
SecureIP User Guide



Table of Contents

Table of Contents	1
Activation Overview	2
Introduction.....	3
SecureIP Firewall Management and Reporting	3
SecureIP Firewall Management	4
Security Reports	4
Other Firewall Benefits	4
Customer Reporting Portal	4
SecureIP Gateway Antivirus Scanning Option	5
About Managed Gateway Antivirus Scanning.....	5
SecureIP Gateway AntiVirus Scanning Service Benefits	6
SecureIP Remote Access VPN and Site-to-Site VPN Options	6
SecureIP Web Content Filtering Option	6
Web Content Filtering Benefits	7
How Web Content Filtering Works	7
SecureIP Firewall Service Summary.....	9
Hardware and Software	9
SecureIP Services Provisioning	10
SecureIP Reporting Guide	11
SecureIP Firewall Bandwidth Utilization Reports	11
Protocol Usage	13
SecureIP Firewall Security Reports.....	16
Alert Levels	20
Types of Attacks	20
Protocol Descriptions.....	21
Cavalier Business Customer Care and Support Services	23
FAQs.....	24

Activation Overview

The following section provides an overview of the SecureIP service activation process.

1. Customer is required to provide necessary information for services activation, which includes:

- Names and email addresses for authorized contacts.
- External IP address for each firewall.
- External subnet mask for each firewall.
- Internal IP address for each firewall.
- DHCP requirements.
- Firewall configuration files of your previous firewall or detailed configuration requirements.
- Physical address for each location a firewall is to be deployed.

2. Cavalier preconfigures firewall and installs at customer locations along with Internet access device.

4. Cavalier completes configuration remotely.

After the configuration is complete, your SecureIP service is fully operational.

Introduction

Protecting your critical information assets does not stop once your security architecture has been implemented. In order to defend against unauthorized network intrusion, you must continuously monitor your security devices, servers, applications and other networked devices for signs of malicious activity and respond to them in a timely manner. Every aspect of your security solution must be kept updated in real time to keep pace with the evolving threat environment.

Cavalier's SecureIP is a sophisticated yet flexible solution backed by dedicated, around-the-clock security expertise skilled in sifting through the volumes of log files and security alerts to identify the critical threats from the benign events and false-positives in real-time, 24X7.

Cavalier's basic Secure IP Firewall service includes firewall management and reporting. This core service can be upgraded by individually adding one or more optional services including web content filtering, gateway antivirus scanning, and/or email SPAM filtering. Once the basic SecureIP Firewall is installed, you can add any optional services to your existing SecureIP service without deploying additional hardware. Cavalier's SecureIP Firewall Bundle offers the customer the basic SecureIP Firewall bundled with the most popular optional add-on services at a savings over purchasing the bundled service elements ala carte.

Additional SecureIP options include Remote Access VPN which allows remote users to securely access your LAN; Site-to-Site VPN which securely connects two or more of your locations; and Desktop Anti-Virus.

Cavalier's SecureIP services provide the following benefits:

- Reduced capital outlays and operating costs.
- Reduced total cost of ownership.
- No additional staff needed.
- Minimal setup required.

SecureIP Firewall Management and Reporting

Cavalier offers the SecureIP Firewall solution as a first line of defense against threats aimed at your corporate network. Our SecureIP Firewall Service includes ongoing assessments of your firewall and DNS setup, firewall administration, including rule changes, maintenance of traffic flow, and firewall reporting. You can request changes to your firewall configuration at any time; these change requests are then reviewed, implemented, and documented by approved

security personnel. Cavalier's SecureIP Firewall Service helps you achieve the full value from your telecommunications solution investment. With this service, you can be confident that your firewall(s) – which deliver your security strategy's first line of defense – are available, performing well and have not been compromised.

Cavalier currently deploys SecureIP services on the Fortinet Unified Threat Management (UTM) hardware platform.

SecureIP Firewall Management

In addition to maintaining the firewall's configuration according to your needs, Cavalier will monitor the allowed traffic into the firewall to identify and report on common network attack patterns as they occur.

Security Reports

The managed firewall service includes two firewall reports provided online through your secure web-accessible Customer Firewall Portal.

- Monthly firewall bandwidth report that shows outbound traffic. This report highlights top users of network resources and user activity for a variety of different protocols.
- Firewall security report, detailing inbound network activity on a daily, weekly or monthly basis. An executive summary provides an overview of security alerts on the firewall over a specific period of time.

