5.0.0

TippingPoint™ Threat Protection System

SSL Inspection Deployment Guide

Actionable threat defense against known and zero-day attacks

Legal and notice information

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint Threat Protection System SSL Inspection Deployment Guide

Contents

About this guide

This guide is intended for network administrators and specialists who monitor and manage system security. The information provided describes how to protect inbound SSL traffic by implementing SSL inspection for TippingPoint Threat Protection System (TPS) devices.

This section covers the following topics:

- *Related documentation* on page 1
- *Product support* on page 1

Related documentation

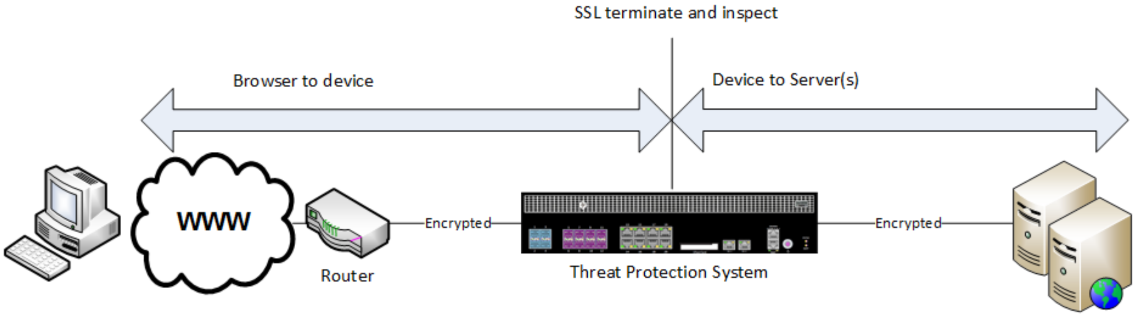
A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at *https://tmc.tippingpoint.com*. The documentation generally includes installation and user guides, command line interface (CLI) references, safety and compliance information, and release notes.

Product support

Information for you to contact product support is available on the TMC at *https://tmc.tippingpoint.com*.

Overview

The TippingPoint Threat Protection System (TPS) provides in-line, real-time threat protection for inbound SSL traffic to your servers. The TPS manages its own private keys and certificates from the servers it is securing; these can either be stored on the device itself or accessed at run-time from the Security Management System (SMS).



With access to the server certificate and private key, the TPS is a transparent proxy that receives and decrypts SSL data, inspects it using the Threat Suppression Engine, and then encrypts it before sending it to the actual destination.

Additional considerations

When deploying SSL inspection, consider the following:

Consideration	Description
Inbound IPv4 traffic only	The TPS inspects inbound IPv4 traffic, including HTTP and HTTPS traffic. Inbound SSL inspection does not support: • IPv6 traffic, including IPv4 over IPv6 tunneling. • Outbound IPv4 traffic and IPv6 traffic.
Tunneled traffic	Supported SSL encapsulations: • GRE (Generic Routing Encapsulation) * • IPv4 (IP-in-IP) • One layer of tunneling only for both GRE and IPv4-in-IPv4 SSL inspection does not include support for GTP or IPv6 encapsulations. * GRE support includes the mandatory GRE fields. Optional GRE key configuration is also supported, but the key needs to be the same value for both directions. Other optional GRE fields, such as GRE sequence number, are not supported.
Quarantine hosts and redirecting HTTP traffic to another site	When configuring an Action Set to quarantine hosts, if you also configure the response to HTTP traffic sent from quarantined host to "redirect to the following site," HTTP traffic from the quarantined host is redirected but HTTPS traffic is not redirected.
Filter Precedence	The TPS processes filters in the following order of precedence: 1. Inspection Bypass Rules 2. Traffic Management Filters 3. RepDV 4. Quarantine 5. Digital Vaccine Filters

Consideration	Description
	When encrypted traffic is routed through the device and: • SSL inspection is configured, the TPS order of precedence applies to the decrypted traffic. The TPS does not quarantine or Digital Vaccine filter traffic without first decrypting the traffic. • SSL inspection is not configured, the device performs Inspection Bypass, Traffic Management, RepDV, and quarantine filtering against the encrypted traffic. Digital Vaccine filters are applied, but do not match against encrypted payload.
Non-encrypted traffic when SSL is configured	• The TPS will drop non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile but send cleartext traffic before starting an SSL handshake (as some protocols allow via *STARTTLS*). • The TPS device will drop non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile due to the lack of an SSL handshake.
Traffic Management filters - Trust action	The TPS continues to proxy the SSL session between the client and the server when HTTPS traffic matches a traffic management filter which is set to Trust (incoming traffic is trusted and not inspected).
Packet trace	Packet Trace as an action includes the decrypted traffic.
Traffic capture	Traffic capture by tcpdump does not include the decrypted contents.
L2FB/ZPHA	When the TPS enters Layer-2 Fallback (L2FB) or Zero Power High Availability (ZPHA), the proxied SSL sessions are cleared.

Requirements

Make sure your environment meets the following requirements:

- SSL certificate and private key from the server that hosts the SSL/TLS compliant application.
- A supported TippingPoint TPS device with an SSL Inspection license. With TOS v5.0.0 and later, SSL inspection is supported on TX Series (8200TX and 8400TX), 2200T, and Virtual TPS (performance image only, with RDRAND instruction recommended) security devices. For information about how to deploy the vTPS for SSL inspection, see the *vTPS Deployment Guide* on the TMC at *https://tmc.tippingpoint.com*.

  Note: SSL inspection is not supported on the TippingPoint 440T TPS security device.

- Cipher suite support – SMS v5.0.0 and later is capable of configuring the following ciphers if your TOS supports them. Older versions of the TOS may have limited cipher support. Profile distribution extended status alerts you to any errors:
  - Protocols:
    - TLS v1.2 (enabled by default)
    - TLS v1.1 (enabled by default)
    - TLS v1.0 (enabled by default)
    - SSL v3.0 (disabled by default)

    Note: TLS Heartbeat Extension (*https://tools.ietf.org/html/rfc6520*) is not supported.

  - Key exchange:
    - Ephemeral Elliptic Curve Diffie-Hellman with RSA signatures (ECDHE-RSA).

      The ECDHE-RSA cipher suite extends SSL inspection capability to Perfect Forward Secrecy (PFS). ECDHE-RSA is enabled by default.

    - RSA (enabled by default)
  - Authentication:
    - RSA (enabled by default)
  - Encryption:
    - AES256 (enabled by default)
    - AES128 (enabled by default)
    - 3DES (enabled by default)

        - DES (disabled by default)
    - MAC:
        - SHA384 (enabled by default)
        - SHA256 (enabled by default)
        - SHA1 (enabled by default)
- VLAN translation cannot be used in conjunction with SSL inspection.
- SSL inspection requires Asymmetric Network mode to be disabled on the device. By default, the Asymmetric Network option is disabled.

Manage SSL inspection from the SMS

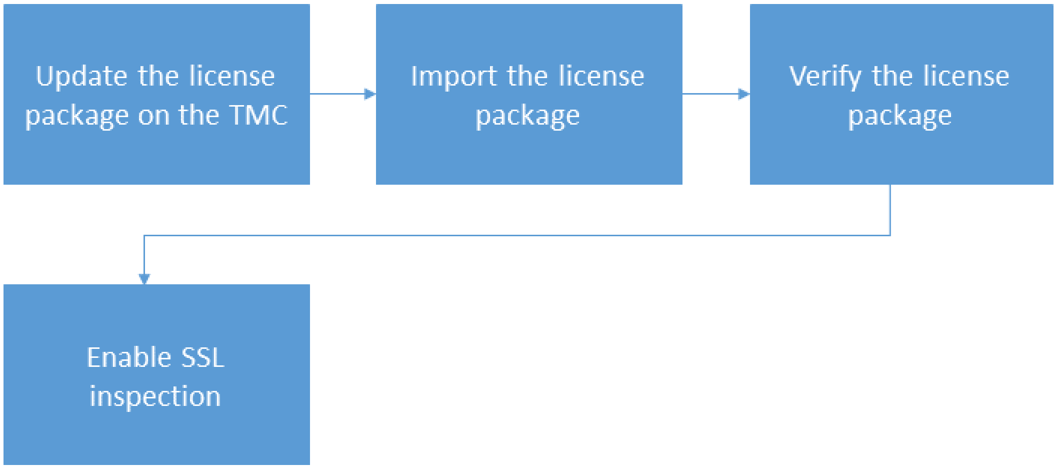
From the SMS, you can set up and manage SSL inspection. For more information, see the following sections.

Before you configure SSL inspection

Before you configure SSL inspection, update the SMS settings for SSL inspection.

Important: To inspect SSL sessions, the device must be licensed for SSL inspection.

The process is:


Update the license package on the TMC
Import the license package
Verify the license package
Enable SSL inspection

The following information provides more details:

- *Update the license package* on page 7
- *Import the license package* on page 8
- *Verify the license package* on page 8
- *Enable SSL inspection* on page 9

Update the license package

Update the license package to assign an available SSL inspection license to any supported TPS security device. SSL inspection is licensed separately. To request an SSL Inspection license, contact your sales representative.

Note: Manage your license package by using the License Manager on the TMC at *https://tmc.tippingpoint.com/TMC/*. When you log on to the TMC, the License Manager is under **My Account > License Manager**.

Import the license package

If the SMS is configured to automatically download Digital Vaccine (DV) filters from the TippingPoint TMC, the SMS also downloads the most recent license package within 30 minutes. If your SMS is connected to the TMC, you do not need to manually import the license package.

To manually import the license package

1. Log on to the TMC at *https://tmc.tippingpoint.com*.
2. In the navigation bar, click **My Account** and select **TippingPoint License Package**.
3. Download and save the license package to your local system.
4. Log in to the SMS.
5. In SMS tools, click **Admin**.
6. In the left navigation pane, click **Licensing**.
7. On the TippingPoint Licensing Package panel, click **Import**.

Verify the license package

Verify the SSL inspection license is enabled on each TPS device.

Important: To enable the SSL inspection license, you must reboot the device.

To verify the license package

1. In the SMS client, open the Licensing screen in the Admin Workspace.

   From the Licensing screen, you can view the Licensing Details panel.

   The Licensing Details panel displays status and information for the license on each managed device. Details include device name and IP address, next license expiration date, and license status.

2. To view licensed capabilities for an individual device, select the expand button next to the device.

   If the SSL Inspection feature indicates:

   - **Reboot required**, reboot the device to complete the installation.
   - **Deny**, install a license package with SSL inspection assigned to the device. See *Update the license package* on page 7 for more information.

Enable SSL inspection

From the SMS, enable SSL inspection to activate SSL inspection on the device. While SSL inspection is disabled, you can configure SSL inspection on the device.

Important: To enable SSL inspection, the license package on the device must allow SSL inspection. If the device is not licensed for SSL inspection, the SMS displays a notification.

To enable SSL inspection

1. Select **Devices > All Devices >** device-name **> Device Configuration**.
2. Click the **Edit > Device Configuration**.

   The Device Configuration dialog opens.

3. Click the SSL Inspection property sheet.
4. To view the SSL ciphers that are supported by a device, click **View Supported SSL Ciphers**.

   The Supported SSL Ciphers dialog box is displayed.

