_LS_UPDATE_SHORT_PACKET	444

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
OSPF_LSA_EXTERNAL_BAD_FLAGS	443
OSPF_LSA_EXTERNAL_SHORT_PACKET	443
OSPF_LSA_INVALID_OPTS	444
OSPF_LSA_MAX_AGE	444
OSPF_LSA_MAX_SEQNUM	332
OSPF_LSA_SHORT_PACKET	445
OSPF_LSA_NETWORK_BAD_PACKET	445
OSPF_LSA_SUMMARY_MALFORMED_PACKET	445
OSPF_LSA_NETWORK_SHORT_PACKET	445
OSPF_LSA_ROUTER_BAD_PADDING	446
OSPF_LSA_ROUTER_BAD_FLAGS	446
OSPF_LSA_ROUTER_SHORT_PACKET	446
OSPF_LSA_SUMMARY_SHORT_PACKET	446
OSPF_LSID_ATTACK	332
OSPF_LSREQ_BAD_LENGTH	444
OSPF_NULL_AUTHENTICATION	506
OSPF_PACKET_LEN_MISMATCH	445
OSPF_SHORT_PACKET	446
OSPF_SIMPLE_AUTHENTICATION	443
OSPF_UNKNOWN_LSA_TYPE	446
OSPF_UNKNOWN_TYPE	446
POP3_CLIENT_BAD_CMD_ARGUMENT	447
POP3_CLIENT_BAD_INIT_COMMAND	447
POP3_CLIENT_CRLF_EXPECTED	447
POP3_CLIENT_DATA_AFTER_QUIT	447
POP3_CLIENT_FAILED_LOGIN	447
POP3_CLIENT_INVALID_COMMAND	447
POP3_CLIENT_LONG_COMMAND	333
POP3_INVALID_ARG_TO_QUIT	447
POP3_SERVER_LONG_LINE	333
POP3_SERVER_BAD_BASE64_STR	448
POP3_SERVER_BAD_GREETING	448
POP3_SERVER_INVALID_CHAR_IN_RESPONSE	448
POP3_SERVER_INVALID_RESPONSE	448
POP3_USER_ROOT	333

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
RLOGIN_FROOT_EXPLOIT_ATTEMPTED	333
RLOGIN_INVALID_CLI_INIT	449
RLOGIN_INVALID_CLI_LOGIN_FIELD	449
RLOGIN_INVALID_SER_LOGIN_FIELD	449
RLOGIN_INVALID_SERVER_INIT	449
RLOGIN_INVALID_TERM_FIELD	450
RLOGIN_INVALID_USERNAME	450
RLOGIN_LOGIN_FAILED	448
RLOGIN_LONG_TERMINAL	334
RLOGIN_ROOT_LOGIN_FAILED	448
RPC_BUFFER_OVERFLOW	450
RPC_INVALID_ACCEPTED_TYPE	450
RPC_INVALID_MTYPE	451
RPC_INVALID_REJECTED_REPLY	451
RPC_INVALID_VERSION	451
RPC_MOUNTD_LONG_DIRNAME	325
RPC_NULL_RMFRAG	451
RPC_PACKET_OVERRUN	452
RPC_RUNT_PACKET	452
RPC_SHORT_PAYLOAD	452
RPC_STATD_LONG_HOSTNAME	342
RSH_FROOT_EXPLOIT_ATTEMPTED	334
RSH_INVALID_USERNAME	453
RSH_INVALID_CLI_LOGIN_FIELD	453
RSH_INVALID_COMMAND_LINE	453
RSH_INVALID_LOC_LOGIN_FIELD	454
RSH_INVALID_SERVER_INIT	454
RSH_LOGIN_FAILED	452
RSH_ROOT_LOGIN_FAILED	453
SENSOR_ERROREXIT_FAILURE	353
SENSOR_IFDEVOPEN_FAILURE	353
SENSOR_MALLOC_FAILURE	353
SENSOR_PORTMAP_BAD	353
SENSOR_RCRDINIT_FAILURE	354
SENSOR_SNIFF_DATA_BAD	353

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
SMB_DEL_ACCESS_DENIED	454
SMB_GUEST_LOGON_ATTEMPT	456
SMB_INVALID_HEADER	456
SMB_OOB_DATA_WINNUKE	302
SMB_SESSION_ACCESS_DENIED	454
SMB_SESSION_BAD_PASSWORD	455
SMB_SHORT_BATCHED_PAYLOAD	456
SMB_SHORT_PASSWORD	457
SMB_TREE_ACCESS_DENIED	455
SMB_TREE_BAD_PASSWORD	455
SMTP_AUTHENTICATION_FAILED	457
SMTP_BAD_EMAIL_ADDRESS	457
SMTP_BAD_SERVER_BANNER	458
SMTP_BAD_SERVER_DATA	458
SMTP_BUFFER_OVERFLOW_ATTEMPT	334
SMTP_CLIENT_BAD_BDAT_ARG	458
SMTP_CLIENT_BAD_DOMAINNAME	459
SMTP_CLIENT_CYBERCOP_SECURITY_SCAN	358
SMTP_CLIENT_DATA_BEFORE_HELO	458
SMTP_CLIENT_HELO_BOF	335
SMTP_CLIENT_MALFORMED_COMMAND	459
SMTP_CLIENT_PIPE_EXPLOIT_ATTEMPT	334
SMTP_EXPN_DOS	457
SMTP_PROBABLE_NOOP_BUFFER_EXPLOIT	335
SMTP_ROOT_INFO_GATHERING_ATTEMPT	358
SMTP_SENDMAIL_BO	335
SNMP_ASN1_DATALENGTH_IMPOSSIBLE_STATE	336
SNMP_ASN1_DATALENGTH_RIDICULOUS_WIDTH	336
SNMP_ASN1_DATALENGTH_VALUE_TOO_LARGE	336
SNMP_ASN1_DATALENGTH_VALUE_TOO_SMALL	460
SNMP_ASN1_INTERNALERROR_OVERREAD_OCTETSTRING	337
SNMP_ASN1_NESTEDSEQUENCE_OVERFLOW	338
SNMP_ASN1_TOO_MANY_NESTED_LEVELS	461
SNMP_ASN1_TYPE_ILLEGAL_LONG_ENCODING	339
SNMP_ASN1_TYPE_UNRECOGNIZED	340

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
SNMP_EMPTY_COMMUNITY_STRING_BULKREQUESTPDU	463
SNMP_EMPTY_COMMUNITY_STRING_REQPDU	464
SNMP_EMPTY_COMMUNITY_STRING_TRAPPDU	465
SNMP_ERROR_DATA_AFTER_MESSAGE_END	342
SNMP_ERROR_INDEX_PAST_END_OF_MSG	342
SNMP_INSECURE_COMMUNITY_STRING_BULKREQUESTPDU	466
SNMP_INSECURE_COMMUNITY_STRING_REQPDU	467
SNMP_INSECURE_COMMUNITY_STRING_TRAPPDU	468
SNMP_INTERNALERROR_IMPOSSIBLE_SNMP_STATE	343
SNMP_INVALID_BULK_MAXREPETITIONS	469
SNMP_INVALID_BULK_NONREPEATERS	470
SNMP_INVALID_ERROR_INDEX	471
SNMP_INVALID_ERROR_STATUS	472
SNMP_INVALID_GENERIC_TRAP	473
SNMP_INVALID_MSGHEADER_MSGFLAGS_SIZE	343
SNMP_INVALID_MSGHEADER_MSGID	474
SNMP_INVALID_MSGHEADER_MSGMAXSIZE	475
SNMP_INVALID_MSGHEADER_MSGSECMODEL	476
SNMP_MSGHEADER_OVERLONG_SEQUENCE	344
SNMP_SCOPEDPDU_OVERLONG_SEQUENCE	345
SNMP_TOO_MANY_VARBIND_PAIRS	346
SNMP_UNEXPECTED_MESSAGE_END	477
SNMP_UNEXPECTED_TYPE_FOR_BULKREQUEST_MAXREPETITIONS	478
SNMP_UNEXPECTED_TYPE_FOR_BULKREQUEST_NONREPEATERS	479
SNMP_UNEXPECTED_TYPE_FOR_BULKREQUESTPDU_REQUEST_ID	480
SNMP_UNEXPECTED_TYPE_FOR_COMMUNITY_NAME	481
SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_MSGFLAGS	482
SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_MSGID	483
SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_MSGMAXSIZE	484
SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_SECMODEL	485
SNMP_UNEXPECTED_TYPE_FOR_MSGSECPARAMS	486
SNMP_UNEXPECTED_TYPE_FOR_PDU	487
SNMP_UNEXPECTED_TYPE_FOR_PDU_REQUEST_ID	488
SNMP_UNEXPECTED_TYPE_FOR_REQUEST_ERROR_INDEX	489
SNMP_UNEXPECTED_TYPE_FOR_REQUEST_ERROR_STATUS	490

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
SNMP_UNEXPECTED_TYPE_FOR_SCOPEDPDU_CONTEXTENGINEID	491
SNMP_UNEXPECTED_TYPE_FOR_SCOPEDPDU_CONTEXTNAME	492
SNMP_UNEXPECTED_TYPE_FOR_SCOPEDPDUDATA	493
SNMP_UNEXPECTED_TYPE_FOR_SNMP_MESSAGE	347
SNMP_UNEXPECTED_TYPE_FOR_TRAP_ENTERPRISE_OID	494
SNMP_UNEXPECTED_TYPE_FOR_TRAP_GENERIC_TYPE	495
SNMP_UNEXPECTED_TYPE_FOR_TRAP_SOURCE_ADDRESS	496
SNMP_UNEXPECTED_TYPE_FOR_TRAP_SPECIFIC_TYPE	497
SNMP_UNEXPECTED_TYPE_FOR_TRAP_TIMESTAMP	498
SNMP_UNEXPECTED_TYPE_FOR_V1_PDU	499
SNMP_UNEXPECTED_TYPE_FOR_V3_MSGHEADER	500
SNMP_UNEXPECTED_TYPE_FOR_VARBIND_DATA	501
SNMP_UNEXPECTED_TYPE_FOR_VARBIND_LIST	502
SNMP_UNEXPECTED_TYPE_FOR_VARBIND_OID	503
SNMP_UNEXPECTED_TYPE_FOR_VARBIND_PAIR	504
SNMP_UNEXPECTED_TYPE_FOR_VERSION	348
SNMP_UNRECOGNIZED_SNMP_VERSION	505
SNMP_VARBIND_PAIR_OVERLONG_SEQUENCE	349
SOCKS_INVALID_DATA	461
SOCKS4_INVALID_RESPONSE	461
SOCKS4_REQUEST_DENIED	461
SOCKS4_UNAUTHENTICATED	506
SOCKS5_AUTHENTICATION_FAILURE	461
SOCKS5_CHAIN_ATTEMPT	462
SOCKS5_COMMAND_NOT_SUPPORTED	462
SOCKS5_INVALID_REQUEST	462
SOCKS5_INVALID_REQUEST_VERSION	462
SOCKS5_INVALID_RESPONSE_VERSION	462
SOCKS5_NULL_DESTADDRESS	462
SOCKS5_REQUEST_DENIED	462
SOCKS5_UNAUTHENTICATED	506
TELNET_LD_ENVIRONMENT	350
TELNET_LIVINGSTON_DOS	301
TELNET_LOGIN_INCORRECT	505
TELNET_RESOLV_ENVIRONMENT	350

Table B-1 Alphabetical listing of base events types and their associated page (Continued)

Base Event	Page
TELNET_ROOT_LOGIN_FAILED	505
TELNET_SGI_FMTSTRING_VULN	351
TELNET_WINGATE_PROMPT	506
TOMCAT_CROSS_SITE	361
W32_NIMDA_A_MM	328
W32_NIMDA_E_MM	330
WIN_DNS_DATA_AFTER_END	506

Denial-of-Service

Echo/Chargen Flood

Base Event: COUNTER_BAD_SERVICES_DOS

Details: Echo or chargen traffic has been detected. This is flagged as an event because echo and chargen are largely deprecated protocols and their heavy usage should be considered an unusual event. An attacker can use echo and chargen services to perform a denial-of-service attack. The attacker often locates a host running these services and then sends traffic to them designed to force the host to send a reply to a secondary victim host. Done in volume, this can create a denial-of-service attack. If the flood is traced back, it leads only to the primary victim host.

Response: Response to echo/chargen floods typically involves locating the flooding host first and disabling these services. Note that the original traffic to the primary victim is forged in this case so the source addresses do not provide any information useful for locating the true source. If it is possible to trace the traffic back to the source, the source can be shut down and possibly prevent further attacks.

Affected: This attack tends to target UNIX systems (as the primary victim).

False Positives: None known.

References: CVE-1999-0103

CERT

Finger DOS

Base Event: FINGER_FORWARDING_ATTEMPT

Details: A finger request was made that included a finger forwarding attempt. These requests are used to flood the resources on the target host by creating a finger request loop.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. If a flood is currently active, you can use network filters to mitigate the effect.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0105

http://www.whitehats.com (arachNIDS #251)

Finger Specifications

Fragmentation Attack

Base Event: IP_FRAG_NOMATCH

Details: Two overlapping fragments were found to have different data in the overlapping region. This may indicate a possible attempt to evade detection or filtering by a security device. Tools like “fragrouter” are used by an attacker to fragment their attacks such that some security devices will not properly reassemble the packets.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

Fragmentation Attack

Base Event: IP_FRAG_ODDLENGTH

Details: An IP fragment was detected with an invalid fragment length. This may indicate a fragmentation denial-of-service attack that is known to crash some operating system network stacks.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system. Since the source address is usually forged it is not possible to locate the attacker by examining the attack packets.

Affected: No specific targets.

False Positives: None known.

Fragmentation Attack

Base Event: IP_FRAG_OVERDROP1

Details: An “overdrop” attack was detected. An “overdrop” attack involves an attacker sending oversized IP packets. This triggers a bug in the victim systems which can cause performance problems.

The IP_FRAG_OVERDROP1 event corresponds to detecting that a fragmented datagram would reassemble to a IPV4 datagram larger than 65535 bytes by sending a single fragment whose offset and payload size would simply add up to be larger than 65535.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system.

Affected: No specific targets.

False Positives: None known.

Fragmentation Attack

Base Event: IP_FRAG_OVERDROP2

Details: An “overdrop” attack was detected. An “overdrop” attack involves an attacker sending oversized IP packets. This triggers a bug in the victim systems which can cause performance problems.

The IP_FRAG_OVERDROP2 event corresponds to detecting that fragments received would reassemble to a IPV4 datagram larger than 65535 bytes by sending out of order fragments such that the IP header of the reassembled datagram contains options, making the IP header larger than the standard 20 bytes allowed for average IP headers, and that this in conjunction with fragments already received would reassemble into a datagram larger than 65535 bytes.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system.

Affected: No specific targets.

False Positives: None known.

Fragmentation Attack

Base Event: IP_FRAG_OVERDROP3

Details: An “overdrop” attack was detected. An “overdrop” attack involves an attacker sending oversized IP packets. This triggers a bug in the victim systems which can cause performance problems.

The IP_FRAG_OVERDROP3 event corresponds to detecting that fragments received would reassemble to a IPV4 datagram larger than 65535 bytes by sending out of order fragments such that the IP header of the reassembled datagram contains options, making the IP header larger than the standard 20 bytes allowed for average IP headers, and that this in conjunction with fragments already received would reassemble into a datagram larger than 65535 bytes. The IP_FRAG_OVERDROP3 event differs from OVERDROP2 (even though both detect overdrop as a result of an out of order offset zero fragment using IP header options to push an already reassembled datagram past the 65535 byte limit) in that the OVERDROP3 event is only thrown when both the first and last fragments have been seen for the given datagram reassembly, but OVERDROP2 does not require that the last fragment has been seen.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system.

Affected: No specific targets.

False Positives: None known.

Fragmentation Attack

Base Event: IP_FRAG_TEARDROP

Details: A “teardrop” attack was detected. A “teardrop” attack involves an attacker sending a packet fragment containing improperly overlapping fragments. This triggers a bug in the victim systems which can cause crashes or performance problems.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0015

ICMP Flood

Base Event: COUNTER_ICMP_HIGH

Details: ICMP traffic is consuming an unusually large percentage of a network link. This is an attempt to flood the target network, usually with ICMP echo requests. An attacker may use the “ping” tool to send a large number of echo requests to the victim system in an attempt to consume most or all of the victim’s network capacity.

Response: Responses to ICMP floods typically include installing some sort of temporary network filter to eliminate the inbound packets and then locating and terminating the source of the flood. Note that in some floods the source addresses of the flooding packets may be forged to make the location effort more difficult.

Affected: No specific targets.

False Positives: It is possible for some legitimate network management tools to be detected as ICMP floods.

References: CERT

IP Fragment Flood

Base Event: COUNTER_IPFRAG_HIGH

Details: IP fragments are consuming an unusually large percentage of the network traffic. This is an attempt to flood the target network, usually with “garbage” packets. An attacker may use a tool to send a large number of IP fragment packets to the victim system or network in an attempt to consume most or all of the victim’s network capacity. It may also be an attempt to flood a particular application or service if targeted at a particular address and port.

Response: Responses to IP fragment floods typically include installing some sort of temporary network filter to eliminate the inbound packets and then locating and terminating the source of the flood. Note that in some floods the source addresses of the flooding packets may be forged to make the location effort more difficult.

Affected: No specific targets.

False Positives: It is possible for legitimate network applications which send large numbers of IP fragments as IP fragment floods. Applications which use UDP as a transport layer are more likely to generate this type of false positive since unlike TCP, UDP has no provisions for breaking up large chunks of data, leaving any such datagram breakup to either the IP layer or the application program.

IP Header Length Overruns Packet Length

Base Event: IP_HEADERLEN_OVERRUNS_PACKETLEN

Details: An IP header length of a defragmented IP datagram indicates a IP header length that exceeds the overall IP packet specified in the IP header.

Affected: No specific targets.

False Positives: None known.

Land Attack

Base Event: IP_SRC_DST_SAME_LAND

Details: A “land” attack has been detected. A “land” attack involves an attacker sending a packet with the source and destination addresses set to the same value was detected. This is a well known denial-of-service attack against some IP stack implementations that results in excessive CPU being consumed on the victim host while the host attempts to respond to itself. This attack may be used both against hosts and network devices.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system. Since the source address is forged it is not possible to locate the attacker by examining the attack packets.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0016

Malformed ICMP Packet

Base Event: ICMP_UNREACH_RUNT

Details: An “ICMP Destination Unreachable” packet was seen on the network, but included a shorter than allowed payload.

Affected: No specific targets.

False Positives: None known.

Runt IP Header

Base Event: IP_RUNT_HEADER_LENGTH

Details: An IP header length shorter than the legal minimum length was specified in the IP header of the packet. This is most likely an attempt to crash the target machine’s IP stack. This attack is used both against hosts and network devices.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system. Since the source address may be forged it is not possible to locate the attacker by examining the attack packets.

Affected: No specific targets.

False Positives: None known.

SYN Flood

Base Event: COUNTER_UNACKED_SYNS_HIGH

Details: This indicates that a large number of packets with the SYN flag have been detected without a following ACK of the TCP connection. This can indicate that a SYN flood denial-of-service attack or that a port scan is taking place. SYN floods involve an attacker sending large number of SYN packets to initiate a TCP connection. The receiving host then begins the process of opening a connection. The attacker however makes no further attempt to complete the connection causing the victim host to wait until a “timeout” period has expired before giving up. Since most systems have some limit on the number of connections that they can open, this causes a denial-of-service as legitimate connections are then ignored. It is often used as a denial-of-service against a particular network service such as a Web server.

Response: Responses to SYN floods typically include installing some sort of temporary network filter to eliminate the traffic while locating the source and terminating it. However since the source address may be forged, if the address range is too widely varied or intentionally crafted, such filters may end up denying service to desired connections as well.

Affected: No specific targets.

False Positives: It is possible that a network condition is causing the security gateway to drop the ACKs, or preventing it from seeing them. Some asymmetric network configurations can cause this type of behavior.

References: CVE-1999-0116

CERT

SYN Flood

Base Event: COUNTER_ICMP_UDPUNREACHABLE_HIGH

Details: This indicates that a large number of ICMP packets indicating that a UDP destination was unreachable have been detected. This can indicate UDP flood denial-of-service attack or that a port scan is taking place. UDP floods involve an attacker sending large number of UDP packets to a destination with the intent of overwhelming the system resources on the victim host.

Response: Responses to UDP floods typically include installing some sort of temporary network filter to eliminate the traffic while locating the source and terminating it. However since the source address may be forged, if the address range is too widely varied or intentionally crafted, such filters may end up denying service to desired connections as well.

Affected: No specific targets.

False Positives: It is possible that some network condition is denying the UDP packets. Some asymmetric network configurations can cause this type of behavior.

Telnet DOS

Base Event: TELNET_LIVINGSTON_DOS

Details: A denial-of-service attempt against a Livingston router administration port was detected. This may indicate an attacker intentionally attempting to prevent access to the victim device.

Response: Response typically includes location of the source and termination of the processes generating the traffic.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0218

http://www.whitehats.com (arachNIDS #370)

Telnet Specifications

UDP Flood

Base Event: COUNTER_UDP_HIGH

Details: UDP traffic is consuming more than 90 percent of the network traffic. This is considered unusual. This is an attempt to flood the target network, usually with “garbage” UDP packets. An attacker may use a tool to send a large number of UDP packets to the victim system or network in an attempt to consume most or all of the victim’s network capacity. It may also be an attempt to flood a particular application or service if targeted at a particular address and port.

Response: Responses to UDP floods typically include installing some sort of temporary network filter to eliminate the inbound packets and then locating and terminating the source of the flood. Note that in some floods the source addresses of the flooding packets are forged to make the location effort more difficult.

Affected: No specific targets.

False Positives: It is possible for legitimate network applications which send large numbers of UDP packets to be detected as UDP floods. Possible examples of this are multimedia applications, some network file sharing applications and various tunneling tools.

References: CERT

Unknown Protocol Flood

Base Event: COUNTER_UNKPROTO_HIGH

Details: A large portion of layer 4 traffic on a link is of an unknown protocol. This is considered unusual, and might be an attempt to flood the target network. An attacker can send a large number of packets to the victim system or network in an attempt to consume most or all of the victim's network capacity. It may also be an attempt to flood an application or service if targeted at a specific address and port. In this case the protocol is not TCP or UDP.

Response: Responses to floods typically include installing some sort of temporary network filter to eliminate the inbound packets and then locating and terminating the source of the flood. Note that in some floods the source addresses of the flooding packets may be forged to make the location effort more difficult.

Affected: No specific targets.

False Positives: It is possible for legitimate network applications which send large numbers of packets of an unknown protocol to be detected as floods.

References: CERT

Winnuke

Base Event: SMB_OOB_DATA_WINNUKE

Details: A WinNuke attack has been detected. WinNuke is specifically designed to crash some versions of the Microsoft Windows operating system. The attacker sends a packet to the netbios port, triggering a bug in the Microsoft Windows networking system and causing the machine to crash. This typically affects only older, unpatched Microsoft Windows systems.