Other Firewall Benefits

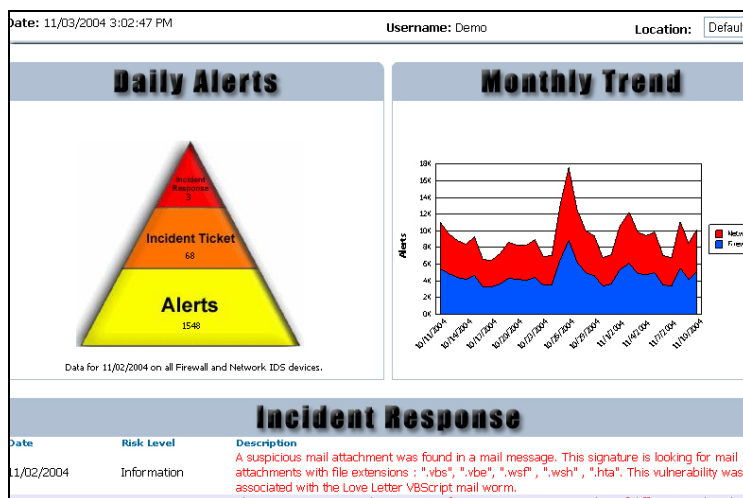
- Continuous event monitoring
- Proven security architecture
- Seamless operations
- Readily available targeted reporting
- Safety and protection of your data
- Compliance with regulatory guidelines (available to healthcare and financial institutions for an additional charge)

Customer Reporting Portal

The SecureIP Firewall removes the complexity from IT security management by offering:

- 24 x 7 IT security services that empower organizations with a proactive approach to managing a sound IT security program.

- Services that are designed to meet the stringent requirements of GLB, HIPAA, and ISO 17799.
- Services that have been put to the test and have been proven to satisfy or exceed regulatory examiners' evaluation criteria.



SecureIP Gateway Antivirus Scanning Option

Cavalier's Gateway AntiVirus Scanning is a real time, scalable and highly reliable solution to help manage your antivirus protection needs. By implementing the Managed Antivirus Scanning Service, you are provided with an added level of protection against the number one enemy facing today's network environments. The Gateway Antivirus Scanning service allows companies to scan all incoming IP traffic (web, email, and ftp) for virus infection. Viruses are eliminated from entering your network since packets are inspected at the gateway between the company's LAN and the Internet. Most importantly, network administrators are relieved of the tedious task of updating virus patterns through the use of automatic updates.

About Managed Gateway Antivirus Scanning

The Gateway Antivirus Scanning service is a Gateway Antivirus solution that stops traffic at the main corporate entry point or gateway before any harm can be caused to your internal network. Cavalier can deploy and configure the SecureIP Gateway Antivirus Scanning solution remotely on the provided UTM device once this device is in place and connected back to Cavalier's Security Operations Center (SOC).

With managed virus detection services, engineers are able to configure, monitor and maintain for you an enterprise-wide antivirus solution from a central location. The service is managed from Cavalier's SOC allowing virus patterns and updates to be

pushed to your network gateway. With SecureIP Gateway Antivirus Scanning, administrators can have confidence that the gateway is protected against the latest virus and malicious content threats.

SecureIP Gateway AntiVirus Scanning Service Benefits

- Central management of your corporate antivirus program
- Provides network-wide virus statistics and analysis
- Allows automatic, single-point updates of virus patterns, engine and patch files
- Enforces enterprise-wide virus protection policy

SecureIP Remote Access VPN and Site-to-Site VPN Options

Cavalier's SecureIP Virtual Private Network (VPN) Services provide routing, encryption, authentication and data integrity for secure connectivity across managed IP networks and the Internet. Cavalier's SecureIP VPN Services connect remote users, branch offices, suppliers, and customers with the cost and performance advantages of public IP networks and the security and control found in private networks.

Cavalier realizes the security concerns with protecting remote users trying to access sensitive information. Cavalier's SecureIP VPN Services provide secure, encrypted paths over the Internet for employees and/or business partners to access confidential institution resources. One of the benefits of using our SecureIP VPN Services is that all encrypted data is checked to ensure that no viruses, malware, spyware or other harmful activity enters your network. We ensure all traffic coming in through the VPN is secure within your solution. In addition, VPN traffic reports are provided via the UTM device's Customer Reporting Portal.

SecureIP Web Content Filtering Option

Cavalier has combined its 24 x 7 security monitoring services with the 'best of breed' web content inspection software to aid organizations in proactively increasing employee productivity while avoiding the legal liability associated with inappropriate web content and simultaneously reducing any unnecessary load on corporate network Internet bandwidth.

Cavalier's SecureIP Web Content Filtering solution offers the most advanced and complete monitored content security product available on the market today, providing the perfect balance between efficient content security and peace of mind. With its unique proactive technologies and advanced architecture, Cavalier's Web Content Filtering solution stays ahead of threats to employee productivity.