5. Configure the following options:

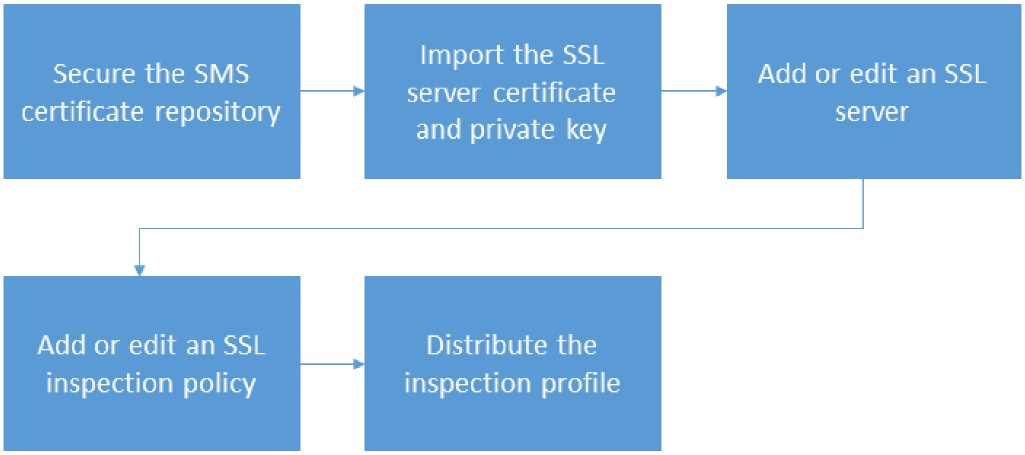
   ◦ **SSL Inspection**. Select this option to enable the device to inspect SSL sessions. If the checkbox is grayed, verify the license package assigns an SSL inspection license to the device.

   ◦ **Persist Private Keys**. Select this option to persist private key information in the system keystore of the device. By default, a managed device automatically retrieves private key information from the SMS but does not persist the information when the device reboots.

Configure SSL inspection

Configure SSL inspection to specify the SSL sessions you want the TPS device to inspect. The TPS cannot effectively inspect the encrypted payload of SSL traffic that does not match the SSL inspection profile.

The process is:


Secure the SMS certificate repository
Import the SSL server certificate and private key
Add or edit an SSL server
Add or edit an SSL inspection policy
Distribute the inspection profile

The following information provides more details:

- *Secure the SMS certificate repository* on page 10
- *Import the SSL server certificate and private key* on page 11
- *Add or edit an SSL server* on page 12
- *Add or edit an SSL inspection policy* on page 13
- *Distribute the inspection profile* on page 14

Secure the SMS certificate repository

Secure the SMS certificate repository by providing a password. If a password already exists for the SMS certificate repository, you can skip this step.

The SMS certificate password protects the private keys in the SMS certificate repository with encryption. When you import certificates with private keys into the SMS certificate repository, the SMS always prompts for the SMS certificate password.

Once you set up the SMS certificate password, keep in mind:

- The SMS does not store the SMS certificate password. You must enter this password every time the SMS server restarts.
- There is no way to recover a lost password. If you lose your password, you must reset your password. Resetting your password deletes all of your private keys in the SMS certificate repository. To resolve this issue, reimport all of your private keys.

To secure the SMS certificate repository

1. Go to **Admin** > **Certificate Management**.
2. Click **Setup Encryption**.

3. Enter and confirm a password.
4. Click **OK**.

   A new RSA key pair is generated after password validation. The new password encrypts the private key of this key pair which encrypts your private keys in your SMS certificate repository.

Import the SSL server certificate and private key

From the SMS, import both the SSL server certificate and its private key from the server of interest. The SMS performs basic validation on the status of the certificate itself.

The SMS copies the device certificate to each device that is configured to use the certificate along with the corresponding private key.

Optionally, you can configure each device to persist private key information in the system keystore. For more information, see *Enable SSL inspection* on page 9.

To import the SSL certificate and private key

1. Select **Admin** > **Certificate Management** > **Certificates**.
2. In the Certificates panel, click **Import** to import a new SSL certificate.

   To update an existing SSL certificate, select the certificate from the list, then click **Import**.

3. Enter the certificate name.

   (Best Practice) Follow a naming convention so that you can easily and reliably assign the correct certificate to an SSL server.

4. Click **Browse** to locate the file.
5. Select the certificate format, either **Base64 Encoded Certificate (PEM)** or **Encrypted Private Key and Certificate (PKCS12)**.

   When selecting:

   - **PEM/DER** format, the private key must be imported in a separate file. Be sure to select the **Include a Private Key** checkbox, and then browse to the private key file. If the private key is encrypted, you must also enter the appropriate password in the Password box.
   - **PKCS12** format, you must enter the appropriate password in the Password box.

6. Click **OK**.

   The appliance imports the certificate and associated private key, and the certificate is displayed in the Device Certificates table.

Add or edit an SSL server

From the SMS, add an SSL server to specify the SSL server configuration, including the SSL service that is accepted on the SSL detection port.

Tip: To view a summary of the existing SSL server configurations, click **Profiles** on the SMS toolbar. Then, in the navigation pane, select **Profiles > Shared Settings > SSL Servers**.

For secure HTTP, IMAP, and POP3 traffic, create a separate SSL server to enable DV filtering on the decrypted SSL service. For example, if the web server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of **POP3** to enable DV filters for POP3.

For other SSL services, such as SMTPS, create an SSL server with a Detection Port that identifies the secure traffic, and a Decrypted Service of **Other**. The TPS applies DV filters to the incoming traffic, but does not apply DV filters to the decrypted SSL service.

To inspect more than one decrypted service on a particular SSL server, define the same server IP for each service you want. For example, you can define a server with IP 1.1.1.1 and port 443 (HTTPS), and another server with IP 1.1.1.1 and port 995 (POP3S), and associate them with the same SSL inspection profile.

To add or edit an SSL server

1. Select **Profiles > Shared Settings > SSL Servers**.
2. In the SSL Server tab of the SSL Servers panel, click **New** or **Edit**.
3. In the **SSL Server** tab, specify the following settings:
   - **Name:** Enter the server name, for example, `myapp_pop3`.

     (Best Practice) Name the server so that you easily associate it with your web server.
   - **Destinations:** Specify the server IPv4 address or CIDR range.
   - **Detection Ports:** Specify the port range of the encrypted application traffic. For example, if the web server accepts POP3S traffic on port 2000, specify `2000`.
   - **Certificate:** Select the SSL certificate for your web server. You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want.
   - **Decrypted Service:** Choose the SSL service that is accepted on the SSL Detection Port to enable filtering for that particular service. If the SSL service you want is not listed, choose **Other**.
   - **Rekey Interval:** Specify the interval, in seconds, that your web server forces renegotiation of the shared SSL key. If your web server does not offer renegotiation of the shared SSL key, leave this blank.

- **Enable logging:** Select this option to enable the TPS to write log information about SSL inspection to the external user disk (CFast or SSD). This option collects detailed logging information and should only be enabled for troubleshooting purposes. For example, enable this option if, after you set up SSL inspection, the TPS device does not see SSL session activity. By default, this option is disabled. For information about viewing log information, see *Verify SSL inspection activity* on page 15.
- **Allow compression:** Select this option to allow the SSL compression algorithm to be negotiated during the SSL handshake. If your web server does not offer negotiation of SSL compression, disable this option. By default, this option is disabled. If you select this option, and your web server does not offer SSL compression, this setting is ignored.
- **Send TCP reset to server for blocked sessions:** Select this option to always send a TCP reset to the server whenever the TPS blocks an SSL session. This option overrides the TCP reset action set, if enabled, on a DV filter.

  (Best Practice) Enable this option so that protected servers can release network resources quickly if flows are blocked. When this option is disabled, the TCP reset action, if enabled on a DV filter, still applies.

4. In the **Cipher Suites** tab, choose the protocols and algorithms that are supported by your web server.

   The Cipher Suite list automatically updates based on your selections. Deselect any cipher suites that you do not want.

5. Click **OK**.
6. Assign the SSL Server to an SSL inspection policy. See the next section for more information.

Add or edit an SSL inspection policy

On the SMS, update an inspection profile to add an SSL inspection policy. The SSL inspection policy specifies each SSL server that you want to protect, and any SSL client exceptions.

Important: Always distribute an inspection profile with an SSL inspection policy to the inbound virtual segment that receives SSL client requests. When assigned properly, the SSL inspection policy enables the device to proxy (and decrypt) the SSL session between both the SSL client and the device, and between the SSL server and the device. If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses. For more information, see *Distribute the inspection profile* on page 14.

Tip: To view a summary of the existing SSL server policies, select **Profiles** > **Inspection Profiles** > *profile name* > **SSL Inspection Policy**.

To add or edit an SSL inspection policy

1. Select **Profiles > Inspection Profiles >** inspection_profile_name **> SSL Inspection Policy**.

2. Select **Locked** to prevent an SMS user from changing the SSL inspection policy directly, or as a child instance in another policy.

   When you select this option, only users with the **Lock SSL Filter** capability (under Profiles > Profile Management > Profile Filter Management > SSL Filter Management > Lock SSL Filter) can change the SSL inspection policy.

3. In the SSL Inspection Policy panel, click **New** or **Edit**.

   The SSL Profile Editor opens.

4. Enter the SSL profile name, for example, myapp_SSLprofile.
5. Under Server Policies, click **Add**.

   The Add SSL Server Policy dialog box opens.

6. Specify the following settings:

   - **Enable:** Deselect the checkbox to exclude this SSL Server Policy from the SSL inspection profile. By default, this option is selected.

   - **Name:** Specify a policy name, for example, that corresponds to the SSL server configuration.

   - **SSL Server:** Choose a server to include in SSL inspection.

   - **Source Address Exception:** Specify any SSL client IPv4 addresses to exclude from SSL inspection.

7. Click **OK**.

   You are now ready to distribute the SSL inspection profile. See the next section for more information.

Distribute the inspection profile

From the SMS, distribute the inspection profile to the virtual segment that receives SSL client requests. Make sure that the inspection profile includes an SSL server policy, and that the SSL server policy specifies the SSL server to which the SSL clients connect.

Important: The SSL server policy enables the device to proxy (and decrypt) the SSL session between both the SSL client and the device, and between the SSL server and the device. If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses.

For example, if you do not want the device to inspect the decrypted payload in the SSL server response, perform the following steps:

1. Add a user-defined virtual segment that meets the following criteria:

   ◦ Source IP address - Specify the SSL server IP address.

- ◦ Physical segment - Specify the corresponding outbound physical segment. For example, if Segment1 (A > B) receives SSL client requests, specify Segment1 (A < B).

2. Distribute an inspection profile to the virtual segment that disables the Application filters and the Security filters. Or, you can disable all filter categories and filter overrides to maximize the available inspection resources.

To distribute the inspection profile

1. On the Profiles navigation pane, expand **Profiles**, and then click **Inspection Profiles**.
2. Select a profile on the Inventory pane, and then click **Distribute**.
3. To distribute the profile to Inspection Segments:
   - In the Targets section, select the **Inspection Segments** tab.
   - To Allow Segment Selection, choose one of the following items from the **Organize By** drop-down box:
     - ◦ **Segment Group**
     - ◦ **Device**
   - Select the appropriate group(s).
4. For a high priority distribution, select the **High Priority** check box.
5. Click **OK**.

> **Note:** When you enter a significant number of changes to the filters within a profile, the period of time that is required to distribute the profile increases. If the profile distribution takes too long, a time-out can occur. For assistance with extending the time-out setting to meet your profile distribution needs, contact TippingPoint product support.

After you configure SSL inspection

After you configure SSL inspection, monitor SSL inspection activity to verify the device is inspecting the SSL sessions you want. If you want to restrict access to the SSL configuration, give permissions to SSL inspection.

Verify SSL inspection activity

From the SMS, monitor SSL inspection on the TPS device.

View event information about SSL inspection activity by choosing from the following:

- **Devices > All Devices > device-name > Events > SSL Sessions** displays active session count information for up to 50 SSL sessions. Filter the list to view details for the sessions you want.