Response: Response to this attack typically includes applying a patch from the vendor to fix the vulnerability on the victim system. The source IP address of the attack may also be useful in locating the source of the attack and preventing further attacks.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0153

Intrusion attempts

Back Orifice Web Server

Base Event: HTTP_RESPMSGHDR_SIG1

Details: The well known response of the back orifice backdoor was detected.

Response: Location and audit of client and server is recommended. The back door software should be removed from the server.

Affected: No specific targets.

False Positives: None known.

References: CERT VN-98.07

Bad Hex Character

Base Event: HTTP_BAD_ESCAPE_SEQUENCE

Details: The IDS component detected a % character (indicating a 2 digit hex byte follows) in a pathname and the next two characters were not valid hex digits. This may be an attempt to exploit the IIS traversal bug.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Bad UTF-8 Hex Character

Base Event: HTTP_URL_OVERLONG_DOT

Details: The IDS component detected an incorrect (too long) representation of a dot (.) character. This may be an attempt to exploit an IIS server.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

BFTP SITE CHOWN BO

Base Event: BFTP_SITE_CHOWN_BUFFER_OVERFLOW

Details: In bftpd, an FTP daemon, there is a buffer overflow in the first parameter passed to the SITE CHOWN command.

Response: Workaround

In /etc/bftpd.conf replace

ENABLE_SITE=yes

with

ENABLE_SITE=no

Affected: Max-Wilhelm Bruker bftpd 1.0.13

False Positives: None known.

References: Security Focus BID: 2120

CVE-2001-0065

CodeRed Worm

Base Event: CODERED_WORM

Details: The code red worm uses a buffer overflow vulnerability in the idq.dll, which runs at the system security level, when handling URL requests. Once an attacker establishes a session on the Web server and causes a buffer to overflow, that attacker can perform virtually any function on that server.

Response: Please refer to the following link for more information about the available fixes:

CodeRed Removal Tool

For Microsoft Windows 2000 Professional, Server and Advanced Server:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

For Microsoft Windows 2000 Datacenter Server, patches are hardware-specific and available from the original equipment manufacturer.

The vulnerability is eliminated beginning with Microsoft Windows XP Release Candidate 1.

Affected: Microsoft IIS 4.0 and 5.0

Microsoft Personal Web Server 4.0

Microsoft Index Server 2.0

Indexing Service in Microsoft Windows 2000

False Positives: None known.

References: Security Focus BID: 2880

CVE-2001-0500

Microsoft Security Bulletin: MS01-033

Symantec Security Response: CodeRed Worm

ColdFusion Expression Evaluator Access

Base Event: HTTP_URL_SIG14

Details: An attempt to access the Macromedia ColdFusion expression evaluator was detected. There is a known vulnerability in Macromedia ColdFusion that could be exploited to delete and display any file in the system.

Response: Location and audit of client and server is recommended. If you intended to be using these CGIs you should contact the vendor for any applicable updates.

Affected: Macromedia ColdFusion Server 2.0, 3.0, 3.0.1, 3.1, 3.1.1, 3.1.2, 4.0.

False Positives: None known.

References: CVE-1999-0477

HTTP Specifications

DeepThroat Trojan

Base Event: FTPSER_TROJAN_DEEPTHROAT

Details: The DeepThroat Trojan horse was detected.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: CAN-1999-0660

http://www.whitehats.com (arachNIDS #406)

FTP Specifications

Direct Perl Access

Base Event: HTTP_URL_SIG5

Details: The HTTP request URL attempted direct access of the Perl executable. This usually represents an attempt to execute arbitrary code on the target system.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: CAN-1999-0509

http://www.whitehats.com (arachNIDS #219)

HTTP Specifications

DNS Exploit Attempt

Base Event: DNS_BAD_COMPRESSION

Details: There was a pointer in a label to the DNS packet header. This represents a mal-formed DNS packet and a possible exploitation attempt of the TSIG bug.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: DNS Specifications

DNS Exploit Attempt

Base Event: DNS_BAD_LABEL_LENGTH

Details: The DNS label length used in host name construction specified an illegal value. This can represent a possible DNS bug exploit attempt.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: DNS Specifications

DNS Exploit Attempt

Base Event: DNS_LONG_NAME

Details: A DNS query was made with a host name over 255 chars; this is outside of the RFC spec.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0275
CVE-1999-0299
CVE-1999-0405
DNS Specifications

DNS Exploit Attempt

Base Event: DNS_LONG_NXT_RDLEN

Details: There was a NXT record in a DNS packet which had an RDLEN well over the values normally used. This is an indication of an attempt to exploit the NXT BIND overflow.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0833
DNS Specifications

DNS Inverse Query

Base Event: DNS_IQUERY

Details: DNS inverse query. Once upon a time they were used to look up IPs, but they are not used anymore.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0009
DNS Specifications

Early UTF-8 Char End

Base Event: HTTP_EARLY_UTF8_END

Details: An early end to what appears as a UTF-8 character was detected. This may be an attempt to exploit the IIS traversal bug.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Finger Backdoor

Base Event: FINGER_CDK_BACKDOOR

Details: Attempt to access the well known CDK back door on the finger port was detected.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: Can-1990-0660
http://www.whitehats.com (arachNIDS #263)
Finger Specifications

Finger Backdoor

Base Event: FINGER_CMD_ROOTSH_BACKDOOR

Details: Attempt to access the well known back door on the finger port was detected.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: Finger Specifications

Finger Exploit Attempt

Base Event: FINGER_ILLEGAL_METACHAR

Details: An attempt was made to finger something with a common shell meta char (for example, “&” or “;”) which is used to pass commands through to the executing shell. Affects EMC DG/UX 5.4 4.11MU02.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: Can-1990-0612
http://www.whitehats.com (arachNIDS #380)
Finger Specifications

FTP Bad Username

Base Event: FTPCLI_USER_BIN

Details: FTP client logon attempt was made using a “bad” user name (bin). This may indicate an attempt to compromise the FTP server.

Response: If seen in sufficient volume or variation audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: FTP Specifications

FTP Bad Username

Base Event: FTPCLI_USER_WAREZ

Details: FTP Client logon attempt was made using a “bad” user name (warez). This may indicate an attempt to access an illicit account on the FTP server.

Response: The server should be audited for presence of this account.

Affected: No specific targets.

False Positives: None known.

References: http://www.whitehats.com (arachNIDS #327)
FTP Specifications

FTP Bounce Attack

Base Event: FTP_BOUNCE_ATTACK

Details: The FTP Bounce attack was detected. This attack may allow a malicious FTP client to redirect attack traffic through a vulnerable FTP server, thereby obfuscating the attack traffic’s true source.

Response: A complete audit of the client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: FTP Specifications

FTP Buffer Overflow

Base Event: FTPCLI_BUFFER_OVERFLOW

Details: An FTP buffer overflow attempt was detected. This indicates an attempt to compromise the server.

Response: Location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: FTP Specifications

FTP Buffer Overflow

Base Event: FTPCLI_NOOP_BUFFER_OVERFLOW

Details: A possible buffer overflow was detected. This indicates than an attempt to compromise the server. In this case an unusually long string of NO-OP codes are detected from the client. NO-OP codes are commonly used in buffer-overflow attacks to increase the chance of exploit code being executed.

Response: Location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: CAN-1999-0368

FTP Specifications

FTP Buffer Overflow

Base Event: FTPSER_BUFFER_OVERFLOW

Details: An FTP buffer overflow attempt was detected. This indicates than an attempt to compromise the server. Examination of the packet contents may provide some additional information about the particular command.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: FTP Specifications

FTP Buffer Overflow

Base Event: FTPSER_NOOP_BUFFER_OVERFLOW

Details: An FTP buffer overflow was detected. This indicates than an attempt to compromise the server. In this case an unusually long string of NO-OP codes are detected from the client. NO-OP codes are commonly used in buffer-overflow attacks to increase the chance of exploit code being executed.

Response: Location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: FTP Specifications

FTP CreateDirectory Buffer Overflow

Base Event: FTP_CREATEDIRECTORY_BO

Details: ProFTPd versions, prior to and including 1.2pre1, as well as wuftpd versions, up to 2.4.2academ[BETA-18] and 2.4.2 beta 18 vr9, are vulnerable to a buffer overflow that could result in remote root access.

The user must have write access and be able to create an unusually long directory or directory structure to exploit this buffer overflow. The precise details of vulnerability have not been determined, but the vendor acknowledges the problem.

Response: The fix for wuftp was incorporated into 2.4.2 beta 18 VR10, released November 1, 1998.

Upgrade to this version or later. proftp resolved this issue with version 1.2.0pre2; a patch is also available for 1.2.0pre1.

Affected:	ProFTPD Project ProFTPD 1.2 ProFTPD Project ProFTPD 1.2pre1 Washington University wu-ftpd 2.4.2(beta 18) VR9 Washington University wu-ftpd 2.4.2academ[BETA-18]
False Positives:	None known.
References:	Security Focus BID: 2242 CVE-1999-0368 CA-99-03: FTP-Buffer-Overflows

FTP CWD ~root

Base Event:	FTP_CWD_ROOT
Details:	An attempt to access restricted files in root's home directory through FTP was detected.
Response:	A complete audit of the client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References:	FTP Specifications

FTP Exploit Attempt

Base Event:	FTPCLI_RETR_USE_COMPRESS_PROGRAM
Details:	Use of the "--use-compress-program <program>" FTP extension was detected. This FTP extension allows for the execution of an arbitrary program on the server host, and should not be used. It's use indicates a possible compromise of the FTP server.
Response:	Location and audit of client and server is recommended. If the extension is enabled, it should be disabled.
Affected:	No specific targets.
False Positives:	None known.
References:	CVE-1999-0202 http://www.whitehats.com (arachNIDS #134) FTP Specifications

FTP Exploit Attempt

Base Event:	FTPCLI_SITE_EXEC
Details:	The site exec FTP extension was detected. This FTP extension allows for the execution of an arbitrary program on the server host, and should not be used. It's use indicates a possible compromise of the FTP server.
Response:	If seen in sufficient volume or variation audit of client and server is recommended. If this extension is enabled, it should be disabled.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0080
CVE-1999-0955
http://www.whitehats.com (arachNIDS #285)
http://www.whitehats.com (arachNIDS #317)
http://www.whitehats.com (arachNIDS #452)
FTP Specifications

FTP IIS Status DOS

Base Event: FTP_TOO_MANY_GLOBS

Details: In IIS, a specially crafted FTP STAT command can crash the service. A number of Cisco products use IIS internally and share its vulnerabilities.

Response: Fixes available.
For information on which patch is appropriate for non-Microsoft products consult the Bugtraq reference.

Affected: IIS 4.0
IIS 5.0
IIS 5.1
Cisco Building Broadband Service Manager 4.0.1 to 5.1
Cisco Call Manager 1.0 to 3.0
Cisco ICS 7750
Cisco IP/VC 3540
Cisco Unity Server 2.0 to 2.4
Cisco uOne 1.0 to 4.0
Microsoft BackOffice 4.0 to 4.5
Microsoft Windows NT 4.0 Option Pack

False Positives: None known.

References: Security Focus BID: 4482
CVE: CAN-2002-0073
CIAC: M-066
CERT: VU#412203
Microsoft: Q317196

FTP Replydirname Buffer Overflow

Base Event: FTP_REPLYDIRNAME_BO

Details: The FTP daemon derived from the 4.x BSD source contains a serious vulnerability that may compromise root access.

A 1-byte overflow in the replydirname() function exists. The overflow condition is due to an off-by-one bug that lets an attacker write a null byte beyond the boundaries of a local buffer and over the lowest byte of the saved base pointer. As a result, the numerical value of the pointer decreases and points to a higher location, or lower address, on the stack than it should. When the replydirname() function returns, the modified and saved base pointer is stored in the base pointer register.

When the calling function returns, the return address is read from an offset to where the base pointer points. The return address will be at the incorrect location, if the base pointer is set to zero.

With the last byte of the base pointer zero, this is a location other than where it should be.

If the attacker has control of this stack region, such as the local variable that contained the extra byte in the first place, he or she can place an arbitrary address there. The function uses this address as the saved return address.

This is the case for ftpd. An attacker is able to force the FTP daemon to look in the user-supplied data for a return address, and then execute instructions at the location as root.

This vulnerability is exploited on systems supporting an anonymous FTP, if a writeable directory exists (such as an “incoming” directory). This is rarely in place by default.

Note: OpenBSD ships with FTP disabled, though it is a commonly used service.

Response: OpenBSD has released a patch for this vulnerability. NetBSD has released patches for versions 1.4.3 and 1.5.

We recommend that users with NetBSD 1.4.2 or earlier upgrade, and then apply one of the patches.

Disabling anonymous FTP may prevent remote users from exploiting this vulnerability.

Stack protection schemes, such as StackGuard or non-executable stack configurations, may limit exploitability.

Affected: BSD ftpd 0.3.2

David A. Holland linux-ftpd 0.17

David Madore ftpd-BSD 0.2.3

NetBSD NetBSD 1.4

NetBSD NetBSD 1.4.1

NetBSD NetBSD 1.4.2

NetBSD NetBSD 1.5

OpenBSD OpenBSD 2.4

OpenBSD OpenBSD 2.5

OpenBSD OpenBSD 2.6

OpenBSD OpenBSD 2.7

OpenBSD OpenBSD 2.8

False Positives: None known.

References: Security Focus BID: 2124

CVE-2001-0053

NetBSD Security Page

OpenBSD Security Information

FTP Site Newer DOS

Base Event: FTPCLI_SITE_NEWER

Details: A denial-of-service in WU-FTPD via the SITE NEWER command, which does not free memory properly.

It may be possible for remote users to cause wu-ftpd to consume large amounts of memory, creating a denial-of-service. If users can upload files, they can execute arbitrary code with the ftpd UID (usually root).

Response: You can upgrade to the newest version of Wu-ftpd (2.6) for any vulnerable platform.

Affected: Washington University wu-ftpd 2.5.0

False Positives: In environments where the SITE NEWER command is used frequently, this signature could produce false positives.

References: CVE-1999-0880

CERT: CA-1999-13

Security Focus BID: 737

FTP WARFtpd Literal Exploit

Base Event: FTPCLI_LITERAL_FILE_ACCESS

Details: WarFTPd ships with various macros to assist in setting up complex FTP sites.

It is possible to remotely call these macros, some of which are used to compromise the server. Some of these macros will provide server and operating system information. They can also be used to reveal the file contents in error messages, including the configuration files for WarFTP, which can also include plaintext administrator passwords.

The extent of the vulnerability differs between versions of WarFTPd:

Version 1.67b2, and prior:

Authenticated users can gain access to the restricted files.

Version 1.70:

Remote attackers can gain access to any file on the system, as well as run any system command with administrative privileges, if an ODBC driver is installed. This is done without being logged on to the FTP server.

Response: Patches have been provided for both v1.70 and v1.67b2 or older, available at:

http://war.jgaa.com/alert/

and:

ftp://ftp.no.jgaa.com/

Affected: Jgaa WarFTPd 1.67b2 and prior

Jgaa WarFTPd 1.70b

False Positives: None known.

References: Security Focus BID: 919

CVE-2000-0044

Jgaa Support Site

SECURITY ALERT - WARFTP DAEMON ALL VERSIONS

WarFTP Homepage

HTTP ASP DataSuffix Request

Base Event: HTTP_IIS_DATA_ACCESS

Details: Microsoft Internet Information Services (IIS) and other NT Web servers contain a vulnerability allowing remote attackers to obtain the requested Active Server Pages (ASP) files.

ASP pages are executed on the server side and the results are sent to a user's browser. However, when an attacker appends the string, "::$DATA" when requesting an ASP page, IIS will respond by returning the contents of the ASP page to the attacker. This is due to IIS improperly handling requests for alternate data streams.

If an attacker directly requests a file with its complete data stream name, an attacker's Web browser will be able to view the contents of the requested file. An attacker can use the obtained information to launch other attacks against a vulnerable system.

Response: We strongly recommend that users of Microsoft IIS upgrade to the latest version. Microsoft suggests, as a work around, that administrators disable read access to any script files.

Patches for other vendors are available at their respective Web sites.

For services not meant for public access, limit access to the trusted hosts and subnets only.

This vulnerability may result in the disclosure of database credentials or other sensitive data. Ensure that the accounts used by Web applications have minimal privileges and Read only access when possible.

This will limit the immediate consequences of account compromise. Enabling connection pooling and similar features, if available, may eliminate the need to include credentials in the ASP files.

Affected: Microsoft IIS 3.0

Microsoft IIS 4.0

Microsoft Personal Web Server 2.0

Microsoft Personal Web Server 3.0

Microsoft Personal Web Server 4.0

Microsoft Windows NT 4.0

False Positives: None known.

References: Security Focus BID: 149

Microsoft Security Bulletin (MS98-003)

HTTP Beck Exploit

Base Event: HTTP_URL_SIG9

Details: An unusually long string of forward slash characters has been detected in an HTTP request URL. This may indicate use of the "Beck" exploit against Apache HTTP servers.

Response: Location and audit of client and server is recommended. You should also contact the server vendor for any applicable updates.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

HTTP Bizdb Command Exploit

Base Event: HTTP_BIZDB_CGI_EXPLOIT

Details: BizDB is a Web database integration product using perl CGI scripts. One of the scripts, bizdb-search.cgi, passes a variable's contents to an unchecked open() call and can therefore be made to execute commands at the privilege level of the Web server.

The variable is dbname, and if it is passed a semicolon followed by shell commands, they will be executed.

This vulnerability cannot be exploited from a browser, as the software checks for a referrer field in the HTTP request. However, you can create a valid referrer field and send programmatically, or by means of a network utility, such as netcat.

Response: This problem has been fixed in the most recent version of BizDB.

Affected: CNC Technology BizDB 1.0

False Positives: None known.

References: Security Focus BID: 1104

BizDB Home Page

HTTP IIS ASP ChunkEncoding DOS

Base Event: HTTP_IIS_CHUNK_ENCODING_BOF

Details: Unchecked buffer in chunked transfer encodings can cause DoS.

If an attacker does a PUT or GET request and sets a large buffer for chunked transfer encoding the service will hang.

The server will only recover when it is restarted or the remote user cancels the session.

Response: Fixes available:

For IIS 4.0

http://download.microsoft.com/download/iis40/Patch/4.2.739.1/NT4/EN-US/chkenc4i.exe

For IIS 4.0 Alpha

http://download.microsoft.com/download/iis40/Patch/4.2.739.1/ALPHA/EN-US/chkenc4a.exe

Affected: Microsoft IIS 4.0 Alpha

Microsoft IIS 4.0

False Positives: None known.

References: BID: 1066

CVE: CVE-2000-0226

MS: FQ00-018

HTTP IIS CMDExecution Access

Base Event: HTTP_IIS_CMDEXECUTION_ACCESS

Details: When Microsoft IIS receives a valid request for an executable file, the filename is then passed to the underlying operating system, which executes the file. In the event IIS receives a specially formed request for an executable file, followed by the operating system commands, IIS will proceed to process the entire string rather than reject it.

Therefore, a malicious user may perform system commands through cmd.exe under the context of the IUSR_machinename account, which could possibly lead to privilege escalation, deletion, addition, file modification, or a full compromise of the server.

To establish successful exploitation, the requested file must be an existing .bat or .cmd file residing in a folder for which the user possesses executable permissions.

November 27, 2000 Update: Georgi Guninski has discovered new variants of this vulnerability that have appeared after applying the patch Q277873, supplied by Microsoft.

December 7, 2000 Update: Billy Nothern has discovered that the commands can also be parsed through ActiveState Perl.

UPDATE: We believe that an aggressive worm may be in the wild that actively exploits this vulnerability.

Response: Microsoft has released patches that eliminate the vulnerability. They also rectify the vulnerability described in: MS00-086).

This patch does not address the new variants discovered by Georgi Guninski on November 27, 2000.

After resolving the issue, try:

- Permitting access for trusted users only.
- Dedicating a separate drive or volume for published content.

Affected: Microsoft IIS 4.0

Microsoft IIS 5.0

False Positives: None known.

References: Security Focus BID: 1912

CVE-2001-0886

Microsoft Security Bulletin: MS01-086

HTTP Infosearch Access

Base Event: HTTP_URL_SIG11

Details: The string “infosrch.cgi” was detected in an URL request. There is a known vulnerability associated with this file which may allow the sender of the request to access files on the Web server host as user “nobody”.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: CVE-2000-0207

http://www.whitehats.com (arachNIDS #290)

HTTP Specifications

HTTP JJ CGI Cmd Exec

Base Event:	HTTP_JJ_CGI_EXPLOIT
Details:	JJ is a sample CGI program distributed with the NCSA HTTPd servers. It directly passes unfiltered user data to the /bin/mail program, and as such, it is used to escape to a shell using the ~ character on systems with a /bin/mail that allows for this. The attacker must know the password that the program requests, though by default, the program uses HTTPdRocKs or SDGROCKS. These default passwords must be changed in the program's source code. The consequence of a successful exploit is a shell with the UID of the server.
Response:	Remove the offending program, jj, from /cgi-bin.
Affected:	Rob McCool jj.c 1.0
False Positives:	None known.
References:	Security Focus BID: 2002

HTTP Long Host Field

Base Event:	HTTP_LONG_HOST_NAME
Details:	The HTTP traffic contained a very long host name. This may be an attempt to exploit certain server vulnerabilities.
Response:	If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References:	HTTP Specifications

HTTP MDAC Component Query

Base Event: HTTP_MDAC_COMPONENT_QUERY

Details: Microsoft Data Access Components (MDAC) contains a buffer overflow vulnerability in a Remote Data Services (RDS) component. The server side RDS component affected is called the RDS Data Stub, while the client side is called the Data Space control.

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code, or at the very least, cause a denial-of-service.

Response: Microsoft has released patches that eliminate the vulnerability. They also rectify the vulnerability described in: MS00-086).

This patch does not address the new variants discovered by Georgi Guninski on November 27, 2000.

After resolving the issue, it is recommended that you:

- Block external access to Web services at the network boundary, unless service is required by external parties.
- Run all client software as a non-privileged user with minimal access rights.
- Do not run Internet Explorer as a user with greater privileges than required.
- Run all server processes as non-privileged users with minimal access rights.
- Running IIS as an unprivileged user will limit the consequences of successful exploitation.
- Do not accept communications that originate from unknown or untrusted sources.
- Do not visit unknown or untrusted Web sites from critical systems.
- Do not open HTML email from unknown or untrusted users.

Affected: Microsoft Data Access Components (MDAC) 2.1

Microsoft Data Access Components (MDAC) 2.5

Microsoft Data Access Components (MDAC) 2.6

Microsoft Internet Explorer 5.01

Microsoft Internet Explorer 5.5

Microsoft Internet Explorer 6.0

False Positives: None known.

References: Security Focus BID: 6214

CAN-2002-1142

Microsoft Security Bulletin MS02-065

CERT Advisory CA-2002-33 Heap Overflow Vulnerability in Microsoft Data Access Components (MDAC)

HTTP MSFrontpage fpcount B0

Base Event: HTTP_FPCOUNT_EXPLOIT

Details: A buffer overflow exists in fpcount.exe, a site hit counter included with Microsoft FrontPage 98 Server Extensions prior to version 3.0.2.1330.