Cavalier's Web Content Filtering solution is a hosted service designed to provide Web URL filtering for schools, libraries, government agencies, and businesses of all sizes. This solution also includes the FortiGuard Rating Server from our UTM device manufacturer, Fortinet. The

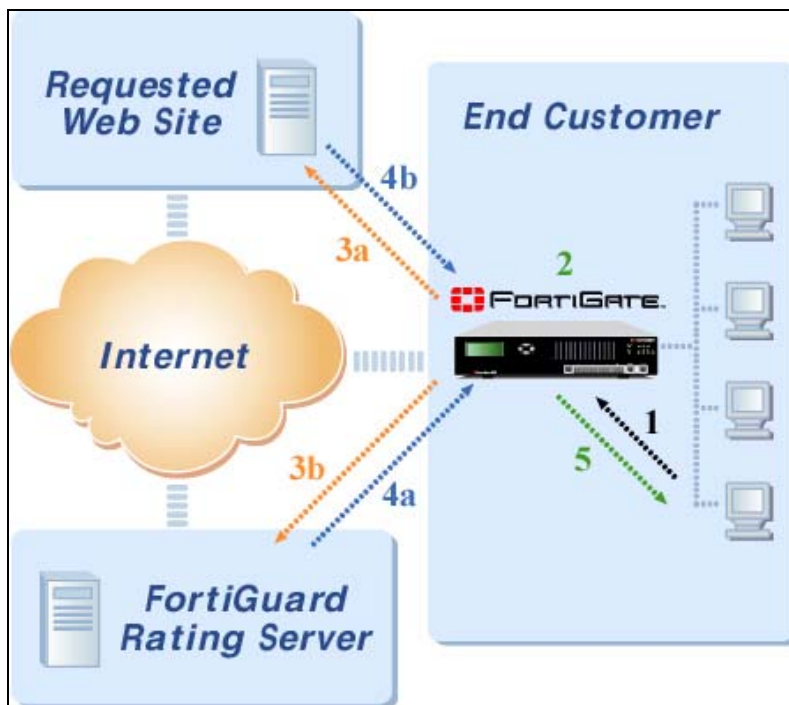
FortiGuard Rating Server is a master web site ratings database that is made up of 5 million web sites and over 1 billion pages, sorted into 56 categories. The FortiGuard web filtering solution reduces the substantial risks and legal liability associated with inappropriate and illegal content.

Web Content Filtering Benefits

- Fast and transparent real-time inspection of Internet traffic
- Web-filtering database of more than five million websites organized into 56 content categories
- 24 x 7 monitoring and technical support
- Trained and certified security professionals

How Web Content Filtering Works

The following diagram details how Firewall Web Content Filtering works.



1. User requests a URL.
2. If the rating for the URL is already cached in the FortiGate unit, it is immediately compared with the policy for the user. If the site is allowed, the page is requested (3a) and the response is retrieved (4b).
3. If the URL rating is not in the FortiGate cache, the page is requested (3a) and a rating request is made simultaneously to the FortiGuard Rating Server (3b).

4. When the rating response is received by the FortiGate unit (4a), it is compared with the requestor's policy (2). The response from the Web site (4b) is queued by the FortiGate unit if necessary until the rating is received.
5. If the policy is to allow the page, the Web site response (4b) is passed to the requestor (5). Otherwise, a user-definable "blocked" message is sent to the requestor and the event is logged in the web content filtering log.

SecureIP Firewall Service Summary

DESCRIPTION	COVERAGE
Hours of Operation	24 x 7 x 365
<u>Response Time</u>	
<i>Critical</i>	4 Hours
<i>Non-Critical</i>	Next Business Day
Change Request Incidents	3 per Month (Advance Scheduled)
Security Incident Alerts	Unlimited
<u>Monitoring</u>	
<i>Uptime</i>	8:30 AM - 6:30 PM (M-F)
<u>Security Reporting</u>	
<i>Daily</i>	Included
<i>Weekly</i>	Included
<i>Monthly</i>	Included
<u>VPN Support</u>	
<i>Remote VPN</i>	Per Incident
<i>Site-to-Site VPN</i>	Per Incident
<u>Additional Services</u>	
<i>OS Upgrades</i>	Fee Based
<i>Patch Updates</i>	Fee Based
<i>Subscription Updates</i>	Included

Hardware and Software

- Fortinet FortiGate security device (provided by Cavalier)
 - 8 x 5 Forticare hardware maintenance/support coincident with MSA term
 - Next business day replacement of failed UTM device
 - FortiGuard service subscription coincident with MSA term for: Firewall, Antivirus, SPAM Filtering, and Web Content Filtering
 - Transfer of administrative credentials to Cavalier
- Fortinet VPN client software for remote VPN options.

SecureIP Services Provisioning

Before Cavalier can provision your SecureIP services, we require the following information:

- Names and email addresses for authorized contacts.
- External IP address for each firewall.
- External subnet mask for each firewall.
- Internal IP address for each firewall.
- DHCP requirements.
- Firewall configuration files or detailed configuration requirements.
- Physical shipping addresses for each location an appliance is to be deployed.