- **Devices > All Devices > device-name > Events > Traffic > SSL Decrypted Traffic** displays overall SSL traffic seen and amount inspected.
- **Devices > All Devices > device-name > Events > Traffic > Active SSL Connection Rate** displays the total number of new SSL connections that were created during the 1-minute reporting interval.
- **Devices > All Devices > device-name > Events > Traffic > New SSL Connection Rate** displays the average number of new SSL connections created per second during the 1-minute reporting interval.

To view logging information about SSL inspection, choose **Events > SSL Inspection Logs**. The SSL Inspection log displays SSL session information for the SSL servers with logging enabled, including information about SSL sessions that failed to negotiate SSL parameters. By default, when you add an SSL server, logging is disabled. The SSL inspection log does not contain SSL system errors; check the System log.

Note: When you delete an SSL inspection profile or policy, corresponding SSL connections continue to be inspected until the SSL connection closes, but the SSL inspection log incorrectly indicates that the SSL connections have an unknown profile or policy. You can disregard these entries. The device stops logging these connections after the SSL connections close.

If you do not see SSL sessions for a particular server, edit the SSL server to enable logging and then review this log for useful troubleshooting information. When you finish troubleshooting, disable logging on the server.

The SSL Inspection log does not log SSL sessions that are Blocked or Quarantined:

- Both the IPS Block and Alert logs (**Monitor > IPS**) and the Quarantine log (**Monitor > Quarantine**) have an “SSL Inspected” (y/n) column to report on SSL sessions.

  Note: If you see an unexpected alert on a profile that inspects outbound SSL traffic, keep in mind that the device proxies (and decrypts) the SSL session between both the SSL client and the device (inbound segment), and between the SSL server and the device (outbound segment). If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses.

- The Reputation Block and Alert logs (**Monitor > Reputation**) do not report on SSL sessions because Reputation is analyzed prior to SSL Inspection.

Replace a certificate

Replace an SSL server certificate before it expires. When you replace a certificate, keep these points in mind:

- A certificate with a private key should always be replaced by another certificate with a private key.

- A certificate without a private key should always be replaced by another certificate without a private key.
- The replacement certificate is always new to the SMS certificate repository.
- You must have the *Device X509 Certification Configuration* capability in your user role for all of the devices where the certificate is replaced.
- The SMS replaces the certificate on any applicable devices. If the SMS cannot communicate with a particular managed device, the SMS displays an error message.

Note: Certificate replacement requires the *Admin X509 Certificate Management* capability in your user role.

To replace a certificate

1. In SMS tools, click **Admin**.
2. In the left navigation pane, click **Certificate Management > Certificates**.
3. Click **Replace**.
    - For certificates with a private key, browse to and open a certificate.
    - For PEM/DER certificates, browse to and open the associated private key.
4. (Optional) Provide a password to encrypt the private key.
5. Click **OK**.

    The replaced certificate is saved under the original name with `_REPLACED` appended.

Add SSL inspection to the user role

From the SMS, grant permissions to SSL inspection so that an assigned user group can configure SSL inspection. By default, SSL inspection permissions are granted to the Administrator role.

Grant role-based permissions to:

- SSL inspection profiles
- SSL servers
- SSL global settings
- SSL log
- SSL event information

Note: Only custom user roles can be edited; the default user roles cannot be edited.

To update the user role

1. In SMS tools, click **Admin**.

2. In the left navigation pane, click **Authentication and Authorization** > **Roles**.
3. Click **New** to create a user role or **Edit** to change an existing role. When creating a new role, select one of the default roles to use as a template base role for the new role.
4. In the Role dialog box, click the **Capabilities** property sheet.
5. In the Capabilities property sheet, under:
   - **Profiles > Shared Settings Management**, check or uncheck **SSL Server Management**.
   - **Devices > Device Section > Device Management > Event Management**, check or uncheck **View SSL inspection log**.

Grant the user group access to the SSL server

In the SMS, grant the user group access to the SSL servers that you have defined as part of your SSL inspection configuration. By default, a user group has access to all SSL servers, including new SSL servers that have yet to be defined.

To give access to SSL servers

1. In SMS tools, click **Admin**.
2. In the left navigation pane, click **Authentication and Authorization > Groups**.
3. Click **New** to create a group or **Edit** to change an existing group.
4. In the Group dialog box, click the **SSL Servers** property sheet.
5. Check or uncheck the SSL servers to which the group has access.
6. Click the **Profiles** property sheet.
7. Check or uncheck the SSL inspection profiles to which the group has access.

Manage SSL inspection from the LSM

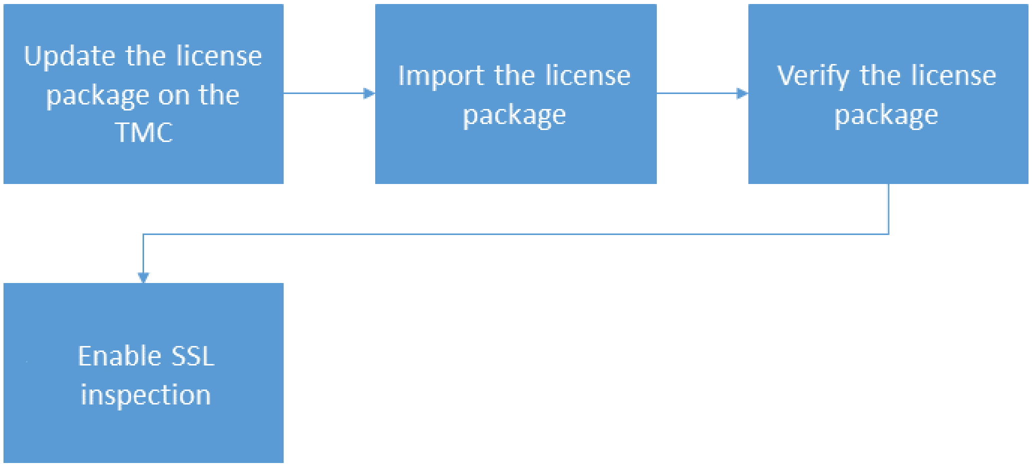
From the LSM, you can set up and manage SSL inspection on a TPS device that is not already managed by the SMS. For more information, see the following sections.

Before you configure SSL inspection

Before you configure SSL inspection, update the device settings for SSL inspection.

Important: To inspect SSL sessions, the device must be licensed for SSL inspection.

The process is:


Update the license package on the TMC
Import the license package
Verify the license package
Enable SSL inspection

The following information provides more details:

- *Update the license package* on page 19
- *Import the license package* on page 20
- *Verify the license package* on page 20
- *Enable SSL inspection* on page 21

Update the license package

Update the license package to assign an available SSL inspection license to any supported TPS security device. SSL inspection is licensed separately. To request an SSL Inspection license, contact your sales representative.

Note: Manage your license package by using the License Manager on the TMC at *https://tmc.tippingpoint.com/TMC/*. When you log on to the TMC, the License Manager is under **My Account > License Manager**.

Import the license package

From the LSM, import an updated license package with an SSL inspection license assigned to the device.

To import the license package

1. Log in to the TMC at *https://tmc.tippingpoint.com*.
2. In the navigation bar, click **My Account** and select **TippingPoint License Package**.
3. Download and save the license package to your local system.

   When the download completes, log out of the TMC.
4. Log in to the LSM on the TPS device where you want to import the license package.
5. From the LSM, select **System > Update > System, DV, Licenses**.
6. In the License Version panel, click **Install**.

   You are prompted to reboot the device to apply changes. If necessary, save any uncommitted changes to the Running configuration and save them to the Startup configuration before you reboot the device.

Verify the license package

Verify the SSL inspection license is enabled on the TPS device.

Important: To enable the SSL inspection license, you must reboot the device.

To verify the license package

1. From the LSM, select **System > Update > System, DV, Licenses**.
2. In the License Version panel, browse the list of licenses and validate that the SSL Inspection feature has a Permit status of **Allow**.

   If the SSL Inspection feature indicates:

   ◦ **Reboot required**, reboot the device to complete the installation.

   ◦ **Deny**, install a license package with SSL inspection assigned to the device. See *Update the license package* on page 19 for more information.

Enable SSL inspection

From the LSM, enable SSL inspection to activate SSL inspection on the TPS device. While SSL inspection is disabled, you can configure SSL inspection on the device.

Important: To enable SSL inspection, the license package on the device must allow SSL inspection. If the device is not licensed for SSL inspection, the LSM banner displays a notification.

To enable SSL inspection

1. From the LSM, select **Policy > SSL Inspection**.

   The SSL Inspection Profiles panel opens.

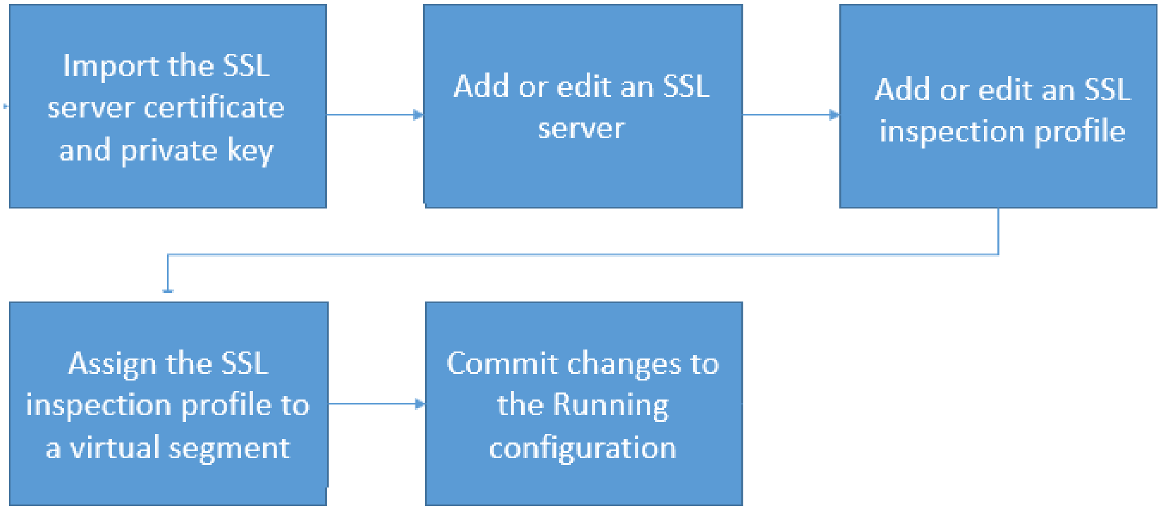
2. Select **Enable SSL Inspection**.

   If the **Enable SSL Inspection** checkbox is grayed, verify the license package allows SSL inspection.

Configure SSL inspection

Configure SSL inspection to specify the SSL sessions you want to inspect. The TPS cannot effectively inspect the encrypted payload of SSL traffic that does not match the SSL inspection profile. Configuring SSL inspection is a deferred commit operation. After you complete your configuration, commit your changes.

The process is:


Import the SSL server certificate and private key
Add or edit an SSL server
Add or edit an SSL inspection profile
Assign the SSL inspection profile to a virtual segment
Commit changes to the Running configuration

The following information provides more details:

- *Import the SSL server certificate and private key* on page 22

- *Add or edit an SSL server* on page 22
- *Add or edit an SSL profile* on page 24
- *Assign the SSL profile to a virtual segment* on page 25
- *Commit changes to the Running configuration* on page 27

Import the SSL server certificate and private key

From the LSM, add or edit a device certificate to import both the SSL certificate and private key from the server of interest. To commit changes to the TPS, you must import both the SSL certificate and its private key. The TPS does not attempt to validate the status of a device certificate.