To determine the version number of the Microsoft FrontPage Server Extensions on a Web server, open the Web with the Microsoft FrontPage Explorer and click the Tools | Web Settings command. On the Configuration tab, check the Microsoft FrontPage Server Extensions Version field.

Response: An update to 3.0.2.1330 was available from the vendor as part of their product support. However, Microsoft FrontPage 98 is no longer supported by the vendor. Consider upgrading to a newer version.

Affected: Microsoft FrontPage 98 Server Extensions prior to version 3.0.2.1330

False Positives: None known.

References: BID: 2252

CAN-1999-1376

HTTP WinApache Bat Exec

Base Event: HTTP_BAT_FILE_PIPE

Details: A vulnerability has been discovered in the batch file handler for Apache on Microsoft Windows operating systems.

Special characters (such as |) may not be filtered by the batch file handler when a Web request is made for a batch file. As a result, a remote attacker may be able to execute arbitrary commands on the host running the vulnerable software. This may be exploited via a specially crafted Web request which contains the arbitrary commands to be executed.

Note that Web servers on Microsoft Windows operating systems normally run with SYSTEM privileges. The consequences of exploitation is that a remote attacker may be able to fully compromise a host running the vulnerable software.

The 2.0.x series of Apache for Microsoft Windows ships with a test batch file which may be exploited to execute arbitrary commands. Since this issue is in the batch file handler, any batch file which is accessible via the Web is appropriate for the purposes of exploitation.

Response: This issue has been addressed in Apache 1.3.24 and 2.0.34-BETA for Microsoft Windows operating systems. Administrators are advised to upgrade.

Please refer to the following link for the patch:

Apache Software Foundation

Affected: Apache Software Foundation Apache 1.3.6win32 to 1.3.23win32

Apache Software Foundation Apache 2.0.28-BETA win32 and 2.0.32-BETA win32

False Positives: The likelihood of a false positive only exists if the piping is used by certain users to perform legitimate requests.

References: CAN-2002-0061

BID: 4335

IMAP Authentication Buffer Overflow

Base Event: IMAP_AUTH_BUFFOVERFLOW

Details: IMAP authentication buffer overflow event.

References: CVE-1999-0005

IMAP Authentication Type Buffer Overflow

Base Event: IMAP_AUTH_TYPE_BOF

Details: IMAP buffer overflow of authentication type event.

References: CVE-1999-0005

IMAP Buffer Overflow

Base Event: IMAP_URL_TOO_LONG

Details: The URL provided as part of an IMAP exchange was too long. This indicates a possible buffer overflow attempt, which may crash a vulnerable system or give an attacker unauthorized access.

IMAP Login Buffer Overflow

Base Event: IMAP_CLI_USERID_QUOTED_TOO_LONG

Details: A quoted UID presented to the server by the client was longer than 100 characters.

IMAP Login Buffer Overflow

Base Event: IMAP_CLI_USERID_TOO_LONG

Details: A UID presented to the server by the client was longer than 100 characters.

IMAP Login Buffer Overflow

Base Event: IMAP_URL_USER_TOO_LONG

Details: A URL UID presented to the server by the client was longer than 100 characters.

IMAP Mailbox Buffer Overflow

Base Event: IMAP_MAILBOX_BOF

Details: A mailbox name longer than 512 chars was detected. This is considered unusual and is flagged as a possible buffer overflow exploit attempt.

References: CVE-1999-0005

Intel NOPs

Base Event: HTTP_URL_SIG0

Details: Intel NOP instructions have been detected in an HTTP URL. This represents a possible buffer overflow attempt.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Intel NOPs

Base Event: HTTP_BODY_SIG1

Details: Intel NOP instructions were detected inside the body of an HTTP request. This indicates a possible attempted buffer overflow attack.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Intel NOPs

Base Event: HTTP_REQMSGHDR_SIG0

Details: Intel NOP instructions have been detected in an HTTP header. This represents a possible buffer overflow attempt.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Intel NOPs

Base Event: HTTP_RESPMSGHDR_SIG0

Details: Intel NOP instructions have been detected in an HTTP header. This represents a possible buffer overflow attempt.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: CAN-1999-0660

HTTP Specifications

IRC Backdoor

Base Event: IRCCLISER_EL15SPY_ANSWER

Details: This is a signature detection event for a well known IRC worm (EL15SPY). The characteristic answer to a bait string “are_u” is sent (“EL15_send_kisses_to_U_:)__come_on!”).

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Backdoor

Base Event: IRCCLISER_EL15SPY_NOTIFICATION

Details: This is a signature detection event for a well known IRC worm (EL15SPY). This event indicates the notification of an infected client (IP, server, and port).

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Backdoor

Base Event: IRCCLISER_JOINED_BO_OWNED

Details: Someone joined an IRC channel with the name bo_owned. This is a signature of a well known IRC back door.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_AZACO_WORM

Details: Detection of the “azaco” worm. This is a signature detection event for a well known IRC worm.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_CLAWFINGER_WORM

Details: Detection of the “clawfinger” worm. This is a signature detection event for a well known IRC worm.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_EL15BMP_WORM

Details: Detection of the “el15bmp” worm. This is a signature detection event for a well known IRC worm.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_LIFESTAGES_WORM

Details: The life stages worm. This is a signature detection event for a well known IRC worm. The pattern detected is “dccsend life_stages.txt.shs”

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_LOA_WORM

Details: Detection of the “loa” worm. This is a signature detection event for a well known IRC worm.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_LUCKY_WORM

Details: Detection of the “lucky” worm. This is a signature detection event for a well known IRC worm.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_PR0N_WORM

Details: The IRC worm “pr0n” was detected. This is a signature detection event for a well known IRC worm. The pattern detected is “dcssend pron.bat”.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRC Worm

Base Event: IRCCLISER_SEPTIC_WORM

Details: The IRC worm “septic” was detected. This is a signature detection event for a well known IRC worm.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: IRC Specifications

IRIX webdist CGI Access

Base Event: HTTP_URL_SIG13

Details: An attempt to access the webdist CGI was detected. There is a known vulnerability in the webdist.cgi program that allows the sender of the request to execute commands on the Web server host with the privileges of the httpd daemon.

Response: Location and audit of client and server is recommended. If you intend to use these CGIs you should contact the vendor for any applicable updates.

Affected: SGI IRIX 5.0, 5.1, 5.2, 5.3, 6.1, 6.2, and 6.3.

False Positives: None known.

References: CVE-1999-0039

HTTP Specifications

Java ServerSocket

Base Event: HTTP_BODY_SIG3

Details: A Java instruction opening a server socket was detected inside the body of an HTTP request. This may indicate that someone is attempting to have a Web browser execute Java code that opens up a listening socket to circumvent network security measures.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: CVE-2000-0711

HTTP Specifications

Malformed LDAP Traffic

Base Event: LDAP_ASN1_NESTEDSEQUENCE_OVERFLOW

Details: An element of ASN.1 encoded LDAP data overran the size specified by one of its parent data sequence.

References: LDAP RFC 2251

LDAP RFC 2252

LDAP RFC 2253

LDAP RFC 2254

LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ANS1_UNEXPECTED_DATA_AFTER_SEQUENCE

Details: A sequence of LDAP ASN.1 encoded data elements failed to terminate even after all the expected elements had been seen.

References: LDAP RFC 2251

LDAP RFC 2252

LDAP RFC 2253

LDAP RFC 2254

LDAP RFC 2255

Microsoft FrontPage PWS

Base Event: HTTP_URL_SIG15

Details: An attempt to exploit the double-dot bug in Microsoft FrontPage Personal Web Server was detected. This attack may allow an attacker to access system files on an unpatched Web server.

Response: Response typically includes application of a vendor patch to the victim system.

Affected: Microsoft FrontPage servers

False Positives: None known.

References: HTTP Specifications

Mountd Exploit Attempt

Base Event: RPC_MOUNTD_LONG_DIRNAME

Details: The directory name that you are trying to mount is longer than 512 bytes.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0002

RPC Specifications

MS FrontPage Backdoor

Base Event: HTTP_URL_SIG3

Details: An attempt to access a well known back door in Microsoft FrontPage was made. A back door may let an intruder into your system.

Response: Location and audit of client and server is recommended. You should also contact the server vendor for any applicable updates.

Affected: Servers running Microsoft FrontPage.

False Positives: None known.

References: HTTP Specifications

MySQL INC Access

Base Event: HTTP_URL_SIG2

Details: An attempt to access the pcssmysqladm/incs was detected. This indicates an attempt to exploit an ill configured MySQL server that allows for traversal and retrieval of administrative files.

Response: Location and audit of client and server is recommended. You should also contact the server vendor for any applicable updates.

Affected: PCCS-Linux MySQLDatabase Admin Tool 1.2.3,1.2.4;

NOT vulnerable PCCS-Linux MySQLDatabase Admin Tool 1.2.5.

False Positives: None known.

References: CVE-2000-0707

http://www.whitehats.com (arachNIDS #300)

Bugtraq #1557

HTTP Specifications

Nessus Probe

Base Event: HTTP_URL_SIG8

Details: A probe from a Nessus scanner was detected. Nessus is a popular vulnerability assessment scanner. While it is intended for internal audit use, it may be used by attackers to locate exploitable vulnerabilities in your network.

Response: Responses typically include locating the source of the probe.

Affected: No specific targets.

False Positives: None known.

References: Nessus

Netscape Directory Index Bug

Base Event:	HTTP_URL_WPARG
Details:	An attempt was made to exploit the “?wp-c*” Netscape Directory Server info leak bug.
Response:	Location and audit of client and server is recommended. If you intend to use these CGIs you should contact the vendor for any applicable updates.
Affected:	No specific targets.
False Positives:	None known.
References:	CVE-2000-0236 HTTP Specifications

Netscape Overflow

Base Event:	HTTP_BODY_SIG2
Details:	Shell code for well known Netscape client overflow was detected inside the body of an HTTP request. This indicates a possible attempted buffer overflow attack.
Response:	Location and audit of client and server is recommended. You should also contact the client vendor for any applicable updates.
Affected:	No specific targets.
False Positives:	None known.
References:	HTTP Specifications

Nimda Worm A

Base Event: W32_NIMDA_A_MM

Details: The worm takes advantage of a vulnerability in Microsoft IIS which could enable a remote user to execute arbitrary commands. This is due to the handling of CGI filename program requests.

By default IIS performs two separate actions on CGI requests. The first action decodes the filename to determine the file type (for example, .exe, .com, and so forth) and the legitimacy of the file. IIS then carries out a security check. The final process decodes the CGI parameters, which determines whether the file will be processed or not.

The final process includes an undocumented third action: not only does IIS identify the supplied CGI parameters, but it also decodes the previously security check approved CGI filename. Therefore, if a filename composed of escaped characters passes the security check, the second process will unescape the escaped characters contained in the filename, revealing the intended actions. Depending on what the escaped characters represent, varying actions may be performed. For example,

'..%255c' represents '..\', so decoding '..%255c' to '..\' could leverage directory traversal attacks.

The method by which this vulnerability is exploited could allow the execution of arbitrary commands.

Note that these requests are fulfilled in the context of the IUSR_machinename account. An attacker exploiting this vulnerability is able to gain access to the host with these privileges. It may be possible for them to gain further privileges and completely compromise the system from this point.

It has been reported that various encoding combinations under Microsoft Windows 2000 Professional and Server may yield different outcomes.

It has also been reported that Personal Web Server 1.0 and 3.0 is vulnerable to this issue.

The worm Nimda (and variants) actively exploit this vulnerability.

Nimda sends itself out by email, searches for open network shares, attempts to copy itself to unpatched or already vulnerable Microsoft IIS Web servers, and is a virus infecting both local files and files on remote network shares. The worm uses the Unicode Web Traversal exploit to spread to victims surfing an already infected Web server. If you visit a compromised Web server, you will be prompted to download an .eml (Microsoft Outlook Express) email file, which contains the worm as an attachment. When the worm arrives by email, the worm uses a MIME exploit allowing the virus to be executed just by reading or previewing the file.

Response: Please refer to the following link for more information about the worm itself and possible fixtools against it:

Symantec Write-up for W32.Nimda.A@mm

After resolving the issue, try:

- Do not accept communications from unknown hosts.
- Dedicating a separate drive or volume for published content.
- Not running certain services on critical systems, especially those that accept untrusted input.

Affected:	Microsoft IIS 5.0 Microsoft IIS 4.0 Microsoft IIS 3.0 Microsoft Personal Web Server 3.0 Microsoft Personal Web Server 1.0
False Positives:	None known.
References:	Security Focus BID: 1806 CVE-2001-0884 Symantec Write-up for W32.Nimda.A@mm

Nimda Worm E

Base Event: W32_NIMDA_E_MM

Details: The worm takes advantage of a vulnerability in Microsoft IIS which could enable a remote user to execute arbitrary commands. This is due to the handling of CGI filename program requests.

By default IIS performs two separate actions on CGI requests. The first action decodes the filename to determine the file type (for example, .exe, .com, and so forth) and the legitimacy of the file. IIS then carries out a security check. The final process decodes the CGI parameters, which determines whether the file will be processed or not.

The final process includes an undocumented third action: not only does IIS identify the supplied CGI parameters, but it also decodes the previously security check approved CGI filename. Therefore, if a filename composed of escaped characters passes the security check, the second process will unescape the escaped characters contained in the filename, revealing the intended actions. Depending on what the escaped characters represent, varying actions may be performed. For example, '..%255c' represents '..\', so decoding '..%255c' to '..\' could leverage directory traversal attacks.

The method by which this vulnerability is exploited could allow the execution of arbitrary commands.

Note that these requests are fulfilled in the context of the IUSR_machinename account. An attacker exploiting this vulnerability is able to gain access to the host with these privileges. It may be possible for them to gain further privileges and completely compromise the system from this point.

It has been reported that various encoding combinations under Microsoft Windows 2000 Server and Professional may yield different outcomes.

In addition, it was reported that Microsoft Personal Web Server 1.0 and 3.0 is vulnerable to this issue.

The worm Nimda(and variants) actively exploit this vulnerability.

Nimda sends itself out by email, searches for open network shares, attempts to copy itself to unpatched or already vulnerable Microsoft IIS Web servers, and is a virus infecting both local files and files on remote network shares. The worm uses the Unicode Web Traversal exploit to spread to victims surfing an already infected Web server. If you visit a compromised Web server, you will be prompted to download an .eml (Outlook Express) email file, which contains the worm as an attachment. When the worm arrives by email, the worm uses a MIME exploit allowing the virus to be executed just by reading or previewing the file.

Response: Please refer to the following link for more information about the worm itself and possible fixtools against it:

Symantec Write-up for W32.Nimda.E@mm

After resolving the issue, try:

- Not accept communications from unknown hosts.
- Dedicating a separate drive or volume for published content.
- Not running certain services on critical systems, especially those that accept untrusted input.

Affected: Microsoft IIS 5.0
Microsoft IIS 4.0
Microsoft IIS 3.0
Microsoft Personal Web Server 3.0
Microsoft Personal Web Server 1.0

False Positives: None known.

References: Security Focus BID: 1806
CVE-2001-0884
Symantec Write-up for W32.Nimda.E@mm

NNTP Exploit Attempt

Base Event: NNTPCLI_BUFFER_OVERFLOW_ATTEMPT

Details: A possible buffer overflow attempt was detected from a NNTP client. An unchecked buffer exists in the routine that handles logon information in the Cassandra NNTP v1.10 server. Entering a logon name that consists of over 10,000 characters will cause the server to stop responding until the administrator restarts the application.

Response: Audit of the server and verification of product patch level is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: Cassandra NNTP v1.10 server

False Positives: None known.

References: Security Focus BID: 1156
CVE-2000-0341
NNTP Specifications

NPH Test CGI Access

Base Event: HTTP_URL_SIG4

Details: The HTTP request URL attempted to access generic NPH test scripts that were shipped with some versions of apache. This is a concern since many test and demo scripts shipped with Web servers are notorious for not being implemented with an eye towards network security and may be exploited.

Response: Location and audit of client and server is recommended. You should also disable the test scripts on the server.

Affected: No specific targets.

False Positives: None known.

References: CVE-2001-0045
HTTP Specifications

OSPF LSID Attack

Base Event: OSPF_LSID_ATTACK

Details: The link state ID and the advertising router ID of a router-type link state advertisements (LSA) were different. This violation of the RFC is not handled properly by some routing implementations and may cause a segmentation fault in a receiving router.

References: OSPF RFC

Design and Implementation of a Scalable Intrusion Detection System for the Protection of Network Infrastructure

OSPF Max SegNum Attack

Base Event: OSPF_LSA_MAX_SEQNUM

Details: The OSPF message contained a link state advertisement (LSA) with the sequence number set to the maximum allowed value. This situation almost never occurs in normal network traffic. Many routing implementations do not handle purging of records with maximum sequence numbers set and this attack is used to maliciously control the network topology database for up to one hour.

References: OSPF RFC

Design and Implementation of a Scalable Intrusion Detection System for the Protection of Network Infrastructure

Overlong UTF-8 Character

Base Event: HTTP_UTF8_LONG_CHAR

Details: What appears to be an overly long UTF-8 character was detected. This may be an attempt to exploit the Microsoft IIS traversal bug.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

PHF Access

Base Event: HTTP_URL_SIG7

Details: The HTTP request attempted to access a PHF CGI. PHF was a white pages CGI program distributed with some older Web servers. It is known to be easily exploitable and should no longer be in widespread use. This event indicates that a probe for the existence of PHF was detected.

Response: Location and audit of client and server is recommended. You should also disable the PHF CGIs on the server.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0067

PHP mlog Access

Base Event: HTTP_URL_SIG10

Details: An attempt to access the “mlog.phtml” file was detected. The “mlog.phtml” file is an example for the PHP script language. The default examples lack sufficient checking to the input arguments and may be exploited to read all the files accessible to the Web server processes. The scan utility Whisker has been known to attempt access of “mlog.phtml”.

Response: Location and audit of client and server is recommended. You should also disable the mlog.phtml scripts on the server.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0346

HTTP Specifications

POP3 Buffer Overflow

Base Event: POP3_CLIENT_LONG_COMMAND

Details: The POP3 client sent a command that exceeded the maximum permitted length. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Buffer Overflow

Base Event: POP3_SERVER_LONG_LINE

Details: The POP3 server exceeded maximum permitted line length in a response. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 User “root”

Base Event: POP3_USER_ROOT

Details: The POP3 client attempted to log into the POP3 server with the username of “root”. This may be an attempt to access restricted resources or compromise the server.

Rlogin Exploit Attempt

Base Event: RLOGIN_FROOT_EXPLOIT_ATTEMPTED

Details: A logon name of “-froot” was used. This flag is passed to the login program to bypass logon credentials and log in as root on vulnerable hosts.

Response: If seen in sufficient volume or variation audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets

False Positives: None known.

References: CAN-1999-0651

Rlogin Specifications

Rlogin Long TERM Variable

Base Event: RLOGIN_LONG_TERMINAL

Details: The TERM field (terminal type) specified by the client was unusually long. This may indicate an attempt to perform a buffer overflow attack on the server.

Response: If seen in sufficient volume or variation audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets

False Positives: None known.

References: Rlogin Specifications

RSH Exploit Attempt

Base Event: RSH_FROOT_EXPLOIT_ATTEMPTED

Details: A logon name of "-froot" was used. This flag is passed to the login program to bypass logon credentials and log in as root on vulnerable hosts.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: AIX 3.x, Linux kernel.

False Positives: None known.

References: CVE-1999-0113

http://www.whitehats.com (arachNIDS #386)

http://www.whitehats.com (arachNIDS #387)

SMTP Buffer Overflow Attempt

Base Event: SMTP_BUFFER_OVERFLOW_ATTEMPT

Details: An overflow attempt was detected against the SMTP daemon. This usually indicates that an attacker is attempting sendmail overflow attacks. A buffer overflow is usually an attempt to gain access to the system by having the targeted service execute code on the attacker's behalf which modifies the system in some way.

Response: Response typically involves locating the source and verifying if it is a legitimate client or not. If you suspect the attack was successful, an audit of the victim system is also useful.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0203

SMTP Specifications

SMTP Exploit Attempt

Base Event: SMTP_CLIENT_PIPE_EXPLOIT_ATTEMPT

Details: An attempt was made to send mail to an account that started with a pipe ("|"). This may indicate that an attempt is being made to trick the SMTP daemon into executing a local program.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: http://www.whitehats.com (arachNIDS #245)

SMTP Specifications

SMTP HELO Buffer Overflow Attempt

Base Event: SMTP_CLIENT_HELO_BOF

Details: An overflow attempt was detected against the SMTP daemon. This usually indicates that an attacker is attempting sendmail overflow attacks. A buffer overflow is usually an attempt to gain access to the system by having the targeted service execute code on the attacker's behalf which modifies the system in some way.

Response: Response typically involves locating the source and verifying if it is a legitimate client or not. If you suspect the attack was successful, an audit of the victim system is also useful.

Affected: No specific targets.

False Positives: None known.

References: SMTP Specifications

SMTP Overflow Attempt

Base Event: SMTP_PROBABLE_NOOP_BUFFER_EXPLOIT

Details: NO-OP instructions were found in a email recipient's address. This may indicate an attempted buffer overflow attack.

Response: Location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: SMTP Specifications

SMTP Sendmail Header Overflow

Base Event: SMTP_SENDMAIL_BO

Details: Sendmail is a widely used Mail Transfer Agent (MTA) for UNIX and Microsoft Windows systems.

A remotely exploitable vulnerability has been discovered in Sendmail. The vulnerability is due to a buffer overflow condition in the SMTP header parsing component. Remote attackers may exploit this vulnerability by connecting to target SMTP servers and transmitting to them malformed SMTP data.

The overflow condition occurs when Sendmail processes incoming e-mail messages containing malformed address parameters in a field such as "From:" or "CC:". One of the checks to ensure that the addresses are valid is flawed, resulting in a buffer overflow condition. Successful attackers may exploit this vulnerability to gain root privileges on affected servers remotely.

An exploit for this vulnerability is currently circulating on the internet.

Response: Administrators are advised to upgrade to 8.12.8 or apply available patches to prior versions of the 8.x tree.

Affected: Sendmail versions 5.2 to 8.12.7

False Positives: None known.

References: Security Focus BID: 6991
CAN-2002-1337
CERT: CA-2003-07

SNMP Malformed BER/ASN.1 data encoding

Base Event: SNMP_ASN1_DATALENGTH_IMPOSSIBLE_STATE

Details: This represents an internal error and should never occur.

SNMP Malformed BER/ASN.1 data encoding

Base Event: SNMP_ASN1_DATALENGTH_RIDICULOUS_WIDTH

Details: An element of BER encoded ASN.1 data specified an integer larger than 32 bits for the data length. SNMP data should never require numbers this large to describe their length, and indicates either a non-conforming SNMP implementation or an intrusion attempt.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

SNMP Malformed BER/ASN.1 data

Base Event: SNMP_ASN1_DATALENGTH_VALUE_TOO_LARGE

Details: An element of BER encoded ASN.1 data specified a data field size that was too large for its indicated primitive type.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

SNMP Malformed BER/ASN.1 data encoding

Base Event: SNMP_ASN1_INTERNALERROR_OVERREAD_OCTETSTRING

Details: Rare conditions can cause the SNMP traffic analyzer to over read a data field and mis-interpret new data elements as part of the previous data field. In all cases where this is possible the data is mal-formed anyway, and could indicate a possible attack.