If you did not provide this information at the time you ordered new services, you will need to present this information to Cavalier before we can enable your newly ordered SecureIP services.

The following actions are required to install the provided UTM device and implement SecureIP services:

1. Cavalier will contact you prior to your scheduled "cut date."
2. Cavalier will send an installation technician on site to complete the physical installation of the preconfigured UTM device and the Internet access device.
3. Cavalier will verify remote connectivity to the installed UTM device.
4. Cavalier will complete the remote lock-down of the UTM device.
5. Cavalier will then complete any additional configuration requirements and option activation (such as remote VPNs).
6. Cavalier will test and verify all required connectivity and that all traffic is flowing normally into and out of your network.
7. Cavalier will send you login credentials for your customer reporting portal via secure email.

SecureIP Reporting Guide

This section describes the reports available for common tasks you will perform and notifications you will receive when you use SecureIP services. These reports are available in your secure reporting portal available at <https://www.cavtel.com/cavconnect/login.php>. After your device installation is complete, Cavalier provides you with the login credentials you use to access your secure portal.

SecureIP Firewall Bandwidth Utilization Reports

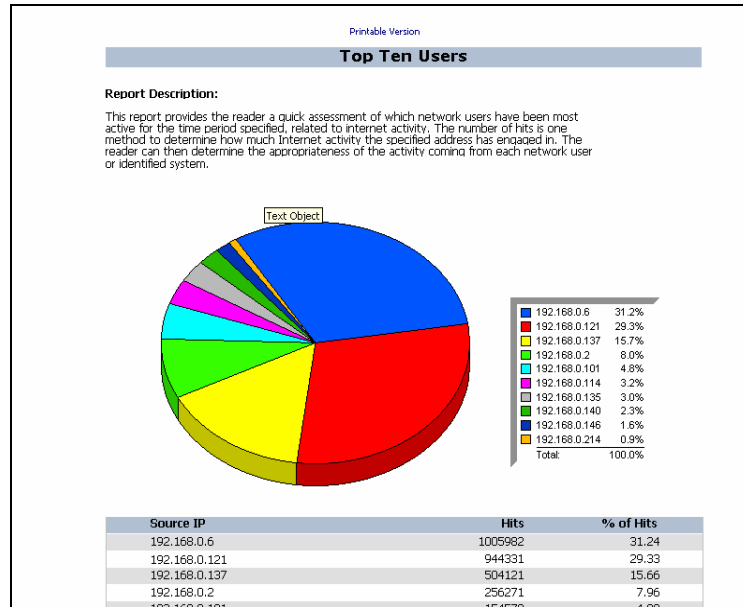
In these reports, users on your network are identified by IP (Internet Protocol) addresses. Destination IP addresses in these reports are queried against a DNS (Domain Name Server) where possible and appear as domain names whenever possible. Networks that do not have associated DNS names will appear as the raw public IP addresses. If a site is listed by IP address instead of the domain name, you can type that address into your Internet browser to display the location.

The term "hits" used in these reports refers to the number of times a particular site was visited and the number of times that site was refreshed with information during the sessions.

The following bandwidth utilization reports are available within the secure Customer Reporting Portal:

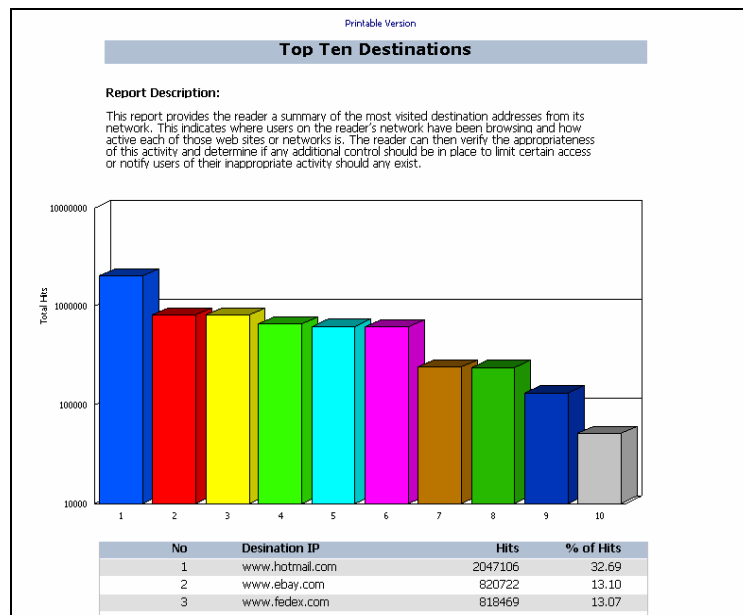
Top 10 Users

A pie chart that depicts the network users who have been most active on the Internet over a one-month period.



Top 10 Destinations

A bar chart of the 10 most visited sites (websites or other networks) going out from the firewall over a one-month period. The chart depicts the number of hits on these sites as a percentage of the total number of hits.



