TREND MICRO™

TippingPoint™

Intrusion Prevention System (IPS)

Local Security Manager User Guide

Actionable threat defense against advanced targeted attacks.

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

Publication: November 2019

System overview

The TippingPoint system is a high-speed, comprehensive security system that includes the Intrusion Prevention System (IPS), Local Security Manager (LSM), Digital Vaccine, the Security Management System Appliance, and the Core Controller.

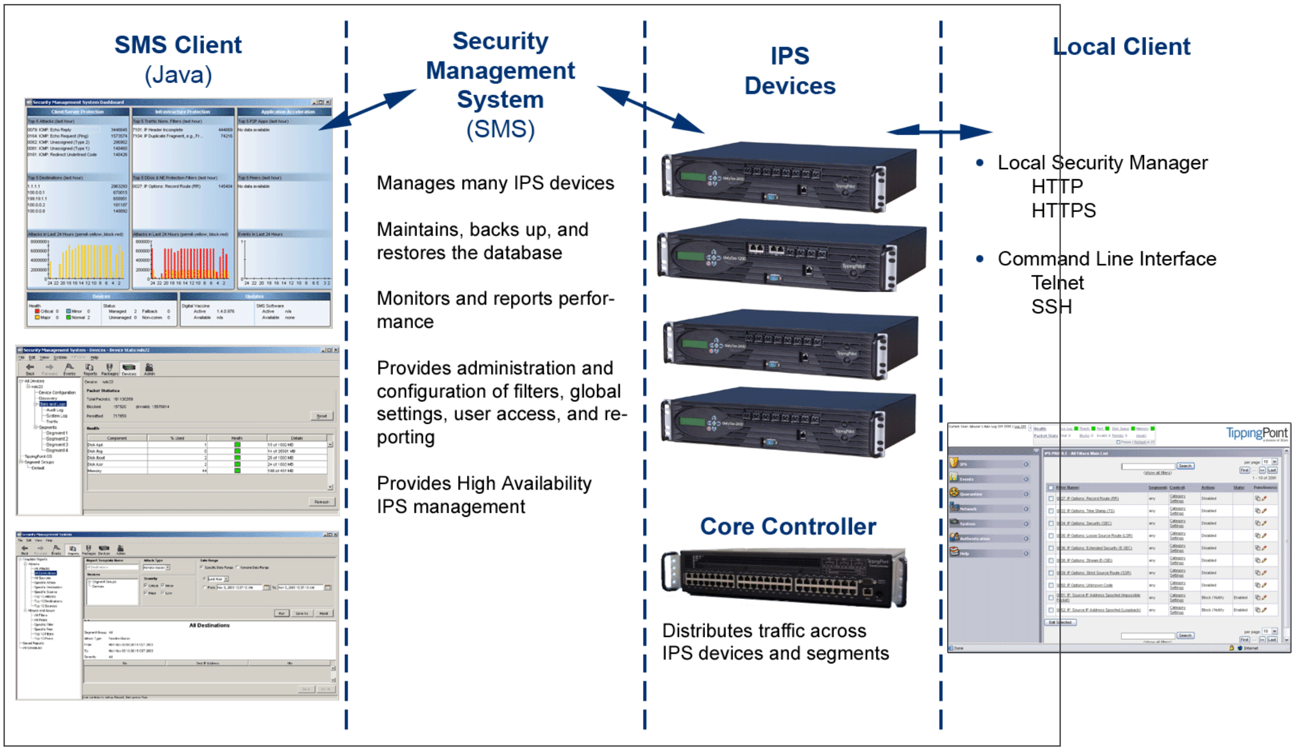
Enterprise security schemes once consisted of a conglomeration of disparate, static devices from multiple vendors. Today, TippingPoint's security system provides the advantages of a single, integrated, highly adaptive security system that includes powerful hardware and an intuitive management interface.

This topic includes the following information:

- *TippingPoint architecture*
- *Security Management System (SMS)*
- *Intrusion Prevention System devices*
- *Core Controller*
- *High availability*
- *Threat Suppression Engine*
- *Threat Management Center*

TippingPoint architecture

The TippingPoint System uses a flexible architecture that consists of a Java-based SMS Client, SMS Management Server, IPS device(s), and Local Clients including the Local Security Manager (LSM) and Command Line Interface (CLI). The system may also include the Core Controller, a hardware appliance that balances traffic loads for one or more IPSes. The following diagram provides an overview of the architecture:



SMS Client
(Java)
Security
Management
System
(SMS)
Manages many IPS devices
Maintains, backs up, and restores the database
Monitors and reports performance
Provides administration and configuration of filters, global settings, user access, and reporting
Provides High Availability IPS management
IPS
Devices
Core Controller
Distributes traffic across IPS devices and segments
Local Client
Local Security Manager
HTTP
HTTPS
Command Line Interface
Telnet
SSH
TippingPoint

FIGURE 1. TippingPoint architecture

Security Management System (SMS)

The SMS core components include:

- **SMS Secure Server** —hardware appliance for managing multiple devices
- **SMS Home Page** — web-based interface with links to current client software, documentation, and the Threat Management Center
- **SMS Management Client** — Java-based application for Windows or Linux workstations used to manage your TippingPoint system
- **Graphical User Interface (GUI)**
- **Dashboard**
- **Command Line Interface (CLI)**

The SMS communicates with managed devices that are installed in your network.

The SMS architecture also includes the following components:

- **Threat Management Center (TMC)** — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.
- **Digital Vaccine (DV)** — Update service that includes up-to-date filter packages for protecting your network.
- **Managed Devices** — TippingPoint IPS or Core Controller devices that are installed in your network.

SMS server

The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. The SMS provides the following functionality:

- **Enterprise-wide device status and behavior monitoring** — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status.
- **IPS networking and configuration** — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group.
- **Filter customization** — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings.
- **Filter and software distribution** — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.

SMS client

The TippingPoint Security Management System (SMS) client provides services and functions to monitor, manage, and configure the entire TippingPoint system. This client is a Java-based application installed and accessed on a computer running the appropriate operating system. Each user receives a specific user level with enhanced security measures to protect access and configuration of the system.

You can install and use the SMS client on computers with Microsoft Windows, Mac, or Linux operating systems.

The SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. You can create, save, and schedule reports using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. You can modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.

The SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. Included in the SMS dashboard display are the following items:

- Entries for the top five filters triggered over the past hour in various categories
- A graph of triggered filters over the past 24 hours
- The health status of devices
- Update versions for software of the system

Through the Dashboard, you gain an overview of the current performance of your system, including notifications of updates and possible issues with devices monitored by the SMS.

Intrusion Prevention System devices

Intrusion Prevention System (IPS) devices protect your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client.

Each device provides intrusion prevention for your network according to the number of network connections and hardware capabilities. IPS devices also have built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

TippingPoint Intrusion Prevention Systems are optimized to provide high resiliency, and high-availability security for remote branch offices, small-to-medium and large enterprises and collocation facilities. Each IPS can protect network segments from both external and internal attacks.

Multiple TippingPoint devices can be deployed to extend this unsurpassed protection to hundreds of enterprise zones. You can monitor and manage the devices by using the local client available on each device, or by using the SMS client to monitor and manage well over a hundred devices. The TippingPoint N-Platform and NX-Platform devices support IPv6, tunneling (including GRE and multi-layer tunnels), and inspection bypass rules for trusted traffic.

IPS local clients

The TippingPoint System provides various points of interaction, management, and configuration of the IPS. The clients include graphical user interfaces (GUI) and command line interfaces (CLI). These clients include the following:

- **Local Security Manager (LSM)** — Web-based GUI for managing one IPS device. The LSM provides HTTP and HTTPS (secure management) access. This access requires access from a supported web browser (Internet Explorer, Mozilla Firefox, and Netscape). Using the LSM, you have a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides reports to monitor the device traffic, triggered filters, and packet statistics.
- **Command Line Interface (CLI)** — Command line interface for reviewing and modifying settings on the device. The CLI is accessible through Telnet and SSH (secure access).
- **LCD Panel** — Several IPS TippingPoint devices provide an LCD panel to view, configure, and modify some device settings.

Core Controller

The TippingPoint Core Controller is a hardware-based device that enables inspection of up to 20Gbps of traffic by sending the traffic to as many as 24 IPS device segments. The Core Controller can control traffic across its three 10GbE network segment pairs and across multiple TippingPoint E-Series IPS devices. IPS devices are connected by 1GbE uplinks, and each packet that is received on a 10GbE Core Controller interface passes through a load balancer that then determines the IPS connection to use for transmitting the packet.

The Core Controller provides:

- 10GbE bidirectional traffic inspection and policy enforcement
- High Availability with an optional Smart ZPHA module
- Central management through the SMS

Note

The Core Controller can be used with the 2400E and 5000E IPS devices, and with all N-Platform and NX-Platform devices.

High availability

TippingPoint devices are designed to guarantee that your network traffic always flows at wire speeds in the event of internal device failure. The TippingPoint System provides Network High Availability settings for Intrinsic Network HA (INHA) and Transparent Network HA (TNHA). These options enact manually or automatically, according to settings you enter using the clients (LSM and SMS) or LCD panel for IPS devices. Zero-Power High Availability (ZPHA) is available for the IPS as an external modular device, as optional bypass I/O modules on NX-Platform devices, and for the Core Controller as an optional Smart ZPHA module.

The IPS uses INHA for individual device deployment and TNHA for devices deployed in redundant configurations in which one device takes over for another in the event of system failure. With INHA, a failure puts the device into Layer-2 Fallback mode and permits or blocks traffic on each segment. In TRHA, users configure their IPS devices so that when one device experiences a system failure, traffic can be routed to the other device with no interruption in intrusion prevention services.

SMS high availability provides continuous administration through an active-passive SMS system configuration. A passive SMS is configured, synchronized with the active system, and waits in standby mode and monitors the health of the active system. If the health or communications check of the active system fails, the passive SMS will be activated.

The ZPHA modular device can be attached to an IPS to route traffic in the event of power loss. Smart ZPHA modules, which are wired into the device, and bypass I/O modules, which are installed directly into NX-Platform devices, perform the same function.

Threat Suppression Engine

The Threat Suppression Engine (TSE) is a line-speed hardware engine that contains all the functions needed for Intrusion Prevention, including:

- IP defragmentation
- TCP flow reassembly
- Statistical analysis
- Traffic shaping
- Flow blocking

- Flow state tracking
- Application-layer parsing of over 170 network protocols

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination.

The combination of high-speed network processors and custom chips provides the basis for IPS technology. These highly specialized traffic classification engines enable the IPS to filter with extreme accuracy at gigabit speeds and microsecond latencies. Unlike software-based systems whose performance is affected by the number of filters installed, the highly-scalable capacity of the hardware engine allows thousands of filters to run simultaneously with no impact on performance or accuracy.

Threat Management Center

The Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.

The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on your network. The filters provide the following protections:

- **Application Protection** — Defend against known and unknown exploits that target applications and operating systems:
    - Attack Protection filters — Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include vulnerabilities and exploits filters.
    - Security Policy filters — Detect and block traffic that might or might not be malicious. This traffic might be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary to your company's security policies.
    - Reconnaissance filters — Detect and block scans, sweeps, and probes for vulnerabilities and information about your network. These filters include probes and sweeps/scans filters.
    - Informational filters — Detect and block classic Intrusion Detection System (IDS) infiltration.
- **Infrastructure Protection** — Protect network bandwidth and network infrastructure elements, such as routers and firewalls, from attack using a combination of filter types:
    - Network Equipment Protection filters — Protect networked equipment from attacks.
    - Traffic Normalization filters — Detect and block abnormal or malicious traffic.
- **Performance Protection** — Allow key applications to have a prioritized bandwidth-access setting that ensures mission-critical applications have adequate performance during times of high congestion:
    - Misuse and Abuse filters — Protect the resources and usage of file sharing across networks and personal computers. These filters protect peer-to-peer services.
    - Traffic Management filters — Protect the network by shielding against IP addresses or permitting only a set of IP addresses.

IPS concepts and the LSM

The TippingPoint Intrusion Prevention System (IPS) device protects your network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client. Each device provides intrusion prevention for your network according to the amount of network connections and hardware capabilities.

The Local Security Manager (LSM) provides a user-friendly, browser-based GUI for administering the IPS.

This topic describes IPS concepts and the login and navigation procedures of the LSM user interface.

- *IPS deployment*
- *Threat Suppression Engine*
- *IPS filtering*
- *Security notes*
- *TippingPoint N-platform and NX-platform features*
- *Logging in to the LSM*
- *The LSM screen layout*
- *System summary*

IPS deployment

A single IPS can be installed at the perimeter of your network, at the network core, on your intranet, or in all three locations. The following diagram shows an example of a corporate network with IPS devices deployed in a variety of locations.

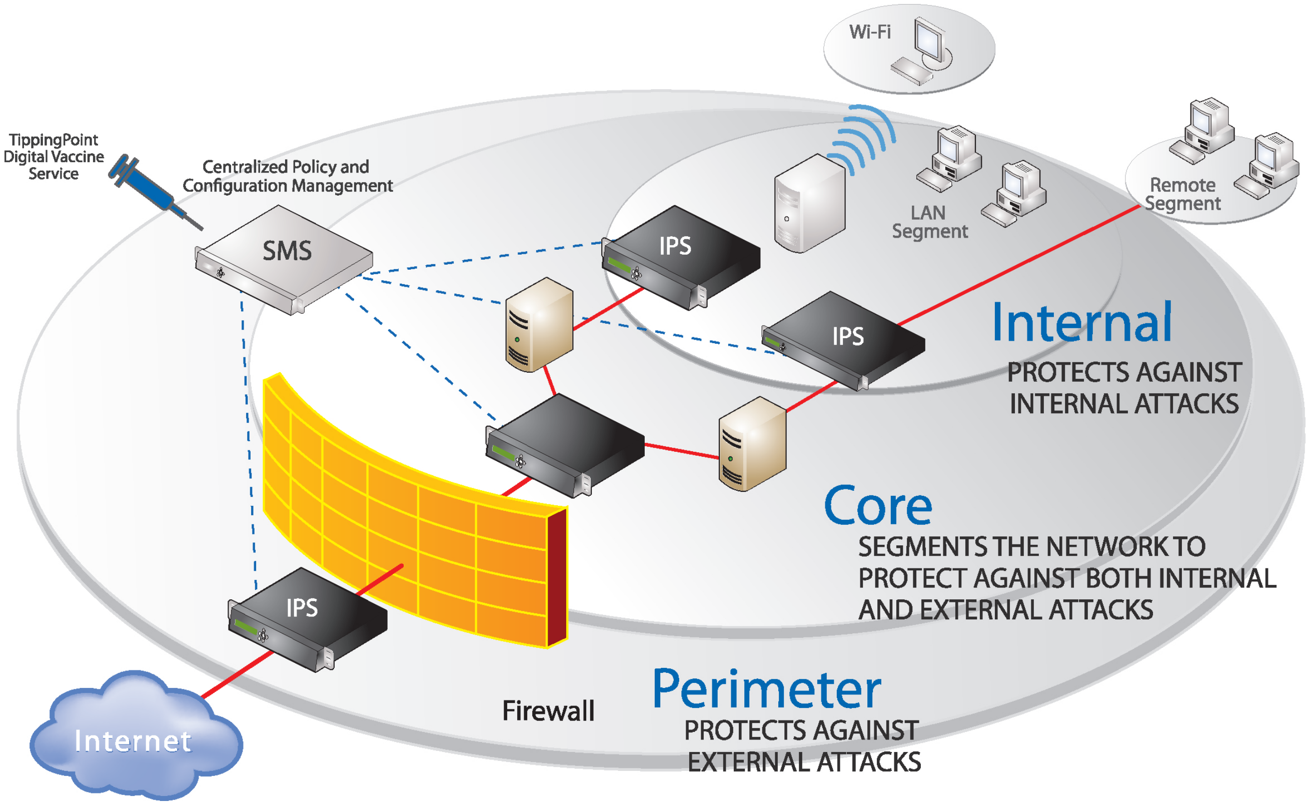

Wi-Fi
TippingPoint Digital Vaccine Service
Centralized Policy and Configuration Management
SMS
IPS
LAN Segment
Remote Segment
IPS
Internal
PROTECTS AGAINST INTERNAL ATTACKS
Core
SEGMENTS THE NETWORK TO PROTECT AGAINST BOTH INTERNAL AND EXTERNAL ATTACKS
IPS
Internet
Firewall
Perimeter
PROTECTS AGAINST EXTERNAL ATTACKS

FIGURE 2. IPS deployment example

Threat Suppression Engine

The main component of the IPS device is the Threat Suppression Engine (TSE), a custom engine that detects and blocks a broad range of attacks at wire speeds. The TSE is a flow-based network security engine, in which each packet is identified as a component of a flow and each flow is tracked in the connection table on the IPS. A flow is uniquely identified by its packet header information:

- IPv4 or IPv6 protocol (ICMP, TCP, UDP, other)
- source and destination IP addresses
- source and destination ports

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. When a packet matches an IPS filter, the IPS handles the packets based on the action set configured on the filter. For example, if the action set is **Block**, then the packet is dropped and subsequent packets from the same flow are dropped without inspection. The IPS device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes. Logging options are also available to review the types of traffic being filtered by the device. You can customize the default action sets, or create your own based on your network requirements.

IPS filtering

The TSE uses Digital Vaccine (DV) filters to police your network and to screen out malicious or unwanted traffic. In addition to the DV filters, the IPS also provides Traffic Management filters, which are custom filters that react to traffic based on source IP address, destination IP address, port, protocol, or other defined values. Traffic management filters are applied to traffic before DV filters. Depending on how the filters are configured, traffic might or might not require further inspection.

The Digital Vaccine package

DV filters are contained in a Digital Vaccine (DV) package. All IPS devices have a DV package installed and configured to provide out-of-the-box IPS protection for the network. After setting up the IPS, you can customize the filters in the DV through the LSM. To ensure that you have the most up-to-date DV package, use the Update page in the LSM to download the latest package. See *Viewing and managing current digital vaccine filters*.

The filters within the DV package are developed by TippingPoint’s Digital Vaccine Labs to protect the network from specific exploits as well as potential attack permutations to address for Zero-Day threats. These filters include traffic anomaly filters and vulnerability-based filters. Vulnerability-based filters are designed to protect the network from an attack that takes advantage of a weakness in application software. For viruses that are not based on a specific vulnerability in software, the DV provides signature filters. TippingPoint delivers weekly DV updates that can be automatically installed on the IPS device (**System > Update**). If a critical vulnerability or threat is discovered, DV updates are immediately distributed to customers. See *Enable auto update for digital vaccine*.

Tip

In addition to providing a download location for Digital Vaccine packages, the TMC also provides DV product documentation that includes more detailed information about the filters included in the DV package, filter updates, and other related information.

Additional Digital Vaccine filter subscription services are offered by DVLabs for organizations that experience heavier risk factors for threats that go beyond the scope of the standard Digital Vaccine coverage. These services include the following services:

- Reputation Feed (Rep Feed) — provides reputation filters for suspect IP addresses and domains.
- Malware Filter Package — provides advanced malware protection.

For information about registering for a Digital Vaccine subscription service, contact your TippingPoint customer representative.

Filter components

IPS filters have the following components, which determine the filter type, global and customized settings, and how the system responds when the TSE finds traffic matching the filter:

- **Category** — Defines the type of network protection provided by the filter. The category is also used to locate the filter in the LSM and to control the global filter settings using the Category Setting configuration.
- **Action set** — Defines the actions that execute when the filter is matched.
- Adaptive Filter Configuration State — Allows you to override the global Adaptive Filter configuration settings so that the filter is not affected by adaptive filtering. See also *Adaptive filtering*.
- **State** — Indicates if the filter is enabled or disabled. If the filter is disabled, the TSE does not use the filter to evaluate traffic.

Category settings

Category settings are used to configure global settings for all filters within a specified category group. DV filters are organized into groups based on the type of protection provided:

- **Application Protection Filters** defend against known exploits and exploits that can take advantage of known vulnerabilities targeting applications and operating systems. This filter type includes the subcategories `Exploits`, `Identity Theft`, `Reconnaissance`, `Security Policy`, `Spyware`, `Virus`, and `Vulnerabilities`.
- **Infrastructure Protection Filters** protect network bandwidth and network infrastructure elements, such as routers and firewalls, from attack by using protocols and detecting statistical anomalies. This filter type includes the subcategories `Network Equipment` and `Traffic Normalization`.
- **Performance Protection Filters** block or rate-limit traffic from applications that can consume excessive bandwidth, leaving network resources available for use by key applications. This filter type includes the subcategories `IM`, `P2P`, and `Streaming Media`.

Category Settings are used to assign global configuration settings to filters in a subcategory. For example, if you decide not to use any filters to monitor P2P traffic, you can change the category settings for the Performance Protection P2P filter group to disable these filters. Category settings consist of the following global parameters:

- **State** — Determines whether filters within the subcategory are enabled or disabled. If a category is disabled, all filters in the category are disabled.
- **Action Set** — Determines the action set that filters within a category execute when a filter match occurs. If the `Recommended` action set is configured, filters within the category are configured with the settings recommended by the Digital Vaccine team. If required, you can override the category setting on individual filters by editing the filter to define custom settings.

For more information, see *Edit DV filter category settings* and *Edit category settings for a filter group*.

Filter override settings

For the best system performance, TippingPoint recommends that you use global category settings and the `Recommended` action set for all DV filters. However, in some cases, you might need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network.

Filter override settings specify custom settings to be applied to the filter in the Security Profile. After a filter has been customized, it is not affected by the global Category Settings that specify the filter State and Action. For more information, see *Edit individual filter settings*.

Filter limits and exceptions

Limits and exceptions change the way filters are applied based on IP address. For example, you can specify a limit setting so that filters only apply to specific source and destination IP addresses or address ranges. If a filter has both global and filter-level exception settings, the Threat Suppression Engine uses the filter-level settings to determine how to apply the filter. You can configure the following limit and exceptions from the LSM:

- **Filter Exceptions** (specific) — Allow traffic that would normally trigger a filter to pass between specific addresses or address ranges without triggering the filter. Configured from the Filter Edit page, these exceptions apply only to the filter where they were configured.
- **Limit Filter to IP Addresses** (global) — Only apply filters to traffic between specified source and destination IP address pairs. You can configure IP address limits that apply to Application Protection, Traffic Normalization, and Network Equipment Protection filter types. You can configure separate limits that apply only to Performance Protection filters.
- **Exceptions** (global) — Exclude traffic between specified source and destination IP address pairs. You can configure exceptions for the following filter types: Application Protection, Traffic Normalization, Network Equipment Protection, and Performance Protection filters. These exceptions are global for all specified filters.

For more information, see *Configure global IP address limits and exceptions*.

Adaptive filtering

With Adaptive Filtering, the Threat Suppression Engine automatically manages filter behavior when the IPS device is under extreme load conditions. This feature protects against the potential adverse effects of a filter that interacts poorly with the network environment by preventing the device from entering High Availability mode. For more information, see *Configure adaptive filter settings*.

Adaptive filtering works by monitoring each filter to identify any suspected of causing congestion. When it identifies a filter, it manages the filter using one of the following methods, depending on how the global or filter-level Adaptive Filtering is configured:

- **Automatic Mode** — This setting enables the IPS device to automatically disable and generate a system message regarding the defective filter.
- **Manual** — This setting enables the IPS device to generate a system message regarding the defective filter. However, the filter is not disabled.

Jumbo frame support

The TippingPoint Operating System supports inspection of jumbo frames up to 9234 bytes. This includes the14-byte Ethernet header, 9216 bytes of payload data, and the 4-byte Ethernet checksum.

Note

Jumbo frame inspection is not currently supported on the TippingPoint 10.

TippingPoint N-platform and NX-platform features

The TippingPoint N-Platform and NX-Platform enable management of IPv6 traffic and tunneled traffic. These devices also permit the use of inspection bypass rules and X.509 certificates.

Best effort mode

Best Effort mode protects latency-sensitive applications by not inspecting packets if the latency introduced by inspecting them exceeds the configured threshold. Best Effort mode is enabled with the following command:

```
debug np best-effort enable [-queue-latency <microseconds>]

[-recover-percent <percent>]
```

When Best Effort mode is enabled, the default latency threshold is set at 1000 microseconds, and the default recovery percentage at 20%. The device enters Best Effort mode when latency reaches 1000 microseconds, and exits the mode when latency drops to 200 microseconds (20% of 1000).

For detailed information about Best Effort Mode, refer to the *IPS Command Line Interface Reference* .

Note

Best Effort Mode is not available on the TippingPoint 10, 110, and 330.

IPv6 inspection and management

TOS 3.6 and later supports IPv6 traffic inspection, and IPv6 options are available when configuring the Security Profile options. The majority of existing TippingPoint filters are compatible with both IPv4 and IPv6 traffic. The host management port, default gateway, and management port routes can also be configured with IPv6 addresses.

The LSM also includes a Named Networks function, accessible through the **System > Named Networks** page, which enables you to assign names to specific IPv4 and IPv6 address prefixes.

Inspection of tunneled traffic

TOS 3.6 and later enables inspection of a wide range of tunneled traffic, including:

- GRE (Generic Routing Encapsulation)
- GTP (GPRS Tunneling Protocol)
- Mobile IPv4 (IP-in-IP)
- IPv6, including 6-in-4, 4-in-6, and 6-in-6
- Tunnels up to 10 layers of tunneling or a header size of 256 bytes.

Inspection bypass rules

The TippingPoint 2500N, TippingPoint 5100N, TippingPoint 6100N, and the TippingPoint NX-platform devices enable users to configure inspection bypass rules. Traffic that matches inspection bypass rules is directed through the IPS without inspection. These rules can be applied to traffic according to source or destination IP address, port, or CIDR (Classless Inter-Domain Routing), or to traffic moving through specific ports.

Inspection bypass rules are defined with the `conf t inspection-bypass` command in the Command Line Interface (CLI). Refer to the *IPS Command Line Interface Reference* for more information.

Note

This feature is *not* supported on the TippingPoint 660N, 1400N, 10, 110, or 330.

sFlow® record emission

The NX-Platform devices and TPS devices use sFlow record emission to sample a random flow of traffic and send the data to a collector server for analysis. The analysis gives security teams a more holistic view of traffic patterns, which enables early detection and remediation of anomalous or malicious flows.

With sFlow sampling, network and security administrators establish a baseline of typical application traffic to identify unusual patterns. Users specify the following information:

- The IP address of the collection repository. Two collector IP addresses (either IPv4 or IPv6) are supported for IPS devices with TOS v3.6.0 and later installed, and for TPS devices with TOS v5.0.0 and later installed.
- The network segments that have this feature enabled. Although you can enable or disable sampling globally, you still must configure the rate on a per-segment basis.
- The sample rate. Configure this rate at the segment level. Faster links enable larger sample rates.

Tip

Segments for NX-Platform and TX Series devices are on the I/O modules. When you remove a module from a slot, the module's segment configuration and the availability state of its ports remain unchanged. For this reason, consider disabling sFlow on the module's segment port before removing the module. This prevents the device from sending extraneous port statistics counters to any configured sFlow collectors.

The data that is sampled is sent as an sFlow datagram packet to the collector server where analysis occurs. You can then generate reports, including comparison charts, that provide visibility of network congestion and potential security incidents, thereby enhancing the scalability of the network. The SMS can perform data analysis using the SMS Collector.

Note

The option for sFlow sampling is supported on NX-Platform devices and TPS devices only. *Learn more* about configuring sFlow on segments and configuring an sFlow collector.

Device support: NX-Platform devices and all TPS devices

Note

This feature is not supported on vTPS virtual appliances.

Additional event information for filter events

TOS 3.6 and later uses X-Forwarded-For and True Client technology to identify a request’s source IP address without administrators having to refer to proxy logs or web server logs. When this feature is turned on, additional fields in the event logs display the true client IP address before it is overwritten by a forwarding proxy IP address. This visibility lets security teams set a more accurate network-based user policy.

For more information, see *Capture additional event information*.

Event logs in TOS 3.7 and later can also provide HTTP context information. Additional fields in the logs display an attacker’s URI, method, and hostname information.

Note

The HTTP Context feature is *not* available on the TippingPoint 10, 110, and 330.

Logging in to the LSM

The IPS device provides simultaneous support for up to 10 web client connections, 10 telnet/SSH (for CLI) connections, and one console connection. Logging in with the CLI is discussed in the *IPS Command Line Interface Reference*.

Note

Depending on your security settings, warnings might display when accessing the client. Loading an X.509 certificate will not affect these warnings. See *X.509 certificates*.

Security notes

Because the LSM manages the IPS device through a web browser, take the following security precautions.

- Some browser features, such as password caching, are inappropriate for security use and should be turned off.
- The IPS should use the HTTPS server, not the HTTP server. HTTP servers allow usernames and passwords to travel unencrypted over networks and are not secure. You can modify the server configuration using the `conf t server` command. For details, see the *IPS Command Line Interface Reference*.

CAUTION!

Failure to follow these security guidelines can compromise the security of your IPS device.

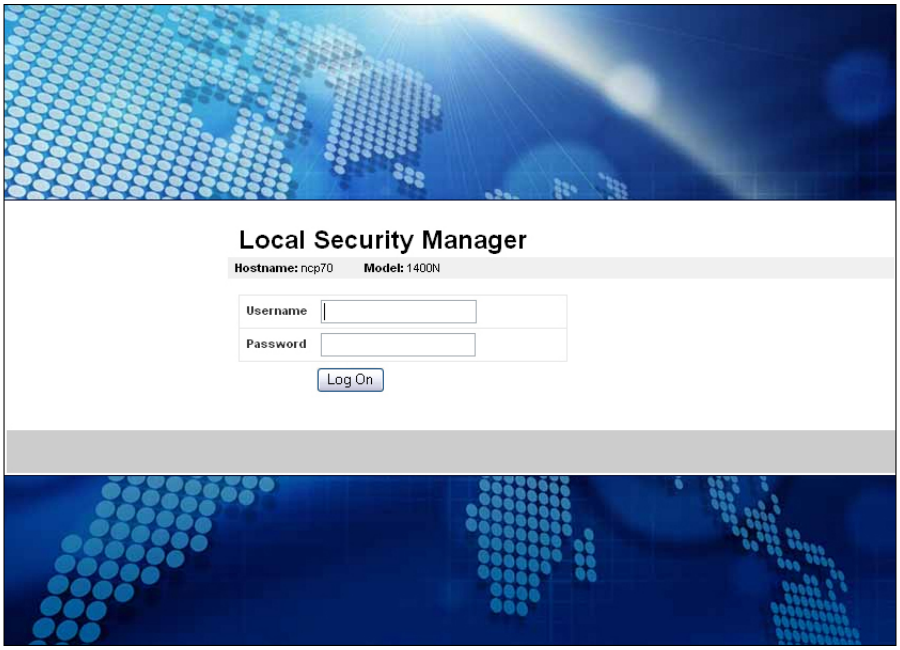
TippingPoint recommends that you use the most current version of Internet Explorer or Firefox. For the best user experience, follow these browser recommendations:

- **Internet Explorer**
  Change your cache setting in Internet Explorer for improved browser reliability with TippingPoint devices. Open the Internet Options for your browser (**Tools > Internet Options**). On the General tab, select the **Settings** option for Temporary Internet Files. In the Check for new versions section, select **Every visit to the page**. Save these settings. Cookies for previous versions of the LSM might conflict with cookies in the updated version. If the browser receives `404 Page Not Found` errors or displays blank LSM frames, the cookies on the computer might be out of sync. To remedy this, delete the existing cookies and open a new session. On the General tab of the Internet Options dialog, click **Delete Cookies**. Restart Internet Explorer, connect to the LSM, and continue as before.
- **Mozilla Firefox**
  Certificate exceptions cannot be added when managing an IPv6 device on an IPv6 network with Firefox 4 or later. To add a certificate exception in an IPv6 environment, use a different browser or the CLI.