To import the SSL certificate and private key

1. Select **Authentication > X.509 Certificates > Device Certificates**.
2. In the Device Certificate panel, click **Import** to import a new SSL certificate.

   To update an existing SSL certificate, select the certificate from the list, and then click **Import**.
3. Enter the certificate name.

   (Best Practice) Follow a naming convention so that you can easily and reliably assign the correct certificate to an SSL server.
4. Click **Browse** to locate the file.
5. Select the certificate format, either **Base64 Encoded Certificate (PEM)** or **Encrypted Private Key and Certificate (PKCS12)**.

   When selecting:

   ◦ **PEM** format, the private key must be imported in a separate file. Be sure to select the **Include a Private Key** checkbox, then browse to the private key file. If the private key is encrypted, you must also enter the appropriate password in the Password box.

   ◦ **PKCS12** format, you must enter the appropriate password in the Password box. Note that only one certificate/private key pair can be imported, along with all of the CA certificates contained in the file.
6. Click **OK**.

   The appliance imports the certificate and associated private key, and the certificate is displayed in the Device Certificates table.

Add or edit an SSL server

From the LSM, add an SSL server to specify the SSL server configuration to proxy, including the SSL service that is accepted on the SSL detection port.

For secure HTTP, IMAP, and POP3 traffic, create a separate SSL server to enable DV filtering on the decrypted SSL service. For example, if the web server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of POP3 to enable DV filters for POP3.

For other SSL services, such as SMTPS, create an SSL server with a Detection Port that identifies the secure traffic, and a Decrypted Service of Other. DV filters are applied to the incoming traffic, but are not applied to the decrypted SSL service.

To inspect more than one decrypted service on a particular SSL server, define the same server IP for each service you want. For example, you can define a server with IP 1.1.1.1 and port 443 (HTTPS), and another server with IP 1.1.1.1 and port 995 (POP3S), and associate them with the same SSL inspection profile.

To add or edit an SSL server

1. Select **Policy > SSL Inspection > Servers**.
2. In the SSL Servers panel, click **Add** or **Edit**.

   The Edit SSL Server dialog box displays.

3. In the **SSL Server Config** tab, specify the following settings:

   - **Name -** Enter the server name, for example, `myapp_pop3`.

     (Best Practice) Name the server so that you can easily associate it with your web server.

   - **Server Certificate:** Select the SSL certificate for your web server.

     Note: The LSM does not validate the server certificate.

   - **Server Addresses:** Specify the server IPv4 address or CIDR range.

   - **Decrypted Service:** Choose the SSL service that is accepted on the SSL Detection Port to enable filtering for that particular service. If the SSL service you want is not listed, choose **Other**.

   - **SSL Detection Ports:** Specify the port range of the encrypted application traffic. For example, if the web server accepts POP3S traffic on port 2000, specify `2000`.

   - **Rekey Interval:** Specify the interval, in seconds, that your web server forces renegotiation of the shared SSL key. If your web server does not offer renegotiation of the shared SSL key, leave this blank.

   - **Enable logging:** Select this option to enable the TPS to write log information about SSL inspection to the external user disk (CFast or SSD). This option collects detailed logging information and should only be enabled for troubleshooting purposes. For example, enable this option if, after you set up SSL inspection, the TPS does not see SSL session activity. By default, this option is disabled. For information about viewing log information, see *Verify SSL inspection activity* on page 27.

- **Allow compression:** Select this option to allow the SSL compression algorithm to be negotiated during the SSL handshake. If your web server does not offer negotiation of SSL compression, disable this option. By default, this option is disabled. If you select this option, and your web server does not offer SSL compression, this setting is ignored.
- **Send TCP reset to server for blocked sessions:** Select this option to always send a TCP reset to the server whenever the TPS blocks an SSL session. This option overrides the TCP reset action set, if enabled, on a DV filter.

  (Best Practice) Enable this option so that protected servers can release network resources quickly if flows are blocked. When this option is disabled, the TCP reset action, if enabled on a DV filter, still applies.

4. In the **Cipher Suites** tab, choose the protocols and algorithms that are supported by your web server.

   The Cipher Suite list automatically updates based on your selections. Deselect any cipher suites that you do not want.

5. Click **OK**. You are now ready to assign the SSL server to an SSL inspection profile.

Add or edit an SSL profile

From the LSM, add or edit an SSL profile to specify each SSL server that you want to protect, and any SSL client exceptions.

Important: Always assign the SSL profile to the inbound virtual segment that receives SSL client requests. When assigned properly, the SSL profile enables the device to proxy (and decrypt) the SSL session between both the SSL client and the device, and between the SSL server and the device. If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses. For more information, see *Assign the SSL profile to a virtual segment* on page 25.

To add or edit an SSL inspection profile

1. Select **Policy > SSL Inspection > Profiles**.
2. In the SSL Inspection panel, click **Add** or **Edit**.

   The SSL Profile Editor opens.

3. Enter the SSL profile name, for example, myapp_SSLprofile.
4. Under Server Policies, click **Add**.

   The Add SSL Server Policy dialog box opens.

5. Specify the following settings:

- **Enable:** Deselect the checkbox to exclude this SSL Server Policy from the SSL inspection profile. By default, this option is selected.
- **Name:** Specify a policy name, for example, that corresponds to the SSL server configuration.
- **SSL Server:** Choose a server to include in SSL inspection.
- **Source Address Exception:** Specify any client IP addresses to exclude from SSL inspection.

6. Click **OK**.

   You are now ready to assign the SSL inspection profile to a virtual segment.

Assign the SSL profile to a virtual segment

From the LSM, assign the SSL profile to the inbound virtual segment that receives SSL client requests. Make sure that the SSL profile specifies the SSL server to which the SSL clients connect.

Important: Always assign the SSL profile to the inbound virtual segment that receives SSL client requests. When assigned properly, the SSL profile enables the device to proxy (and decrypt) the SSL session between both the SSL client and the device, and between the SSL server and the device. If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses.

For example, if you do not want the device to inspect the decrypted payload in the SSL server response, add a user-defined virtual segment that meets the following criteria:

- Source IP address – Specify the SSL server IP address.
- Physical segment – Specify the corresponding outbound physical segment. For example, if Segment1 (A > B) receives SSL client requests, specify Segment1 (A > B).
- IPS profile – Assign an IPS profile that disables the IPS category rules. Or, you can disable all filter categories and filter overrides to maximize the available inspection resources.

To assign the SSL profile to a virtual segment

1. From the LSM menu, click **Network > Virtual Segments**.
2. Click **Add** or **Insert** to create a new virtual segment, or click **Edit** to edit an existing virtual segment. Virtual segments that are created by the system can have their profiles modified but are otherwise read-only.
   - Clicking **Add** adds the new virtual segment after all the other user-created virtual segments.
   - Clicking **Insert** inserts the new virtual segment just before the currently selected virtual segment.

- All system-created virtual segments always appear at the end of the list.

3. In the Add Virtual Segment dialog or Edit Virtual Segment dialog, specify the following:

    - Name – (Required) Name used to identify the virtual segment. Each virtual segment must have a unique name.
    - Description – An optional parameter to provide more detailed information about the virtual segment.
    - IPS Profile – Security profile that you want to apply to the virtual segment. A virtual segment can have only one IPS profile applied to it.
    - Reputation Profile – Reputation profile that you want to apply to the virtual segment. A virtual segment can have only one Reputation profile applied to it.
    - Traffic Management Profile – Traffic Management profile that you want to apply to the virtual segment. A virtual segment can have only one Traffic Management profile applied to it.
    - SSL Profile – SSL profile that you want to apply to the virtual segment. A virtual segment can have only one SSL profile applied to it.
    - Physical Segments – Physical segment associated with the virtual segment. All physical segments are directional.
    - Traffic Criteria – (Required) Specify any one or all of the following: VLAN ID, Source IP, and Destination IP. For example, omit VLAN ID and specify Destination IP. When specifying a VLAN ID, specify a value between 1 and 4094 in which the segment is included. There can be no duplicate VLAN IDs or overlapping VLAN ranges. All 4094 VLAN IDs can be used per virtual segment (a VLAN range of 1–100 counts as 100 IDs). At least one traffic criteria (VLAN ID, source IP address, or destination IP address) must be defined for each virtual segment.
    - Source IP Address – Source CIDR associated with the virtual segment. Addresses must be valid IPv4 format. The host portion of address/mask must be 0 (zero). No more than 250 addresses may be specified.
    - Destination IP Address – Destination CIDR associated with the virtual segment. Addresses must be valid IPv4 format. The host portion of address/mask must be 0 (zero). No more than 250 addresses may be specified.

4. Click **OK**.

> **Note:** Virtual segments must be created with a physically available segment. If creating a virtual segment generates a UDM warning in the system log, ensure you have associated the virtual segment with a valid physical segment.

Commit changes to the Running configuration

From the LSM, commit your changes to the Running configuration.

Depending on the type of configuration change, the device commits changes to the Running configuration:

- Automatically. An *instant commit* is one that is applied immediately to the Running configuration. Only some items, including Action Sets and Notification Contacts, are instant-commit features. A bright yellow notice is displayed on all features that use instant commit.
- Manually. A *deferred commit* is one that is not immediately committed to the Running configuration. Uncommitted changes are placed into a pending state until you explicitly commit them to the Running configuration. When you log out of the LSM, pending changes are lost.

  Defer your commit until you have completed the necessary configuration changes, and then commit all of the changes at once. For example, when creating an SSL server, you must also import a device certificate and assign to the server before you can commit your changes.

To commit your pending changes to the Running configuration:

- In the Configuration menu, click **Commit pending changes**.

After you configure SSL inspection

After you configure SSL inspection, monitor SSL inspection activity to verify the TPS device is protecting the correct SSL sessions. If you want to restrict access to SSL configuration, update the user role.

Verify SSL inspection activity

From the LSM, monitor SSL inspection activity.

View information about SSL inspection activity by choosing from the following:

- **Monitor > Sessions > SSL Sessions** displays active session count information for up to 50 SSL sessions. Filter the list to view details for the sessions you want.
- **Monitor > Network > SSL Bandwidth** displays overall SSL traffic seen and amount inspected.
- **Reports > Activity > SSL > Connections** displays the total number of new SSL connections that were created during the 1-minute reporting interval.
- **Reports > Activity > SSL > Connection Rate** displays the average number of new SSL connections created per second during the 1-minute reporting interval.

To view logging information about SSL inspection, choose **Monitor > Logs > SSL Inspection**. The SSL Inspection log displays SSL session information for the SSL servers with logging enabled, including information about SSL sessions that failed to negotiate SSL parameters. By default, when you add an SSL server, logging is disabled. The SSL inspection log does not contain SSL system errors; check the System log.

Note: When you delete an SSL profile or policy, corresponding SSL connections continue to be inspected until the SSL connection closes, but the SSL inspection log incorrectly indicates that the SSL connections have an unknown profile or policy. You can disregard these entries. The device stops logging these connections after the SSL connections close.

To display sessions details, such as connection resets, click **Columns > Details**. If you do not see SSL sessions for a particular server, enable logging on that server and then review this log for useful troubleshooting information. When you finish troubleshooting, disable logging on the server. You can also configure notification contacts and thresholds for SSL inspection logs.

The SSL Inspection log does not log SSL sessions that are Blocked or Quarantined:

- Both the IPS Block and Alert logs (**Monitor > IPS**) and the Quarantine log (**Monitor > Quarantine**) have an "SSL Inspected" (y/n) column to report on SSL sessions.

  Note: If you see an unexpected alert on a profile that inspects outbound SSL traffic, keep in mind that the device proxies (and decrypts) the SSL session between both the SSL client and the device (inbound segment), and between the SSL server and the device (outbound segment). If necessary, update the inspection profile on the corresponding outbound virtual segment to properly filter the decrypted server responses.