Users with Destinations

A chart of the top 10 users and the sites visited over a one-month period. It is a listing by company IP address and then by websites or networks. If inappropriate activity is identified in either of the first two reports, you will be able to gain more intelligence regarding who, when, where and how often from this report. This report could serve as documentation should any action need to be taken against an employee for inappropriate use or abuse of the Internet which violated company policy.

Top Web Sites

A bar chart of the top 30 most actively visited sites by your network. This report helps you identify staff utilization of the network to conduct research and other activities.

Top FTP Sites

A bar chart of the top 30 most actively visited sites from which file transfers were conducted. FTP refers to File Transfer Protocol. See "Protocol Descriptions" for more information on protocols. This chart identifies both sites from which files were downloaded and sites to which files were posted from your network.

Top Mail Server

A bar chart of the most frequently accessed SMTP (Simple Mail Transfer Protocol) Sites using Port 25 on the firewall over a one-month period. This includes both sending and receiving mail sites. See "Protocol Descriptions" for more information on SMTP protocol.

TCP Hourly Traffic

Monthly average of the TCP (Transmission Control Protocol) hourly traffic. See "Protocol Descriptions" for more information on TCP protocol.

UDP Hourly Traffic

Monthly average of the UDP hourly traffic. See "Protocol Descriptions" for more information on UDP protocol.

Protocol Usage

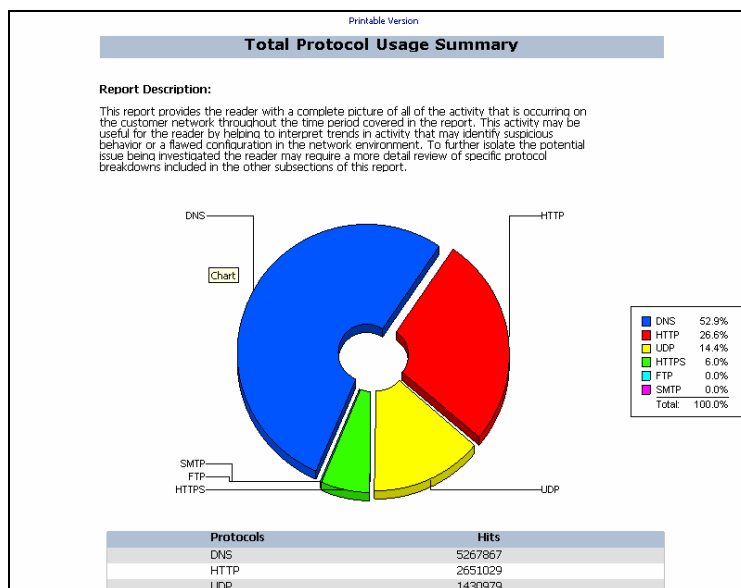
A protocol is a documented format for the transmission of data between two networked devices. A protocol is essentially a "language" that computers use to communicate. For this communication to take place between two computers, both machines must use the same language. Computers use many different protocols to communicate. In most cases, computers will use standard network communication protocols; however, proprietary protocols are used

in some cases. A description of protocols can be found in the “Protocol Descriptions” section of this document.

The following protocol utilization reports are available within the secure Customer Reporting Portal:

Total usage

This pie chart report provides you with a complete picture of all of the activity that is occurring on your network over a one-month period. This activity may be useful by helping to interpret trends in activity that may identify suspicious behavior or a flawed configuration of the network environment. To further isolate any potential issue you may require a more detailed review of specific protocol breakdowns included in the subsections of this firewall bandwidth report.



HTTP usage

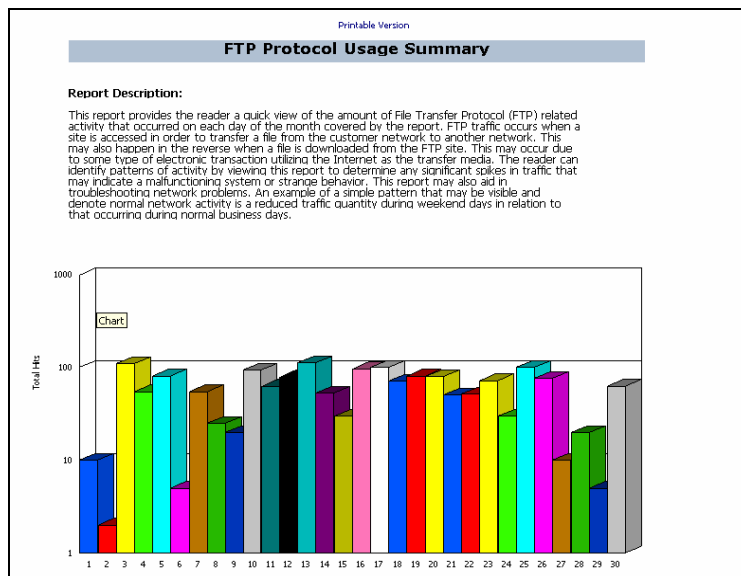
This bar chart provides a quick view of the amount of Hyper-Text Transfer Protocol (HTTP) activity that occurred on each day of the month covered by this report. HTTP activity is typical web browsing that takes place by clicking on websites. This activity relates to web browsing of Internet websites. As users access a site via the Internet, data will flow between your network and the site. The report shows the volume of activity associated with each of the most active users. Spikes in traffic may indicate a malfunctioning system or unusual employee behavior. This report may aid you in troubleshooting network problems. An example of a simple pattern that may be visible and reflect normal network activity is a reduction of traffic quantity on weekends.

