



TippingPoint™

Intrusion Prevention System (IPS)

Command Line Interface Reference

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

© Copyright 2020 Trend Micro Incorporated. All rights reserved.

Trend Micro, the Trend Micro t-ball logo, TippingPoint, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Publication: July 2020

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:

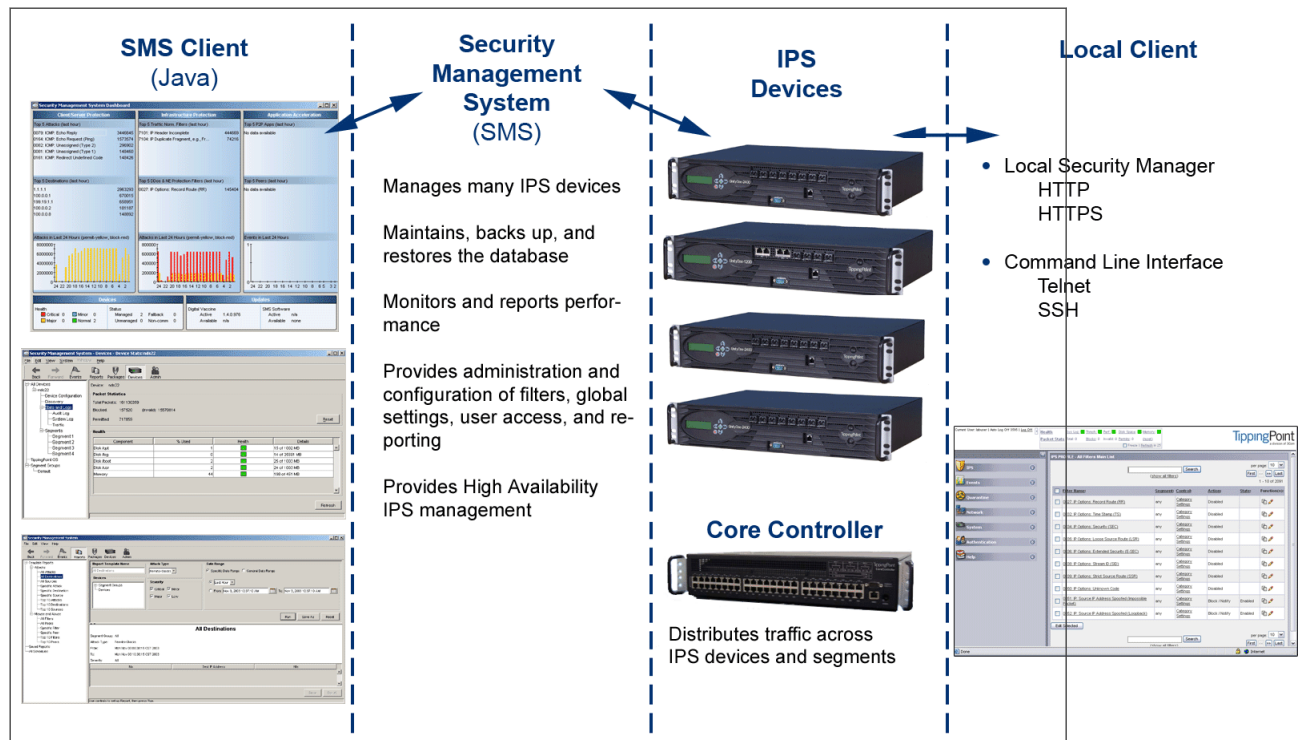


FIGURE 1. TippingPoint architecture

Security Management System (SMS)

Describes the core components of the 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 TNHA, multiple IPS devices are synchronized so that when one device experiences a system failure, traffic is 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.

TSE features include:

- 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.

Initial configuration

Describes the procedures for initial TippingPoint IPS configuration.

The TippingPoint IPS Out of Box Experience (OBE) setup wizard provides a convenient method for entering configuration data when installing, moving, or reconfiguring a TippingPoint IPS device. The wizard runs automatically on the console that is connected to the device via the console port or on the LCD keypad. You can also initialize the setup wizard at any time by entering the **setup** command in the CLI.

This topic is a guide for the CLI and LCD keypad versions of the OBE wizards and includes the following information:

- [CLI setup](#)
- [Additional configuration](#)

CLI setup

Describes how to get started using the command line interface.

Before you begin, ensure that a console is connected to the TippingPoint IPS device via the console port, and that the console is powered on and ready. When you turn on the IPS, you will see several status messages before the OBE setup wizard initializes.

When the OBE setup wizard runs, the following screen appears:

```
Welcome to the TippingPoint Technologies Initial Setup wizard.
```

```
Press any key to begin the Initial Setup Wizard or use LCD panel.
```

Press any key to begin the OBE setup wizard. The following message appears:

```
You will be presented with some questions along with default values in brackets[]. Please update any empty fields or modify them to match your requirements. You may press the ENTER key to keep the current default value. After each group of entries, you will have a chance to confirm your settings, so don't worry if you make a mistake.
```

Continue to the following section for instructions on account security.

Account security level

The Security Level dialog sets the security level that restricts user names and passwords.

The default security level is Level 2, but you have the option to select one of three available levels:

```
There are three security levels for specifying user names and passwords:
```

```
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 2 alpha characters
- at least 1 numeric character
- at least 1 non-alphanumeric character

Please specify a security level to be used for initial super-user name and password creation. As super-user, you can modify the security level later on via Command Line Interface (CLI) or Local Security Manager (LSM).

Security level [2]:



Note

For maximum security, TippingPoint recommends setting the account security level to 2.

Super-user data

The Super-User Data dialog sets the super-user login name and password.

The login name and password cannot contain spaces and must meet the restrictions of the security level that you set in the Security Level dialog. The following tables list examples of valid login names and passwords.

SECURITY LEVEL	VALID LOGIN NAMES	VALID PASSWORDS
Level 0	fredj	<i>mypass</i>
Level 1	fjohnson	<i>mypassword</i>
Level 2	fjohnson fredj123 fredj-123 fredj-*123	<i>my-pa55word</i> <i>my-b1rthday</i> <i>myd*g'snam3</i>

In this example, the password is presented in italics. In the actual dialog, the password would not be visible.

Please enter a user name that we will use to create your super-user account. Spaces are not allowed.

Name: superuser

Do you wish to accept [superuser] <Y,[N]>:Y

Please enter your super-user account password: root--00

Verify password: root--00

Saving information...Done

```
Your super-user account has been created.
```

```
You may continue initial configuration by logging into your device.
```

```
After logging in, you will be asked for additional information.
```

After logging in at the prompt, you can continue with the OBE setup wizard.

Host management port options

The Host Management port is the Ethernet port located on the host processor module.

Use the IP address of the Host Management port to connect to the TippingPoint IPS when you use the Command Line Interface and the LSM.

In this example, the host IP address is 10.252.0.71, the host name is device71, and the location is Lab. The network mask is the default setting.

```
The host management port is used to configure and monitor this device via a network connection (e.g., a web browser).
```

```
Enter Management IPv4 Address [none]: 10.252.0.71
```

```
Enter Network IPv4 Mask [255.255.255.0]:
```

```
Enable IPv6 [No]: y
```

```
Enable IPv6 Address Autoconfig [No]: y
```

```
Enter Host Name [myhostname]: device71
```

```
Enter Host Location [room/rack]: Lab
```

```
Host IPv4: 10.252.0.71/24
```

```
IPv6 Enabled: Yes
```

```
Host Link-Local IPv6: fe80::207:99ff:fe66:6999/64
```

```
Host IPv6: Auto
```

```
Host Name: device71
```

```
Host Location: Lab
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

Management IPv4 address

The Host IP address is the IP address through which you access the TippingPoint IPS.

The Host IP address must meet the following criteria:

- Must be standard IPv4 address format.

- Must be contained within the local network, but must *not* be contained within any subnets that pass traffic through the Multi-Zone Defense Module. If you assign the management port an IP address that is within a subnet connected through the Multi-Zone Defense Module interface card, the interfaces will not perform reliably.
- Must be accessible from the workstation from which you will manage the device.

Network IPv4 Mask

The network mask for the subnet on which the TippingPoint IPS is located.

Enable IPv6/Enable IPv6 address autoconfig

Select **Y** for both of these options to enable IPv6 on the device and to automatically configure the IPv6 address.

Host name

The host name of the TippingPoint IPS. Use the name that the IPS will be known as on your network.

Host location

The host location is the physical location of the TippingPoint IPS. It is for informational purposes only.

Default gateway options

The Default Gateway options configure the routing information that the TippingPoint IPS needs to communicate with other networks.



Note

If the TippingPoint IPS Host Management Port and the workstation from which you will manage the IPS are on different subnets, you must define a default gateway or an additional route to enable network-based management of your IPS. See [Management port routing options](#).

In this example, the default gateway address is 10.252.0.254.

```
The default gateway is a router that enables this device to communicate with other
devices on the management network outside of the local subnet.
```

```
Do you require a default gateway? <Y, [N]>: y
```

```
Enter IPv4 Gateway Address (a value of 0.0.0.0 removes the default gateway)
[0.0.0.0]: 10.252.0.254
```

```
IPv4 Gateway Address: 10.252.0.254
```

```
IPv6 Gateway Address: Auto
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: A
```

Default gateway

The default gateway is the IP address through which communications with other subnets are routed.

If the TippingPoint IPS sends a message to an IP address outside of its subnet, the message and the reply go through the default gateway.

You can specify both an IPv4 and an IPv6 address.



Tip

Using additional routes instead of a default gateway helps assure that your Management Port only communicates with explicitly authorized network segments. See *Management port routing options*.

DNS configuration

The DNS configuration options define the DNS servers that the TippingPoint IPS will use to resolve host names.

```
The DNS server resolves hostnames to IP addresses.
```

```
Would you like to configure a DNS server? <Y,[N]>:y
```

```
Enter the Primary DNS server IP Address: [none]: 152.67.140.3
```

```
Would you like to configure a secondary DNS server (currently not configured)?  
<Y,[N]>:
```

```
Enter the DNS Domain Name []: tippingpoint.com
```

```
DNS Primary Server: 152.67.140.3
```

```
DNS SecondaryServer:
```

```
Domain Name: tippingpoint.com
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

Timekeeping options

The TippingPoint IPS can keep time using its internal CMOS clock or it can use an Internet Simple Network Time Protocol (SNTP) server.

If you decide to use SNTP for timekeeping, the TippingPoint IPS comes with the following SNTP servers defined as the default primary and secondary SNTP servers:

- National Institute of Standards and Technology (192.43.244.18)
- US Naval Observatory (192.5.41.40)



Note

If you use the CLI `show sntp` command, the TippingPoint IPS displays the current settings for Primary Addr and Secondary Addr. If SNTP timekeeping is turned off (`conf t no sntp`), the last SNTP servers defined (or default if never defined) are shown.



CAUTION!

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

The Timekeeping Options dialog follows:

```
Timekeeping options allow you to set the time zone, enable or disable daylight
saving time, and configure or disable SNTP.
```

```
Would you like to modify timekeeping options? <Y,[N]>: y
```

```
Enter time zone or '?' for complete list [GMT]: CST
```

```
Automatically adjust clock for daylight saving changes? [Yes]: Y
```

```
Do you want to enable the SNTP client? [No]: Y
```

```
Enter Primary SNTP Server address [192.43.244.18]:
```

```
Enter Secondary SNTP Server address [192.5.41.40]:
```

```
TimeZone: CST
```

```
DST enabled: Yes
```

```
SNTP enabled: Yes
```

```
SNTP Primary Server: 192.43.244.18
```

```
SNTP Secondary Server: 192.5.41.40
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
```

Time zone

Sets the local time zone on the device. System logs are kept in Universal Time (UTC), but the TippingPoint IPS calculates local time for display purposes.

Daylight Saving Time

Enables or disables the option to calculate time based on the time of year.

For configuring Daylight Saving Time for your specific region, refer to [conf t clock](#).

Primary time server

The IP address of the SNTP server that your TippingPoint IPS uses to keep time.

Secondary time server

The IP address of the SNTP server that your TippingPoint IPS uses to keep time if the primary server is unavailable.

After the setup wizard

After you have completed the initial setup wizard, if you have changed from the HTTPS or SNMP server settings, you must reboot.

Use the **reboot** command in the CLI. After the IPS reboots, you can use the Local Security Manager GUI to perform monitoring and configuration tasks or use the **setup** command in the CLI to perform additional configuration tasks. See [Additional configuration](#).

Additional configuration

Provides links to topics that describe various configuration tasks.

After you have completed the initial setup wizard through the Command Line Interface or on the LCD screen, you can further configure your TippingPoint IPS. These subsequent setup options include the following:

- [Web, CLI, and SNMP server options](#)
- [Restricted SMS access](#)
- [Ethernet port settings](#)
- [Management port routing options](#)
- [Default alert information](#)

Web, CLI, and SNMP server options

The Web, CLI, and SNMP Server Options dialog enables and disables TippingPoint IPS servers.

Always use the secure Web and CLI servers (HTTPS and SSH) when conducting normal operations. Use the non-secure servers (HTTP and telnet) only for troubleshooting if the secure servers are unusable.



Note

You do not need to run any servers if you want to control your TippingPoint IPS through the serial port only. However, you cannot manage filters or perform network discovery scans without servers. You can turn off all servers by using the **conf t server** commands. For changes to HTTP or HTTPS to take effect, reboot the device.

```
Server options allow you to enable or disable each of the following servers: SSH,
Telnet, HTTPS, HTTP, and SNMP.
```

```
Would you like to modify the server options? <Y, [N]>: y
```

```
Enable the SSH server? [Yes]:y
```

```
Enable the Telnet server? [No]:n
```

```
Enable the HTTPS server ('No' disables SMS access)? [Yes]:y
```

```
Enable the HTTP server? [No]:n
```

```
Enable the SNMP agent ('No' disables SMS and NMS access)? [Yes]:y
```

```
SSH: Yes
```

```
Telnet: No
```

```
HTTPS: Yes
```

```
HTTP: No
```

```
SNMP: Yes
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: e
```

SSH server

Enables encrypted terminal communications.

The SSH server must be enabled to establish a secure CLI session over your network. This option is enabled by default.

When you establish an SSH session to the IPS security device by using OpenSSH version 7.2 (and later), the SSH client displays the following error:

```
Connection to ip_address port 22: DH GEX group out of range
```

By default, newer versions of OpenSSH no longer connect to the IPS security device because of an increase in the minimum number of bits that are required for the key exchange.

To avoid this issue, update the key exchange algorithms on the SSH client computer to allow `diffie-hellman-group1-sha1` for compatibility with the IPS security device. For example, run the following command:

```
ssh -o KexAlgorithms=diffie-hellman-group1-sha1 <device_ip_address>
```

Telnet Server

Enables telnet connections to the IPS.

The telnet server can be enabled to run non-secure CLI sessions over your network. This option is disabled by default.



CAUTION!

Telnet is not a secure service. If you enable telnet, you endanger the security of your TippingPoint device. Use SSH instead of telnet when you are conducting normal operations.

HTTPS server

Enables secure web access and encrypted file transfers over the network.

The HTTPS server must be enabled to use SMS management. You can also run the LSM using the HTTPS server. This option is enabled by default.

HTTP server

Enables non-secure web access.

You can enable the HTTP server to run non-secure LSM session on your network. This option is disabled by default.



CAUTION!

HTTP is not a secure service. If you enable HTTP, you endanger the security of your TippingPoint device. Use HTTPS instead of HTTP for normal operations.

SNMP server

The SNMP Server provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP).

The SNMP server must be enabled to use SMS management or to allow NMS access. This option is enabled by default.

Restricted SMS access

The Restricted SMS Access dialog enables you to guard against unauthorized management of the device by a Security Management System (SMS).

Using this option, the device accepts management only from an SMS at a specified IP address. When you execute the **setup sms** command, you are prompted to enter the IP address or CIDR of the SMS device that you want to manage the device. The system displays this address as an Allowed SMS, and you are then prompted to save your changes.

```
Enter Security Management System IP Address or CIDR [none]: 123.45.67.890
```

```
Allowed SMS: 123.45.67.890
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
```

Ethernet port settings

The Ethernet Port settings dialog enable and disable ports, and also set port speed, duplex, and negotiation settings.

You can only access the Ethernet Port Setup by using the **setup ethernet-port** command in the CLI.



Tip

You can configure Ethernet ports individually using the **conf t interface ethernet** command.



CAUTION!

When you configure an Ethernet port using the command line interface, the port will be shut down. Use the **conf t int ethernet <segment> <port> no shutdown** command to restart the port.

The Ethernet Port Options dialog configures individual port values for the IPS Ethernet interfaces.

```
Would you like to modify the Ethernet ports <Y,[N]>:y
```

```
We will now configure your Ethernet ports.
```

```
Configure port 1A (Ethernet Port)? <Y,[N]>:y
```

```
This port is currently enabled, would you like to disable it? <Y,[N]>:n
```

```
Please enter values for the following options
```

```
Line speed [1000]:
```

```
Duplex setting [Full]:
```

```
Auto negotiation [On]:
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

```
Configure Port 2 (Ethernet Port)? <Y,[N]>:
```

Line speed

The line speed setting for a port.

You can set a port to 10, 100, or 1000 Kbps.