- The Reputation Block and Alert logs (**Monitor > Reputation**) do not report on SSL sessions because Reputation is analyzed prior to SSL Inspection.

Add SSL inspection to the user role

From the LSM, grant permissions to SSL inspection so that an assigned user group can configure SSL inspection. By default, SSL inspection permissions are given to the Administrator role.

Give role-based permissions to:

- SSL inspection profiles
- SSL servers
- SSL global settings
- SSL log
- SSL reports

Note: Only custom user roles can be edited; the default user roles cannot be edited.

To give permissions for SSL inspection

1. Select **Authentication > User Roles**.
2. Click **Add** to create a user role or **Edit** to change an existing custom user role.

3. Enter a name.
4. (Optional) Enter a description for the user role.
5. Select one of the default roles to use as a template base role for the new role.
6. Check or uncheck each capability, including SSL inspection, for the new role.
7. Select either **Read-only** or **Read/Write** for the state.

Best Practices

Use this checklist to verify that your SSL inspection configuration conforms to the recommended best practices.

☐	To help avoid assigning the wrong certificate and private key to a server, use a naming convention for the certificate, private key, and SSL server. The device does not validate the certificate and private key.
☐	Set role-based access controls to limit access to SSL inspection.
☐	Check the System log for errors.
☐	Keep your certificates up-to-date. Whenever you update a certificate on your server, be sure to also import the updated certificate into the device or the SMS. If a certificate expires, the System log generates an error.

Troubleshoot SSL inspection

If SSL clients cannot reach the server, check Traffic Management and Reputation filters to verify the sessions of interest are not being blocked. Traffic Management and Reputation filters are applied before SSL inspection. See the following sections for additional troubleshooting information.

Basic troubleshooting

If SSL clients are reaching the server but the TPS device is not inspecting some or all of the encrypted sessions of interest, perform the following basic troubleshooting steps:

- Check the System Log to determine whether the TPS device is bypassing SSL sessions.
- Check the SSL Server IP and ports.
- Check the server policies on the SSL Profile to verify a source IP exception is not bypassing SSL inspection.
- Check the virtual segments that have been assigned the SSL profile:

  a. If the virtual segment designates a segment, is it the correct segment? For example, is it supposed to be interface 1A or 3A? If it is only one direction, is it the correct direction, such as **A > B** or **A < B**?

  b. If the virtual segment defines VLANs, are they correct for the SSL Servers?

  c. If the virtual segment defines Source IP Addresses, are the SSL clients coming from those addresses?

  d. Finally, if the virtual segment defines Destination IP Addresses, are the SSL servers in those addresses?

To verify	Do this
The TPS is not bypassing SSL sessions	On the device, check the System Log for an entry similar to the following: `SSL Inspection reached Critical threshold of Max Concurrent Connections. Action: Allow but bypass Inspection` If the number of concurrent SSL sessions exceeds the maximum threshold as specified by the entry in the System Log, the TPS device does not inspect them. If necessary, reconfigure SSL inspection to reduce the number of concurrent SSL connections. For information

To verify	Do this
	about configuring SSL inspection to block SSL sessions that exceed the maximum threshold, contact TippingPoint product support.
SSL inspection license is installed and valid	For a managed device, see *Verify the license package* on page 8 for more information. For an unmanaged device, see *Verify the license package* on page 20 for more information.
SSL inspection is enabled	For a managed device, see *Enable SSL inspection* on page 9 for more information. For an unmanaged device, see *Enable SSL inspection* on page 21 for more information.
The correct certificate and key are installed	For a managed device, see *Import the SSL server certificate and private key* on page 11 for more information. For an unmanaged device, see *Import the SSL server certificate and private key* on page 22 for more information.
The SSL server matches the correct IP address and port	For a managed device, see *Add or edit an SSL server* on page 12 for more information. For an unmanaged device, see *Add or edit an SSL server* on page 22 for more information.
The profile is applied to the correct virtual segments	For a managed device, see *Distribute the inspection profile* on page 14 for more information. For an unmanaged device, see *Assign the SSL profile to a virtual segment* on page 25 for more information.
The virtual segment includes the desired SSL server IP addresses and ports	Verify the SSL clients are reaching the SSL server.

Advanced troubleshooting

If the basic troubleshooting does not resolve your issue, perform the following steps on the device:

1. Verify the list of inspected SSL sessions. In the LSM, click **Monitor > Sessions > SSL Sessions** or, from the CLI run the show tse ssl-inspection command.

   Entries are only present for the life of the session. If necessary, use the `debug np ssl-clear` command to forcibly close the SSL sessions. If an entry does not exist, proceed to the next step.

2. Run the debug np stats show npSslInspStats command to check the connection counters. If they are all zero, then it is likely that you have a configuration issue. If there are refused connections, it is also a configuration issue, but there are likely incompatible ciphers or it is trying to use compression when the profile does not support it. For more information, see *Basic troubleshooting* on page 31.
3. Run the debug np stats show npSslInspProtocolStats command and keep the following points in mind:

   - Non-zero entries in "other cipher" indicate a possible unsupported cipher. The other error counters narrow the source of the problem to at least the server or the client.

   - Server connection failures, it is the same possibility, but with the added chance that the server might be asking for a client certificate, which the proxy does not support with this release.

4. Run the debug np stats show npTcpProxyStats command to confirm whether the profile and server is configured to correctly match traffic. If the results are all zero, then no traffic is being sent for inspection. If there is any TCP traffic matching a profile, the results are non-zero.

CLI Reference for SSL inspection

This section describes the CLI commands for configuring and troubleshooting SSL inspection.

Troubleshoot

This section describes the CLI commands on the TPS device for troubleshooting SSL inspection.

show license

Syntax

```
show license
```

Example

```
ips{}show license
License: 5.0.0.46
Feature                  Status          Permit   Expiration   Details
--------                 ------          -------  ----------   --------
License                  OK              Allow    9/30/2015
Update TOS               OK              Allow    9/30/2015
Update DV                OK              Allow    9/30/2015
MalwareAuxDv             OK              Allow    9/30/2015
Auxiliary DV:ScadaAux    OK              Allow    9/30/2015
Auxiliary DV:Other       OK              Allow    9/30/2015
ReputationDV             OK              Allow    9/30/2015
SSL Inspection           OK              Allow    9/30/2015
Throughput Upgrade       Info            Deny     Never        Not licensed to
                                                               use this feature.
Feature                  Active       After Reboot
-------                  ------       ------------
Throughput Upgrade       20000 Mbps   No change
SSL Inspection           Allow        No change
```

display conf

Displays information on a particular configuration file in either the `start` configuration or the `running` configuration.

Syntax

`display conf start|running` *conf-name*

Example

Enter the `display conf` command and press the Tab key twice to display a list of available configuration files.

```
ips{}display conf running
aaa                actionsets        autodv            certificates
dns                gen               highavailability  inspection-bypass
interface          ips               log               notifycontacts
ntp                reputation        segment1          segment2
segment3           segment4          segment5          segment6
segment7           segment8          snmp              ssl-inspection
traffic-management virtual-segments  vlan-translations debug
```

Example

Displays SSL configuration.

```
ips{}display conf running ssl-inspection
  # SSL INSPECTION STATEMENTS
  disable
  # SSL SERVERS
  server "swdevts4b"
    ip address 10.1.2.78/32
    detection-port 443
    detection-port 999
    decrypted-service http
    cipher-suite RSA-3DES-EDE-CBC-SHA1
    cipher-suite RSA-AES128-CBC-SHA1
    cipher-suite RSA-AES256-CBC-SHA1
    protocol TLSv1.0
    protocol TLSv1.1
    protocol TLSv1.2
    certificate swdevts4b
    logging
    tcp-reset
  exit
  server "swdevts4b_server"
    ip address 10.1.2.2/32
    detection-port 443
    detection-port 999
    decrypted-service http
    cipher-suite RSA-3DES-EDE-CBC-SHA1
    cipher-suite RSA-AES128-CBC-SHA1
    cipher-suite RSA-AES256-CBC-SHA1
    protocol TLSv1.0
    protocol TLSv1.1
    protocol TLSv1.2
    certificate swdevts4b_cert
    logging
    tcp-reset
  exit
  # SSL PROFILES
  profile "swdevts4b"
    policy "swdevts4b"
      enable
      server "swdevts4b"
    exit
  exit
  profile "swdevts4b_profile"
    policy "swdevts4b_policy"
      enable
      server "swdevts4b_server"
    exit
  exit
  # LOG SERVICE
    log sslInspection "Management Console" ALL
    log sslInspection "Remote System Log"  ALL
```

show tse

Shows threat suppression engine information.

Syntax

```
show tse (connection-table(blocks|trusts)|rate-limit|ssl-
inspection)
```

Example of connection-table blocks

```
ips{}show tse connection-table blocks
Blocked connections: 1 of 1 shown.

Protocol Src/Dest IP  Port         Src/Dest IP  Port  Reason
TCP      10.1.3.1     36051        10.1.3.2     44    6551: TCP: IPS Test Filter

Virtual Segment ID    In Interface Out Interface
segment6 (A > B)      unknown      unknown
```

Example of rate-limit

```
ips{}show tse rate-limit
Rate limit streams: 1 of 1 shown.

Protocol Src/Dest IP  Port   Src/Dest IP  Port   Reason
TCP      10.1.3.1     36052  10.1.3.2     44     6551: TCP: IPS Test Filter

Virtual Segment ID    In Interface Out Interface
segment6 (A > B)      unknown      unknown
```

Example of ssl-inspection

```
ips{}show tse ssl-inspection
SSL Inspected Sessions: 1 of 1 shown.

Client IP  Port   Interface  Proto    Cipher
---------- -----  ---------- -------  ----------------------
10.1.3.1   42523  5B         TLSv1.2  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Server IP  Port   Interface  Proto    Cipher
---------  ------ ---------  ------   -----------------------------
10.1.3.2   443    5A         TLSv1.2  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

debug

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

Syntax

```
debug
```

```
Valid entries at this position are:

aaa                 aaa debug options
autoDV              Access automatic Digital Vaccine (AutoDV) functions
busy-wait           Wait for UDM
core-dump           Enable or disable core dumps
echo                Echo text to console
factory-reset       Factory Reset
force-obe           Forces re-run of OBE on the next reset
ini-cfg             .ini values
np                  Network processor
reputation          Reputation utilities
show                Show current .ini values
snapshot            Manage system snapshots
UDM                 UDM debug options
```

Examples

See the following examples for more information about debug commands.

debug factory-reset

```
debug factory-reset

WARNING!!!
```

```
This command WILL reset this device to factory default
configuration.

This will remove all network and security configuration, user
accounts log files, snapshots and applied software upgrades

You will NOT be able to recover any of this data from the device
after this command has been confirmed

After the factory reset completes, the device will automatically
reboot and display the OBE

Warning: Type the word 'COMMIT' to continue: COMMIT
```

debug np best-effort options

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 not inspected 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.

Best Effort mode is supported on the 2200T TPS only.

Subcommands

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

Subcommand	Description	Usage
`enable`	Enables Best Effort mode.	`debug np best-effort enable [-queue-latency <microseconds>] [-recover-percent <percent>]`
`disable`	Disables Best Effort mode.	`debug np best-effort disable`

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.	`debug np best-effort enable -queue-latency <`*`microseconds`*`>`
`-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).	`debug np best-effort enable -recover-percent <`*`percent`*`>`

debug np mcfilt-regex options

Microfilter regular expression statistics.