HTTPS usage

This bar chart provides a quick view of the amount of Hyper-Text Transfer Protocol Secure (HTTPS) activity that occurs each day. HTTPS is a protocol that is used when a secure communication is established with a website. This occurs with some types of electronic transactions using the Internet as the transfer medium (e.g. credit card transactions).

FTP usage

This bar chart provides a quick view of the amount of File Transfer Protocol (FTP) activity that occurs each day. FTP traffic occurs when a web site is accessed in order to transfer a file to or from your network. This chart shows the number of times a given file transfer is attempted but does not necessarily reflect the number of actual file transfers occurring on a given day.



DNS usage

This bar chart shows the number of times an IP address is translated into a website name using the Domain Name Server (DNS) protocol. It is an indication of the Internet usage on a particular day during the month of the report.

TCP usage

This bar chart shows the traffic on the firewall using the TCP protocol over a one-month period.

UDP usage

This bar chart shows the traffic on the firewall using the UDP protocol over a one-month period.

SMTP usage

This bar chart shows the mail traffic on the firewall over a one-month period.

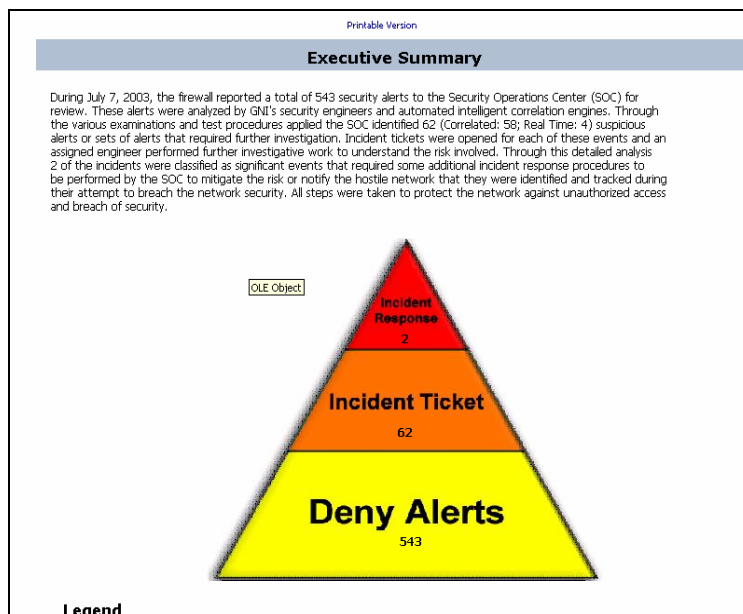
SecureIP Firewall Security Reports

The following firewall security reports are available within the secure Customer Reporting Portal:

Executive Summary

The Executive Summary report is divided into three sections: a summary at the top, a pyramid in the middle, and a legend at the bottom. The summary shows the time period, total number of alerts, the number of suspicious alerts (broken down into either real time or correlated), and the number of incident responses. Further detail is provided on the distinction between the types of alerts. The pyramid is a visual interpretation of the alert information. The legend details the following alert levels depicted by the pyramid:

- Incident Ticket – These are events that raised suspicion within the SOC and required further monitoring. Upon completion of the monitoring, it was determined that the event was not threatening to your environment due to network configuration or other criteria. Although these events were subsequently reclassified as lower risk incidents, they will be correlated against future attack scenarios launched against the network.
- Alerts – these are the detail points that are sent from the firewall devices to the SOC to be used in the correlation systems that identify malicious behavior on your network.



Correlated Tickets

Trending firewall alerts over period of time (daily, weekly, or monthly) creates a correlated ticket. A correlated ticket reflects a suspicious set of security events from a specific source network. The alerts in these tickets may have started out as low priority but due to their frequency, source, and behavioral patterns, the priority of these alerts is elevated. For more detail, see the Hostile Networks report in the Security Report section at the end of this report.

Printable Version

Correlated Tickets

Report Description:
This report provides the correlation ticket's detail documentation for each of the Incidents worked on by the SOC engineers during the term of the reporting period. These tickets exclude those that were elevated to Incident Response status.

