

---

## Configure HTTP/HTTPS Proxy

 For supported software information, click [here](#).

Versa Operating System™ (VOS™) devices inspect HTTPS traffic without decrypting the connections. While the HTTP content of an HTTPS session is encrypted, the SSL certificate is transmitted without encryption. You can configure VOS devices to inspect the various attributes of the SSL certificate and enforce policy based on the inspection.

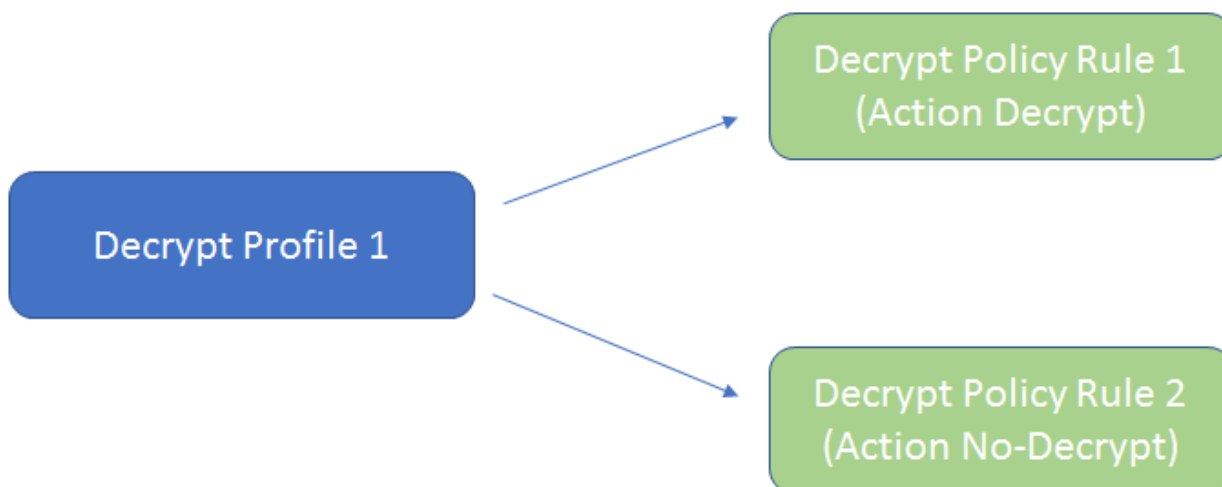
Note that the VOS software does not support decryption of the QUIC protocol. For the VOS security software modules to work, you must block QUIC traffic.

---

## Configure SSL Inspection and Decryption

For SSL inspection, you configure a decryption policy, which includes one or more rules, and you configure one or more decryption profiles. You associate a decryption profile with a decryption policy, and in this way the profile is applied to traffic that matches a rule in the decryption policy. You can configure one or more decryption profiles for each tenant.

As an example of a decryption policy, you can apply a decryption profile that enforces decrypt and do not decrypt actions, as illustrated in the following figure.



To define traffic decryption for security policies on VOS devices, you configure a decryption policy on the VOS device. In the decryption policy, you specify the URL categories for the traffic that you want to decrypt. Currently, VOS devices

support only HTTPS.

Normally, encrypted traffic is not blocked, and it is shaped according to the security settings. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network.

You can configure a decryption profile that contains SSL inspection and policy enforcement information.

Applying a decryption policy requires a certificate.

You can configure the policy action for SSL certificates based on the following:

- Restricted certificate extensions
- Sites with expired SSL certificates
- Sites with untrusted issuers
- Unsupported ciphers
- Unsupported key lengths
- Unsupported versions

You can configure the following policy actions to apply to the inspection results:

- Alert
- Allow
- Drop packet
- Drop session
- Reject

To configure SSL inspection and decryption, you do the following:

1. [Create a CA certificate key.](#)
2. [Create a certificate on a VOS device.](#)
3. [Configure an SSL decryption and inspection profile.](#)
4. [Configure an SSL decryption policy.](#)
5. [Configure an SSL decryption policy rule.](#)
6. [Upload a trusted CA database.](#)
7. [Upload a CA certificate.](#)

You can also [export a CA certificate to a file.](#)