Response: Location and audit of victim is recommended.

Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

SNMP Malformed BER/ASN.1 data encoding

Base Event:	SNMP_ASN1_NESTEDSEQUENCE_OVERFLOW
Details:	An element of BER encoded ASN.1 data overran the size set by its parent data sequence.
Response:	Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

SNMP Malformed BER/ASN.1 data encoding

Base Event: SNMP_ASN1_TYPE_ILLEGAL_LONG_ENCODING

Details: A long form BER encoding of an ASN.1 type code was detected. These are not permitted in the subset of BER/ASN.1 used by SNMP.

Response: Location and audit of victim is recommended.

Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

SNMP Malformed BER/ASN.1 data encoding

Base Event:	SNMP_ASN1_TYPE_UNRECOGNIZED
Details:	The data type on an encoded data element was not one of the data types permitted by SNMP.
Response:	Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Sparc NOPs

Base Event: HTTP_BODY_SIG0

Details: Sparc NOP instructions were detected inside the body of an HTTP request. This represents a possible buffer overflow attempt.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Sparc NOPs

Base Event: HTTP_URL_SIG1

Details: Sparc NOP instructions were detected in an HTTP URL. This represents a possible buffer overflow attempt.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Statd Exploit Attempt

Base Event: RPC_STATD_LONG_HOSTNAME

Details: This event is triggered If the host name specified in an RPC statd request is over 512 bytes.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0018

RPC Specifications

Suspicious SNMP Traffic

Base Event: SNMP_ERROR_DATA_AFTER_MESSAGE_END

Details: Additional data was found in a connection after the end of an otherwise normal SNMP message.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_ERROR_INDEX_PAST_END_OF_MSG

Details: The error index pointed to a VarBind pair that does not exist in the current SNMP message.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_INTERNALERROR_IMPOSSIBLE_SNMP_STATE

General: This should be impossible to generate and represents a bad internal error in SNMP decoding.

Suspicious SNMP Traffic

Base Event: SNMP_INVALID_MSGHEADER_MSGFLAGS_SIZE

Details: The data size for the “Message Flags” parameter of the message header data for a V3 SNMP message was indicated to be larger than the allowed size.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_MSGHEADER_OVERLONG_SEQUENCE

Details: The end of a V3 message header was encountered, but the encapsulating BER encoded ASN.1 sequence did not end as expected.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_SCOPEDPDU_OVERLONG_SEQUENCE

Details: The end of a V3 message header was encountered, but the encapsulating BER encoded ASN.1 sequence did not end as expected.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_TOO_MANY_VARBIND_PAIRS

Details: More VarBind pairs were found in a SNMP message than the maximum number allowed. Other fatal errors would be expected to crop up before this since many more VarBind pairs are allowed (2147483647) than is reasonably expected to fit inside a message.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_SNMP_MESSAGE

Details: The primitive type for the top level SNMP message did not match any of the expected data types for that parameter. This essentially means the SNMP traffic is totally unrecognizable as such.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_VERSION

Details: The primitive type for the SNMP version did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_VARBIND_PAIR_OVERLONG_SEQUENCE

Details: The end of a VarBind pair was encountered, but the encapsulating BER encoded ASN.1 sequence did not end as expected.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Telnet LD Exploit

Base Event: TELNET_LD_ENVIRONMENT

Details: LD environment variables were detected in a Telnet session. LD environment variables are used to fool insecure remote hosts into loading alternatives to system libraries. This may be an attempt to compromise the victim system.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: Can-1999-0073
http://www.whitehats.com (arachNIDS #367)
Telnet Specifications

Telnet RESOLV Exploit

Base Event: TELNET_RESOLV_ENVIRONMENT

Details: An attempt was made to influence the resolver libraries on the remote host through the passing of RESOLVE* environment variables. This event is very similar to the TELNET_LD_ENVIRONMENT event. LD environment variables are used to fool insecure remote hosts into loading alternatives to system libraries. This is an attempt to compromise the victim system.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: http://www.whitehats.com (arachNIDS #304)

Telnet Specifications

Telnet RLD Exploit

Base Event: TELNET_SGI_FMTSTRING_VULN

Details: An attempt to exploit SGI format string vulnerabilities exposed through RLD_* environment variables was detected. This is an attempt to compromise the victim system.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References: CVE-2000-0733

http://www.whitehats.com (arachNIDS #304)

Telnet Specifications

Test CGI Access

Base Event: HTTP_URL_SIG6

Details: The HTTP request URL attempted to probe for the existence of well known test CGIs. This is a concern since many test and demo scripts shipped with Web servers are notorious for not being implemented with an eye towards network security and are known to be exploitable.

Response: Location and audit of client and server is recommended. You should also disable the test scripts on the server.

Affected: No specific targets.

False Positives: None known.

References: CVE-2000-0070

http://www.whitehats.com (arachNIDS #218)

http://www.whitehats.com (arachNIDS #224)

Bugtraq #686

Bugtraq #2003

HTTP Specifications

WARFtpd Literal Exploit

Base Event: FTP_WARFTPD_MACROS

Details: WarFTPd ships with various macros to assist in setting up complex FTP sites.

It is possible to remotely call these macros, some of which are used to compromise the server. Some of these macros provide server and operating system information. They can also be used to reveal the file contents in error messages, including the configuration files for WarFTP, which can also include plaintext administrator passwords.

The extent of the vulnerability differs between versions of WarFTPd:

Version 1.67b2, and prior:

Authenticated users can gain access to the restricted files.

Version 1.70:

Remote attackers can gain access to any file on the system, as well as run any system command with administrative privileges, if an ODBC driver is installed. This is done without being logged on to the FTP server.

Response: Patches have been provided for both v1.70 and v1.67b2 or older, available at:

http://war.jgaa.com/alert/

and:

ftp://ftp.no.jgaa.com/

Affected: Jgaa WarFTPd 1.67b2 and prior

Jgaa WarFTPd 1.70b

False Positives: None known.

References: Security Focus BID: 919

CVE-2000-0044

Jgaa Support Site

SECURITY ALERT - WARFTP DAEMON ALL VERSIONS

WarFTP Homepage

Webcom Guestbook Access

Base Event: HTTP_URL_SIG12

Details: An attempt to access the webcom guestbook CGI file was detected. There is a known vulnerability in this freeware guestbook CGI. Exploits make requests to either rguest.exe or wguest.exe on the Web server to gain access to files the Web server can access.

Response: Location and audit of client and server is recommended. If you intend to use these CGIs you should contact the vendor for any applicable updates.

Affected: WebCom datakommunikation Guestbook 0.1.

False Positives: None known.

References: CVE-1999-0467

Bugtraq #2024

HTTP Specifications

Web Phorum Backdoor

Base Event: HTTP_REQMSGHDR_SIG1

Details: An indicator of a Web Phorum backdoor was detected in an HTTP header. The cookie “php_auth_user=boogieman” granted administrator access to the Phorum, potentially even to the system.

Response: Location and audit of client and server is recommended. If you intended to be using this product you should contact the vendor for any applicable updates.

Affected: No specific targets.

False Positives: None known.

References: HTTP Specifications

Operational events

Sensor Data Read Error

Base Event: SENSOR_SNIFF_DATA_BAD

Details: A sensor has failed to properly parse its data file. The sensor will not start up if it cannot properly parse this file.

Sensor Device Open Failure

Base Event: SENSOR_IFDEVOPEN_FAILURE

Details: A sensor has failed to open an interface device. Check to make sure that the device name was properly entered in the console.

Sensor Error On Exit

Base Event: SENSOR_ERROREXIT_FAILURE

Details: A sensor has exited with a non-zero error code. This may indicate a problem with the system or configuration.

Sensor Memory Allocation Error

Base Event: SENSOR_MALLOC_FAILURE

Details: A sensor has failed to allocate needed memory on start-up. Possible causes are the system does not have the recommended minimum amount of RAM or that extraneous processes are running.

Sensor Portmap Read Error

Base Event: SENSOR_PORTMAP_BAD

Details: A sensor has failed to properly parse the port mapping configuration file. The sensor will not start up if it cannot properly parse this file.

Sensor Record File Open Failure

Base Event: SENSOR_RCRDINIT_FAILURE

Details: A traffic recording sensor has exited due to a failure to open the file for recorded traffic. Check to make sure that the system has sufficient free disk space.

Probes

DNS Probing

Base Event: DNS_BIND_HESIOD

Details: A bind HESIOD query was made. You can use these to mine data from the running version bind.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References: DNS Specifications

Finger Probing

Base Event: FINGER_ONLYNUMERIC_REQUEST

Details: A numeric finger request was detected. Numeric finger requests are generally an attempt to probe for user accounts.

Response: If seen in sufficient volume or variation location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0612
http://www.whitehats.com (arachNIDS #376)
Finger Specifications

Finger Probing

Base Event: FINGER_ROOT_REQUEST

Details: A finger request was issued for root. This generally represents an attempt at information probing.

Response: If seen in sufficient volume or variation location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0612
http://www.whitehats.com (arachNIDS #376)
Finger Specifications

Finger Probing

Base Event: FINGER_SEARCH_REQUEST

Details: This generally represents an attempt at information probing.

Response: If seen in sufficient volume or variation location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: CVE-1999-0612
http://www.whitehats.com (arachNIDS #375)
Finger Specifications

FTP Probing

Base Event: FTPCLI_ADMHACK_SCAN

Details: An “adm hack” FTP scan was detected. This is likely an information gathering attempt.

Response: Location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: http://www.whitehats.com (arachNIDS #375)
FTP Specifications

FTP Probing

Base Event: FTPCLI_ISS_SCAN

Details: An FTP scan by ISS Internet Scanner was detected. ISS Scanner is a system administration tool intended to aid in diagnosing security risks. An attacker may use it to gather vulnerability information about your systems.

Response: Location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: FTP Specifications

FTP Probing

Base Event: FTPCLI_RETR_PASSWD

Details: An attempt to retrieve the password file was detected. The RETR command was issued with the string “passwd” in the argument. This indicates someone attempting to use FTP to copy your password file (usually for later cracking).

Response: Location and audit of client is recommended. If the FTP server logs indicate a successful transfer of the password file, presume it’s cracked. All users listed in that password file should immediately change their passwords.

Affected: No specific targets.

False Positives: None known.

References: http://www.whitehats.com (arachNIDS #375)

http://www.whitehats.com (arachNIDS #375)

FTP Specifications

FTP Probing

Base Event: FTPCLI_SAINT_SCAN

Details: An FTP scan from Saint was detected (a “PASS” was issued with the string “-saint@” in the argument). Saint is a system administration tool intended to aid in diagnosing security risks. It is used by attackers to gather vulnerability information about your systems.

Response: Location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

FTP Probing

Base Event: FTPCLI_SATAN_SCAN

Details: An FTP scan from SATAN was detected (a “PASS” was issued with the string “-satan@” in the argument). SATAN is a system administration tool intended to aid in diagnosing security risks. Attackers use it to gather vulnerability information about your systems.

Response: Location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: http://www.whitehats.com (arachNIDS #329)

Portscan

Base Event: COUNTER_TCP_PORTSCAN

Details: A TCP port scan was detected. A port scan is typically an information gathering or probing attempt. An attacker will use a scan to determine which network ports have programs listening on them. An attacker can also identify the application and target operating system. This information is used to focus subsequent attacks.

Port scans may vary in method and timing. An attacker often uses these variations in an attempt to evade or penetrate defensive measures such as security gateways or intrusion detection systems. Port scans are detected by monitoring patterns in TCP connection activity in a given network and observing activity characteristic of a port scan.

Response: Responses to TCP port scans typically include locating the source of the scan and identifying the operator. Note that in many scans some of the source addresses are forged to make the location effort more difficult. If the origin of the scan appears to cross a security gateway or other perimeter filter, responses may also include review and modification of that devices configuration to prevent future successful scanning attempts.

Affected: No specific targets.

False Positives: It is possible for some legitimate network management tools which perform network probing to be detected as port scans.

Portscan

Base Event: COUNTER_UDP_PORTSCAN

Details: A UDP port scan was detected. A port scan is typically an information gathering or probing attempt. An attacker will use a scan to determine which network ports have programs listening on them. They may also be able to identify the application and target operating system. This information is used to focus subsequent attacks.

Port scans may vary in method and timing. An attacker often uses these variations in an attempt to evade or penetrate defensive measures such as security gateways and intrusion detection systems. UDP port scans are detected by monitoring patterns in UDP connection activity and corresponding ICMP unreachable errors in a given network and observing activity characteristic of a port scan.

Response: Responses to UDP port scans typically include locating the source of the scan and identifying the operator. Note that in many scans some of the source addresses are forged to make the location effort more difficult. If the origin of the scan appears to cross a security gateway or other perimeter filter, responses may also include review and modification of that devices configuration to prevent future successful scanning attempts.

Affected: No specific targets.

False Positives: It is possible for some legitimate network management tools which perform network probing to be detected as port scans.

Portsweep

Base Event: COUNTER_TCP_PORTSWEEP

Details: A TCP port sweep has been detected. TCP port sweeps are used to determine if a particular port is open on a set of machines and is used to focus subsequent attacks. A sweep is essentially a port scan of a set of machines (usually a range of IP addresses) looking for one particular service (for example, a Web server).

Response: Responses to port sweeps typically include locating the source of the scan and identifying the operator. Note that in many scans some of the source addresses are forged to make the location effort more difficult. If the origin of the scan appears to cross a security gateway or other perimeter filter, responses may also include review and modification of that devices configuration to prevent future successful scanning attempts.

Affected: No specific targets.

False Positives: It is possible for some legitimate network management tools to be detected as port sweeps.

Portsweep

Base Event: COUNTER_UDP_PORTSWEEP

Details: A UDP port sweep has been detected. UDP port sweeps are used to determine if a particular port is open on a set of machines and is used to focus subsequent attacks. A sweep is essentially a port scan of a set of machines (usually a range of IP addresses) looking for one particular service (for example, a DNS server).

Response: Responses to port sweeps typically include locating the source of the scan and identifying the operator. Note that in many scans some of the source addresses are forged to make the location effort more difficult. If the origin of the scan appears to cross a firewall or other perimeter filter, responses may also include review and modification of that devices configuration to prevent future successful scanning attempts.

Affected: No specific targets.

False Positives: It is possible for some legitimate network management tools to be detected as port sweeps.

SMTP Probing

Base Event: SMTP_CLIENT_CYBERCOP_SECURITY_SCAN

Details: A Cybercop SMTP scan was detected.

Response: Location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References: CAN-1999-0531
http://www.whitehats.com (arachNIDS #371)
http://www.whitehats.com (arachNIDS #372)

SMTP Probing

Base Event: SMTP_ROOT_INFO_GATHERING_ATTEMPT

Details: An attempt to gather information about the root account through EXPN was detected.

Response: The EXPN command should be either disabled or restricted on the server. If seen in volume or variation location and audit of client is recommended.

Affected: No specific targets.

False Positives: None known.

References CVE-1999-0531
http://www.whitehats.com (arachNIDS #31)
SMTP Specifications

Signatures

BD DeepThroat Activity

Base Event:

Details: DeepThroat is a backdoor program that affects Microsoft Windows 9x and NT machines. It includes an FTP server and various controls that allow malicious actions, such as passwords theft and remote screenshot captures.

DeepThroat consists of a client program called “DeepThroat Remote Control” which is run on a remote computer to gain access to any computer on the network. In this case, an executable server program must be installed on the victim’s computer to permit remote access to the victim’s computer in a manner similar to Netbus, BackOrifice and other internet “Remote administration” Trojan horses.

Response: Users should keep current on virus definitions and continue to monitor for DeepThroat on the network using a commercial intrusion detection system (IDS).

Affected: Microsoft Windows 9x and NT Machines.

False Positives: None known.

References CAN-1999-0660

HTTP CGI Count Request

Base Event:

Details: Wwwcount (count.cgi) is a very popular CGI program used to track Web site usage that enumerates the number of hits on given Web pages and increments them on a 'counter'. In October of 1997 two remotely exploitable problems were discovered with this program. The first problem, though somewhat innocuous in that it only allowed remote users to view .gif files to which they were not supposed to have access. The danger is these .gif files contain sensitive data relating to demographics and finances.

The second and more serious problem is a buffer overflow in QUERY_STRING environment variable handled by the program. In essence, a remote user can send an overly long query to the program, overflow a buffer and execute their own commands at whatever privilege level the program is running as.

Response: If you are running version 2.3 of Wwwcount it is suggested you upgrade immediately. In the meantime you may wish to consider removing the execution bit on this program.

Affected: Muhammad A. Muquit wwwcount 2.3

False Positives: None known.

References CVE-1999-0021

Security Focus BID: 128

Security Focus Advisory: 171

HTTP FormMail Command Exec

Base Event: FORMMAIL_COMMAND_EXEC

Details: Matt Wright's FormMail is a Web-based email gateway. In versions 1.9 and earlier, the "recipient" hidden field is not checked for the semi-colon(;), the shell command separation character. This enables remote arbitrary command execution.

Response: Upgrade to a newer version.

Affected: Matt Wright FormMail 1.9 and earlier.

False Positives: None known.

References CVE-1999-0172

Security Focus BID: 2079

HTTP Htgrep CGI File Access

Base Event: HTGREP_CGI_FILE_ACCESS

Details: Htgrep CGI program lets remote attackers read arbitrary files by specifying the full pathname in the hdr parameter.

Response: Make sure that you are using the latest set of definitions to prevent such attacks.

Affected: Microsoft Windows NT, UNIX and Linux. (all versions).

False Positives: This signature may produce false positives when any legitimate traffic that attempts to use htgrep in a similar manner as the vulnerability.

References CAN-2000-0832

HTTP IIS ISAPI Extension

Base Event:

Details: The worm uses a buffer overflow vulnerability in the idq.dll, which runs at the System security level, when handling URL requests. Once an attacker establishes a session on the Web server and causes a buffer to overflow, that attacker could perform virtually any function on that server.

Response: Contact Microsoft for the latest patches.

Affected: Microsoft IIS 4.0 and 5.0

Microsoft Personal Web Server 4.0

Microsoft Index Server 2.0

Indexing Service in Windows 2000

False Positives: This signature can produce false positives when users give commands with tilde (~) characters.

References Security Focus BID: 2880

CVE-2001-0500

Microsoft Security Bulletin: MS01-033

Symantec Security Response: CodeRed Worm

HTTP MDAC IIS Component Query

Base Event: HTTP_MDAC_QUERY

Details: Microsoft Data Access Components (MDAC) contains a buffer overflow vulnerability in a Remote Data Services (RDS) component. The server side RDS component affected is called the RDS Data Stub, while the client side is called the Data Space control.

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code, or at the very least, cause a denial-of-service.

Response: Contact Microsoft for the latest patches.

Affected: Microsoft Data Access Components (MDAC) 2.1

Microsoft Data Access Components (MDAC) 2.5

Microsoft Data Access Components (MDAC) 2.6

Microsoft Internet Explorer 5.01

Microsoft Internet Explorer 5.5

Microsoft Internet Explorer 6.0

False Positives: None known.

References CAN-2002-1142

Microsoft Security Bulletin: MS02-065

CERT Advisory: CA-2002-33

HTTP MS IIS TranslateF Request

Base Event:

Details: Microsoft IIS 5.0 lets remote attackers obtain source code for .ASP files and other scripts by means of an HTTP GET request with a “Translate: f” header, also known as the “Specialized Header” vulnerability.

Microsoft IIS 5.0 has a dedicated scripting engine for advanced file types such as ASP, ASA, HTR, and so forth. The scripting engines handle requests for these file types, processes them accordingly, and then executes them on the server.

It is possible to force the server to send back the source of known scriptable files to the client if the HTTP GET request contains a specialized header with ‘Translate: f’ at the end of it, and if a trailing slash ‘/’ is appended to the end of the URL. The scripting engine will locate the requested file, however, it will not recognize it as a file that needs to be processed and will proceed to send the file source to the client.

Response: Contact Microsoft for the latest patches.

Affected: Microsoft IIS 5.0

False Positives: This signature can produce false positives when users give commands with tilde (~) characters.

References Security Focus BID: 1578

CVE-2000-0778

Microsoft Security Bulletin: MS00-033

HTTP Tomcat Cross Site Scripting

Base Event: TOMCAT_CROSS_SITE

Details: Apache Tomcat is a freely available, open source Web server maintained by the Apache Foundation. It is available for use on UNIX and Linux variants as well as Microsoft Windows operating environments. A vulnerability has been reported for Apache Tomcat 4.0.3 on Microsoft Windows and Linux platforms. Reportedly, it is possible for an attacker to launch a cross site scripting attack.

When servlet mapping is enabled, it is possible to invoke various servlets and cause Apache Tomcat to throw an exception. This will make cross site scripting attacks possible.

The ‘invoker’ servlet is mapped to ‘/servlet/’. This mapping allows for the execution of anonymous servlet classes that have not been defined in the file, /tomcat-install-dir/conf/web.xml.

This may enable a remote attacker to steal cookie-based authentication credentials from legitimate users of a host running Apache Tomcat.

Response: Use proxy servers to filter untrusted traffic. Filtering scripts from inappropriate sources is a good policy, but you should design rules with care to ensure they not only allow acceptable activity but are also effective. You should ensure that the filtering rules and/or underlying software recognize URL encoded characters, unexpected combinations of characters, or extra whitespace, for example. Try to make rule sets as comprehensive (or non-specific) as possible without affecting acceptable usage.

Set Web browser security to disable the execution of script code or active content. If it is not required, disable Java Script (and other script) execution in your Web browser. This is particularly crucial on systems used for maintenance of your infrastructure, production workstations, etc.

Deploy network intrusion detection systems to monitor network traffic for malicious activity. As a part of a comprehensive security policy, you should monitor for unexpected behavior occurring on your network and inspect all instances to determine the source and purpose. Types of activity that should be monitored include: unexpected changes in network performance such as variations in traffic load at specified times; traffic coming from or going to unexpected locations; connections made at unusual times; repeated, failed connection attempts; unauthorized scans and probes; non-standard or malformed packets (protocol violations). It is important to regularly audit logs.