```
debug np regex [clear|show option]
```

Option	Description
`clear`	Clears regular expression statistics.
`show average`	Sorts and displays network processor information based on average time.
`show count`	Specifies the number of entries to display. Default: 10
`show evaluations`	Sorts and displays network processor information based on the number of evaluations.
`show matches`	Sorts and displays network processor information based on the number filter matches.
`show maximum`	Sorts and displays network processor information by maximum time.

Option	Description
	Default: The default display if you do not specify another option.
`show total`	Sorts and displays network processor information by total time.

debug np regex options

Regular expression statistics.

```
debug np regex [clear|show option]
```

Option	Description
`clear`	Clears regular expression statistics.
`show average`	Sorts and displays network processor information based on average time.
`show count`	Specifies the number of entries to display. Default: 10
`show evaluations`	Sorts and displays network processor information based on the number of evaluations.
`show matches`	Sorts and displays network processor information based on the number filter matches.
`show maximum`	Sorts and displays network processor information by maximum time. Default: The default display if you do not specify another option.
`show total`	Sorts and displays network processor information by total time.

debug np stats options

Show/clear engine statistics.

```
debug np stats [clear|help|show]
```

Option	Description
`clear`	Clears regular expression statistics.
`help`	Lists available statistics tables.
`show`	Shows system information. **Note:** When an active session is closed, the session count is decremented. If the session count was already set to zero by the `clear` command, then the session count incorrectly appears as a very large number.

debug np stats show npSslInspStats Example

The following example displays SSL inspection activity on the device:

```
ips{}debug np stats show npSslInspStats
Connections:
 clientConnections = 1        ; Number of client connections
 clientConnectionFailures = 0 ; Number of client connection failures
 serverConnections = 1        ; Number of server connections
 serverConnectionFailures = 0 ; Number of server connection failures
 refusedConnections = 9       ; Number of refused sessions
Sessions:
 activeSessions = 0           ; Number of active sessions
 inspectedSessions = 1        ; Number of inspected sessions
 blockedSessions = 0          ; Number of blocked sessions
 trustedSessions = 0          ; Number of trusted sessions
 flushTrustedSessions = 0     ; Number of flushed trusted sessions
 shuntedSessions = 0          ; Number of shunted sessions
 blockedMaxSslConnections = 0 ; Number of blocked sessions due to max conn limit
 allowedMaxSslConnections = 0 ; Number of allowed sessions due to max conn limit
Renegotiation:
 renegotiationServerSide = 1 ; Number of renegotiations initiated by the server
 renegotiationClientSide = 2 ; Number of renegotiations initiated by the client
 renegotiationProxy = 0      ; Number of renegotiations initiated by the proxy
Certificate Requests:
 clientCertificateRequests=0 ; Number of client certificates requested by server
Other:
 mbufFails = 0 ; Number of failures to get a free message buffer
```

Note: When an active session is closed, the session count is decremented. If the session count was already set to 0 by the `clear` command, then the session count will incorrectly appear as a very large number.

debug np congestionx Example

The following example displays potential causes of network congestion:

```
ips{}debug np congestionx
Device      Bypassed   Dropped    Out of
----------- ---------- ---------- ----------
BCOM                 0          0       1447
NIC Ingress          0 893353197360 111669151015
CPU Ingress          0          0       1448
CPU Egress           0          0       1448
NIC Egress           0          0 111669151015
System RL                       0       1448
```

debug np diagx Example

The following example displays diagnostic information:

```
ips{} debug np diagx -details
Switch (packet flow from top left counterclockwise)
         1A               0               0
     Bypass               0               0
     Uplink               0               0      RX Dropped   0     RX Pause   0

Processor
      CPU A               0               0
     Engine               0               0
    Dropped               0
    Blocked               0
  Policy RL               0
  System RL               0

Time since last snapshot: 1 minute, 12 seconds
```

debug np regex Example

The following example sorts the network processor information based on the average time:

```
ips{}debug np regex show average
------------------------------------------------------------------------------
Filter      CRC     Flag  Max(us)  Avg(us)       Evals    Matches   Total(us)
------------------------------------------------------------------------------
   3179  0x0f7b8828   P        795      768           4       0        3073
   4062  0xaf664079   PS       595      466           4       4        1866
   5995  0xed3a9991   R        308      234           4       0         938
```

```
 10762  0xf4a09ead   P        614       169          8      0       1350
  6413  0xbea34771   R        114       109          2      0        218
 10777  0x602fe470   R        417       105         55      0       5750
  6416  0xb34d4b62   R        102       102          1      0        102
  6417  0x65b97c0b   R         98        98          1      0         98
  6356  0x4b09bc88   R        103        85          4      0        341
  6662  0x96dcebfe   P        130        80         18      0       1439
```

debug np ssl-clear Example

The `debug np ssl-clear` command clears any "stale" sessions and forces clients to reconnect. This is a useful troubleshooting tool for features that have a session state. The following example terminates any SSL sessions that are proxied by the TPS device and clears the sessions information from the LSM:

```
ips{}debug np ssl-clear
```

debug np stats Example

The following example displays system information:

```
ips{}debug np stats help
  udmAggStats                  (CP only)    UDM Aggregation Statistics
  cpMiscStats                  (CP only)    Control Plane Miscellaneous Stats
  npMetadataStats              (DP only)    Event Metadata Statistics
  npIrrStats                                NetPal Inverted Reroute Stats
  npMicrofilterStats           (DP only)    NetPal Microfilter Statistics
  npHttpResponseStats          (DP only)    HTTP Response Statistics
  dpalStats                    (CP only)    DPAL counters
  asFlowControlStats                        Action Set Flow Control Stats
  fqStats                      (DP only)    FlowQueue Stats
  npScanSweepMemStats                       NetPal Scan/Sweep Memory Stats
  npScanSweepStats                          NetPal Scan/Sweep Statistics
  dpsIpcClassStats                          dpsIpc per-class stats
  npZlibStats                               NetPal Zlib Statistics
  sleuthPatterns               (CP only)    Sleuth pattern table stats
  ruleStatsStats                            stats about rule stats
  dpsIpcConv                                dpsIpc Conversion stats
  npTrafficCaptureStats                     NetPal traffic capture stats
  dpsIpcRpcStats               (CP only)    dpsIpcRpc Stats
  dpwdStats                    (CP only)    DP Watchdog Statistics
  eccStatsXlrC                 (CP only)    XLRC's ECC Stats
  eccStatsXlrB                 (CP only)    XLRB's ECC Stats
  eccStatsXlrA                 (CP only)    XLRA's ECC Stats
  eccStats                     (DP only)    ECC Stats
  dpsTiming                    (DP only)    Timing Subsystem
  dpsIpcCPStats                (CP only)    dpsIpc CP Stats
  lwipStats                    (DP only)    lwip Stats
  dpsIpcStats                               dpsIpc Stats
```

```
snakeStats                               Snake Stats
npTurboSimLfhStats          (DP only)    Turbo Simulator LF Hash Stats
npQuarantineActionLfhStats  (DP only)    Quarantine Action LF Hash Stats
npQuarantineAqciLfhStats    (DP only)    Quarantine AQCI LF Hash Stats
npQuarantineStats                        NetPal Quarantine Packet Stats
npSynProxyStats             (DP only)    NetPal SYN Proxy Statistics
npIpReputationIpcStats                   IP Reputation command IPC Stats
npIpReputationRequestStats  (CP only)    (null)
npIpReputationCallbackStats (DP only)    IP Reputation Callback Stats
npDnsReputationStats        (DP only)    DNS Reputation Statistics
npIpReputationStats         (DP only)    IP Reputation Statistics
npUrlReputationStats        (DP only)    URL Reputation Statistics
npHreStats                  (DP only)    Rule Statistics
npSoftLinxStats             (DP only)    NetPal SOFTLINX Statistics
trhaStats                   (CP only)    TRHA Statistics
npTcpStateStats             (DP only)    TCP State module stats.
rlStats                     (DP only)    Policy Rate Limiter Statistics
npHCDspStats                (DP only)    NetPal HardCode Statistics
npIPDgrams                  (DP only)    (null)
npZoneStats                 (DP only)    ZoneStats
npTelnetStats               (DP only)    TELNET Decode Statistics
npSnmpStats                 (DP only)    SNMP Decode Statistics
npSmtpStats                 (DP only)    SMTP Decode Statistics
npSmbStats                  (DP only)    SMB Decode Statistics
npRpcStats                  (DP only)    RPC Decode Statistics
npMsrpcStats                (DP only)    MS-RPC Decode Statistics
npOspfStats                 (DP only)    OSPF Decode Statistics
npImapStats                 (DP only)    IMAP Decode Statistics
npHttpStats                 (DP only)    HTTP Decode Statistics
ahpStats                    (DP only)    ahp Stats
npFtpStats                  (DP only)    FTP Decode Statistics
npDnsStats                  (DP only)    DNS Decode Statistics
udmCbStats                               UDM Callback Statistics
npTTStats                                NetPal Trust Table Statistics
npCTStats                                NetPal Connection Table Statistics
pcbStats                    (DP only)    PCB Stats
txStats                     (DP only)    TX Stats
rxStats                     (DP only)    Rx Stats
threadFwdStats              (DP only)    NetPal Parse Packet Statistics
npHardCodeStats             (DP only)    HardCode Packet Statistics
npFilterStatsInst           (DP only)    (null)
npReparseStatsInst          (DP only)    NetPal Non-ingress Parse Packet Stats
npParseStatsInst            (DP only)    NetPal Parse Packet Statistics
npTcpReas                   (DP only)    TCP Reassembly Statistics
npReasIpv6                  (DP only)    IPv6 Reassembly Statistics
npReas                      (DP only)    IPv4 Reassembly Statistics
dpk                         (DP only)    Data Plane Stats
triv                                     Sample stats
```

```
ips{}debug np stats show trhaStats
TRHA:
    trhaSend = 0    ; trhaSend
    trhaReceive = 0 ; trhaReceive
    trhaDropped = 0 ; trhaDropped
Host Communication:
    hostCommSend = 0    ; hostCommSend
    hostCommReceive = 0 ; hostCommReceive
    hostCommDropped = 0 ; hostCommDropped
Delay:
    delayTotal = 0 ; delayTotal
    delayCount = 0 ; delayCount
```

debug np port Example

The following example displays system information:

```
ips{}debug np port show
PORT status:
Local Device 0  (switch in NORMAL mode) --------------------------------
Port  Bcm  Num   Admin    Status Speed  AutoNeg Pause  Mode  MTU  Medium SP MMU
                                                                            cells
 enet1  ge1  3   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet2  ge0  2   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet3  ge3  5   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet4  ge2  4   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet5  ge5  7   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet6  ge4  6   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet7  ge7  9   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet8  ge6  8   Disabled DOWN   1Gbps  auto      -    GMII  1526  Fiber  0   0
 enet9  ge9  11  Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet10  ge8  10  Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet11  ge11 13  Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet12  ge10 12  Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet13  ge13 15  Disabled DOWN       -  auto      -   SGMII  1526 Copper  0   0
enet14  ge12 14  Disabled DOWN       -  auto      -   SGMII  1526 Copper  0   0
enet15  ge15 17  Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
enet16  ge14 16  Enabled  UP     1Gbps  auto    none  SGMII  1526 Copper  0   0
uplnk0  xe0  26  Uplink   UP    10Gbps  none    none  XGMII 16356  Fiber  0   0
uplnk1  xe1  27  Uplink   UP    10Gbps  none    none  XGMII 16356  Fiber  0   0
uplnk2  xe2  28  Uplink   DOWN  10Gbps  none      -   XGMII 16356  Fiber  0   0
uplnk3  xe3  29  Uplink   DOWN  10Gbps  none      -   XGMII 16356  Fiber  0   0
ips{}debug np port diags 1A
Port:                   enet1 (uport 1; port 3)
Enable state:           Disabled
Link status:            DOWN
Laser status:           SFP absent and laser off
Linkscan mode:          SW
Auto-negotiated:        (no link)
```

```
Port ability:               fd = 100MB,1000MB
                            hd = <none>
                            intf = gmii
                            medium = <none>
                            pause = pause_tx,pause_rx,pause_asymm
                            lb = none,MAC,PHY
                            flags = autoneg
Advertised ability:         fd = 1000MB
                            hd = <none>
                            intf = <none>
                            medium = <none>
                            pause = <none>
                            lb = <none>
                            flags = <none>
STP mode:                   Forward
Learn mode:                 FWD
Untag priority mask:        0
Multicast flood (pfm):      FloodNone
Interface:                  GMII
Max_frame size:             1526
MDIX mode:                  ForcedNormal, Normal
Medium:                     Fiber
```

debug show settings Example

The `debug show settings` command provides an overview your debug configuration. In the following example, best-effort mode is enabled.