  If your browser receives `404 Page Not Found` errors or displays blank LSM frames, the cookies on the computer might be out of sync. To resolve these issues, clear the cache, delete the cookies, and restart the browser.
- **Pop-Up Blocking**
  If your browser has pop-up blocking enabled, some elements in the LSM might not display correctly. TippingPoint recommends that you enable pop-ups for the LSM by adding the device's URL to the browser pop-up exceptions list.

1. In the web browser address bar, enter `https://` followed by the IP address or hostname of your IPS device.

2. The LSM login page is displayed in the browser. The page displays the name and model of the device.



Local Security Manager

Hostname: ncp70 Model: 1400N

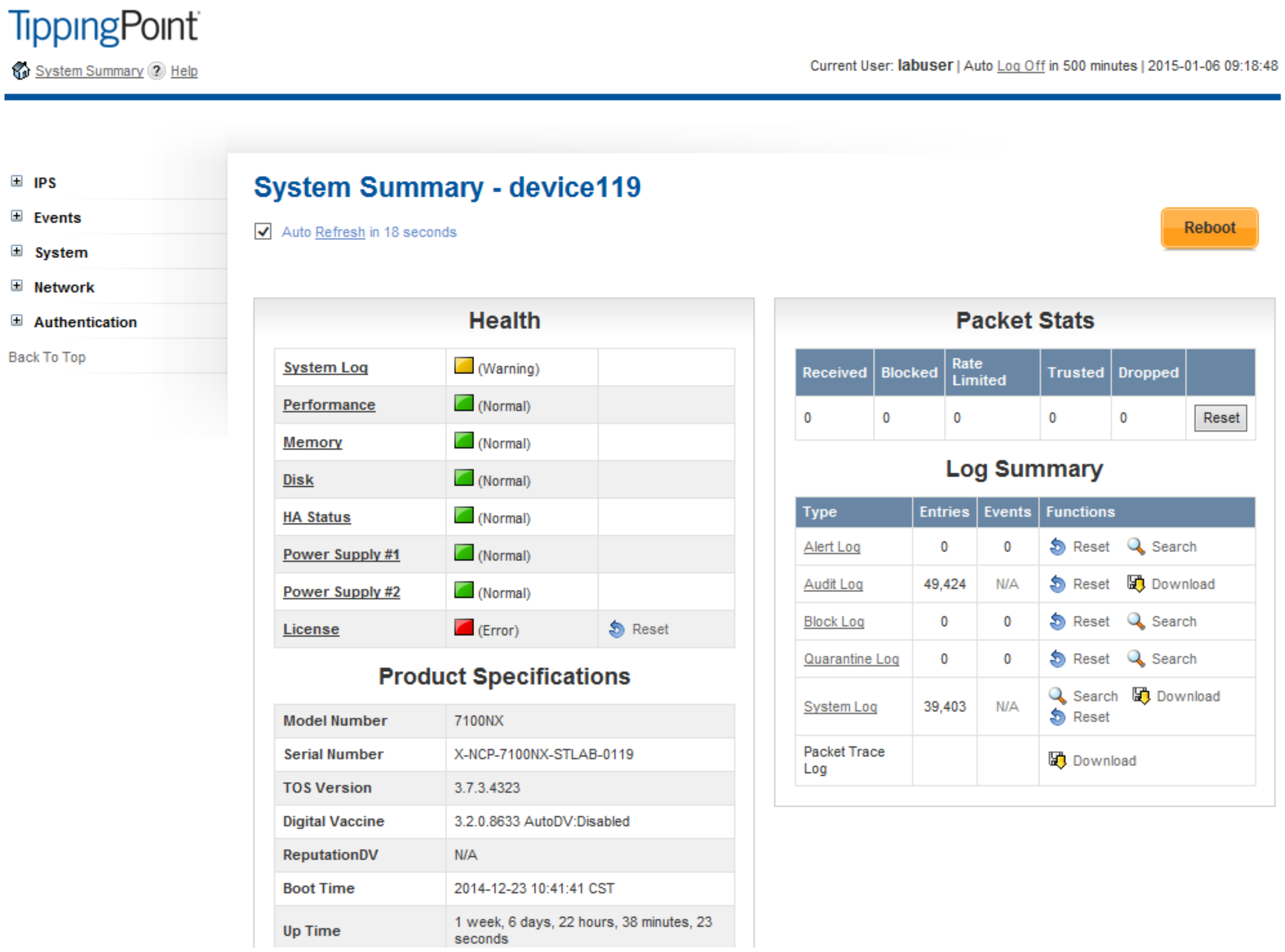
3. Enter your username and password.
4. Click **Log On**. The LSM confirms that your username is valid on the IPS. If the username is valid, the LSM software opens. If the username is not valid, the LSM login page is displayed again.

After logging in, you can access the areas of the LSM permitted by your user role. For information on user roles and access, see *Authentication*.

The LSM screen layout

The LSM screen displays information in the following areas:

- **Menu Bar** — Provides quick access to the System Summary page and the online Help. Displays current user and system status.
- **Navigation** — Provides access to the LSM menu functions.
- **Content and Functionality** — Displays the pages from which you can monitor the device operation and performance, view current configuration settings, and modify configuration. The content refreshes when you click a link in the Navigation pane or when you select buttons or links within a page. When you first log in to the LSM, the System Summary page automatically displays in this area.



Current User: **labuser** | Auto Log Off in 500 minutes | 2015-01-06 09:18:48

System Summary - device119

☑ Auto Refresh in 18 seconds

Health

System Log	🟨 (Warning)	
Performance	🟩 (Normal)	
Memory	🟩 (Normal)	
Disk	🟩 (Normal)	
HA Status	🟩 (Normal)	
Power Supply #1	🟩 (Normal)	
Power Supply #2	🟩 (Normal)	
License	🟥 (Error)	Reset

Product Specifications

Model Number	7100NX
Serial Number	X-NCP-7100NX-STLAB-0119
TOS Version	3.7.3.4323
Digital Vaccine	3.2.0.8633 AutoDV:Disabled
ReputationDV	N/A
Boot Time	2014-12-23 10:41:41 CST
Up Time	1 week, 6 days, 22 hours, 38 minutes, 23 seconds

Packet Stats

Received	Blocked	Rate Limited	Trusted	Dropped	
0	0	0	0	0	Reset

Log Summary

Type	Entries	Events	Functions
Alert Log	0	0	Reset Search
Audit Log	49,424	N/A	Reset Download
Block Log	0	0	Reset Search
Quarantine Log	0	0	Reset Search
System Log	39,403	N/A	Search Download Reset
Packet Trace Log			Download

Menu bar

The following table lists the available options in the Main Menu Bar:

OPTION	DESCRIPTION
System Summary	Displays the System Summary. See *System summary* .
Online Help	Launches the online Help.
Current User	The username of the currently logged-in user.
Current date and time	The current date and time on the IPS device. The date and time settings on the device are determined by the time synchronization method and time zone configured for the device. For details, see *Time options*.
Auto Log Off	Logs you out of the LSM. For security purposes, LSM sessions have a timeout period. The timeout period sets the length of the idle time before the LSM automatically ends the session and logs out the user. The default timeout period is 60 minutes. LSM administrators with super-user access can change the default timeout period in the Preferences page. See *Preferences*.

Navigation

The following table lists the available options in the navigation area and describes the functionality that each option enables you to access.

Option	Description
IPS	• Create and manage security profiles to monitor traffic. • Create and manage traffic management filters, action sets, and ports for IPS services. • Manage and configure settings for IPS filters, the Threat Suppression Engine (TSE), and global Adaptive Filters. See *IPS filtering*.
Events	• View, download, print, and reset Alert, Audit, Block, and System logs. • View graphs reporting on traffic flow, traffic-related events, and statistics on triggered filters (attack, rate limit, and adaptive filter). • Monitor, search, and maintain traffic streams for adaptive filtering, blocked streams, and rate-limited streams. • View health information including status of hardware components, performance, system health, and system logs. • View reports on traffic flow, traffic-related events, and triggered filters (attack, rate limit, and adaptive filter). See *Events: logs, traffic streams, reports*.
System	• Configure system controls, such as the management port, time options, SMS/NMS interaction, High Availability, disk and memory usage thresholds. • Download and install software and Digital Vaccine updates. See *System*.
Network	• View and configure high availability and link down synchronization settings for segments. • View and configure network ports including options to enable and restart ports. • View and configure virtual ports used to section the network by ports and VLAN IDs. See *Network*.
Authentication	Create, modify, and manage user accounts. See *Authentication*.

Content and functionality

The LSM displays all data in the Content and Functionality area. Links selected on these pages might display additional pages or dialog boxes depending on the feature selected.

- **Title Bar** — On each page, you can see the position of the page in the menu hierarchy provided in the title bar. For example, on the Alert Log page, the menu hierarchy indicates that the page is accessed through the **Events > Logs** sub-menu. You can navigate up the hierarchy from the current location by clicking on the link in the hierarchy listing.
- **Auto Refresh** — Some screens (such as the System Summary screen) automatically refresh themselves periodically. To disable the auto refresh function, deselect the **Auto Refresh** check box. To manually refresh, click **Refresh**. To reconfigure the Page Refresh Time, see *Preferences*.

System summary

The System Summary page is the first page that is displayed when you log in to the LSM. To access the System Summary page at any time, click the View System Summary icon in the Menu Bar.

The System Summary page includes the following:

- *Health*
- *Product specifications*
- *Reboot device*
- *Packet stats*
- *Log summary*

Health

The Health section of the Statistics frame includes color health indicators for each of the following IPS components:

- System Log
- Performance
- Memory
- Disk
- HA Status
- Power Supply Status
- License

On NX-Platform devices, each power supply is listed separately.

For detailed information about each of the health indicators, click on the corresponding link next to the color indicator. The colors indicate the current state of each component:

- **Green** — No problems
- **Yellow** — Major warning
- **Red** — Critical warning
- **Grey** — Service is disabled

Click Major and Critical warning indicators to view the error that caused the condition. When you view the error, the indicator is reset and its color changes back to green. You can set the warning thresholds on the **System > Thresholds** page. For more information, see *Set disk usage and memory thresholds*.

Product specifications

The Product Specification section displays the following information:

- **Model Number** — Model number of the IPS.
- **Serial Number** — Serial number of the IPS.
- **TOS Version** — Version number of the TippingPoint Operating System.

- **Digital Vaccine** — Version number of the Digital Vaccine.
- **ReputationDV** — ThreatDV version. Available only if you have purchased a ThreatDV license.
- **Boot Time** — Time when the IPS was last started.
- **Up Time** — Length of time that the IPS has been operating continuously.

Reboot device

To reboot the device, click **Reboot**.

Packet stats

The Packet Stats section provides basic traffic statistics:

- **Received** — Total number of packets received and scanned by the TSE.
- **Blocked** — Total number of packets that have been blocked by the TSE.
- **Rate Limited** — The number of packets that matched a filter configured to a rate-limited action set.
- **Trusted** — The number of packets that were passed as trusted.
- **Dropped** — Total number of packets dropped because they are not properly formed or formatted.

To reset the counters, click **Reset**.

Packet counters provide a snapshot of network traffic by displaying the number of packets tracked. If the number is less than 1 million KB, the Packet Stats section displays the full amount. When the number reaches the million and billion mark, the number displays as a decimal amount with a letter (such as G for gigabytes). The unit factors include, M for mega, G for giga, and T for tera. To view the full amount, hover your mouse over the displayed number.

Note

The packet totals give a partial account of blocked activity according to the filters. All other filter results affect the packet totals. The counters are not synchronized with each other. Packets can be counted more than once in some situations.

Log summary

The Log Summary section displays the number of entries and events for each type of Event Log. In addition, it enables you to download, search, or reset the following logs:

- Alert Log
- Audit Log (Super-User only)
- IPS Block Log
- Quarantine Log
- System Log
- Packet Trace Log

Review logs in detail on the Events > Logs page. For more information about logs, see *Logs*.

Technical support landing page

The Technical Support Landing page is a simplified page that offers the following options to TippingPoint 10 users only:

- **Reboot** — Reboot the device.
- **Force L2FB** — Place the device in Layer-2 Fallback mode.
- **Contact Tech Support** — Send an email to TippingPoint technical support. An email server must be configured to enable this option.
- **Log Off** — Log off from the device.

This page can be viewed in English, Spanish, Mandarin, French, and Portuguese. The Technical Support Landing page is enabled on a per-user basis for Administrators and Super Users when the user is created. When the option is enabled for a user, the user sees only this page on login, instead of the standard LSM System Summary page. For more information, see *Create a new user account*.

Note

Before using the Contact Tech Support feature, you must configure Email and SMTP server settings on the IPS device from the Email Server page. For details, see *Email server*.

IPS filtering

You can monitor and configure the settings for the IPS System from the IPS menu pages.

- **Security Profiles** — View, create, and manage the security profiles to provide Digital Vaccine (DV) filter coverage across virtual network segments.
- **Traffic Management Profiles** — View, create, and manage the traffic management profiles to monitor network traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values.
- **Action Sets** — View, manage, and create actions that define the operations a filter performs when a traffic match occurs.
- **Reputation Groups** — Manage IP reputation groups, both those made available through the TippingPoint IP Reputation service and those configured manually by the user.
- **Notification Contacts** — Configure notification contacts to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the IPS device.
- **IPS Services** — Add and manage nonstandard ports supported by the IPS device. Use this feature to configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic. When filters scan traffic against the standard ports for listed services, the engine then accesses and scans traffic against the list of additional ports.
- **Preferences** — Reset IPS filters to the factory default values; configure timeout, logging, and congestion threshold settings to manage performance of the Threat Suppression Engine; and configure the Adaptive Filter feature used to protect IPS performance from the effects of over-active filters.

This topic discusses following information:

- *Security profiles*
- *IPS Digital Vaccine Filters*

- *Traffic management profiles*
- *Reputation groups*
- *Action sets*
- *Notification contacts*
- *Services*
- *Preferences*

Security profiles

A security profile defines the traffic that the IPS monitors and the DV filters that the IPS applies. Traffic monitoring is based on incoming and outgoing port pairs. You can use the default DV filter configuration to protect the segment or customize the configuration as required. The segment specifies both the port and the traffic direction, which allows you to define separate security profiles for traffic in and out of a port.

The default security profile is set to ANY incoming ports and ANY outgoing ports, with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic on any virtual segment configured on the device is monitored according to the IPS filter configuration recommended by TippingPoint. You can edit the default security profile to customize the virtual segments that it applies to and modify the filter settings, or create your own security profiles as required.

Note

Before creating security profiles, verify that the network and system configuration on the IPS device is set up correctly for your environment. In particular, configure all required ports before creating the security profiles to protect them.

When a security profile is initially created, the recommended settings for all filter categories are enabled.

Use the Security Profiles page to perform the following tasks:

- View, create, edit, and delete security profiles
- Change category settings for a group of filters
- Override global filter settings and create filter-level settings
- Restore filter to global category settings

Note

If you use an SMS to configure your profiles or devices with any UTF-8 encoding, make sure that you have UTF-8 encoding enabled for the web browser you use to launch the LSM interface and the terminal emulator you use to launch the command line interface.

The Security Profile page includes the following information:

PARAMETER	DESCRIPTION
Profile Name	The name assigned to the security profile. The default security profile is preconfigured on the device. You can customize this profile to add virtual segment or modify global and individual filter settings.
Description	A description of the security profile, if a description has been defined.

Parameter	Description
✎	Click to edit the security profile.
✖	Click to delete the security profile.

To manage the virtual segments associated with security profiles, use the Virtual Segments page. See *Virtual segments*.

Note

If a traffic management profile has been configured with a virtual segment that is not protected by an IPS security profile, the segment will be listed in the table in red along with the following message:

```
No security profile is assigned to the in/out pair. Traffic
will NOT be inspected by the IPS.
```

To correct the error, add the segment to an existing security profile, or create a new security profile to protect it.

For more information, see:

- *Sample security profiles*
- *Applying security profiles to traffic*
- *Create a security profile*
- *Edit a security profile*
- *IPS Digital Vaccine Filters*

Sample security profiles

The following table shows a sample port configuration for an IPS device:

Name	Network Port	VLAN
ANY	ANY	ANY
1A	1	ANY
1B	2	ANY
Marketing-A	1	6
Marketing-B	2	6

The following table lists some sample security profiles you can create to monitor traffic on a device with the configuration shown in the preceding table.

Name	Segment(s) (Incoming, Outgoing)	Description
Marketing	Marketing-a ==> Marketing-b Marketing-b ==> Marketing-a	Monitor all VLAN 6 traffic on port 1 and port 2 in both directions.
LAN	1A ==> 1B 1B ==> 1A	Monitor all traffic between port 1 and port 2, except traffic tagged for VLAN 6. VLAN 6 traffic is covered by the Marketing security profile above.

NAME	SEGMENT(S) (INCOMING, OUTGOING)	DESCRIPTION
Default	ANY <==> ANY	Monitor all incoming and outgoing traffic with any port/VLAN ID except traffic on virtual segment 1A <==> 1B. This traffic is already covered by the LAN and Marketing profiles.

Default security profile

The default security profile is set to the ANY< ==> ANY virtual segment with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic in any virtual segment configured on the device is monitored according to the DV filter configuration recommended by TippingPoint.

You can edit the default security profile to customize the virtual segments that it applies to and create custom filter settings, or create your own security profiles as required. TippingPoint recommends that you keep the default security profile with the default virtual segment ANY <==> ANY. This configuration ensures that all traffic is inspected by the IPS using the default security profile, if the traffic does not match a more specific virtual segment configuration.

Applying security profiles to traffic

In the IPS, it is possible for a packet to match more than one security profile depending on how the virtual segments are configured within each profile. As a general rule, the IPS device applies the filtering rules specified in the security profile that has the most specific virtual segment defined. To determine specificity, the IPS device always considers the incoming zone first. Refer to the following examples to see how the IPS applies filtering rules when a packet matches more than one security profile.

Example 1: Packet matches two profiles

With this configuration, a packet going from virtual port 1A to virtual port 1B matches both security profile #1 and #2. The IPS device applies the filtering rules from security profile #1 to the packet because the virtual port 1A is more specific than the virtual port ANY.

SECURITY PROFILE	APPLIES TO SEGMENT
#1	1A (any VLAN) ==> 1B (any VLAN)
#2	ANY < ==> ANY

Example 2: Packet matches a profile with specified ports

With this configuration, a packet going from the virtual port 1A to 1B matches security profiles #1, #2 and #3. However, the IPS device applies filtering rules from security profile #3 to the packet because the 1A virtual port is more specific than the virtual port ANY.

SECURITY PROFILE	APPLIES TO SEGMENT(S)
#1	ANY <==> ANY
#2	ANY ==> 1B
#3	1A ==> 1B

Example 3: Packet matches a profile with a specific VLAN tag

With this configuration, a packet tagged as VLAN 6 traveling between 1A and 1B matches all the security profiles. However, the IPS device applies filtering rules from security profile #1 because the VLAN 6 tag is the most specific classification criteria.

SECURITY PROFILE	APPLIES TO SEGMENT(S)
#1	Marketing -a (1A, VLAN 6) ==>Marketing-b (Port 2, VLAN 6) Marketing -b ==> Marketing-a
#2	1A <==> 1B
#3	ANY < ==> ANY

Create a security profile

Describes how to create a security profile.

Procedure

1. Use the navigation bar to access the Security Profiles page.
2. Click **Create Security Profile**. The Create Security Profiles page is displayed.
3. Enter the **Profile Name** and, if desired, **Description**.
4. Select the **Deployment** setting, or leave the setting at default. Deployment mode can vary depending on where the device is deployed in your network. The following modes are available:
   - **Default** — Recommended for all deployment scenarios.
   - **Core** — Recommended for deployment in network core.
   - **Edge** — Recommended for deployment in Web Farm/DMZ.
   - **Perimeter** — Recommended for deployment in Internet entry point.
   - **Aggressive** — Offers a more aggressive security posture; profiles using this mode might require tuning, based upon specific application protocol usage.
5. Apply the security profile to virtual segments in the **Virtual Segments** section by selecting the virtual segment from the drop-down menu and click **Add to table** below.
6. If required, modify category settings, filter overrides, limits, and exceptions.
7. Click **Create**.

Edit a security profile

Describes how to edit a security profile.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.
2. Click the name of the profile that you want to edit. The Edit Security Profile page is displayed.

3. Select the **Deployment** setting or leave the setting at default. Deployment mode can vary depending on where the device is deployed in your network.

   The following modes are available:

   - **Default** — Recommended for all deployment scenarios.
   - **Core** — Recommended for deployment in network core.
   - **Edge** — Recommended for deployment in Web Farm/DMZ.
   - **Perimeter** — Recommended for deployment in Internet entry point.
   - **Aggressive Security** — Offers a more aggressive security posture; profiles using this mode might require tuning, based upon specific application protocol usage.

4. Apply the security profile to virtual segments in the **Virtual Segments** section by selecting the virtual segment from the drop-down menu and clicking **Add to table below**. Click delete (✖) to delete a virtual segment from the profile.
5. Review or configure additional configuration options. You can modify category settings, filter overrides, DDoS filters, reputation filters, limits, and exceptions.
6. Click **Save** to update the security profile.

   > **Note**
   >
   > Virtual segments that are associated with only one profile are deleted from the system completely when they are removed from that profile.

IPS Digital Vaccine Filters

IPS Digital Vaccine (DV) Filters monitor traffic passing between network segments. Based on the security profiles configured on the device, the IPS applies the filters to traffic on each segment included in the profile. Each security profile has its own filter settings. Within a security profile, you can accept the recommended settings for a filter category, or, if necessary, customize individual filters based on your network environment and security needs. For detailed information about the concepts behind DV filters, see *IPS filtering*.

Categories and category settings are used to configure global settings for all filters within a specified category group. Filter settings are used to override the global settings for individual filters within a category group.

Configure filters separately for each security profile configured on the IPS device. When a profile is initially created, all filters are set to the default Category Settings. You can change the category settings for filters or edit individual filters from the Edit Security Profile page in the LSM.

Because of the large number of DV filters available on the device, the LSM provides a search interface on the Security Profiles page to view and edit filters. For instructions on using this interface and on editing filters, see the following topics:

- *View DV filters*
- *Edit DV filter category settings*
- *Edit category settings for a filter group*
- *Edit individual filter settings*
- *Capture additional event information*
- *Configure global IP address limits and exceptions*

- *Reset an individual filter*

View DV filters

Describes how to view and manage the filters configured on a security profile.

You can view and manage the filters configured on a security profile with the **Filters** and **Filter Search** menu pages. Both pages can be accessed from the Filter Overrides section of the Edit Security Profile pages.

Procedure

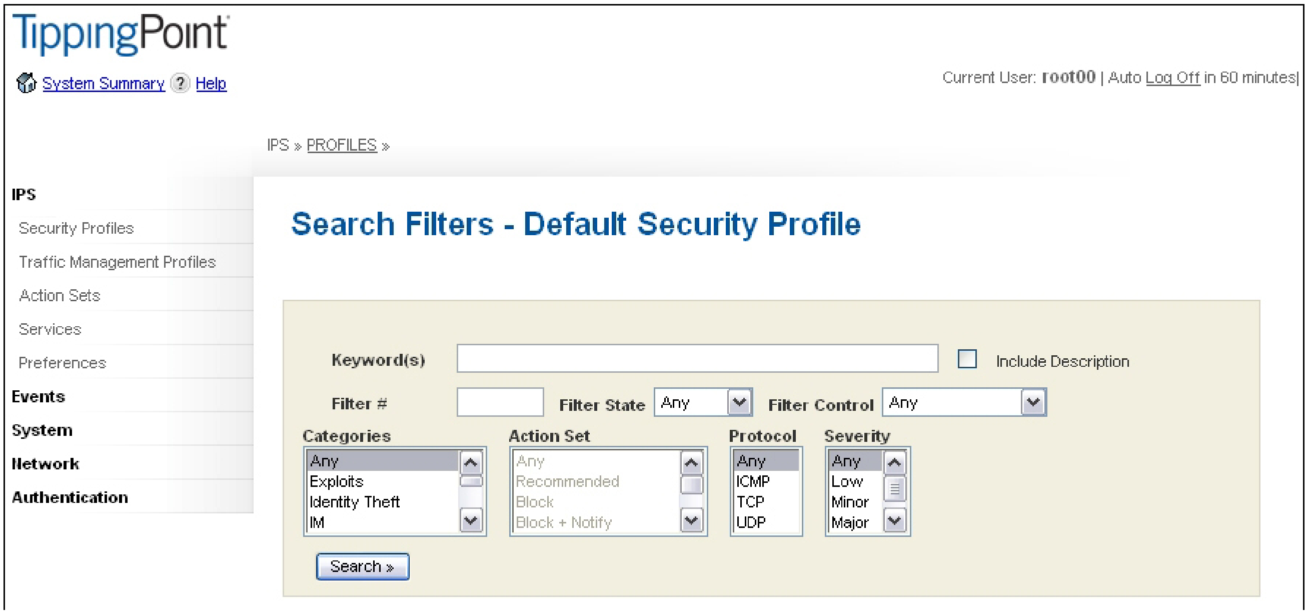
1. On the LSM menu, click **IPS > Security Profiles**.
2. Click the name of the profile that you want to edit.

   The Edit Security Profile page is displayed.
3. Under **Filter Overrides**:
   - To access the Filters page, use the **View all filters** link. See *Filters list*.
   - To access the Filter Search page, click **Search All Filters**. See *Filter search*.

   You can complete the following tasks from these pages:
   - View current filters
   - Sort the filter list
   - Locate a filter or group of filters
   - Add a filter to the filter override list for a security profile
   - Remove a filter from selected security profiles
   - View the filter description page, which includes information about the filter, recommended settings, and the current filter state

Filter search

The Filter Search page enables you to view all filters or only those matching user-specified search criteria. Access the Filter Search page by clicking **Search All Filters** while editing a security profile. To sort filter search results, click the appropriate column heading in the **Filters List** table.



TippingPoint

System Summary Help

Current User: root00 | Auto Log Off in 60 minutes|

IPS » PROFILES »

IPS
- Security Profiles
- Traffic Management Profiles
- Action Sets
- Services
- Preferences

Events

System

Network

Authentication

Search Filters - Default Security Profile

Keyword(s) ________ □ Include Description

Filter # ____ Filter State: Any Filter Control: Any

Categories: Any, Exploits, Identity Theft, IM

Action Set: Any, Recommended, Block, Block + Notify

Protocol: Any, ICMP, TCP, UDP

Severity: Any, Low, Minor, Major

You can search for filters according to the following parameters:

Parameter	Description
Keywords	Words or phrases in the filter names. You can search for a specific filter name or for a specific substring in the filter name. A Keyword search is a string search, not a Boolean search, and is not case-sensitive. If you enter a phrase, the results will contain the exact phrase. For example, if you enter “ICMP reply” the search will *not* return a filter whose description is “ICMP: Echo Reply”
Include Description	Option that expands the search to find the specified keyword(s) in the filter descriptions as well as in the filter names.
Filter #	The unique filter ID number.
Filter State	Current operating states. You can select one of the following states: Any, Disabled, or Enabled.
Filter Control	The filter configuration. You can select one of the following states: Any, Category Settings (defaults), or Override (customized).
Categories	IPS filter category groups. You can choose from all groups in the Application Protection, Infrastructure Protection, and Performance Protection categories.
Action Set	Action sets assigned to filters. You can choose from all the default and custom Action Sets configured on the device.
Protocol	Transport protocols that filters can apply to.
Severity	Severity Levels assigned to filters.

For details on performing a filter search see the following topics:

- *View filters with recommended (default) settings*

- *View filter overrides and custom settings*

Filters list

The Filters List page lists all filters that are configured on a security profile. Access this page by selecting **View all filters** on the Security Profile page. Because of the large number of filters, it might take some time for the system to display the page.

The Filters List page includes a search form, which includes the same features as the Filter Search page. For more information about the search form, see *Filter search*.

The Filters List table includes the following features:

PARAMETER	DESCRIPTION
Check Box	Selects the filters that you want to add to the security profile. If a filter entry has no check box, that filter has already been added to the security profile.
Filter Name	The unique identifying number and name of the filter. The name includes the protocol to which the filter applies and other descriptive information about the purpose of the filter (`0079: ICMP:Echo Reply`). These names are assigned by the TippingPoint Digital Vaccine team. Click the name of the filter to view filter information.
Control	Indicates whether the filter configuration uses the default category settings or user-customized settings. To view and manage customized filters, select the filter from the Filters table on the Security Profile page.
Action	The action set currently assigned to the filter. If an enabled filter uses a defined **Deployment** mode (**Default**, **Core**, **Edge**, **Perimeter**, or **Aggressive Security**; see *Edit a security profile*), the Action is inherited from the **Deployment** mode. If the filter has an override, the action selected in the override is displayed.
State	Indicates whether the filter is enabled (in use) or disabled.
Function(s) ➕	Indicates whether the filter can be added to the security profile.

For details on viewing filters on the Filter List page, see the following topics:

- *View filters with recommended (default) settings*
- *View filter overrides and custom settings*

Adding a filter to a security profile

Describes how to add a filter to a security profile.

There are multiple methods for adding a filter to a security profile:

- Select one or more filters from a filter search. See *View filters with recommended (default) settings*.
- Select one or more filters from the Filters List. See *View filters with recommended (default) settings*.
- Use the Security Profile section on the View Filter page. See *Edit individual filter settings*.

View filters with recommended (default) settings

Describes how to view filters that have the default settings.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. In the **Filter Overrides** section:
    - Select **View all filters** to view the Filters page. Because of the large number of filters, this action might take some time to execute. You can sort the filters by filter name, control type, action, or state by clicking the appropriate column heading in the **Filters List** table.
    - Select **Search All Filters** to view the Search Filters page. Enter one or more search parameters and click **Search**.

    In the Filters list generated by **View all filters** or by filter searches, you can perform the following tasks:

    - Select a filter that you want to customize by clicking on the filter name. See *Edit individual filter settings*.
    - Add a single filter to the current security profile by clicking the green plus-sign icon.
    - Add multiple filters to the current security profile by selecting the check boxes next to the filter names and clicking **Add Selected Filters**.

View filter overrides and custom settings

Describes how to view filter overrides and custom settings.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. In the **Edit Security Profile** page, scroll down to the **Filter Overrides** section.
4. In the Filter Overrides section, you can perform the following tasks:
    - View and edit a filter by clicking on the **Filter Name**.
    - Remove the filter override and return the filter to its default settings by clicking the **Delete** icon.