Ticket	Final Risk	Open Date	Alert Name	Source IP	Destination IP
6900	High	7/7/2003 1:07:27AM	IP Spoof	192.168.227.42	192.168.51.245
Technical Description This ticket was created as a result of a set of security events that caused a high degree of suspicion related to the communication and behavioral patterns observed from the source network identified. For more detail descriptions of the group of security events which together elevated the risk rating and triggered this incident ticket please view the Hostile Network Detail Report.					
Actions Taken The source network has been added to a high-watch list and will be flagged for review if used in future attacks against the customer network. The correlation of this event and other suspicious behavior sets originating from this source will provide greater capability to determine future malicious intent originating against the customer network. After further analysis no addition action was deemed necessary at this time by the Security Operations Center.					
6901	High	7/7/2003 1:07:27AM	IP Spoof	192.168.227.42	192.168.51.244
Technical Description This ticket was created as a result of a set of security events that caused a high degree of suspicion related to the communication and behavioral patterns observed from the source network identified. For more detail descriptions of the group of security events which together elevated the risk rating and triggered this incident ticket please view the Hostile Network Detail Report.					
Actions Taken The source network has been added to a high-watch list and will be flagged for review if used in future attacks against the customer network. The correlation of this event and other suspicious behavior sets originating from this source will provide greater capability to determine future malicious intent originating against the customer network. After further analysis no addition action was deemed necessary at this time by the Security Operations Center.					

Incident Response Activity

This report summarizes the security events that required the use of the pre-defined incident response procedure. These procedures consist of: researching the event, notifying the intruder that they have been engaged in malicious activity against a protected network, and completing steps necessary to mitigate the risks associated with the identified event.

Some of these incidents may require your additional action or review to properly mitigate the risk and close the ticket. Incident Response Activity events are the response to a high priority alert that appears either in the real-time tickets or the correlated tickets section of this report. These are the most severe incidents that can occur on your firewall.

Hostile Networks – Top Sources

This report identifies networks that have shown a higher than normal intent to cause damage, interrupt service or infect your network with viruses during the time period covered in this report. This type of activity has caused these networks to be labeled as hostile to your environment.

This information is helpful to conduct further research identifying true intent of the hostile system, to contact the network administrator of the hostile network, and to build more intelligent modeling to identify future malicious behavior that will enable you to deploy more proactive strategies to protect your environment.

Hostile Networks – Sources and Destinations

This report presents the detail activity associated with each network identified as hostile. The data included shows each security event originated by the source of the attacks.

This report provides a good foundation for understanding the intent of activity being performed by hostile networks. This report will help identify cases where an intruder's behavior is growing more harmful over time or combinations of activity may prove more harmful than events examined individually.

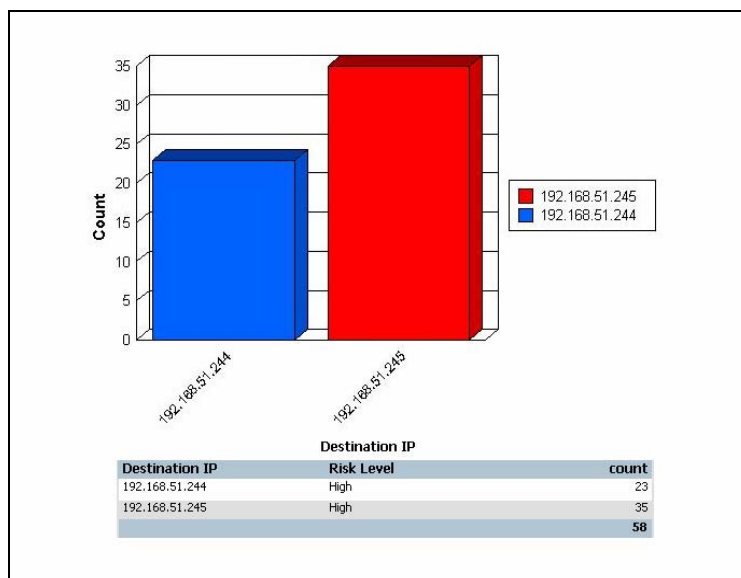
Targets of Attack – Top Destinations

This report summarizes the targets of attacks that are launched against your network devices. This report is used to gain an understanding of how the network perimeter is being viewed by outside attackers and what is being perceived as a valuable target.

This information is helpful in drawing conclusions about the intentions of hostile activity and about your Internet footprint (this is the apparent size of your network to public users on the Internet). If the footprint is too large it may encourage a greater amount of interest from random malicious users. You can use this data to proactively identify growing issues or carry out risk mitigation activities where possible.

Targets of Attack – Destinations and Sources

This report supplies information regarding the detail surrounding attacks launched against specific components of your network perimeter. You can use this data to further identify the intentions of a malicious user or a growing threat specific to an individual network device or other component.



