TREND MICRO™

TippingPoint™ SSL Inspection

User Guide

Privacy and Personal Data Collection Disclosure

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

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

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

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

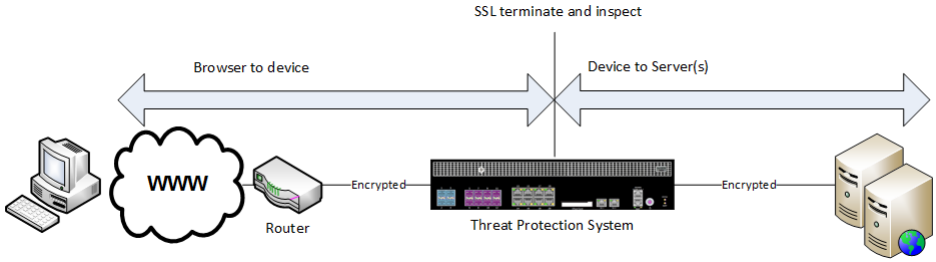
https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

Publication: June 2019

Overview

The Threat Protection System (TPS) security device 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; you can either store them on the device or access them at run-time using the Security Management System (SMS).



With access to your 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.

Considerations

When deploying SSL inspection, consider these points:

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 requires the key to be the same value for both directions. SSL inspection does not support other optional GRE fields, such as GRE sequence number.
Quarantine hosts and redirecting HTTP traffic to another site	When configuring an Action Set to quarantine hosts, if you also configure the response to redirect traffic to an HTTP server, the device redirects the HTTP traffic from the quarantined host but does not redirect the HTTPS traffic.

CONSIDERATION	DESCRIPTION
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 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 apply Digital Vaccine filters to traffic without first decrypting the traffic. If SSL inspection is not configured, the device applies Inspection Bypass, Traffic Management, RepDV, and quarantine filtering against the encrypted traffic. The device applies Digital Vaccine filters, but they do not match against encrypted payload.
Non-encrypted traffic when SSL is configured	• The TPS device drops 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 drops 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 device continues to proxy the SSL session between the client and the server when HTTPS traffic matches a traffic management filter that 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	The TPS device clears proxied SSL sessions when the device enters Intrinsic HA Layer-2 Fallback or Zero Power High Availability (ZPHA).

Requirements

Make sure your environment meets the following requirements:

- Device support – the following TPS devices support SSL inspection:
  - TX Series (5500TX, 8200TX, and 8400TX devices)
  - 2200T device
  - Virtual Threat Protection System (vTPS) (performance mode only, with RDRAND instruction recommended) security devices. For information about how to deploy the vTPS virtual appliance for SSL inspection, see the *vTPS User Guide*.

Note

If you need to configure SSL v3.0 with TLS, always configure all TLS protocols, including TLS v1.0, TLS v1.1, and TLS v1.2. You must enable all SSL protocols between the configured lowest-strength and highest-strength SSL protocols.

Note

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

- Licensing – SSL Inspection is licensed separately. To request an SSL Inspection license, contact your sales representative.
- Cipher suite support – The SMS is capable of configuring the following ciphers if your TOS supports them. Older TOS versions may have limited cipher support. Profile distribution extended status alerts you to any errors:
  - Protocols:
    - TLS v1.2, v1.1, and 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 algorithms:
    - 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 algorithm:
    - RSA (enabled by default)
  - Bulk encryption algorithms:
    - AES256 and AES128 (enabled by default)
    - 3DES (enabled by default)
    - DES (disabled by default)
  - Message Authentication Code (MAC) algorithms:
    - SHA384, SHA256, and SHA1 (enabled by default)
- VLAN translation – SSL inspection requires that you do not configure VLAN translation on the device.
- Asymmetric Network mode – SSL inspection requires that you do not enable Asymmetric Network mode on the device.

License the device

Update your license package to assign an available SSL inspection license to any supported TPS security device.