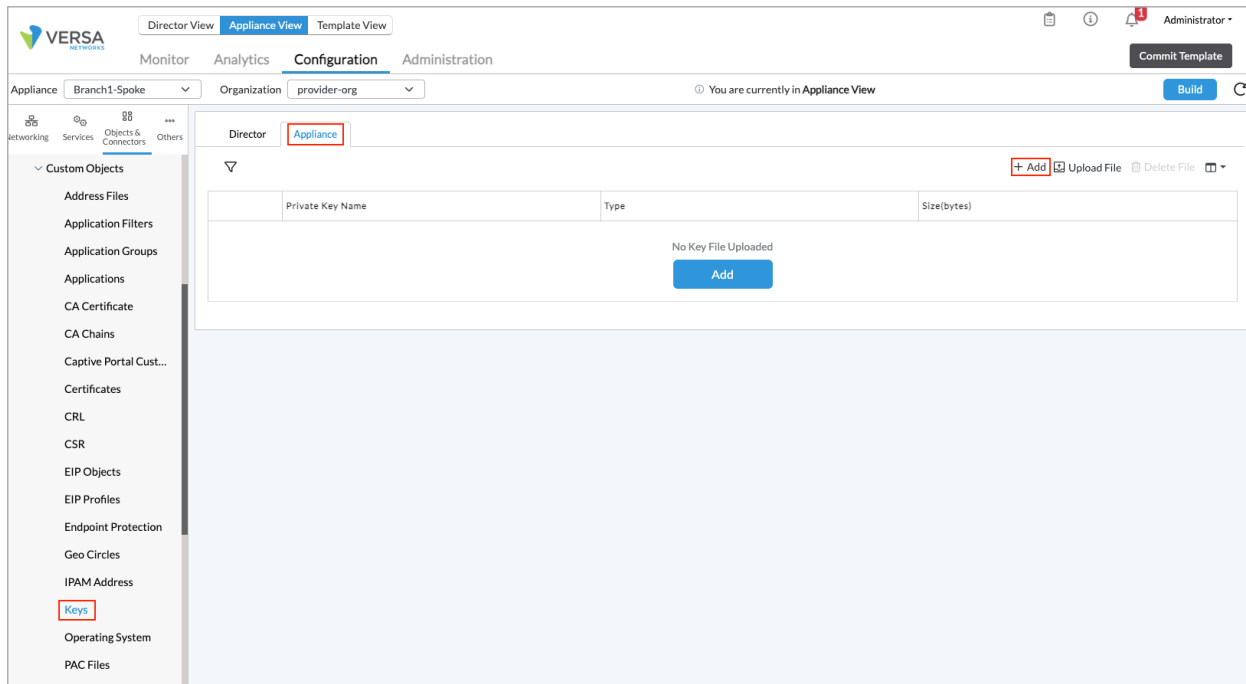
---

## Create a CA Certificate Key

On a VOS device, a key is required to access secured traffic using a certificate. To secure the traffic on a VOS device, you can use either a self-signed CA certificate or a trusted CA certificate.

To create a key for a CA certificate:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Objects & Connectors > Objects > Custom Objects > Keys in the left menu bar.



5. Select the Appliance tab, and then click the **+** Add icon in the main pane. In the Generate Key on Appliance popup window, enter information for the following fields.

Generate Key On Appliance

Name \*

Type

RSA

▼

Type

2048

▼

Pass Phrase

👁

OK

Cancel

Field	Description
Name	Enter a name for the certificate key.
Type	Select the encryption type to use to securely encode and decode the information: <ul style="list-style-type: none"> <li>◦ ECDSA</li> <li>◦ RSA</li> </ul>
Size	Select the RSA key size: <ul style="list-style-type: none"> <li>◦ 2048 bits</li> <li>◦ 4096 bits</li> </ul>
Pass Phrase	Enter the pass-phrase key, or password, to use to encrypt the file that contains the RSA key.