Intrusion Alert – Top Alerts

Bar chart of the types of alerts that occurred on the firewall and the number of times that each type occurred.

Intrusion Alert – Alert Details

This report provides additional detail about the alerts that were recorded and forwarded to the SOC from the UTM device. This information is accumulated over

various periods of time to help identify trends in behavior patterns that would cause suspicion and help you identify malicious activity targeted at your network.

Alert Levels

Default Risk Level

Individual alerts have a default risk that is assigned to them automatically, before any other factors are taken into consideration. This risk level may be inaccurate depending on factors such as the total number of alerts, related alerts from the same source address, similar alerts from different source addresses, etc.

GNI Risk Level

This is the actual risk assessment by Cavalier security operations personnel. This risk level indicates that other factors have been taken into consideration when the risk was evaluated. For example, a relatively low default risk may be raised if there is an excessively high number of alerts, or vice versa; an alert with a high default risk may be considered a lower risk if there were no related attacks during the same time frame.

Types of Attacks

IP Spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Port Scanning

The act of systematically scanning a computer's ports. Since a port is one of many similar places where information can go into and out of a computer, port scanning is utilized to identify open doors to a computer. Port scanning has legitimate uses in managing networks but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Syn Flood Attack

A type of denial of service attack in which a large number of TCP SYN packets (the first packet in a TCP/IP connection), usually with spoofed source IP addresses, are sent to a target. The target system replies with the corresponding ACK

(acknowledgement) packets and waits for the final packet of the TCP/IP three-way handshake. Because the source IP address of the initial packet is spoofed, the target never will receive the final packet, leaving it to hold TCP/IP sessions open until they time out. A SYN flood causes so many simultaneous TCP/IP open sessions that the system becomes overwhelmed and cannot handle any more network traffic

Protocol Descriptions

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. Since it is limited in its ability to queue messages at the receiving end, SMTP is usually used with one of two other protocols (POP3 or Internet Message Access Protocol) that let the user save messages in a server mailbox and download them periodically from that server. In other words, users typically employ a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been collected for them at their local server. Most mail programs such as Eudora let you specify both an SMTP server and a POP server. On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail. Sendmail is a commercial package which includes a POP3 server and also comes in a version for Windows NT.

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track

of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address

Cavalier Business Customer Care and Support Services

Cavalier's Business Customer Care and Support can be reached 24 hours a day, 7 days a week by contacting:

PHONE: (866) 221-1063

EMAIL: help@cavtel.net

FAQs

Below are some answers to frequently asked questions about Cavaliers SecureIP Services.

What reports are available through the Customer Reporting Portal?

You can view the following reports: Firewall Security, Firewall Bandwidth and Gateway Antivirus.

Is there a “complete” report for downloading the Firewall Security, Firewall Bandwidth and Antivirus sections?

Yes, there is a complete report option for these reports. For firewall bandwidth, the “complete report” option is per section because the PDF file would be very large for the whole report. For instance, the “general” section can be made into a single report, etc.

Can I search for a specific IP address that is attacking us, within a date range?

The Firewall Security report allows you to search a specific day, week or month. Within each of those reports you can look at the details of alert activity by source IP address within the “Security Reports” section.

I see that there are some top ten user reports. Is there a way to pull specific reports on the usages of just one user (would list all activities of that user)?

No. We currently provide firewall bandwidth reports for only the top users within each protocol. If you would like a custom report for a single user it can be done as an ad-hoc report. An ad-hoc report charge will apply.

Is there a way within the reports to compare the last few months to see if the number of attacks is getting more or less?

Current trending of information over many months is not available.

There are different reports for the different services (Firewall and Anti-Virus). is there a single summary report that would summarize both of these services? The only single summary report is provided by the Incident Response Tickets, which roll up critical tickets for all devices.

Is there a report of the UTM device configuration status?

No. The Cavalier can provide a configuration summary upon request. You can also request a copy whenever changes are made to the UTM device.

What is the process that we need to perform to pull the reports for an audit / exam?

Pull the Monthly Executive Summaries from the Firewall Security reports. These summaries are already formatted to meet this type of requirement.

What are our responsibilities for maintaining the provided hardware?

Because Cavalier owns the provided UTM device hardware, the following apply to the equipment used to provide SecureIP services:

- There is no hardware maintenance fee.
- If the provided hardware breaks, Cavalier fixes it or replaces it by the next business day.

If we need to make a change, can we do this or would we need to submit this change to Cavalier for support?

All change requests are submitted to and processed by Cavalier. A change control procedure is followed to verify your request and appropriate policy to change.

Is there a limit for configuration changes on Firewall services?

The SecureIP Firewall Service includes 3 configuration changes per month. If for some reason, more than 3 changes are required in any one month, additional charges may apply.