Affected:	Apache Software Foundation Tomcat 4.0.3
False Positives:	None known.
References	CAN-2002-0682 Security Focus BID: 5193

Info2www CGI Command Exec

Base Event:	INFO2WWW_CGI_CMD_EXEC
Details:	The info2www script allows HTTP access to information stored in GNU EMACS Info Nodes. This script fails to properly parse input and is used to execute commands on the server with permissions of the Web server, by passing commands as part of a variable. Potential consequences of a successful exploitation involve anything the Web server process has permissions to do, including possibly Web site defacement.
Response:	Version 1.2 of the script does not suffer from this issue. Upgrade to the latest version.
Affected:	Roar Smith info2www 1.0 to 1.1.
False Positives:	None known.
References	CVE-1999-0266 Security Focus BID: 1995

MSSQL NULL Packet DOS

Base Event:	MSSQL_NULL_PACKET_DOS
Details:	If Microsoft SQL Server 7.0 receives a TDS header with three or more NULL bytes as data it will crash. The crash will generate an event in the log with ID 17055 “fatal exception EXCEPTION_ACCESS VIOLATION”.
Response:	Contact Microsoft for the latest updates.
Affected:	Microsoft SQL Server 7.0
False Positives:	None known.
References	Microsoft Security Bulletin: MS-059

MSSQL StackOverflow

Base Event: MSSQL_STACKOVERFLOW

Details: A vulnerability was discovered in Microsoft SQL Server 2000 that could allow remote attackers to gain access to the target hosts.

A problem in the SQL Server Resolution Service makes it possible for a remote user to execute arbitrary code on a vulnerable host. An attacker could exploit a stack-based overflow in the resolution service, by sending a maliciously crafted UDP packet to port 1434.

UDP port 1434 is designated as the Microsoft SQL Monitor port. Clients connect to this port to discover how connections to the SQL Server should be made. When the SQL Server receives a packet starting with byte 0x04, followed by four “A” characters, the SQL server attempts to open the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion.

If a large number of bytes are appended to the packet, the buffer overflow condition is triggered, and as a result, the attacker can overwrite the key areas in memory and obtain control over the SQL Server process. Custom crafting the exploit code to execute the arbitrary instructions in the security context of the SQL Server may be possible. This action may provide a remote attacker with local access on the underlying host.

The W32.SQLEXP.Worm Microsoft SQL Server exploited this vulnerability.

Response: Contact Microsoft for the latest updates.

Affected: Microsoft Data Engine 2000

Microsoft SQL Server 2000 SP2

Microsoft SQL Server 2000 SP1

Microsoft SQL Server 2000

False Positives: None known.

References CAN-2002-0649

Security Focus BID: 5311

Symantec Security Response: W32.SQLExp.Worm

Microsoft Security Bulletin: MS-039

WuFTPd Heap Overflow

Base Event:

Details: A remote user can cause a heap overflow in wu-ftpd by sending a specially crafted sequence of commands to it. This vulnerability affected a large number of UNIX vendors.

Response: Contact your vendor for a patch.

Affected: Versions of wu-ftpd prior to 2.6.2.

False Positives: This signature can produce false positives when users give commands with tilde (~) characters.

References Security Focus BID: 3581

CVE-2001-0550

Red Hat Advisory

Suspicious activity

BGP Authentication Failure

Base Event: BGP_AUTH_FAILURE

Details: A BGP authentication failure was detected. This is an indication that an attack is being launched on the network routers.

References BGP Specifications

BGP Generic Error

Base Event: BGP_GENERIC_ERROR_CONDITION

Details: A BGP NOTIFICATION message, indicating a protocol error condition, was detected. This is an indication that an attack is being launched on the network routers.

References BGP Specifications

BGP Invalid AGGREGATOR Length

Base Event: BGP_UPDATE_AGGREGATOR_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid AGGREGATOR length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid ASPATH Length

Base Event: BGP_UPDATE_ASPATH_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid ASPATH length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Attribute Flags

Base Event: BGP_BAD_ATTRIBUTE_FLAGS

Details: The lower four bits of the attribute flags field in a BGP UPDATE message must be set to zero, but were not. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Capability Length

Base Event: BGP_OPEN_INVALID_CAPABILITY_LENGTH

Details: The BGP OPEN message capability field had a field length disallowed by the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid COMMUNITIES Length

Base Event: BGP_UPDATE_COMMUNITIES_BAD_LENGTH

Details: The BGP OPEN message capability field had a field length disallowed by the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Hold Time

Base Event: BGP_INVALID_HOLD_TIME

Details: The BGP OPEN message advertised a hold time that falls outside the allowed range of values. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid LOCAL_PREF Length

Base Event: BGP_UPDATE_LOCAL_PREF_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid ATOMIC_AGGREGATE length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid KEEPALIVE Message Length

Base Event: BGP_BAD_KEEPALIVE_MSG_LENGTH

Details: The BGP KEEPALIVE message length was outside the limitations specified in the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Marker

Base Event: BGP_BAD_MARKER

Details: The BGP OPEN message marker has to consist of all 1s (0xFF), but a different marker was sent. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Marker

Base Event: BGP_OPEN_CAPABILITY_LENGTH_MISMATCH

Details: The BGP OPEN message capability length was invalid. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Message Length

Base Event: BGP_BAD_MSG_LENGTH

Details: The BGP message length was outside the limitations specified in the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid MULTI_EXIT_DISC Length

Base Event: BGP_UPDATE_MULTI_EXIT_DISC_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid MULTI_EXIT_DISC length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Network Reachability Length

Base Event: BGP_UPDATE_NETWORK_REACH_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid Network Reachability length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Next Hop Length

Base Event: BGP_UPDATE_NEXT_HOP_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid NEXT_HOP length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid NOTIFICATION Message Length

Base Event: BGP_BAD_NOTIFICATION_MSG_LENGTH

Details: The BGP NOTIFICATION message length was outside the limitations specified in the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid OPEN Message Length

Base Event: BGP_BAD_OPEN_MSG_LENGTH

Details: The BGP OPEN message length was outside the limitations specified in the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Origin Length

Base Event: BGP_UPDATE_ORIGIN_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid ORIGIN length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Origin Value

Base Event: BGP_UPDATE_ORIGIN_INVALID_VALUE

Details: The BGP UPDATE message contained an invalid ORIGIN value. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid ORIGINATOR_ID Length

Base Event: BGP_UPDATE_ORIGINATOR_ID_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid ORIGINATOR_ID length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Path Attribute Length

Base Event: BGP_PATH_ATTRIBUTE_BAD_LENGTH

Details: The BGP UPDATE message contained an invalid path attribute length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid PATHSEG Length

Base Event: BGP_UPDATE_ASPATH_BAD_PATHSEGLEN

Details: The BGP UPDATE message contained an invalid PATHSEG length in the ASPATH path attribute. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid PATHSEGTYPE

Base Event: BGP_UPDATE_ASPATH_BAD_PATHSEGTYPE

Details: The BGP UPDATE message contained an invalid PATHSEGTYPE in the ASPATH path attribute. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid ROUTE REFRESH Message Length

Base Event: BGP_BAD_ROUTE_REFRESH_LENGTH

Details: The BGP message length was outside the limitations specified in the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Unknown Message Type

Base Event: BGP_UNKNOWN_MSG_TYPE

Details: The BGP message type falls outside the possible range of values specified by the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid UPDATE Message Length

Base Event: BGP_BAD_UPDATE_MSG_LENGTH

Details: The BGP UPDATE message length was outside the limitations specified in the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Invalid Withdrawn Route Length

Base Event: BGP_BAD_WITHDRAWN_ROUTE_LENGTH

Details: The BGP UPDATE message contained an invalid withdrawn route length. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Negative LOCAL_PREF

Base Event: BGP_UPDATE_NEG_LOCAL_PREF

Details: The BGP UPDATE message had the high-order bit set on the LOCAL_PREF field. Some routers may interpret this field as negative, leading to invalid route tables.

References BGP Specifications

BGP Negative MULTI_EXIT_DISC

Base Event: BGP_UPDATE_NEG_MULTI_EXIT_DISC

Details: The BGP UPDATE message had the high-order bit set on the MULTI_EXIT_DISC field. Some routers may interpret this field as negative, leading to invalid route tables.

References BGP Specifications

BGP Possible Buffer Overflow

Base Event: BGP_OVERLONG_OPT_PARAMS

Details: The length of the optional parameters included in the BGP OPEN message is longer than allowed. This violation of the standard could indicate an attempt to compromise the protocol.

References BGP Specifications

BGP Unauthenticated Connection

Base Event: BGP_NONAUTH_CONNECTION

Details: The BGP version number was not 4. BGP4 is the current Internet standard, and use of a BGP version other than 4 is suspicious.

References BGP Specifications

BGP Unsupported Version Number

Base Event: BGP_UNSUPPORTED_VERSION_NUM

Details: The BGP version number was not 4. BGP4 is the current Internet standard, and use of a BGP version other than 4 is suspicious.

References BGP Specifications

DNS Malformed Data

Base Event: DNS_INVALID_ADDRLEN

Details: In the additional record section of a DNS packet an IPv4 address was detected that was not 4 bytes long.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References DNS Specifications

DNS Malformed Data

Base Event: DNS_INVALID_TTL

Details: A TTL (Time To Live) value larger than the maximum legal value according to the RFC was detected in a DNS packet.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References DNS Specifications

DNS Malformed Data

Base Event: DNS_DATA_AFTER_END

Details: Extra data was sent after a valid DNS packet. Probably an overflow attempt.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References DNS Specifications

DNS Malformed Data

Base Event: DNS_PACKET_OVERRUN

Details: Extra data was sent after a valid DNS packet. This represents a possible overflow attempt.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References DNS Specifications

DNS Malformed Data

Base Event:	DNS_RUNT_PACKET
Details:	Over TCP DNS this event indicates that a DNS packet specified a packet length that was shorter than the DNS packet header.
Response:	If seen in sufficient volume or variation location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.
Affected:	No specific targets.
False Positives:	None known.
References	DNS Specifications

FaxSurvey CGI Passwd Access

Base Event:	HTTP_FAXSURVEY_ACCESS
Details:	Hylafax is a popular Fax server software package designed to run on multiple UNIX operating systems. Unpatched versions of Hylafax ship with an insecure script, Faxsurvey, which allows for remote command execution, with the privileges of the Web server process. This vulnerability is exploited by passing the command as a parameter to the script. See the exploit for further details. Consequences could include Web site defacement, exploitation of locally accessible vulnerabilities to gain further privileges, and so on.
Response:	Disable the affected script and/or upgrade to a newer version of Hylafax.
Affected:	Hylafax Hylafax 4.0pl2.
False Positives:	None known.
References	Security Focus BID: 2056 Hylafax Homepage

Finger Malformed Data

Base Event:	FINGER_BAD_REQUEST
Details:	A request was made that wasn't a finger request.
Response:	If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.
Affected:	No specific targets.
False Positives:	None known.
References	Finger Specifications

Finger Malformed Data

Base Event: FINGER_EXCESS_DATA

Details: Extra data was sent after a valid finger request. This represents a possible birds of a feather (BOF) attack or that a shell has been spawned.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Finger Specifications

FTP Auth Failure

Base Event: FTPSER_NOT_LOGGED_IN

Details: An FTP operation occurred with the user not logged in. This event is used to catch everything from FTP logon failures to sending FTP commands to the server before a valid logon has been established.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

FTP High-Bit ASCII

Base Event: FTP_INVALID_UTF8_HIGH_ASCII

Details: Traffic that violates the FTP RFC was detected. This is likely the result of an FTP client or server that does not conform to the FTP standard sending high-bit ASCII characters (possibly non-English filenames) without encoding them with UTF-8.

FTP Malformed Data

Base Event: FTP_BAD_PORT_CMD_ARG

Details: An invalid argument to the FTP PORT command was detected. This could indicate an attempt to compromise the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible the client or server is using an unofficial extension or a non-compliant implementation of FTP.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_BAD_PORT_CMD_IPNUM

Details: An invalid IP address argument to the FTP PORT command was detected. This could indicate an attempt to compromise the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible the client or server is using an unofficial extension or a non-compliant implementation of FTP.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_BAD_RANDOM_COMMAND

Details: A FTP command was sent to the server that was not composed of alphabetic characters. No FTP commands should be composed of non-alphabetic characters. This may indicate a compromised server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible this is a client or server using an unofficial extension or non-compliant implementation.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_INVALID_UTF8

Details: Invalid UTF-8 character encoding has been detected in an FTP session. Bytes in a UTF-8 character after the character length specification fall into a limited range; this event is recorded if these encoding characters fall outside that range. It is possible this indicates an attempt to compromise the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant UTF-8 encoding implementation.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_LONG_COMMAND

Details: An FTP command was sent which was longer than eight bytes. No FTP commands should be longer than eight bytes. This may indicate a compromised server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible this is a client or server using an unofficial extension or non-compliant implementation.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_PORT_CMD_TOO_MANY_ARGS

Details: Invalid arguments to the FTP PORT command was detected. This could indicate an attempt to compromise the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible the client or server is using an unofficial extension or a non-compliant implementation of FTP.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_RNTO_WITHOUT_RNFR

Details: An FTP RNTO command was detected without a corresponding RNFR command. This is unusual behavior.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

FTP Malformed Data

Base Event: FTP_UNRECOGNIZED_COMMAND

Details: An unrecognized FTP command was sent to the FTP server. This could indicate a compromised server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible the client or server is using an unofficial extension or a non-compliant implementation of FTP.

References FTP Specifications

FTP Malformed Data

Base Event: FTPCLI_EXPECTED_ALLORESP

Details: A storage or append operation should immediately follow an FTP ALLO command, but something else was sent. It is possible this indicates an attempt to compromise the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

FTP Malformed Data

Base Event: FTPCLI_EXPECTED_CRLF

Details: An FTP command was not properly terminated. According to the RFC, a pair of CR/LF characters is expected at this point from the FTP client. For example, the CR/LF should appear after the client issues commands like “CDUP,” “REIN,” “QUIT,” “PASV,” or “ABOR,” which do not take any arguments, or commands like “STRU,” “MODE,” or “TYPE,” and the legal values for their arguments. This event is triggered if something else was sent.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible that this is a non-compliant server implementation of FTP.

References FTP Specifications

FTP Malformed Data

Base Event: FTPCLI_EXPECTED_LF

Details: An FTP was not properly terminated. According to the RFC, a pair of CR/LF characters is expected at this point from the FTP client. For example, the CR/LF should appear after the client issues commands like “CDUP,” “REIN,” “QUIT,” “PASV,” or “ABOR,” which do not take any arguments, or commands like “STRU,” “MODE,” or “TYPE,” and the legal values for their arguments. This event is triggered if something other than the LF character was sent after the CR character.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible that this is a non-compliant server implementation of FTP.

References FTP Specifications

FTP Malformed Data

Base Event: FTPCLI_EXPECTED_RNTO

Details: A RNFR command was sent, but was followed by something other than a RNTO command.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

FTP Malformed Data

Base Event: FTPCLI_SENT_CEL_COMMAND

Details: A “CEL” command was sent from an FTP client. This command is usually not implemented.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

FTP Malformed Data

Base Event: FTPSER_AUDIOGALAXY_EXTRA_AFTER_IP

Details: Audio galaxy is another protocol that operates on the FTP port. Audio galaxy is only supposed to send an IP address and disconnect. This event is generated when extra data is sent after the IP address.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command. If you do not intend to allow tunneling through FTP in your network you may also want to add some network filters.

Affected: No specific targets.

False Positives: It is possible this is some unexpected change to or variation in Audio galaxy.

References Audio Galaxy

FTP Specifications

FTP Malformed Data

Base Event: FTPSER_EXPECTED_LF

Details: An FTP command was sent without the proper line termination.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

FTP Malformed Data

Base Event: FTPSER_UNKNOWN_RESPONSE_FROMUNKNOWN

Details: Server sent something that didn't start with a numeric, which is outside the FTP protocol specification. It is possible this indicates an attempt to compromise the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References FTP Specifications

HSRP Buffer Overflow

Base Event: HSRP_OVERLONG_PACKET

Details: The HSRP datagram exceeded the length mandated by the RFC, indicating a possible buffer overflow attack. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HSRP Coup

Base Event: HSRP_COUP

Details: An HSRP Coup message indicates that a new router has assumed the role of the active router. This may indicate a change in router status. If seen in sufficient volume, it may indicate a problem with the routers or that an attack is being launched.

References HSRP Specifications

HSRP Inconsistent State

Base Event: HSRP_WRONG_STATE_FOR_SPEAKING

Details: According to the HSRP RFC, only a router in the Listen, Speak, Standby, or Active states may send out an HSRP message. However, an HSRP message was detected from a router that is in Initial or Learn states. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HSRP Inconsistent Time Fields

Base Event: HSRP_HOLDTIME_GT_HELLOTIME

Details: The HSRP HOLDTIME field was less than the HELLOTIME field, which is explicitly disallowed by the RFC. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HSRP Invalid Opcode

Base Event: HSRP_INVALID_OPCODE

Details: An invalid opcode field was detected in an HSRP datagram. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HSRP Invalid State

Base Event: HSRP_INVALID_STATE

Details: An invalid state field was detected in an HSRP datagram. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HSRP Invalid TTL Field

Base Event: HSRP_BAD_TTL

Details: According to the RFC, datagrams carrying HSRP traffic have to have the Time-To-Live field set to 1 in the IP header, though sometimes values of 2 may be seen during normal HSRP datagram exchange. Traffic was detected with a TTL value of greater than 2, which may indicate a spoofed packet or a deliberate attempt to compromise the protocol.

References HSRP Specifications

HSRP Invalid Version Number

Base Event: HSRP_INVALID_VERNUM

Details: The current HSRP version described by the most current RFC is version 0, but a different version field was seen. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HSRP Nonauthenticated Connection

Base Event: HSRP_NONAUTH_CONNECTION

Details: An HSRP datagram with the default authentication field was seen. This is insecure and vulnerable to spoofing attacks. Routers participating in HSRP should be configured to use authenticated HSRP datagram exchange.

References HSRP Specifications

HSRP Resign From Nonactive Router

Base Event: HSRP_NONACTIVE_RESIGN

Details: The HSRP Resign message is used to indicate that an active router (router forwarding packets on behalf of the virtual router) has ceded to a different router. However, a Resign message was received from a router which is not the currently active router. This violation of the standard could indicate an attempt to compromise the protocol.

References HSRP Specifications

HTTP %00 Null Encoding

Base Event:	HTTP_NULL_ENCODE
Details:	The %00 null encoding was detected in the URL of the HTTP request. This may cause a premature end to processing of the URL on some systems, and may be an exploit attempt.
Response:	Location and audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References	HTTP Specifications

HTTP /../ Vulnerability

Base Event:	HTTP_DOT_DOT
Details:	An attempt to specify the relative path by means of ".." was detected. This may be an attempt to access disallowed files.
Response:	Location and audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	Relative paths including ".." may be legitimate HTTP traffic.
References	HTTP Specifications

HTTP /etc/passwd Access

Base Event:	HTTP_ETC_PASSWD_ACCESS
Details:	An attempt to access the /etc/passwd file was detected. This file contains the passwords of all users on a UNIX system.
Response:	Location and audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References	HTTP Specifications

HTTP .htaccess Probe

Base Event:	HTTP_HTACCESS_PROBE
Details:	An attempt to access the .htaccess file was detected. The .htaccess file is usually restricted and includes information which should not be directly served to Web clients. This may be an attempt to access disallowed files or a part of an intelligence gathering attack.
Response:	Location and audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References	HTTP Specifications

HTTP Campas CGI Passwd Access

Base Event:	HTTP_CAMPAS_ACCESS
Details:	Campas is a sample CGI script shipped with some older versions of NCSA HTTPd, which is an obsolete Web server package. The versions that included the script could not be determined, as the server is no longer maintained; however, version 1.2 of the script itself is known to be vulnerable. The script fails to properly filter user-supplied variables, and as a result, is used to execute commands on the host with the privileges of the Web server. Commands are passed as a variable to the script, separated by %0a (linefeed) characters. See the exploit for an example. Successful exploitation of this vulnerability is used to deface the Web site, read any files to which the server process has access, get directory listings, and execute anything to which the Web server has access.
Response:	Delete the sample script, as it is not necessary for normal Web server function.
Affected:	NCSA httpd-campas 1.2
False Positives:	There are no known False Positives associated with this signature.
References	Security Focus BID: 1975 NCSA HTTPd Page NCSA's "Security Concerns on the Web" Page

HTTP cfcache.map Access

Base Event:	HTTP_CFCACHE_MAP_ACCESS
Details:	An attempt to access the cfcache.map file was detected. This may reveal information about restricted files on the Web server.
Response:	Location and audit of client and server is recommended.
Affected:	ColdFusion Server 4.0x.
False Positives:	None known.
References	HTTP Specifications

HTTP CGI Htmlscript ViewSource

Base Event:	HTTP_HTMLSCRIPT_ACCESS
Details:	Miva's htmlscript CGI program provides a unique scripting language with HTML type tags. Note: htmlscript is an older product that Miva no longer distributes under this name. Versions of the htmlscript interpreter (a CGI script) prior to 2.9932 are vulnerable to a file-reading directory traversal attack, using the relative paths (for example, "../../../../../../etc/passwd"). An attacker would only need to append this path as a variable passed to the script by means of a URL. You can retrieve the contents of any file to which the Web server process has read access using this method.
Response:	Location and audit of client and server is recommended.
Affected:	Miva htmlscript 2.0.
False Positives:	None known.
References	Security Focus BID: 2001 Miva Corporation

HTTP Computrace Active

Base Event:	HTTP_COMPUTRACE_ACTIVE
Details:	HTTP traffic characteristic of a Computrace transmission were detected. Computrace is a computer tracking service used to monitor and track physical assets (for example, laptops).
Response:	Location and audit of client is recommended.
Affected:	No specific targets.
False Positives:	None known.
References	www.computrace.com

HTTP fileexists.cfm Access

Base Event:	HTTP_FILEEXISTS_CFM_ACCESS
Details:	An attempt to access the fileexists.cfm file was detected. This script may reveal information about restricted files on the Web server.
Response:	Location and audit of client and server is recommended.
Affected:	ColdFusion Server 4.0x.
False Positives:	None known.
References	HTTP Specifications

HTTP FrontPage Admin Probe

Base Event:	HTTP_FRONTPAGE_ADMIN_PROBE
Details:	An attempt to access the administrators.pwd file was detected. This file contains encrypted passwords and may be used to compromise the system.
Response:	Location and audit of client and server is recommended.
Affected:	Microsoft FrontPage.
False Positives:	None known.
References	HTTP Specifications

HTTP High-Bit ASCII

Base Event:	HTTP_BAD_REQURL5_HIGH_ASCII
Details:	Traffic that violates the HTTP RFC was detected. This is likely the result of a Web browser that does not conform to the HTTP standard sending high-bit ASCII characters (possibly non-English filenames) without encoding them with UTF-8.

HTTP HtSearch CGI Passwd Access

Base Event:	HTTP_HTSEARCH_FILE_ACCESS
Details:	Htdig is a Web content search engine for UNIX platforms. The software is set up to allow for file inclusion from configuration files. Any string surrounded by the opening single quote character (‘) is taken as a path to a file for inclusion, for example: some_parameter:‘var/htdig/some_file’ Htdig also allows included files to be specified by means of form input. Therefore, any Web user can specify any file for inclusion into a variable.
Response:	Administrators should upgrade to htdig version 3.1.5, which is fixed.
Affected:	The htDig Group htDig 3.1.1 The htDig Group htDig 3.1.2 The htDig Group htDig 3.1.3 The htDig Group htDig 3.1.4 The htDig Group htDig 3.2.0b1
False Positives:	None known.
References	Security Focus BID: 1026 Htdig Home Page

HTTP IIS ASP Showcode

Base Event: HTTP_SHOWCODE_ASP_ACCESS

Details: A sample Active Server Page (ASP) script, installed by default on Microsoft Internet Information Server (IIS) 4.0, gives the remote users access to view any file, which is readable by the Web server, on the same volume as the Web server.