6. Click OK.

## Create a Certificate on a VOS Device

To create a certificate on a VOS device and associate it with a certificate key:

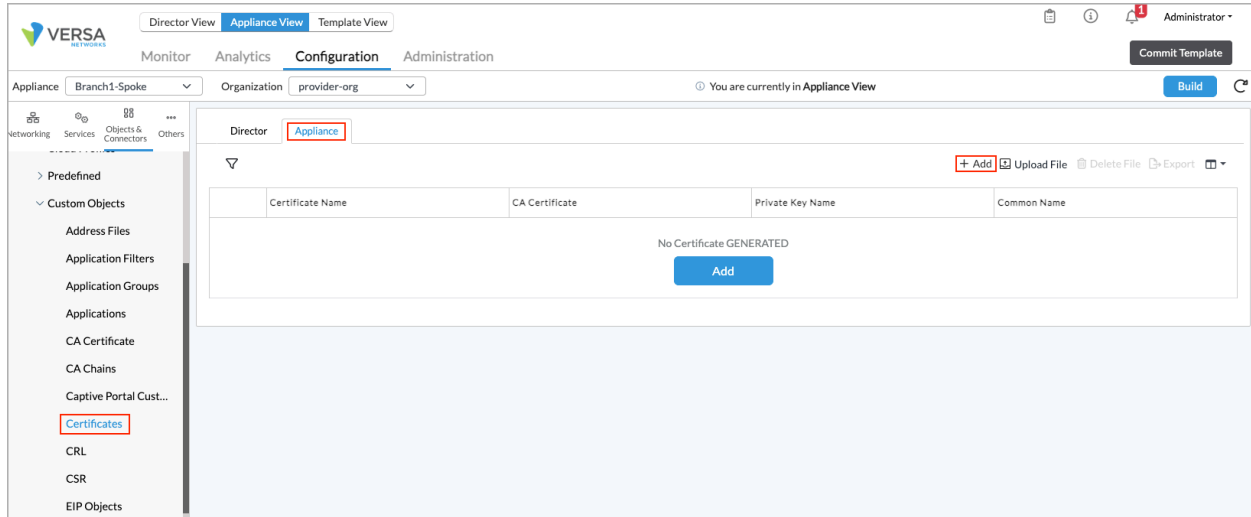
1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.


[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)

Updated: Wed, 23 Oct 2024 08:18:18 GMT

Copyright © 2024, Versa Networks, Inc.

- c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Objects & Connectors > Objects > Custom Objects > Certificates in the left menu bar.



5. Select the Appliance tab, and then click the  Add icon in the main pane. In the Generate Certificate on Appliance popup window, enter information for the following fields.

Generate certificate On Appliance

Certificate Name \*

Validity (days)

Certificate Attributes

CA Certificate

☐ True

☒ False

Serial#

Signature Algorithm

SHA1

Common Name \*

Email ID

Country Name

State or Province

Locality

Organization

provider-org

Organization Unit

Private Key Name \*

--Select--

+ Private Key

OK

Cancel

Field	Description
Certificate Name	Enter a name for the certificate.
Validity	Enter how long the certificate is valid, in days <i>Default: 365 days</i>
Certificate Attributes (Group of Fields)	Configure properties of the certificate.
◦ CA Certificate	Click true to have the certificate be a trusted CA certificate.
◦ Serial Number	Enter the serial number of the certificate.
◦ Signature Algorithm	Select the signature algorithm to use with the certificate: <ul style="list-style-type: none"> <li>◦ SHA-1</li> <li>◦ SHA-256</li> <li>◦ SHA-384</li> </ul>
◦ Common Name	Enter a common name for the certificate.
◦ Email ID	Enter the email address to which to send the certificate.
◦ Country Name	Enter the country where the VOS device is located.
◦ State or Province	Enter the state or province where the VOS device is located.
◦ Locality	Enter additional information about the location of the VOS device.
◦ Organization	Enter the name of the organization or entity to which the VOS device belongs.
◦ Organization Unit	Enter the name of the organizational unit to which the VOS belongs.
Private Key Name	Select the name of the key to associate with the certificate.
+ Private Key	Click to add a private key.