Edit DV filter category settings

By default, a security profile uses the default category settings for all filters available in the Digital Vaccine package. In some cases, you might not need a particular filter or category of filters. For example, if you do not have a particular type of web server installed on your network, you might want to disable filters that protect that type of web server against attack. From the LSM, you can modify the filter configuration for a security profile by category or by changing individual filter settings. You can make the following types of changes:

- Edit a Filter Category Group to enable/disable all filters in the group or change the assigned action for all filters in the group.
- Edit an individual filter or group of filters to modify the State, Action, Adaptive Filter Configuration State, or Exceptions settings.

When you edit a filter, the changes only affect the security profile in which you make the edits. This allows you to have different filter configurations for different network segments.

For details on editing filters, see the following topics:

- *Edit category settings for a filter group*
- *Edit individual filter settings*

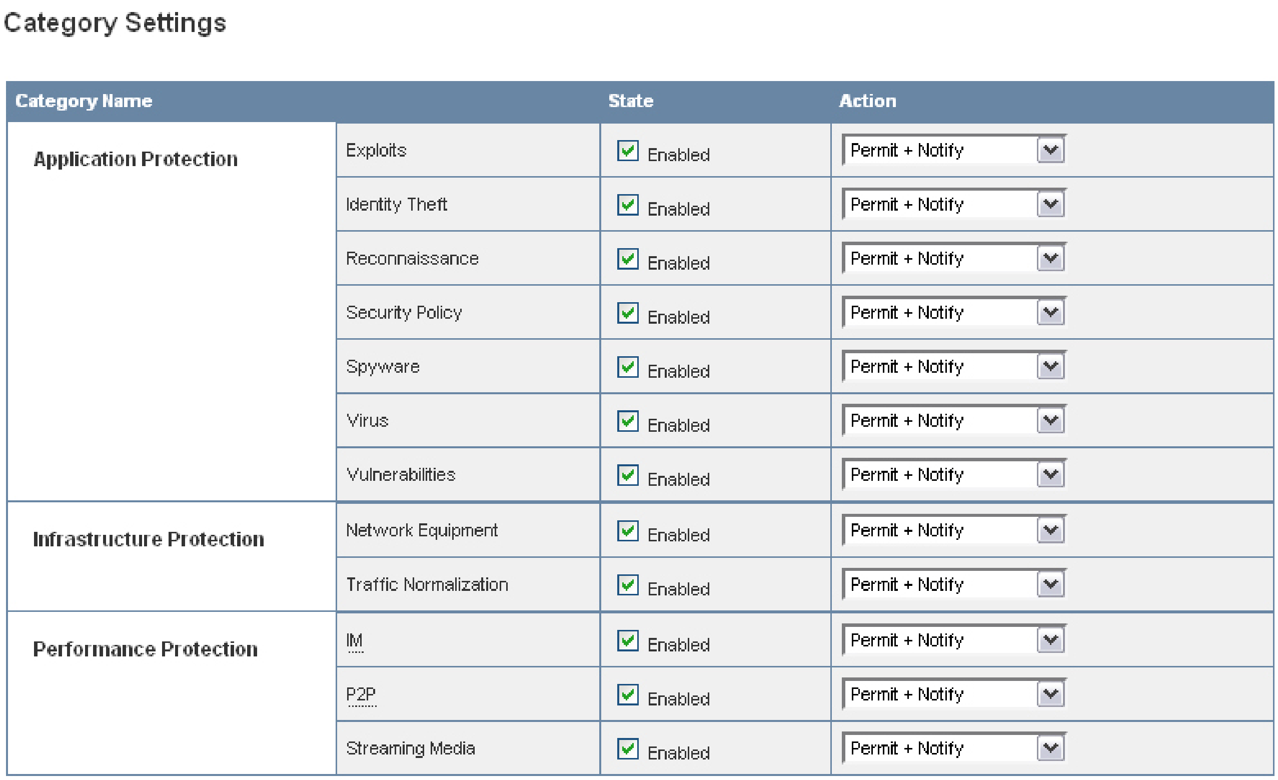
Note

If the category setting is enabled and you disable the filter, the filter might still display as enabled.

Edit category settings for a filter group

Describes how to edit category settings for a filter group.

For the best system performance, TippingPoint recommends that you use global Category Settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network. For more information about editing individual filters, see *Edit individual filter settings*.



Category Settings

Category Name		State	Action
Application Protection	Exploits	☑ Enabled	Permit + Notify
	Identity Theft	☑ Enabled	Permit + Notify
	Reconnaissance	☑ Enabled	Permit + Notify
	Security Policy	☑ Enabled	Permit + Notify
	Spyware	☑ Enabled	Permit + Notify
	Virus	☑ Enabled	Permit + Notify
	Vulnerabilities	☑ Enabled	Permit + Notify
Infrastructure Protection	Network Equipment	☑ Enabled	Permit + Notify
	Traffic Normalization	☑ Enabled	Permit + Notify
Performance Protection	IM	☑ Enabled	Permit + Notify
	P2P	☑ Enabled	Permit + Notify
	Streaming Media	☑ Enabled	Permit + Notify

When you change the Category Settings for a group of filters, the settings will not affect any filters that have been customized (overridden). Filters that have been customized appear on the Edit Security Profiles page in the Filter Overrides section. On the Filters List page, these filters are listed with Control = Filter.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.

2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. On the Edit Security Profile page, locate the category in the **Category Settings** table.
4. Modify the settings as required:
    - **State** — Enables or disables all filters in the group.
    - **Action** — Selects the Action Set that will be used for *all* filters in the group. The Recommended Action Set is the system default for all category groups. If this action is selected, each filter in the group is configured with the settings recommended by TippingPoint. Filters within the group can have different settings for State and Action.
    - Click **Save** (at the bottom of the **Security Profile** page).

Edit individual filter settings

Describes how to edit individual filter settings.

For the best system performance, TippingPoint recommends that you use global category settings and the recommended action set for all DV filters. However, in some cases, your network requirements might require you to override the category settings and recommended action for individual filters. After a filter has been customized, it is not affected by the global category settings that specify the filter State and Action. For more information about editing category settings, see *Edit category settings for a filter group*.

Procedure

1. Search for the filter that you want to modify. See *View filters with recommended (default) settings*.
2. On the View Filter page, add the filter to the appropriate security profile by selecting it in the **Security Profiles** table.
3. After making changes, click **Save**. From the Filter List page you can add other filters to the profile.
4. On the LSM menu, click **IPS > Security Profiles**.
5. Click the pencil (Edit) icon for the profile containing the filter you want to edit.
6. On the Edit Security Profile page, scroll down to the Filter Overrides section, select the filter you want to edit, and click **Edit Selected Filters**.

    The Edit Filter page is displayed.
7. Modify the filter settings as required.
    - To use a different action set for the filter, select the **Override** option in the **Action/State** section and select the action set that you want to use. To enable or disable the filter, select or deselect the **Enabled** checkbox.
    - Select the Adaptive Filter Configuration state appropriate to your network.
    - Define IP address exceptions for the filter. Enter source or destination IP addresses and click **Add to table below** to create IP address exceptions.
    - Click **Save**.

> **Note**
>
> If the action for the filter is set to **Recommended** and you do not change it, the filter might remain disabled even when you select the **Enabled**check box. This happens when the recommended setting for the filter state is **Disabled**. To enable a filter with this setting, change the action from **Recommended** to another option.

Note

Entering an IPv4-mapped address in IPv6 notation will only match addresses that actually appear in IPv6 packets on the wire. They will not match IPv4 packets. Similarly, a range entered in IPv4 notation will only match IPv4 packets, and not IPv6 packets that contain the equivalent IPv4-mapped addresses. To match both notations, use both. In fields where `any` is allowed, you can enter `any4` to match IPv4 packets, `any6` to match IPv6 packets, and `any` to match both IPv4 and IPv6 packets.

Note

When using wildcards to create an IPv6 address exception, use a wildcard character to represent each field. For example, input using the following format is valid: `a:b:c:d:e:f:*:*` The following format would be rejected as invalid: `a:b:c:d:e:*`

Create or edit a DDoS filter

Describes how to create or edit DDoS filters.

When a DDoS filter is enabled, the filter always proxies the SYN packet. It does not allow the packets to continue to the destination, and does not drop the packets.

Note

DDoS filters will not take effect if asymmetric mode is enabled on the device. See *Configure the Threat Suppression Engine (TSE)*.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.

   After making changes, click **Save**. The Security Profiles page lists the selected filters in the **Filters** table.
3. On the Edit Security Profile page, click **Edit DDoS Filters For This Profile**.

   The DDoS Filters List page is displayed.
4. To create a DDoS filter, click **Create DDoS Filter**. To edit an existing filter, click on the filter's name from the list.
5. In the **Filter Parameters** section, do the following:

   a. Enter the **Filter Name**.

   b. Select the **Action** that determines how the device will manage traffic that triggers the filter: **Block + Notify** or **Block**.

   c. Enter a **Destination IP** address or a CIDR to specify a set of IP addresses to which the filter applies.
6. If you have enabled SYN proxy DDoS protection, specify the threshold SYN flood for this IP address or CIDR. When the threshold is reached, a notification is sent to the block log.
7. Click **Create** or **Save** to return to the DDoS Filters List page.
8. On the DDoS Filters List page, click **Edit Profile** to return to the Security Profile page.

Edit reputation filter settings

Describes how to edit reputation filter settings.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. On the Edit Security Profile page, click **Edit Reputation Filters For This Profile**.

   The Reputation Filters List page is displayed.

4. Modify the following settings as needed:

   - Under **Apply Reputation Filters**, select whether you want the filter to apply to traffic source IP addresses, destination IP addresses, or both. Source and Destination IP Addresses can be entered in CIDR format, as `any`, or as `*`.

     Note

     Reputation filter hits in the logs appear to report traffic protocol as `ip` instead of `ip6`. These hits are actually showing the matched signature's *`protocolType`* instead of the traffic *`protocolType`*. Traffic protocols can be confirmed by checking the source and destination addresses.

   - Select whether you want packets to be permitted or dropped when reputation lookup is pending.
   - Under **Reputation Filter Exception Settings**, enter IP addresses or DNS domains to which reputation filters are not applied. The addresses can be source, destination, or both.

5. Click **Apply** to save the settings and return to the Security Profile page.

   Note

   For more information about reputation groups and ThreatDV, see *Reputation groups*.

Create or edit a reputation filter

Describes how to create or edit reputation filters.

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. On the Edit Security Profile page, click **Edit Reputation Filters For This Profile**.

   The Reputation Filters List page is displayed.

4. Click **Create Reputation Filter**.

   The **Create Reputation Filter** page is displayed.

5. Select the Reputation Group.
6. Enable the filter by selecting the **Enabled** check box. Disable the filter by deselecting it.
7. Select the action set that you want to apply to the filter.

Important

When using quarantine actions sets with reputation filters, remember that the quarantine also applies to any hosts communicating with the reputation entries.

For example, if host1 is included in a reputation with an action set of quarantine and host2 attempts to communicate with host1, host2 will also be quarantined and all communications will be blocked. As a best practice, add quarantine exceptions for hosts that you never want to quarantine, such as the Default Gateway and DNS Server. For more information on creating exceptions, see *Configure an action set*.

8. Enter a traffic threshold.

9. Click **Apply** to save the filter and return to the Reputation Filters List page.

Capture additional event information

Describes how to identify the true IP address of an attacker and the HTTP URI and hostname information associated with an event.

Some attackers use strategic methods to hide their source information. For example, the IP address of the attacker displayed in the Source Address field of the Alert Log or Block Log can belong to a forwarding proxy server. To identify the true IP address of the attacker:

Procedure

1. On the LSM menu, click **IPS > Security Profiles**.

2. On the Security Profiles page, click on the name of the security profile that you want to edit.

3. On the Edit Security Profile page, click the **Client IP (X-Forwarded-For & True-Client-IP)** checkbox in the Capture Additional Event Information section.

What to do next

To collect HTTP URI and hostname information associated with an event:

1. On the LSM menu, click **IPS > Security Profiles**.

2. On the Security Profiles page, click on the name of the security profile that you want to edit.

3. On the Edit Security Profile page, click the **HTTP Context (Hostname, URI, Method)** checkbox in the Capture Additional Event Information section.

Note

The HTTP Context feature is not available on the TippingPoint 10, 110, and 330.

The event logs display details of the attacker in the Additional Information field. A Client IP Address field shows the IPv4 or IPv6 address of subsequent attackers. This information can be collected for a profile.

X-Forwarded-For & True-Client-IP information can also be collected for a remote syslog or an SNMP trap. For more information, see *Syslog servers*.

The data collected with this feature is used for logging purposes only. To block the IP address for the profile, you must configure an action set for that packet. For more information, see *Configure an action set*.

Configure global IP address limits and exceptions

Describes how to configure limits and exceptions of global IP addresses.

Procedure

1. From the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. In the **Limits/Exceptions** section, add IP addresses to Application Protection Filter Exclusives, Application Protection Filter Exceptions, and Performance Protection Filter Exclusives:
   a. Enter the **Source Address.** Source and Destination IP Addresses can be entered in CIDR format, as `any`, or as `*`.
   b. Enter the **Destination Address**.
   c. Click **Add to table below**.
   d. Repeat this process for each IP address exception required.
4. Click **Apply**.

Note

Entering an IPv4-mapped address in IPv6 notation will only match addresses that actually appear in IPv6 packets on the wire. They will not match IPv4 packets. Similarly, a range entered in IPv4 notation will only match IPv4 packets, and not IPv6 packets that contain the equivalent IPv4-mapped addresses. To match both notations, use both.

Note

In fields where `any` is allowed, you can enter `any4` to match IPv4 packets, `any6` to match IPv6 packets, and `any` to match both IPv4 and IPv6 packets.

Note

When using wildcards to create an IPv6 address exception, use a wildcard character to represent each field. For example, input using the format `a:b:c:d:e:f:*:*` is valid and the format `a:b:c:d:e:*` would be rejected as invalid.

Delete a global limit/exception setting

Describes how to delete global limit/exception settings.

Procedure

1. From the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. In the **Limits/Exceptions** section, review the global limit and exception address entries. Click the delete icon (✖) to delete an entry.
4. Click **Apply**.

What to do next

To delete a filter-level exception, edit the filter. For details, see *Edit individual filter settings*.

Reset an individual filter

Describes how to delete global limit/exception settings.

If you have created a filter override in a security profile, you can restore the filter to its default settings by deleting the filter from the Security Profile Filters table.

Procedure

1. From the LSM menu, click **IPS > Security Profiles**.
2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. In the **Filter Overrides** table, find the entry for the filter override you want to remove and click delete (✖). The filter is restored to the recommended settings for the category it belongs to.

What to do next

You can also reset all filters to their factory default settings from the IPS Preferences page. For details, see *Reset security policy*.

⚠ **CAUTION!**

If you use the IPS Preferences page to reset the filters to their default settings, all filters will be set to their recommended state and all user-customized action sets, rate limits, and thresholds will be deleted. You will also lose the security profiles and custom security profile settings that you have created.

Traffic management profiles

Use the Traffic Management Profiles page (**IPS > Traffic Management Profiles**) to view, create, edit, or delete a traffic management profile and apply traffic management profiles to virtual segments. A traffic management profile consists of the following components:

- **Profile Details** — Profile name and description.
- **Virtual Segments** — Specifies the incoming and outgoing virtual ports to which the Traffic Profile applies.
- **Filters** — One or more filters to manage the traffic based on Protocol or IP address and port. Each filter defines the type of traffic to be monitored and the action to be taken when the filter is triggered.

Traffic that triggers the traffic management filter is managed based on the filter action configured, which can be any of the following:

- **Block** — Traffic that triggers the filter is denied.
- **Allow** — Allows traffic that meets the filter criteria.
- **Rate Limit** — Rate limits traffic that meets the filter criteria.
- **Trust** — Allows traffic that meets the filter criteria through the IPS device without being inspected.

Traffic that is allowed or rate-limited based on a traffic management filter goes on to be inspected based on the security profile configuration (DV filtering). In other words, traffic is not allowed through the device based solely on the traffic management filter criteria, unless the filter is configured with the Trust action.

Note

Quarantine actions take priority over traffic management trust filters.

The Traffic Management Profiles page lists all the traffic management profiles currently configured on the device and includes the following information:

Parameter	Description
Profile Name	The name assigned to the traffic management profile.
Description	A description of the traffic management profile, if a description has been defined.
✎	Click to edit the traffic management profile.
✖	Click to delete the traffic management profile.

To manage the virtual segments associated with security profiles, use the Virtual Segments page. See *Virtual segments*.

Note

The segment that you select must be configured on an IPS security profile. Otherwise, traffic on the segment is not inspected by the IPS Digital Vaccine filters. If a traffic management filter has been configured with a segment that is not protected by an IPS security profile, the segment will be listed in the Security Profile Virtual Segments table in red along with the following message.

```
No security profile is assigned to the in/out pair. Traffic
will NOT be inspected by the IPS.
```

To correct the error, add the segment to an existing security profile, or create a new security profile to protect it.

This topic discusses the following information:

- *Applying traffic management profiles to traffic*
- *Create a traffic management profile*
- *Edit a traffic management profile*
- *Traffic management filter parameters*
- *Configure a traffic management filter*

Applying traffic management profiles to traffic

You can use traffic management filters to prioritize traffic or implement security policy. For example, you might define the following IP filters for your Web servers in a lab that denies access to external users:

- Block traffic if the source is on an external subnet that arrives through port 80 and is destined for the IP address of your Web server.
- Block traffic if the source is your Web server, the source port is 80, and the destination is any external subnet.

You can define multiple traffic management rules in each profile. In general, when defining filters for network segments, more specific filters should come first. For example, a more specific IP filter might block traffic with fully qualified source and destination IP addresses and ports. More general ones, like those that apply to subnets, should follow.

The following table lists several examples of traffic management filters:

Source address	Destination address	Protocol	Source port	Destination port	Action
any	any	UDP	any	53	Allow
any	any	UDP	any	any	Block
any	any	ICMP	any	any	20 Mbps rate-limit
any	1.2.3.4	TCP	any	80	Allow
any	any	TCP	any	80	Block
66.94.234.13	any	IP	any	80	Block

These filters perform the following actions:

- Block all UDP traffic except DNS requests. DNS requests are inspected for attacks.
- Limit all ICMP traffic to 20 Mbps.
- Block all HTTP traffic except for server 1.2.3.4.
- Block IP fragments coming from IP address 66.94.234.13 on any port going to port 80.

Create a traffic management profile

Describes how to create a traffic management profile.

If you have created a filter override in a security profile, you can restore the filter to its default settings by deleting the filter from the Security Profile Filters table.

Procedure

1. From the LSM menu, click **IPS > Traffic Management Profiles**.
2. Click **Create Traffic Mgmt Profile**.
3. On the Create Traffic Management Profiles page, enter the **Profile Name**. You can also enter a description of the profile.
4. Apply the security profile to virtual segments in the **Virtual Segments** section by selecting the virtual segment from the drop-down menu and click **Add to table below**.
5. Repeat this process until you have added all the required virtual segments.
6. Click **Create**.

What to do next

After creating the Traffic Management profile, you need to edit it to add traffic management filters. See *Edit a traffic management profile*.

Note

The virtual segment that you specify must also be assigned to a security profile. For details, see the virtual segments field description in the traffic management filters table in *Traffic management profiles*.

Edit a traffic management profile

Describes how to edit a traffic management profile.

If you have created a filter override in a security profile, you can restore the filter to its default settings by deleting the filter from the Security Profile Filters table.

Procedure

1. From the LSM menu, click **IPS > Traffic Management Profiles**.
2. On the Traffic Management Profiles page, click on the name of the traffic management profile that you want to edit.
3. Apply the security profile to virtual segments in the **Virtual Segments** section by selecting the virtual segment from the drop-down menu and click **Add to table below**. Click delete (✖) to delete a virtual segment from the profile.
4. Review additional configuration options. Perform the following tasks as needed:
   - To add a traffic management filter, click **Add Traffic Management filter**. For details on creating a traffic management filter, see *Configure a traffic management filter*.
   - To change the precedence of traffic management filters, drag and drop the filter to the appropriate position in the filter list.
   - To edit an existing traffic management filter, click either the filter name or edit (✎) in the Functions column.
   - To delete an existing filter, click delete (✖).
5. After you have completed the changes, click **Save** to update the traffic management profile.

Note

Virtual segments that are associated with only one profile are deleted from the system completely when they are removed from that profile.

Traffic management filter parameters

Describes the configuration parameters for traffic management filters.

PARAMETER	DESCRIPTION
Filter Parameters	The name assigned to the traffic management filter.
Action	Indicates how the IPS device will manage traffic that triggers the filter. The following options are available: • **Block** — Traffic that triggers the filter is denied. • **Allow** — Allows traffic that meets the filter criteria. • **Rate Limit** — Rate limits traffic that meets the filter criteria. • **Trust** — For trusted servers or traffic, allows traffic that meets the filter criteria to pass through the IPS device without being inspected.
Protocol	Specifies which protocol the filter checks for: **IP**, **ICMP**, **TCP**, or **UDP**. • To apply the filter only to IP fragments, select **Apply only to IP fragments**. • To change the protocol to IPv6 and IPv6 equivalents, select IPv6. Selecting ICMP and IPv6 changes the protocol to ICMPv6.

PARAMETER	DESCRIPTION
Source	Specifies the source IP address and port for traffic that will be managed by the filter.
Destination	Specifies the destination IP address and port for traffic that will be managed by the filter.
ICMP	If the filter applies to ICMP traffic and you want to monitor a specific type of ICMP message, this parameter specifies the ICMP message **Type** and **Code**.

Configure a traffic management filter

Describes how to configure a traffic management filter.

Traffic management filters are configured in the context of a traffic management profile that determines which network segments are monitored by the filter. For details on creating a profile, see *Create a traffic management profile*.

Procedure

1. From the LSM menu, click **IPS > Traffic Management Profiles**.
2. On the Traffic Management Profiles page, click on the name of the traffic management profile that you want to edit.
3. In the **Profile Details (Advanced)** section in the **Filters** table, click **Add Traffic Management filter**. To edit an existing filter, click the filter name.
4. Enter or edit the filter Name.
5. Select the parameters for the filter:
   - Use the **State** field to enable or disable the filter. When you create a new filter, it is enabled by default.
   - Select either **Block**, **Allow**, **Rate Limit** and a rate limit action set, or **Trust** for the **Action**. Trusted traffic will not be inspected by the IPS.
   - Select the **Protocol** this filter checks for from the drop-down list: **IP**, **ICMP**, **TCP**, or **UDP**.
   - To change the protocol to IPv6 and its equivalents, select IPv6. If this option is selected, only IPv6 addresses are allowed. If unselected, only IPv4 addresses are allowed.
   - For the **Source** and **Destination**, type the **IP Address** and **Port** (if applicable) that identifies the traffic to be monitored. IP addresses can be specified in CIDR format, as `any` or as `*`. Click **IPv6 Info** for more information about using IPv6 addresses.
   - If the protocol type is ICMP and you only want to monitor specific ICMP traffic, enter the ICMP Type and Code (0-255).
6. Click **Create** or **Save** to return to the Edit Traffic Management Profile page.
7. Click the **Save** button to update the profile with the new filter information.

Note

Entering an IPv4-mapped address in IPv6 notation will only match addresses that actually appear in IPv6 packets on the wire. They will not match IPv4 packets. Similarly, a range entered in IPv4 notation will only match IPv4 packets, and not IPv6 packets that contain the equivalent IPv4-mapped addresses. To match both notations, use both. In fields where `any` is allowed, you can enter `any4` to match IPv4 packets, `any6` to match IPv6 packets, and `any` to match IPv4 or IPv6 packets depending on whether IPv6 is selected.

Note

When using wildcards to create an IPv6 address exception, use a wildcard character to represent each field. For example, input using the following format is valid: `a:b:c:d:e:f:*:`* The following format would be rejected as invalid: `a:b:c:d:e:*`

Reputation groups

As a part of security profiles, users can create groups of IP addresses and DNS names, known as reputation groups. Reputation filters enable you to apply block, permit, or notify actions across an entire reputation group.

When an IP address or DNS name is added to a reputation group, it is added to the device's reputation database. Incoming traffic is checked against the database, and the appropriate reputation filters are then applied. While the address or name is being looked up, you can choose to have packets from a suspect address dropped or permitted. See *Create or edit a reputation filter* for more information.

Note

Reputation filter hits in the logs appear to report traffic protocol as `ip` instead of `ip6`. These hits are actually showing the matched signature's *`protocolType`* instead of the traffic *`protocolType`*. Traffic protocols can be confirmed by checking the source and destination addresses.

The TippingPoint SMS offers additional reputation features; refer to the *Tipping Point Security Management System User Guide* for more information.

Use the Reputation Groups page to perform the following tasks:

- View existing reputation groups
- Manually create reputation groups
- Access security profile pages to create and edit reputation group filters

The Reputation Group feature enables you to create groups of IPv4, IPv6, and DNS addresses and define an action set to apply to all of those addresses.

The Reputation Groups page lists the following information:

PAGE SECTION	PARAMETER	DESCRIPTION
Reputation Groups List	Name	The name assigned to the reputation group.
	Description	A description of the reputation group, if a description has been defined.
	Entries	Addresses entered in the reputation group.
	Function(s) ✎ ✖	 Click to edit the reputation group. Click to delete the reputation group.

Page Section	Parameter	Description
Security Profiles	Profile Name	The name assigned to the security profile that has reputation filters configured on it.
	Description	A description of the security profile, if a description has been defined.
	✏	Click to edit the reputation filters defined on the profile.

This topic discusses the following information:

- *TippingPoint ThreatDV*
- *Create a reputation group*
- *Create a reputation filter*
- *Edit a reputation filter*

TippingPoint ThreatDV

The TippingPoint ThreatDV is a licensed service that identifies and delivers suspect IPv4 and IPv6 and DNS addresses to subscribers. The addresses are tagged with reputation, geographic, and other identifiers for ready and easy security policy creation and management. The service provides the addresses and tags multiple times a day in the same fashion as Digital Vaccines.

Note

While any user can manually create reputation groups and filters, the ThreatDV is available only to users who have licensed the service from TippingPoint. For more information about this service, ask your TippingPoint representative.

Create a reputation group

Describes how to create a reputation group.

Procedure

1. Click **Create Reputation Group** to access the Create Reputation Groups page.
2. Enter a name for the reputation group.
3. Enter a brief description of the group.
4. Enter an IPv4, IPv6, or DNS address in the **Address** field.
5. Click **Add to table below** to add the address to the group.
6. Repeat steps 4–5 until you have added all of the addresses that you want to add to the group.
7. Click **Create**.

Create a reputation filter

Describes how to create a reputation filter.

Procedure

1. On the Reputation Groups page, click the **pencil** icon next to the name of the security profile to which you want to add a reputation filter.

   The Reputation Filters List page is displayed.

2. Click **Create Reputation Filter**.

   The Create Reputation Filter page is displayed.

3. In the **Filter Parameters** section, do the following:

   - Enter the **Filter Name**.
   - Select the **Action** that determines how the device manages traffic that triggers the filter: **Block + Notify** or **Block**.
   - Enter a **Destination IP** address or a CIDR to which the filter applies.

4. Click **Save** to return to the Reputation Filters List page.

Edit a reputation filter

Describes how to edit a reputation filter.

Procedure

1. On the Reputation Groups page, click the **pencil** icon next to the name of the security profile to which you want to add a reputation filter.

   The Reputation Filters List page is displayed.

2. Click the **pencil** icon next to the name of the Reputation Filter that you want to edit.

   The Create Reputation Filter page is displayed.

3. In the **Filter Parameters** section, do the following:

   a. Enter the **Filter Name**.

   b. Select the **Action** that determines how the device manages traffic that triggers the filter: **Block + Notify** or **Block**.

   c. Enter a **Destination IP** address or a CIDR to specify a set of IP addresses to which the filter applies.

4. When editing a reputation filter, you can also add exceptions.

5. Click **Save** to return to the Reputation Filters List page.

Delete a reputation filter

Describes how to delete a reputation filter.

Procedure

1. On the Reputation Groups page, click the **pencil** icon next to the name of the security profile to which you want to add a reputation filter.

   The Reputation Filters List page is displayed.

2. Click the **Delete** icon next to the name of the reputation group that you want to delete.
3. Confirm that you want to delete the filter.

Action sets

Action sets determine what the IPS device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:

- **Actions** determine where a packet is sent after it is inspected:
  - *A permit* action allows a packet to reach its intended destination.
  - A *block* action discards a packet. A block action can also be configured to *quarantine* the host and/or perform a *TCP reset*.
  - A *rate limit* action enables you to define the maximum bandwidth available for the traffic stream.
  - A trust action allows the designated traffic to bypass all inspection; the traffic is transmitted immediately. Trust has lower latency than Permit, and using it can reduce load on the CPU and processors.
- **Packet Trace** allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.
  - **Priority** sets the relative importance of the information captured. Low priority items are discarded before medium priority items if there is a resource shortage.
  - **Verbosity** determines how much of a suspicious packet will be logged for analysis. If you choose *full* verbosity, the whole packet is recorded. If you choose *partial* verbosity, you can choose how many bytes of the packet (from 64 to 1600 bytes) the packet trace log records.
- **Notification Contacts** indicate the contacts to notify about the event**. These contacts can be systems, individuals, or groups.**

Note

You must create or modify a notification contact before configuring an action set that uses the contact. For details, see *Notification contacts*.

You can also configure a Block action to perform a TCP Reset. This option resets the TCP connection for the source or destination IP when the Block action executes.

Note

Globally enabling the TCP Reset option can negatively impact your system performance. TippingPoint recommends using this option for issues related to mail clients and servers on email-related filters.

Use the Action Sets page to perform the following tasks:

- View and manage existing actions
- Create and Edit action sets

By default, Block and Permit action sets are configured on the IPS. You can also create Rate Limit action sets and Quarantine actions.

The Action Sets page lists the following actions:

Action name	Description
Recommended	The default action set as determined by the filter's category settings. When this action set is assigned to a filter, the filter uses the recommended action setting for the default category settings. The Recommended action set can enable different configurations for filters within the same category. Under a Recommended category setting, some filters are disabled while others are enabled; some might have permit actions assigned while others are set to block.
Block (+TCP Reset)	Blocks a packet from being transferred to the network. TCP Reset is an option for resetting blocked TCP flows.
Block + Notify (+TCP Reset)	• Blocks a packet from being transferred. • Notifies all selected contacts of the blocked packet. TCP Reset is an option for resetting blocked TCP flows.
Block + Notify + Trace (+TCP Reset)	• Blocks a packet from being transferred. • Notifies all selected contacts of the blocked packet. • Logs all information about the packet according to the packet trace settings. TCP Reset is an option for resetting blocked TCP flows.
Permit + Notify	Permits a packet and notifies all selected contacts of the packet.
Permit + Notify + Trace	• Permits a packet. • Notifies all selected contacts of the packet, and logs all information about the packet according to the packet trace settings.
Trust	• Not configured on the device by default; you must create a Trust action set for this action to appear on the table. • Allows trusted traffic to pass without inspection. • Lower latency than Permit. • Cannot be used with DDoS or IP Reputation filters.