```
ips{}debug show settings
Core dumps:       Disabled
Best Effort:      Enabled
Snapshot Version: Ignore
```

show np tier-stats

Displays statistics for monitoring activity since the last reboot of the device. Reboot the device to reset these counters.

Syntax

```
show np tier-stats
```

Example

```
ips{}show np tier-stats
----------------------------------------------------------
Tier 1 (Physical Ports):
----------------------------------------------------------
Rx Mbps                =        261.7  (1,250.0)
```

```
Tx Mbps               =        270.4  (1,248.6)
Rx Packets/Sec        =     31,054.0  (111,814.0)
Tx Packets/Sec        =     45,279.0  (111,682.0)
Utilization           =         23.7% (100.0%)
Ratio to next tier    =        100.0% [0.0%]
----------------------------------------------------------
Tier 2 (Software Fastpath):
----------------------------------------------------------
Rx Mbps               =        261.7  (838.2)
Rx Packets/Sec        =     31,054.0  (74,982.0)
Tx trust packets/sec  =          0.0  (0.0)
Utilization           =         23.7% (76.2%)
Ratio to next tier    =        100.0% [99.6%]
----------------------------------------------------------
Tier 3 (IPS Engine Fastpath):
----------------------------------------------------------
Rx Mbps               =        261.7  (836.4)
Rx Packets/Sec        =     31,054.0  (74,781.0)
Tx trust packets/sec  =          0.0  (0.0)
Utilization           =         23.7% (76.0%)
Ratio to next tier    =          0.0% (0.0%)
----------------------------------------------------------
Tier 4 (IPS Engine Slowpath):
----------------------------------------------------------
Rx Mbps               =          0.0  (0.0)
Rx Packets/Sec        =          0.0  (2.0)
Rx due to:
   Trigger match       =          0.0% (0.0%)
   Reroute             =          0.0% (50.0%)
   TCP sequence        =          0.0% (0.0%)
   Protocol decode     =          0.0% (0.0%)
Utilization           =          0.0% (0.0%)
Ratio to deep         =          0.0% (0.0%)
----------------------------------------------------------
Tier 5 (SSL Inspection):
----------------------------------------------------------
Rx Mbps               =        252.7  (257.7)
Rx Packets/Sec        =     21,823.0  (22,256.0)
Utilization           =         22.9% (23.4%)
```

show ssl-inspection congestion

Shows SSL inspection information, including the average number of SSL connections per second, the number of current SSL connections (and the device limit), and whether SSL sessions that exceed the device limit are not inspected or blocked. By default, SSL sessions that exceed the device limit are not inspected.

Syntax

```
show ssl-inspection congestion
```

Example

```
ips{}show ssl-inspection congestion
SSL connection rate:      3.15 conn/sec
SSL current connections:  152 of max 100000 connections
SSL congested action:     Pass
```

keystore

Changes the keystore mode to enable private keys to be secured in the device keystore or the SMS. This command automatically clears the contents of the keystore. If the device is managed by the SMS, first unmanage the device, then use this command to persist private keys on the device.

Only use this command when **absolutely necessary,** such as when the device has lost contact with the SMS, or other similar troubleshooting situations. Under normal conditions, this setting should only be changed by using the SMS.

Change the keystore mode, for example, if the SMS is unreachable and you want the device to persist its own private keys. Use the `sms-unmanage` command to unmanage the device, and then use the `keystore on-device` command to change the keystore mode to the local keystore. After you change the keystore mode, use the `save-config` command to copy the running configuration (which includes the private keys in the Running configuration) to the Start configuration. If the private keys are not in the running configuration, for example, because you rebooted the device after you unmanaged it, use the `private-key` command to import the private keys manually.

Note: When the keystore mode is *sms-managed*, private keys are not persisted in the device keystore.

Syntax

```
keystore on-device|sms-managed
```

Related commands

Command	Description
ips{running-certificates}private-key on page 54	Import the private key from your web server into the local keystore on the device.
ips{running-certificates}certificate on page 53	Import the certificate from your web server into the local keystore on the device.

Command	Description
ips{running-sslinsp}server on page 56	Add an SSL server to the device with the same security settings as your web server, and assign the corresponding certificate and private key.

Configure

This section describes the CLI commands for configuring SSL inspection.

master-key

You can set the master key to a device-generated key that is unique to the device or specify your own *master key passphrase*. By default, TOS v5.0.0 and later encrypts the system keystore with a device-generated master key.

(Best Practice) To avoid keystore issues with a TOS rollback, set the master key to a passphrase that you specify. If the keystore in the rollback image is secured with a different master key than the master key that is set on the device, you can set the master key to the correct passphrase. For more information, see the *Local Security Manager User Guide*.

Before you change the master key, keep in mind the following points:

- By default, the external user disk is not encrypted. You can easily access the contents of the external user disk from a different device.
- If you choose to encrypt the external user disk, the master key encrypts and decrypts the external user disk.
  - If you change the master key while the external user disk is encrypted, all traffic logs, snapshots, ThreatDV URL Reputation Feed, User-defined URL Entries database, and packet capture data are erased from the external user disk.
  - To access the contents of an encrypted external user disk from a different device, for example to restore a snapshot, the same master key must also be set on the device.

Enter an option to set the master key:

- `passphrase` – This option allows you to specify a passphrase for the master key.

  The passphrase must meet the following complexity requirements:

  - Must be between 9 and 32 characters in length
  - Combination of uppercase and lowercase alpha and numbers

  - Must contain at least one special character (!@#$%)

- `device-generated-key` – This option generates a passphrase for the master key.

Syntax

```
master-key (set [device-generated-key|passphrase]|reset-keystore)
```

Example

Set the system master key with your own passphrase.

For security purposes, this command requires you to re-enter your password. If you incorrectly enter your password too many times, you are temporarily locked out for two minutes. To verify your account lock status, enter the `show user locked` command.

```
{}master-key set passphrase
Please validate with your user password:
user password: ********
WARNING: Master key will be set to a passphrase and used to
encrypt the keystore and user disk.
WARNING: This device is currently using a device generated
key. Changing this key will make keystore data in snapshots
created with the previous key non-recoverable.
Do you want to continue (y/n)? [n]: y
Enter Master Key   : **********
Re-enter Master Key: **********
Success: Master key has been set.
```

Example

Set the system master key to a device-generated master key.

For security purposes, this command requires you to re-enter your password. If you incorrectly enter your password too many times, you are temporarily locked out for two minutes. To verify your account lock status, enter the `show user locked` command.

```
{}master-key set device-generated-key
Please validate with your user password:
user password: ********
WARNING: Master key will be set to a device generated key and used
to encrypt the keystore and user disk.
Keystore data in snapshots created with the device generated key
can only be restored to this device.
Do you want to continue (y/n)? [n]: y
Success: Master key has been set to device generated key.
```

Example

Reset the keystore to erase the contents of the system keystore. This command does not change the master key.

For security purposes, this command requires you to re-enter your password. If you incorrectly enter your password too many times, you are temporarily locked out for two minutes. To verify your account lock status, enter the `show user locked` command.

```
{}master-key reset-keystore
Please validate with your user password:
user password: ********
WARNING: This device is currently using a device generated key.
Changing this key will make keystore data in snapshots created with
the previous key non-recoverable.
WARNING: Resetting keystore will delete all private keys currently
held in the keystore.
Do you want to continue (y/n)? [n]: y
Success:
WARNING: All private keys in the keystore have been deleted. Running
configuration may be in an inconsistent state. Please re-import any
previously saved private keys to ensure configuration consistency.
```

user-disk

Mounts, unmounts, and formats the external user disk (CFast or SSD).

After you mount the user disk, the device can automatically mount the disk when you reboot the device.

You can also enable encryption on the external user disk to secure its contents with the system master key. The external user disk stores all traffic logs, snapshots, and packet capture data. By default, the external user disk is not encrypted.

Before you secure the external user disk, keep in mind the following points:

- When you change the encryption status of the external user disk, the device automatically formats the disk and all traffic logs, snapshots, and packet capture data are erased. On large, external CFast disks (32 GB or more), it can take 40 seconds or more to complete disk format and encryption operations.
- The system master key encrypts and decrypts the external user disk. To access the contents of an encrypted external user disk from a different device, for example to restore a snapshot, the same master key must also be set on the device.

Syntax

```
user-disk (encryption (enable|disable) | format | mount |
unmount)
```

Example

Unmount the external user disk.

```
ips{}user-disk unmount
WARNING: Unmounting the external user disk will disable snapshot and
packet capture, and traffic related logs
will be stored in memory only.
Do you want to continue (y/n)? [n]: y
Success: User disk unmounted.
```

Example

Mount the external disk and enable the device to automatically mount the disk on boot.

```
ips{}user-disk mount
Note: The external user disk will be used for snapshots, packet captures
and traffic related logs. The external user disk will be automatically
mounted on rebooted.
Do you want to continue (y/n)? [n]: y
Success: User disk mounted.
```

Example

Format the external user disk.

```
ips{}user-disk format
WARNING: This action will erase all existing data on the external user disk!
Do you want to continue (y/n)? [n]: y
Success: User disk format completed.
```

Example

Enable encryption on the external user disk.

```
ips{}user-disk encryption enable
WARNING: Changing the encryption status of the user disk will erase all
traffic log, snapshot, and packet capture data on the disk.
Do you want to continue (y/n)? [n]: y
Success: User disk encryption enabled.
```

Related commands

show user-disk on page 52

master-key on page 49

show user-disk

Syntax

```
show user-disk
```

Example

```
ips{}show user-disk
External User Disk
   Status:       Mounted
   Encryption:   None
   Capacity:     3952263168 bytes
   Used:         784158720 bytes
   Free:         2907357184 bytes
```

ips{running-certificates}certificate

Add or update a device certificate with the certificate contents from your web server. To inspect secure sessions, the TPS requires both the certificate and private key from your web server.

(Best Practice) Name the certificate so that you can safely and reliably assign it to the correct SSL server.

When the keystore mode is **sms-managed**, use the SMS to manage device certificates and private keys.

Syntax

```
certificate CERTNAME
```

Example

Import the certificate contents from your web server into a device certificate named *mycertname*.

```
ips{running-certificates}certificate mycertname
  Please enter the PEM encoded certificate contents (including
  BEGIN CERTIFICATE and END CERTIFICATE lines):
    -----BEGIN CERTIFICATE-----
    .
    .
    .
    -----END CERTIFICATE-----
```

Related commands

Command	Description
ips{running-certificates}private-key on page 54	Import the private key from your web server into the local keystore on the TPS device.
ips{running-sslinsp}server on page 56	Add an SSL server to the TPS device with the same security settings as your web server, and assign the corresponding certificate and private key.

ips{running-certificates}private-key

Import a private key into the keystore on the device and assign it to the specified device certificate. Use the `save-config` command to secure the private key in the keystore.

To inspect secure sessions, the TPS requires both the certificate and private key from your web server.

When the keystore mode is **sms-managed**, this command is not applicable. Use the SMS to manage device certificates and private keys.

Syntax

```
private-key CERTNAME
```

Example

Import the private key from your web server into the keystore and assign it to its corresponding *`mycertname`* device certificate. Note that if a private key is encrypted, you are automatically prompted to provide the passphrase.