IIS 4.0 installs some sample ASP scripts, including one called, “showcode.asp.” This script lets clients view the source of other sample scripts by means of a browser. The “showcode.asp” script does not perform sufficient checks and allows the files outside the sample directory to be requested. In particular, it does not check for “..” in the path of the requested file.

The script takes one parameter, “source”, which is the file to view. The script’s default location URL is: http://www.sitename.com/msadc/Samples/SELECTOR/showcode.asp

Similar vulnerabilities have been noted in ViewCode.asp, CodeBrws.asp and Winmsdp.exe.

Response: Do not install the sample code on the production servers. If you have installed the sample code, remove it or install the patches.

Affected: Microsoft IIS 4.0

Microsoft IIS 4.0alpha

Microsoft Site Server 3.0alpha

Microsoft Site Server 3.0i386

Microsoft Site Server 3.0SP1 alpha

Microsoft Site Server 3.0SP1 i386

Microsoft Site Server 3.0SP2 alpha

Microsoft Site Server 3.0SP2 i386

Microsoft Site Server Commerce Edition 3.0alpha

Microsoft Site Server Commerce Edition 3.0i386

Microsoft Site Server Commerce Edition 3.0SP1 alpha

Microsoft Site Server Commerce Edition 3.0SP1 i386

Microsoft Site Server Commerce Edition 3.0SP2 alpha

Microsoft Site Server Commerce Edition 3.0SP2 i386

False Positives: None known.

References Security Focus BID: 167

Q231368: Solution Available for File Viewers Vulnerability

Q231656: Preventing ViewCode.asp from Viewing Known Server Files

HTTP IIS CGI Newdsn

Base Event: HTTP_NEWDSN_EXE_ACCESS

Details: Microsoft IIS 3.0 was delivered with a sample program, newdsn.exe, installed by default in the directory, wwwroot/scripts/tools/. Executing this program with a properly submitted URL could allow for remote file creation. The created file is a Microsoft Access Database, but can have any extension, including .html.

Response: Currently, the Security Focus staff is not aware of any vendor-supplied patches for this issue. If you feel we are in error, contact us at: vuldb@securityfocus.com.

Affected: Microsoft IIS 3.0.

False Positives: None known.

References Security Focus BID: 1818

IIS 3.0 newdsn.exe allows remote creation of arbitrary files

HTTP IIS Source Code View Attempt

Base Event: HTTP_IIS_OBTAIN_CODE

Details: This vulnerability may reveal source code to certain scripts on Microsoft IIS servers.

Response: Location and audit of client and server is recommended.

Affected: Microsoft IIS Web servers

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_CONTENT_LENGTH

Details: The Content-Length header field value specified in the HTTP response had an invalid format.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_CONTENT_RANGE

Details: The Content-Range header field value specified in the HTTP response had an invalid format.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_MSGHDR_TEXT

Details: HTTP headers lines generally consist of a header name followed by a colon and value for the header. This event indicates that the text of the header value was out of the valid character range allowed by the HTTP RFC.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_REQ_MSGHDR

Details: HTTP request headers lines generally consist of a header name followed by a colon and value for the header. This event indicates that the text of a header name was out of the valid character range allowed by the HTTP RFC.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_RESP_BYTE_UNIT

Details: The Content-Range header field value specified in the HTTP response had an invalid format.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_RESP_MSGHDR

Details: HTTP response header lines generally consist of a header name followed by a colon and header value. This event indicates that the text of a header name was out of the valid character range allowed by the HTTP RFC.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_BAD_STATUSTEXT

Details: The text after the server status response (the first line of an HTTP response) did not comply with the restrictions in the RFC.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Data

Base Event: HTTP_UNKNOWN_STATUS

Details: This event indicates that the status response that appears in the first line of an HTTP server response did not comply with the format specified by the RFC.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Request

Base Event: HTTP_MISSING_HOST

Details: An HTTP 1.1 request was detected which did not contain the Host request-header. This is a violation of the HTTP 1.1 standard and may indicate an attempt to compromise the server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Transport Encoding

Base Event: HTTP_BAD_CHUNKED_HEX

Details: The HTTP traffic contained badly formatted encoding. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed Transport Encoding

Base Event: HTTP_NO_CRLF_AFTER_CHUNK

Details: The HTTP traffic was missing not properly terminated. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQUEST

Details: The HTTP request contained characters out of the valid character range as specified by the HTTP RFC. (For example, terminal control characters or delete characters in the request.)

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL0

Details: The URL in an HTTP CONNECT request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL1

Details: The URL in an HTTP request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL2

Details: The URL in an HTTP request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL3

Details: The URL in an HTTP request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL4

Details: The URL in an HTTP request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL5

Details: The URL in an HTTP request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event: HTTP_BAD_REQURL6_0

Details: The opaque section of the URL in an HTTP request did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP Malformed URL

Base Event:	HTTP_NEWLINES_IN_REQUEST_PATH
Details:	The HTTP URL observed did not conform to the HTTP RFC. This may be an attempt to exploit certain server vulnerabilities.
Response:	If seen in sufficient volume or variation, audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References	HTTP Specifications

HTTP SCO Skunkware ViewSource Traversal

Base Event:	HTTP_VIEW_SOURCE_ACCESS
Details:	view-source is a script included with the httpd package, which is bundled with Skunkware 2.0. Skunkware 2.0 is a variant of the UNIX operating system distributed by Santa Cruz Operations. A problem with the view-source script may allow remote access to restricted files. The problem occurs in the handling of slashes and dots when appended to the view-source script. By appending a series of double-dots and slashes to a query using the view-source script, it is possible to traverse the directory structure on a Web server. In turn, viewing the contents of the directories and the files of the httpd process, which the UID can read, is possible. This flaw enables a user with malicious motives to read files on a remote system and gather intelligence for an attack against the system, as well as other potentially sensitive information.
Response:	Location and audit of client and server is recommended.
Affected:	SCO Skunkware 2.0.
False Positives:	None known.
References	Security Focus BID: 2251

HTTP sourcewindow.cfm Access

Base Event:	HTTP_SOURCEWINDOW_CFM
Details:	An attempt to access the sourcewindow.cfm file was detected. This script may reveal information about restricted files on the Web server.
Response:	Location and audit of client and server is recommended.
Affected:	Macromedia ColdFusion Server 4.0x.
False Positives:	None known.
References	HTTP Specifications

HTTP Tilde Access

Base Event:	HTTP_TILDE_ACCESS
Details:	An attempt to access a file via the relative path of '~' was detected. This may allow an intruder access into the Web server's home directory with older Web servers.
Response:	If seen in sufficient volume or variation audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References HTTP Specifications

HTTP URL Directory Traversal

Base Event: HTTP_URL_DIRECTORY_TRAVERSAL

Details: Microsoft IIS 4.0 and 5.0 are both vulnerable to double dot "../" directory traversal exploitation if the extended UNICODE character representations are used in substitution for "/" and "\".

Unauthenticated users may access any known file in the context of the IUSR_machinename account. The IUSR_machinename account is a member of the Everyone and Users groups by default. Therefore, you can delete, modify, or execute any file on the same logical drive as any Web-accessible file, which is accessible to these groups.

Successful exploitation would yield the same privileges as a user who could successfully log on to the system, without any credentials, to a remote user.

It was discovered that a Windows 98 host running the Microsoft Personal Web Server is also subject to this vulnerability (March 18, 2001).

The Code Blue Worm exploited this vulnerability.

UPDATE: We believe that an aggressive worm is in the wild that actively exploits this vulnerability.

Response: The patch released with the advisory MS00-057 eliminates this vulnerability. Users who have already applied this patch do not need to take further action.

Otherwise, the patch is available at the following locations:

For Microsoft IIS 4.0:

Microsoft Q269862

Microsoft Q269862

For Microsoft IIS 4.0alpha:

Microsoft Q269862

Microsoft Q269862

For Microsoft IIS 5.0:

Microsoft Q269862

For Microsoft Personal Web Server 4.0:

David Raitzer pws_patch.zip

Affected: No specific targets.

False Positives: None known.

References Security Focus BID: 1806

Security Focus BID: 2708

CVE-2001-0333

CVE-2000-0884

F-Secure Computer Virus Information Pages: CodeBlue

FW: ISSalert: ISS Alert: Code Blue Worm

TROJ_BLUECODE.A

HTTP WinApache Bat Exec

Base Event:	HTTP_CMD_FILE_PIPE
Details:	A vulnerability was discovered in the batch file handler for Apache on Microsoft Windows operating systems. Special characters (such as |) may not be filtered by the batch file handler when a Web request is made for a batch file. As a result, a remote attacker may be able to execute arbitrary commands on the host running the vulnerable software. This may be exploited by means of a specially crafted Web request which contains the arbitrary commands to be executed. Note that Web servers on Microsoft Windows operating systems normally run with SYSTEM privileges. The consequences of exploitation is that a remote attacker is able to fully compromise a host running the vulnerable software. The 2.0.x series of Apache for Microsoft Windows ships with a test batch file which may be exploited to execute arbitrary commands. Since this issue is in the batch file handler, any batch file which is accessible by means of the Web is appropriate for the purposes of exploitation.
Response:	This issue has been addressed in Apache 1.3.24 and 2.0.34-BETA for Microsoft Windows operating systems. Administrators are advised to upgrade.
Affected:	Apache Software Foundation Apache 1.3.6win32 to 1.3.23win32 Apache Software Foundation Apache 2.0.28-BETA win32 and 2.0.32-BETA win32
False Positives:	The likelihood of a false positive only exists if the piping is used by certain users to perform legitimate requests.
References	CAN-2002-0061 Security Focus BID: 4335

Ident Malformed Data

Base Event:	IDENT_BAD_ERROR
Details:	An ident error response was detected that contained things other than alpha numerics for the error. This may indicate a compromised ident server.
Response:	If seen in sufficient volume or variation, audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	It is possible this is a non-compliant ident implementation.
References	Ident Specifications

Ident Malformed Data

Base Event:	IDENT_BAD_OSNAME
Details:	The operating system name in an ident response was not one of the allowed values according to the protocol specification. This may indicate a compromised ident server.
Response:	If seen in sufficient volume or variation, audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	It is possible this is a non-compliant ident implementation.
References	Ident Specifications

Ident Malformed Data

Base Event: IDENT_BAD_PORTNUMBERS

Details: A port number that doesn't correspond to any existing connection was specified in an ident request. This may be an information gathering or attempt or it may just be a latent request for an old connection.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References Ident Specifications

Ident Malformed Data

Base Event: IDENT_BAD_REQUEST

Details: An ident request that does not conform to the specification was detected. This may indicate an information gathering attempt.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant ident implementation.

References Ident Specifications

Ident Malformed Data

Base Event: IDENT_BAD_RESPONSE

Details: A response was detected that does not conform to the ident RFC. This may indicate a compromised ident server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant ident implementation.

References Ident Specifications

Ident Malformed Data

Base Event: IDENT_BAD_USERNAME

Details: The user name in an ident response did not conform to the protocol specification. This may indicate a compromised ident server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant ident implementation.

References Ident Specifications

Ident Malformed Data

Base Event: IDENT_BUFFER_OVERFLOW

Details: The user name in an ident response was longer than 16 bytes. While not a violation of the protocol, this is suspicious and may indicate a compromised ident server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant ident implementation.

References Ident Specifications

Ident Malformed Data

Base Event: IDENT_DATA_PAST_CLOSE

Details: Extra data was detected in an ident exchange (data past the end of a valid protocol exchange). This may indicate a compromised ident server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant ident implementation.

References Ident Specifications

Ident Malformed Data

Base Event: IDENT_DATA_PAST_REQUEST

Details: Data was detected after the end of a valid ident request. This may indicate a compromised ident server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is a non-compliant ident implementation.

References Ident Specifications

IMAP Failed Login

Base Event: IMAP_FAILED_LOGIN

Details: A failed IMAP authentication attempt was detected.

IMAP Protocol Violation

Base Event: IMAP_CLI_ENCRYPTED_OR_INVALID_AUTH_OR_BASE64

Details: Invalid IMAP client side auth/base64 or using encrypted connection.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_ASTRING_CRLF

Details: The IMAP exchange expected an “astring” followed by a CRLF, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_AUTH

Details: Invalid IMAP client side lead string in the AUTH state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_AUTH_TYPE

Details: Invalid IMAP client side authentication type in the AUTH TYPE state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_COMMAND_AUTH

Details: Invalid IMAP client side command string in the COMMAND AUTH state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_COMMAND_NONAUTH

Details: Invalid IMAP client side command string in the COMMAND NONAUTH state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_COMMAND_SELECT

Details: Invalid IMAP client side command string in the COMMAND SELECT state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_LIST_MAILBOX_COMMAND

Details: An invalid list mailbox command by the client was detected. This violation of the standard could indicate an attempt to compromise the protocol.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_SELECT

Details: Invalid IMAP client side lead string in the SELECT state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_UNKNOWN

Details: Invalid IMAP client side lead string in the UNKNOWN state.

IMAP Protocol Violation

Base Event: IMAP_CLI_INVALID_USERID

Details: The IMAP exchange expected a user ID, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_EXPECTED_CRLF

Details: The IMAP exchange expected CRLF, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_EXPECTED_LF

Details: The IMAP exchange expected LF, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_EXPECTED_LTPAREN

Details: The IMAP exchange was at a point where a left parentheses was expected, but something else was sent instead.

IMAP Protocol Violation

Base Event: IMAP_EXPECTED_TXT_CHAR_RTBRACKET_SPACE

Details: The IMAP exchange expected text followed by a close bracket, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_2ASTRING_TRANS

Details: The IMAP exchange was expecting a space field separator, but something else was sent instead.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ALL_SMART

Details: An IMAP violation occurred while parsing a message.

IMAP Protocol Violation

Base Event: IMAP_INVALID_APPEND

Details: An IMAP violation occurred while parsing an APPEND command.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ASTRING_LIST

Details: An IMAP violation occurred while parsing an astring list.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ASTRINGS_TRANS

Details: The IMAP exchange was expecting a space field separator, but something else was sent instead.

IMAP Protocol Violation

Base Event: IMAP_INVALID_CAPABILITY

Details: Invalid IMAP server side capability sent.

IMAP Protocol Violation

Base Event: IMAP_INVALID_CHAR8

Details: The IMAP exchange was sent an unexpected NULL character.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_BCC

Details: The IMAP exchange expected an envelope BCC field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_CC

Details: The IMAP exchange expected an envelope CC field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_DATE_SUBJ

Details: The IMAP exchange expected an envelope date and subject, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_FROM

Details: The IMAP exchange expected an envelope FROM field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_INREPLYTO

Details: The IMAP exchange expected an envelope IN REPLY TO field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_MESGID

Details: The IMAP exchange expected an envelope MESGID field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_REPLY_TO

Details: The IMAP exchange expected an envelope REPLY TO field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_SENDER

Details: The IMAP exchange expected an envelope SENDER, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_ENV_TO

Details: The IMAP exchange expected an envelope TO field, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_FETCH

Details: An IMAP violation occurred while parsing a FETCH command.

IMAP Protocol Violation

Base Event: IMAP_INVALID_FLAGLIST

Details: An IMAP violation occurred while parsing a flag list.

IMAP Protocol Violation

Base Event: IMAP_INVALID_FLAGS

Details: An IMAP violation occurred while parsing mailbox list flags.

IMAP Protocol Violation

Base Event: IMAP_INVALID_LIST_MAILBOX_COMMAND

Details: An invalid list mailbox command by the client was detected. This violation of the standard could indicate an attempt to compromise the protocol.

IMAP Protocol Violation

Base Event: IMAP_INVALID_LITERAL

Details: The IMAP exchange expected a literal string, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_MAILBOXLIST

Details: The IMAP exchange expected a mailbox list, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_MAILBOX_MAILBOX

Details: Malformed mailbox arguments to an IMAP command were sent by the client. This violation of the standard could indicate an attempt to compromise the protocol.

IMAP Protocol Violation

Base Event: IMAP_INVALID_MIME2_B_ENCODED_TEXT

Details: An IMAP violation occurred while parsing MIME2 B encoded data.

IMAP Protocol Violation

Base Event: IMAP_INVALID_MIME2_ENCODE

Details: An IMAP violation occurred while parsing MIME2 encoded data.

IMAP Protocol Violation

Base Event: IMAP_INVALID_MIME2_Q_ENCODED_TEXT

Details: An IMAP violation occurred while parsing MIME2 Q encoded data.

IMAP Protocol Violation

Base Event: IMAP_INVALID_NADDRESS

Details: The IMAP exchange expected an astring followed by a CRLF, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_NAMESPACE

Details: The IMAP exchange expected a namespace, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_NAMESPACE_EXT

Details: The IMAP exchange expected a namespace, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_NSTRING_LIST

Details: An IMAP violation occurred while parsing an nstring list.

IMAP Protocol Violation

Base Event: IMAP_INVALID_NZNUMBERS

Details: An IMAP violation occurred while parsing an “nznumber.”

IMAP Protocol Violation

Base Event: IMAP_INVALID_PARTIAL

Details: An IMAP violation occurred while parsing a FETCH command.

IMAP Protocol Violation

Base Event: IMAP_INVALID_QUOTA_LIST

Details: The IMAP exchange expected a quota list, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_QUOTA_TR

Details: An IMAP violation occurred while parsing quota data.

IMAP Protocol Violation

Base Event: IMAP_INVALID_QUOTED

Details: The IMAP exchange expected a quoted string, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_QUOTED_USERID

Details: The IMAP exchange expected a quoted user ID, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_RESP_CODE

Details: An invalid IMAP response code was sent.

IMAP Protocol Violation

Base Event: IMAP_INVALID_RESP_TXT

Details: An IMAP violation occurred while parsing response text.

IMAP Protocol Violation

Base Event: IMAP_INVALID_RESP_TXT2

Details: An IMAP violation occurred while parsing response text.

IMAP Protocol Violation

Base Event: IMAP_INVALID_RESP_TXT_CODE

Details: An invalid IMAP response code was sent.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SEARCH

Details: An IMAP violation occurred while parsing a SEARCH command.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SEARCH_DATE

Details: The search date in a client command was invalid. This violation of the standard could indicate an attempt to compromise the protocol.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SEARCH_MISMATCHED_PAREN

Details: An IMAP violation occurred while parsing a SEARCH command.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SEARCH_SET

Details: An IMAP violation occurred while parsing a SEARCH command set.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SECTION

Details: The IMAP exchange expected a section, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SER_FLAGLIST

Details: An IMAP violation occurred while parsing a server side flag list.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SER_MESG_ATTRIB

Details: An IMAP violation occurred while parsing server side message attributes.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SET

Details: The IMAP exchange expected a set, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SETQUOTA_LIST

Details: The IMAP exchange expected a setquota list, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SETQUOTA_PR

Details: An IMAP violation occurred while parsing setquota data.

IMAP Protocol Violation

Base Event: IMAP_INVALID_SPACE_TRANSITION

Details: The IMAP exchange was expecting a space field separator, but something else was sent instead.

IMAP Protocol Violation

Base Event: IMAP_INVALID_STATUS_ATTRB_NUM

Details: An IMAP violation occurred while parsing status command numbers.

IMAP Protocol Violation

Base Event: IMAP_INVALID_STAT_ATTRB_NUM_PRS

Details: The IMAP exchange expected a status attribute, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_STATUS_ATTRIBS

Details: The IMAP exchange expected a status attribute, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_STORE_ATTRIBS

Details: The IMAP exchange expected a store attribute, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_STRING_LIST

Details: An IMAP violation occurred while parsing a string list.

IMAP Protocol Violation

Base Event: IMAP_INVALID_S_ASTRING_TRANS

Details: The IMAP exchange was expecting a space field separator, but something else was sent instead.

IMAP Protocol Violation

Base Event: IMAP_INVALID_S_MAILBOX_TRANS

Details: The IMAP exchange was expecting a space field separator, but something else was sent instead.

IMAP Protocol Violation

Base Event: IMAP_INVALID_TXT

Details: The IMAP exchange expected text followed by a CRLF, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_INVALID_URL

Details: An IMAP violation occurred while parsing a URL.

IMAP Protocol Violation

Base Event: IMAP_INVALID_USERID_LITERAL

Details: The IMAP exchange expected a literal user ID, but was sent something else.

IMAP Protocol Violation

Base Event: IMAP_SER_INVALID_ANY

Details: Invalid IMAP server side lead string in the ANY state.

IMAP Protocol Violation

Base Event: IMAP_SER_INVALID_GREETING

Details: Invalid initial IMAP server side greeting.

IMAP Protocol Violation

Base Event: IMAP_SER_INVALID_MSG_ATT

Details: An IMAP violation occurred while parsing server side message attributes.

IMAP Protocol Violation

Base Event: IMAP_SER_INVALID_NONAUTH

Details: The server sent an invalid command in a non-authenticated state. This violation of the standard could indicate an attempt to compromise the protocol.

IMAP Protocol Violation

Base Event: IMAP_SER_INVALID_TAGGED_ANY

Details: Invalid IMAP server side lead string in the TAGGED ANY state.

IMAP Protocol Violation

Base Event: IMAP_SER_INVALID_UNTAGGED_ANY

Details: Invalid IMAP server side lead string in the UNTAGGED ANY state.

IMAP URL Invalid Login

Base Event: IMAP_URL_INVALID_LOGIN

Details: An invalid IMAP logon with URL encoding was detected.

IRC Malformed Data

Base Event: IRCCLISER_BAD_AFTER_NICK

Details: This event indicates that data was received after the IRC NICK (PASS) was transmitted by the client. According to the RFC, no data is expected after the proper termination of the NICK (PASS) command.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

IRC Malformed Data

Base Event: IRCCLISER_BAD_AFTER_USER

Details: This event indicates that data was received after the IRC USER (PASS) was transmitted. According to the RFC, no data is expected after the proper termination of the USER (PASS) command.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

IRC Malformed Data

Base Event: IRCSER_UNKNOWN_AFTERPASS

Details: The first data sent by the client after a PASS command was unrecognized. Valid commands here include “SERVER,” “ERROR,” and “CAPAB.”