The **Action Sets** page provides the following information for each action configured on the device:

Column	Description
Action Set	The name of the action set.
Action(s)	The actions included in the action set.
TCP Reset	Indicates whether the option to reset a TCP connection is enabled. With *TCP reset* enabled, the system resets the TCP connection for the source or destination IP when the Block action executes. This option can be configured on Block action sets.
Packet Trace	Indicates whether packet tracing is enabled.
Contact(s)	Where notifications are sent if a Notification Contact is configured on the action set.
Function(s) ✏ ✖	Click on these icons to edit or delete an action set. You cannot delete a default action set or an action set that is currently assigned to a filter, and you cannot edit the *Recommended* action set.

This topic discusses the following information:

- *Rate limit action sets*
- *Quarantine actions*

- *Configure an action set*

Rate limit action sets

A Rate Limit action set defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps action set, then both “Echo Requests” and “Redirect Undefined Codes” filters share the 10 Mbps “pipe” as opposed to each filter getting a dedicated 10 Mbps pipe.

The supported rates are subject to restrictions based on the device model. Any of these listed rates can be used as long as it does not exceed 25% percent of the total bandwidth of the product.

Quarantine actions

Quarantine allows the system to block or permit packets based on the IP addresses in the packet that triggers the filter. When a filter with a quarantine option is triggered, the system installs a block for the quarantined IP address and quarantines the IP address based on the instructions in the action set. If the quarantine action is combined with a Block action, the flow is blocked. The quarantine action can also be combined with a Permit action, in which case the flow is permitted while the IP address is placed in quarantine. For a list of quarantine options, see *Configure an action set*.

When using quarantine actions sets with reputation filters, remember that the quarantine also applies to any hosts communicating with the reputation entries. For example, if host1 is included in a reputation with an action set of quarantine and host2 attempts to communicate with host1, host2 will also be quarantined and all communications will be blocked. As a best practice, add quarantine exceptions for hosts that you never want to quarantine, such as the Default Gateway and DNS Server. For more information on creating exceptions, see *Configure an action set*.

Quarantine actions can also occur at a user-defined threshold. You can configure permit and trust actions to take effect before the threshold is triggered.

For example, you can display a Quarantine web page to notify a quarantined user of the problem and provide instructions for fixing it, or the action can redirect all traffic from the quarantined IP address to a quarantine server that provides instructions to correct the problem.

Note

Quarantine actions take priority over traffic management trust filters.

Configure an action set

Describes how to configure an action set.

Procedure

1. On the LSM menu, click **IPS > Action Sets**.
2. On the Action Sets page, click **Create Action Set**. To edit an existing action set, click the action set name.
3. Enter or edit the action set name.
4. Select the parameters for the action set:
   - **Permit** — Allows traffic. Can be used in conjunction with quarantine.
   - **Rate Limit** — Limits the speed of traffic. You must select a **Rate**.

- **Block** — Blocks traffic from entering the network. Can be used in conjunction with quarantine.
- **TCP Reset** — Used with the **Block** action, resets the source, destination, or both IPs of an attack. This option resets blocked TCP flows.
- **Trust** — Allows traffic to pass without inspection.
- **Packet Trace** — Enables or disables packet tracing. Specify **Priority** and **Verbosity**; if you choose partial verbosity, enter the number of bytes to capture (between 64–1600).

5. Select the contact that will be notified when the action occurs. If there are no contacts displayed, you must create an Email or SNMP Notification Contact first. See *Create an email or SNMP notification contact*.
6. You can select the quarantine options for the action set:
   - **No** — The action set does not include a Quarantine action.
   - **Immediate** — When the action set is triggered, the quarantine goes into immediate effect.
   - **Quarantine After** — When the desired threshold is reached, the quarantine goes into effect.
7. If **Immediate** or **Quarantine After** was selected in the preceding step, you can further configure the following Quarantine options:
   - **HTTP Traffic** — HTTP requests from the quarantined host can be blocked, redirected to a web server, or redirected to a custom page that displays information about the filter that triggered the quarantine action.
   - **Non-HTTP Traffic** — Non-HTTP requests can be blocked or permitted.
   - **Limit quarantine to the following IP address(es)** — Enables the quarantine to be restricted to a limited set of hosts.
   - **Do not quarantine the following IP address(es)** — Enables an exceptions list of hosts that will not be quarantined.
   - **Allow quarantined hosts to access the following IP address(es)** — Enables quarantined hosts to access selected IP addresses.
8. Click **Create** or **Save**.

Notification contacts

Configure notification contacts to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the IPS device. The traffic-related event can be the result of triggering an IPS filter configured with an action set that specifies a notification contact. A notification contact can be any of the following:

- **Remote System Log** — Sends messages to a syslog server on your network. This is a default contact available in all IPS action sets. Before using this contact, configure the IP address and port for the syslog server (**System > Syslog Servers**).
- **Management Console** — Sends messages to the LSM or the SMS device management application. This default contact is available in all action sets. If this contact is selected, messages are sent to the Alert or IPS Block Log in the LSM, depending on whether a permit or block action has executed. When the device is under SMS management, messages are also sent to the SMS client application. This notification contact does not require any configuration, although you can change the default name and aggregation period.
- **Email or SNMP** — Sends messages to the email address or specified SNMP. All email or SNMP contacts must be added from the Notification Contacts page. If the default email server is not configured on the device, you are prompted to configure it before adding a contact.

Note

Before creating an Email or notification contact, you must configure Email and SMTP server settings on the IPS device from the Email Server page. For details, see *Email server*.

After configuring notification contacts, you can select them for IPS filter events when you create or edit the action set assigned to the filter.

Use the Notification Contacts page to perform the following tasks:

- View existing notification contacts
- Add new contacts

The Notification Contacts page lists the following information:

PARAMETER	DESCRIPTION
Contact Name	The name assigned to the contact.
Type	The type of contact. The type can be MGMT, SYSLOG, or Email.
Period	The aggregation period, in minutes, for the contact.
Other Parameters	Other information about the contact. For example, the Remote System Log contact shows the number of remote syslog servers configured for the device.
Function(s) ✎ ✖	Click on these icons to edit or delete a contact. Note: The Management Console and Remote System Log cannot be deleted from this list.

This topic discusses the following information:

- *Alert aggregation and the aggregation period*
- *Configure the management console contact*
- *Configure the remote system log contact*
- *Create an email or SNMP notification contact*
- *Delete a notification contact*

Alert aggregation and the aggregation period

The IPS uses alert aggregation to prevent system performance problems resulting from an excessive number of notification requests. Because a single packet can trigger an alert, attacks with large numbers of packets could potentially flood the alert mechanism used to send out notifications. Alert aggregation allows you to receive alert notifications at intervals to prevent this flooding. For example, if the aggregation interval is 5 minutes, the system sends an alert at the first IPS filter trigger, collects subsequent alerts and sends them out every five minutes.

On the IPS, alert aggregation is controlled by the *aggregation period* that you configure when you create a notification contact. This setting is required for all notification contacts.

CAUTION!

Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the higher the system load. In the event of a flood attack, a short aggregation period can lead to system performance problems.

In addition to the user-configured aggregation period, the system also provides alert aggregation services to protect the system from over-active filters that can lower performance.

For email contacts, the aggregation period works in conjunction with the *email threshold* setting configured for the email server. See *Email server*.

Configure the management console contact

Describes how to configure the management console contact.

Procedure

1. On the LSM menu, click **IPS > Notification Contacts**.
2. On the Notification Contacts page, click **Management Console**.
3. Edit the **Contact Name**. By default, it is `Management Console`.
4. Enter the **Aggregation Period** for notification messages in minutes.
5. Click **Save**.

Configure the remote system log contact

Describes how to configure the remote system log contact.

Designating a remote system log as the notification contact sends messages to a syslog server on your network. This is a default contact available in all IPS action sets. Before using this contact, configure the IP address and port for the syslog server (**System > Syslog Servers**).

CAUTION!

Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol with no additional security protections. Use remote syslog only on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

Procedure

1. On the LSM menu, click **IPS > Notification Contacts**.
2. On the Notification Contacts page, click **Remote System Log**.
3. Enter the remote system log's host IP address and port number.
4. Select an **Alert Facility** and a **Block Facility**: none or select from a range of 0 to 31.

   The syslog server uses these numbers to identify the message source.
5. Select a **Delimiter** for the generated logs: **tab**, **comma**, **semicolon**, or **bar**.
6. Enter a **Remote system log aggregation period** in minutes.
7. Click **Add to table below** to add the remote syslog server.
8. Repeat steps 3–7 to add additional remote system log servers.
9. Click **Save** to save the changes.

Note

Verify that your IPS can reach the remote system log server on your network. If the remote system log server is on a different subnet than the IPS management port, you might need to configure the routing. For details, see *Management routing*.

Create an email or SNMP notification contact

Describes how to create a contact for email or SNMP notification.

Procedure

1. On the LSM menu, click **IPS > Notification Contacts**.
2. Click **Add Contact**.
3. On the Create Contact page, select **Email** or **SNMP**.
4. Enter the contact name.
5. Enter the **Aggregation Period**. Longer aggregation periods improve system performance.
6. If the contact is an email contact, enter the address where notifications are to be sent in the **To Email Address** field. If the contact is an SNMP contact, enter the host IP address and port number.
7. Click **Create** to save the changes.

Note

SNMP notification contacts require SNMPv2, and do not work when SNMPv2 is disabled. See *Configuring SMS information* and *Viewing or configuring NMS information*.

Note

Before creating an Email or notification contact, you must configure Email and SMTP server settings on the IPS device from the Email Server page. For details, see *Email server*.

If the email is not sent correctly, ensure that:

- the default email server is configured. See *Email server*.
- the email server is reachable from the IPS.
- the email allows mail relaying and that you use the account/domain that the email server accepts.

Delete a notification contact

Describes how to delete a notification contact.

You cannot delete the default Remote System Log and Management Console contacts or a Notification Contact if it is currently configured on another action set.

Procedure

1. On the LSM menu, click **IPS > Notification Contacts**.

2. On the Notification Contacts page, click the delete (✖) button.

3. On the confirmation dialog, click **OK**.

Visibility

Describes how to enable the sFlow® feature.

Use the IPS Visibility page to enable sFlow sampling on a random flow of network traffic. Sampling can be configured on a global (all IPS segments) or segment-by-segment basis. When sFlow is enabled, network and security administrators can establish a baseline of typical application traffic to identify unusual patterns. Data is collected and sent as an sFlow packet to a collection repository where it is analyzed.

To enable the sFlow feature globally across all segments:

Procedure

1. From the LSM menu, click **IPS > Visibility**.

2. Select **Enabled**.

3. Type the IP address for the collector server.

   Two collector IP addresses (IPv4 or IPv6) are supported for TOS V. 3.6 and later. Beginning with SMS version 4.2.0, the SMS can perform the data analysis with its SMS Collector feature.

4. Specify the network port as required. The default port is `6343`.

5. Click **Add to table below**.

6. Click **Apply**.

   Tip

   Be sure that the device can reach the remote system log server on your network. If the server is on a different subnet than the IPS management port, you might need to configure the routing to that subnet (see *Management routing*).

   This feature is supported on TippingPoint NX-Platform devices only.

What to do next

To enable the sFlow feature on a segment-by-segment basis:

1. From the LSM menu, click **Network > Segments**.

2. Click the segment on which you want to enable sFlow.

3. On the Edit IPS Segment page, specify the sample rate (1 out of *x* packets, default is 1000).

Services

Use the IPS Services page to configure additional ports associated with specific applications, services, and protocols to expand the range of traffic scanned by the IPS device. During the inspection process, the IPS device first scans traffic against the standard ports for listed services, and then scans traffic against the list of additional ports. You can configure up to 16 additional ports for each service other than HTTP. For HTTP, only eight additional ports are allowed.

Note

Although the LSM allows you to configure more than eight HTTP ports, the inspection reliability diminishes substantially when more than eight ports are configured.

The IPS Services page provides the following information:

PARAMETER	DEFINITION
Application	Type of application or network service.
Protocol	The protocol for the application.
User-Defined Ports	The list of the custom ports defined on the IPS.
System-Defined Ports	The list of supported ports per application.

This topic discusses the following information:

- *Add a port*
- *Delete a Port*

Add a port

Describes how to add a port.

Procedure

1. From the LSM menu, click **IPS > Services**.
2. On the IPS Services page, click **Add Port Configuration**.
3. On the Create Port Configuration page in the Application Type/Port Assignment section, select the **Application Type** and enter a **Port Number**.
4. Click **Create** and click **OK** on the confirmation pop-up.

CAUTION!

TippingPoint does not recommend configuration of user-defined, non-standard ports. Enabling non-standard ports can have a detrimental effect on the performance of the device.

Delete a Port

Describes how to delete a port.

You can only delete custom ports configurations. You cannot delete any of the default port configurations configured on the IPS device. You can delete only one port at a time.

Procedure

1. From the LSM menu, click **IPS > Services**.
2. On the IPS Services page, click **Delete Port**.
3. On the Delete Port Configuration page, select the **Application Type** for the port configuration to delete.

The selection list only includes applications that have been configured with a custom port.

4. Select the **Port Number** that you want to delete.

5. Click **Delete** to delete the port and return to the IPS Services page.

Preferences

Use the IPS Preferences page (**IPS > Preferences**) to configure settings related to the Threat Suppression Engine and filtering performance.

This topic discusses the following information:

- *Reset security policy*
- *Configure the Threat Suppression Engine (TSE)*
- *Traffic management filter parameters*
- *Configure adaptive filter settings*

Reset security policy

Describes how to restore IPS filters and associated settings to the factory default settings.

To restore IPS filters and associated settings to the factory default settings, use the Reset Security Policy option on the Preferences page.

CAUTION!

The Reset Security Policy action restores all filters to their recommended category settings. You will lose any filter customizations made in the security profiles. You will also lose any user-created action sets, rate limits, and traffic thresholds, and other user-configured options. You cannot undo this action.

Procedure

1. From the LSM menu, click **IPS > Preferences**.

2. On the IPS Preferences page, click **Reset** in the Reset Security Policy section.

3. Click **OK** on the confirmation pop-up.

Configure the Threat Suppression Engine (TSE)

Describes how to configure the Configure Threat Suppression Engine (TSE).

On the IPS Preferences page, you can configure global settings for the TSE in the Configure Threat Suppression Engine section.

Procedure

1. From the LSM menu, click **IPS > Preferences**.

2. On the IPS Preferences page in the **Configure Threat Suppression Engine (TSE) table**, change the configuration parameters as required.

3. To configure **Congestion Percentage** and **Disable Time** for the disable logging feature, select **Disabled if congested in** the **Logging Mode** field.

4. Select any other options you want to configure.

5. Click **Apply**.

Note

Enabling or disabling IDS mode requires a system reboot. IDS mode becomes disabled if you manually enable performance protection or set Adaptive Filtering mode to Automatic.

Traffic management filter parameters

Describes the TSE configuration parameters.

Parameter	Description
Connection Table Timeout (TCP)	Specifies the global timeout interval for TCP traffic on the connection table. For blocked streams in the connection table, this value determines the time interval that elapses before the blocked connection is cleared from the connection table. Before the timeout occurs, any incoming packets for that stream are blocked at the IPS device. After the connection is cleared (the timeout interval expires), the incoming connection is allowed until traffic matches another blocking filter. Blocked streams can also be cleared from the connection table manually from the Blocked Streams page (**Events > Managed Streams > Blocked Streams**).
Connection Table Timeout (non-TCP)	Specifies the global timeout interval for non-TCP traffic on the connection table.
Trust Table Timeout	Specifies the global timeout interval for the trust table. This value determines the time interval that elapses before the trusted connection is cleared from the trust table.
Quarantine Timeout	Specifies the global timeout for the quarantine table. For quarantined hosts in the quarantine table, this value determines the time interval that elapses before the quarantined host is cleared from the quarantine table. After the quarantined host is cleared (the timeout interval expires), quarantined addresses can be automatically released, if that option is selected.

Parameter	Description
Asymmetric Network	Specifies whether the IPS device is configured for an asymmetric network. When asymmetric configuration is enabled, the IPS device does not see both sides of a TCP connection. This option is enabled by default. **Note** You must disable Asymmetric Network mode in order to run DDoS filters and the following filter numbers (all disabled by default): • 13360: SMB: Sourcefire Snort rule Buffer Overflow Vulnerability • 13405: RFB: GNOME Vino VNC Server Denial-of-Service Vulnerability • 13566: HTTP: Microsoft SharePoint 2010 Flat Forum Page • 16310: TLS: OpenSSL Denial-of-Service Vulnerability over SMTP • 16564: TCP: Kerberos 5 SPNEGO Token Denial-of-Service Vulnerability • 28018: SMB: Response for Domain Computers from Domain Controller • 30094: SMTP: Exim BDAT Use-After-Free Vulnerability • 30473: HTTP: Squid Proxy log_uses_indirect_client Denial-of-Service Vulnerability • 31765: HTTP: Squid Reverse Proxy sslBumpAccessCheck Denial-of-Service Vulnerability (ZDI-18-309) • 33923: HTTP: Google Golang Get Command Execution Vulnerability
Logging Mode	Configure settings to prevent traffic-related event notifications (such as those generated when a triggered filter is configured with a Block+Notify or Permit+ Notify action set) from causing network congestion. • **Logging Mode** determines whether logging is enabled/disabled when the network becomes congested. **Always** indicates that the system continues logging even if traffic is dropped under high load. **Disable if congested** indicates the logging will be disabled when the system reaches the specified congestion percentage. • **Congestion Percentage** can be configured if the disable logging option is selected. This value specifies the amount of network congestion that can occur before the system disables logging functions. • **Disable Time** specifies the amount of time (default is10 minutes) that logging is disabled before the service is restarted. When the downtime expires, the system re-enables logging and displays the number of missed notifications.
Congestion Notification	Specifies whether alert messages get sent when the overall device congestion exceeds the specified threshold.

Parameter	Description
HTTP Response Processing	Specifies inspection of encoded HTTP responses. • **Accelerated inspection of encoded HTTP responses** — Hardware acceleration is used to detect and decode encoded HTTP responses. • **Inspect encoded HTTP responses** — Enables strict detection and decoding of encoded HTTP responses. • **Ignore encoded HTTP responses** — The device does not detect or decode encoded HTTP responses. • **Enable URL & NCR encoding** — Decodes and inspects encoded HTTP responses. Enabled by default. This feature will not work if **Ignore encoded HTTP responses** is selected.
DNS reputation NXDOMAIN response	Allows the IPS to respond with `NXDOMAIN (name does not exist)` to clients that make DNS requests for hosts that are blocked.
IDS Mode	When IDS mode is enabled, it adjusts the device configuration so that the device operates in a manner suitable for Intrusion Detection System (IDS) scenarios and filter configurations. • Performance protection is disabled. • Adaptive Filtering is set to Manual. • Filters currently set to Block are not switched to Permit, and Block filters can still be set. When IDS Mode settings are changed, reboot the device for the change to take effect.

Configure adaptive filter settings

Describes how to configure adaptive filter settings.

On the IPS Preferences page, you can configure the global settings for the adaptive filtering. At the filter level, you have the option to disable adaptive filter configuration so that a filter is never impacted by adaptive filter settings on the device. For details, see *Edit DV filter category settings*.

You can view the effects of adaptive filter configuration in the **Ten Most Recent** table, which displays the ten filters most recently affected by the adaptive filter. You can also manage the global adaptive filter configuration and the filter-level configuration. To change filter-level configuration, click on the linked name of a filter in the list. For more information, see *Adaptive filter report* .

Procedure

1. From the LSM menu, click **IPS > Preferences**.
2. On the IPS Preferences page in the **Adaptive Configuration Settings** table, select the mode:
   - **Auto** — This setting enables the IPS device to automatically disable and log any defective filter.
   - **Manual** — This setting enables the IPS device to log any defective filter. However, the filter is not disabled.
3. Select the severity of the system log message that is automatically generated when a filter triggers the Adaptive Filter function.
4. Click **Apply**.

Events: logs, traffic streams, reports

The Events menu pages of the LSM allow you to monitor system performance and review traffic-related events. The menu provides the following options:

- **Logs** — View information on system events and traffic-related events triggered by IPS filters and policies. Logs include alert, quarantine, block, audit, and system logs.
- **Managed Streams** — Review and manage traffic streams that have been blocked, rate-limited, trusted, or quarantined by IPS policies. You can also manually quarantine or release a quarantined IP address.
- **Health** — Review the current status and network performance of the IPS device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance.
- **Reports** —View graphs showing information on traffic flow, traffic-related events, and statistics on triggered filters (filter matches, rate limit, traffic, DDoS, quarantine, and adaptive filter).

This topic discusses the following subjects:

- *Logs*
- *Managed streams*
- *Health*
- *Reports*

Logs

The logs provide information on system events and traffic-related events triggered by the filters that are configured on the device. Each menu page also provides functions to manage the log files. Logs also indicate the interfaces through which administrators interacted with the system, such as the LSM, the CLI, or an SMS.

The IPS device maintains an historical log file and a current log file for each log. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted. When the log is rolled over, the system generates a message in the Audit log. If you want to save all log data and create a backup, you can configure the system to offload log messages to a remote system log.

You can reset a log from its menu page, or use the Reset (↻) function on the System Summary page.

Note

TippingPoint recommends that you install a compact flash card for log storage or designate a remote system log location.

This topic discusses the following information:

- *Alert log*
- *Quarantine log*
- *Block log*
- *Audit log*
- *System log*
- *Viewing logs*

- *Downloading a log*
- *Resetting a log*
- *Searching a log*

Alert log

The alert log documents network traffic that triggers IPS filters configured with the following action sets:

- Permit + Notify
- Permit + Notify + Trace
- Trust + Notify
- Rate Limit + Notify

Any user can view the log, but only administrator and super-user level users can reset the log.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send Alert log entries to a remote syslog server from the Notification Contacts page. For more information, see the *Configure the remote system log contact*.

An Alert log entry contains the following fields:

Column	Description
Log ID	The system-assigned log ID number.
Date/Time	A date and time stamp in the format `YYYY-MM-DD HH:MM:SS`.
Severity	Indicates the severity of the triggered filter: • 4: Critical • 3: Major • 2: Minor • 1: Low When the log is downloaded, the severity is indicated with a number.
Filter Name	The name of the triggered IPS filter.
Rate Limit	If applicable, the rate limiter rate that was defined in the triggered action set and a link to the action set on which the log entry was generated. This field is blank for Permit and Trust action log entries.
Protocol	The name of the protocol that the action affects.
Virtual Segment	The virtual segment on which the alert occurred (such as 1A-1B).
Source Address	The source address of the triggering traffic.
Source Port	The source port of the triggering traffic.
Dest Address	The destination address of the triggering traffic.
Dest Port	The destination port of the triggering traffic.
Packet Trace	Indicates if a packet trace is available.
Client-IP	If the Capture Additional Event Information feature is enabled, provides the IP address of the attacking client.

Column	Description
Hit Count	Number of packets that have been detected if packet trace is enabled.
Additional Info ⓘ	An icon appears if and any additional information about the event is detected (the Capture Additional Event Information feature must be enabled). Additional information can include XFF, TCIP, HTTP method, HTTP host, and HTTP URI length. When you click the icon, a dialog displays any of the additional information that was captured.

Quarantine log

The Quarantine log records the IP addresses that have been added to and removed from quarantine. Quarantine logging operates independently of a policy's notification contacts, and quarantine events are always recorded in a log file and on the remote syslog server if configured to do so.

Any user can view the log, but only administrator and super-user level users can reset the log.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send quarantine log entries to a remote syslog server from the Syslog Servers page. For more information, see the *Syslog servers*.

A Quarantine log entry contains the following fields:

Column	Description
Log ID	A system-assigned log ID number.
Date/Time	A date and time stamp in the format *YYYY-MM-DD HH:MM:SS*.
Virtual Segment	The virtual segment on which the alert occurred (such as 1A-1B).
Source Address	The source IP address of the triggering traffic.
Action	Indicates whether the IP address was added to the quarantine or removed from quarantine.
Reason	The filter that triggered the quarantine action. • If the quarantine action was triggered manually, the notation is displayed. • If the action was triggered by Transparent HA, the notation is displayed.

Block log

The IPS Block log documents packets that trigger IPS filters configured with any action that includes a Block + Notify or Block + Notify + Trace action, including Quarantine and TCP Reset action sets.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send IPS Block log entries to a remote syslog server from the Notification Contacts page. For more information, see *Configure the remote system log contact*.

An IPS Block log entry contains the following fields:

Column	Description
Log ID	The system-assigned log ID number.
Date/Time	A date and time stamp in the format *YYYY-MM-DD HH:MM:SS*.

Column	Description
Severity	Indicates the severity of the triggered filter: • 4: Critical • 3: Major • 2: Minor • 1: Low When the log is downloaded, the severity is indicated with a number.
Filter Name	The name of the triggered IPS filter.
Protocol	The name of the protocol that the action affects.
Virtual Segment	The virtual segment on which the alert occurred (such as 1A-1B).
Source Address	The source address of the triggering traffic.
Source Port	The source port of the triggering traffic.
Dest Address	The destination address of the triggering traffic.
Dest Port	The destination port of the triggering traffic.
Client-IP	If the Capture Additional Event Information feature is enabled, provides the IP address of the attacking client.
Hit Count	Number of packets that have been detected that matched the filter. Applies only if packet trace is enabled.
Additional Info ⓘ	An icon appears if and any additional information about the event is detected (the Capture Additional Event Information feature must be enabled). Additional information can include XFF, TCIP, HTTP method, HTTP host, and HTTP URI length. When you click the icon, a dialog displays any of the additional information that was captured.

Audit log

The Audit log tracks user activity that might have security implications, including user attempts (successful and unsuccessful) to do the following:

- Change user information
- Change IPS, routing or network configuration
- Gain access to controlled areas (including the audit log)
- Update system software and attack protection filter packages
- Change filter settings

Note

Only users with Super-user access level can view, print, reset, and download the Audit log.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send audit log entries to a remote syslog server from the Syslog Servers page. For more information, see the *Syslog servers*.

An Audit log entry contains the following fields:

Column	Description
Log ID	The system-assigned log ID number.
Log EntryTime	A date and time stamp in the format *YYYY-MM-DD HH:MM:SS*.
User	The login name of the user who performed the audited action. The user listed for an event can include SMS, SYS, and CLI.
Access	The access level of the user performing the action.
IP Address	The IP address from which the user performed the action.
Interface	The interface with which the user logged in: WEB for the LSM, CLI for the command line interface. For system-initiated actions, SYS displays in this field.
Component	The area in which the user perform an action (LOGIN, LOGOUT, and Launch Bar Tabs).
Result	The action performed or the result of a LOGIN or LOGOUT attempt.
Action	The action performed as a result. For example, Log Files Reset.

System log

The System log contains information about the software processes that control the IPS device, including startup routines, run levels, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with your IPS device.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send System log entries to a syslog server from the Syslog Servers page. For more information, see *Syslog servers*.

Note

Users with any access level can view and print the system log, but only Administrator and Super-user level users can reset this log. For information on Adaptive Filter messages, see *Configure adaptive filter settings*. System log entries are sent to the syslog server only after the device has fully booted. During the boot sequence, entries cannot be sent because network ports are not yet enabled. When the boot sequence completes, the device sends a startup message to the syslog server.

A System log entry contains the following fields:

Column	Description
Log ID	A system-assigned log ID number.
Log Entry Time	A date and time stamp in the format *YYYY-MM-DD HH:MM:SS*.
Severity Level	Indicates whether the log entry is informational (INFO) or whether it indicates an error or critical condition (ERR or CRIT).
Component	Indicates which software component sent the message to the log.
Message	Text of the log entry.

All information logged by the LSM can be offloaded to a remote syslog server. Options to configure logging behavior for traffic-related events are available from the Notification Contacts page (**IPS > Notification Contacts**). To use remote logging options, you must configure the contact information for the remote syslog servers. For more information about configuring the Remote System Log contact for the Alert and Block Logs, see *Configure the remote system log contact*.

CAUTION!

Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol with no additional security protections. Therefore, use remote syslog only on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

Viewing logs

On each log page, the functions available for the log are displayed at the top of the page. You can also access the log functions from the **System Summary** page. The following table describes these functions:

Function	Icon/Field	Description
View	📄	To customize the display, specify the desired value in the **Records per page** field. To page through log entries, use the Navigation functions in the upper and lower left corners: **<<** Go to first page **<** Go to previous page **>** Go to next page **>>** Go to last page
Download	💾	Click the Download icon to download an electronic copy of the log or report. When you download some logs, the downloaded log file contains additional information that is not displayed in the LSM interface. For more information, see *Log formats*.
Search	🔍	Click the Search icon to search for an entry in the log or report.
Reset	🔄	Use the Reset icon to clear a log of all current entries. The log then begins compiling new information. Depending on your access level, this icon might not be available in the Audit and System logs.

Downloading a log

Describes how to download and save a log.

The IPS device maintains two files for each log: a historical log file and a current log file. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted. To save log data, download the log. In the LSM, the log view displays both current and historical log entries.

Procedure

1. In the LSM, select the log that you want to download.
2. On the log page, click the Download icon. The Download Log page is displayed.
3. Verify that the **Log Type** drop-down list box has the correct log selected.
4. In the **Log Entry** section, specify one of the following criteria for which log entries will be included in the downloaded file:
   - **All** — Downloads all entries in the current and historical log files.
   - **Time Range** — Downloads all entries within the specified dates and times.

- **ID Range** — Downloads all logs with log ID numbers within the specified range.

5. In the **Options** section, select one or both boxes for file format options:

    - **Comma delimited format (csv)** — Saves the file as a comma-delimited file.
    - **Open in browser** — Opens the download file in the web browser.

6. Click **Download**.

Note

Downloaded logs provide more detailed information on each event than what is displayed in the LSM interface. For more information, see *Log formats*. In the downloaded log, file entries are in a tab-delimited format with a line feed character terminating each line. Use WordPad or a spreadsheet application to view downloaded log files on a Windows workstation.

Resetting a log

Describes how to reset a log.

When you reset a log, the LSM starts a new log file beginning with the current date and time based on the system time. All previous information is permanently deleted. For record keeping, you may want to download the log before performing a reset. For more information, see *Downloading a log*.

Note

Only Administrator and Super-user level users can reset the system log. Only Super-user level users can reset the audit log.

Procedure

1. In the LSM, select the log that you want to reset.
2. Click **Reset**.

    A confirmation message is displayed, prompting if you want to reset the log.

3. Click **OK**.

Searching a log

Describes how to search for specific log entries.

Each log page provides a search function to help locate specific entries.

Procedure

1. Select the log that you want to search and click the **Search** button at the top of the page.
2. In the Search Log page, specify the search criteria.

    The available criteria will vary depending on the log that you are searching.

CRITERIA	DESCRIPTION
All	Searches all log entries.

CRITERIA	DESCRIPTION
Date Range	Locates all logs between the specified dates and times.
Severity	The severity includes low, minor, major, and critical events.
Filter Name	The filter that triggered logged events.
Protocol	The name of the protocol that the action affects.
Source Address	The source address of the triggering traffic.
Source Port	The destination address of the triggering traffic.
Destination Address	The destination address of the triggering traffic.
Destination Port	The destination port of the triggering traffic.
Client-IP Address	Block Log and Alert Log only. The source address of the attacking client (if enabled).
Component	Audit Log only. The type of event recorded by the Audit Log.

3. Choose the **# of Results to Display** from the drop-down box [optional].

4. Click **Search**.

Tip

When you enter filter names or IP addresses, you can enter partial names or addresses. For example, you can enter the first few letters or numbers in a filter name, or the first few numbers of an IP address.