Duplex setting

The duplex setting for the port. Copper can be set to **full** or **half**. Fiber ports can be set to **full**.

Auto negotiation

The auto negotiation setting determines whether the port negotiates its speed based on the connection it can make.

Management port routing options

The Management Port Routing options dialog configures management port routes.

You can access the Management Port Routing options only by using the **setup host** command in the CLI.

These options enable the TippingPoint IPS device to be managed from a different network than the one to which the management port is connected. You can define up to 12 routes that your Management Port can use to communicate with other subnets.



CAUTION!

Define additional routes with care. The broader the definition of additional routes you use, the greater the chance that an unauthorized user can reach your IPS.

```
Would you like to modify management port routes? <Y, [N]>:y
```

```
Currently, the additional routes are as follows:
```

#	Destination	Gateway
1	any4	10.252.0.254
2	none	none
3	none	none
4	none	none
5	none	none
6	none	none
7	none	none
8	none	none
9	none	none
10	none	none
11	none	none
12	none	none

```
Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]: c
```

The new route is added to the list. The following example shows an example of a routing table that has had both IPv4 and IPv6 addresses added to it:

Currently, the additional routes are as follows:

#	Destination	Gateway
1	any4	10.252.0.254
2	1.2.3.0/24	10.252.0.123
3	fc01:afc::102:300/120	fe80::205:9bff:fe86:1234
4	none	none
5	none	none
6	none	none
7	none	none
8	none	none
9	none	none
10	none	none
11	none	none
12	none	none



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.

Destination network

The IP network address of the subnet with which you want the IPS to communicate.

Gateway

The IP address on the IPS subnet that can communicate with the destination network.

Default alert information

The Default Alert options dialog defines the default sender and recipient for filter alert emails.

You can only access the Default Alert options by using the **setup email-default** command in the CLI.

```
Enter TO: email address (128 max. characters)
```

```
Must be a full email address (e.g., recipient@company.com) []:
employee@company.com
```

```
Enter FROM: email address (128 max. characters)
```

```
Must be a full email address (e.g., sender@company.com) []: tpt3@company.com
```

```
Enter FROM: Domain Name (128 max. characters, e.g., company.com) []: company.com
```

```
Enter email server IP address []: 1.2.3.4
```

```
Enter period (in minutes) that email should be sent (1 - 10080) [1]: 5
```

```
To: employee@company.com
```

```
From: tpt3@company.com
```

```
Domain: company.com
```

```
Email Server: 1.2.3.4
```

```
Period (minutes): 5
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

TO email address

The email address to which alert notifications will be sent.

The address must be:

- less than 129 characters long
- a valid email address. For example: johndoe@mycompany.com

FROM email address

The address that alert notifications will contain in the from field.

The address must be:

- less than 129 characters long
- a valid email account name on the SMTP server
- a valid email address on the SMTP server

Domain

The domain name of the SMTP server.

Email server IP address

The address where the SMTP server is located.

The address must be a valid IP address for an SMTP server.

Period

The aggregation period for email alerts.

The first time a filter that calls for email notification is triggered, the system sends an email notification to the target named in the filter. At the same time, the aggregation timer starts. The TippingPoint device counts additional filter triggers, but does not email another notification until it sends a count of all filter triggers that occurred during that period. The timer continues to count and send notifications at the end of each period. The period must be an integer between 1 and 10,080 representing minutes between notifications.

Navigation

Provides links to topics that describe commands for navigating the CLI.

The Command Line Interface (CLI) is a standard embedded system command line interface that provides access to hardware and embedded software configuration. This topic describes logging in and issuing commands with the CLI.

- [Log in to the CLI](#)
- [Navigation](#)
- [Session settings](#)

Log in to the CLI

Log in to the CLI to run TippingPoint IPS commands.

To access the CLI, connect to your device by using one of the following methods:

- Establish an SSH session to your device. To establish an SSH session, you need:
 - An SSH client
 - The management IP address of the device

When you establish an SSH session to the IPS security device by using OpenSSH version 7.2 (and later), the SSH client displays the following error:

```
Connection to ip_address port 22: DH GEX group out of range
```

By default, newer versions of OpenSSH no longer connect to the IPS security device because of an increase in the minimum number of bits that are required for the key exchange.

To avoid this issue, update the key exchange algorithms on the SSH client computer to allow `diffie-hellman-group1-sha1` for compatibility with the IPS security device. For example, run the following command:

```
ssh -o KexAlgorithms=diffie-hellman-group1-sha1 <device_ip_address>
```

- Connect to your device directly through the console terminal.

Contact your TippingPoint administrator to request login credentials if needed.

To log in to the CLI

Procedure

1. Connect to your device through SSH or the console terminal.

2. Enter your username at the **Login** prompt.
 3. Enter your password at the **Password** prompt.
-

Navigation

Provides links to topics with information about the different command types and features.

The TippingPoint Command Line Interface offers the following features:

- [Command types](#)
- [Use hierarchical commands](#)
- [Command hints](#)
- [Command completion](#)

Command types

Identifies the two types of CLI commands.

The CLI has two types of commands.

- **Global commands:** Available from within any menu level in the CLI. Global commands do not report on or change configuration items. These commands are listed by the command **help commands**.
- **Hierarchical commands:** Configure, manage, and display TippingPoint IPS configuration. Some IPS commands are hierarchical and are available only within a menu or submenu.

Use hierarchical commands

The CLI divides the hierarchical commands into functional areas.

There are several commands that lead to submenus, including **configure terminal** and **show**.

Context sensitive prompt

The CLI prompt helps indicate what menu level you are currently using.

The top-level menu prompt is:

```
hostname#
```

When you enter a submenu, the prompt changes to indicate the current menu level. For example, changing to the **show** submenu will change the CLI prompt from:

```
hostname# show
```

to

```
hostname (show) #
```

Exit submenus

The **exit** command steps back to the previous menu, or up one submenu.

The **exit all** command returns you to the **hostname#** menu level.

Special characters

The CLI treats # and ? as special characters. Typically, the CLI uses the # character as a comment delimiter and the ? character as a tool for bringing up help. So whenever these two characters occur as part of a string, you must enclose the string in double quotation marks to denote that the characters are included as part of a literal string. For example:

```
conf t user add operuser3 -password "test##99" -role operator
```

Otherwise, the CLI will not process the characters correctly.

Command hints

On each command level, you can view the hierarchical commands available at that level by typing a question mark (?).

Command completion

The CLI attempts to match partially typed commands with valid commands.

For example, if you type:

```
reb?
```

The CLI interprets this command as if you typed the following:

```
reboot
```

You can also use the Tab key for command completion.

Commands to edit command line entries

Lists commands used for editing command line entries.

The following commands can be used to edit your command line entries:

KEY COMBINATION	EDIT FUNCTION
Ctrl-d	Delete current character
Ctrl-u	Delete text up to cursor
Ctrl-k	Delete from cursor to end of line
Ctrl-a	Move to beginning of line
Ctrl-e	Move to end of line
Ctrl-p	Get prior command from history
Ctrl-n	Get next command from history
Ctrl-b	Move cursor left
Ctrl-f	Move cursor right
Esc-b	Move back one word

KEY COMBINATION	EDIT FUNCTION
Esc-f	Move forward one word
Esc-c	Convert rest of word to uppercase
Esc-l	Convert rest of word to lowercase
Esc-d	Delete remainder of word
Ctrl-w	Delete word up to cursor
Ctrl-t	Transpose current and previous character
Ctrl-z	Enter command and return to root prompt
Ctrl-l	Refresh input line
up arrow	Put last command on the command line
!! <cr>	Execute last command

Session settings

The CLI contains commands to configure how your terminal session behaves.

The following table lists the default terminal settings and the CLI commands that you can use to change the settings.

SETTING	DESCRIPTION	DEFAULT VALUE	COMMAND TO CHANGE SETTING
columns	Sets the width of the session window in number of columns.	80	<code>conf t session col <number of columns></code>
rows	Sets the height of the session window in number of columns.	25	<code>conf t session row <number of rows></code>
more	When enabled, displays large amounts of information in page-by-page format.	SSH: Off Console: on	<code>conf t session more</code> <code>conf t session no more</code>
wraparound	When enabled, wraps lines of text.	on	<code>conf t session no wrap</code>
timeout	Sets the period of inactivity after which a user will be logged off.	20 minutes	<code>conf t session timeout <number of minutes></code>

See the command `conf t session` for more information.



Note

The timeout persists only if the `-persist` option is used when configuring the terminal session timeout. The `-persist` option requires super-user privileges.



Tip

For best viewing, set your terminal software's row and column settings to match your CLI session's row and column settings.

TippingPoint IPS commands

This topic provides links to topics with reference information for the Command Line Interface (CLI) for the TippingPoint IPS.

Conventions

Describes the organizational and stylistic conventions used in the CLI.

This topic is divided into sections by top-level commands. Some top-level commands, such as **configure terminal**, have been split up for easier reference. Each command section has the following information:

- Description
- Required privileges
- Subcommands and/or options
- Examples of usage

Variables are enclosed in angle brackets. For example, a snapshot name variable is represented as `<snapshot name>`. Optional flags and variables are enclosed in square brackets. For example, an optional profile name is represented as `[-profile <profile name>]`.



CAUTION!

The square brackets are included in usage examples for clarification purposes only. Do not type these brackets when entering a command.

Global commands

The commands in this topic manage your CLI session.

The settings and results do not persist across multiple sessions. These commands are available to all users and user roles.

- *alias*
- *clear*
- *cls*
- *exit*
- *help*
- *history*
- *logout*
- *quit*
- *tree*
- *who*
- *whoami*

alias

Creates aliases for commands or command strings.

Description

You can define an alias to represent all of or a portion of a command line including:

- a command
- a command option
- a command flag or option
- a combination of command, options, and flags

Usage

```
alias <alias> "<command_string>"
```

The following table lists examples of user-created command aliases.

DEFINE ALIAS	BEFORE ALIAS	AFTER ALIAS
alias s1A "show conf int eth 1A"	show conf int eth 1A	s1A
alias 1A "int eth 1A"	show conf int eth 1A	show conf 1A
	conf t int eth 1A shutdown	conf t 1A shut
alias eth "int eth"	show conf int eth 1A	show conf eth 1A
	show conf int eth 1A	show conf eth 1A
alias sc "show conf"	show conf int eth 1A	sc int eth 1A
	show conf clock	sc clock

clear

Resets logs or hardware interfaces.

Required privilege

Admin, Super-User



Note

Users with Admin privileges cannot clear the audit log or execute the **clear configuration** command.

Subcommands

The **clear** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
adaptive-filter	Re-enables a filter that has been disabled because of adaptive-filter configuration.	clear adaptive-filter <number>

SUBCOMMAND	DESCRIPTION	USAGE
configuration	Resets the device configuration settings to the factory defaults. Use the <code>-echo</code> option to echo the command when it is executed.	<code>clear configuration</code>
connection-table	Use the <code>blocks</code> option to clear all connection table block entries. Use the <code>trusts</code> option to clear all trust table entries.	<code>clear connection-table blocks</code> <code>clear connection-table trusts</code>
counter interface	Clears interface counters.	<code>clear counter interface</code>
counter policy	Clears policy counters.	<code>clear counter policy</code>
interface	Clears the interface. When used without options, it resets all interfaces.	<code>clear interface</code> <code>clear interface ethernet <port></code>
log	Clears log files. When used without options, it erases all entries in all logs.	<code>clear log</code> <code>clear log alert</code> <code>clear log audit</code> <code>clear log block</code> <code>clear log packet-trace</code> <code>clear log quarantine</code> <code>clear log system</code>
np	Clears np statistical information. <ul style="list-style-type: none"> <code>mcfilt-rule-stats</code> clears microfilter rules and flow statistics <code>rule-stats</code> clears rule statistics <code>softlinx</code> clears Softlinx-related statistics <code>tier-stats</code> clears tier statistics 	<code>clear np mcfilt-rule-stats</code> <code>clear np rule-stats</code> <code>clear np softlinx</code> <code>clear np tier-stats</code>
ramdisk stats	Clears RAM disk statistics.	<code>clear ramdisk stats</code>
rate-limit	Clears rate-limited streams from the data table.	<code>clear rate-limit streams</code>
slot	Sets the module slot and module type to Empty.	<code>clear slot <slot number></code>

**Note**

`clear counter interface`, `clear interface`, and `clear log` are disabled when the device is managed by an SMS.

cls

Clears the terminal screen.

Usage

```
cls
```

exit

Backs you out of one or more command levels.

For detailed information about command hierarchy, see [Use hierarchical commands](#).

Usage

```
exit
```

```
exit all
```

help

Displays documentation about the specified command.

At the CLI prompt, you can access the help topics for commands. You can also specify help for commands and edit keys.

Usage

```
help
```

```
help commands
```

```
help edit
```

history

Displays a list of commands that have been executed during the current CLI session.

Usage

```
history
```

logout

Logs you out of the TippingPoint IPS.

Usage

```
logout
```

quit

Logs you out of the TippingPoint IPS.

Usage

```
quit
```

tree

Displays the full command tree.

Usage

```
tree
```

who

Shows the usernames, connection methods, IP addresses, and login times of all the users who are currently logged in to IPS.

By default, the login time is shown in the time zone that you set during setup or with the `conf t clock` command. Use the `-utc` option to view the login times in Universal Time.

Required Privilege

Admin, Super-User

Usage

```
who
```

```
who -utc
```

whoami

Displays the username, role, and path of the currently logged-in user.

Usage

