

Inspection of SSL Traffic Overview

Secure Sockets Layer (SSL) is a cryptographic protocol that adds security to TCP/IP communication. Several versions of the SSL and Transport Layer Security (TLS) protocols are in widespread use in applications like Web browsing, electronic mail, Internet faxing, instant messaging, and voice over IP (VoIP). SSL and TLS encrypt the Transport Layer protocol datagrams that carry the payload of these communications. While encryption is an excellent way to keep private data from prying eyes, without inspection by the IDP appliance, it also unwittingly opens a network to dangerous viruses, trojans, or network attacks.

To inspect the HTTP payload of HTTPS traffic, the IDP Series device must decrypt the HTTPS session. Your security policy can examine both the SSL session and the decrypted HTTP payload.

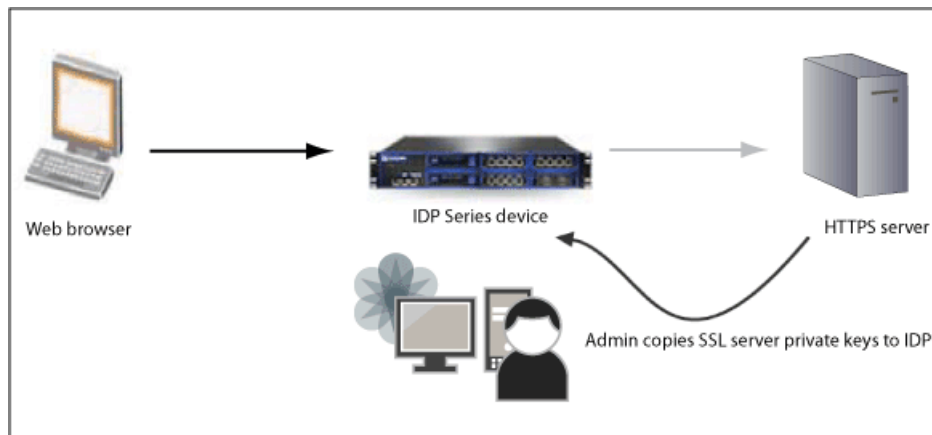
The following sections describe alternative methods you can use to enable SSL inspection:

- Using the SSL Server Private Keys on page 1
- Using a Root Certificate Authority in SSL Forward Proxy Operations on page 2
- Supported SSL Specifications on page 2

Using the SSL Server Private Keys

As of IDP Release 3.2r1, we have supported inspection of client-to-server traffic to internal SSL servers. As shown in Figure 1, this method depends on administrative access to the SSL server private keys.

Figure 1: SSL Inspection Using SSL Server Private Keys

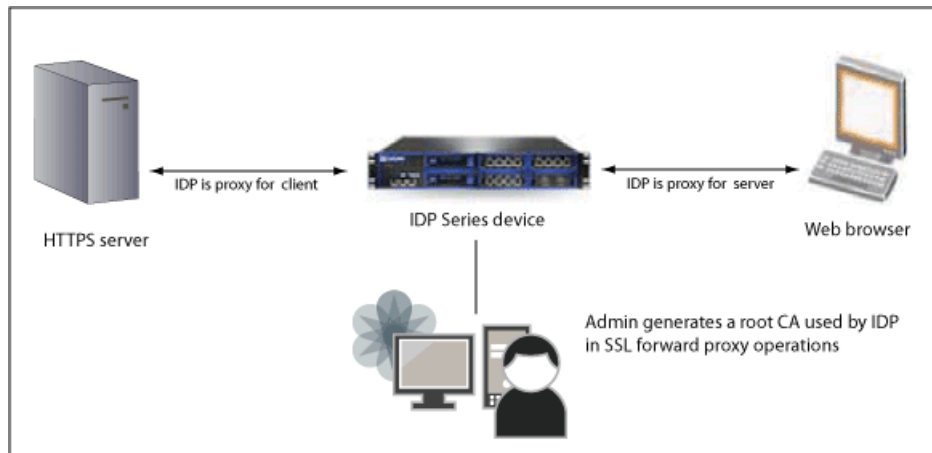


You must be able to copy the SSL server private key to the IDP SSL keystore. The IDP Series device uses the key to decrypt the inbound traffic so that it can inspect the payload. The private key must be in Privacy-Enhanced Mail (PEM) format. We have verified support for the following RSA private key lengths: 1024 bits, 2048 bits, 3072 bits, and 4096 bits.