Managed streams

The Managed Streams menu pages provide options to review and manage traffic streams that have been blocked or rate-limited by IPS policies. These events are captured by the Threat Suppression Engine (TSE), which uses a blend of ASICs and network processors to detect threats and anomalies in network traffic. There are four types of managed traffic streams:

- **Blocked streams** — Traffic streams detected and blocked based on filters configured with a Block action set.
- **Rate-Limited streams** — Traffic streams detected and rate-limited based on filters configured with a rate-limit action set.
- **Quarantined** — Hosts and addresses that have been quarantined based on traffic that triggered a quarantine filter.
- **Trusted** — Traffic that has been trusted based on a trust action set.

This topic discusses the following information:

- *Blocked streams*
- *Search blocked streams*
- *Flush blocked streams*
- *Rate-limited streams*
- *Search rate-limited streams*
- *Flush rate-limited streams*

- *Quarantined addresses*
- *Force IP address into quarantine*
- *Search quarantined addresses*
- *Flush quarantined addresses*
- *Trusted streams*
- *Search trusted streams*
- *Flush trusted streams*

For more information about action sets, see *Action sets*.

Blocked streams

When traffic triggers an IPS filter that has been configured with a Block or Block+Notify action, traffic from the source IP address and port is blocked and an entry is added to the Blocked Streams page, based on the contact configuration in the action set. From the Blocked Streams page, you can:

- View and search for information on blocked streams
- Manually clear all or selected blocked stream connections

The Blocked Streams table displays up to 50 entries. Entries are added when the block event occurs. Entries are automatically removed when the connection times out based on the **Connection Table timeout** setting configured from the IPS Preferences page. The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry from the table with the Flush function, which unblocks the stream.

For each blocked traffic stream, the Blocked Streams page provides the following information.

FIELD	DESCRIPTION
Protocol	Protocol used by the blocked connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Virtual Segment	The virtual port pair where traffic was blocked or rate-limited.
Reason	The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.

Search blocked streams

Describes how to search blocked streams for criteria that you specify.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Blocked Streams**.
2. Enter search criteria for any of the following:

- **Protocol** — The protocol for the connection: All, TCP, UDP, ICMP, ICMPv6
- **Src/Dest Address** — The traffic source or destination IP address
- **Port** — The traffic source or destination IP port

Entering `0` or `any` in the fields you do not want to specify allows you to search on any of the fields (combination or single).

3. Click **Search**.

What to do next

To reset the search, click **Reset**.

Note

When you specify a source or destination IP address and port, ensure that the specified port number corresponds to the IP address.

Flush blocked streams

You can manually unblock all or selected streams using the Flush functions available on the Blocked Streams page.

Note

Flushing all blocked streams can cause temporary congestion.

Flush all blocked streams

Describes how to flush all blocked streams

Procedure

1. From the LSM menu, click **Events > Managed Streams > Blocked Streams**.
2. Scroll to the bottom of the Blocked Streams page.
3. Click **Flush All**.

Flush selected blocked streams

Describes how to flush selected blocked streams

Procedure

1. From the LSM menu, click **Events > Managed Streams > Blocked Streams**.
2. Select the streams that you want to flush by clicking the check box next to the entry.
3. Scroll to the bottom of the Blocked Streams page.
4. Click **Flush Selected**.

Rate-limited streams

When traffic triggers an IPS filter configured with a rate-limit action set, traffic from the source IP and port is limited based on the rate-limit settings. Traffic from the source IP address and port to the destination IP address and port remains rate-limited until the connection timeout period expires, or until the connection is manually terminated from the LSM.

From the Rate Limited Streams page, you can:

- View and search for information on rate-limited streams
- Manually terminate all or selected rate-limited stream connections

For more information about performing these tasks, see *Search rate-limited streams* and *Flush rate-limited streams*.

The Rate Limited Streams table displays up to 50 entries. Entries are added when the rate-limit event occurs. Entries are automatically removed when the connection times out based on the **Connection Table timeout** setting configured from the IPS Preferences page. The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry with the **Flush** functions, which removes the rate limit from the stream.

The **Rate Limited Streams** table provides the following information:

COLUMN	DEFINITION
Protocol	Protocol used by the rate-limited connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Virtual Segment	The virtual port pair where the stream is rate limited.
Reason	The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.

Search rate-limited streams

Describes how to search rate-limited streams.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Rate Limited Streams**.
2. Enter search criteria for any of the following:
   - **Protocol** — The protocol for the connection: All, TCP, UDP, ICMP, ICMPv6
   - **Src/Dest Address** — The traffic source or destination IP address
   - **Port** — The traffic source or destination IP port

   Entering `0` or `any` in the fields you do not want to specify allows you to search on any of the fields (in combination or singly).
3. Click **Search**.

What to do next

To reset the search, click **Reset**.

Flush rate-limited streams

You can manually remove a connection from the table for all or selected streams using the Flush functions available on the Rate Limited Streams page.

Flush all rate-limited streams

Describes how to flush all rate-limited streams.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Rate Limited Streams**.
2. Scroll to the bottom of the Rate Limited Streams page.
3. Click **Flush All**.

Flush selected rate-limited streams

Describes how to flush selected rate-limited streams.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Rate Limited Streams**.
2. Select the streams that you want to flush by clicking the check box next to the entry.
3. Scroll to the bottom of the Rate Limited Streams page.
4. Click **Flush Selected**.

Quarantined addresses

When traffic triggers an IPS filter that has been configured with a Quarantine action, the host is quarantined and an entry is added to the Quarantined Addresses page, based on the contact configuration in the action set. From the Quarantined Addresses page, you can:

- Manually force an address into quarantine
- Search for quarantined addresses
- Manually release all or selected quarantined hosts

For more information about performing these tasks, see:

- *Force IP address into quarantine*
- *Search quarantined addresses*
- *Flush quarantined addresses*.

The **Quarantined Address(es)** table provides the following information:

Column	Definition
IP Address	IP address under quarantine.
Reason	The reason the IP address is under quarantine.

Force IP address into quarantine

Describes how to force and IP address into quarantine.

Note

To force IP addresses into quarantine, you must have quarantine action sets defined. See *Configure an action set*.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Quarantined Addresses**.
2. Enter the IP address that you want to quarantine.
3. Click **Quarantine**.

   The address is added to the Quarantined Address(es) table.

Search quarantined addresses

Describes how to search quarantined IP addresses.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Quarantined Addresses**.
2. Enter the IP address for which you want to search.
3. Click **Search**.

   The Quarantined Address(es) table is filtered to match the search terms.

What to do next

To reset the search, click **Reset**.

Flush quarantined addresses

You can manually remove addresses from quarantine for all or selected addresses using the Flush functions available on the Quarantined Addresses page.

Flush all quarantined addresses

Describes how to flush all quarantined addresses.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Quarantined Addresses**.

2. Scroll to the bottom of the Quarantined Addresses page.

3. Click **Flush All**.

Flush selected quarantined addresses

Describes how to flush selected quarantined addresses.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Quarantined Addresses**.

2. Select the addresses that you want to flush by clicking the check box next to the entry.

3. Scroll to the bottom of the Quarantined Addresses page.

4. Click **Flush Selected**.

Trusted streams

When traffic triggers an IPS filter configured with a Trust action set, traffic from the source IP and port is recorded on the Trusted Streams page. From the Trusted Streams page, you can:

- View and search for information on trusted streams
- Manually clear all or selected trusted stream connections

For more information about performing these tasks, see *Search trusted streams* and *Flush trusted streams*. For more information about the trust action, see *Configure an action set*.

The Trusted Streams table displays up to 50 entries. Entries are added when the trust action occurs. Entries are automatically removed when the connection times out based on the **Trust Table timeout** setting configured from the IPS Preferences page. The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry with the **Flush** functions, which removes the trusted stream from the table.

The **Trusted Streams** table provides the following information:

COLUMN	DEFINITION
Protocol	Protocol used by the trusted connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Virtual Segment	The virtual port pair where the stream is rate limited.
Reason	The filter link that details why the traffic connection stream was trusted. Click the link to display and manage the filter.

Search trusted streams

Describes how to search trusted streams by criteria that you specify.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Trusted Streams**.
2. Enter search criteria for any of the following:
   - **Protocol** — The protocol for the connection: All, TCP, UDP, ICMP
   - **Source or Destination Address** — The traffic source or destination IP address
   - **Source or Destination Port** — The traffic source or destination IP port

   Entering `0` or `any` in the fields you do not want to specify allows you to search on any of the fields (in combination or singly).
3. Click **Search**.

   The **Trusted Streams** table is filtered to match the search terms.

What to do next

To reset the search, click **Reset**.

Flush trusted streams

You can manually remove a connection from the table for all or selected streams using the Flush functions available on the Trusted Streams page.

Flush all trusted streams

Describes how to flush all trusted streams.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Trusted Streams**.
2. Scroll to the bottom of the Trusted Streams page.
3. Click **Flush All**.

Flush selected trusted streams

Describes how to flush selected trusted streams.

Procedure

1. From the LSM menu, click **Events > Managed Streams > Trusted Streams**.
2. Select the streams that you want to flush by clicking the check box next to the entry.
3. Scroll to the bottom of the Trusted Streams page.
4. Click **Flush Selected**.

Health

The Health menu pages show the current status and network performance of the IPS device. The menu provides the following options:

- **Monitor** — View status and statistics for device and module health, performance and throughput.
- **Performance** — View device throughput status and performance. Access the Performance Wizard, which provides information on current device status and advice on fixing any issues the device is experiencing.
- **Port Health** — View information for each Ethernet port on the device including current configuration settings.
- **High Availability** — View information on current high-availability status.

This topic discusses the following information:

- *Monitor*
- *Performance*
- *Port health*
- *High availability*

Monitor

Use the Monitor page (**Events** > **Health** > **Monitor**) to view and monitor device state and health. The Device Health table displays the current status of a variety of chassis components, including power modules, fans, temperature, and memory and disk space usage.

COLUMN	DESCRIPTION
Component	The component or resource being monitored. These components include the following: • Power Supply Status • Memory • Disk system • Disk user • Disk ramLog • Disk ramTmp • Disk ramRO • Temperature • I2C buses* • Fans* • Voltage *Each power supply and each fan is listed separately.

COLUMN	DESCRIPTION
State	The current operating status of the component or resource being monitored. • **Normal** — usage is at normal levels • **Major** — usage has reached the major threshold setting specified for the device • **Critical** — usage has reach the critical threshold setting specified for the device To set the thresholds that trigger the Major and Critical states for memory and disk usage, go to the **System > Thresholds** page.
Graph	A bar graph depicting the current usage level of the component or resource.
Details	The units being measured in the graph. For example, the memory component displays the percentage of total available memory in use.

Performance

To view the current throughput performance of the device, click **Events > Monitor > Performance**.

Segments are grouped according to module on the NX-Platform devices. Each module occupies a **Slot**, which appears as a subsection of the Port Health table. The table displays both aggregate performance statistics and statistics broken down by segment.

The Performance/Throughput table displays the following information:

COLUMN	DESCRIPTION
Component	The port being monitored.
State	The current operating status of the port. • **Normal** — The port is active without errors. • **Major** — The port is active but has errors. • **Critical** — The port is waiting for traffic or usage in a stand-by mode. • **Out-of-service** — The port is not working or disabled. • **Diagnostic** — The port is running a diagnostic. • **Inactive** — The port is not in use or is disabled.
Graph	A bar graph depicting the current usage level of the port.
Details	Percentage of throughput used.

The System Performance Messages table appears below the Performance/Throughput table. This table provides information about current system performance. If the system is experiencing problems, the table displays messages indicating the cause of the problem and with suggested remedies.

Port health

To view Port Health information for each port on the device, click **Events > Health > Port Health**. The Port Health table displays the following information:

Column	Description
Port	Port number, listed by segment.
Speed	Port speed.
Duplex	Indicates if the port is set to full or half for duplex.
State	• A description of the current operation state of the port: • **Active** — The port is active without errors. • **Out-of-service** — The port has been disabled. • **Active With Faults** — The port is enabled but disconnected. • **Degraded** — The port is enabled but inactive. • An indication of the traffic throughput state of the port: • **Green** — Traffic throughput is below 80 percent. • **Yellow** — A minor threshold has been reached with traffic throughput at 80 percent or above. • **Red** — A major threshold has been reached with traffic throughput at 99 percent or above.
Info	The current state of any SFP or XFP module attached to the port.
Link Status	Indicates if the link is down or up.
Media	The port medium, which can be copper or fiber.
Type	The type of the port.

Segments are grouped according to module on the NX-Platform devices. Each module occupies a **Slot**, which appears as a subsection of the Port Health table.

High availability

The High Availability page lists the current high availability status for the following High Availability features:

- Intrinsic Network High Availability
- Transparent High Availability
- Zero-Power High Availability

Some devices support the Smart ZPHA module in conjunction with the 10GbE segments. Users who have the Smart ZPHA module see two entries under Zero Power High Availability:

- **External** — The external ZPHA module.
- **10GbE Segment** — The Smart ZPHA module. It is listed by the 10GbE segment name.

Intrinsic network HA

Intrinsic Network HA (INHA) determines how the IPS device manages traffic on each segment in the event of a system failure. When the system fails, the device goes into Layer-2 Fallback mode and either permits or blocks all traffic on each segment, depending on the Layer-2 Fallback action setting for the segment. When the device is in Layer-2 Fallback mode, any traffic allowed through the device will not be inspected; it simply passes through the device.

A lack of reported errors or congestion through the TSE does not guarantee that the components receive correct and error-free traffic. The INHA monitors the TSE for several points of failure and applies failure detection logic against the system. All components for the INHA are checked for failure.

The IPS device performs the following checks to detect a failed condition and trigger a Layer-2 Fallback:

- **Check back-pressure** — Presence of back-pressure indicates packets are queued for processing. It indicates a failure if it does not process packets.
- **Determine traffic requirements** — If the IPS does not pass traffic, the ability to detect a failed TSE is more difficult. A minimum rate of traffic must pass through the IPS for best TSE-failure detection.
- **Handle non-atomic nature of the data path** — Packet pass through each component at different times and rates. The status of each component is determined independently of each other. INHA uses sampling to determine if the TSE is healthy.
- **Check and transmit the inbound receive counters** — Each component has *receive* counters incremented by packets received from the previous component. The component transmits these counters incremented as packets to the next component. These counters are the most accurate and most complicated way of detecting TSE health.
- **Dropped packets exceeds threshold** — If too many packets awaiting deep inspection are queued up, packets are dropped.
- **Memory lows** — Whether available system memory is too low for proper operations.
- **Various chip set errors** — Represents possible hardware problems.

Each component also has a specific set of functions for failure checking.

You can view and configure the Layer-2 Fallback behavior for each segment from the Network Segments page (**Network > Segments**). The default setting for each segment is to permit all traffic. This setting is usually preferred by service providers because it prevents a device outage from becoming a network outage. However, for greater security, you might want to change the default Layer-2 Fallback setting to **block all** to guarantee that no uninspected traffic enters the network.

You can view and manually change the current INHA state (**normal** or **Layer-2 Fallback**) from the High Availability menu page.

Transparent HA

Transparent High Availability allows users to install two IPS devices in a redundant network configuration. Users configure their IPS devices so that when one device experiences a system failure, traffic can be routed to the other device with no interruption in intrusion prevention services.

Note

Data might not reach the peer machine if “active” machines are under extremely heavy load.

Transparent HA requires you to configure two IPS devices with the same settings. Before you can configure the Transparent HA settings on a device, the devices must meet the following network setup and communication requirements:

- Both devices must be from the same product family and running the same TOS version. For example, a device running TOS 2.5.x cannot be paired with one running TOS 3.2.x.
- Each device must have a secure connection to the network and to the other device in the Transparent HA pair.
- Both devices must be able to communicate on TCP port 9591.
- A device configured with Transparent HA can only connect and communicate with a partner configured to talk to other IPS devices configured with TRHA. In other words, both machines participating must point to each other. Each device must be configured with the partner serial number and IP address.

CAUTION!

A hijacked IPS or a rogue IPS that “steals” the IP address of a TRHA partner can communicate with a legitimate IPS.

You can configure the Transparent HA settings and manually enable or disable the feature from the device High Availability menu page. See *Configuring high availability from the LSM*.

Note

If your system has two IPS devices communicating through Transparent HA, a change to the global timeout for the connection table at one IPS device will not propagate to the other IPS. You must make this change on each device accordingly.

Zero-power HA

Zero-Power High Availability provides high availability through an external device, a Smart ZPHA module, or through bypass I/O modules. Some devices support the Smart ZPHA module in conjunction with the 10GbE segments. For detailed information about the Smart ZPHA module, refer to the TippingPoint Smart ZPHA Installation Guide.

Editing high availability configuration

Describes how to set or change your high availability settings.

Procedure

1. On the High Availability page, click any of the High Availability links. The High Availability page is displayed.
2. Edit your High Availability settings as needed:
   - **Intrinsic Network HA** — Select **Normal** to handle traffic normally. Select **Layer-2 Fallback** to place the device in Layer-2 Fallback mode.
   - **Transparent HA** — Select the check box to enable Transparent HA. You must enter the IP address of the partner device that will process traffic when the current device is unavailable.
   - **Zero-Power HA** — Select **Normal** to handle traffic normally. Select **Bypass** to bypass the device.
3. Click **Apply** to apply the changes.

Reports

The **Reports** provide access to detailed information about the LSM system alert and traffic activity. Data for each report is gathered in real time. You can use the **Refresh** option on each report page to get the most current report information. On some reports, an **Animate Charts** option is available.

The following Reports are available:

- **Filter Matches** — Displays data on traffic that has been filtered by the device based on the Digital Vaccine filter configuration in a Security Profile.
- **Rate Limits** — Displays a bar graph showing the percentage of rate-limit bandwidth used for each action set configured with a rate limit.
- **Traffic** — Displays traffic flow data categorized by transmission type, protocol, frame size, and port.
- **DDoS** — Displays the number of DDoS attacks on the system.

- **Quarantine** — Provides data on the number of hosts that have been quarantined over a selected time period.
- **Adaptive Filter** — Displays the global Adaptive Filter settings and a list of the 10 most recent filters impacted by adaptive filtering. You can also edit the Adaptive Filter settings from this report page.

This topic discusses the following information:

- *Filter match reports*
- *Rate-limit reports*
- *Traffic reports*
- *DDoS report*
- *Quarantine report*
- *Adaptive filter report*

Filter match reports

The Filter Match Reports page allows you to view data on traffic that has been filtered by the device based on the Security Profile configuration. This report reflects activity resulting from Digital Vaccine Filters.

Note

Additional information on filter match events is available in the LSM logs. For more information, see *Logs*.

Traffic data is reported based on the view options you select. Each graph displays data based on the percentage of traffic affected by the filters.

- **Top Ten Filters** — Displays a bar graph of the top 10 attack filters. The graph also lists a packet count.
- **Severity** — Displays a bar graph of attacks categorized as Low, Minor, Major, and Critical. The graph also lists the number of attacks. The severity levels are assigned by the TippingPoint Digital Vaccine team and are included as part of the filter definition.
- **Action** — Displays the actions taken on filtered traffic. The graph also lists the number of packets processed with each action. The following actions are listed:
    - Block
    - Permit
    - Rate limit
    - Trust
    - Packet
    - Packet Trace
    - For dropped packet information, see *Packet stats*.
- **Protocol** — Displays attack traffic categorized by protocol (ICMP, ICMPv6, UDP, TCP, IPv4-Other, and IPv6-Other). The graph also lists the number of filtered packets for each protocol.
- **Virtual Segments: All** — Displays amount of all attack traffic reported by the virtual segment where the traffic was filtered.
- **Virtual Segments: Permit** — Displays amount of attack traffic permitted reported by virtual segments.

- **Virtual Segments: Block** — Displays amount of attack traffic blocked reported by virtual segment.
- **Reset** — Resets all data value to 0 (zero) so that traffic can be remeasured.

Rate-limit reports

A rate-limit action set defines the maximum amount of bandwidth available for traffic matching IPS filters that have the action set assigned. If two or more IPS filters use the same rate-limit action set, then all packets matching these filters share the bandwidth. For each rate-limit action set, the Rate Limit Reports page allows you to view the percentage of bandwidth consumed by rate-limited traffic graphed as a function of time. Data is reported based on the view options you select in the Rate Limit Reports page:

- **Rate Limit Action Set Name** — The list of available rate limit action sets is provided at the top of the rate limit table. To view the percentage of rate-limited bandwidth used for an action set, click on the action set name to update the report.
- **Reporting time interval** — Select the time interval for the reporting period: **Last 24 hours, Last 60 Minutes, Last 300 seconds**.

Note

The Rate Limit report is available only if an action set has been configured with the Rate Limit action.

For more information about rate-limit action sets, see *Action sets*. For more information about rate-limited traffic streams, see *Rate-limited streams*.

Traffic reports

The traffic report provides profile data on the packets flowing through the device (permitted packets only). Traffic data is reported based on the view option you select on the Traffic Reports page:

- **Transmission Types** — The number of packets transmitted for each of the following transmission types: Unicast, Broadcast, MultiCast, MAC control, FCS Errors, Align Errors.
- **Protocol** — The number of packets transmitted by ICMP, ICMPv6, UDP, TCP, IPv4-Other, IPv6-Other, ARP, and Ethernet-Other.
- **Frame size** — Traffic profile by frame size, specified by byte ranges.
- **By Port** — Traffic profile by port.

To update the traffic statistics over time, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.

DDoS report

The DDoS report shows how often DDoS filters have been triggered over a selected time period. The display is based on the view options that you select on the DDoS Report page.

- **Rejected SYNs/sec and Proxied Connections/sec** — In the first drop-down menu, you can view the data by the total number of rejected SYNs per second or proxied connections per second. This data is listed by DDoS filter.
- **Time Period** — In the second drop-down, you can select parameters to view the reports over the following time periods:
  - 35 days

- 24 hours
- 60 minutes
- 60 seconds

Quarantine report

The Quarantine report provides data on the number of hosts that have been quarantined over a selected time period. The display is based on the view options that you select on the Quarantine Report page.

- **Hosts, Packets, or Pages** — In the first drop-down menu, you can select parameters to view the data by the total number of quarantined hosts, the number of packets blocked, source pages, and redirected pages.
- **Time Period** — In the second drop-down, you can select parameters to view the reports over the following time periods:
  - 35 days
  - 24 hours
  - 60 minutes
  - 60 seconds

Adaptive filter report

From the Configure Adaptive Filter Events Report page, you can:

- Review and modify the global Adaptive Filter configuration.
- View a list of the 10 most recent filters managed by adaptive filtering.
- Disable adaptive filter settings for an individual filter.

The Configure Adaptive Filter Events report page provides the following information:

COLUMN	DEFINITION
Settings	Allows you to change the global system configuration for the Adaptive Filter function. For more information, see *Configure adaptive filter settings*.
Ten Most Recent table	Displays the ten most recent filters managed by adaptive filtering. • **Filter Name** — The name of the filter being managed by the Adaptive Filter function. Click on the name of the filter for more information. • **Filter State** — Indicates if the filter is enabled or disabled. • **Adaptive Filter State** — Indicates if adaptive filtering is enabled or disabled for the filter. • **Function(s)** — Actions that can be performed on the filter.

For more information about the Adaptive Filters, see *Configure adaptive filter settings*.

To disable adaptive filtering on a single filter

Describes how to disable adaptive filtering on a single filter.

Procedure

1. Click the filter's name.
2. On the Edit Filter page, click **Do not apply adaptive configuration settings to this filter**.

To change global adaptive filter settings

Describes how to change global adaptive filter settings.

Procedure

1. From the LSM menu, click **Events > Reports > Adaptive Filter**.
2. On the Configure Adaptive Filter Events page, select the mode:
   - **Auto** — Enables the IPS device to automatically disable and log any defective filter.
   - **Manual** — Enables the IPS device to log any defective filter. However, the filter is not disabled.
3. Select the severity of the system log message that is automatically generated when a filter triggers the Adaptive Filter function.
4. Click **Apply**.

System

The System menu in the LSM provides options for managing TOS and Digital Vaccine packages, system configuration options, and access to external resources, such as syslog and email servers and remote management applications.

This topic includes the following subjects:

- *Update*
- *Management port*
- *Management routing*
- *Time options*
- *SMS/NMS*
- *High availability*
- *Compact flash*
- *Thresholds*
- *Email server*
- *Syslog servers*
- *Remote servers*
- *Named networks*
- *License*

- *Technical support report*

Update

In the LSM, you can manage system software and Digital Vaccine filter packages from the Update pages. These pages are located under the **System > Update** menu.

- **Update Summary** — Lists the following information:
  - Device product code and serial number. The serial number can be used to create a TMC account, and might also be needed when you contact TippingPoint Technical Support.
  - Currently installed versions of the TOS, the Digital Vaccine (DV), and other DV packages (Reputation DV, Auxiliary DVs, custom DV (if applicable)), and license package. A rollback icon indicates that there is at least one prior version of the IPS software on the device to which you can rollback. See *Rolling back to a previous TOS version*.
  - Previously installed TOS versions. You can delete TOS software and Digital Vaccine versions installed on the device.
  - Any auxiliary DV packages that have been installed.
- **Install Package** — Enables installation of TOS, DV, IP Reputation, SSL key, or license packages.
- **Auto DV Update** — Enables configuration of automatic DV updates.
- **System Snapshot** — Enables creation and management of system snapshots.

The device and software state information provided by the Update page is discussed in the following topics:

- *Managing current TOS software*
- *Viewing and managing current digital vaccine filters*
- *System snapshots*

Managing current TOS software

You can download and install TOS updates from the **System > Update > Install Package** page.

When downloading and installing a software package, verify that the package you download is not larger than the listed amount of free space. An unpacked package might require more space than anticipated, depending on your device model, saved snapshots and rollback versions, and the size of the available update. To make sure the device has enough disk space, you can delete previously installed software images from the Update page.

This topic discusses the following information:

- *Updating the TOS software*
- *Download a TOS software update*
- *Install a software update*
- *Rolling back to a previous TOS version*
- *Delete a previously installed TOS software version*

Updating the TOS software

When improvements or additions are made to the IPS system, TippingPoint releases a software update on the TMC Web site (https://tmc.tippingpoint.com). You can download and install updates from this site.

CAUTION!

You must read the release notes posted with the TOS software update package on the TMC. The release notes contain information that can make the difference between a successful software update and an unsuccessful software update.

TOS updates are hitless by default, and the device continues to inspect traffic flow while the software is updated until the device is rebooted. You also have the option to place the device in Layer-2 Fallback mode during the software update. In this mode, individual segment settings are enforced during the update, including during the subsequent reboot. For example, traffic is permitted through the device without inspection for each segment where the Layer-2 Fallback option is set to Permit. However, traffic will be blocked on any segment where the Layer-2 Fallback option is set to Block.

Note

During a TOS update on TippingPoint 10, 110, and 330 devices in which Layer-2 Fallback mode is selected, all segments will be in Permit mode during the reboot stage regardless of the segment settings.

When you perform a software update, your current configuration and filter settings are persisted forward and an archive copy of your current filter settings is saved. If you perform a software rollback in the future, any changes made to your filter settings after the update will not be preserved.

During a graceful shutdown, as during an update or reboot (in the LSM or command in the CLI), Packet Trace data might not be automatically flushed to disk. To guarantee Packet Trace data is flushed to disk, do the following:

- Click on any Packet Trace icon in the alert or block logs
- Click on the Packet Trace (TCPDUMP) icon

The update takes approximately 30 minutes for the entire procedure, depending on your download speed. The following table provides a summary of the process with time estimates.

STEP	TASK	MANUAL OR AUTOMATIC	ESTIMATED TIME	LINK STATUS
1	Download the package	Manual	Varies	Up
2	Install the package	Manual	15–20 minutes	Up
3	Reboot the TippingPoint device	Automatic	5 minutes	Intrinsic Network HA
4	Commit and update the changes	Automatic	A few seconds	Intrinsic Network HA

In the Intrinsic Network High Availability (INHA) state, the links remain up, but inspection is bypassed. For more information about INHA, see *Intrinsic network HA*.

Note

Traffic is inspected during a hitless update; however, during a hitless reboot, traffic is not inspected. Hitless reboots are not supported on the TippingPoint 10, 110, or 330.

Download a TOS software update

Describes how to download a TOS software update.

Note

To force IP addresses into quarantine, you must have quarantine action sets defined. See *Configure an action set*.

Procedure

1. Log in to the LSM.
2. From the LSM menu, click **System > Update > Install Package**.
3. On the Install Package page under Step 1, click **Threat Management Center** to access the TippingPoint Threat Management Center.
4. Log in to the Threat Management Center. If necessary, create an account from the login page.
5. From the top menu bar on the TMC home page, click **Releases > Software > [*`modeltype`*] > [*`modelnumber`*]**.

   The model number and type is available on the LSM home page.
6. Click on the software update that you want to download. On the Software Details page, review the information about the package.
7. Click the **Download** tab to download the package to your local system. Make sure to note the download location and the file size.

After you have downloaded the update, you can install it from the LSM Update page. For details, see *Install a software update*.

Note

If you are installing an IP Reputation package or a license package, the procedure is similar. You must purchase the appropriate package and receive the download instructions from your TippingPoint representative.

Install a software update

Describes how to install a TOS software update.

Prior to installing the new software, back up any custom filters you have created and implemented. The update overwrites these files.

When you perform an update of the software, the Update page displays a set of status messages. See *Log formats* for details.

CAUTION!

During the LSM install, do not close the browser window or navigate off the Update page while the software installs.

Procedure

1. Download a software update package from TMC.
2. If you are not already on the Install Package page, navigate there (**System > Update > Install Package**).
3. Verify available disk space on the TOS & DV Update page.

   a. If the update package that you downloaded is smaller than the requirement listed, proceed to Step 4.

   b. If the update package is larger than the number listed, delete older versions of the software to free disk space. For details see, *Delete a previously installed TOS software version*.

   After freeing disk space, return to the **System > Update > Install Package** page.
4. If you choose to, enable one or both of the following options:

- **Enable High Priority Preference** — Gives requests from the software update process the highest system priority until the update completes. However, the system does not give package installation processes priority over attacks. If an attack occurs during an update, the system does not give priority to the update process at that time.
- **Enable Layer-2 Fallback** — Places the device in Layer-2 Fallback while the software update takes place. If selected, all segments are placed in L2FB.

5. Click **Browse** to select the update package file that you downloaded from the Threat Management Center.
6. Click **Install** to install the software update.

   When updating the IPS software, the progress bar might be interrupted by a pop-up message window. If this occurs, you need to monitor the update process using the system log. If the system log does not show any errors during the update process, the IPS reboots when the update is complete.

When the installation completes, the IPS performs a soft reboot. After the reboot, you can log back in to the system.

Note

If you are installing an IP Reputation package or a license package, the procedure is similar. You must purchase the appropriate package and receive the download instructions from your TippingPoint representative.

Rolling back to a previous TOS version

Describes how to roll back to a previous TOS.

A rollback operation reverts the currently running software version on your IPS device to a previous working version. The system retains the settings and configurations of your system. However, depending on the version of the TOS you rollback to, not all functionality will be available.

CAUTION!