Note

Manage your license package by using the License Manager on the TMC. When you log in to the TMC, the License Manager is under **My Account > License Manager**.

You can configure the SMS to automatically download updates from the TMC. The SMS downloads the most recent license package to the device within 30 minutes. If necessary, manually import the license package.

1. In the SMS tools, click **Admin**.
2. Click **Licensing**.
3. In the **Licensing** workspace, expand your device to view its capabilities.
4. Ensure that the SSL Inspection capability is assigned to the device and is Allowed. If necessary, the SMS prompts you to resolve any issues:
   - **Reboot required** – Reboot the device to enable the SSL inspection license.
   - **Deny –** Verify the license package assigns the SSL inspection capability to the device.

Enable SSL inspection

Update the device configuration to enable SSL inspection and optionally, to retain private key information. To optimize the available resources on the device, do not enable SSL inspection until you are ready to inspect secure traffic.

Before you begin

If necessary, you can disable SSL inspection on the device and configure SSL inspection.

Procedure

1. In the SMS tools, click **Devices**.
2. Click **All Devices** > ***device_name*** > **Device Configuration**.
3. In the **Device Configuration** workspace, click **Edit**.
4. In **SSL Inspection** options, view the supported SSL ciphers on the device.
5. Configure the following options:
   - **SSL Inspection** – Updates the device configuration to enable SSL Inspection. If the checkbox is grayed, verify the license package has assigned the SSL Inspection capability to the device.
   - **Persist Private Keys** – Enables private key information to be retained in the system keystore. By default, the device automatically retrieves private key information from the SMS and temporarily retains the information in memory until 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.

Complete these tasks to configure SSL inspection:

- *Import an SSL server certificate and private key*
- *Add an SSL server*
- *Add an SSL inspection policy*

Import an SSL server certificate and private key

SSL inspection requires both the SSL certificate and private key from your server of interest. The SMS performs basic validation on the status of the certificate itself. When using a certificate chain, always import any intermediate certificates.

Important

Keep your certificates up-to-date. Whenever you update a certificate on your SSL server, be sure to also replace the certificate on the SMS. *Learn more*.

Procedure

1. In the SMS tools, click **Admin**.
2. Click **Certificate Management** > **Certificates**.
3. In the **Certificates** workspace, click **Import**.
4. In the Import Certificate dialog, enter a certificate name that follows a naming convention so that you can easily assign the correct certificate to the corresponding SSL server.
5. Click **Browse** to locate the certificate file.
6. Select the certificate format, either **Base64 Encoded Certificate (PEM)** or **Encrypted Private Key and Certificate (PKCS12)**.

   Depending on the certificate format, consider the following points:

   - **PEM/DER** format – Always import the private key 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, always enter the appropriate password in the Password box.
   - **PKCS12** format – Enter the appropriate password to import the certificate/key pair. When using a certificate chain, always include any intermediate CA certificates in your import file. Only one file can be imported with the certificate/private key pair and any intermediate CA certificates.
7. Click **OK**. You are now ready to add the SSL certificate to an SSL server.

Add an SSL server

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 Decrypted Service of Other. The TPS device applies DV filters to the incoming traffic, but does not apply them 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.

Procedure

1. In the SMS tools, click **Profiles**.
2. Click **Profiles** > **Shared Settings** > **SSL Servers**.
3. In the **SSL Servers** workspace, click **New**.
4. In the SSL Server dialog, specify the following settings:
   - **Name:** Enter an SSL server proxy name that corresponds to your Web server name so that you can easily associate it with your web server.
   - **Destinations:** Specify the SSL server IPv4 address or CIDR range.
   - **Detection Ports:** Specify the port range of the encrypted application traffic. For example, if your 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, 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 device 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.
   - **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.

     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.
5. 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.
6. Click **OK**. You are now ready to add the SSL server to an SSL inspection policy.