```
whoami
```

TipingPoint Operating System commands

The commands in this topic configure, manage, and display information about the Tipping Point Operating System (TOS) and its users.

- [*boot*](#)
- [*compact-flash*](#)
- [*configure terminal*](#)
- [*debug*](#)
- [*fips*](#)
- [*halt*](#)
- [*high-availability*](#)
- [*ping*](#)
- [*quarantine*](#)
- [*reboot*](#)
- [*setup*](#)
- [*show*](#)
- [*show configuration*](#)
- [*show np tier-stats*](#)
- [*show stacking*](#)

- [snapshot](#)
- [tech-support-report](#)

boot


Manages boot images on the device.

Required privilege

Super-user, Admin

Subcommands

The **boot** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
list-image	Shows a list of all available boot images.	<code>boot list-image</code>
remove-image	Removes a boot image from the device's hard disk. The image is identified by version number.  CAUTION! Removing a boot image permanently erases it.	<code>boot remove-image <version></code>
rollback	Rolls the boot image back to the next most recent valid boot image. This command can be used to revert the operating system to a previous version.	<code>boot rollback</code>



Note

boot remove-image and **boot rollback** are disabled when the device is managed by an SMS.

compact-flash

Controls the external storage card on the TippingPoint IPS devices.

The external storage card is used to store logs, snapshots, and other system data.



Note

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

Required privilege

Admin, Super-User, Operator

Subcommands

The **compact-flash** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
format	Formats the external storage card.	<code>compact-flash format</code>
mount	Manually mounts the inserted external storage card.	<code>compact-flash mount</code>
unmount	Unmounts the external storage card so that the user can remove it.	<code>compact-flash unmount</code>

configure terminal

The **configure terminal** commands configure IPS settings.

The command can be abbreviated as **conf t**. The following configure terminal commands are available:

- *conf t action-set*
- *conf t authentication remote*
- *conf t autodv*
- *conf t auxdv delete*
- *conf t category-settings*
- *conf t clock*
- *conf t compact-flash*
- *conf t cpu-utilization*
- *conf t default-alert-sink*
- *conf t default-gateway*
- *conf t email-rate-limit*
- *conf t filter*
- *conf t high-availability*
- *conf t host*
- *conf t inspection-bypass*
- *conf t inspection-bypass add*
- *conf t interface ethernet*
- *conf t interface mgmtEthernet*
- *conf t interface settings*
- *conf t lcd-keypad*
- *conf t log audit*
- *conf t log snmp-add-event-info*
- *conf t monitor*
- *conf t named-ip*

- *conf t nms*
- *conf t notify-contact*
- *conf t port*
- *conf t profile*
- *conf t protection-settings*
- *conf t radius-server*
- *conf t ramdisk*
- *conf t remote-syslog*
- *conf t reputation*
- *conf t reputation group*
- *conf t segment*
- *conf t server*
- *conf t service-access*
- *conf t session*
- *conf t sms*
- *conf t snmp*
- *conf t traffic-mgmt*
- *conf t tse*
- *conf t user*
- *conf t user options*
- *conf t virtual-port*
- *conf t virtual-segment*
- *conf t vlan-translation*

conf t action-set

Configures new or existing action sets.

The subcommands specify the actions taken.

Required privilege

Admin, Super-User

Subcommands

The **conf t action-set** command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
allowed-dest	Adds or removes a quarantine allowed destination.	<pre>conf t action-set <action set name> allowed-dest <destination address> add conf t action-set <action set name> allowed-dest <destination address> remove</pre>
apply-only	Adds or removes a CIDR from the quarantine apply-only list.	<pre>conf t action-set <action set name> apply- only <CIDR> add conf t action-set <action set name> apply- only <CIDR> remove</pre>
block	<p>Creates or modifies an action set that blocks traffic. The following secondary actions can be added:</p> <ul style="list-style-type: none"> quarantine: host IP address is placed into quarantine. Use no quarantine to remove the address from quarantine. reset-both: TCP reset on the source and destination. reset-destination: TCP reset on the destination. reset-source: TCP reset on the source. reset-none: no TCP reset. 	<pre>conf t action-set <action set name> quarantine conf t action-set <action set name> no quarantine conf t action-set <action set name> block reset-both conf t action-set <action set name> block reset-destination conf t action-set <action set name> block reset-none conf t action-set <action set name> block reset-source</pre>
delete	Deletes the named action set.	<pre>conf t action-set <action set name> delete</pre>
http-block	Blocks http requests from quarantined hosts.	<pre>conf t action-set <action set name> http- block</pre>
http-page	Creates a web page to display when a quarantined host makes a web request.	<pre>conf t action-set <action set name> http- page [-show-name <name of page>] [-show- desc <description of page>] [-custom-text <content of page>]</pre>
http-redirect	Redirects http requests from a quarantined host to a specified URL.	<pre>conf t action-set <action set name> http- redirect <url></pre>
non-http-block	Blocks non-http requests from quarantined hosts. Permits non-http requests with no non-http-block .	<pre>conf t action-set <action set name> non- http-block</pre>
notify-contact	Adds or removes a notification contact from an action set.	<pre>conf t action-set <action set name> notify- contact add <contact name> conf t action-set <action set name> notify- contact remove <contact name></pre>
packet-trace	Enables and sets packet trace settings. Set a priority (high, medium, or low) with the -priority option and the number of bytes to capture (64-1600) with the -capture-size option. Use no packet-trace to disable packet tracing.	<pre>conf t action-set <action set name> packet- trace [-priority <priority>] [-capture- size <bytes>] conf t action-set <action set name> no packet-trace</pre>

SUBCOMMAND	DESCRIPTION	USAGE
permit	Creates or modifies an action set that permits traffic. Use the quarantine command to quarantine permitted traffic and no quarantine to stop quarantining permitted traffic.	<pre>conf t action-set <action set name> permit conf t action-set <action set name> permit quarantine conf t action-set <action set name> permit no quarantine</pre>
rate-limit	Creates or modifies an action set that rate-limits traffic. Enter the desired threshold in Kbps.	<pre>conf t action-set <action set name> rate-limit <threshold></pre>
rename	Renames the action set.	<pre>conf t action-set <action set name> rename <new action set name></pre>
threshold	Sets the quarantine threshold in seconds (1-10000).	<pre>conf t action-set threshold <seconds></pre>
threshold-period	Sets the quarantine threshold period in minutes (1-60).	<pre>conf t action-set threshold-period <minutes></pre>
trust	Creates or modifies a trust action set.	<pre>conf t action-set <action set name> trust</pre>
whitelist	Creates a whitelist of trusted IP addresses by using the add or remove subcommands.	<pre>conf t action-set <action set name> whitelist add <IP address> conf t action-set <action set name> whitelist remove <IP address></pre>

conf t authentication remote

Manages remote authentication.

Description

Remote authentication enables the device to use a remote RADIUS or TACACS+ server as an authentication proxy, or, if the device is managed by SMS, to use the SMS as an authentication proxy. When a user logs in, the device sends the login information to the remote server or SMS, which then authenticates the account against one or more account repositories.



Note

Remote authentication with the SMS will only function when network TCP port 10043 is open and not blocked by the firewall. RADIUS and TACACS+ have no such port constraints, although they do have default ports. Administrators must make sure that those configured ports are not blocked by the firewall.


Required privilege

Admin, Super-User

Subcommands

The **conf t authentication remote** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
enable	Enables remote authentication.	<pre>conf t authentication remote enable radius conf t authentication remote enable tacacs conf t authentication remote enable sms</pre>

SUBCOMMAND	DESCRIPTION	USAGE
disable	Disables remote authentication.	<code>conf t authentication remote disable</code>
timeout	<p>Sets the remote authentication server timeout. The value should be greater than the timeout configured on the SMS.</p> <hr/> <p> Note This subcommand is valid only with SMS remote authentication.</p>	<code>conf t authentication remote timeout <seconds></code>

conf t autodv

Enables and disables the automatic download service for Digital Vaccine (DV) updates.

This command requires a day of week and time of day for the download. If required, use the **-period** option to set the number of days between checks.

Required privilege

Admin, Super-User

Usage

```
conf t autodv day <day of week> time <time of day> -period <number of days>
```

```
conf t no autodv
```

conf t auxdv delete

Deletes an Auxiliary DV package installation from the device.



This command is disabled when the device is under SMS control.

Required privilege

Admin, Super-User

Usage

```
conf t auxdv delete <type>
```

Usage notes

<type> represents the name of the Auxiliary DV package being deleted. To view the installed Auxiliary DV packages, run the **show auxdv** command.

TOS version 3.7 and later supports multiple types of Auxiliary DVs. Ensure that you specify the correct type when running this command.

conf t category-settings

Enables and disables filter categories.

The command also enables you to assign a specific action set to each category. The following filter categories can be configured:

- exploits
- identity-theft
- im
- network-equipment
- p2p
- reconnaissance
- security-policy
- spyware
- streaming-media
- traffic-normal
- virus
- vulnerabilities

Required privilege

Admin, Super-User

Subcommands

The `conf t category-settings` command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
enable	Enables a filter category and assigns the named action set to the category. Enable the filter category for a specific profile with the <code>-profile</code> option.	<code>conf t category-settings [-profile <profile name>] <filter category> enable -action-set <action set></code>
disable	Disables the filter category.	<code>conf t category-settings [-profile <profile name>] <filter category> disable</code>

conf t clock

Sets the software clock on the IPS device.


Clock changes are synchronized with the appropriate clock driver, and the change is entered in the audit log.

Required privilege

Admin, Super-User

Subcommands

The `conf t clock` command uses the following subcommands.

SUBCOMMAND	DESCRIPTION	USAGE
date	Sets the date.	<code>conf t clock date <YYYY-MM-DD></code>
dst	Enables or disables Daylight Savings Time.	<code>cconf t clock dst</code> <code>conf t clock no dst</code>
time	Sets the time according to the 24-hour clock. For example, to set the clock to 3:30 PM, enter 15:30.	<code>cconf t clock time <HH:MM:SS></code>
timezone	<p>Sets the time zone. For a list of available time zones, use the command <code>show timezones</code>. Because Daylight Savings Time (DST) calculations vary in different parts of the world, use the following options to specify DST for your region:</p> <ul style="list-style-type: none"> <code>-beginDST</code> – Date and hour DST begins (<i>mmddhh</i>) <code>-endDST</code> – Date and hour DST ends (<i>mmddhh</i>) <p>These values hold true until they are deleted, at which time the internal default values are used.</p> <hr/> <p> Note Starting and ending values have to be respecified each year. For best practice, reconfigure these after DST ends.</p>	<code>conf t clock timezone <timezone> -beginDST <mmddhh> -endDST <mmddhh></code>

conf t compact-flash

Configures the mounting options for the external storage card.

By default, the device is set to automatically mount external storage cards when inserted.

Note

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

Required privilege

Admin, Super-User

Subcommands

The `conf t compact-flash` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
<code>operation-mode authenticate</code>	Sets the device to require authentication when an external storage card is inserted.	<code>conf t compact-flash operation-mode authenticate</code>

SUBCOMMAND	DESCRIPTION	USAGE
<code>operation-mode auto-mount</code>	Sets the device to automatically mount external storage cards when inserted.	<code>conf t compact-flash operation-mode auto-mount</code>

conf t cpu-utilization

Configures the period over which average CPU utilization is calculated.

The period is specified in seconds. To view processes and utilization, see [debug information](#).

Required privilege

Admin, Super-User

Usage

```
conf t cpu-utilization <period in seconds>
```

conf t default-alert-sink

Defines the default email recipient of traffic-triggered alerts.



Note

The email notification server must be an SMTP server that the IPS device can reach through its host management port. You might have to add an additional route to your host management port using the `conf t interface mgmtEthernet` command to enable this communication. See [conf t interface mgmtEthernet](#).

Required privilege

Admin, Super-User

Subcommands

The `conf t default-alert-sink` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
<code>domain</code>	Defines the domain name of the email notification server.	<code>conf t default-alert-sink domain <domain name></code>
<code>from</code>	Defines the email address for the IPS device. This must be a valid email user name on the notification server.	<code>conf t default-alert-sink from <email address></code>
<code>no</code>	Removes the default email destination.	<code>conf t no default-alert-sink</code>
<code>period</code>	Defines the default period of time in which the TippingPoint device accumulates notifications before sending an aggregate notification email.	<code>conf t default-alert-sink period <minutes></code>
<code>server</code>	Defines the IP address of the email notification server. To remove the IP address of the email notification server, enter <code>none</code> for the IP address.	<code>conf t default-alert-sink server <IP address></code> <code>conf t default-alert-sink server none</code>

SUBCOMMAND	DESCRIPTION	USAGE
to	Defines the email address of the alert recipient. This must be a valid email address.	<code>conf t default-alert-sink to <email address></code>

conf t default-gateway

Defines a default gateway IP address for your IPS.

This gateway is used by the management port to communicate with devices located on other network segments. Use the **conf t no default-gateway** command to disable the default gateway IP address.

Required privilege

Admin, Super-User

Usage

```
conf t default-gateway <IP address>
```

```
conf t no default-gateway
```

conf t email-rate-limit

Configures the maximum number of email notifications that the system will send every minute.

The minimum is 1, and the maximum is 35.

Required privilege

Admin, Super-User

Usage

```
conf t email-rate-limit <number>
```

conf t filter

Configures a filter's state and action set category and enables or disables the filter.

Filters are identified with unique numbers. When you configure, enable, or disable a filter, enter the number for the filter. Only the **reset** subcommand supports **all** as an option.

Required privilege

Admin, Super-User

Subcommands

The **conf t filter** command uses the following subcommands:



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
adaptive-config	Enables or disables adaptive filtering. Apply the change to a specific security profile with the -profile option.	<code>conf t filter <filter number> [-profile <profile name>] adaptive-config</code> <code>conf t filter <filter number> no adaptive-config</code>
add-exception	Creates and adds an exception to a filter, identified by source or destination IP address. Apply the change to a specific security profile with the -profile option.	<code>conf t filter <filter number> [-profile <profile name>] add-exception <source IP address> <destination IP address></code>
delete-copy	Deletes a copy of the filter. Apply the change to a specific security profile with the -profile option.	<code>conf t filter <filter number> [-profile <profile name>] delete-copy</code>
disable	Disables a filter. Apply the change to a specific security profile with the -profile option.	<code>conf t filter <filter number> [-profile <profile name>] disable</code>
enable	Enables a filter. Apply the change to a specific security profile with -profile option. Apply the change to a specific action set with the -action-set option.	<code>conf t filter <filter number> [-profile <profile name>] -action-set <action set name> enable</code>
remove-exception	Removes an exception from a filter. Apply the change to a specific profile with the -profile option.	<code>conf t filter <filter number> [-profile <profile name>] remove-exception</code>
reset	Resets filters to the default values.	<code>conf t filter <filter number> reset</code> <code>conf t filter all reset</code>
threshold	Sets the port scan and host sweep filter threshold.	<code>conf t filter threshold</code>
timeout	Sets the port scan and host sweep filter timeout.	<code>conf t filter timeout</code>
use-category	Sets a filter to use the default action set of its category and removes any previous overrides. Apply the change to a specific profile with the -profile option.	<code>conf t filter <filter number> [-profile <profile name>] use-category</code>

conf t high-availability

Enables and disables transparent network high availability (transparent HA) and configures the partner device's IP address.

Transparent HA updates data tables between two devices to quickly and efficiently transfer network traffic from one device to the other without the need to rebuild data tables.

Required privilege

Admin, Super-User

Subcommands

The `conf t high-availability` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
disable	Disables transparent HA.	<code>conf t high-availability disable</code>
enable	Enables transparent HA.	<code>conf t high-availability enable</code>
partner	Sets the IP address and serial number of the partner device. Use no partner to clear the address.	<code>conf t high-availability partner <IP address> <serial number></code> <code>conf t high-availability no partner</code>
l2fb	For 10/110/330 IPS devices only, sets the means by which the device goes in and out of Layer-2 Fallback (L2FB). You can configure L2FB using a link transition via hardware relays, or you can change the L2FB behavior to be software instantiated. <ul style="list-style-type: none"> hardware: The hardware ZPHA relays are used for L2FB. When the device enters and exits L2FB, a brief link transition occurs. This is the default option. Hardware L2FB is recommended, unless link transitions will cause network failover issues. software: No link transition occurs when the device enters and exits L2FB. 	<code>conf t high-availability l2fb hardware</code> <code>conf t high-availability l2fb software</code>

conf t host

Configures the host management port's name and location strings.

TippingPoint recommends using this command to limit access to the management port.



Note

The IPS must not be under SMS control when changing management port settings.

Required privilege

Admin, Super-User

conf t host fips-mode requires Super-User.

Subcommands

The **conf t host** command uses the following subcommands:



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
dns	Sets the DNS server. The secondary server is optional.	<code>conf t host dns <domain name> <primary server> [<secondary server>]</code>
fips-mode	<p>Enables FIPS mode.</p> <ul style="list-style-type: none"> crypto: Only FIPS-approved cryptographic algorithms are allowed, but some FIPS 140-2 requirements are not enforced. Once enabled, this mode can be disabled. full: Only FIPS-approved cryptographic algorithms are allowed, and all FIPS 140-2 requirements are enforced. Once enabled, this mode <i>cannot</i> be disabled. Only a factory reset can take the device out of this mode. A warning message prompts you to confirm the setting. A reboot is required to complete the configuration. <p>For more information about FIPS, see fips.</p>	<pre>conf t host fips-mode crypto conf t host fips-mode full</pre>
ip-filter	Permits or denies communications with the management port from specified IP addresses. Management port IP setting defaults to "permit any IP". Use this subcommand to limit management port access to designated IP addresses.	<pre>conf t host ip-filter deny <IP address> conf t host ip-filter permit <IP address></pre>
location	Sets a text string that identifies the location of the device. The string is restricted to 63 characters.	<code>conf t host location <location></code>
lsm disable	Disables the LSM without disabling http or https. (A reboot is required after the command is entered.)	<code>conf t host lsm disable</code>
lsm enable	Enables the LSM. (A reboot is required after the command is entered.)	<code>conf t host lsm enable</code>
name	Sets a text string that identifies the name of the device. The string is restricted to 63 characters.	<code>conf t host name <name></code>

conf t inspection-bypass

Enables, disables, or removes inspection bypass rules. Inspection bypass rules direct traffic through the IPS without inspection.

The rules are identified by an ID number that is generated by the IPS when the rule is created with the **conf t inspection-bypass add** command. You can view a list of current inspection bypass rules with the **show inspection-bypass** command.

**Note**

Inspection bypass rules are available only on the TippingPoint 2500N, TippingPoint 5100N, TippingPoint 6100N, and NX-Platform devices.

Required privilege

Admin

Options

The `conf t inspection-bypass` command uses the following options:

OPTION	DESCRIPTION	USAGE
add	Adds an inspection bypass rule. See conf t inspection-bypass add .	<code>conf t inspection-bypass add</code>
clear-stats	Clears statistics associated with an inspection bypass rule.	<code>conf t inspection-bypass clear-stats <rule_ID></code>
enable	Enables an inspection bypass rule.	<code>conf t inspection-bypass enable <rule_ID></code>
disable	Disables an inspection bypass rule.	<code>conf t inspection-bypass disable <rule_ID></code>
remove	Removes an inspection bypass rule.	<code>conf t inspection-bypass remove <rule_ID></code>

conf t inspection-bypass add

Creates and defines an inspection bypass rule.

When you define an inspection bypass rule, using an option without a specified value defaults to a value of “any”.

**Note**

Inspection bypass rules are available only on the TippingPoint 2500N, TippingPoint 5100N, TippingPoint 6100N, and NX-Platform devices.

Required privilege

Admin

Options

The `conf t inspection-bypass add` command uses the following options:

OPTION	DESCRIPTION	USAGE
-eth	EthType. You can also use the strings <code>ip</code> or <code>!ip</code> .	<code>conf t inspection-bypass add -eth <EthType></code>
-ports	The port or ports to which the rule is applied. For more information, see the Ports topic that follows this table.	<code>conf t inspection-bypass add -ports <value> -<option></code>
-gre	Specifies GRE tunneling traffic. Default value is <code>any</code> . You can also specify <code>present</code> or <code>absent</code> .	<code>conf t inspection-bypass add -gre <value></code>

OPTION	DESCRIPTION	USAGE
-mipv4	Specifies mobile IPv4 tunneling traffic. Default value is any . You can also specify present or absent .	<code>conf t inspection-bypass add -mipv4 <value></code>
-ipv6in4	Specifies IPv6 6-in-4 tunneling traffic. Default value is any . You can also specify present or absent .	<code>conf t inspection-bypass add -ipv6in4 <value></code>
-vlan	Numeric value or range specifying the permitted VLAN IDs. .	<code>conf t inspection-bypass add -vlan <value></code>
-mpls	Numeric value or range specifying the permitted MPLS IDs.	<code>conf t inspection-bypass add -mpls <value></code>
-ip-proto	IP protocol value. For more information, see the <code>ip-proto</code> topic that follows this table.	<code>conf t inspection-bypass add -ip-proto <value></code>
-ip-saddr	Source CIDR specification. Enter in the form <code>xxx.xxx.xxx.xxx/xx</code> .	<code>conf t inspection-bypass add -ip-saddr <CIDR range></code>
-ip-daddr	Destination CIDR specification. Enter in the form <code>xxx.xxx.xxx.xxx/xx</code> .	<code>conf t inspection-bypass add -ip-daddr <CIDR range></code>
-upd-sport	UDP source port.	<code>conf t inspection-bypass add -upd-sport <value></code>
-upd-dport	UDP destination port.	<code>conf t inspection-bypass add -upd-dport <value></code>
-tcp-sport	TCP source port.	<code>conf t inspection-bypass add -tcp-sport</code>
-tcp-dport	TCP destination port.	<code>conf t inspection-bypass add -tcp-dport</code>

Ports

The **-ports** option can be one or more comma-delimited 1GbE ports (1A, 1B, 2A, 2B, 3A, 3B). If you do not specify a port or define the **-ports** option as **ANY**, the inspection bypass rule is applied to all ports on all segments.

A single inspection bypass rule can apply to all segments, to both ports on one segment, or to one port on one segment. You cannot apply a single inspection bypass rule to ports on two different segments. Instead, you must create a separate inspection bypass rule for each segment.

Example: rules applied to a single segment

If you want to permit traffic that uses the IP Mobility protocol (MOBILE) on both ports of Segment 1, you would define the inspection bypass rule with the following command:

```
hostname# conf t inspection-bypass add -ports 1A,1B -ip-proto MOBILE
```

Example: rules applied across multiple segments

If you want to permit traffic that uses the IP Mobility protocol (MOBILE) on both ports of Segment 1 and Segment 2, you would need to define two inspection bypass rules with the following commands:

```
hostname# conf t inspection-bypass add -ports 1A,1B -ip-proto MOBILE
```

```
hostname# conf t inspection-bypass add -ports 2A,2B -ip-proto MOBILE
```

However, if you want to permit that traffic across all ports on all segments, you can define a single inspection bypass rule with the following command:

```
hostname# conf t inspection-bypass add -ip-proto MOBILE
```

When no segment is specified, the command defaults apply the inspection bypass rule to all ports on all segments.

ip-proto

A full list of IP protocol values can be found at the Internet Assigned Numbers Authority website at <http://www.iana.org/assignments/protocol-numbers>.

conf t interface ethernet

Configures IPS interfaces. Refer to physical interfaces by their segment and port numbers.

On NX-Platform devices, ports are presented in the format Slot-SegmentPort. For example, port 4A on slot 3 would be specified as “3-4A”.

Required privilege

Admin, Super-User

Options

The **conf t interface ethernet** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
duplex	Sets the duplex speed to half or full.	<code>conf t interface ethernet <port> duplex half</code> <code>conf t interface ethernet <port> duplex full</code>
linespeed	Sets the line speed. You can set the speed to 10, 100, 1000, or 10000.	<code>conf t interface ethernet <port> linespeed <speed></code>
negotiate	Enables or disables auto-negotiate.	<code>conf t interface ethernet <port> negotiate</code> <code>conf t interface ethernet <port> no negotiate</code>
shutdown	Shuts down the port. Use no shutdown to reactivate the port after a shutdown command or after configuration has changed.	<code>conf t interface ethernet <port> shutdown</code> <code>conf t interface ethernet <port> no shutdown</code>



Note

When the auto-negotiate feature is on, the IPS device automatically negotiates the highest common speed and duplex that the IPS and the link partner both support. When the auto-negotiate feature is turned off, users can configure all fiber ports (SFP, SFP+, QSFP+) only to their default settings using the **linespeed** subcommand even though the hardware might list other optional values. The 12 fixed RJ-45 copper ports, however, can be configured to 10 Mbps, 100 Mbps, or 1 Gbps using the **linespeed** subcommand.

conf t interface mgmtEthernet

Configures the management port.

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 direct attack on the management port from the Internet. For more management port configuration settings, see [conf t host](#).

Required privilege

Admin, Super-User

Options

The `conf t interface mgmtEthernet` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
duplex	Sets the duplex speed to half for full.	<code>conf t interface mgmtEthernet duplex half</code> <code>conf t interface mgmtEthernet full</code>
ip	Sets the IP address for the management Ethernet port. The address can be IPv4 or IPv6. Use CIDR notation to set the subnet mask. The default mask is used when the user specifies a non-CIDR IP address.	<code>conf t interface mgmtEthernet ip <IP address></code>
ipv6	Enables or disables IPv6 support on the management port.	<code>conf t interface mgmtEthernet ipv6</code>
ipv6auto	Enables or disables automatic IPv6 configuration, which allows the device to get an IPv6 address automatically from the subnet router.	<code>conf t interface mgmtEthernet ipv6auto</code>
linespeed	Sets the line speed. You can set the speed to 10, 100, or 1000.	<code>conf t interface mgmtEthernet linespeed <speed></code>
negotiate	Enables or disables auto-negotiate.	<code>conf t interface mgmtEthernet negotiate</code> <code>conf t interface mgmtEthernet no negotiate</code>
physical-port	Specifies the physical port.	<code>conf t interface mgmtEthernet physical-port <port></code>
route	Sets or removes the default route for the management Ethernet port.	<code>conf t interface mgmtEthernet route <destination> <gateway IP address or CIDR></code> <code>conf t interface mgmtEthernet no route <destination></code>
vlan	Specifies the VLAN ID.	<code>conf t interface mgmtEthernet vlan <vlan ID></code>

Note

When the auto-negotiate feature is on, the IPS device automatically negotiates the highest common speed and duplex that the IPS and the link partner both support. When the auto-negotiate feature is turned off, users can configure all fiber ports (SFP, SFP+, QSFP+) only to their default settings using the **linespeed** subcommand even though the hardware might list other optional values. The 12 fixed RJ-45 copper ports, however, can be configured to 10 Mbps, 100 Mbps, or 1 Gbps using the **linespeed** subcommand.

conf t interface settings

Enables or disables Medium Dependence Interface (MDI) detection when auto-negotiation is off.

These settings do not affect the management port.

Note

Changes to the MDI settings do not go into effect until the link is shut down. These settings affect all ports and are not configurable on a port-by-port basis.

Required privilege

Admin, Super-User

Options

The **conf t interface settings** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
detect-mdi	Enables or disables MDI detection.	<pre>conf t interface settings detect-mdi enable</pre> <pre>conf t interface settings detect-mdi disable</pre>
mdi-mode	Sets the MDI mode to mdi or mdix . The default setting is mdix . The mdi setting has no effect if auto-negotiation is enabled, detect-mdix is enabled, or the port media is fiber.	<pre>conf t interface settings mdi-mode mdi</pre> <pre>conf t interface settings mdi-mode mdix</pre>

conf t lcd-keypad

Enables or disables the keypad and buttons for the LCD keypad.

Required privilege

Admin, Super-User

Options

The **conf t lcd-keypad** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
backlight	Sets the intensity of the backlighting in a range from 1 (dimpest) to 100 (brightest).	<pre>conf t lcd-keypad backlight <number></pre>
contrast	Sets the contrast in a range from 1 to 50.	<pre>conf t lcd-keypad contrast <number></pre>
disable	Disables the LCD keypad.	<pre>conf t lcd-keypad disable</pre>
enable	Enables the LCD keypad.	<pre>conf t lcd-keypad enable</pre>

conf t log audit

Configures the audit log and the actions that are documented in the log.

Required privilege

Admin, Super-User

Usage

```
conf t log audit select <activity>
```

```
conf t log audit select no <activity>
```

The following activities can be documented in the audit log:

• boot	• monitor
• compact-flash	• policy
• configuration	• report
• conn-table	• segment
• device	• server
• general	• slot
• high-availability	• sms
• host	• time
• host-communications	• tse
• ip-filter	• update
• login	• user
• logout	

conf t log snmp-add-event-info

Configures whether the SNMP traps receive additional information, such as the client IP address. The minimum is 1, and the maximum is 35.

Required privilege

Admin, Super-User

Usage

```
configure terminal log snmp-add-event-info enable
```

```
configure terminal log snmp-add-event-info disable
```

conf t login-banner

Configures a login consent banner for websites.

The banner notifies entrants that the website or server they are about to enter is private and activity may be subject to monitoring. Users who enable the login banner must configure text, which can consist of up to a 50-character title and a 1500-character message. Only printable ASCII characters are supported.

To display the following ASCII characters in the login banner text message, use the following 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

Required privilege

Admin, Super-User

Usage

```
conf t login-banner [ enable | disable ] -title <title text> -text <message text>
```

conf t monitor

Enables or disables power supply monitoring and sets hardware monitoring thresholds for IPS disk usage, memory, and temperature values.

Required privilege

Admin, Super-User

Subcommands

The `conf t monitor` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
<code>disable power-supply</code>	Disables power supply monitoring.	<code>conf t monitor disable power-supply</code>
<code>enable power-supply</code>	Enables power supply monitoring. If any power supplies experience an interruption, the system logs a critical message in the system log and sends a notification to the SMS if the device is under SMS management.	<code>conf t monitor enable power-supply</code>
<code>threshold</code>	<p>Sets threshold values for disk usage, memory, and temperature values. Disk and memory thresholds are expressed in percentages, and temperature thresholds are expressed in degrees Celsius.</p> <ul style="list-style-type: none"> The major threshold value must be set at a value less than the critical threshold value and that allows time to react before a problem occurs. The critical threshold value should generate a warning before a problem causes damage. 	<pre>conf t monitor threshold disk -major <60-100> -critical <60-100> conf t monitor threshold memory -major <60-100> -critical <60-100> conf t monitor threshold temperature - major <40-80> -critical <40-80></pre>

conf t named-ip

Enables you to assign names to IPv4 and IPv6 addresses.

A name acts as an alias for the named IPv4 or IPv6 network. 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.

Required privilege

Admin, Super-User

Subcommands

The `conf t named-ip` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add	Adds a new named IP address to the system.	<code>conf t named-ip add <IP address> <name></code>
delete	Removes a name.	<code>conf t named-ip remove <name></code>
modify	Modifies a name.	<code>conf t named-ip modify <name></code>
rename	Renames a named IP address.	<code>conf t named-ip rename <old name> <new name></code>

conf t nms

Configures information for a network management system (NMS).

The NMS community string is separate from the string used by SMS. Use **conf t no nms** to disable NMS options.

Required privilege

Admin, Super-User

Subcommands

The **conf t nms** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
community	Sets the NMS community string. The string is limited to 31 characters.	<code>conf t nms community <string></code>
syscontact	Sets the NMS SNMP sysContact string. The string is limited to 192 characters.	<code>conf t nms syscontact <string></code>
trap-destination	Adds or removes an NMS trap IP address. You can also specify a port number with the -port option. For SNMPv3, the following options are also available: <ul style="list-style-type: none"> • -user • -password • -engine • -des 	<pre>conf t nms trap-destination add <IP address> -port <port number> conf t nms trap-destination remove <IP address> conf t nms trap destination add <IP address> port <port number> -user <user ID> -password <password> -engine <engine> -des <destination></pre>

conf t notify-contact

Sets the aggregation period for notification contacts.

You must enter the name of an existing notification contact and an aggregation period in minutes.



CAUTION!

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

Required privilege

Admin, Super-User

Usage