If you perform a rollback, read the release notes for both the software version you are rolling back from and the software version you are rolling back to.

When you perform a TOS rollback, current configuration settings are preserved, but filter settings revert to the settings that were in effect when the rollback version was archived. Any filter changes made after the target rollback version are deactivated, including attack protection filter updates.

Procedure

1. On the **System > Update > Update Summary** page in the **Current Installed Versions** table, click the **Rollback** icon in the **Functions** column for the TOS Software.

   A confirmation message is displayed.
   The IPS device deletes the current operating system files and reinstalls the previous operating system files. The Update page displays a set of status messages. When the installation completes, the device performs a soft reboot. See *Log formats* for details about the update status messages.
2. After the devices installs the previous TOS version, log in to the LSM again.

To restore the operating system you rolled back from, perform a software update installation on your IPS device.

Delete a previously installed TOS software version

Describes how to delete a previously installed TOS.

Deleting a previously installed TOS version frees disk space on the device. After a TOS version is deleted, it is no longer available for rollback.

CAUTION!

Unless the device is out of disk space, do not delete the previous TOS image that you were running. If the current TOS image becomes corrupted, you can roll back to the previous version as explained in *Rolling back to a previous TOS version*.

Procedure

1. On the **System > Update > Update Summary** page in the **Previous TOS Versions** table, review the list of previous versions and decide which is safe to delete.
2. Click the delete icon (✖) in the **Functions** column for the TOS software package you would like to delete.

   A confirmation message is displayed.
3. Click **OK**.

Viewing and managing current digital vaccine filters

You can download and install DV updates from the Install Package page, and configure automatic DV updates from the Auto DV Update page.

When downloading and installing a DV package, verify that the package you download is not larger than the listed amount of free space. An unpacked package might require more space than anticipated, depending on your device model, saved snapshots and rollback versions, and the size of the available update. To make sure the device has enough disk space, you can delete previously installed software images from the Update page.

This topic discusses the following information:

- *Updating the digital vaccine (filters)*
- *Enable auto update for digital vaccine*
- *Manually download a DV update*
- *Manually install a DV update*

Updating the digital vaccine (filters)

When new types of network attack are discovered, or when detection methods for existing threats improve, the Digital Vaccine team at the Threat Management Center (TMC) creates and releases new filters to add to your filter database. These filters are released as Digital Vaccine (DV) packages.

When a new DV package is available for download, the TMC team sends notifications to existing customers. You have two options to update the DV on your device:

- Configure the Auto DV option on your device so that the device checks for new DV packages and automatically updates the device as necessary.
- Manually download and install the DV package.

Note

You cannot rollback to a previous Digital Vaccine version. If you want to use a previous version of a Digital Vaccine, download an older version of the Digital Vaccine package from the TMC.

To make sure the device has enough disk space, you might need to delete previously installed software images from the Update page. For details, see *Delete a previously installed TOS software version*.

Enable auto update for digital vaccine

Describes how to configure your IPS to update your digital vaccine automatically.

If AutoDV is configured, the system automatically checks the DV version when you open the Auto DV Update page. The status is listed in the **Auto Update** section. To perform an update immediately, click **Update Now**.

Procedure

1. From the LSM menu, click **System > Update > Auto DV Update**.
2. Click the **Enabled** check box to enable the option.
3. Select the type of schedule that you want to use for the DV update process.
   - **Periodic** — Performs an update every number of days starting from a set day. The option includes a time to perform the update.
   - **Calendar** — Performs an update on a set day and time per week.
4. Set the update parameters.
5. Click **Apply**. To perform an update immediately, click **Update Now**.

Manually download a DV update

Describes how to download a DV update from the TMC.

You can manually download the most current DV from the TippingPoint Threat Management Center, and then manually install the DV update.

Procedure

1. From the LSM menu, click **System > Update > Install Package**.
2. On the Install Package page, click **Threat Management Center** to access the TippingPoint Threat Management Center.
3. Log in to the Threat Management Center. If necessary, create an account from the login page.
4. From the top menu bar on the TMC home page, click **Releases > Digital Vaccine** to display the list of digital vaccine filters available.
5. Click on the software update that you want to download. On the Software Details page, review the information about the package.

   Note

   For DV packages, you cannot rollback to a previous version. To use a previous version, download that version from the TMC.

6. Click the **Download** tab to download the package to your local system. Make sure to note the download location and the file size.

Manually install a DV update

Describes how to install a DV update.

Procedure

1. Download a DV package from TMC.
2. If you are not already on the Install Package page, navigate there (**System > Update > Install Package**).
3. Verify available disk space on the Install Package page.
   a. If the DV package is smaller than the required space, proceed to Step 4.
   b. If the DV package is larger than the number listed, delete older versions of the software to free disk space. For details see, *Delete a previously installed TOS software version*. After freeing disk space, return to the TOS/DV Update page and repeat Step 2 and 3.
4. If you choose to, enable one or both of the following options:
   - **Enable High Priority** — Gives requests from the DV update process the highest system priority until the update completes. However, the system does not give package installation processes priority over attacks. If an attack occurs during an update, the system does not give priority to the update process at that time.
   - **Enable Layer-2 Fallback** — Places the device in Layer-2 Fallback while the DV update takes place.
5. Click **Browse** to select the DV update package file that you downloaded from the Threat Management Center.
6. Click **Install** to install the DV update.

   While the new file is loaded onto your IPS device, an Update Progress page displays the current status of the update. After the installation completes, you are returned to the Update page. The new version is displayed in the **Version** column of the **Current Installed Versions** table.

System snapshots

From the **Update > System Snapshots** page, you can create, manage, restore and import local snapshots for your IPS device. System snapshots can be restored on the same software version on which they were created. After restoring a snapshot, the device always restarts.

Before taking a system snapshot, ensure that a correctly formatted external storage card is available.

Important

For external storage on N-Platform devices, a CompactFlash card is required. For external storage on NX-Platform devices, a CFast card is required.

CAUTION!

You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices managed by SMS. Do not perform an Update of your software while running a snapshot. The system can experience conflicts.

The System Snapshots page provides the following information.

Column	Definition
Name	Name of the snapshot.
Date	The date the snapshot was generated.
Software Build	The build number for the TOS software running when the snapshot was generated.
Digital Vaccine	The version number of the Digital Vaccine package running when the snapshot was generated.
Model Type	The model name of the device on which the snapshot was generated.
Functions ✖ ⟳ 💾	Icons representing functions to manage snapshots. The following functions are available: • Delete a snapshot • Restore a snapshot • Import a snapshot

This topic discusses the following information.

- *Create a snapshot*
- *Import a snapshot*
- *Restore a snapshot*
- *Export a snapshot*
- *Delete a snapshot*

Create a snapshot

Describes how to create a snapshot.

Procedure

1. From the LSM menu, click **System > Update > System Snapshots**.
2. In the **Create snapshot** field, type a name for the snapshot.
3. Select **Include Reputation addresses** to include any user-entered IP and DNS reputation entries.
4. Select **Include Reputation DV** to include the files from the Reputation DV package.
5. Select **Include Management Port Configuration** to include the network configuration from your IPS's management port. For more information on these settings, see *Management port*.
6. Click **Create**.

> **Note**
>
> Including Reputation addresses and Reputation DV can generate a very large snapshot file. However, under certain circumstances, excluding Reputation addresses or the Reputation DV can cause errors. See *Restore a snapshot*.

Import a snapshot

Describes how to import a snapshot.

Procedure

1. From the LSM menu, click **System > Update > System Snapshots**.
2. In the **Import Snapshot** field, click **Browse** to select the file to import.
3. Click **Install**. The selected snapshot uploads and is displayed in the list of snapshots.

Restore a snapshot

Describes how to restore a snapshot.

When you restore a snapshot, you replace all current settings with those from the snapshot. After restoring a snapshot, the device always restarts.

CAUTION!

You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices managed by SMS.

Procedure

1. From the LSM menu, click **System > Update > System Snapshots**.
2. In the Restore Snapshot field, select whether you want the imported snapshot to exclude the management port configuration settings. For more information on these settings, see *Management port*.
3. In the **Function(s)** column for the snapshot you want to restore, click **Restore** (⟳).

Snapshots and Reputation Feed

Errors occur when you restore a snapshot that meets the following criteria:

- Reputation Feed filters are configured.
- Snapshot excludes Reputation addresses or the Reputation DV.

After restoring this snapshot, you cannot manually create filters, and Reputation filters will be marked with an error message, as in the following example:

```
Group Not Found - Filter  Block + Notify + Trace  Enabled Delete
```

When you delete all Reputation filters designated with `Group Not Found`, manual filter creation will be re-enabled.

Export a snapshot

Describes how to export a snapshot.

Procedure

1. From the LSM menu, click **System > Update**.

2. Click the **System Snapshots** tab.
3. In the **Current Snapshots** table, locate the snapshot you want to export.
4. In the **Function(s)** column, click the **Export** () button.

   When you export a snapshot, you save the snapshot to a local directory to later import if needed.

Delete a snapshot

Describes how to delete a snapshot.

Procedure

1. From the LSM menu, click **System > Update**.
2. Click the **System Snapshots** tab.
3. Locate the snapshot you want to delete.
4. Click the **Delete** (✗) icon.

Login consent banner

TOS Version 3.8.0 introduces support for a user-configurable login banner.

> To configure a banner message, you must have Super-User or Admin privileges.

Select **System > Login Banner**, and select the **Login Banner Enabled** checkbox.

- Enter text for the login banner title (maximum of 50 printable ASCII characters).
- Enter text for the login banner text (maximum of 1500 ASCII characters).

To display the following ASCII characters in the login banner text message using the CLI, use these key combinations:

- For a double-quote ("), type `\q`
- For a hash tag (#), type `\p`
- For a backward slash (\), type `\\`
- For a new line, type `\n`

When your login banner is complete, click **Apply**. To see how it will display, click the **Login Banner Preview**. Banner messages can be turned off without erasing the banner text.

Management port

The management port is a separate network connection used to communicate with your TippingPoint IPS device. During the initial IPS setup, you configure the network setting for the management port via the serial console. After the IPS is installed, you can use the Management Port option in the LSM (**System > Management Port**) to review or modify the management port configuration.

You can manage the management port settings and reboot the IPS device through the Management Port page.

The Management Port page includes the following features and options:

Feature	Description
Reboot Device	Reboots the device.
Management Port Services	Manages the web and CLI access services. By default, these options are set to HTTPS and SSH.
IPv4 Address	The IP address used to connect to your TippingPoint device. Must be a valid IPv4 address on the network segment to which the device is connected, in the form `xxx.xxx.xxx.xxx/xx`. If the routing prefix size is not specified, the default is 24. TippingPoint recommends configuring the management port on the IPS to use a non-routed IP address from the RFC 1918 Private Address space. This helps to prevent a direct attack on the management port from the Internet.
Default IPv4Gateway	The gateway through which the TippingPoint device communicates with external network entities. Must be a valid IP address in the form `xxx.xx.xxx.xxx/xx`. If the routing prefix size is not specified, the default is 24.
IPv6 Link-Local Address	The link-local IPv6 address for the device. This field is read-only.
IPv6 Auto	Indicates whether automatic IPv6 configuration is enabled on the device.
IPv6 Auto Address	If automatic configuration is enabled, the IPv6 address assigned by the router. This field is read-only.
IPv6 Address	The IPv6 address used to connect to your TippingPoint device. Enter `none` if automatic configuration is enabled.
Default IPv6 Gateway	The IPv6 gateway through which the TippingPoint device communicates with external network entities. Enter `none` if automatic configuration is enabled.
Host Name	The host name of the device. Must be a valid host name on your network segment, with a maximum of 32 characters.
Host Location	Optional description of the location of the TippingPoint device, with a maximum of 32 characters.
Active FIPS Mode	Shows the currently active FIPS mode. • **Crypto** — Only FIPS-approved cryptographic algorithms are allowed, and other FIPS 140-2 requirements are not enforced. • **Full** — Only FIPS-approved cryptographic algorithms are allowed, and all FIPS 140-2 requirements are enforced. • **Disable** — Non-FIPS-approved cryptographic algorithms are allowed.
Configured FIPS Mode	Shows the FIPS mode that will be enabled when the device is rebooted.
Active SSL Cert	Shows the status of the SSL certificate. • **Authorized** — The device is using the default SSL certificate that shipped with the device or an authorized SSL key has been installed from a TippingPoint-provided SSL key package. • **Generated** — A self-signed key is enabled on the device. Obtain an authorized SSL key from TippingPoint.
Serial Number	The device serial number.
DNS Primary Server	The IP address of the Domain Name Service (DNS) that is consulted for IP address resolution. Must be a valid IPv4 or IPv6 address.

FEATURE	DESCRIPTION
DNS Secondary Server	The IP address of the backup or secondary DNS host. Must be a valid IPv4 or IPv6 address.
DNS Domain Name	The name of the domain to use when resolving host names. This name is concatenated to form a fully qualified internet host name.
Auto Negotiation	Indicates whether auto-negotiation is enabled on the device.
Line Speed	The management port line speed.
Current Line Speed	The current management port line speed setting.
Duplex Setting	The management port duplex setting.

CAUTION!

Do not configure the device to run the HTTP or Telnet server during normal operations. HTTP and Telnet are not secure and a malicious party could intercept user names and passwords.

Note

TippingPoint recommends using the port IP address filter feature to limit access to the management port. Refer to `conf t host` in the *IPS Command Line Interface Reference* for more information. IPv6 options are disabled if IPv6 was not enabled during the initial setup. Refer to the *IPS Command Line Interface Reference* for information about enabling IPv6 on the IPS. See also *Management routing*. Making changes to the IPv4 and IPv6 addresses, Default IPv4 or IPv6 Gateway, Auto-Negotiation, Line Speed, and Duplex Setting can interrupt your LSM session.

This topic discusses the following information:

- *Reboot the IPS*
- *Configure the management port*

Reboot the IPS

Describes how to reboot the IPS.

Procedure

1. In the Navigation pane, click **System > Management Port**.
2. Click the **Reboot** button.
3. A confirmation message is displayed warning you to save all of your work prior to rebooting.
4. Perform any saves prior to the reboot.
5. Click **OK**.

Configure the management port

Describes how to configure the management port.

Making changes to the IPv4 address, IPv6 address, Default IPv4 Gateway, Default IPv6 Gateway, Auto-Negotiation, Line Speed, and Duplex Setting can interrupt your LSM session.

Procedure

1. In the Navigation pane, click **System > Management Port**.
2. Edit the management port settings as needed.
3. Click **Apply**.
4. Perform any saves prior to the reboot.
5. Click **OK**.

What to do next

Note

TippingPoint recommends using the port IP address filter feature to limit access to the management port. Refer to `conf t host` in the *IPS Command Line Interface Reference* for more information.

Note

If your IPS will communicate with devices on a different subnet, you might need to configure the management routing for this communication. You might have to define a route or gateway for SMS devices, time servers (for NTP and SNTP), email servers (for email alerts), and workstations (for remote access to the CLI or LSM). For details, see *Management routing*.

Management routing

Routing options enable communication with network subnets other than the subnet on which the management port is located. If your IPS only communicates with devices on the local network subnet, you do not need to configure a management port route, regardless of whether you are using IPv4 or IPv6.

However, if you are using IPv4 and the IPS does communicate with devices that are not on the local IPv4 subnet or accessible through the default gateway, you must define the routes to these devices. The automatic configuration option is only available for IPv6.

If IPv6 automatic configuration is enabled on the management port page (see *Management port*) and an IPv6 autoconfig router is present, IPv6 routing is handled automatically, and you do not need to define additional IPv6 routes. If automatic configuration is disabled, you must add an IPv6 route to communicate with a device that is not on the local subnet and is not accessible through the default gateway.

1. In the Navigation pane, click **System > Management Routing**.
2. On the Management Routing page, type the destination CIDR in the **Destination Network** field.
3. Type the **Gateway** IP address used by the IPS to communicate with the destination network.
4. Click **Add**.

Note

Whether or not static route entries are included in routing tables depends on several topology factors. These include network specificity, metrics, and whether the next hop IP is on the associated interface. Other routing types, redistributions, and firewall rules also impact static route entries in the routing tables.

Time options

The IPS device uses the system time in log files. To ensure log file accuracy, facilitate log analysis, and establish predictable scheduling, configure the correct time zone and timekeeping mechanism before using the device in a live environment.

Use the Time Options page (**System > Time Options**) to configure the time zone and timekeeping mechanism for the IPS device:

- **Time Zone** — IPS logs are kept in Universal Time (UTC or Greenwich Mean Time). Use this option to configure the time zone so that log times are translated into local values when displayed.
- **Clock Source** — Configures the source of timekeeping for the device. Choose from using the internal clock of the device as an independent time source, or synchronize the internal clock with user-defined Simple Network Time Protocol (SNTP) or Network Time Protocol (NTP) servers.

Configuring the time zone

Describes how to specify the time zone for the IPS.

Use the Time Zone configuration option to specify the IPS time zone. The default time zone for the IPS device is Universal Time (UTC or Greenwich Mean Time). If you change the default, the LSM logs display time data based on the specified time zone.

Note

Although the system logs are kept in Universal Time (UTC), the LSM translates UTC time values into local time values for viewing purposes.

Procedure

1. From the LSM, click **System > Time Options**.
2. In the **Time Zone** field, select the correct time zone from the drop down list.
3. If necessary, click the check box to **Automatically adjust clock for daylight saving changes**.
4. Click **Apply**.

Setting the internal clock

Describes how to set the internal clock.

Your TippingPoint IPS contains an internal CMOS clock. By setting the internal clock time, you can set the device to keep time independently.

Procedure

1. From the LSM, click **System > Time Options**.
2. Select **Internal Clock**.
3. To automatically populate the date and time settings, do one of the following:
   - Click **Set Time to Local Browser Time**.
   - Type the **Date** and **Time**.

4. Click **Apply**.

Configuring the SNTP server

Describes how to keep system time using the SNTP server.

To keep system time for your TippingPoint IPS using a Simple Network Time Protocol (SNTP) server, you must define primary and secondary SNTP Servers. SNTP servers are central servers that keep time coordinated with a central atomic clock. SNTP servers help keep network time synchronized so that network events that occur on different hosts can be compared.

Be sure that you configure all SNTP clients (both TippingPoint IPS and other network devices) to use the same SNTP servers. Using the same SNTP servers helps ensure that event times from different network entities can be meaningfully compared.

CAUTION!

Using external SNTP servers can make your IPS susceptible to a man-in-the-middle attack. It is more secure to use an SNTP server on a local, protected network.

Procedure

1. From the LSM, click **System > Time Options**.
2. Select the **SNTPServer** option.
3. Enter the IP address for a **Primary SNTP** server and a **Secondary SNTP** server.
4. Enter the **Duration** in minutes.
5. Enter the **Offset** in seconds.
6. Enter the **Port** for the server.
7. Enter the amount of seconds for a **Timeout**.
8. Enter the maximum amount of **Retries** for connecting.
9. Click **Apply**.

Configuring the NTP server

Describes how to keep system time using the NTP server.

To avoid the man-in-the-middle vulnerability of SNTP servers, users can configure an NTP server to authenticate NTP messages received from NTP servers and peers. Any attacks of the NTP infrastructure that attempt to inject false time messages must have these messages authenticated (if the **Authentication Enabled** option is selected). When authentication is enabled, all time messages are authenticated by the client before they can be accepted as a time source.

The following restriction applies to N-series devices only: Enabling NTP and then switching to SNTP causes the SNTP feature to fail. After switching from the NTP feature to SNTP or the Manual/Internal Clock, reboot the device for the change to take effect.

Procedure

1. From the LSM, click **System > Time Options**.

2. Select the **NTP Server** option.

3. Optionally set the polling period for the server to 16, 32, or 64 seconds.

   The default is 16 seconds.

4. Click the **Add Key** button to specify an ID and Key ID on a server.

   A Key ID can be a number between 1 and 65535 that corresponds to a Key ID on a server. The Authentication Key value corresponds to an authentication key on an NTP server.

5. Click the **Add Server** button.

   a. In the Server field, specify the hostname or IP address of an NTP server.

   b. If you want to enable authentication, select the **Authentication Enabled** checkbox.

   c. Associate a key ID you specified in step 4 with the server.

   d. In the Version field, specify the version of NTP for the server (1–3).

      If authentication is enabled, select version 3.

   e. If you decide to add an additional NTP server (you can add up to two), specify which is the preferred server by selecting **Preferred**.

6. Click **Apply**.

SMS/NMS

The TippingPoint Security Management System (SMS) enables you to remotely monitor and manage IPS devices and perform the following tasks:

- View, manage and edit device configuration.
- Review logs and reports.
- Configure virtual ports and security policy.
- Distribute the port and policy configuration to multiple IPS devices.

From an network management system (NMS), you can remotely *monitor* the events and system status of the IPS device. Configuring an NMS enables applications to monitor the IPS device.

When a device is under SMS management, the message `DEVICE UNDER SMS CONTROL` is displayed in red at the top of each page in the LSM and the SMS/NMS page displays the serial number and the IP address of the controlling SMS. In this state, you can view system configuration and status. However, you can only edit Authentication configuration.

This topic discusses the following information:

- *Configuring SMS information*
- *Viewing or configuring NMS information*
- *Disable/enable SMS management*

Note

Communication between the IPS device and the SMS or NMS is managed by the SNMP server, which provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). Enable the SNMP server by selecting the SNMP V2 or SNMP V3 option during the SMS/NMS configuration process. If you disable both of these options, SMS and NMS functionality is also disabled.

Configuring SMS information

Describes how to configure an SMS to manage your device.

Procedure

1. From the LSM menu, click **System > SMS/NMS**.
2. Enter an **SMS Authorized IP Address/CIDR**.

   The default value is **Any**, which means that any SMS can manage the device. To specify a range of IP addresses, enter an IP address block (`10.100.230.0/24`, for example). This allows any SMS on the specified IP subnet to manage the device.
3. Select **SNMP V2** or **SNMP V3**.
4. Click **Apply**.

   Note

   Reboot the device for the SNMP settings to take effect.

   Note

   SNMP notification contacts require SNMPv2 and do not work when SNMPv2 is disabled.

   Note

   If the SMS resides on a different IP subnet than the IPS device, you might need to configure the routing to that subnet. For details, see *Management routing*. If the IPS device has previously been managed by an SMS, the serial number, IP address, and port for SMS are displayed.

Viewing or configuring NMS information

Describes how to set NMS Trap destinations.

You can add multiple NMS Trap destinations. The IPS device sends event and activity notifications to the specified destinations. The settings enable an NMS system to submit get, get next, walk, and trap requests for SNMP V2 and SNMP V3.

Procedure

1. From the LSM menu, click **System > SMS/NMS**.
2. Select **SNMP V2** or **SNMP V3.**

   This selection determines your NMS Trap options.

3. Enter the **NMS Community String**.

   The string can be 1-31 characters long.

4. Enter the **NMS Trap information**:

   - If SNMP V2 is selected, only the IP Address and Port are required.
   - If SNMP V3 is selected, you must also enter the engine ID, username, and password, and you must select AES or DES encryption.

5. Click **Add to table below**.

6. Click **Apply**.

Note

Reboot the device for the SNMP settings to take effect.

Note

SNMP notification contacts require SNMPv2 and do not work when SNMPv2 is disabled.

Disable/enable SMS management

Describes how to set whether the device is managed by SMS.

Procedure

1. From the LSM menu, click **System > SMS/NMS**.

2. If the device is currently being managed, remove the selection from the **SMS Control: Enabled** check box.

3. If the device is not currently under management and an SMS serial number and IP address are displayed, click the **SMS Control: Enabled** check box to turn management control over to the specified SMS.

4. If the device has never been managed by an SMS (the **Enabled** check box is not available), you can start managing it by logging in to an SMS system with an authorized IP address.

   For details on configuring an authorized IP address, see *Configuring SMS information*.

High availability

IPS devices provide High Availability (HA) functionality to minimize network downtime in the event of a device failure. The High Availability feature allows you to view the current HA status and change the configuration as needed. Three types of High Availability mechanisms are available:

- Intrinsic Network HA (INHA) for individual device deployment.
- Transparent High Availability (TRHA) for devices deployed in a redundant configuration in which users can configure one device to take over for the other in the event of system failure.
- Zero-Power High Availability, which provides high availability through an external device, a Smart ZPHA module, or optional bypass I/O modules on NX-Platform devices. Some devices support the Smart ZPHA module in conjunction with the 10GbE segments. Users who have the Smart ZPHA and bypass I/O modules see two entries under Zero Power High Availability: Normal and Bypass.

The High Availability page includes the following fields.

FEATURE	DESCRIPTION
Intrinsic Network HA	• **State** — Enables you to manually change the HA state for the device. Selecting **Layer-2 Fallback** and clicking **Apply** triggers high availability. Traffic flowing through each segment on the device is either blocked or permitted based on the segment configuration. Any permitted traffic will not be inspected. Select **Normal** to return the device to normal operation. • **Current State** — Indicates the current Intrinsic Network HA state of the IPS device. In **Normal** state, the device is operating normally and inspecting traffic. In **Layer-2 Fallback** state, the device is in Layer-2 fallback mode, handling traffic on each segment based on the Layer-2 fallback action setting (permit or block) for the segment. Any traffic allowed through the device is not inspected.
Transparent HA	• **Enabled** — Enables Transparent HA. If selected, you must specify the IP address for the other IPS device configured as the HA partner. • **Partner IP Address** — Specifies the IP address of the other IPS device in the transparent HA pair. • **Partner Serial Number** — Specifies the serial number of the other IPS device in the transparent HA pair. • **Current State** — Indicates the current TRHA state. • **Communication error** — Indicates that an error occurred during communication. • **Latency** — Indicates that the IPS is experiencing delays and possible intermittent packet loss when communicating with its HA partner. • **Normal** — Indicates that the system is operating normally.
Zero Power HA	• **Normal** — Indicates that the device is operating normally. • **Bypass** — Indicates that ZPHA is enabled. • **Current State** — Indicates the current ZPHA state.

Configuring high availability from the LSM

Describes how to configure high availability from the LSM.

Procedure

1. From the LSM menu, click **System** > **High Availability**.
2. Edit your High Availability settings as needed:
   - **Intrinsic Network HA** — Select **Normal** to handle traffic normally. Select **Layer-2 Fallback** to place the device in **Layer-2 Fallback** mode.
   - **Transparent HA** — Select the check box to enable Transparent HA. You must enter the IP address and serial number of the partner device that will process traffic when the current device is unavailable.
   - **Zero-Power HA** — Select **Normal** to handle traffic normally. Select **Bypass** to bypass the device.
3. Click **Apply** to apply the changes.

Compact flash

The Compact Flash page displays the model number, serial number, revision number, and capacity of the external storage card currently inserted in the device. To mount, unmount, or change the configuration of the card, you must use the command line interface. Refer to the entries for the `compact-flash` and `conf t compact-flash` commands in the *IPS Command Line Interface Reference*.

Note

For external storage on N-Platform devices, a CompactFlash card is required. For external storage on NX-Platform devices, a CFast card is required.

Note

The `conf t compact-flash` command is not supported on the TippingPoint 10/110/330 models.

Thresholds

Use the Thresholds page to configure the thresholds for the system settings that are reported on the System Summary and Monitor pages. See *System summary* and *Health* for more information about those pages.

On the Thresholds page, you can specify the following settings:

- Disk Usage Threshold.
- Memory Usage Thresholds.
- Power Supply Monitoring: Turn on the power supply monitor feature. When this option is selected, a Power Supply Status indicator displays on the System Summary and Monitor (**Events > Health > Monitor**) pages to monitor the state of the power supplies for an IPS device.

Set disk usage and memory thresholds

Describes how to set disk and memory usage thresholds.

When setting disk and memory usage thresholds, set the major threshold to a level that provides enough time to react before the situation is critical. For example, for disk usage, set a level where the disk is getting full, but is not so full that system activity is interrupted. The major threshold default value for both disk and memory usage is 90%. Set the critical threshold at a level that warns users *before* damage is about to occur. The critical threshold default value for both disk and memory usage is 95%.

Note

TippingPoint recommends that you do not change these values from their defaults.

Procedure

1. From the LSM menu, click **System > Thresholds**.
2. On the Thresholds page, specify the disk and memory thresholds.

    a. For **Disk Usage Threshold**, enter a numeric value for the **Major Levels** and the **Critical Levels**.

    Ensure that the value for the major level value is lower than the value for the critical level.

    b. For **Memory Usage Threshold**, enter a numeric value for the **Major Levels** and the **Critical Levels**.

Ensure that the value for the major level value is lower than the value for the critical level.

3. Enable or disable power supply monitoring as required.

   This option is enabled by default.

4. Click **Apply**.

What to do next

To reset the values to the default settings, click **Reset to Defaults**.

Email server

Describes how to configure the default email settings.

Use the Email Server page to configure the default email settings that are used when a triggered IPS filter sends an email. After configuring the Email Server, configure email contact information from the Notification Contacts page (**IPS > Action Sets**, then select **Notification Contacts**). See *Notification contacts*.

Procedure

1. From the LSM menu, click **System > Email Server**.

2. On the Email Server page, type the **Default To Email Address**.

   This address displays in the **To Email Address** field when a user creates an email contact from the LSM.

3. Type the **From Email Address**.

   This address is used as the **Reply-To** address for messages sent from the IPS device.

4. Type the **From Domain Name**, such as `tippingpoint.com`.

5. Enter the **SMTP Server IP Address**.

   The IPS device must be able to reach the SMTP server that will be handling the email notifications.

6. Enter a value for the **Email Threshold (per minute)**.

   This limits the numbers of emails sent per minute. The default is 10 emails per minute.

7. Click **Apply**.

What to do next

Note

To remove the configured IP address, replace the value for the **SMTP Server IP Address** with `none`.

Email threshold

By default, the system allows 10 email alerts per minute. On the first email alert, a one-minute timer starts. The systems sends email notifications until the threshold is reached. Any notifications received after the threshold is reached are blocked. After one minute, the system resumes sending email alerts. The system generates a message in the system log whenever email notifications are blocked.

Testing email

When you are finished, you can click the **Test Email** button to test the email server configuration. The IPS attempts to send an email message using the server defined in the default email settings. If the email fails to be sent properly, check for the following possible causes:

- Email server must be reachable from the IPS.
- Email server might not allow mail relaying. Ensure that the email service accepts the account/domain.

For more information about sending emails from the IPS device, see *Create an email or SNMP notification contact*.

Syslog servers

Describes how to configure a remote syslog server for backing up log data.

To maintain and back up all log data from the IPS device, you can configure remote syslog servers for the System, Audit, and Quarantine logs. Quarantine messages are marked for the `auth` facility. You can also configure remote syslog servers for traffic-related event logging (alerts and blocks). For details, see *Configure the remote system log contact*.

Procedure

1. From the LSM menu, click **System > Syslog Servers**.
2. Select **Enable syslog offload** for each log you want to offload.
3. Type the IP address for the remote server.
4. Enable or disable RFC format for the remote syslog messages as required.
5. Enable or disable additional event information, which includes the true Client IP address, for the remote syslog messages as required.
6. Enable or disable additional event information for SNMP traps as required.
7. Click **Apply**.

What to do next

Note

Be sure that the device can reach the remote system log server on your network. If the server is on a different subnet than the IPS management port, you might need to configure the routing to that subnet (see *Management routing*).