Add an SSL inspection policy

Add an SSL inspection policy to your inspection profile to specify the SSL traffic that you want to inspect, and any client exceptions. Always add an SSL inspection policy to the inspection profile that is assigned to the virtual segment that receives the initial SSL client request to your server.

Procedure

1. In the SMS tools, click **Profiles**.

2. Click **Profiles** > **Inspection Profiles** > ***profile_name*** > **SSL Inspection Policy**.
3. In the **Server Policies** workspace, click **New**.
4. In the Create SSL Inspection Policy dialog, 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 can change the SSL inspection policy.

   Tip

   The **Lock SSL Filter** capability is located under **Profiles > Profile Management > Profile Filter Management > SSL Filter Management**.

5. Specify a policy name, for example, that corresponds to the SSL server configuration.
6. Under Settings, specify the following options:
   - **SSL Server:** Choose the SSL server you want this inspection policy to proxy.
   - **Source Address Exception:** Click **Add** to specify any SSL client IPv4 addresses to exclude from SSL inspection.
7. Click **OK**. You are now ready to distribute your updated inspection profile with the SSL inspection policy.

Inspection profile distribution

Always distribute the inspection profile with your SSL inspection policy to the virtual segment that receives the SSL client request.

Important

You do not need to distribute an SSL inspection policy to the virtual segment that receives the SSL server response. 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 you do not want the device to inspect the decrypted payload in the SSL server response, distribute an inspection profile to the outbound virtual segment that disables the Application filters and the Security filters. To maximize available inspection resources on the device, disable all filter categories and filter overrides in the inspection profile for the outbound virtual segment.

Grant permissions to SSL inspection

Grant permissions so that an assigned user group can configure SSL inspection for particular SSL servers.

Add SSL inspection to the user role

Grant permission to a user role to configure SSL inspection, including:

- SSL inspection profiles
- SSL servers
- SSL global settings

- SSL log
- SSL event information

By default, permissions for SSL inspection are granted to the Administrator role.

Procedure

1. In SMS tools, click **Admin**.
2. Click **Authentication and Authorization** > **Roles**.
3. In the **User Roles** workspace, click **New** to create a user role based on an existing role or click **Edit** to change an existing role. You cannot change the default user roles.
4. In **Capabilities** options, configure the **SSL Server Management** inspection capability under **Profiles** > **Shared Settings Management**.

Grant the user group access to the SSL server

Grant a user group access to your SSL servers. By default, a user group has access to all SSL servers, including new SSL servers that have yet to be defined.

Procedure

1. In the SMS tools, click **Admin**.
2. Click **Authentication and Authorization** > **Groups**.
3. In the **User Groups** workspace, click **New** to create a group or **Edit** to change an existing group.
4. From the **SSL Servers** node, deselect an SSL server to deny access.
5. From the **Profiles** node, deselect an SSL inspection profile to deny access.
6. From the **Devices** node, deselect a device to deny access.

Troubleshoot SSL inspection

If SSL clients cannot reach the server, check Traffic Management and Reputation filters to verify the sessions of interest are not blocked. Traffic Management and Reputation filters are applied before SSL inspection.

View event information

Check the IPS Block and Alert logs, and the Quarantine log for event information about SSL traffic. These logs include an **SSL Inspect** column to report on SSL sessions.

Only URL Reputation gets SSL inspected sessions reported in the Reputation Block and Alert logs. IP and DNS Reputation do not report on SSL sessions because they are analyzed prior to SSL Inspection.

Note

If you see unexpected alerts on SSL traffic, the inspection profile might be inspecting the decrypted server response. *Learn more*.

1. In the SMS tools, click **Devices**.
2. Click **All Devices** > ***device_name***, and then complete these tasks:
   - Click **Events**, and then click the **SSL Sessions** tab to view active session count information for up to 50 SSL sessions.
   - Click **Events** > **Traffic** to view traffic graphs for SSL traffic.