```
conf t notify-contact <contact name> <aggregation period>
```

conf t ntp

Configures NTP timekeeping options.



CAUTION!

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


Required privilege

Admin, Super-User

Options

The `conf t ntp` command uses the following options:

SUBCOMMAND	DESCRIPTION	USAGE
<code>add-key</code>	<p>Adds a key for authenticating. Options include:</p> <ul style="list-style-type: none"> <code>-index</code>: the Key ID, required for authentication, as a unique integer value ranging from 1–65535 that one or more servers reference. <code>-value</code>: the authentication password string ranging from 1–32 characters. 	<pre>conf t ntp add-key -index <number> -value <string></pre>
<code>add-server</code>	<p>Adds a server for authenticating. Options include:</p> <ul style="list-style-type: none"> <code>-host</code>: specifies the hostname or IP address of the NTP server. <code>-index</code>: references the defined key for authentication. <code>-version</code>: (optional) indicates the version of the NTP protocol that is running on the server. Default is 3. <code>-preferred</code>: (optional) indicates whether this is the preferred server. Default is no. <code>-auth</code>: enables or disables authentication. Default is disable. 	<pre>conf t ntp add-server -host <host> -index <number> -version <number> -preferred [yes no] -auth [enable disable]</pre>
<code>-polling period</code>	<p>The <code>-polling period</code> option is specified in 16, 32, or 64 seconds. Default is 16.</p>	<pre>conf t ntp -polling-period [16 32 64]</pre>

SUBCOMMAND	DESCRIPTION	USAGE
<code>disable</code> <code>enable</code>	<p>Disables or enables NTP. NTP is disabled by default.</p> <hr/> <p> Note Specifying one of these options automatically performs the opposite option for SNTP. This ensures that only one time protocol is active at a time.</p>	<pre>conf t ntp disable conf t ntp enable</pre>
<code>delete</code>	Deletes a specified server or key, or all servers or keys.	<pre>conf t ntp delete server [<hostname or IP address> all] conf t ntp delete key [<index number> all]</pre>

conf t port

Configures the protocols that are permitted on the IPS ports.

This command enables the user to specify non-standard TCP/UDP ports to help check for signature matches. The available options include:

• auth	• pop3
• nstcp	• portmappertcp
• dnsudp	• portmapperudp
• finger	• rlogin
• ftp	• rsh
• http	• smb
• imac	• smtp
• ircu	• snmptcp
• ms-sql	• snmpudp
• nntp	• ssh
• pop2	• telnet

Required privilege

Admin, Super-User

Subcommands

The `conf t port` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
<code>add</code>	Adds a protocol to a port.	<code>conf t port <protocol> add <segment><port></code>
<code>delete</code>	Removes a protocol from a port.	<code>conf t port <protocol> remove <segment><port></code>

conf t profile

Creates, modifies, or deletes security or traffic management profiles.

**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.

Required privilege

Admin, Super-User

Subcommands

The **conf t profile** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add-pair	Adds a port pairing to a profile.	<code>conf t profile <profile name> add-pair <port pair></code>
client-ip	Enables or disables a client IP address on a profile.	<code>conf t profile client-ip enable</code> <code>conf t profile client-ip disable</code>
delete	Deletes an existing profile.	<code>conf t profile <profile name> delete</code>
description	Enters a description string for the profile.	<code>conf t profile <profile name> description "<description>"</code>
deployment	Sets the deployment mode. Deployment modes offer increased flexibility for filter settings. TippingPoint provides recommended settings customized for different deployment types, including Core, Edge, or Perimeter. Use <code>show deployment-choices</code> to see your options.	<code>conf t profile deployment core</code> <code>conf t profile deployment edge</code> <code>conf t profile deployment perimeter</code> <code>conf t profile deployment default</code>
http-context	Enables or disables HTTP URI information to identify the name of a web resource.	<code>conf t profile http-context enable</code> <code>conf t profile http-context disable</code>
remove-pair	Removes a port pairing from a profile.	<code>conf t profile <profile name> remove-pair <port pair></code>
rename	Renames a profile.	<code>conf t profile <profile name> rename <new profile name></code>
security	Creates a security profile. You can add a description string with the <code>-description</code> option.	<code>conf t profile <profile name> security</code> <code>conf t profile <profile name> security -description "<description>"</code>
traffic-mgmt	Creates a traffic management profile. You can add a description string with the <code>-description</code> option.	<code>conf t profile <profile name> traffic-mgmt</code> <code>conf t profile <profile name> traffic-mgmt -description "<description>"</code>

conf t protection-settings

Creates global exceptions and apply-only restrictions for Application Protection, Infrastructure Protection, and Performance Protection filters.

You must specify the profile to which the settings apply.

Required privilege

Admin, Super-User

Subcommands

The `conf t protection-settings` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
<code>app-except</code>	Adds or removes a global exception for Application Protection and Infrastructure Protection filters.	<pre>conf t protection-settings app-except add <source IP address> <destination IP address> - profile <profile name> conf t protection-settings app-except remove <source IP address> <destination IP address> -profile <profile name></pre>
<code>app-limit</code>	Adds or removes an apply-only restriction for Application Protection and Infrastructure Protection filters.	<pre>conf t protection-settings app-limit add <source IP address> <destination IP address> - profile <profile name> conf t protection-settings app-limit remove <source IP address> <destination IP address> -profile <profile name></pre>
<code>dns-except</code>	Adds or removes a DNS exception for Application Protection and Infrastructure Protection filters.	<pre>conf t protection-settings dns-except add <DNS> -profile <profile name> conf t protection-settings dns-except remove <DNS> -profile <profile name></pre>
<code>ip-except</code>	Adds or removes an IP address exception for Application Protection and Infrastructure Protection filters. This exception applies to source and destination IP addresses.	<pre>conf t protection-settings ip-except add <IP address> -profile <profile name> conf t protection-settings ip-except remove <IP address> -profile <profile name></pre>
<code>perf-limit</code>	Adds or removes an apply-only restriction for Performance Protection filters.	<pre>conf t protection-settings perf-limit add <source IP address> <destination IP address> - profile <profile name> conf t protection-settings perf-limit remove <source IP address> <destination IP address> -profile <profile name></pre>

`conf t radius-server`


Configures a RADIUS server to be used for remote authentication for the device.

Required privilege

Super-User

Subcommands

The `conf t radius-server` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add	<p>Configures a RADIUS server for remote authentication.</p> <ul style="list-style-type: none"> • priority – Assigns the priority of the remote server. Values are between 1 and 3. • IP address – Must be an IPv4 address in dotted format. • port – Available ports between 1 and 65535. Default is 1812. • shared secret – Case-sensitive string with a maximum length of 64 characters. • authentication type – PAP or EAP-MD5-Challenge (RFC 3748). <hr/> <p> Note Users interested in TLS can alternatively use PEAP/EAP-MSCHAPv2 authentication. This protocol requires an X509 certificate for the RADIUS server and can only be set through the LSM.</p> <hr/> <ul style="list-style-type: none"> • timeout – Can be between 1 and 14 seconds. Default is 3 seconds. • attempts allowed – Can be between 1 and 5 attempts. Default is 3 seconds. 	<pre>conf t radius-server add -priority <priority-value> <ip-address> [port <port number>] secret <shared secret> [auth-type <PAP MD5>] [timeout <timeout-value>] [attempts <attempts-value>]</pre>
delete	Removes a RADIUS server for remote authentication.	<pre>conf t radius-server delete -priority <priority-value></pre>
modify	Modifies a RADIUS server for remote authentication. See the add subcommand for option descriptions.	<pre>conf t radius-server modify -priority <priority-value> <ip-address> [port <port number>] secret <shared secret> [auth-type <PAP MD5>] [timeout <timeout-value>] [attempts <attempts-value>]</pre>

conf t ramdisk

Configures log file synchronization between the RAM disk and the hard disk.

Required privilege

Admin, Super-User

Options

The **conf t ramdisk** command uses the following options:

SUBCOMMAND	DESCRIPTION	USAGE
force-sync	Immediately synchronizes the RAM disk with the hard disk. You can synchronize all files, or specify alert , audit , block , or sys .	<pre>conf t ramdisk force-sync all conf t ramdisk force-sync <file></pre>
sync-interval	<p>Sets the synchronization interval in seconds. With a value of 0 (zero), all writes are immediately written to the hard disk. With a value of -1, the file is written to the hard disk when a conf t ramdisk force-sync command is executed, the device is rebooted or halted, or when the device enters high availability fallback mode.</p> <p>You must specify alert, audit, block, or sys.</p>	<pre>conf t ramdisk sync-interval <file></pre>

conf t remote-syslog

Configures a remote recipient of IPS attack and block messages in syslog format.

Many operating systems provide the ability to receive remote syslog messages, and third-party remove syslog packages are also available.



Note

Designating a remote syslog server does not automatically send attack and block notifications to that server. You must also select the Remote System Log contact by going to the Filters/Vulnerability filters/Action Sets area in the LSM and either creating or editing an action set. After you apply these changes, active filters that are associated with this action set will send remote messages to the designated server.



CAUTION!

Use remote syslog only on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol. It does not offer any additional security protections. You should not use remote syslog unless you can be sure that syslog messages will not be intercepted, altered, or spoofed by a third party.

Required privilege

Admin, Super-User

Options

The **conf t remote-syslog** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add-event-info	Enables or disables additional information, including client IP address, on the remote syslog.	<pre>conf t remote-syslog add-event-info enable conf t remote-syslog add-event-info disable</pre>
audit	Enables or disables remote syslog for the Audit log.	<pre>conf t remote-syslog audit <IP address> - port <port> conf t remote-syslog no audit</pre>

SUBCOMMAND	DESCRIPTION	USAGE
delete	Deletes a remote syslog collector.	<code>conf t remote-syslog delete <IP address> -port <port></code>
rfc-format	EnableDs or disables RFC format on the remote syslog.	<code>conf t remote-syslog rfc-format enable</code> <code>conf t remote-syslog rfc-format disable</code>
quarantine	Enables or disables remote syslog for the Quarantine log.	<code>conf t remote-syslog quarantine enable</code> <code>conf t remote-syslog quarantine disable</code>
system	Enables or disables remote syslog for the System log.	<code>conf t remote-syslog system <IP address> -port <port></code> <code>conf t remote-syslog no system</code>
update	Creates or updates a remote syslog collector. A collector is specified by IP address and port. You also have the option to include a delimiter and facility numbers for alert messages, block messages, and misuse/abuse messages. Facility numbers can be any number from 0-31 inclusive. Delimiter options include tab, comma, semicolon, and bar.	<code>conf t remote-syslog update <IP address> -port <port> -alert-facility <number></code> <code>conf t remote-syslog update <IP address> -port <port> -block-facility <number></code> <code>conf t remote-syslog update <IP address> -port <port> -misuse-facility <number></code> <code>conf t remote-syslog update <IP address> -port <port> -delimiter <character></code>

conf t reputation

Configures the behavior of IP Reputation filters.

Reputation filters enable you to apply block, permit, or notify actions across an entire reputation group. For specific information about configuring reputation groups, see [conf t reputation groups](#).

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

If you do not specify a security profile in which to configure the filter, the filter is applied to the Default security profile.

TippingPoint ThreatDV

The TippingPoint ThreatDV is a licensed service that identifies and delivers suspect IPv4, 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 like Digital Vaccines do.



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.

Required privilege

Admin, Super-User

Subcommands

The `conf t reputation` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
action-when-pending	The action that the IPS takes on traffic coming from the specified IP address while the IP reputation filter is caching the address. The default action is permit .	<pre>conf t reputation action-when-pending [-profile <security profile name>] permit</pre> <pre>conf t reputation action-when-pending drop [-profile <security profile name>] permit</pre>
check-dest-address	Enables or disables action on the traffic destination IP address.	<pre>conf t reputation check-dest-address [-profile <security profile name>] enable</pre> <pre>conf t reputation check-dest-address [-profile <security profile name>] disable</pre>
check-source-address	Enables or disables action on the traffic source IP address.	<pre>conf t reputation check-source-address [-profile <security profile name>] enable</pre> <pre>conf t reputation check-source-address [-profile <security profile name>] disable</pre>
filter	<p>Configures reputation filters and maps a security profile to a reputation group.</p> <ul style="list-style-type: none"> delete-copy: Deletes a filter. disable: Disables a filter without deleting it. enable: Enables a filter and maps it to a reputation group. <p>The -threshold option sets a reputation filter threshold based on the IP reputation information maintained by the TippingPoint TMC. Entries that exceed the TMC-set threshold are acted upon by the IPS.</p>	<pre>conf t reputation filter <group name> [-profile <security profile name>] delete-copy</pre> <pre>conf t reputation filter <group name> [-profile <security profile name>] disable</pre> <pre>conf t reputation filter <reputation group name> [-profile <security profile name>] enable [-threshold <number>] -action-set <action set name></pre>

conf t reputation group

Creates and configures groups of IPv4, IPv6, and DNS addresses and define an action set to apply to all of those addresses.

After a group is configured, security profiles can be configured to apply reputation filters to the group.

Required privilege

Admin, Super-User

Options

The **conf t reputation group** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add-domain	Adds a domain to a reputation group.	<pre>conf t reputation group add-domain <name> <domain></pre>
add-ip	Adds an IP address to a reputation group.	<pre>conf t reputation group add-ip <name> <domain></pre>
create	Creates an IP reputation group.	<pre>conf t reputation group create <name> [-description "description of option"]</pre>
delete	Deletes an IP reputation group.	<pre>conf t reputation group delete <name></pre>

SUBCOMMAND	DESCRIPTION	USAGE
<code>remove-domain</code>	Removes a domain from a reputation group.	<code>conf t reputation group remove-domain <name> <domain></code>
<code>remove-ip</code>	Removes an IP address from a reputation group.	<code>conf t reputation group remove-ip <name> <domain></code>
<code>rename</code>	Renames an IP reputation group.	<code>conf t reputation group rename <old name> <new name></code>

conf t segment

Configures and names segments, and also configures the intrinsic network high availability (INHA) action for segments.

On NX-Platform devices, ports are presented in the format Slot-Segment. For example, segment 4 on slot 3 would be specified as “3-4”.

Required privilege

Admin, Super-User

Subcommands

The `conf t segment` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
<code>high-availability</code>	Sets the intrinsic network high availability (fallback) option for the segment. If the segment is set to <code>block</code> , all traffic through that segment is denied in the fallback state. If the segment is set to <code>permit</code> , then all traffic is permitted in the fallback state.	<pre>conf t segment <segment name> high-availability block conf t segment <segment name> high-availability permit</pre>
<code>link-down</code>	<p>Configures the Link-Down Synchronization mode and timeout length. The following modes are available:</p> <ul style="list-style-type: none"> <code>hub</code>: Ensures the partner port is unaffected when the link goes down. <code>breaker</code>: Requires both the port and its partner to be manually restarted when the link goes down. <code>wire</code>: Automatically restarts the partner port when the link comes back up. <p>Valid range of timeout is 0 to 240 seconds.</p>	<pre>conf t segment <segment name> link-down hub conf t segment <segment name> link-down breaker -timeout <seconds> conf t segment <segment name> link-down wire -timeout <seconds></pre>

SUBCOMMAND	DESCRIPTION	USAGE
name	<p>Defines a name for the segment with a maximum of 32 characters. Set the name to</p> <pre>""</pre> <p>to remove the name from the segment. Names must conform to the following rules:</p> <ul style="list-style-type: none"> • Can only contain letters A-Z and a-z, digits 0-9, single spaces, periods (.), underscores (_), and dashes (-). • Must include at least one non-digit character. • Cannot begin or end with spaces. 	<pre>conf t segment <segment name> name "<segment name>"</pre>
physical-ports	Specifies the physical ports.	<pre>conf t segment physical-port <port a> <port b></pre>
restart	Restarts a segment.	<pre>conf t segment <segment number> restart</pre>
sflow	On NX-Platform devices only, enables or disables sFlow sampling on the specified segment. Specify a sampling rate for <number>.	<pre>conf t segment <segment name> sflow enable <number></pre> <pre>conf t segment <segment name> sflow disable</pre>

conf t server

Activates and deactivates communications services on your IPS device.



CAUTION!

The **conf t server** command enables you to activate the telnet server and HTTP. Telnet and HTTP are *not* secure services. If you enable telnet and HTTP, you endanger the security of your TippingPoint device. Use SSH instead of telnet and HTTPS instead of HTTP when you are conducting normal operations.



CAUTION!

The SMS requires HTTPS communications. If you turn off the HTTPS server, the SMS cannot manage your TippingPoint device.

Required privilege

Admin, Super-User

Subcommands

The **conf t server** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
browser-check	Enables and disables browser checking.	<pre>conf t server browser-check</pre> <pre>conf t server no browser-check</pre>

SUBCOMMAND	DESCRIPTION	USAGE
http	Enables and disables HTTP. You must reboot the device after changing HTTP settings.	<code>conf t server http</code> <code>conf t server no http</code>
https	Enables and disables HTTPS. You must reboot the device after changing HTTPS settings.	<code>conf t server https</code> <code>conf t server no https</code>
ssh	Enables and disables SSH.	<code>conf t server ssh</code> <code>conf t server no ssh</code>
telnet	Enables and disables telnet.	<code>conf t server telnet</code> <code>conf t server no telnet</code>
tls	Enables and disables TLS v1.0, v1.1, and v1.2 separately. By default, TLS v1.1 and TLS v1.2 are enabled. Beginning with TOS v3.9.1, TLS v1.0 is disabled by default.	<code>conf t server tls TLSv10</code> <code>conf t server tls no TLSv10</code> <code>conf t server tls TLSv11</code> <code>conf t server tls no TLSv11</code> <code>conf t server tls TLSv12</code> <code>conf t server tls no TLSv12</code>

conf t service-access

Enables and disables a special remote access user login that can be used by a TippingPoint technical support representative to retrieve diagnostic information.

This special login functions only if you specifically enable it, and it will be deleted after the technical support representative logs out. If you need technical support again in the future, you must reissue the command.



Note

When you issue the `configure terminal service-access` command, the IPS returns the serial number and a “salt” value. You must retain these numbers for the technical support representative.

To manually disable service access, use the `conf t no service-access` command.

Required privilege

Super-User

Usage