For more information, see *Logs* and *Log formats*.

Remote servers

User authentication is usually accomplished using the local password database. TippingPoint IPS devices also support the use of remote authentication servers. Administrators can select between a Remote Authentication Dial In User Service (RADIUS) server and a Terminal Access Controller Access-Control System Plus (TACACS+) server for central authentication of users.

Up to three RADIUS or TACACS+ servers can be configured and prioritized (in the order in which they are provisioned). Attempts to configure more than three servers return an error.

When selecting a remote authentication server, consider the following:

- RADIUS authenticates over UDP, which requires it to account for transmission errors, such as packet loss. Only passwords are encrypted between a RADIUS client and server.
- TACACS+ authenticates over TCP. Because TCP is a connection-oriented protocol, TACACS+ does not require transmission control the way RADIUS does. While RADIUS encrypts only passwords, TACACS+ uses MD5 encryption on all communication and is consequently less vulnerable to attacks.

When you set up each remote server account, you must first specify the source of authentication:

- **Local Authentication only** — A hashed password for the user account is required. Authentication occurs against a user database stored locally on the IPS device. If you migrate an account from local authentication to remote authentication, the password requirement is removed.
- **SMS Remote Authentication** — The SMS handles user authentication. If you choose to use SMS as the authentication source, specify the **Time Out Interval** (in number of seconds).
- **RADIUS Remote Authentication** — The RADIUS server handles authentication. You can specify up to three RADIUS servers. User management remains on the device.
- **TACACS+ Remote Authentication** — The TACACS+ server handles authentication. You can specify up to three TACACS+ servers. User management remains on the device.

Note

RADIUS authentication is supported only on N-Platform and NX-platform devices running TOS v3.7.0 or later. TACACS+ authentication is supported only on N-Platform and NX-platform devices running TOS v3.8.0 or later. If the device does not support RADIUS or TACACS+ authentication, those options are disabled.

Authentication mechanism matrix

The following table provides considerations when deciding to use the different authentication mechanisms.

	Local Authentication	RADIUS Authentication	TACACS+ Authentication	SMS Authentication
Is the password security level setting applicable?	No	Yes	Yes	Yes
Do password expiration settings apply?	No	Yes	Yes	Yes
Will the SMS-configured failed login attempts settings apply (will the account be locked out)?	Yes	No	No	Yes
Is a local user account required?	Yes	Yes	Yes	Yes
Is the local password used?	Yes	No	No	No

	LOCAL AUTHENTICATION	RADIUS AUTHENTICATION	TACACS+ AUTHENTICATION	SMS AUTHENTICATION
What is the failover protocol?	Not applicable.	Authentication should only use the primary RADIUS server. If that destination is unreachable, the secondary server becomes the default. If that destination is unreachable, the tertiary server becomes the default.	Authentication should only use the primary TACACS+ server. If that destination is unreachable, the secondary server becomes the default. If that destination is unreachable, the tertiary server becomes the default.	Authentication should only use the primary remote server (either RADIUS or TACACS+). If that destination is unreachable, the secondary remote server becomes the default. If that destination is unreachable, the tertiary remote server becomes the default.
What is the authentication precedence if an account is flagged local?	Device(IPS/TPS/SMS)	Not applicable.	Not applicable.	SMS

Adding a RADIUS server

Describes how to add a RADIUS server.

Procedure

1. From the LSM menu, click **System > Remote Servers**.
2. Select **RADIUS Remote Authentication**.
3. Configure up to three RADIUS servers in the order in which you want the device to contact them for authentication.
4. For RADIUS Server 1, click **Edit**.
5. Provide information for the following fields:

SETTING	DESCRIPTION
IP Address	IP Address of the RADIUS server.
Port	Port on the RADIUS server that listens for authentication requests. The default port is 1812.
Secret/Confirm Secret	Case-sensitive string used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file. Maximum is 64 characters.

Setting	Description
Authentication Protocol	Authentication method used on the RADIUS server: • PAP • PEP/EAP-MSCHAPv2 **Note** To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS server. • EAP-MD5-Challenge (RFC 3748) **Note** Users interested in TLS can alternatively use PEAP/EAP-MSCHAPv2 authentication.
Certificate	Certificate to import if using PEAP/EAP-MSCHAPv2 protocol.
Timeout	Timeout, between 1 and 14 seconds, for communication with the RADIUS server. Default is 3 seconds.
Attempts	Number of times, between 1 and 5, communication with the RADIUS server is attempted. Default is 3 attempts.

6. Enter a valid User Name and Password for the server (and confirm).
7. Click **Test** to verify a successful connection to the RADIUS server. A popup message reveals one of three possible results:
   - **Timeout** — An incorrect IP address or Protocol entry caused the application to hang.
   - **Failure** — An incorrect value was entered in the fields for secret, username, or password.
   - **Success** — All fields were entered correctly and a remote connection to the RADIUS server succeeded.
8. Click **Save**.

What to do next

Note

Modifications to individual settings for each server will be prompted with a confirmation popup before the changes are committed. No individual settings can be deleted. To delete a configuration, you must delete the entire server entry. Another confirmation popup appears before the server can be removed.

Adding a TACACS+ server

Describes how to add a TACACS+ server.

Procedure

1. From the LSM menu, click **System > Remote Servers**.
2. Select **TACACS+ Remote Authentication**.

3. Configure up to three TACACS+ servers in the order in which you want the device to contact them for authentication.
4. For TACACS+ Server 1, click **Edit**.
5. Provide information for the following fields:

SETTING	DESCRIPTION
Address	Specify the remote TACACS+ server by one of the following: • IPv4 Address • IPv6 Address • hostname • hostname+domain name
Port	Port on the TACACS+ server that listens for authentication requests. The default port is 49.
Secret/Confirm Secret	Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 63 characters.
Authentication Protocol	Authentication method used on the TACACS+ server: • ASCII • PAP (default) • CHAP • MSCHAP
Timeout	Timeout, between 1 and 15 seconds, for communication with the TACACS+ server. Default is 3 seconds.
Attempts	Number of times, between 1 and 10, communication with the TACACS+ server is attempted. Default is 3 attempts.

6. Enter a valid User Name and Password for the server (and confirm).
7. Click **Test** to verify a successful connection to the TACACS+ server. A popup message reveals one of three possible results:
   - **Timeout** — An incorrect IP address or Protocol entry caused the application to hang.
   - **Failure** — An incorrect value was entered in the fields for secret, username, or password.
   - **Success** — All fields were entered correctly and a remote connection to the TACACS+ server succeeded.
8. Click **Save**.

What to do next

Note

Modifications to individual settings for each server will be prompted with a confirmation popup before the changes are committed. No individual settings can be deleted. To delete a configuration, you must delete the entire server entry. Another confirmation popup appears before the server can be removed.

Named networks

Use the Named Networks page to assign names to IPv4 and IPv6 addresses. A network name acts as an alias in the LSM for the named IPv4 or IPv6 network, and in any list where the IP address would normally appear, the network name appears instead. You can also enter the network name in any IP address field.

Note

Network names are presentation-only. Any configuration settings are associated with the IP address, and changing the network name does not change the configuration. For example, if the name of IP address `100.23.45.123` is changed from `Corporate` to `Corporate-A`, all configuration settings associated with IP address `100.23.45.123` are retained.

The Named Networks page includes the following features:

FEATURE	DESCRIPTION
Enable named networks	Enables the display of named networks in the LSM. **Note** Named networks can always be used, regardless of whether this option is selected. This option merely toggles the LSM display of IP addresses.
Always show full octet/word	Controls the display of named networks when a named network prefix does not fall on an octet boundary in IPv4 or a word boundary in IPv6. **Example:** A user assigns the name `NamedNetwork` to IPv4 address `192.168.128.0/17`. When this option is enabled, the LSM displays the address `192.168.129.1` as `NamedNetworkIPv4:129.1`. When this option is disabled, the LSM displays the address as `NamedNetworkIPv4:1.1`.
Named Network table	Displays all named networks currently configured on the device.

Adding a named network

Describes how to add a named network.

Procedure

1. From the LSM menu, click **System > Named Networks**.
2. Click **Add a new Named Network**.
3. Enter the network name and the IPv4 or IPv6 address.
4. Click **Save**.

   The new named network is added to the list.

License

The License page displays the current licensing information for the device and its associated TippingPoint services.

The Status table on the License page includes the following fields.

FEATURE	DESCRIPTION
Feature	The name of the licensed feature or service: • **LICENSE** — The default license for the TippingPoint device. • **UPDATE TOS** — The license enabling you to update the TOS on the device. • **UPDATE DV** — The license enabling you to update the latest TippingPoint Digital Vaccine filters. • **Auxiliary DV** — An optional license for additional Digital Vaccine features. • **ReputationDV** — An optional license for ReputationDV. For more information about licensing, ask your TippingPoint representative.
Status	The current license status.
Permit	Indicates whether the feature is currently enabled on the device.
Expiration	The date that the license expires.
Details	Additional information about the license.

Technical support report

Use the Technical Support Report page to arrange for the LSM to send you a status report in an email based on the email server settings you configured.

The status report is compressed into a `.tgz` file that contains the following log files and other informational `.txt` files:

- `alertlog.txt`
- `auditlog.txt`
- `blocklog.txt`
- `systemlog.txt`
- `quarantine.txt`
- `config.txt`
- `general.txt`
- `interfaces.txt`
- `memory.txt`
- `np.txt`
- `processes.txt`
- `statistics.txt`
- `fpga.txt`
- `bcmBootLog`

Select the **Include Snapshot** check box to include a system snapshot in the `.tgz` compressed file.

For more information on configuring the email server, see *Email server*.

Network

The **Network** menu pages in the LSM enable you to view and modify the setup of the IPS device so that it can work within your network environment. The following menu options are available:

- **Segments** — View and manage segment configuration for Layer-2 Fallback (high availability) and link down synchronization.
- **Network Ports** — Disable, enable, or restart a port, and manage port configuration (auto-negotiation and line speed).
- **Virtual Ports** — Create and manage virtual ports that logically classify your network by transport ports, CIDR (Classless Inter-Domain Routing) addresses, and VLAN IDs so that you can apply IPS filtering to traffic.
- **Virtual Segments** — Create and manage virtual segments to further refine the network traffic classifications.
- **VLAN Translation** — Enable translation of traffic between different VLANs or between VLAN and non-VLAN interfaces.
- **Network Tools** — Review the types of traffic that your network is receiving.

This topic discusses the following subjects:

- *Segments*
- *Network ports*
- *Virtual ports*
- *Virtual segments*
- *VLAN translation*
- *Network tools*

Segments

Use the Segments page to view segments on the IPS device and on all the I/O modules. The TippingPoint IPS enables you to protect multiple network segments. Each segment is composed of a pair of ports on the IPS device; for example, ports 1A and 1B compose one segment. These two ports integrate the IPS into the network.

From the Segments page you can access the Edit IPS Segment page for each segment, where you can complete the following tasks:

- View current high availability and link-down synchronization for each network segment
- Edit HA settings for Layer-2 fallback and link-down synchronization

Segment configuration defines how the IPS device handles traffic and port status. You can specify settings for the following options:

- **Intrinsic Network HA Layer-2 Fallback Action** determines if the device permits all traffic or blocks all packet transfers on that segment if the device goes into high availability.
- **Link-Down Synchronization** allows you to configure the IPS to force both ports down on a segment when the device detects a link state of down on one of the ports. When link-down synchronization is enabled, the IPS monitors the link state for both ports on a segment. If the link goes down on either port, both ports on the segment are disabled. This functionality propagates the link state across the IPS.

When link-down synchronization is enabled, segment monitoring begins only after link-up is detected on both ports. When link-down synchronization disables the ports on a segment, two audit log messages are generated. The first message in the audit log corresponds to the port with the link down. The second message corresponds to the segment partner. Additionally, an error message is added to the system log indicating which port was detected with the link-down, activating link-down synchronization for that segment.

Note

In addition to the physical segments on the device, you can also configure virtual segments, a software representation of ports composed of two virtual ports (incoming and outgoing) that allows you to classify and filter traffic on the network by both physical port and VLAN ID.

Segments on the NX-platform

Segments are grouped by module on the NX-Platform devices. Each module occupies a slot, which appears as a subsection of the Segments table.

The number of the slot is reflected in the segment number. For example, segment 3 in the module inserted in slot 2 would be listed as Segment 2-3. The ports that compose that segment would be ports 2-3A and 2-3B.

Edit IPS segment page

Use the Edit IPS Segment page to configure the high availability and link-down synchronization settings for each segment.

The following segment configuration parameters are available:

Column	Description
Segment	The segment name. By default the segment name corresponds to the ports on the device. For example: • N-Platform: Segment 1 comprises ports 1A and 1B. • NX-Platform: Segment 1-1 comprises ports 1-1:A and 1-1:B. You can edit the segment name to make it more meaningful. For example, if the LAN is connected to Segment 1, you can change the segment name to `LAN`.
Intrinsic Network HA	Indicates if traffic is permitted or blocked when the device goes into Layer-2 Fallback mode. For more information about high availability, see *High availability*.
Link Down Synchronization	Indicates how the IPS device manages the ports on the segment when the device detects a link-down on one of the ports. • **Hub** — The partner port is unaffected. • **Breaker** — The partner port is disabled. Both ports must be manually restarted. • **Wire** — The partner port is disabled and is automatically restarted when the original link-down is resumed.
Wait Time	When LDS is set to Breaker or Wire, this field indicates the length of time a port must be down before the partner port is also taken down. The default is 1 second. The wait time can be any value from 0 to 240 seconds.
sFlow	On NX-Platform devices only, indicates whether sFlow is enabled on the segment.
Sample rate	On NX-Platform devices only, indicates the segment's sFlow sample rate. Faster segment links support higher sample rates.

COLUMN	DESCRIPTION
Function(s)	Click edit (✏) to modify the segment.

Configure a segment

Describes how to configure a segment.

Procedure

1. From the LSM menu, click **Network > Segments**.
2. Click the name of the Segment you want to edit.
3. On the Edit IPS Segment page, enter or change the **Segment Name**.
4. Specify the Intrinsic Network High Availability (INHA) layer-2 fallback action:
   - **Block All** stops all packet transfer if the device goes into high availability.
   - **Permit All** permits all packet transfer in the event of a fallback.
5. For link-down synchronization, select an option and enter a **Wait Time** between 0–240 seconds.
   - **Hub** — Partner port is unaffected.
   - **Breaker** — Partner port is disabled, and manual restart is required.
   - **Wire** — Partner port is disabled and is automatically restarted when the original link-down is resumed.
   - **Wait Time** — When LDS is set to **Breaker** or **Wire**, the length of time a port must be down before the partner port is also taken down.
6. If sFlow sampling is enabled on the segment, specify the sample packet rate in the **Sample rate 1 out of** field.

   The default is `1000`.

   > Note
   >
   > In order to configure sFlow sampling at the segment level, you must first configure the IP address of the collector server. For more information, see *Visibility*.

   This feature is supported on TippingPoint NX-Platform devices only.
7. Click **Save**.

What to do next

> Note
>
> Segment names can only include letters, numerals, underscores (_), and spaces.

Network ports

Use the Network Ports pages to perform the following tasks:

- View a list of network I/O modules and their ports
- View and edit current port configuration
- Disable/enable Auto Negotiation
- Disable/enable ports
- Restart a port

Note

You can view the current status and port configuration from the Port Health page. See *Port health* for more information. You can configure high availability and link-down synchronization settings for port pairs, or segments, from the Segments page. See *Configure a segment* for more information.

By default, the IPS device sets all ports to auto-negotiate. With this setting, the IPS port negotiates the highest line speed supported by both the IPS port and its link partner. TippingPoint recommends configuring both the IPS ports and the link partners to auto-negotiate because it is the best, most reliable way to establish and maintain links. However, if the IPS device cannot establish or maintain a link when auto-negotiate is set, you might need to disable auto-negotiation and configure the line speed and duplex settings.

When configuring the ports, remember that both link partners must be configured with identical settings. If one port is configured to auto-negotiate, the other port must also be configured to auto-negotiate. If only one port is configured to auto-negotiate, the link might come up, but one or both partners may experience poor performance or RX errors.

The following table describes the port configuration parameters.

Column	Description
Port	The IPS port number.
Auto Negotiation	Indicates whether the port auto-negotiates line speed or uses the line speed and duplex settings as a forced port configuration. By default, Auto Negotiation is enabled. • If Auto Negotiation is enabled, the IPS device automatically negotiates the highest common speed and duplex that the IPS and the link partner both support. • If Auto Negotiation is disabled, the manually configured Line Speed and Duplex settings are used. You might want to disable auto-negotiation on some older networks if the IPS device is unable to establish or sustain the link with its partner.
Line Speed	The line speed setting for the port.
Duplex Setting	Indicates whether the port is set to full- or half-duplex.
Media	Indicates whether the port is copper or fiber.
Port Enabled	Indicates whether the port is currently enabled or disabled.
Restart	Select this check box to restart the port when you click **Apply**.

Note

When auto-negotiation is disabled, some port options might be limited. For example, 1000 Mbps line speed is only available for copper ports when auto-negotiation is enabled. When auto-negotiation is disabled, the line speed can only be set to 100 Mbps or 10 Mbps.

This topic discusses the following information:

- *Network ports on the NX-platform*
- *Edit port configuration*
- *Disable a port*
- *Restart a port*
- *Correcting port link-down errors*

Network ports on the NX-platform

Ports are grouped by module on the NX-Platform devices. Each module occupies a slot, which appears as a subsection of the Ports table. Each port is listed in the format `SegmentName`:`Port`. By default, the segment name is in the format Slot-Segment.

For example, port A on segment 3 in the module inserted in slot 2 would be listed as Segment 2-3:A. However, if Segment 2-3 was renamed, the port would be listed as `SegmentNewName`:A.

The Network Ports page also includes a Slot Configuration table at the bottom of the page.

COLUMN	DESCRIPTION
Slot	Identifies the slot number.
Status	Indicates whether a slot is empty, active, or experiencing an error.
Clear Configuration	Clears the existing configuration on the slot if the slot is empty.
Module Type	The type of module currently occupying the slot: • TippingPoint 6-Segment Gig-T module • TippingPoint 6-Segment GbE SFP module • TippingPoint 4-Segment 10GbE SFP+ module • TippingPoint 1-Segment 40GbE QSPF+ module • TippingPoint 4-Segment Gig-T Bypass Module • TippingPoint 2-Segment 1G Fiber SR Bypass Module • TippingPoint 2-Segment 1G Fiber LR Bypass Module • TippingPoint 2-Segment 10G Fiber SR Bypass Module • TippingPoint 2-Segment 10G Fiber LR Bypass Module If no module is inserted, the field is described as Empty.

Edit port configuration

Describes how to configure your port settings.

For more information about port settings, see the port configuration parameters table in *Network ports*.

After making port configuration changes, select the **Restart** option and click **Apply** to restart the port and ensure proper functioning of the device.

If you use a copper-fiber translator, disable auto-negotiation on the IPS before clicking the **Restart** button. Some translators do not support auto-negotiation. When the copper cable is pulled, these translators do not attempt to auto-negotiate with the device. The device driver attempts to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode.

Procedure

1. From the LSM menu, click **Network > Network Ports**.
2. Set the **Auto Negotiation** option for the port you want to configure.

   Deselecting **Auto Negotiation** enables configuration fields for **Line Speed** and **Duplex Setting** if the port supports custom configuration of these settings.
3. Edit **Line Speed** and **Duplex** settings as required.
4. Select the **Duplex** setting: **Full** or **Half**.
5. Check the **Restart** checkbox.
6. Click **Apply** to save the configuration and restart the port.

What to do next

Note

When auto-negotiation is disabled, some port options might be limited. For example, 1000 Mbps line speed is only available for copper ports when auto-negotiation is enabled. When auto-negotiation is disabled, the line speed can only be set to 100 Mbps or 10 Mbps. To run 10G fiber ports in 10G mode, ensure auto-negotiation is disabled (the default). When auto-negotiation is enabled for 10G ports, the speed drops to 1G. When the auto-negotiate feature is turned off, users can configure all fiber ports (SFP, SFP+, QSFP+) only to their default settings even though the hardware might list other optional values. The 12 fixed RJ-45 copper ports can be configured to either 10 Mbps or 100 Mbps using the LSM, or to 10 Mbps, 100 Mbps, or 1 Gbps using the command-line interface.

Disable a port

Describes how to diable a port.

Procedure

1. From the LSM menu, click **Network > Network Ports**.
2. On the Port Configuration page, uncheck the **Port Enabled** checkbox.
3. Click **Apply** to save the configuration and restart the port.

Restart a port

Describes how to restart a port.

If you use a copper-fiber translator (such as Netgear), turn off auto-negotiation on the IPS before clicking the **Restart** button. Netgear does not support auto-negotiation. When the copper cable is pulled, Netgear does not attempt to auto-negotiate with the device. The device driver attempts to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode.

Procedure

1. From the LSM menu, click **Network > Network Ports**.
2. Select the **Restart** option next to the port that you want to restart.

3. Click **Apply** to save the configuration and restart the port.

Correcting port link-down errors

Describes how to correct port errors in which links cannot be established.

If the IPS device has errors indicating that the ports are unable to establish link, check the connections on the device.

If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the device driver attempts to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode. In addition, Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the IPS device.

Procedure

1. From the LSM menu, click **Network > Network Ports**.
2. On the Port Configuration page, clear the **Auto Negotiation** checkbox for the port that is not working.
3. Click the **Restart** checkbox.
4. Click **Apply** to restart the port.

   With auto-negotiation disabled, the port should reset.

Virtual ports

Use the Virtual Ports page to complete the following tasks:

- View a summary of current configuration for all Virtual Ports.
- Create a Virtual Port.
- Change the name of a default virtual port.
- Edit the configuration for a custom virtual port.
- Delete a custom virtual port.

A virtual port is a logical section of the network that is associated with the following:

- One or more physical ports. By default, an IPS device is configured with virtual ports that represent each physical port pairing on the device. Examples:
  - N-Platform: virtual ports 1A and 1B correspond to ports A and B on Segment 1.
  - NX-Platform: virtual ports 2-1:A and 2-1:B correspond to ports A and B on Segment 1 in slot 2.

For more information about segment configuration, see *Segments*.

- One or more VLAN IDs. The default configuration encompasses all traffic on the port with any VLAN ID.
- CIDR (Classless Inter-Domain Routing) ranges. When a CIDR range is specified, profiles can be applied to incoming packets based on their source and destination IP addresses.

By defining virtual ports, you can further classify and filter traffic on the network and help refine the settings in security and traffic management profiles. For more information about profiles, see *Security profiles* and *Traffic management profiles*.

The following table describes the Virtual Port configuration parameters.

PARAMETER	DESCRIPTION
Show predefined virtual ports	The virtual ports that are defined by default. By default, the name is the same as the physical port number.
Name	The name used to identify the virtual port.
Description	An optional parameter to provide more detailed identification information about the virtual port.
Physical Ports	The number of the physical port assigned to the virtual port.
VLAN IDs	The VLAN ID in which the port is included. A VLAN ID of `any` spans across all physical ports.
CIDRs	The CIDRs associated with a virtual port.
Functions	Functions that you can perform on the virtual port.

This topic includes the following information:

- *Virtual port example*
- *Configuration overview: ports and segments*
- *Create a virtual port*
- *Edit a virtual port*
- *Delete a virtual port*

Virtual port example

The following figure illustrates a sample virtual port configuration on an IPS device with four ports.

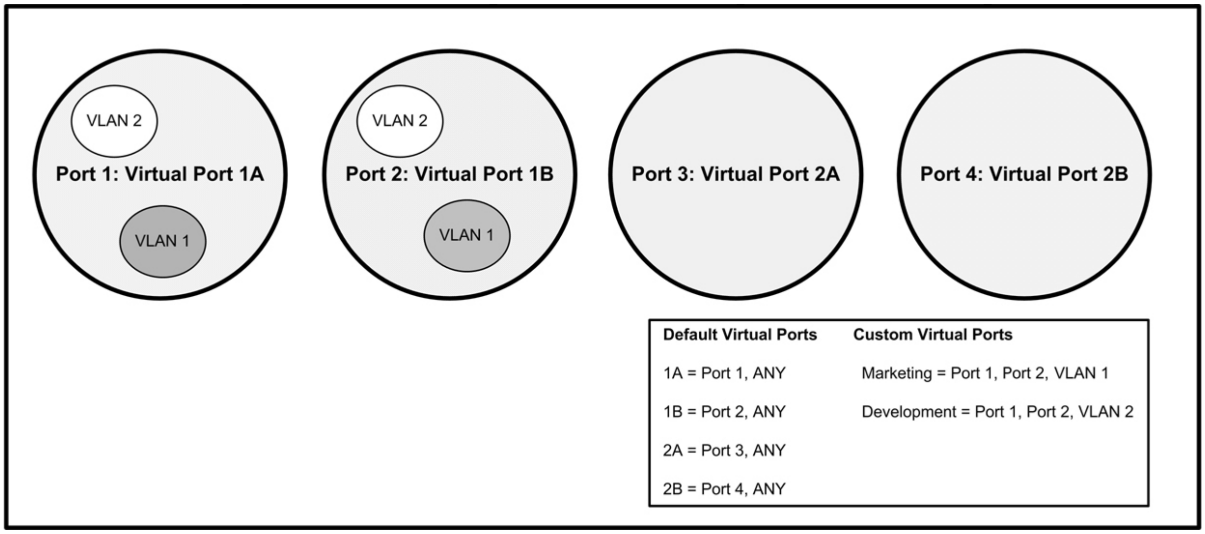


FIGURE 3. Configuring virtual ports using physical ports and VLANs

In this example, the IPS device is configured with the four default ports: 1A, 1B, 2A, and 2B and two custom virtual ports: Marketing and Development. The default ports have the VLAN ID configured as ANY, which means that traffic on any of the ports with any VLAN tag is classified the same. The custom virtual ports allow you to apply separate IPS filtering and policies to traffic with the specified VLAN tag on the specified ports.

Configuration overview: ports and segments

The IPS has a default configuration so that the device can pass traffic in most network environments after it has been installed and configured. However, you might need to customize the configuration for your network. The following list describes common configuration steps:

1. Modify default settings for high availability and link-down synchronization for physical segments.
2. Modify physical port default settings for auto-negotiation, line speed, duplex, and state (enable/disable).
3. Rename default virtual ports, or create custom ports to classify network traffic to be filtered by the IPS device.
4. After customizing virtual ports, you can configure the filters to monitor traffic on the ports from the IPS menu.

Create a virtual port

Describes how to create a virtual port.

Procedure

1. From the LSM menu, click **Network > Virtual Ports**.
2. Click **Create**.

   The Create Virtual Port page is displayed.
3. Enter the **Port Name** for the new virtual port.
4. If you choose, enter a **Description**.
5. Enter the **Network Ports** that you want to include in the definition.

   You can click the **Select** icon to open the Port Picker tool, which displays all available physical ports. To add your physical port choices to the virtual port, click **Add**.
6. If you want to include VLAN IDs in the virtual port definition, enter the VLAN IDs in the VLAN ID field. Enter multiple VLAN IDs as a comma-separated list of numbers or ranges of numbers (such as `5,7,25-33, 35`).

   The first number in a range must be less than the last number. VLAN IDs cannot be less than 1 or greater than 4094.
7. If you want to include CIDRs in the virtual port definition, enter the values in the format `xxx.xxx.xxx.xxx/xx`. IPv6 is also supported.
8. Click **Create** to create the port and save the configuration.

   Note

   With tagged ports, you can add as many physical ports/VLAN IDs to a virtual port definition as you require.

Edit a virtual port

Describes how to edit a virtual port.

Procedure

1. From the LSM menu, click **Network > Virtual Ports**.
2. Click the **Edit** icon for the virtual port that you want to edit.

   The virtual port configuration fields are displayed at the top of the table.
3. Edit the **Port Name** and **Description** as necessary.
4. Enter the **Physical Ports** that you want to include in the definition.
5. If you want to include VLAN IDs in the virtual port definition, enter the VLAN IDs in the **VLAN IDs** field.

   Enter multiple VLAN IDs as a comma-separated list of numbers or ranges of numbers (such as `5,7,25-33, 35`). The first number in a range must be less than the last number. VLAN IDs cannot be less than 1 or greater than 4094.
6. If you want to include CIDRs in the virtual port definition, enter the values in the format `xxx.xxx.xxx.xxx/xx`.

   IPv6 is also supported.
7. Click **Save** to save the configuration.

Note

With tagged ports, you can add as many physical ports/VLAN IDs to a virtual port definition as you require.

Delete a virtual port

Describes how to delete a virtual port.

Procedure

1. From the LSM menu, click **Network > Virtual Ports**.
2. In the table, locate the virtual port that you want to delete.
3. Click **Delete**.

Virtual segments

Virtual ports can also be organized into virtual segments. A virtual segment is made up of any two virtual ports that might include CIDR specifications, and can have a security profile and traffic management profile applied to it. Virtual segments enable further management of VLAN traffic.

Virtual segments are saved on the IPS in a prioritized table, and security profiles and traffic management profiles are applied in order of priority. For example, if port 1A is assigned to two different virtual segments, the profiles that are assigned to the higher-priority segment are applied to the traffic on that port before the profiles assigned to the lower-priority segment.

The following table describes the Virtual Segment configuration parameters.

PARAMETER	DESCRIPTION
Precedence	Use the icon in this column to drag and drop virtual segments into the desired precedence order. The topmost virtual segment has the highest precedence.

Parameter	Description
Incoming Virtual Port	The incoming virtual port for the virtual segment. See *Virtual ports*.
Outgoing Virtual Port	The outgoing virtual port for the virtual segment.
Security Profile	The security profile applied to the virtual segment.
Traffic Management Profile	The traffic management profile applied to the virtual segment.
Functions	Click on the icons to delete an existing virtual segment or add a new one.

Create a virtual segment

Describes how to create a virtual segment.

Procedure

1. From the LSM menu, click **Network > Virtual Segments**.
2. From the drop-down menus on the bottom line of the table, select the incoming and outgoing virtual ports.
3. Select the security profile and traffic management profile that you want to apply to the virtual segment.
4. Click **Add**.

Note

Virtual segments must be created with a physically available virtual port. When a virtual segment is created with a physically unavailable virtual port, a UDM warning is displayed in the system log.

Delete a virtual segment

Describes how to delete a virtual segment.

Procedure

1. From the LSM menu, click **Network > Virtual Segments**.
2. In the table, locate the virtual segment that you want to delete.
3. Click **Delete**.