Using a Root Certificate Authority in SSL Forward Proxy Operations

As of IDP Release 5.0r2, we support inspection of traffic to HTTPS servers where you do not have access to the SSL private key, such as outbound traffic to the WWW. As shown in Figure 2, this method uses a root certificate authority (CA) to proxy the SSL key negotiation. The IDP Series device inserts itself into the SSL key negotiation phase so that it can decrypt the HTTPS session and inspect the session and payload according to your security policy.

Figure 2: SSL Inspection Using a Root CA



When the special root CA is present, the IDP Series device intercepts the HTTPS connection and makes a request to the server as if it were the client; it presents to the client a CA (derived from the special root CA) as if it were the server. The IDP Series device then negotiates the key exchange, decrypts the session, inspects the payload, and re-encrypts the session as necessary before forwarding.

To ensure employee or customer privacy, you can configure a whitelist to exclude matching sessions from being processed by the SSL forward proxy feature. Traffic to destination servers on your whitelist is not intercepted and is passed through uninspected.



NOTE: When both the CA and server private keys are present, the IDP Series device uses the SSL forward proxy method to inspect HTTPS traffic.

Supported SSL Specifications

The IDP Series appliance supports decryption of HTTPS traffic that uses SSLv3 and TLSv1. The IDP Series appliance can inspect an SSLv2 header for anomalies, but it cannot decrypt and examine the HTTP payload in such sessions. In addition, the IDP Series appliance does not support inspection of compressed TLS traffic.

Table 1 lists the SSL cipher suites supported by the two IDP SSL inspection methods.

Table 1: Supported SSL Cipher Suites

Cipher Suite	Decryption Using Private Keys	Decryption Using Forward Proxy
Name: TLS_RSA_WITH_NULL_MD5 Authorization: RSA Key Exchange: RSA Encryption: NULL Digest: MD5	Yes	Yes
Name: TLS_RSA_WITH_NULL_SHA Authorization: RSA Key Exchange: RSA Encryption: NULL Digest: SHA	Yes	Yes
Name: TLS_RSA_WITH_RC4_128_MD5 Authorization: RSA Key Exchange: RSA Encryption: RC4_128 Digest: MD5	Yes	Yes
Name: TLS_RSA_WITH_RC4_128_SHA Authorization: RSA Key Exchange: RSA Encryption: RC4_128 Digest: SHA	Yes	Yes
Name: TLS_RSA_WITH_DES_CBC_SHA Authorization: RSA Key Exchange: RSA Encryption: DES_CBC Digest: SHA	Yes	Yes

Table 1: Supported SSL Cipher Suites (continued)

Cipher Suite	Decryption Using Private Keys	Decryption Using Forward Proxy
Name: TLS_RSA_WITH_3DES_EDE_CBC_SHA Authorization: RSA Key Exchange: RSA Encryption: 3DES_EDE_CBC Digest: SHA	Yes	Yes
Name: TLS_RSA_WITH_AES_128_CBC_SHA Authorization: RSA Key Exchange: RSA Encryption: AES_128_CBC Digest: SHA	Yes	Yes
Name: TLS_RSA_WITH_AES_256_CBC_SHA Authorization: RSA Key Exchange: RSA Encryption: AES_256_CBC Digest: SHA	Yes	Yes

Related Topics The following related topics are included in the *IDP Concepts and Examples Guide*:

- Example: Implementing Inspection of Outbound SSL Traffic
- Example: Exempting Outbound SSL Traffic from Inspection

The following related topics are included in the *IDP Administration Guide*:

- Using the SSL Private Server Key to Enable Inspection of SSL Traffic
- Using the SSL Forward Proxy Feature to Enable Inspection of HTTPS Traffic
- Exempting HTTPS Traffic from Inspection

Published: 2010-01-12