```
conf t service-access
```

conf t session

Configures the display of the CLI session on your management terminal.

Except for the timeout option, configure terminal session commands are not persistent and session changes will be lost when you log out. This command is enabled when the SMS manages the device.

Required privilege

Admin, Super-User, Super-User only for **timeout**.

Options

The `conf t session` command uses the following options:

SUBCOMMAND	DESCRIPTION	USAGE
<code>columns</code>	Sets the column width of the terminal session.	<code>conf t session columns <number of columns></code>
<code>more</code>	Enables or disables page-by-page output.	<code>conf t session more</code> <code>conf t session no more</code>
<code>rows</code>	Sets the row height of the session.	<code>conf t session rows <number of rows></code>
<code>timeout</code>	Sets the inactivity timeout. The <code>-persist</code> option applies this value to future sessions for all users as well as the current session.	<code>conf t session timeout <minutes></code> <code>conf t session timeout <minutes> -persist</code>
<code>wraparound</code>	Enables or disables text-wrapping for long text lines.	<code>conf t session wraparound</code> <code>conf t session no wraparound</code>

`conf t sms`

Enables or disables SMS management of the IPS and configures SMS communications.

Required privilege

Admin, Super-User

Options

The `conf t sms` command uses the following options:

SUBCOMMAND	DESCRIPTION	USAGE
<code>[no options]</code>	Enables SMS management.	<code>conf t sms</code>
<code>ip</code>	Sets the IP address and port of the SMS that will manage the IPS.	<code>conf t sms ip <IP address> -port <port></code>
<code>must-be-ip</code>	Enables or disables restriction of SMS management to a specified IP address. Only the SMS with this IP can manage the device.	<code>conf t sms must-be-ip <IP address or CIDR></code> <code>conf t sms no must-be-ip</code>
<code>no</code>	Disables SMS management.	<code>conf t no sms</code>
<code>v2</code>	Enables or disables SNMP v2 communication.	<code>conf t sms v2</code> <code>conf t sms no v2</code>
<code>v3</code>	Enables or disables SNMP v3 communication.	<code>conf t sms v3</code> <code>conf t sms no v3</code>

`conf t snmpv3`

Enables you to configure an SNMPv3 user.

A limit of 31 SNMPv3 users can be created at a time.

Required privilege

Admin

SubcommandsThe `conf t snmpv3` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add	<p>Creates a new SNMPv3 user.</p> <ul style="list-style-type: none"> • -name: SNMPv3 username. • -authkey: (Required) Authentication key or password. If you specify an asterisk (*) for the password, you will be prompted for the password. Minimum of 8 characters. • -authalgorithm: Authentication algorithm. Can be either <code>md5</code> or <code>sha</code>. The default is <code>sha</code>. • -privkey: Privacy key for SNMPv3 responses. If you specify an asterisk (*) for the password, you will be prompted for the password. Minimum of 8 characters. If this option is omitted, the value supplied for <code>-authkey</code> is used. • -privalgorithm: Privacy algorithm for SNMPv3 responses. Can be either <code>des</code> or <code>aes</code>. The default is <code>aes</code>. 	<pre>conf t snmpv3 add -name <username> - authkey <password> -authalgorithm <value> - privkey <key value> -privalgorithm <value></pre>
delete	<p>Removes an SNMPv3 user. No SNMPv3 requests will succeed until a replacement SNMPv3 user is defined.</p>	<pre>conf t snmpv3 delete -name <username></pre>

SUBCOMMAND	DESCRIPTION	USAGE
modify	<p>Modifies an SNMPv3 user.</p> <ul style="list-style-type: none"> • -name: SNMPv3 username. • -authkey: (Required) Authentication key or password. Minimum of 8 characters. • -authalgorithm: Authentication algorithm. Can be either <code>md5</code> or <code>sha</code>. The default is whatever is currently defined if no value is supplied. • -privkey: Privacy key for SNMPv3 responses. Minimum of 8 characters. If this option is omitted, the value supplied for <code>-authkey</code> is used. • -privalgorithm: Privacy algorithm for SNMPv3 responses. Can be either <code>des</code> or <code>aes</code>. The default is whatever is currently defined if no value is supplied. 	<pre>conf t snmpv3 modify -name <username> - authkey <password> -authalgorithm <value> - privkey <key value> -privalgorithm <value></pre>

conf t sntp

Configures SNTP timekeeping options.



CAUTION!

Using external SNTP servers could possibly 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.

Required privilege

Admin, Super-User

Options

The `conf t sntp` command uses the following options:

SUBCOMMAND	DESCRIPTION	USAGE
[no options]	Enables SNTP.	<code>conf t sntp</code>
duration	Sets the interval at which the IPS checks with the time server. A 0 (zero) value causes time to be checked once on boot.	<code>conf t sntp duration <minutes></code>
no	Disables SNTP.	<code>conf t no sntp</code>
offset	If the difference between the new time and the current time is equal to or greater than the offset, the new time is accepted by the IPS. A 0 (zero) value forces time to change every time the IPS checks.	<code>conf t sntp offset <seconds></code>

SUBCOMMAND	DESCRIPTION	USAGE
port	Identifies the port to use for the time server.	<code>conf t sntp port <port></code>
primary	Sets or removes the IP address of your primary SNTP time server.	<code>conf t sntp primary <IP address></code> <code>conf t sntp no primary</code>
retries	Sets the number of retries that the device attempts before declaring the SNTP connection is lost.	<code>conf t sntp retries <number></code>
secondary	Sets or removes the IP address of your secondary SNTP time server.	<code>conf t sntp secondary <IP address></code> <code>conf t sntp no secondary</code>
timeout	Sets the number of seconds that the device waits before declaring the SNTP connection is lost.	<code>conf t sntp timeout <seconds></code>

conf t tacacs-server

Configures a TACACS+ server to be used for remote authentication for the device.

Required privilege

Super-User

Subcommands

The **conf t tacacs-server** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add	<p>Configures a TACACS+ server for remote authentication.</p> <ul style="list-style-type: none"> • priority – Assigns the priority of the remote server. Values are between 1 and 3. • server – Must be an IPv4 or IPv6 address in dotted format. • port – Available ports between 1 and 65535. Default is 49. • shared secret – Case-sensitive string with a maximum length of 63 characters. • authentication type – <ul style="list-style-type: none"> • ASCII • PAP (default) • CHAP • MSCHAP • timeout – Can be between 1 and 15 seconds. Default is 15 seconds. Default is 3 seconds. • attempts allowed – Can be between 1 and 10 attempts. Default is 3 attempts. 	<pre>conf t tacacs-server add -priority <priority-value> <server> [-port <port number>] -secret <shared secret> [-auth-type <ASCII PAP CHAP MSCHAP>] [-timeout <timeout-value>] [-attempts <attempts- value>]</pre>
delete	Removes a TACACS+ server for remote authentication.	<pre>conf t tacacs-server delete -priority <priority-value></pre>
modify	Modifies a TACACS+ server for remote authentication. See the add subcommand for option descriptions.	<pre>conf t tacacs-server modify -priority <priority-value> <server> [-port <port number>] -secret <shared secret> [-auth-type <ASCII PAP CHAP MSCHAP>] [-timeout <timeout-value>] [-attempts <attempts- value>]</pre>

conf t traffic-mgmt

Configures traffic management filters.

Required pPrivilege

Admin, Super-User

Subcommands

The following subcommands can be used to create or modify an existing traffic management filter. If more than one traffic management profile is defined on the system, you must specify the profile name.

The **conf t traffic-mgmt** command uses the following options.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
icmp	Enables SNTP.	<code>conf t traffic-mgmt icmp [-type <ICMP type>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code>
icmp6	Creates an ICMPv6 traffic management filter. You can also specify the ICMPv6 type, or use any to apply the filter to all types.	<code>conf t traffic-mgmt icmp6 [-type <ICMP type>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code>
ip	Creates a IP traffic management filter. You can also specify whether the IP fragments are filtered with the -ip-frag-only or -no-ip-frag-only options.	<code>conf t traffic-mgmt ip [-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code> <code>conf t traffic-mgmt ip [-no-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code>
ip6	Creates a IPv6 traffic management filter. You can also specify whether the IP fragments are filtered with the -ip-frag-only or -no-ip-frag-only options.	<code>conf t traffic-mgmt ip6 [-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code> <code>conf t traffic-mgmt ip6 [-no-ip-frag-only] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code>
tcp	Creates a TCP traffic management filter. You can also specify the TCP source and destination ports.	<code>conf t traffic-mgmt tcp [-srcport <TCP port>] [-destport <TCP port>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code>
udp	Creates a UDP traffic management filter. You can also specify the UDP source and destination ports.	<code>conf t traffic-mgmt udp [-srcport <UDP port>] [-destport <UDP port>] <filter name> [-profile <profile name>] [-srcaddr <source IP address>] [-destaddr <destination IP address>]</code>

The following subcommands can be used only to modify an existing traffic management filter. If more than one traffic management profile is defined on the system, you must specify the profile name.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
allow	Permits all traffic that fits the named filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] allow</code>
block	Blocks all traffic that fits the named filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] block</code>

SUBCOMMAND	DESCRIPTION	USAGE
delete	Deletes the named filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] delete</code>
position	Changes the priority of the filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] position <number></code>
rate-limit	Rate-limits and applies the named action set to all traffic that fits the filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] rate-limit <action set name></code>
rename	Renames the filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] rename</code>
trust	Enables trust of all packets that match the filter.	<code>conf t traffic-mgmt <filter name> [-profile <profile>] trust</code>

conf t tse

Configures settings for the Threat Suppression Engine (TSE).

Required privilege



Admin, Super-User

Subcommands

The `conf t tse` command uses the following options.

SUBCOMMAND	DESCRIPTION	USAGE
adaptive-filter	Sets the adaptive filter mode to automatic or manual.	<code>conf t tse adaptive-filter mode automatic</code> <code>conf t tse adaptive-filter mode manual</code>
afc-severity	Sets the severity of messages logged by the Adaptive Filter Configuration (AFC). Options include: <ul style="list-style-type: none"> <code>critical</code> <code>error</code> <code>warning</code> <code>info</code> 	<code>conf t tse afc-severity <severity></code>
asymmetric-network	Enables or disables asymmetric mode for the TSE. Use asymmetric mode if your network uses asymmetric routing.	<code>conf t tse asymmetric-network enable</code> <code>conf t tse asymmetric-network disable</code>
congestion	Enables or disables notification when traffic congestion reaches a defined threshold.	<code>conf t tse congestion notify enable - threshold <threshold></code> <code>conf t tse congestion notify disable</code>

SUBCOMMAND	DESCRIPTION	USAGE
connection- table	<p>Sets the timeout for the connection tables.</p> <ul style="list-style-type: none"> • non-tcp-timeout: Defines the timeout for non-TCP connections. The range is 30 to 1800 seconds. • timeout: Defines the global connection table timeout. The range is 30 to 1800 seconds. • trust-timeout: Defines the timeout for the trust table. The range is 30 to 1800 seconds. 	<pre>conf t tse connection-table non-tcp- timeout <seconds> conf t tse connection-table timeout <seconds> conf t tse connection-table trust-timeout <seconds></pre>
gzip- compression	<p>Enables or disables GZIP decompression.</p>	<pre>conf t tse gzip-compression enable conf t tse gzip-compression disable</pre>
http-encoded-resp	<p>Specifies inspection of encoded HTTP responses.</p> <ul style="list-style-type: none"> • accelerated: Hardware acceleration is used to detect and decode encoded HTTP responses. • inspect: Enables strict detection and decoding of HTTP responses. • ignore: The device does not detect or decode HTTP responses. • url-ncr: Decodes URL and NCR encoding. 	<pre>conf t tse http-encoded-resp accelerated conf t tse http-encoded-resp inspect conf t tse http-encoded-resp ignore conf t tse http-encoded-resp url-ncr [enable disable]</pre>

SUBCOMMAND	DESCRIPTION	USAGE
http-mode	<p>Enables inspection of all HTTP filters on all TCP traffic. This is useful in configurations that require many more than the eight standard and eight configurable nonstandard HTTP ports. No reboot is necessary after enabling or disabling this feature.</p> <hr/> <p> Note</p> <p>This feature should only be enabled on IPS devices that primarily handle HTTP traffic. Non-HTTP traffic, such as SMB or FTP, can cause performance degradation of the device. Avoid using “well-known” port numbers when mapping HTTP traffic. Using port numbers associated with other protocols or applications could adversely affect the operation of the device. As a best practice, map HTTP port numbers in the range of 49152 – 65535. See http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt for a complete list of registered port numbers.</p>	<code>conf t tse http-mode [enable disable]</code>
ids-mode	<p>Enables or disables IDS mode. When enabled, IDS mode configures the device to operate in a manner similar to an Intrusion Detection System (IDS).</p> <ul style="list-style-type: none"> • Performance protection is disabled. • Adaptive Filtering mode is set to Manual. • Filters currently set to Block are not switched to Permit, and Block filters can be still be set. <hr/> <p> Note</p> <p>IDS mode becomes disabled if you manually enable performance protection or set Adaptive Filtering mode to Automatic.</p>	<pre>conf t tse ids-mode enable conf t tse ids-mode disable</pre>

SUBCOMMAND	DESCRIPTION	USAGE
inspection-offload	<p>Offloads inspection processing from your servers to improve network performance.</p> <ul style="list-style-type: none"> auto: Determines when to use hardware inspection offload. full: Uses hardware inspection offload whenever possible. 	<pre>conf t tse inspection-offload auto conf t tse inspection-offload full</pre>
logging-mode	<p>Sets the logging mode:</p> <ul style="list-style-type: none"> conditional: Improves performance by turning off alert/block logging when the device experiences a specified amount of congestion. This feature is enabled by default. The -threshold setting defines the percentage of packet loss that turns off logging. The -period setting sets the length of time logging remains off. unconditional: The device always logs alerts and blocks, even if traffic is dropped under high load. 	<pre>conf t tse logging-mode conditional - threshold <percentage> -period <seconds> conf t tse logging-mode unconditional</pre>
protection-severity	<p>Sets the protection severity level for log messages (default: warning). Options include:</p> <ul style="list-style-type: none"> critical error warning info 	<pre>conf t tse protection-severity <severity></pre>
quarantine	<p>Sets the quarantine duration. The range is 1 to 1440 minutes.</p>	<pre>conf t tse quarantine <minutes></pre>
reputation nxdomain-response	<p>Responds with NXDOMAIN (name does not exist) to clients that make DNS requests for hosts that are blocked.</p>	<pre>conf t tse reputation nxdomain-response enable conf t tse reputation nxdomain-response disable</pre>
sflow	<p>On NX-Platform devices only, enables or disables global sFlow.</p>	<pre>conf t tse sflow disable conf t tse sflow enable</pre>
sflow collector	<p>On NX-Platform devices only, adds or removes collector IP address. You must manually enable the collector IP address that you add. Two collector IP addresses (either IPv4 or IPv6) are supported for TOS V. 3.6.</p>	<pre>conf t tse sflow collector add <IP Address> <optional Port> conf t tse sflow collector remove <IP Address> <optional Port></pre>

conf t user

Manages user accounts.

This command is enabled when the device is managed by an SMS. For more information about editing user options, see [conf t user options](#).

Required privilege

Super-User



Note

All users can modify their own passwords. Only the super-user can execute other commands on user accounts.

Subcommands

The **conf t user** command uses the following subcommands.



Note

Do not use quotation marks in passwords. Quotation marks are treated differently depending on how you enter them and where you place them within a password and can lead to confusion when attempting to log in to the TippingPoint device.

SUBCOMMAND	DESCRIPTION	USAGE
add	<p>Adds a user. Requires the following options:</p> <ul style="list-style-type: none"> name: Login name. Maximum of 31 characters. auth: Specifies how user is authenticated. role: Privilege level. Privileges can be operator, administrator, or super-user. password: Password. Maximum 32 characters. If you do not create a password, you will be asked if you want to do so. -tech-support: Enables the Technical Support Landing Page when the user logs in to the LSM. (TippingPoint 10 only) 	<pre>conf t user add <username> -password <password> -auth [local RADIUS TACACS +] -role <role></pre>
enable	<p>Enables a user account that has been disabled due to lockout or expiration.</p>	<pre>conf t user enable <username></pre>

SUBCOMMAND	DESCRIPTION	USAGE
modify	Modifies the named user. Requires one or more of the following options: <ul style="list-style-type: none"> • auth: Specifies how user is authenticated. • role: Privilege level. Privileges can be operator, administrator, or super-user. • password: Password. Maximum 32 characters. • -tech-support: Enables the Technical Support Landing Page when the user logs in to the LSM. (TippingPoint 10 only) 	<pre>conf t user modify <username> -password <password> -auth [local RADIUS TACACS +] -role <role></pre>
remove	Removes a user login.	<pre>conf t user remove <username></pre>

conf t user options

Enables you to view or change the security options for all user accounts on the TippingPoint device.

If you use **conf t user** options without any options, it displays the current settings.

Security levels

Security levels are defined as follows:

- Level 0: User names cannot contain spaces. Passwords are unrestricted.
- Level 1: User names must contain at least 6 characters without spaces. Passwords must contain at least 8 characters without spaces.
- Level 2: Includes Level 1 restrictions and requires the following:
 - 2 alphabetic characters
 - 1 numeric character
 - 1 non-alphanumeric character (special characters such as !? and *).

Required privilege

Super-User

Subcommands

The **conf t user options** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
attempt-action	Specifies the action to take when the maximum number of login attempts is reached. <ul style="list-style-type: none"> disable: Requires a super-user to re-enable the user. lockout: Prevents the user from logging in for the lockout-period. notify: Posts a notification to the audit log. 	<pre>conf t user option attempt-action disable conf t user option attempt-action lockout</pre>
expire-action	Specifies the action to take when a user account expires. <ul style="list-style-type: none"> disable: Disables the account. expire: Expires the account. notify: Audits the expiration to the audit log. 	<pre>conf t user option expire-action disable conf t user option expire-action expire conf t user option expire-action notify</pre>
expire-period	Sets the number of days before a password expires. Valid values are 0, 10, 20, 30, 45, 90, 332, and 365. With a value of 0, passwords do not expire.	<pre>conf t user option expire-period <value></pre>
lockout-period	Sets the number of minutes that a user is locked out after the maximum number of unsuccessful login attempts.	<pre>conf t user option lockout-period <value></pre>
max-attempts	Sets the maximum number of login attempts that are permitted before the action specified in attempt-action takes place. Valid values are integers between 1 and 10, inclusive.	<pre>conf t user option max-attempts <value></pre>
security-level	Sets the security level for user names and passwords. Valid values are integers between 0 and 2 inclusive. Refer to the Security Levels section above.	<pre>conf t user option security-level <value></pre>

conf t virtual-port

Configures the network virtual ports.

Required privilege

Admin, Super-User

Subcommands

The **conf t virtual-port** command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
add-row	Configures the physical port, VLAN ID, and CIDR associated with a virtual port. Leaving an option blank sets the value to <i>any</i> .	<code>conf t virtual-port <port name> add-row -port-list <physical port> -vlan-list <VLAN ID> -cidr-list <CIDR address></code>
create	Creates a virtual port and assigns a name. The maximum number of characters is 32. Spaces are not allowed. Use the <code>-description</code> option to add a description.	<code>conf t virtual-port <name> create [-description "<description>"] <zones></code>
delete	Deletes a virtual port.	<code>conf t virtual-port <name> delete</code>
description	Enters a description of the virtual ports.	<code>conf t virtual-port <name> description "<description>"</code>
remove-row	Removes the physical port, VLAN, and CIDR associated with a virtual port, resetting its values to <i>any</i> .	<code>conf t virtual-port <port name> remove-row</code>
rename	Changes the name of the virtual ports.	<code>conf t virtual-port <name> rename <new name></code>
zones	Sets the physical port list and VLAN list for a virtual port.	<code>conf t virtual-port <name> zones <VLAN range></code>

conf t virtual-segment

Configures, updates, or deletes network virtual segments.

Required privilege

Admin, Super-User

Subcommands

The `conf t virtual-segment` command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
delete	Deletes a virtual segment.	<code>conf t virtual-segment <incoming virtual port> <outgoing virtual port> delete</code>
position	Sets the precedence of a virtual segment. Assigning a position of 1 gives the segment topmost precedence.	<code>conf t virtual-segment <incoming virtual port> <outgoing virtual port> [-position <position in list>]</code>
update	Creates, moves, or edits a virtual segment.	<code>conf t virtual-segment <incoming virtual port> <outgoing virtual port> update</code>

conf t vlan-translation

Adds or removes a VLAN translation setting.

For detailed information about the concepts behind VLAN translation, refer to the information in the *Local Security Manager (LSM) User Guide*. Use the **-auto-reverse** flag to automatically create a reverse VLAN translation.

Required privilege

Admin, Super-User

Usage

```
conf t vlan translation add <incoming VLAN ID> <outgoing VLAN ID>
```

```
conf t vlan translation add <incoming VLAN ID> <outgoing VLAN ID> -auto-reverse
```