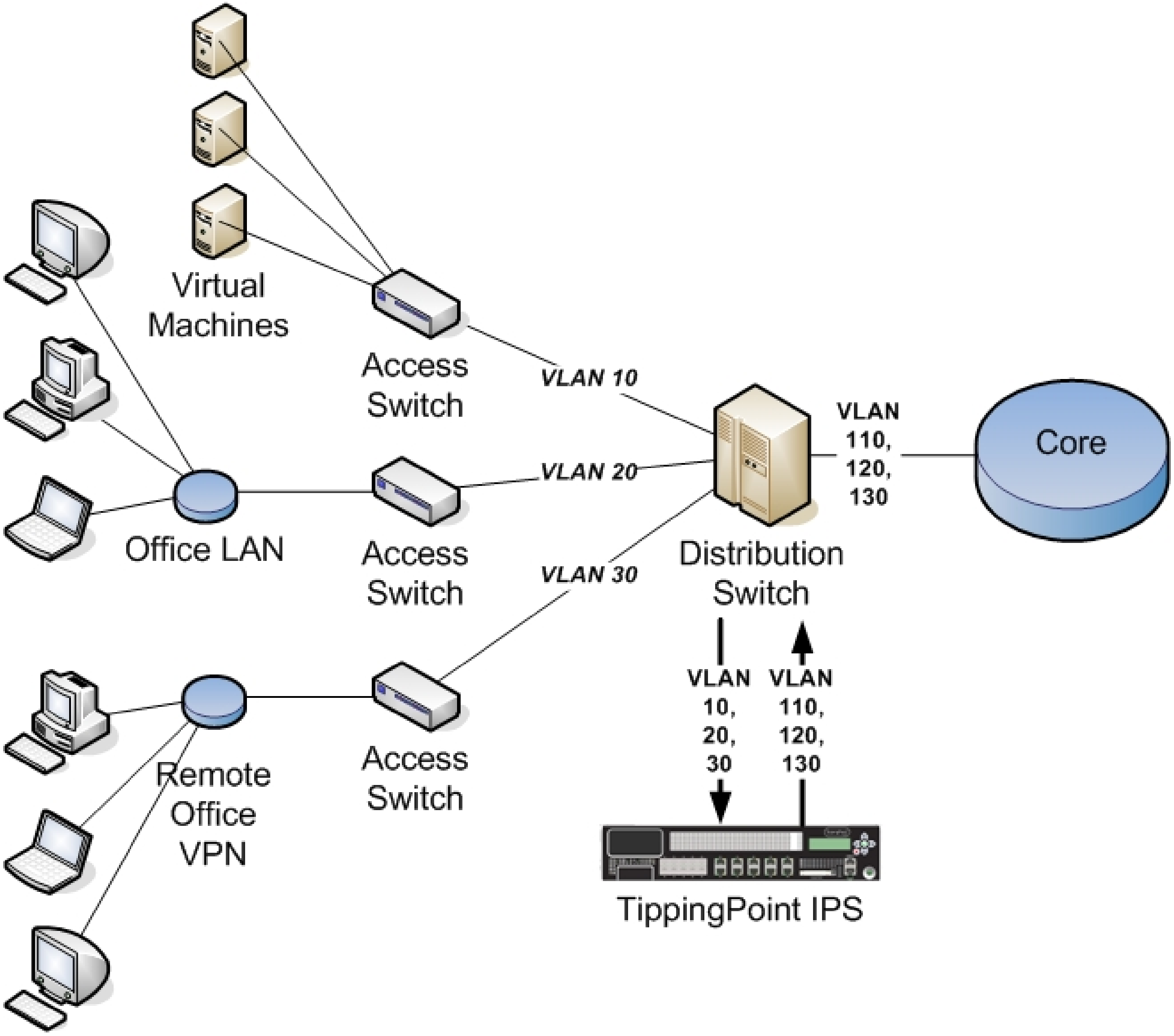
VLAN translation

With the IPS VLAN translation feature, you can deploy an IPS on an aggregation or distribution switch and selectively inspect traffic based on the switch configuration. This feature translates traffic between different VLANs or between VLAN and non-VLAN interfaces.

Note

VLAN Translation is not supported on the TippingPoint 10/110/330.

The following diagram shows a sample deployment of an IPS on a network in which three VLANs connect to a central distribution switch. The traffic is routed from the switch to the IPS, which inspects the traffic, performs the translation tasks, and routes the inspected traffic back onto the network.



You can configure the aggregation switch to send traffic to the IPS on a selective basis, focusing inspection capacity on the VLANs where the need is greatest.

Note

Security policies are applied to the incoming VLAN ID only. VLAN mappings must be unique, with one incoming VLAN paired with one outgoing VLAN. The IPS does not translate one-to-many VLAN mapping.

The following table describes the VLAN Translations configuration parameters.

Parameter	**Description**
Incoming Port	The IPS virtual port through which incoming traffic arrives.
Incoming VLAN ID	The ID of the incoming VLAN.
Outgoing VLAN ID	The ID of the outgoing VLAN.
Auto-Reverse	Select this option to enable automatic reverse VLAN translation. This option is enabled by default.

The following table describes the parameters listed in the VLAN Translations table.

Parameter	**Description**
Input Port	The IPS physical port through which incoming traffic arrives.
Input VLAN	The ID of the incoming VLAN.
Output VLAN	The ID of the outgoing VLAN.
Output Port	The IPS physical port through which outgoing traffic leaves.
Auto-Reverse	Indicates whether automatic reverse VLAN translation is enabled.
Function	Click on the icon to delete an existing VLAN translation.

Create a VLAN translation

Describes how to create a VLAN translation.

Procedure

1. From the LSM menu, click **Network > VLAN Translation**.
2. Use the drop-down menu to select the incoming port.
3. Enter the incoming and outgoing VLAN IDs. IDs must be between 1 and 4094, inclusive.
4. Configure the reverse translation option as necessary.
5. Click **Add to table below**.

Delete a VLAN translation

Describes how to delete a VLAN translation.

Procedure

1. From the LSM menu, click **Network > VLAN Translation**.
2. Click the Delete icon in the Function column.
3. When prompted, confirm the deletion of the VLAN translation.

Network tools

The Network Tools page includes the Traffic Capture feature. This feature enables you to capture a selection of traffic received by the device, including traffic that triggers filters and traffic that does not trigger any filters. You can capture up to

10,000,000 packets, 10 MB (10,000,000 bytes), or 100 files of IPv4 and IPv6 traffic. The traffic capture files are saved on the external storage card.

You can run up to five concurrent traffic captures.

The following table describes the Traffic Capture configuration parameters:

Parameter	Description
Filename	The name under which you want to save the traffic capture file. If you do not specify a name, the file is saved with a default name of the date and time at which the capture was initiated, in the format `YYYYMMDD-HHMMSS.pcap`.
Max Packets	The number of packets at which the traffic capture stops. The default is 100.
Max File Size	The capture file size at which the traffic capture stops. The size is defined in bytes. The default is 1,000,000.
Virtual Segment	The virtual segment on which you want to capture traffic. The default is all defined virtual segments.
Expression	Enables you to refine the types of packets that are captured. See *Traffic capture expressions*.

The following table describes the parameters listed in the Traffic Capture table.

Parameter	Description
Date	Date on which the traffic capture was initiated.
Time	Time at which the traffic capture was initiated.
Filename	The name of the traffic capture files.
Size	The size of the traffic capture file in bytes.
Packets	The number of packets in the traffic capture.
Function(s)	Click on the icons to download or delete a traffic capture file. If a traffic capture is currently in progress, a Stop button will be visible.

Starting a traffic capture

Describes how to start a traffic capture.

Procedure

1. From the LSM menu, click **Network > Network Tools**.
2. Specify the required parameters in the Traffic Capture Details section.
3. Enter an expression as necessary.
4. Click **Start**.

   The traffic capture start immediately, and stops when the specified thresholds are reached or when you click **Stop**. You can run up to five concurrent traffic captures.

Traffic capture expressions

Use traffic capture expressions to narrow down the types of traffic that are captured. Expressions follow the same syntax as those used in **tcpdump** and **libpcap**. You can use them to filter packets according to protocols, ports, destinations, content, or combinations of these.

For example, to capture only TCP traffic, enter the following expression in the **Expression** field:

```
tcp
```

To capture all traffic to and from IP address 172.31.255.254, enter:

```
host 172.31.255.254
```

To capture all traffic from that address, enter:

```
src 172.31.255.254
```

To capture all traffic to that address, enter:

```
dst 172.31.255.254
```

To capture all traffic from that address to IP address 10.10.10.10, enter:

```
src 172.31.255.254 and dst 10.10.10.10
```

The following, more complex example captures IPv4 HTTP packets that are transmitting to and from port 80, and includes only packets that contain data. SYN, FIN, and ACK packets are excluded.

```
tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)
```

For more information about expression syntax, refer to the **libpcap** library manual page at http://www.unix.com/man-page/FreeBSD/7/pcap-filter/.

Authentication

The LSM **Authentication** pages enable administrators to create and manage user accounts, set user account preferences, and manage X.509 certificates.

This topic includes the following subjects:

- *User list*
- *Preferences*
- *X.509 certificates*

User list

Use the User List page to view the users currently configured on the device. The User List page provides the following information about the users:

Heading	Description
Username	The user name.
Access Level	The access level granted to the user.

Heading	Description
Password Expiration	The number of days remaining before the user's password expires. This field is disabled if the user account is configured for remote authentication.
State	Indicates whether the user account is enabled or disabled.
Authentication	Indicates whether the user authenticates locally or remotely (RADIUS or TACACS+).
Function(s)	Functions that you can perform on the user account.

This topic discusses the following subjects:

- *User accounts*
- *Access level*
- *Username and password requirements*
- *Create a new user account*
- *Changing passwords*

User accounts

A **User** account provides users with access to the TippingPoint Operating System (TOS) to manage IPS devices through the LSM web interface or from the Command Line Interface (CLI). The management functions available to a user are determined by the account security level configured on the account. Accounts can only be defined in the embedded TOS user database on the IPS.

Access level

You can configure one of three access levels for each user account:

- **Operator** — Base-level administrator user who monitors the system and network traffic.
- **Administrator** — Enhanced administrator user who can view, manage, and configure functions and options in the system.
- **Super user** — Administrator user who has full access to all LSM and CLI functions.

The following table summarizes the functions available to users based on the assigned access level (Operator, Administrator, or Super-user) assigned to their user account.

Functional Area	Operator	Administrator	Super-user
IPS/Quarantine	view	all	all
Network	view	all	all
System	view	all	all
Events/Logs	view all except Audit log	view all except Audit log	all
Update	view	all	all
Configure	view	all except system time	all

Functional Area	Operator	Administrator	Super-user
Admin	• change own password • view system log	• change own password • view system log	all, including • change Idle Timeout • change Password Expiration
Help	view	view	view

Username and password requirements

Restrictions on username and password values for user accounts are determined by the Security Level preference setting configured on the Preferences page. Username and password requirements are the same for local users and TOS users. There are three possible security levels available on the IPS:

- **Level 0** — User names and passwords are unrestricted.
- **Level 1** — Names must be at least 6 characters long; passwords at least 8.
- **Level 2** — In addition to level 1 restrictions, passwords must contain:
  - at least two alpha characters
  - at least one numeric character
  - at least one non-alphanumeric character

The default security level preference is **Maximum Security Checking**.

The following table provides examples of valid usernames and passwords based on the default setting for username/ password Security Level (Maximum Security Checking):

Security Level	Valid Login Names	Valid Passwords
Level 0	fredj	mypass
Level 1	fjohnson	mypassword
Level 2	fjohnson fredj123 fredj-123 fredj-*123	my-pa55word my-b1rthday myd*g’snam3

See *User list*.

Create a new user account

Describes how to create a new user account.

Only a user with Super-user access level can create a user account. The username and password must conform to the security level on the device:

- **Level 0** — Usernames and passwords are unrestricted.
- **Level 1** — Names must be at least 6 characters long; passwords at least 8.

- **Level 2** — In addition to level 1 restrictions, passwords must contain:
  - at least two alpha characters
  - at least one numeric character
  - at least one non-alphanumeric character

Note

The TippingPoint 10/110/330 devices include an option for Administrators and Super users. Select **Enable technical support landing page** to enable the simplified LSM for this user. For more information, see *Technical support landing page*.

Procedure

1. From the LSM menu, click **Authentication > User List**.
2. Click **Create A New User**.

   The Create User screen is displayed.
3. Enter a **Username**.
4. Select the **Access Level** for the account:
   - Operator
   - Administrator
   - Super User
5. Select whether the new user authenticates locally or remotely (through a RADIUS or TACACS+ server).
6. If a remote authentication server was selected, the **Password** field is disabled. If local authentication was selected, enter a **Password**.

   Note

   When a user account changes from local to remote, this password is permanently removed from the device. If the account ever changes back to local, a new password must be selected.
7. For user accounts that use local authentication, verify the password by re-entering it in **Confirm Password** field.
8. Click **Create**.

Changing passwords

Describes how to change a password.

All TOS users who authenticate locally can change the password on their own account. Only users with super user access can change passwords on any account. The password must conform to the security level on the device:

- **Level 0** — Usernames and passwords are unrestricted.
- **Level 1** — Names must be at least 6 characters long; passwords at least 8.
- **Level 2** — In addition to level 1 restrictions, passwords must contain:
  - at least two alpha characters

- at least one numeric character
- at least one non-alphanumeric character

Note

The TippingPoint 10/110/330 devices include an option for Administrators and Super users. Select **Enable technical support landing page** to enable the simplified LSM for this user. For more information, see *Technical support landing page*.

Procedure

1. From the LSM menu, click **Authentication > User List**.
2. On the User List page, click your **Username**.
3. On the **Edit User** page, select the **Change Password** check box.
4. Enter your new **Password**.
5. Verify the password by re-entering it in **Confirm Password**.
6. Click **Save**.

Preferences

From the Preferences page on the Authentication menu, TOS users with an Administrator or Super-user security level can configure preferences to manage the security settings that affect user account access and session management.

Tip

Session time-outs and password expiration periods might be covered in your company's information security policy. Consult your security policy to be sure you configure these values appropriately.

The following table provides information on the general user security preferences parameters:

FIELD	DESCRIPTION
Web Idle Timeout	Time (in minutes) that can elapse with no user activity before the LSM logs out account access.
Page Refresh Time	The time period for the **Auto Refresh** option available on pages that have dynamic content, such as the System Summary page, Log pages, and Health page. If the option is enabled on a page, a countdown timer (starting with the value of **Page Refresh Time**) is started as soon as the page is opened. When the countdown expires, the page automatically refreshes.

The following table provides information on the TOS user security preferences parameters:

FIELD	DESCRIPTION
Security Level	Determines the length and complexity requirements for passwords. The following options are available: • **No Security Checking** (Level 0) — Usernames cannot have any spaces. Passwords are not required. • **Basic Security Checking** (Level 1) — Usernames must be 6–32 characters long; passwords must be 8–32 characters long. • **Maximum Security Checking** (Level 2) — In addition to the Level 1 requirements, passwords must contain at least one numeric character and one non-alphanumeric character (special characters such as ! ? and *). This is the default setting.
Max Login Attempts	Number of failed login attempts allowed before the system takes the action specified in the **Failed Login Action** field.
Failed Login Action	The action the system takes when the **Max Login Attempts** count has been exceeded. The following options are available: • Lockout Account. For this option, specify a **Lockout Period**. • Disable Account. • Audit Event. This option creates an entry in the Audit log documenting the failed login attempt.
Lockout Period	If **Lockout Account** is selected as the **Failed Login Action**, this value determines the duration of the lockout.
Password Expiration	(Local Authentication users only) Specifies how frequently users are required to change their passwords. TippingPoint recommends that password expiration periods should be a minimum of 30 days and maximum of 90 days.
Password Expiration Action	(Local Authentication users only) Determines which action the system takes in response to a password expiration event. The following options are available: • Force user to change the password when it expires. • Notify user of expiration. If this option is selected, the system notifies the user 5 days before the expiration occurs and at each subsequent login prompting the user to change the password before accessing the LSM. • Disable the account.

Set user preferences

Describes how to set user preferences.

If the fields on the Preferences page are read-only, your account does not have the required security access to edit the preferences. You must have an account with Administrator or Super-user access.

Procedure

1. From the LSM menu, click **Authentication > Preferences**.

   The Preferences page is displayed.

2. Change the values as necessary.

3. Click **Save**.

X.509 certificates

Use the X.509 Certificates page to add X.509 certificates. The IPS supports the following certificates:

- Certificate Authorities (CA) in PEM or DER format
- Certificate Revocation Lists (CRL) in PEM or DER format
- Multiple PEM certificates contained in a single file

The IPS uses the uploaded X.509 certificate to check incoming certificates when the user connects to the LSM.

- If the incoming certificate is not yet valid, has expired, has been revoked, or is otherwise invalid, the IPS logs an error in the system log and blocks the connection.
- If the incoming certificate is valid but has an unknown issuer, is self-signed, or includes the wrong purpose, the IPS permits the connection, but logs a warning in the system log.
- If the incoming certificate is valid and has a known issuer, the IPS completes the connection and does not record any errors in the system log.

Certificates can be obtained from or signed by a third party. You can also use self-signed certificates.

Note

Invalid certificates, including expired and revoked certificates, can still be used according to the administrator’s discretion.

This section includes the following topics:

- *Import a CA certificate*
- *Import a CRL certificate*

Import a CA certificate

Describes how to import a certificate authority (CA) certificate.

If the fields on the Preferences page are read-only, your account does not have the required security access to edit the preferences. You must have an account with Administrator or Super-user access.

Procedure

1. From the LSM menu, click **Authentication > X.509 Certificates.**
2. In the **File to Import** field, click **Browse** and select the CA certificate you want to install.
3. Click **Import**.

   The certificate is displayed in the Current Certificate Authorities table.

Import a CRL certificate

Describes how to import a certificate revocation list (CRL) certificate.

Procedure

1. From the LSM menu, click **Authentication > X.509 Certificates.**
2. In the **File to Import** field, click **Browse** and select the CRL certificate you want to install.
3. Click **Import**.

   The certificate is displayed in the Current Certificate Authorities table.

Log formats

This topic provides information on the formats of each of the downloaded logs from the Local Security Manager (LSM). This includes information on the remote syslog format and High Availability messages contained in the System Log, as well as messages received during the system update process.

You can download text-only versions of all LSM logs and view them in a browser window or save them in a file. Saved log files can be offloaded to a remote syslog server. In the System Log, the fields displayed in the LSM match the fields in the downloaded log. In the other logs, the fields displayed in the LSM are only a subset of what is available in the downloaded log file.

This section documents all fields available in the downloaded versions of these logs. These field definitions are helpful when reading the downloaded log file. They contain the description of the data so that you can format the desired fields in a reporting program such as Excel or Access, or send them to a remote syslog server.

- *Delimiters*
- *Alert, block, and quarantine log formats*
- *Audit Log Format*
- *System log format*
- *Remote syslog log format*
- *High availability log messages*
- *System update status messages*

Delimiters

When you download a log from the LSM, data is formatted using one of the following delimiters:

- **Tab-delimited** — Default field names are not displayed in the tab-delimited format.
- **Comma-delimited format (csv)** — Data is separated by commas. The first row of the log file lists the field names.

For both types of delimiters, the subfields within the Message field are always tab-delimited. If a Message subfield is not used, a tab is inserted to move onto the next subfield.

Alert, block, and quarantine log formats

Alert, block, and quarantine logs all share a similar format.

Comma-delimited block log entry

The following example shows a comma-delimited Block Log entry:

```
7,2013-02-14 14:44:07,INFO,BLK,Block,v7,2,
[dc12e035-6a2d-11e2-9209-78acc0efb007],1,
[00000001-0001-0001-0001-000000000164],icmp,0,
,95.235.120.27,0,95.235.120.231,0,1,2,0,[cc2f252a-1a57-4d00-8dc8-
a34e69992c46],ANY,[cc2f252a-1a57-4d00-8dc8-a34e69992c46],ANY,
1360853047,0733333304,1, ,pt2,40,2,2, ,Block,
[57ec4769-ca05-4dc5-8e79-a34c182adc48],Block + Notify +
Trace,0,95.235.120.27,N/A,0418
```

When opened in an application such as Excel, each comma-delimited item is displayed in an individual column.

The following table describes the fields included in the alert, block, and quarantine logs:

FIELD NAME	DESCRIPTION
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event. The format is: *YYYY-MM-DD24H:MI:SS*
Sev	Severity of the alert, from least to most severe: • INFO = for information only • WARN = warning • ERR= error • CRIT = critical
Comp	Software component that generated the message: • ALT = Alert Log • BLK = IPS Block Log
Log	Log in which the message was recorded: • Alert = for Alert Log • Block = for Block Log
Vers	Version number of the policy.
Alert_type	A bit field that identifies the type of message alert, such as traffic threshold or invalid.
Policy	ID numbers for the policy, enclosed within brackets ([]). Default policies begin with [00000002-...
Max_qual_sev	Message severity: • 1= low • 2 = minor • 3 = major • 4 = critical
Sig	The Signature UUID from the DV, enclosed within brackets ([]). Default signatures begin with [00000001-...
Prot	Protocol of the alert. For example, HTTP, IP, TCP, IDP, and ICMP.
Reserved	Not used.

FIELD NAME	DESCRIPTION
Src	Packet’s source IP address.
Src_port	Packet’s source port number.
Dest	Packet’s destination IP address. Not applicable in quarantine logs.
Dest_port	Packet’s destination port number. Not applicable in quarantine logs.
Packets_delta	The aggregated number of messages received.
MPHY	The number of the physical port number on which the packet arrived.
VLAN	The number of the VLAN on which the packet arrived.
In_sec_zone	The UUID of the security zone on which the packet arrived.
In_sec_zone_name	The name of the security zone on which the packet arrived. For example: `ANY`
Out_sec_zone	The UUID of the security zone on which the packet went out.
Out_sec_zone_name	The name of the security zone on which the packet went out. For example: `ANY`
Start_sec	Beginning timestamp of the aggregation period, in seconds.
Start_nsec	Beginning timestamp of the aggregation period, in nanoseconds.
Period	Aggregation period, in minutes. `0` = no aggregation.
Params	A string of values for special message formats used for traffic thresholds. This value is usually blank.
Trace_ver	Packet trace flag/version. • `pt0` = off • `pt2` = on Not applicable in quarantine logs.
Bucket_id	Packet trace aggregation bucket sequence number.
Trace_beg	Packet trace aggregation bucket beginning sequence number. Not applicable in quarantine logs.
Trace_end	Packet trace aggregation bucket ending sequence number. Not applicable in quarantine logs.
Reason	Used in quarantine logs to list the reason for quarantine: Manual, TRHA, or a DV.
Action	The quarantine action taken, either Added or Removed. Used only in quarantine logs.
Flow_control	The action taken by the action set: Permit, Rate Limit, or Trust.
Action_set	The rate-limit action.
Rate	A numerical value followed by a unit. The unit can be Kbps or Mbps.
Client-IP	Client IP address (Capture Additional Event Information feature must be enabled).

Field Name	Description
Metadata	Additional client information (Capture Additional Event Information feature must be enabled).
Len	Number of characters in the line. This is used for reverse parsing of the entry.

Audit Log Format

Describes the alert log fields.

Comma-delimited audit log entry

An example of a comma-delimited audit log entry follows:

```
14,2008-10-21 17:32:34,8,CLI,0.0.0.0,Host,0,0,root00,"Host name changed to ncp88"
```

The following table describes the downloadable format of the audit log:

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event. The format is: *YYYY-MM-DD 24H:MI:SS*
Access	The access-level of the user performing the action.
Type	The interface from which the user logged in. • WEB for the LSM • CLI for the Command Line Interface • SYS for the console
Address	The IP address from which the user connected to perform the action.
Cat	The area in which the use performed an action (LOGIN, LOGOUT, and Launch Bar tabs).
Result	The result of the audited action: • 0 = Pass • 1 = Fail
Flag	Not used.
User	The login name of the user performing the action. The user listed for an event can include SMS, SYS, and CLI. These entries are automatically generated when one of these application performs an action.
Message (Contained within quotes.)	The message text associated with the event. The action performed as a result. For example: "Host name changed to ncp88".

System log format

Describes the system log fields.

Comma-delimited system log entry

An example of a comma-delimited system log entry follows:

```
121,2008-10-21 17:49:33,INFO,INT,"System Initialization Complete"
```

The following table describes the downloadable format of the system log:

FIELD NAME	DESCRIPTION
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event. The format is: *YYYY-MM-DD 24H:MI:SS*

Sev	Severity of the alert, from least to most severe:
	INFO = for information only
	WARN = warning
	ERR= error
	CRIT = critical

Comp	Software component that generated the message. Examples: SYS, UDM, and HTP.
Message (Contained within quotes.)	The message text associated with the event. For a list of High Availability messages, see section *High availability log messages*.

Remote syslog log format

Describes the remote syslog format for the alert and block logs.

Packet data sent to a collector

Note

For the system and audit logs, there is no specific format for the remote syslog. For these logs, the downloaded file is sent directly to the remote syslog server as a straight data dump without any manipulation of the data.

The following is an example of packet data sent to a collector. Note that collectors might display the header portion of the stream differently. In this example, the header follows the standard syslog format.

```
        <36>2015-05-20T21:27:07-05:00 drg1202 ALT,v7,
20150520T212707+0000,drg1202/10.99.13.152,2,1,Permit,Low,
545bb935-ff2e-11e4-9236-78acc0f29b78,
"1591: Tunneling: HTTPort Data transfer",
"1591: Tunneling: HTTPort Data transfer",tcp," ",
64.83.28.78,20480,216.136.107.233,1168,20150520T212707+0000,1," ",0,
ANY-ANY,3f0f3fe0-ff2e-11e4-9236-78acc0f29b78,Remote,0,216.136.107.136,
xff:ipv4:216.136.107.136
```

Using the previous log entry as the example, the message is as follows:

```
        ALT,v7,20150520T212707+0000,
drg1202/10.99.13.152,2,1,Permit,Low,
545bb935-ff2e-11e4-9236-78acc0f29b78,
"1591: Tunneling: HTTPort Data transfer",
"1591: Tunneling: HTTPort Data transfer",tcp,,
64.83.28.78,20480,216.136.107.233,1168,20150520T212707+0000,1," ",0,
ANY-ANY,3f0f3fe0-ff2e-11e4-9236-78acc0f29b78,Remote,0,216.136.107.136,
xff:ipv4:216.136.107.136
```

The character located between each field is the configured delimiter. In this case, the delimiter is a comma. The following table details the fields and their descriptions:

FIELD	DESCRIPTION
1	Log type: • `ALT`: alert • `BLK`: block • `QRN`: quarantine
2	Version of this message format.
3	ISO 8601 Date-Time-TZ when this alert was generated.
4	Hostname/IP address that generated the alert. The hostname is enclosed in quotes if the name contains non-alphanumeric characters, such as spaces.
5	Sequence ID.
6	(reserved)
7	Action performed (`Block` or `Permit`).
8	Severity (`Low`, `Minor`, `Major`, or `Critical`).
9	Policy UUID.
10	Policy Name.
11	Signature Name.
12	Protocol name (`icmp`, `udp`, `tcp`, or `unknown`).
13	(reserved)
14	Source address.
15	Source port.
16	Destination address.
17	Destination port.
18	ISO 8601 Date-Time-TZ when the aggregation period started.
19	Number of events since start of aggregation period.
20	Traffic Threshold message parameters.
21	Traffic capture available on device. If a packet trace is captured, three numbers separated by periods indicate the capture. If there was no packet trace, a `0` is indicated.
22	Slot and segment of event.
23	Action set UUID.

FIELD	DESCRIPTION
24	Action set name.
25	Action set rate limit.
26	Client IP address (Capture Additional Event Information feature must be enabled).
27	Additional client information (Capture Additional Event Information feature must be enabled).

Remote syslog RFC format

The default remote syslog message format for the system and audit logs is backward-compatible with earlier IPS releases, but is not consistent with RFC 3164. RFC format can be enabled for these logs so that the remote syslog messages meet RFC requirements. This setting has no effect on the format of alert and block log remote syslog messages. When RFC format is enabled, the message format differs as follows:

- The year is not included in the message header.
- The extra space before the hostname is removed.
- The header tag that contains the type of log is formatted as `type:` instead of `[type]`.

For example, in the default format, an audit log message would read as follows:

```
<6>NOV 19
          16:58:07 2010 hostname [audit] user=[username] src=1.2.3.4 iface=3 access=8
          Logged out by user
```

The same message in RFC format would read as follows:

```
<6>Nov 19
          17:01:15 hostname audit:user=[username] src=1.2.3.4 iface=3 access=8
          Logged out by user
```

For information about enabling RFC format, see *Syslog servers*.

High availability log messages

The High Availability mechanism records messages to the system log.

The High Availability mechanism records the following messages to the system log. For details on the system log, see *System log format*.

MESSAGE	TYPE	DESCRIPTION
`Layer 2 Fallback (Intrinsic HA) cause: failed manually`	Critical	User has manually placed the IPS device into HA from the LSM (**System > HA**) or the CLI.
`Layer 2 Fallback (Intrinsic HA) cause: none (cleared manually)`	Informational	User has manually taken the IPS device out of HA via the LSM or the CLI.

Message	Type	Description
Layer 2 Fallback (Intrinsic HA) cause: • suspended task • memory issue • hardware breakpoint • TSE failure • Software watchdog timeout • watchdog timeout • Threshold Failure • OAM Fault Recovery	Critical	When the IPS device goes into HA because of an internal system failure, an error message indicates the cause of the failure. Use this information when you contact TippingPoint Technical Support for assistance.

System update status messages

Describes how the LSM provides status on the progress of an update.

The LSM provides update status on the progress of the update. The messages include "<Update State>:<qualifier>". The <Update State> indicates the state of the update. The <qualifier> provides information about the state.

The following table details the messages that display on the LCD screen during an update of the TOS:

Update State	Description
Ready	Device is ready for an update.
Updating	Device is in the process of updating.
UpdateCommitting	Device has rebooted and is processing the final update steps.
UpdateFailure	Device failed update. The screen displays the reason.
Rollback	Device is in the process of rollback.
RollbackCommitting	Device has rebooted and is processing the final rollback steps.
RollbackFailure	Device failed rollback. The screen displays the reason.
Failsafe	Device was unable to load a valid image and is running a scaled-back image.

If an error occurs, the information changes. The state displays as "UpdateFailure:<state>." where <state> is one of the listed states in the preceding table. The listed state displays a qualifier and message regarding the state.

The following table details the qualifier and messages:

Update Failure Qualifier	Message
OK	Normal operation, no errors.
InvalidUpdateState	Current action is restricted while device is in this state. Fix problem and reset Update State.

UPDATE FAILURE QUALIFIER	MESSAGE
InvalidLocation	Package file not found at that location.
RebootDuringUpdate	Device was rebooted during update. Check system log for recommendations.
TarChecksumError	Checksum error when extracting the archive: Corrupted package.
TarExractError	File system error when extracting the archive.
ArchiveCreateFailure	File system error creating rollback archive.
SystemError	General error during update.
WrongPlatformType	Package is for a different platform. Make sure you have correct TippingPoint supplied IPS package.
PackageReadError	General error while reading package. Possible truncated or corrupted package; download new package from TMC and retry update.
WrongPackageType	Package is of unknown type, not an OS or DV package. Make sure you have correct TippingPoint supplied IPS package.
NotEnoughFreeSpace	Not enough available disk space. Remove older installed images.
UnsignedPackage	Package does not have proper TippingPoint digital signature.
MemoryError	Memory error when installing package. Reboot may be necessary.
BadCertificate	Package does not have proper TippingPoint digital certificate.
DowngradeRevisionNotSupported	Using update to install some older versions is not supported.
PackageOpenError	Unable to open package. Make sure you have a correct TippingPoint-supplied IPS package.
CannotUpdateDVWhenTSEIsBusy	Unable to update Threat Suppression Engine packages while the system is busy reloading filters. Retry operation at a later time.