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

IRC Malformed Data

Base Event: IRCSER_UNKNOWN_INIT

Details: A Client initialization sequence was sent to server that did not comply with the IRC specification.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

IRC Malformed Data

Base Event: IRCSERSER_UNKNOWN_AFTERPASS

Details: An unknown command was sent after a PASS command in an IRC session.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

IRC Malformed Data

Base Event: IRCSERSER_INVALID_CAPAB

Details: The IRC server responded to a CAPAB query with an invalid answer.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

IRC Malformed Data

Base Event: IRCSERSER_UNKNOWN_AFTERPASSCAPABS

Details: After a successful IRC passwd and capabilities exchange, invalid data was sent.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References IRC Specifications

Malformed LDAP Traffic

Base Event: LDAP_ASN1_DATALENGTH_IMPOSSIBLE_STATE

Details: Please contact technical support if you see this error as it should be impossible to generate.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_DATALENGTH_RIDICULOUS_WIDTH

Details: An element of BER encoded ASN.1 data specified an integer larger than 32 bits for the data length. LDAP data should never require numbers this large to describe their length, and indicates either a non-conforming LDAP implementation or an intrusion attempt.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_DATALENGTH_VALUE_TOO_LARGE

Details: An element of ASN.1 encoded LDAP data specified a data field size that was too large for its indicated primitive type.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_DATALENGTH_VALUE_TOO_SMALL

Details: An element of ASN.1 encoded LDAP data specified a data field size that was too small for its indicated primitive type.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_RUNT_SEQUENCE

Details: A sequence of LDAP ASN.1 encoded data ended with fewer data elements than was expected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ADDREQUEST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Add Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ATTRIBUTELIST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within an attribute list.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ATTRIBUTETYPEANDVALUES

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within an attribute type description and values binding.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ATTRIBUTEVALUEASSERTION

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within an attribute value assertion.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_BINDREQUEST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Bind Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_BINDRESPONSE

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Bind Response PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_COMPAREREQUEST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Compare Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_CONTROL

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a single LDAP Control.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_EXTENDEDREQUEST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Extended Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_EXTENDEDRESPONSE

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Extended Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_FILTER

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Filter.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_LDAPMESSAGE

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a LDAP Message envelope.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_LDAPRESULT

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a LDAP Result derived PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MATCHINGRULEASSERTION

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Matching Rule Assertion.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MODIFICATIONDIRECTIVE

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Modification Directive.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MODIFYDNREQUEST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Modify DN Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_MODIFYREQUEST

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Modify Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_REFERRAL

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a LDAP referral.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_ROOT

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within the client/server data stream outside of any known protocol PDUs.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SASLCREDENTIALS

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within SASL Credentials.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEARCHREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Add Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEARCHRESULTENTRY

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Search Result Entry PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQOFATTRDESC

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Sequence of Attribute Descriptions.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQUENCEOFCONTROL

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Sequence of LDAP Controls.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQUENCEOFMODIFICATION

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Sequence of Modifications.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SEQUENCEOFSUBSTRINGS

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a sequence of substrings.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SETOFATTRIBUTEVALUE

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a Set of Attribute Values.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_ILLEGAL_LONG_ENCODING_IN_SUBSTRINGFILTER

Details: A long form BER encoding of an ASN.1 LDAP type was detected, but these are not permitted in the subset of BER/ASN.1 used by LDAP. The log ASN.1 tuple type encoding was detected within a substring filter.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ADDREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Bind Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ATTRIBUTELIST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of an Attribute List.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ATTRIBUTETYPEANDVALUES

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of an attribute type description and values binding.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ATTRIBUTEVALUEASSERTION

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of an Attribute Value Assertion.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_BINDREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Bind Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_BINDRESPONSE

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Bind Response PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_COMPAREREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Compare Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_CONTROL

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a single LDAP Control.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_EXTENDEDRESPONSE

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Extended Response PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_EXTENDEDREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Extended Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_FILTER

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Filter.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_LDAPMESSAGE

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a LDAP Message envelope.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_LDAPRESULT

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a LDAP Result derived PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MATCHINGRULEASSERTION

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Matching Rule Assertion.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MODIFICATIONDIRECTIVE

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Modification Directive.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MODIFYDNREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Modify DN Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_MODIFYREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Modify Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_REFERRAL

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a LDAP Referral.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_ROOT

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of the client/server data streams outside of any LDAP message envelopes.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SASLCREDENTIALS

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of SASL Credentials.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEARCHREQUEST

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Search Request PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEARCHRESULTENTRY

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Search Result Entry PDU.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFATTRIBUTEDESCRIPTION

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Sequence of Attribute Descriptions.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFCONTROL

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Sequence of LDAP Controls.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFMODIFICATION

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Sequence of Modifications.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SEQUENCEOFSUBSTRINGS

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a sequence of substrings.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SETOFATTRIBUTEVALUE

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a Set of Attribute Values.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_TYPE_UNRECOGNIZED_IN_SUBSTRINGFILTER

Details: The data type on an encoded data element was not one of the data types permitted by LDAP within the context of a substring filter.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ABANDONREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Abandon Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ADDREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Add Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ASSERTIONFILTER_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Assertion Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ASSERTIONFILTER_IN_FILTER

Details: Within the context of a Filter, a Assertion Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRDESC_IN_ATTRTYPEANDVALUES

Details: Within the context of a Attribute type description and values binding, an Attribute Description data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTEDESC_IN_MATCHINGRULEASSERTION

Details: Within the context of a Matching Rule Assertion, an Attribute Description data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTEDESC_IN_SEQOFATTRDESC

Details: Within the context of a Sequence of Attribute Descriptions, an Attribute Description data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTEDESC_IN_SUBSTRINGFILTER

Details: Within the context of a Matching Rule Assertion, an Attribute Description data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTELIST_IN_ATTRIBUTELIST

Details: Within the context of an Attribute List, a Attribute List data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBUTELIST_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, an Attribute List was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRIBVALUE_IN_SETOFATTRIBVALUES

Details: Within the context of a Set of Attribute Values, an Attribute Value data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRLIST_IN_ADDREQUEST

Details: Within the context of a Add Request PDU, an Attribute List was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ATTRVALUES_IN_ATTRTYPEANDVALUES

Details: Within the context of a Attribute type description and values binding, an Attribute Values List data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_AVA_IN_COMPAREREQUEST

Details: Within the context of a Compare Request PDU, a Attribute Value Assertion data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_AVL_IN_SEARCHRESULTENTRY

Details: Within the context of a Search Result Entry PDU, an Attribute Value List data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_BASEDN_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Search Base DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_BINDREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Bind Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_BINDRESP_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Bind Response PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_BOOLEAN_IN_MATCHINGRULEASSERTION

Details: Within the context of a Matching Rule Assertion, a Boolean data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_BOOLEAN_IN_MODIFYDNREQUEST

Details: Within the context of a Modify DN Request PDU, a Boolean data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_BOOLEAN_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Boolean data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_COMPAREREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Compare Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_COMPOUNDFILTER_IN_FILTER

Details: Within the context of a Filter, a Compound Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_COMPOUNDFILTER_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Compound Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_CONTROL_IN_SEQUENCEOFCONTROL

Details: Within the context of a Sequence of LDAP Controls, a LDAP Control data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_CONTROLS_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a LDAP Controls Sequence was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_CRITICALITY_IN_CONTROL

Details: Within the context of a single LDAP Control, a Criticality Flag data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_DELREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Delete Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_ENUM_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Enumerated data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_EXTENDEDREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Extended Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_EXTENDEDRESP_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Extended Response PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_EXTREQNAME_IN_EXTENDEDREQUEST

Details: Within the context of a Extended Request PDU, a Extended Request Name/OID data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_EXTREQVALUE_IN_EXTENDEDREQUEST

Details: Within the context of a Extended Request PDU, a Extended Request Value data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPDN_IN_COMPAREREQUEST

Details: Within the context of a Compare Request PDU, a Object DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPDN_IN_MODIFYDNREQUEST

Details: Within the context of a Modify DN Request PDU, a Object DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPDN_IN_SEARCHRESULTENTRY

Details: Within the context of a Search Result Entry PDU, an Object DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_ATTRIBUTEVALUEASSERTION

Details: Within the context of a Attribute Value Assertion, a LDAP String data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_BINDRESPONSE

Details: Within the context of a Bind Response PDU, a LDAP String (a DN or an error message) data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_CONTROL

Details: Within the context of a single LDAP Control, a LDAP String data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_EXTENDEDRESPONSE

Details: Within the context of a Extended Response PDU, a LDAP String (a DN or an error message) data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_LDAPRESULT

Details: Within the context of a LDAP Result derived PDU, a LDAP String (a DN or an error message) data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPSTRING_IN_SASLCREDENTIALS

Details: Within the context of a SASL Credentials, a LDAP String data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LDAPURL_IN_REFERRAL

Details: Within the context of a LDAP Referral, a LDAP URL data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_LIMIT_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Search Size/Time Limit data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MATCHINGRULEVALUE_IN_MRASSERTION

Details: Within the context of a Matching Rule Assertion, a Matching Rule Value data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MESSAGEID_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a MessageID data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MODIFICATION_IN_SEQUENCEOFMODIFICATION

Details: Within the context of a Sequence of Modifications, a Modification Directive data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MODDNREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Modify DN Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MODREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a modification request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MODSEQUENCE_IN_MODIFYREQUEST

Details: Within the context of a Modify Request PDU, a Modification Sequence was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MODTYPE_IN_MODDIRECTIVE

Details: Within the context of a Modification Directive, a Modification Type Specifier data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MODVAL_IN_MODDIRECTIVE

Details: Within the context of a Modification Directive, a Modification Value data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MRAFILTER_IN_FILTER

Details: Within the context of a Search Request PDU, a Matching Rule Assertion data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MRAFILTER_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Matching Rule Assertion data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_MRID_IN_MRASSERTION

Details: Within the context of a Matching Rule Assertion, a Matching Rule ID data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_NAME_IN_BINDREQUEST

Details: Within the context of a Bind Request PDU, a Bind DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_OBJECTDN_IN_ADDREQUEST

Details: Within the context of a Add Request PDU, a Object DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_OBJECTDN_IN_MODIFYREQUEST

Details: Within the context of a Modify Request PDU, a Object DN data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_PRESENTFILTER_IN_FILTER

Details: Within the context of a Filter, a Attribute Presence Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_PRESENTFILTER_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Attribute Presence Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_REFERRAL_IN_BINDRESPONSE

Details: Within the context of a Bind Response PDU, a LDAP Referral data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_REFERRAL_IN_EXTENDEDRESPONSE

Details: Within the context of a Extended Response PDU, a LDAP Referral data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_REFERRAL_IN_LDAPRESULT

Details: Within the context of a LDAP Result derived PDU, a LDAP Referral data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_RESPNAME_IN_EXTENDEDRESPONSE

Details: Within the context of a Extended Response PDU, a Extended Response Name/OID data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_RESPVALUE_IN_EXTENDEDRESPONSE

Details: Within the context of a Extended Response PDU, a Extended Response Value data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_RESULTCODE_IN_BINDRESPONSE

Details: Within the context of a Bind Response PDU, a LDAP Result Code data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_RESULTCODE_IN_LDAPRESULT

Details: Within the context of a LDAP Result derived PDU, a LDAP Result Code data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SASLAUTH_IN_BINDREQUEST

Details: Within the context of a Bind Request PDU, a SASL Authentication Credentials data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SEARCHREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Search Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SEARCHRESENTRY_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Search Result Entry PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SEARCHRESREF_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Search Result Reference PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SRVRSASLCRED_IN_BINDRESPONSE

Details: Within the context of a Bind Response PDU, a Server SASL Credentials data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRINGFILTER_IN_FILTER

Details: Within the context of a Filter, a Substring Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRINGFILTER_IN_SEARCHREQUEST

Details: Within the context of a Search Request PDU, a Substring Filter data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRING_IN_SEQUENCEOFSUBSTRINGS

Details: Within the context of a Sequence of Substrings, a Substring data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SUBSTRINGS_IN_SUBSTRINGFILTER

Details: Within the context of a Substring Filter, a Sequence of Substrings data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_SIMPLEAUTH_IN_BINDREQUEST

Details: Within the context of a Bind Request PDU, a Simple Authentication Credentials data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_UNBINDREQ_IN_LDAPMESSAGE

Details: Within the context of a LDAP Message envelope, a Unbind Request PDU data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_ASN1_UNEXPECTED_TYPE_VERSION_IN_BINDREQUEST

Details: Within the context of a Bind Request PDU, a LDAP Version data element was received, but was unexpected.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_MODIFYTYPE_UNKNOWN

Details: An unknown modification type was specified.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_DEREFALIASES_UNKNOWN

Details: An unknown policy for dereferencing aliases was specified.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_RESULTCODE_AUTHFAILURE

Details: An authentication failure was detected in a LDAP connection.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_RESULTCODE_RESERVEDVALUEUSED

Details: An reserved result code was returned from the LDAP server.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_RESULTCODE_UNKNOWN

Details: An unknown result code was return from the LDAP server.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event: LDAP_SEARCHSCOPE_UNKNOWN

Details: An unknown search scope was specified.

References LDAP RFC 2251
LDAP RFC 2252
LDAP RFC 2253
LDAP RFC 2254
LDAP RFC 2255

Malformed LDAP Traffic

Base Event:	LDAP_VERSION_UNKNOWN
Details:	An unknown version of the LDAP protocol was specified.
References	LDAP RFC 2251 LDAP RFC 2252 LDAP RFC 2253 LDAP RFC 2254 LDAP RFC 2255

NBT Malformed Data

Base Event:	NBT_INVALID_COMMAND
Details:	Invalid NetBIOS command data sent to a server was detected.
Response:	If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.
Affected:	No specific targets.
False Positives:	None known.
References	SMB Information

NNTP Auth Failure

Base Event:	NNTPCLI_FAILED_AUTHENTICATION
Details:	This event corresponds to the server sending a 482 or 452 response code.
Response:	If seen in sufficient volume or variation, audit of client and server is recommended.
Affected:	No specific targets.
False Positives:	It is possible this is only a user mistyping their password.
References	NNTP Specifications

NNTP Malformed Data

Base Event:	NNTPCLI_EXPECTED_CRLF
Details:	A carriage return linefeed (CRLF) sequence was expected as the next string from the client, however something else was sent. It is possible this indicates an attempt to compromise the server.
Response:	The packet contents should be examined and the server should be audited.
Affected:	No specific targets.
False Positives:	It is possible this is a news client or server using an unofficial protocol extension or non-compliant NNTP implementation.
References	NNTP Specifications

NNTP Malformed Data

Base Event: NNTPCLI_INVALID_ASCII

Details: The NNTP client sent a command with characters outside the ASCII range allowed. It is possible this indicates an attempt to compromise the server.

Response: The packet contents should be examined and the server should be audited. Valid ASCII characters are x00 - 0x7f inclusive.

Affected: No specific targets.

False Positives: None known.

References NNTP Specifications

NNTP Malformed Data

Base Event: NNTPCLI_INVALID_COMMAND

Details: The NNTP client sent an unrecognized command to the server. This could indicate a compromised server.

Response: Audit of the server is recommended. If seen in sufficient volume or variation, location and audit of client is recommended.

Affected: No specific targets.

False Positives: It is possible this is a news client or server using an unofficial protocol extension or non-compliant NNTP implementation.

References NNTP Specifications

NNTP Malformed Data

Base Event: NNTPSER_INVALID_RESPONSE

Details: The NNTP server sent a response that did not comply with the RFC. This event is triggered when the response does not start with a three digit numeric response code. It is possible this indicates an attempt to compromise the server.

Response: The packet contents should be examined and the server should be audited.

Affected: No specific targets.

False Positives: It is possible this is a news client or server using an unofficial protocol extension or non-compliant NNTP implementation.

References NNTP Specifications

NNTP Malformed Data

Base Event: NNTPCLI_INVALID_TEXT

Details: The NNTP client sent data outside of the range allowed. It is possible this indicates an attempt to compromise the server.

Response: The packet contents should be examined and the server should be audited.

Affected: No specific targets.

False Positives: None known.

References NNTP Specifications

NNTP Malformed Data

Base Event: NNTPSER_INVALID_ASCII

Details: The NNTP server responded with characters outside the ASCII range allowed in a response. Valid ASCII characters are x00 - 0x7f inclusive. It is possible this indicates an attempt to compromise the server.

Response: The packet contents should be examined and the server should be audited.

Affected: No specific targets.

False Positives: It is possible this is a news client or server using an unofficial protocol extension or non-compliant NNTP implementation.

References NNTP Specifications

NNTP Malformed Data

Base Event: NNTPSER_INVALID_TEXT

Details: The NNTP server responded with text outside the expected character range. The expected character range includes ASCII characters x00 - 0x7f inclusive. It is possible this indicates an attempt to compromise the server.

Response: The packet contents should be examined and the server should be audited.

Affected: No specific targets.

False Positives: It is possible this is a news client or server using an unofficial protocol extension or non-compliant NNTP implementation.

References NNTP Specifications

OSPF “Hello” Invalid Options

Base Event: OSPF_HELLO_INVALID_OPTS

Details: The options specified in the OSPF Hello message were invalid. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF “Hello” Malformed Neighbor Fields

Base Event: OSPF_HELLO_BAD_NEIGHBOR

Details: The neighbor fields specified in the OSPF Hello message were malformed. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF “Hello” Short Packet

Base Event: OSPF_HELLO_SHORT_PACKET

Details: The OSPF Hello message was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Cleartext Password

Base Event: OSPF_SIMPLE_AUTHENTICATION

Details: An OSPF message with an unencrypted password field was detected. Simple password authentication guards against routers inadvertently joining the routing domain, but provides no security against passive attacks. Anyone with physical access to the network can learn the password and send malicious packets.

References OSPF Specifications

OSPF DB Desc Invalid Flags

Base Event: OSPF_DBDESC_INVALID_FLAGS

Details: The database description OSPF message carried invalid flags. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF DB Desc Invalid Options

Base Event: OSPF_DBDESC_INVALID_OPTS

Details: The database description OSPF message carried invalid options. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF DB Desc Short Packet

Base Event: OSPF_DBDESC_SHORT_PACKET

Details: The database description OSPF message was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF External LSA Invalid Flags

Base Event: OSPF_LSA_EXTERNAL_BAD_FLAGS

Details: The OSPF message contained an external LSA with invalid flag bits set. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF External LSA Short Packet

Base Event: OSPF_LSA_EXTERNAL_SHORT_PACKET

Details: The OSPF message contained an external LSA that was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Invalid Version Number

Base Event: OSPF_BAD_VERSION_NUM

Details: An OSPF packet bearing a version number other than 2 was detected. The most current OSPF protocol version number over IPv4 is 2. This may be an attempt to use an obsolete protocol or to compromise the current protocol.

References OSPF Specifications

OSPF LS Request Bad Length

Base Event: OSPF_LSREQ_BAD_LENGTH

Details: The OSPF LS Request message had an invalid length field. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF LS Update Short Packet

Base Event: OSPF_LS_UPDATE_OVERLONG_PACKET

Details: The OSPF LS Update message was longer than the specified length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF LS Update Short Packet

Base Event: OSPF_LS_UPDATE_SHORT_PACKET

Details: The OSPF LS Update message was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF LSA Invalid Options

Base Event: OSPF_LSA_INVALID_OPTS

Details: The OSPF message contained an LSA with reserved bits set in the options field. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF LSA Max Age

Base Event: OSPF_LSA_MAX_AGE

Details: The OSPF message contained an LSA with an age field that exceeded the maximum allowed age (1 hour). This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF LSA Short Packet

Base Event: OSPF_LSA_SHORT_PACKET

Details: The OSPF message carried an LSA that was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Malformed AUTH Field

Base Event: OSPF_BAD_CRYPTO_AUTH_FIELD

Details: The OSPF message carried an authentication type not in the RFC. This may be either a legitimate message using an unassigned authentication type or an attempt to compromise the authentication mechanism of OSPF.

References OSPF Specifications

OSPF Malformed Network LSA

Base Event: OSPF_LSA_NETWORK_BAD_PACKET

Details: The OSPF message contained a malformed network LSA. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Malformed Summary LSA

Base Event: OSPF_LSA_SUMMARY_MALFORMED_PACKET

Details: The OSPF message contained a malformed summary LSA. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Network LSA Short Packet

Base Event: OSPF_LSA_NETWORK_SHORT_PACKET

Details: The OSPF message contained a network LSA that was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Packet Length Mismatch

Base Event: OSPF_PACKET_LEN_MISMATCH

Details: The length specified in the header of the OSPF packet was different from actual packet length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Router LSA Bad Padding

Base Event: OSPF_LSA_ROUTER_BAD_PADDING

Details: The OSPF message contained a router LSA with invalid padding. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Router LSA Invalid Options

Base Event: OSPF_LSA_ROUTER_BAD_FLAGS

Details: The OSPF message contained a router LSA with invalid flag bits set. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Router LSA Short Packet

Base Event: OSPF_LSA_ROUTER_SHORT_PACKET

Details: The OSPF message contained a router LSA that was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Short Packet

Base Event: OSPF_SHORT_PACKET

Details: An OSPF packet shorter than the size of the OSPF header was received. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Summary LSA Short Packet

Base Event: OSPF_LSA_SUMMARY_SHORT_PACKET

Details: The OSPF message contained a summary LSA that was shorter than minimum required length. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Unknown LSA Type

Base Event: OSPF_UNKNOWN_LSA_TYPE

Details: The OSPF message contained an LSA of unknown type. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

OSPF Unknown Message Type

Base Event: OSPF_UNKNOWN_TYPE

Details: The OSPF message was of an unknown type. This violation of the standard could indicate an attempt to compromise the protocol.

References OSPF Specifications

POP3 Auth Aborted

Base Event: IPOP3_CLIENT_AUTH_ABORTED

Details: The POP3 client aborted an authentication exchange. This is unusual behavior and may indicate an attempt to exploit a vulnerability or to probe for weaknesses.

POP3 Malformed Data

Base Event: POP3_CLIENT_BAD_CMD_ARGUMENT

Details: A POP3 violation was detected in an argument to a client's command. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_CLIENT_BAD_INIT_COMMAND

Details: The POP3 client sent an invalid command to the POP3 server. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_CLIENT_CRLF_EXPECTED

Details: A POP3 violation occurred in a client's command. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_CLIENT_DATA_AFTER_QUIT

Details: The POP3 connection did not close after the client sent the QUIT command to the server. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_CLIENT_FAILED_LOGIN

Details: A failed attempt to authenticate/logon using the POP3 protocol was detected. A failed authentication attempt may be an indication of an attack.

POP3 Malformed Data

Base Event: POP3_CLIENT_INVALID_COMMAND

Details: The POP3 client sent an invalid command to the server. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_INVALID_ARG_TO_QUIT

Details: The POP3 client provided an argument to QUIT, which doesn't take any arguments. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_SERVER_BAD_BASE64_STR

Details: The POP3 server sent an invalid base64 string during an authentication exchange with the client. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_SERVER_BAD_GREETING

Details: The POP3 server sent an invalid greeting upon accepting a client's connection. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_SERVER_INVALID_CHAR_IN_RESPONSE

Details: The POP3 server's response violated POP3 protocol. This violation of the standard could indicate an attempt to compromise the protocol.

POP3 Malformed Data

Base Event: POP3_SERVER_INVALID_RESPONSE

Details: The POP3 server's response violated POP3 protocol. This violation of the standard could indicate an attempt to compromise the protocol.

Rlogin Auth Failure

Base Event: RLOGIN_LOGIN_FAILED

Details: An rlogin failed logon attempt was detected. This may be an attempt to break into the server.

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible that this is a user that mistyped his or her password.

References Rlogin Specifications

Rlogin Auth Failure

Base Event: RLOGIN_ROOT_LOGIN_FAILED

Details: A failed root rlogin attempt was detected. This may be an attempt to break into the server.

Response: Audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible that the administrator mistyped his or her password.