```
conf t vlan translation remove <incoming VLAN ID> <outgoing VLAN ID>
```

debug

Most debug commands should be used only when you are instructed to do so by TippingPoint technical support.

The following commands can be used to improve performance or diagnose network traffic:

- *debug information*
- *debug np best-effort*
- *debug np mcfilt-regex*
- *debug reputation*
- *debug snmp trap*
- *debug traffic-capture*

debug information

The debug information commands display process and CPU Utilization information.

To configure utilization statistics collection, see *conf t cpu-utilization*.

Required privilege

Super-User

Subcommands

The **debug information** command uses the following subcommands.

SUBCOMMAND	DESCRIPTION	USAGE
dp-ps	Lists all processes.	debug information dp-ps
netstat	Prints network connections and interface statistics.	debug information netstat

SUBCOMMAND	DESCRIPTION	USAGE
ticks	Lists the number of processes currently running in the control and data planes, the maximum CPU usage, and the average CPU usage. The following options provide more information: <ul style="list-style-type: none"> • -details: Provides a more detailed list of processes and CPU usage. • -tiers: Lists processes and CPU usage by tier. 	<code>debug information ticks</code>

debug np best-effort

Best Effort mode protects latency-sensitive applications by not inspecting packets if the latency introduced by inspecting them exceeds the configured threshold. When the latency reaches the specified threshold, permitted traffic is shunted until latency falls to the user-defined recovery percentage. When performing SSL inspection, the latency measure and relief only apply on inspection, and do not apply to the SSL and TCP proxy connections.



Note

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

Required privilege

Super-User

Subcommands

The **debug np best-effort** command uses the following subcommands.

SUBCOMMAND	DESCRIPTION	USAGE
enable	Enables Best Effort mode.	<code>debug np best-effort enable [-queue-latency <microseconds>] [-recover-percent <percent>]</code>
disable	Disables Best Effort mode.	<code>debug np best-effort disable</code>

Options

The **debug np best-effort** command uses the following options.

OPTION	DESCRIPTION	USAGE
-queue- latency	Defines the latency threshold at which Best Effort mode is entered. The default is 1000 microseconds.	<code>debug np best-effort enable -queue-latency <microseconds></code>
-recover- percent	Defines the recovery percentage at which Best Effort mode is exited. The default is 20%; if the latency threshold is 1000 microseconds, the device exits Best Effort mode when latency drops to 200 microseconds (20% of 1000).	<code>debug np best-effort enable -recover-percent <percent></code>

debug np mcfilt-regex

The debug microfilter commands display or clear microfilter regular expression statistics.

Required privilege

Super-User

Subcommands

The **debug np mcfilt-regex** command uses the following subcommands.

SUBCOMMAND	DESCRIPTION	USAGE
clear	Clears microfilter regular expression statistics.	<code>debug np mcfilt-regex clear</code>
show	Displays microfilter regular expression statistics.	<code>debug np mcfilt-regex show</code>

debug reputation

The debug reputation commands are used to manage the IP reputation cache and database.

For more information about reputation, see [conf t reputation](#) and [conf t reputation group](#).

Required privilege

Super-User

Subcommands

The **debug reputation** command uses the following subcommands.

SUBCOMMAND	DESCRIPTION	USAGE
clear-caches	Clears the reputation caches.	<code>debug reputation clear-caches</code>

debug snmp trap

The SNMP trap feature enables you to test SNMP trap functionality for NMS devices.


Required privilege

Super-User

Subcommands

The **debug snmp trap** command uses the following subcommands.

SUBCOMMAND	DESCRIPTION	USAGE
list-ID	Lists all the SNMP traps and their object identifiers (OIDs) on a given IPS device.	<code>debug snmp trap list-ID</code>

SUBCOMMAND	DESCRIPTION	USAGE
test	<p>Sends a test SNMP trap request for the specified OID to an NMS server.</p> <hr/> <p> Note Before using this command, configure the NMS server using the <code>conf t nms trap-destination add <IP address> -port <port number></code> command. Alternatively, configure the NMS server by selecting System > SMS/NMS from the LSM menu.</p>	<code>debug snmp trap test <trap-ID></code>

debug traffic-capture

The traffic capture 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.



Note

When a traffic capture is close to filling the storage card, the traffic capture will stop and a warning message is recorded in the system log.

Required privilege

Super-User

Subcommands

The **debug traffic-capture** command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
list	Returns a list of all traffic captures currently saved on the IPS.	<code>debug traffic-capture list</code>
remove	Removes a saved traffic capture. Use the <code>-f</code> flag to force the removal of the file when a traffic capture is in progress.	<code>debug traffic-capture remove <traffic capture filename></code> <code>debug traffic-capture remove -f <traffic capture filename></code>
start	Initiates a traffic capture. This subcommand can be used in conjunction with the options or with an expression.	<code>debug traffic-capture start [-c <number of packets>] [-C <file size>] [-i <virtual segment>] [-w <file>] <expression></code>

SUBCOMMAND	DESCRIPTION	USAGE
stop	If only one traffic capture is currently in progress, terminates the traffic capture in progress. If two or more traffic captures are currently in progress, you must specify a filename.	<code>debug traffic-capture stop</code> <code>debug traffic-capture stop <filename></code>
stop-all	Stops traffic captures currently in progress.	<code>debug traffic-capture stop-all</code>

Options

The `debug traffic-capture` command uses the following options:

OPTION	DESCRIPTION	USAGE
-c	Defines the number of packets at which the traffic capture will stop. The default is 100.	<code>debug traffic-capture start -c <number of packets></code>
-C	Defines the capture file size at which the traffic capture will stop. The size is defined in bytes. The default is 100000.	<code>debug traffic-capture start -C <file size></code>
-i	Sets the virtual segment on which the traffic will be captured. The default is to capture on all segments. The segment should be defined with the syntax 1A-1B .	<code>debug traffic-capture start -i <virtual segment> <expression></code>
-w	Defines a name for the traffic capture file. Do not include an extension; the TOS will automatically append one. The default file name is the date and time at which the traffic capture was initiated, in the format <code>YYYYMMDD-HHMMSS.pcap</code> .	<code>debug traffic-capture start -w <file></code>

Expression usage

Traffic capture expressions are used to narrow down the types of traffic that are captured. This feature supports true tcpdump expressions. For more information about expression usage, refer to [TCPDUMP expressions](#). The expression must be enclosed in straight quotes (").

Examples

To capture only TCP traffic, enter the following command:

```
debug traffic-capture start 'tcp'
```

To capture all traffic to and from IP address 172.31.255.254, enter:

```
debug traffic-capture start 'host 172.31.255.254'
```

To capture all traffic from that address, enter:

```
debug traffic-capture start 'src 172.31.255.254'
```

To capture all traffic to that address, enter:

```
debug traffic-capture start 'dst 172.31.255.254'
```

To capture all traffic from that address to IP address 10.10.10.10, enter:

```
debug traffic-capture start 'src 172.31.255.254 and dst 10.10.10.10'
```

The following, more complex example captures IPv4 HTTP packets on virtual segment 3A-3B that are transmitting to and from port 80, and only includes packets that contain data. SYN, FIN, and ACK packets are excluded.

```
debug traffic-capture start -i 3A-3B 'tcp port 80 and
((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0'
```

fips

Manages FIPS authentication and key information.

For information on enabling FIPS mode, see [conf t host](#).

Required privilege

Super-User

Subcommands

The **fips** command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
auth delete	<p>Reboots the device and wipes out the user database. Use the -add and -password options to create a new default super user. If you do not specify a username and password, you will be forced to create one via the serial port terminal when the device reboots.</p> <ul style="list-style-type: none"> -add: Defines the new default super-user name. -password: Creates a password for the user. If you specify an asterisk (*) for the password, you will be prompted for the password. 	<pre>fips auth delete fips auth delete -add <user name> -password <password></pre>

SUBCOMMAND	DESCRIPTION	USAGE
keys	<p>Manages generated keys and SSL keys. You must specify two options for managing SSL keys. The first option specifies what to do with the generated keys:</p> <ul style="list-style-type: none"> • keep: Saves the keys when the box is rebooted. • generate: Generates a new key on reboot. • delete: Deletes the generated keys on reboot. <p>The second option specifies the action for the authorized SSL key that was originally obtained with the device. This option does not take effect until after a reboot.</p> <ul style="list-style-type: none"> • keep: Saves the key. • delete: Deletes the default key. • restore-default: Restores the default key. 	<pre>fips keys <keep/generate/delete> <keep/delete/restore-default></pre>
restore-ssl	Restores the default SSL key.	<pre>fips restore-ssl</pre>

halt

Shuts down the IPS device.

Use the **now** option to shut the device down immediately. You can also enter 1 to 3600 seconds for the IPS to wait before initiating the halt sequence. You will be prompted to confirm that you want to halt the device.

Required privilege

Admin, Super-User

Usage

```
halt now
```

```
halt <seconds>
```

high-availability

Either forces the system into layer-2 fallback (also known as Intrinsic HA), or returns it to normal mode (inspection).

Although layer-2 fallback is a system-wide setting, you can configure whether traffic is permitted (default) or blocked on a segment-by-segment basis using the **conf t segment high-availability** command.

This command can also control any bypass modules or zero-power HA devices used by the device.

Required privilege

Admin, Super-User

Subcommands

The **high-availability** command uses the following subcommands.



CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
force	<p>The fallback option forces the TippingPoint into fallback or Intrinsic Network High Availability (INHA) mode.</p> <p>The normal option causes the TippingPoint to return to normal (non-INHA) operation .</p>	<pre>high-availability force fallback high-availability force normal</pre>
zero-power	<p>Forces a ZPHA module into one of two modes:</p> <ul style="list-style-type: none"> normal: Traffic passes through the IPS. bypass: Traffic bypasses the IPS. <p>With no options specified, this command affects the external ZPHA module. Use the -segment option to set the mode of a Smart ZPHA module. Use the -slot option to set the mode for bypass I/O modules (BIOMs). A ZPHA module can be one of the following:</p> <ul style="list-style-type: none"> An external module connected to the device through the ZPHA interface. A Smart ZPHA module on the 2500N, 5100N, or 6100N. A BIOM in the NX-platform models. 	<pre>high-availability zero-power bypass-ips [-segment <segment name>] high-availability zero-power no bypass-ips [-segment <segment name>] high-availability zero-power bypass-ips [-slot <slot number>] high-availability zero-power no bypass-ips [-slot <slot number>] high-availability zero-power bypass-ips [-all] high-availability zero-power no bypass-ips [-all]</pre>

ping

Tests whether a particular IP address can be reached and how long it takes to receive a reply.

You can specify an IP address and a number of packets to send. You can send 1 to 9,999 packets.

Required privilege

Admin, Super-User

Options

The ping command uses the following options:

OPTION	DESCRIPTION	USAGE
-q	Suppresses statistics	ping <IP address> <packet count> -q

OPTION	DESCRIPTION	USAGE
-v	Returns verbose results.	ping <IP address> <packet count> -v
-4	IPv4 traffic only.	ping <IP address> <packet count> -4
-6	IPv6 traffic only.	ping <IP address> <packet count> -6

quarantine

Manages the quarantined traffic and IP addresses.

Required privilege

Admin, Super-User

Subcommands

The **quarantine** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
add	Adds an IP address to the quarantine list. You can also enter an action set that applies to all traffic from that IP address.	quarantine add <IP address> <action set name>
empty	Flushes the quarantine list of all IP addresses.	quarantine empty
list	Displays a list of quarantined IP addresses. You can filter the addresses with the filter subcommand and an IP string, and you can use * as a wildcard, as in 100.*.*.*. Corresponds to the Quarantined Address(es) panel on the Events > Managed Streams > Quarantined Addresses page in the LSM.	quarantine list quarantine list filter <IP address>
remove	Removes an IP address from the quarantine list.	quarantine remove <IP address>

reboot

Reboots the device.

You can specify a delay before the device reboots or execute the reboot immediately. Specify a full system restart with the **-full** flag.

Required privilege

Admin, Super-User

Usage

```
reboot
```

```
reboot <0-3600>
```

```
reboot -full
```

setup

Runs the configuration wizard.

For more information about the configuration wizard, refer to [Initial configuration](#). You can also use this command to run specific sections of the configuration wizard.

Required privilege

Super-User; Super-User and Administrator for setup email-default

Subcommands

The `setup` command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
email- default	Configures the default email contact.	setup email-default
ethernet- port	Configures the ethernet ports.	setup ethernet-port
host	Configures the management port.	setup host
servers	Configures Web, CLI, and SNMP servers.	setup servers
sms	Restricts SMS to a specified IP address.	setup sms
time	Configures time management.	setup time
vlan-translation	Configures VLAN translation.	setup vlan-translation

show

Displays the current status of hardware and software components.

To view the information in the current configuration files, use the `show configuration` command. See [show configuration](#).

Required privilege

Admin, Operator, Super-User



Note

Only users with Super-User role can use the `show log audit` command.

Subcommands

The `show` command uses the following subcommands.




CAUTION!

The square brackets are included in usage examples for clarification purposes only, to indicate which flags and variables are optional. Do not type these brackets when entering a command.

SUBCOMMAND	DESCRIPTION	USAGE
action-sets	Displays all action sets with their settings and contacts.	show action-sets
arp	Displays the link level ARP table.	show arp
autodv	Displays the state of the automatic DV feature.	show autodv
auxdv	Displays the Auxiliary DV packages that are installed on the device.	show auxdv
clock	Displays the time and timezone for the internal clock.	show clock show clock -details
compact-flash	Displays whether the storage card is mounted, and if so, its model number, serial number, revision number, capacity, operation mode, and mount status.	show compact-flash
default-alert-sink	Displays the to and from addresses and SMTP settings for the default alert sink.	show default-alert-sink
default-gateway	Displays the IP address of the default gateway.	show default-gateway
deployment-choices	Displays the deployment modes available for the device.	show deployment-choices
dns	Displays the DNS that the device is using.	show dns
filter	Displays description, status, and DV package information for a filter specified by filter number.	show filter <number>
fips	Displays FIPS and key information. Use the -details option for more information.	show fips show fips -details
health	Displays the disk space, memory usage, power supply status, temperature, fans, I2C bus timeouts, and voltage of the device.	show health show health disk-space show health fan show health i2c-bus show health memory show health power-supply show health temperature show health voltage
high-availability	Displays the current HA status. On NX-platforms, the status of each module slot is displayed as being either <code>normal</code> or <code>IPS bypass</code> .	show high-availability

SUBCOMMAND	DESCRIPTION	USAGE
host	Displays the host management port configurable options and the current settings. Use the <code>-details</code> option for more information.	<pre>show host show host -details</pre>
inspection-bypass	Displays the inspection bypass rules.	<pre>show inspection-bypass show inspection-bypass -details</pre>
interface	Displays network interface data. Specify one of the following: <ul style="list-style-type: none"> • <code>mgmtEthernet</code>: Management interface. • <code>ethernet</code>: Port specifier (1A, 1B, etc.). • 	<pre>show interface mgmtEthernet show interface ethernet</pre>
license	Shows the license status for the TOS, Digital Vaccine, and IP Reputation.	<pre>show license</pre>
log	Displays a log file. Only users with super-user privileges can view the audit log.	<pre>show log alert show log audit show log block show log quarantine show log summary show log system</pre>
login-banner	Displays the consent banner that entrants see when accessing a private website.	<pre>show login-banner</pre>
mfg-info	Displays manufacturing information, including the device serial number and MAC address.	<pre>show mfg-info</pre>

SUBCOMMAND	DESCRIPTION	USAGE
np	Displays the network processor statistic sets.	<pre>show np engine show np engine filter show np engine packet show np engine parse show np engine reputation dns show np engine reputation ip show np engine rule show np general show np general statistics show np mcfilt-rule-stats show np packet-size show np packet-size -details show np protocol-mix show np reassembly show np reassembly ip show np reassembly tcp show np rule-stats show np softlinx show np tier-stats</pre>
ntp	Displays the current NTP settings.	show ntp
policy counters	Displays the counters for Total, Invalid, Alert, and Blocked.	show policy counters
profile	Displays detailed information about a named profile. Enclose the name of the profile in quotes "".	show profile "<profile name>"
protection-settings	Displays category settings.	show protection-settings -profile <profile name>
ramdisk	Displays the RAM disk status.	<pre>show ramdisk files show ramdisk stats</pre>
rate-limit-speeds	Displays all valid rate limit speeds.	show rate-limit-speeds
reputation	Displays the reputation groups and filters.	<pre>show reputation show reputation filter <filter name> show reputation groups</pre>
reputation lookup	Looks up an address in the reputation database.	show reputation lookup <IP address>
routes	Displays the configured routes.	show routes

SUBCOMMAND	DESCRIPTION	USAGE
server	Displays the servers running on the device.	show servers
service-access	Displays the status of service access to the device.	show service-access
session	Displays the current session settings.	show session
slot	Displays slot configuration, including the module type currently in the slot.	show slot
sms	Indicates whether an SMS is managing the device and displays information about the SMS.	show sms
snmpv3	Displays the current SNMPv3 settings.	show snmpv3
sntp	Displays the current SNTP settings.	show sntp
stacking	Displays stacking status information.	show stacking
tacacs-server	Displays operational information about servers configured for TACACS+ remote authentication.	show tacacs-server
timezones	Displays the available time zones.	show timezones
traffic-mgmt	Displays all traffic management filters defined in a traffic management profile. You must specify the profile by name unless there is only one profile on the device.	show traffic-mgmt -profile <profile name>
tse	Displays information and settings regarding the Threat Suppression Engine.	show tse adaptive-filter top-ten show tse connection-table blocks show tse connection-table timeout show tse connection-table trusts show tse rate-limit streams
user	Displays the user login accounts on the TippingPoint device.	show user show user -details
version	<p>Displays the version of the TOS software running on the IPS device including the versions of all installed DVs (base DV, ThreatDV, Auxiliary DVs).</p> <hr/> <p> Note</p> <hr/> <p>To view any custom DV Toolkit package that is installed on the device, refer to the Update Summary page on the LSM.</p>	show version
virtual-port	Displays information about a virtual port.	show virtual-port <port number>

SUBCOMMAND	DESCRIPTION	USAGE
virtual- segments	Displays all of the virtual segments configured on the device.	show virtual-segments

show configuration

Shows persistent configuration settings on the IPS.

Show configuration commands can be used to feed configuration information back to the console. Without options, the command shows the system's configuration.



Note

You can use the abbreviation **show conf**. Also, you can define an alias using the **alias** command.

Required privilege

Admin, Operator, Super-User

Subcommands

The **show configuration** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
action-set	Lists all action sets that have been defined for this device. You can also view a single action set by specifying the action set name.	show conf action-set show conf action-set <action set name>
authentication	Displays the remote authentication configuration.	show conf authentication
autodv	Shows configuration settings for the automatic update service for Digital Vaccine packages.	show conf autodv
category-settings	Shows configuration settings for filter categories. You can also view the settings for a single profile by specifying the profile name.	show conf category-settings show conf category-settings -profile <profile name>
clock	Shows time zone and daylight savings time settings.	show conf clock
compact-flash	Shows the storage card operation mode.	show conf compact-flash
default-alert-sink	Shows the default email address to which attack alerts will be directed.	show conf default-alert-sink
default-gateway	Shows the device default gateway.	show conf default-gateway
email-rate-limit	Shows the maximum number of email notifications the system sends every minute. The minimum is 1; the maximum is 35.	show conf email-rate-limit
filter	Shows the filter data for a specific filter, identified by filter number.	show conf filter <number>

SUBCOMMAND	DESCRIPTION	USAGE
high-availability	Shows high availability configuration settings.	<code>show conf high-availability</code>
host	Shows the host name and location.	<code>show conf host</code>
inspection-bypass	Shows the current inspection bypass rule configuration.	<code>show conf inspection-bypass</code>
interface	<p>When used without qualifiers, shows configuration of all ports.</p> <ul style="list-style-type: none"> ethernet: Shows Ethernet port information. Without options, this subcommand shows the status of all Ethernet ports. Use port specifiers (1A, 2A, etc.) to view the status of a single port. mgmtEthernet: Shows Management Ethernet port information. settings: Shows the persistent configuration settings for MDI-detection. 	<code>show conf interface</code> <code>show conf interface ethernet</code> <code>show conf interface mgmtEthernet</code> <code>show conf interface settings</code>
lcd-keypad	Shows the configuration setting for the LCD keypad.	<code>show conf lcd-keypad</code>
log	Shows log configuration.	<code>show conf log</code> <code>show conf log audit-log</code> <code>show conf log snmp-add-event-info</code>
login-banner	Displays the consent banner that entrants see when accessing a private website.	<code>show conf login-banner</code>
monitor	Shows the persistent configuration of monitor thresholds.	<code>show conf monitor</code>
nms	Shows the NMS settings.	<code>show conf nms</code>
notify-contacts	Shows the notification contacts and settings.	<code>show conf notify-contacts</code>
ntp	Shows the NTP configuration settings.	<code>show conf ntp</code>
port	Shows the configuration of all ports on the IPS.	<code>show conf port</code>
profile	Lists all profiles that have been configured on the device. You can view an individual profile by including the profile name.	<code>show conf profile</code> <code>show conf profile <profile name></code>
protection-settings	Shows the protection settings. You can also view the settings for a single profile by specifying the profile name.	<code>show conf protection-settings</code> <code>show conf protection-settings -profile <profile name></code>

SUBCOMMAND	DESCRIPTION	USAGE
radius-server	Shows the properties of any RADIUS servers configured for remote authentication.	show conf radius-server
ramdisk	Shows the RAM disk configuration.	show conf ramdisk
remote	Shows any RADIUS or SMS servers configured for remote authentication.	show conf remote
remote-syslog	Shows the remote syslog configuration and the IP address of the remote log.	show conf remote-syslog
reputation	Shows the configuration of reputation filters and groups, and of the IP Reputation feature.	show conf reputation show conf reputation group show conf reputation filter
segment	Shows the segment configuration. You can view an individual segment by including the segment name.	show conf segment show conf segment <segment name>
server	Shows the device server configuration.	show conf server
service-access	Shows whether service access is enabled or disabled.	show conf service-access
session	Shows the session timeout settings. Use show session to view the current session configuration.	show conf session
sms	Shows if SMS is enabled and other SMS configuration settings.	show conf sms
snmpv3	Shows whether an SNMPv3 user has been defined.	show conf snmpv3
sntp	Shows the SNTP configuration.	show conf sntp
tacacs-server	Shows the properties of any TACACS+ servers configured for remote authentication.	show conf tacacs-server
traffic-mgmt	Shows the traffic management configuration.	show conf traffic-mgmt
tse	Shows the TSE information, including connection table timeout, sFlow (NX-platform devices only), asymmetric network setting, adaptive aggregation threshold, adaptive filter mode, and IDS mode.	show conf tse
user	Shows user options. Use the -details option to view additional information.	show conf user show conf user -details

SUBCOMMAND	DESCRIPTION	USAGE
virtual-port	Shows virtual port configuration. To show the configuration of a specific virtual port, specify the virtual port name.	show conf virtual-port show conf virtual-port <virtual port name>
virtual-segments	Shows the configuration of the virtual segments.	show conf virtual-segments
vlan-translation	Shows the VLAN translation configuration	show conf vlan-translation

show np tier-stats

Displays throughput and efficiency across the different inspection tiers of this device. Use this information to diagnose certain performance-related issues. Run this command on a stacking device to display its stacking statistics.

Required privilege

Admin, Operator, Super-User

Subcommands

None.

Usage

This is the default output for an IPS device with stacking enabled.