```
ips{running-certificates}private-key mycertname
Please enter the PEM encoded private key contents (including BEGIN
PRIVATE KEY and END PRIVATE KEY lines):
-----BEGIN DSA PRIVATE KEY-----
.
.
.
-----END DSA PRIVATE KEY-----
```

Related commands

Command	Description
ips{running-certificates}certificate on page 53	Import the certificate from your web server into the local keystore on the TPS device.
ips{running-sslinsp}server on page 56	Add an SSL server to the TPS device with the same security settings as your web server, and assign the corresponding certificate and private key.

ips{running-sslinsp} Context Commands

Use the `ssl-insp` context to specify the SSL sessions you want to inspect and to enable or disable SSL inspection.

Note: While SSL inspection is disabled, the TPS does not inspect secure sessions but you can still configure SSL inspection.

Syntax

Use the `help` command to display information about the `ssl-insp` context.

```
ips{running-sslinsp}help
Valid commands are:
  delete log sslInspection CONTACT-NAME
  delete profile (all|PROFILE_NAME)
  delete server (all|SERVER_NAME)
  disable
  enable
  help [full|COMMAND]
  log sslInspection CONTACT-NAME [ALL|none]
  profile PROFILE_NAME
  rename profile PROFILE_NAME NEW_PROFILE_NAME
  rename server SERVER_NAME NEW_SERVER_NAME
  server SERVER_NAME
```

ips{running-sslinsp}enable

Use the `enable` command to begin inspecting SSL sessions based on the configuration you specify. While SSL inspection is disabled, you can configure SSL inspection, but no sessions are inspected.

To enable SSL inspection, the TPS device must be licensed for SSL inspection. Use the LSM to verify the SSL inspection license.

Syntax

```
ips{running-sslinsp} [enable|disable]
```

Example

Enable SSL inspection to begin inspecting SSL sessions.

```
ips{running-sslinsp}enable
```

ips{running-sslinsp}log sslInspection

Use the `log ssllInspection` command to save SSL inspection logging information to a particular notification contact. By default, the TPS device saves SSL inspection log information to the "Management Console" notification contact which is available for display from the LSM and is found in the *sslInspection.log* on the device.

Important: To generate SSL inspection log entries, enable logging on the SSL server for troubleshooting purposes only. By default, an SSL server does not generate logging information. See *ips{running-sslinsp}server* on page 56 for more information.

Syntax

```
log sslInspection CONTACT-NAME [ALL|none]
```

Example

Save SSL inspection logging information to the remote system log servers that are configured in the Remote System Log notification contact.

```
ips{running-sslinsp}log sslInspection "Remote System Log"  ALL
```

ips{running-sslinsp}server

Add or edit an SSL server to specify the SSL server configuration you want the TippingPoint security device to proxy, including the SSL service. You must specify the type of secure traffic that is accepted on the SSL detection port. For example, if the server accepts POP3S traffic on port 2000, add an SSL server with a Detection Port of 2000 and a Decrypted Service of POP3. From the server subcontext, you can view and change the default settings for that server. When you finish, assign the SSL server to an SSL inspection profile. Enable logging on the SSL server for troubleshooting purposes only.

Note: To exit the edit configuration mode from any context, type the `!` command and press Enter.

Syntax

```
[delete] server SERVERNAME
```

Example

Add an SSL server named **myserver** with TLS protocols and cipher suites automatically configured.

```
ips{running-sslinsp}server myserver
```

The context changes to the `running-sslinsp-server-myserver` subcontext.

Tip: The `protocol SSL-PROTOCOL` and `cipher-suite SSL-PROTOCOL` options have "auto-" commands to allow selection of cipher suites by protocol or protocols by cipher suite, respectively. Use the "auto-" command to add or delete ciphers based on what protocol is selected and what it supports. For more information about the available commands in the subcontext, type `help` and press Enter.

```
ips{running-sslinsp-server-myserver}help
Valid commands are:
  certificate SERVERCERT
  cipher-suite all|(protocol SSL-PROTOCOL)|CIPHER-SUITE
  compression enable|disable
  decrypted-service SERVICENAME
  delete cipher-suite all|(protocol SSL-PROTOCOL)|CIPHER-SUITE
  delete description
  delete detection-port (all|PORT [to LAST-PORT])
  delete ip address( all|A.B.C.D/M)
  delete protocol all|SSL-PROTOCOL [auto-delete-ciphers]
  delete rekey-interval
  description TEXT
  detection-port PORT [to PORT]ex
  display [xml]
  help [full|COMMAND]
  ip address( A.B.C.D|A.B.C.D/M)
  logging enable|disable
  protocol all|SSL-PROTOCOL [auto-add-ciphers]
  rekey-interval INTERVAL
  tcp-reset enable|disable
```

Type `display` and press Enter to view the settings for the SSL server.

```
ips{running-sslinsp-server-myserver}display
server "myserver"
  detection-port 443
  decrypted-service http
  protocol TLSv1.0
  protocol TLSv1.1
  protocol TLSv1.2
  cipher-suite TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  cipher-suite TLS_RSA_WITH_3DES_EDE_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA256
  cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA256
  logging disable
  compression disable
  tcp-reset enable
exit
```

Note that by default, the IP address and device certificate for the server are not defined, and must be specified separately. For information about changing a particular setting, enter `help` and press Enter.

(Required) Specify the **IP address** of your web server by entering up to 8 IPv4 addresses (separated by commas), or by specifying a CIDR range, such as 192.168.0.1/24.

```
ips{running-sslinsp-server-myserver}ip address 192.168.1.0/24
```

(Required) Specify the **device certificate** that the TPS device uses to decrypt and encrypt HTTP traffic across the specified range of server IP addresses. This setting is required. Make sure that the corresponding private key is assigned to the device certificate.

```
ips{running-sslinsp-server-myserver}certificate mycertificate
```

Type `display` and press Enter to view the updated IP address and certificate for the SSL server.

```
ips{running-sslinsp-server-myserver}display
server "myserver"
  ip address 192.168.0.1/24
  detection-port 443
  decrypted-service http
  protocol TLSv1.0
  protocol TLSv1.1
  protocol TLSv1.2
  cipher-suite TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  cipher-suite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  cipher-suite TLS_RSA_WITH_3DES_EDE_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_128_CBC_SHA256
  cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA
  cipher-suite TLS_RSA_WITH_AES_256_CBC_SHA256
  logging disable
  compression disable
  tcp-reset enable
exit
```

Related commands

Command	Description
ips{running-certificates}certificate on page 53	Import the certificate from your web server into the local keystore on the device.
ips{running-certificates}private-key on page 54	Import the private key from your web server into the local keystore on the device.
ips{running-vsegs-VSEG_NAME}ssl-profile on page 60	Update the virtual segment to assign the SSL inspection profile.
ips{running-sslinsp}profile on page 59	Assign the SSL server to an SSL inspection profile.

ips{running-sslinsp}profile

Add, edit, or delete an SSL inspection profile. An SSL inspection *profile* describes the encrypted traffic that you want to protect using one or more server policies. A *server policy* consists of an SSL server, and any source IP address exceptions. When you add or edit an SSL inspection profile, the CLI context changes to that profile. From the profile subcontext, view and change the default settings for that profile, for example, to add a server policy.

Note: To exit the edit configuration mode from any context, type the `!` command and press Enter.

Syntax

```
[delete] profile PROFILENAME
```

Example

Create a profile named myprofile.

```
ips{running-sslinsp}profile myprofile
```

The context changes to the `myprofile` subcontext.

For information about the available commands in the subcontext , type the `help` command and press Enter.

```
ips{running-sslinsp-myprofile}help
Valid commands are:
  delete description
  delete policy all|POLICYNAME
  description TEXT
  display [xml]
  help [full|COMMAND]
  policy NEWPOLICYNAME
  policy POLICYNAME
  rename policy POLICYNAME NEWPOLICYNAME
```

(Required) Add a policy named `mypolicy` to the profile.

```
ips{running-sslinsp-myprofile}policy mypolicy
```

The context changes to the **mypolicy** policy.

(Required) Assign an SSL inspection server named **mysslserver** to the policy. Note that the SSL server specifies the range of server IP addresses you want to protect along with your SSL server configuration details.

```
ips{running-sslinsp-myprofile-mypolicy}server mysslserver
```

(Optional) Update the policy to specify any source IP addresses that you do not want to inspect. Secure sessions between the server and the specified source IP addresses are not inspected. In the following example, the server policy does not inspect inbound encrypted traffic between **mysslserver** and client IP addresses within the range of 10.7.0.1/24.

```
ips{running-sslinsp-myprofile-mypolicy}ip-exception
 src-address 10.7.0.1/24
```

Related commands

Command	Description
ips{running-certificates}certificate on page 53	Import the certificate from your web server into the local keystore on the device.
ips{running-certificates}private-key on page 54	Import the private key from your web server into the local keystore on the device.
ips{running-vsegs-VSEG_NAME}ssl-profile on page 60	Update the virtual segment to assign the SSL inspection profile.
ips{running-sslinsp}server on page 56	Add an SSL server with its assigned security certificate and private key.

ips{running-vsegs-VSEG_NAME}ssl-profile

Edit the virtual segment to assign an SSL inspection profile.

Syntax

```
ssl-profile PROFILENAME
```

Example

```
ips{running-vsegs}virtual-segment v1
ips{running-vsegs-v1}ssl-profile webprofile
```

Related commands

Command	Description
ips{running-sslinsp}profile on page 59	Create an SSL-inspection profile.

commit

Commits your pending configuration changes to the Running configuration.

When you commit configuration changes, or when changes are committed automatically, the changes are committed to the Running configuration, and the changes are visible to all users. However, when the device reboots, the Running configuration is reset to the Startup configuration. Uncommitted changes and committed changes in the Running configuration are lost.

Tip: To copy the Running configuration to the Startup configuration without exiting the configuration mode, prepend the `save-config` command with an exclamation mark (!), for example `!save-config`. This command does not commit any pending changes to the Running configuration.

Syntax

```
commit
```

To commit your pending changes to the Running configuration, and then copy the Running configuration to the Startup configuration, enter the following commands:

```
ips{running}commit
```

```
ips{running}!save-config
```

Related commands

Command	Description
save-config on page 62	Copy the Running configuration to the Startup configuration.

save-config

Copies the Running configuration to the Startup configuration. When you reboot the device, the Startup configuration is applied to the device.

Tip: To run this command, you must be at the top-level root `ips{}` mode. To run this command without exiting the current context, prepend an exclamation mark (!) to the command. Note when run from a context, this command does not commit your pending changes to the Running configuration.

Syntax

```
save-config
```

Examples

Copies the Running configuration to the Startup configuration. Note that in order to run this command from the top-level prompt, you must commit or discard your pending configuration changes.

```
ips{}save-config

WARNING: Saving will apply this configuration at the next system
start. Continue (y/n)? [n]:
```

The following example copies the Running configuration to the Startup configuration without exiting the configuration mode. Any pending context configuration changes are preserved.

```
ips{running-sslinsp}!save-config

WARNING: Saving will apply this configuration at the next system
start. Continue (y/n)? [n]:
```

Related commands

Command	Description
commit on page 61	Commit your pending changes to the Running configuration.

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM57886/170718