References Rlogin Specifications

Rlogin Malformed Data

Base Event: RLOGIN_INVALID_CLI_INIT

Details: Something that doesn't look like a user name was passed to rlogin as the user name.

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Rlogin Specifications

Rlogin Malformed Data

Base Event: RLOGIN_INVALID_CLI_LOGIN_FIELD

Details: Something that doesn't look like a user name was passed to rlogin as the user name.

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Rlogin Specifications

Rlogin Malformed Data

Base Event: RLOGIN_INVALID_SER_LOGIN_FIELD

Details: The user name on the remote host (or server) provided by the client did not conform to the RFC.

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Rlogin Specifications

Rlogin Malformed Data

Base Event: RLOGIN_INVALID_SERVER_INIT

Details: The server sent back something that doesn't look like the start of a rlogin session when establishing a session.

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Rlogin Specifications

Rlogin Malformed Data

Base Event: RLOGIN_INVALID_TERM_FIELD

Details: An invalid terminal type specified was specified in a rlogin session.

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Rlogin Specifications

Rlogin Malformed Data

Base Event: RLOGIN_INVALID_USERNAME

Details: One of a set of “bad” user names was used in a rlogin attempt (for example, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, or nobody4).

Response: If seen in sufficient volume or variation, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References Rlogin Specifications

RPC Malformed Data

Base Event: RPC_BUFFER_OVERFLOW

Details: A possible buffer overflow was seen in the RPC traffic.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_INVALID_ACCEPTED_TYPE

Details: There are six types of messages that are in an RPC packet (marked by a string of three consecutive null characters, followed by a fourth character of value 0x0 to 0x5). This event is triggered if a type other than the six known types was specified.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_INVALID_MTYPE

Details: A RPC MTYPE was specified that is out of range. MTYPE can only be 0 or 1, even though it is represented as a 32-bit quantity.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_INVALID_REJECTED_REPLY

Details: The RPC reply specifying why a packet was rejected was out of range. According to the specification, rejection replies must contain two characteristic id strings: “null null null null” or “null null null 0x01 null null null” followed by a character in the normal ASCII range.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_INVALID_VERSION

Details: Version number in the RPC packet is invalid.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_NULL_RMFRAG

Details: An RPC packet indicated that a fragment was coming, but the first packet contained no data.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_PACKET_OVERRUN

Details: Extra data was sent after a valid RPC packet. This may be a buffer overflow attempt.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_RUNT_PACKET

Details: A RPC packet length was sent in an RPC packet header that was shorter than the length of a valid RPC header.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RPC Malformed Data

Base Event: RPC_SHORT_PAYLOAD

Details: The end of the valid RPC packet was reached prior to the end of the transport packet. This is in violation of the RFC.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References RPC Specifications

RSH Auth Failure

Base Event: RSH_LOGIN_FAILED

Details: An rsh authentication attempt was made that resulted in failure.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References http://www.whitehats.com (arachNIDS #392)
http://www.whitehats.com (arachNIDS #393)

RSH Auth Failure

Base Event: RSH_ROOT_LOGIN_FAILED

Details: A failed root rsh attempt was detected.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References http://www.whitehats.com (arachNIDS #389)

RSH Bad Username

Base Event: RSH_INVALID_USERNAME

Details: One of a set of “bad” user names was used in a rsh attempt (for example, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, or nobody4).

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

RSH Malformed Data

Base Event: RSH_INVALID_CLI_LOGIN_FIELD

Details: The username logon field sent by the rsh client did not conform to the RSH standard.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

RSH Malformed Data

Base Event: RSH_INVALID_COMMAND_LINE

Details: Something was passed to rsh that doesn’t look like a valid command line.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

RSH Malformed Data

Base Event: RSH_INVALID_LOC_LOGIN_FIELD

Details: An invalid username was specified as the local user in an rsh session.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

RSH Malformed Data

Base Event: RSH_INVALID_SERVER_INIT

Details: The server sent a response that didn't appear to be a normal rsh response.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

SMB Auth Failure

Base Event: SMB_DEL_ACCESS_DENIED

Details: An SMB delete (file or remove directory) command was issued, but the request resulted in an access denied error message.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References SMB Information

SMB Auth Failure

Base Event: SMB_SESSION_ACCESS_DENIED

Details: General SMB access denied condition. For example, if a request to a resource such as disk or printer share is made, but the user ID with which the command is issued is not in the ACL list of the resource, the server will return an error that would trigger this event.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References SMB Information

SMB Auth Failure

Base Event: SMB_SESSION_BAD_PASSWORD

Details: User gave an incorrect password during SMB logon.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References SMB Information

SMB Auth Failure

Base Event: SMB_TREE_ACCESS_DENIED

Details: General SMB access denied condition.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References SMB Information

SMB Auth Failure

Base Event: SMB_TREE_BAD_PASSWORD

Details: User gave an incorrect password during SMB logon.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References SMB Information

SMB Guest Connection

Base Event: NBT_SMB_GUEST_LOGIN

Details: A NetBIOS guest logon attempt was detected.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References CAN-1999-0518

SMB Information

SMB Guest Connection

Base Event: SMB_GUEST_LOGON_ATTEMPT

Details: An SMB logon with the username of “guest” was attempted. Attempts to use default or guest accounts may indicate an information gathering or unauthorized access attempt.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References CAN-1999-0518

SMB Information

SMB Malformed Data

Base Event: SMB_INVALID_HEADER

Details: An invalid SMB packet header was detected.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References CAN-1999-0518

SMB Information

SMB Malformed Data

Base Event: SMB_SHORT_BATCHED_PAYLOAD

Details: The batched payload on the SMB packet was shorter than expected.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: None known.

References CAN-1999-0518

SMB Information

SMB Short Password

Base Event:	SMB_SHORT_PASSWORD
Details:	A logon attempt was made with a short password (under 4 chars).
Response:	If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.
Affected:	No specific targets.
False Positives:	None known.
References	CAN-1999-0518 SMB Information

SMTP Bad Email Address

Base Event:	SMTP_BAD_EMAIL_ADDRESS
Details:	A recipient's email address did not conform to the RFC. This may indicate an attempt to exploit a address handling vulnerability on the server.
Response:	If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.
Affected:	No specific targets.
False Positives:	It is possible this is simply a user or server configuration error.
References	SMTP Specifications

SMTP EXPN denial-of-service

Base Event:	SMTP_EXPN_DOS
Details:	The client sent an invalid EXPN response to an SMTP request. The response may crash the server.
Response:	An audit of the client and server is recommended.
Affected:	No specific targets.
False Positives:	None known.
References	SMTP Specifications

SMTP Login Failed

Base Event:	SMTP_AUTHENTICATION_FAILED
Details:	This corresponds to a SMTP response code of 535 being detected. Large numbers of these may indicate someone attempting to compromise a mail account.
Response:	Response typically involves locating the source and verifying if it is a legitimate client or not.
Affected:	No specific targets.
False Positives:	None known.
References	SMTP Specifications

SMTP Malformed Data

Base Event: SMTP_BAD_SERVER_BANNER

Details: The SMTP server sent an unrecognized banner at the start of an SMTP session. It is possible this could indicate a compromised server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible this is a server configuration error.

References SMTP Specifications

SMTP Malformed Data

Base Event: SMTP_BAD_SERVER_DATA

Details: A catch all error event indicating that the data sent from the SMTP server was not recognized as complying with the SMTP RFCs. It is possible that this represents an attack on the SMTP server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible that this is either something tunneling on the SMTP port or some unusual extension or data being passed over SMTP.

References SMTP Specifications

SMTP Malformed Data

Base Event: SMTP_CLIENT_BAD_BDAT_ARG

Details: The client sent an invalid argument to the SMTP BDAT command.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible that this is a mail client or server using an unofficial protocol extension or non-compliant SMTP implementation.

References SMTP Specifications

SMTP Malformed Data

Base Event: SMTP_CLIENT_DATA_BEFORE_HELO

Details: The SMTP client sent something other than a HELO command at the start of the SMTP session. Well behaved clients should start a connection with a HELO. It is possible this represents a manual probe of the server.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is also possible this is a non-compliant SMTP client implementation.

References SMTP Specifications

SMTP Malformed Data

Base Event: SMTP_CLIENT_MALFORMED_COMMAND

Details: The client sent an SMTP command to the server that was not a recognized RFC 821 command.

Response: If seen in sufficient volume or variation, and other suspicious factors exist, audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible this is a mail client or server using an unofficial protocol extension or non-compliant SMTP implementation.

References SMTP Specifications

SMTP Malformed Domain Name

Base Event: SMTP_CLIENT_BAD_DOMAINNAME

Details: A domain did not conform to the RFC. This may indicate an attempt to exploit a domain handling vulnerability on the server. If seen in sufficient volume or variation audit of client and server is recommended.

Response: If seen in sufficient volume or variation and other suspicious factors exist audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected: No specific targets.

False Positives: It is possible this is simply a user or server configuration error.

References SMTP Specifications

SNMP Malformed BER/ASN.1 data encoding

Base Event:	SNMP_ASN1_DATALENGTH_VALUE_TOO_SMALL
Details:	An element of BER encoded ASN.1 data specified a data field size that was too small for its indicated primitive type.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

SNMP Malformed BER/ASN.1 data encoding

Base Event: SNMP_ASN1_TOO_MANY_NESTED_LEVELS

Details: More levels of nested BER encoded ASN.1 sequences were detected in a SNMP message than the maximum depth implied by the SNMP specifications.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

SOCKS Malformed Data

Base Event: SOCKS_INVALID_DATA

Details: The Client attempted to initiate a SOCKS session with a non-compliant initialization sequence.

SOCKS4 Malformed Data

Base Event: SOCKS4_INVALID_RESPONSE

Details: The SOCKS4 server sent an invalid response.

SOCKS4 Request Denied

Base Event: SOCKS4_REQUEST_DENIED

Details: The SOCKS server sent a response to the client indicating that its request has been denied.

SOCKS5 Auth Failure

Base Event: SOCKS5_AUTHENTICATION_FAILURE

Details: The SOCKS server issued a response to the client that it has failed to authenticate to the SOCKS server.

SOCKS5 Chaining

Base Event: SOCKS5_CHAIN_ATTEMPT

Details: The client sent a request that the SOCKS server set up a connection to another SOCKS server.

SOCKS5 Invalid Command

Base Event: SOCKS5_COMMAND_NOT_SUPPORTED

Details: The SOCKS server sent a response to the client indicating that the command it requested is not supported.

SOCKS5 Malformed Data

Base Event: SOCKS5_INVALID_REQUEST

Details: The Client requested an invalid SOCKS connection type.

SOCKS5 Malformed Data

Base Event: SOCKS5_INVALID_REQUEST_VERSION

Details: The client specified an unrecognized version of SOCKS in its request.

SOCKS5 Malformed Data

Base Event: SOCKS5_INVALID_RESPONSE_VERSION

Details: The SOCKS server responded with an unrecognized version number.

SOCKS5 Malformed Data

Base Event: SOCKS5_NULL_DESTADDRESS

Details: The client requested that the SOCKS server connect it to a NULL destination address.

SOCKS5 Request Denied

Base Event: SOCKS5_REQUEST_DENIED

Details: The SOCKS server sent a response to the client indicating that its request has been denied.

Suspicious SNMP Traffic

Base Event: SNMP_EMPTY_COMMUNITY_STRING_BULKREQUESTPDU

Details: An empty community string was detected in a Bulk Request PDU, (SNMP V2 and higher only). Empty or weak community strings are not considered secure in many network environments.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: Many network devices use weak or empty community strings by default.

References:
RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_EMPTY_COMMUNITY_STRING_REQPDU
Details:	An empty community string was detected in a request PDU, Empty or weak community strings are not considered secure in many network environments.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	Many network devices use weak or empty community strings by default.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_EMPTY_COMMUNITY_STRING_TRAPPDU

Details: An empty community string was detected in a Trap PDU, (SNMP V1 only). Empty or weak community strings are not considered secure in many network environments.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: Many network devices use weak or empty community strings by default.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INSECURE_COMMUNITY_STRING_BULKREQUESTPDU
Details:	An insecure community string (either “public” or “private”) was detected in a Bulk Request PDU, (SNMP V2 and higher only). Empty or weak community strings are not considered secure in many network environments.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	Many network devices use weak or empty community strings by default.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_INSECURE_COMMUNITY_STRING_REQPDU

Details: An insecure community string (either “public” or “private”) was detected in a Request PDU. Empty or weak community strings are not considered secure in many network environments.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: Many network devices use weak or empty community strings by default.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INSECURE_COMMUNITY_STRING_TRAPPDU
Details:	An insecure community string (either “public” or “private”) was detected in a Trap PDU, (SNMP V1 only). Empty or weak community strings are not considered secure in many network environments.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	Many network devices use weak or empty community strings by default.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_INVALID_BULK_MAXREPETITIONS

Details: The value specified for the “Max Repetitions” parameter of a Bulk Request PDU fell outside the allowed bounds. (SNMP V2 and higher only).

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INVALID_BULK_NONREPEATERS
Details:	The value specified for the “Non-Repeaters” parameter of a Bulk Request PDU fell outside the allowed bounds. (SNMP V2 and higher only).
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_INVALID_ERROR_INDEX

Details: The value specified for the “Error Index” parameter of a Request PDU fell outside the allowed bounds.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:
RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INVALID_ERROR_STATUS
Details:	The value specified for the “Error Index” parameter of a Request PDU fell outside the allowed bounds.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INVALID_GENERIC_TRAP
Details:	The “Generic Trap” parameter of a V1 SNMP trap specified an illegal numeric value.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INVALID_MSGHEADER_MSGID
Details:	The value specified for the “Message ID” parameter in the message header data for a V3 SNMP message fell outside the allowed range of values.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_INVALID_MSGHEADER_MSGMAXSIZE

Details: The value specified for the “Max Message Size” parameter in the message header data for a V3 SNMP message fell outside the allowed range of values. This parameter is used to negotiate the maximum message size that two SNMP entities may send to each other, and has a minimum value of 484, and a maximum value of 2^{31} - 1.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_INVALID_MSGHEADER_MSGSECMODEL
Details:	The value specified for the “Message Security Model” parameter in the message header data for a V3 SNMP message fell outside the allowed range of values.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_MESSAGE_END
Details:	The end of an SNMP message was encountered while more data was still expected.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_BULKREQUEST_MAXREPETITIONS
Details:	The primitive type for the “Max Repetitions” field of a Bulk Request PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_BULKREQUEST_NONREPEATERS
Details:	The primitive type for the “Non Repeaters” field of a Bulk Request PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_BULKREQUESTPDU_REQUEST_ID
Details:	The primitive type for the “Request ID” field of a Bulk Request PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_COMMUNITY_NAME

Details: The primitive type for the SNMP community name did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:
RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_MSGFLAGS

Details: The primitive type for the “Message Flags” field of a SNMP v3 message header did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_MSGID

Details: The primitive type for the “Message ID” field of a SNMP v3 message header did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_MSGMAXSIZE
Details:	The primitive type for the “Max Message Size” field of a SNMP v3 message header did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_MSGHEADER_SECMODEL

Details: The primitive type for the “Message Security Model” field of a SNMP v3 message header did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_MSGSECPARAMS
Details:	The primitive type for the “Message Security Parameters” field of a SNMP v3 message did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_PDU
Details:	The primitive type for the PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_PDU_REQUEST_ID
Details:	The primitive type for the PDU Request ID did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_REQUEST_ERROR_INDEX

Details: The primitive type for the error index in a basic PDU did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_REQUEST_ERROR_STATUS
Details:	The primitive type for the error status of a basic PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_SCOPEDPDU_CONTEXTENGINEID

Details: The primitive type for the “Context Engine ID” of a SNMP V3 Scoped PDU did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_SCOPEDPDU_CONTEXTNAME

Details: The primitive type for the “Context NAME” of a SNMP V3 Scoped PDU did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_SCOPEDPDUDATA

Details: The primitive type for Scoped PDU Data in an SNMP v3 message did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:
RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_TRAP_ENTERPRISE_OID
Details:	The primitive type for the “Enterprise OID” field of a V1 Trap PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_TRAP_GENERIC_TYPE

Details: The primitive type for the “Generic Trap Type” field of a V1 Trap PDU did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_TRAP_SOURCE_ADDRESS

Details: The primitive type for the “Trap Source Address” field of a V1 Trap PDU did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

RFC 1155 - SNMP v1 Specifications

RFC 1157 - SNMP v1 Specifications

RFC 1212 - SNMP v1 Specifications

RFC 1901 - SNMP v2c Specifications

RFC 1902 - SNMP v2c Specifications

RFC 1903 - SNMP v2c Specifications

RFC 1904 - SNMP v2c Specifications

RFC 1905 - SNMP v2c Specifications

RFC 1906 - SNMP v2c Specifications

RFC 1907 - SNMP v2c Specifications

RFC 1908 - SNMP v2c Specifications

RFC 2571 - SNMP v3 Specifications

RFC 2572 - SNMP v3 Specifications

RFC 2573 - SNMP v3 Specifications

RFC 2574 - SNMP v3 Specifications

RFC 2575 - SNMP v3 Specifications

SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_TRAP_SPECIFIC_TYPE

Details: The primitive type for the “Specific Trap Type” field of a V1 Trap PDU did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_TRAP_TIMESTAMP
Details:	The primitive type for the “Time Stamp” field of a V1 Trap PDU did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_V1_PDU

Details: The primitive type for the PDU of a V1 SNMP message did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_V3_MSGHEADER
Details:	The primitive type for the message header of a V3 SNMP message did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNEXPECTED_TYPE_FOR_VARBIND_DATA

Details: The primitive type for the data of a VarBind data pair did not match any of the expected data types for that parameter.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References:

- RFC 1155 - SNMP v1 Specifications
- RFC 1157 - SNMP v1 Specifications
- RFC 1212 - SNMP v1 Specifications
- RFC 1901 - SNMP v2c Specifications
- RFC 1902 - SNMP v2c Specifications
- RFC 1903 - SNMP v2c Specifications
- RFC 1904 - SNMP v2c Specifications
- RFC 1905 - SNMP v2c Specifications
- RFC 1906 - SNMP v2c Specifications
- RFC 1907 - SNMP v2c Specifications
- RFC 1908 - SNMP v2c Specifications
- RFC 2571 - SNMP v3 Specifications
- RFC 2572 - SNMP v3 Specifications
- RFC 2573 - SNMP v3 Specifications
- RFC 2574 - SNMP v3 Specifications
- RFC 2575 - SNMP v3 Specifications
- SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_VARBIND_LIST
Details:	The primitive type for the start of a VarBind list did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_VARBIND_OID
Details:	The primitive type for the OID of a VarBind data pair did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event:	SNMP_UNEXPECTED_TYPE_FOR_VARBIND_PAIR
Details:	The primitive type for the start of a single VarBind pair did not match any of the expected data types for that parameter.
Response:	Location and audit of victim is recommended.
Affected:	Hosts running SNMP agents or managers.
False Positives:	None known.
References:	RFC 1155 - SNMP v1 Specifications RFC 1157 - SNMP v1 Specifications RFC 1212 - SNMP v1 Specifications RFC 1901 - SNMP v2c Specifications RFC 1902 - SNMP v2c Specifications RFC 1903 - SNMP v2c Specifications RFC 1904 - SNMP v2c Specifications RFC 1905 - SNMP v2c Specifications RFC 1906 - SNMP v2c Specifications RFC 1907 - SNMP v2c Specifications RFC 1908 - SNMP v2c Specifications RFC 2571 - SNMP v3 Specifications RFC 2572 - SNMP v3 Specifications RFC 2573 - SNMP v3 Specifications RFC 2574 - SNMP v3 Specifications RFC 2575 - SNMP v3 Specifications SNMP FAQ

Suspicious SNMP Traffic

Base Event: SNMP_UNRECOGNIZED_SNMP_VERSION

Details: The SNMP version number was not a recognized value.

Response: Location and audit of victim is recommended.

Affected: Hosts running SNMP agents or managers.

False Positives: None known.

References: RFC 1155 - SNMP v1 Specifications
RFC 1157 - SNMP v1 Specifications
RFC 1212 - SNMP v1 Specifications
RFC 1901 - SNMP v2c Specifications
RFC 1902 - SNMP v2c Specifications
RFC 1903 - SNMP v2c Specifications
RFC 1904 - SNMP v2c Specifications
RFC 1905 - SNMP v2c Specifications
RFC 1906 - SNMP v2c Specifications
RFC 1907 - SNMP v2c Specifications
RFC 1908 - SNMP v2c Specifications
RFC 2571 - SNMP v3 Specifications
RFC 2572 - SNMP v3 Specifications
RFC 2573 - SNMP v3 Specifications
RFC 2574 - SNMP v3 Specifications
RFC 2575 - SNMP v3 Specifications
SNMP FAQ

Telnet Failed Login

Base Event: TELNET_LOGIN_INCORRECT

Details: A Telnet connection was made, but the authentication resulted in failure. This may indicate someone attempting to compromise an account on the target system.

Response: If seen in sufficient volume or variation location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is just someone mistyping a password though it does indicate the use of clear text logons on your network which would pose a security risk since they are vulnerable to sniffing.

References: CAN-1999-0619
http://www.whitehats.com (arachNIDS #127)
Telnet Specifications

Telnet Failed Login

Base Event: TELNET_ROOT_LOGIN_FAILED

Details: A failed attempt was made to logon as root by means of Telnet. This may indicate someone attempting to compromise a root account on the target system.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: It is possible this is just someone mistyping a root password though remote access as root (as opposed to using “su”) is generally a security risk anyways.

References http://www.whitehats.com (arachNIDS #251)

Telnet Specifications

Telnet WinGate Active

Base Event: TELNET_WINGATE_PROMPT

Details: Telnet Wingate activity was detected. This is a common Relay and SOCKs program that may be exploited.

Response: Location and audit of client and server is recommended.

Affected: No specific targets.

False Positives: None known.

References CAN-1999-0657

http://www.whitehats.com (arachNIDS #2366)

Telnet Specifications

Unauthenticated OSPF

Base Event: OSPF_NULL_AUTHENTICATION

Details: An OSPF message with a null authentication field was detected. Unauthenticated OSPF messages are vulnerable to spoofing and other attacks. All devices participating in OSPF should be configured to use cryptographic authentication.

References OSPF Specifications

Unauthenticated SOCKS4 Connection

Base Event: SOCKS4_UNAUTHENTICATED

Details: The SOCKS4 server sent an unauthenticated reply to the client.

Unauthenticated SOCKS5 Connection

Base Event: SOCKS5_UNAUTHENTICATED

Details: The SOCKS5 server sent an unauthenticated reply to the client.

WIN DNS Malformed Data

Base Event: WIN_DNS_DATA_AFTER_END

Details: Probably a Microsoft Windows DNS implementation talking to a Microsoft WINS name server that violates DNS protocol. Extra data was sent after a valid DNS packet. Probably an overflow attempt.

Response: If seen in sufficient volume or variation, location and audit of client and server is recommended. Examination of the packet contents may provide some additional information about the particular command.

Affected:	No specific targets.
False Positives:	None known.
References	DNS Specifications

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

T

U

V

W