```

-----
Stack : Segment Ports
-----
Segment Rx Mbps           =          111.0  (111.0)
Segment Tx Mbps           =          111.0  (111.0)
Stack Balance (A/B/C)     =          99.5% [93.5%]
  drgproto208 Rx Mbps     =           40.0  (40.0)
  drgproto212 Rx Mbps     =           40.1  (40.1)
  dragproto216 Rx Mbps    =           39.5  (39.5)
Segment ratio to tier 1   =          33.4% [32.4%]
-----
Stack : Stack Ports
-----
Stack Rx Mbps             =           79.6  (79.6)
Stack Tx Mbps             =           79.6  (79.6)
Stack Rx > Stack Tx Mbps  =            0.0  (0.0)
Stack Rx > Seg Tx Mbps    =           79.6  (79.6)
Stack Rx > Tier 1         =            0.0  (0.0)
-----
Tier 1:
-----
Rx Mbps                   =           40.0  (40.0)
Tx Mbps                   =           39.8  (39.8)
Rx packets/sec            =       32,511.0  (32,511.0)
Tx packets/sec            =       32,384.0  (32,384.0)
Bypass packets/sec       =            0.0  (0.0)
Bypass to Rx ratio        =            0.0%
A/B/C Balance             =          99.4% (A: 13,429.0 B: 13,731.0 C: 13,698.0)
Utilization                =            0.5% ( 0.5%)
Ratio to next tier         =          100.0% [ 82.8%]
-----

```

```


Tier 2:
-----
Tx trust packets/sec      =          0.0 (0.0)
Utilization                =          0.1% ( 0.1%)
Ratio to next tier         =        100.0% [ 98.2%]
-----

Tier 3:
-----
Rx Mbps                    =          36.6 (37.1)
Rx packets/sec            =       30,140.0 (30,951.0)
Tx trust packets/sec      =          0.0 (0.0)
Utilization                =          0.1% ( 0.1%)
Ratio to next tier         =          0.0% ( 0.0%)
-----

Tier 4:
-----
Rx Mbps                    =          0.0 (0.0)
Rx packets/sec            =          0.0 (0.0)
Rx due to:
  Trigger match           =          0.0% ( 0.0%)
  Reroute                 =          0.0% ( 0.0%)
  Protocol decode         =          0.0% ( 0.0%)
  TCP sequence            =          0.0% ( 0.0%)
Tx trust packets/sec      =          0.0 (0.0)
Utilization                =          0.0% ( 0.0%)
Ratio tier 4 to deep       =          0.0% ( 0.0%)

```

INSPECTION TIER	DESCRIPTION
Stack : Segment Ports	<p>This inspection tier presents the total I/O module throughput for the network segment device as well as the receive rates from the I/O module to each stack member. When stacking is enabled, the following information is displayed:</p> <ul style="list-style-type: none"> • <code>Segment Rx Mbps</code> displays the aggregate received traffic from all network segments on this device. • <code>Segment Tx Mbps</code> displays the aggregate traffic transmitted from all network segments on this device. • <code>Stack Balance (A/B/C)</code> displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. For devices that are in Intrinsic HA L2FB, the Rx rate is zero, and this zero value is included in the load balance calculation. This statistic is similar to the <code>A/B/C Balance</code> percentage in Tier 1. • <code><host n> Rx Mbps</code> displays the traffic balanced from this device's network segments to the other devices in the stack. <p>Note that the number of packets going through each host is flow-based, so it is not uncommon to see a slight difference between them.</p> <ul style="list-style-type: none"> • <code>Segment ratio to tier 1</code> displays the percentage of traffic being inspected by this device as a ratio of the segment Rx traffic.

INSPECTION TIER	DESCRIPTION
Stack : Stack Ports	<p>This inspection tier presents stacking port throughput, including through traffic and return traffic rates.</p> <p>When stacking is enabled, the following information is displayed:</p> <ul style="list-style-type: none"> • <code>Stack Rx Mbps</code> displays the aggregate received traffic from both stacking ports. • <code>Stack Tx Mbps</code> displays the aggregate traffic that is transmitted from both stacking ports. • <code>Stack Rx > Stack Tx</code> displays the total amount of transit or through traffic on the stacking ports, for example, traffic received on Stack port 1 which is forwarded by the switch to stack port 2. • <code>Stack Rx > Seg Tx</code> displays the amount of return traffic coming in on a stacking port that is returning to the outbound network segment. • <code>Stack ratio to tier 1</code> displays the percentage of traffic being inspected by this device as a ratio of the stack Rx traffic.
Tier 1	<p>This inspection tier is responsible for inspection bypass rules and Intrinsic HA L2FB, which prevents network traffic from going to the next tier. This tier is also responsible for the rate limiter, inspection bypass rules, jumbo packet shunting, and the hardware watchdog timer.</p> <ul style="list-style-type: none"> • <code>Rx Mbps</code> and <code>Tx Mbps</code> and <code>Rx packet/sec</code> and <code>Tx packet/sec</code> indicate how much traffic is entering the inspection engine from all the segments. A value in parentheses () represents the high-level watermark and a value in brackets [] represents the low-level watermark since the IPS was powered on or the tier statistics were reset. <hr/> <p> Note Use the <code>clear np tier-stats</code> CLI command to reset tier statistics.</p> <hr/> <ul style="list-style-type: none"> • <code>Bypass Mbps</code> displays the current and maximum throughput that matches an inspection bypass rule. Traffic that matches an inspection bypass rule does not count towards the IPS inspection limits. • <code>A/B/C Balance</code> displays how well the flows are being balanced between the XLRs: <ul style="list-style-type: none"> • <code>100%</code> indicates an even balance across all three XLRs, which is ideal. • <code>0%</code> means that all traffic is going to a single XLR. <p>Note that the number of packets going through each XLR is flow-based, so it is not uncommon to see a slight difference between them.</p> • <code>Utilization</code> displays the percentage of rated system throughput and the percentage of traffic to the next tier. • Inspection bypass rules reduce the value of both <code>Utilization</code> and <code>Ratio to next tier</code>.
Tier 2	<p>This inspection tier is responsible for load-balancing TCP flows through the KS threads. This tier is also responsible for managing traffic management trusts and block filters to prevent traffic from proceeding to the next tier.</p> <p><code>Ratio to next tier</code> accounts for Traffic Management Trust and Block rules and Traffic normalization filters. TCP ACKs are trusted by default, and reduce the Tier 2 ratio to the next tier.</p>
Tier 3	<p>This inspection tier is responsible for finding suspicious traffic that needs to undergo deep inspection. This tier is also responsible for IPv6 + GRE and Mobile IPv4 tunnels, IP reassembly, maintaining the connection table, and TCP state tracking. If triggers are found, this tier determines what filters need to be checked against the packet or flow, turns on soft-reroute for the flow, and, if necessary, sends the packet or flow for deep packet inspection.</p> <p>This section displays how much traffic the KS threads and IP reassembly inspect:</p> <ul style="list-style-type: none"> • <code>Ratio to next tier</code> shows the percentage of traffic that needs TCP reassembly or is suspicious (matched a trigger).

INSPECTION TIER	DESCRIPTION
Tier 4	<p>This inspection tier is responsible for TCP reassembly and threat verification which includes header-based checks, protocol decoders, content search, and regular expression matching. This tier is also responsible for action handling, regardless of whether the packet is dropped, rate limited, or rate limited in the connection table.</p> <ul style="list-style-type: none"> • <code>Rx due to</code> indicates why traffic is going to deep packet inspection: <ul style="list-style-type: none"> • <code>Trigger match</code>. Displays the percentage of traffic that matched a trigger. • <code>Rx due to Reroute</code>. When a packet matches a trigger the following packets which belong to the same flow are required for threat verification. • <code>TCP sequence</code>. If traffic cannot be reordered by KS threads using loopy packet, it must go to Tier 4 for reordering. • <code>Ratio to next tier</code>. Displays the percentage of traffic that matched a filter, regardless of the Action Set. <p>Tuning is required if congestion is occurring or if an IPS is being operated close to its maximum rated throughput. The deeper a flow is inspected, the more processing is required. Therefore, the most performance gains that can be attained by optimizing the KS threads at this level (Tiers 3 and 4). The three most process-intensive operations are:</p> <ul style="list-style-type: none"> • IP reassembly • Threat verification • TCP packet reordering

show stacking

Enter this command to show stacking status information.

Required privilege

Admin, Operator, Super-User

Use

The following example shows the default output for a device that does not support stacking. To support stacking, the device must be a supported model running TippingPoint Operating System (TOS) v3.9.0 (or later).

```
ips# show stacking
This device does not support stacking.
```

The following example shows the default output for a supported device that is not a member of the stack. Unlike the SMS, the device does not validate the presence of the 40 GbE QSFP+ NX module in slot 4.

```
ips# show stacking
Stack member summary
-----
Stacking enabled           : No
Stacking active           : No
Stack member state        : Device Ready to Inspect - Normal
Stack master               : No
```

The following example shows the output for the same device after adding it to a stack of three devices.

```
ips# show stacking
Stack member summary
-----
Stacking enabled           : Yes
```

```
Stacking active           : Yes
Stack member state      : Device Ready to Inspect - Normal
Stack master           : No

Stack summary
-----
Number of devices configured in stack : 3
Number of devices required in stack  : 2
Stack state              : Stack Ready to Inspect - Normal

Device Hostname          Advertised State
-----
device01 (local host)    Device Ready to Inspect - Normal
device02 (master)        Device Ready to Inspect - Normal
device03                  Device Ready to Inspect - Normal
```

Reference

PARAMETER	INFORMATION
Stacking enabled	Indicates whether stacking is enabled on the device.
Stacking active	Indicates whether stacking is currently functioning.
Stack member state	Indicates the current working state of this device on the stack.
Stack master	Indicates whether this device manages the state of the stack.
Number of devices configured in stack	Indicates the number of TippingPoint IPS devices that are connected together through the stacking bus.
Number of devices required in stack	Indicates the minimum number of devices that must be available to the stack for normal operation. If the number of normal devices falls below this threshold, the stack goes into Intrinsic HA L2FB.
Advertised state	Indicates the state that the device advertises to the stack master.

snapshot

Creates and manages snapshots of the device configuration settings.

These snapshots can be applied to other devices, to roll back to previous configurations, and to back up the current configuration.

Required privilege

Admin, Super-User

Subcommands

The **snapshot** command uses the following subcommands:

SUBCOMMAND	DESCRIPTION	USAGE
create	Creates a snapshot with the given name.	snapshot create <snapshot name>
list	Lists all snapshots saved on the device.	snapshot list

SUBCOMMAND	DESCRIPTION	USAGE
remove	Deletes the named snapshot.	<code>snapshot remove <snapshot name></code>
restore	Replaces the current configuration settings with the settings in the named snapshot. This process can take some time and will require a reboot of the device.	<code>snapshot restore <snapshot name></code>

Options

The **snapshot** command uses the following options.



Note

Including Reputation addresses and ThreatDV can generate a very large snapshot file.

OPTION	DESCRIPTION	USAGE
-include-reputation	When this flag is included in the command, the snapshot includes the files from the ThreatDV package in the snapshot.	<code>snapshot create -include-reputation</code>
-include-manual-entries	When this flag is included in the command, the snapshot includes the user-defined IP and DNS reputation entries in the snapshot.	<code>snapshot create -include-manual-entries</code>
-include-network	When this flag is included in the command, the snapshot includes management port configuration information.	<code>snapshot create -include-network</code>
-exclude-network	When this flag is included with the snapshot restore command, the snapshot excludes management port configuration information during the restore process.	<code>snapshot create -exclude-network</code>

tech-support-report

Polls the IPS for statistics and other relevant information and sends the information as a clear-text email message to the specified TippingPoint Technologies email address.

You should execute this command only when requested by TippingPoint support personnel.

Use the **-include-snapshot** option to include a system snapshot in the report.

The command can take up to a minute to execute. The default email options must be configured with the **setup** command for the email transfer to succeed.

Required privilege

Admin, Super-User, Operator

Usage

```
tech-support-report <email address> "<description>"
```

```
tech-support-report <email address> "<description>" -include-snapshot
```

TCPDUMP expressions

The debug traffic capture command uses TCPDUMP expressions to define the traffic captures.

For more information about TCPDUMP expressions, see the TCPDUMP man page at <http://www.tcpdump.org/>.