TRAFFIC GRAPH	INFORMATION
SSL Decrypted Traffic	Displays the overall SSL traffic seen and amount inspected.
Active SSL Connection Rate	Displays the total number of new SSL connections that were created during the 1-minute reporting interval.
New SSL Connection Rate	Displays the average number of new SSL connections created per second during the 1-minute reporting interval.

View log information

The SSL Inspection log displays SSL session information, including information about SSL sessions that failed to negotiate SSL parameters. By default, when you add an SSL server, logging is disabled.

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 contain:

- SSL system errors – Check the System log for SSL-related system errors.
- SSL sessions that are Blocked or Quarantined – Check the IPS Block and Alert logs, and the Quarantine log. These logs include an **SSL Inspect** column to report on SSL sessions.

1. In the SMS tools, click **Events**.
2. Click **SSL Inspection Logs**.
3. In the **SSL Log Entries** workspace, view and query the SSL Inspection log.

Note

When you delete an SSL inspection profile or policy, the device continues to inspect the corresponding SSL connections 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.

Basic troubleshooting

If SSL clients are reaching your server but the TPS device is not inspecting some or all of the encrypted sessions of interest, check the following items:

- System log – Determine whether the TPS device is bypassing SSL sessions.
- SSL server configuration – Verify the SSL server IP and ports.
- SSL inspection profile – Confirm any SSL inspection policies do not include a source IP exception that would bypass SSL inspection.
- Virtual segment – consider the following:

- If the virtual segment designates a segment, confirm that it is the correct segment. For example, confirm that interface 1A receives the SSL client request to your SSL server.
- If the virtual segment defines VLANs, confirm that the VLANs are correct for your SSL server.
- If the virtual segment defines source IP addresses, confirm that the SSL client requests correspond to those IP addresses.
- If the virtual segment defines destination IP addresses, confirm that your SSL server corresponds to one of 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 about configuring SSL inspection to block SSL sessions that exceed the maximum threshold, contact customer support.
SSL inspection license is installed and valid	Verify the license package.
SSL inspection is enabled	Enable SSL inspection.
The correct certificate and key are installed	Import the SSL server certificate and private key.
The SSL server matches the correct IP address and port	Edit the SSL server.
The profile is applied to the correct virtual segments	Distribute the inspection profile.
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, troubleshoot the TPS device.

Procedure

1. Verify the list of inspected SSL sessions. In the LSM, click **Monitor > Sessions > SSL Sessions** or, from the device 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 the connection is trying to use compression when the profile does not support it. *Learn more*.

3. Run the **`debug np stats show npSslInspProtocolStats`** command and consider these points:

   - Non-zero entries in the **`clientCipherOther`** counter – Indicate a possibly unsupported cipher. Use the other error counters to narrow the source of the problem to at least the server or the client.

- Server connection failures – Indicate a possibly unsupported cipher, but with the added chance that the server might be asking for a client certificate, which the proxy does not support.

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

Replace an SSL server certificate

Replace an SSL server certificate before it expires. If a certificate expires, the System log generates an error.

When you replace a certificate, consider these points:

- The SMS replaces the certificate on any applicable devices. Replacing the certificate preserves any existing references to the certificate in the device configuration.
- Changes to the device configuration, including certificate replacement, require you to have the **Device X509 Certification Configuration** capability on the device.
- Certificate replacement requires you to have the **Admin X509 Certificate Management** capability.

Important

When configuring SSL, make sure that you update both the device certificate and the SSL webserver certificate before they expire. If the certificates expire or become out of sync, the SSL connections might fail.

Procedure

1. In the SMS tools, click **Admin**.
2. Click **Certificate Management > Certificates**.
3. In the **Certificates** workspace, select a certificate from the list and 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 SMS appends `_REPLACED` to the name of the original certificate.

   The SMS certificate repository automatically updates any managed devices with the new certificate. The SMS displays an error message if the certificate replacement fails on a particular device.