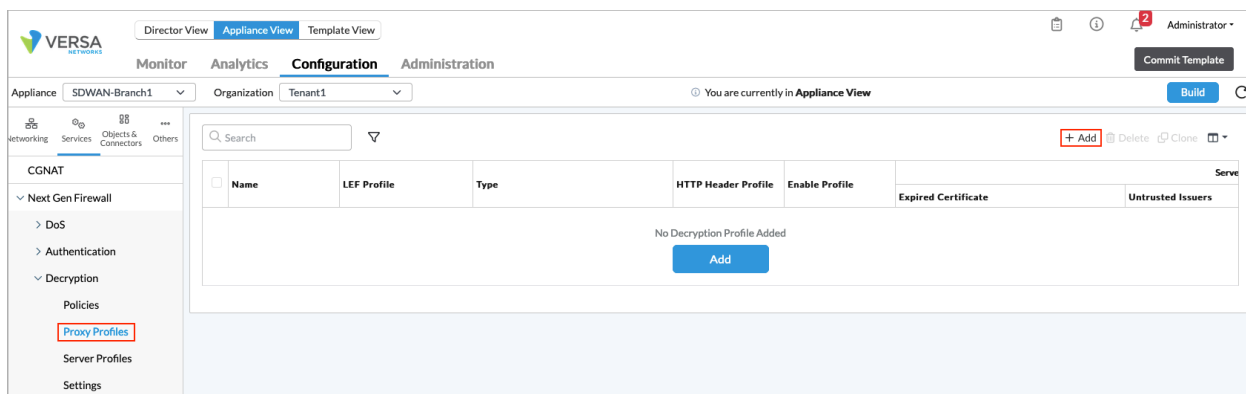
6. Click OK.

## Configure an SSL Decryption Profile

To decrypt or inspect traffic properties, you create an SSL decryption profile and then associate it with a decryption policy rule. The decryption profile is applied to traffic that matches the decryption rule.

To configure an SSL decryption profile:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Services > Next-Gen Firewall > Decryption > Proxy Profiles in the left menu bar.



5. Click the **+** Add icon. The Add Decryption Profile popup window displays. For Releases 22.1.1 and later, the Add Decryption Profile window has four tabs, for Releases 21.2, the Add Decryption Profile window has three tabs, and for earlier releases, it is a single window.
6. Select the General tab, and then enter information for the following fields.



Add Decryption Profile

General

SSL Inspection

SSL Protocol

Advanced

Name \*

Description

Tags

☒ Enable Profile

☐ Support Session Ticket

☒ Use Extended Master Secret

Type \*

--Select--

Trusted Certificate Database \*

default

CA Certificate \*

--Select--

LEF Profile

--Select--

☐ Default Profile

LEF Log Level

Alert

OK

Cancel

Field	Description
Name	Enter a name for the decryption profile.
Description	Enter a text description for the decryption profile.
Tags	Enter a keyword or phrase that allows you to filter the profile name. Tags are useful when you have many profiles and want to view particular ones.
Enable Profile	Click to enable the decryption profile.
Support Session Ticket	Click to enable a session that was created earlier.
Use Extended Master Secret	Click to use the TLS extended master secret extension. This TLS option helps prevent man-in-the-middle attacks.
Type	Select the decryption type to use with the profile, either SSL Forward Proxy or SSL Full Proxy.
<ul style="list-style-type: none"> <li>SSL Forward Proxy</li> </ul>	<p>SSL forward proxy is a transparent proxy that can decrypt and encrypt the SSL/TLS traffic between the client and the server. With a transparent proxy, neither the client nor the server knows about the proxy's presence. Rather, the proxy acts as a server towards the client and as a client towards the server.</p> <p>Whether to decrypt can be controlled through the decryption policy. When the client initiates an SSL/TLS handshake towards the server, the proxy applies the decryption policy to determine whether the traffic needs to be decrypted. If the policy action is to decrypt, the proxy uses the matching SSL profile to initiate the SSL handshake towards the server, and the policy inspects the server certificate and other SSL attributes from the SSL handshake stream. If the inspection is successful, the proxy completes the SSL handshake with the server and generates a server certificate signed with the public key specified in the SSL proxy profile, and it resumes the SSL handshake towards the client. After the SSL handshake between the client and the proxy completes, the proxy is able to decrypt application traffic sent by the client. After</p>

	<p>the traffic is decrypted, it can be examined by the other services in the firewall service chain before before it is encrypted and sent to the server.</p> <p>When you select SSL Forward Proxy mode, the Start TLS fields display. Choose one or more of the following options:</p> <ul style="list-style-type: none"> <li>◦ IMAP</li> <li>◦ POP3</li> <li>◦ SMTP</li> </ul>
<ul style="list-style-type: none"> <li>◦ SSL Full Proxy</li> </ul>	<p>When you select SSL Full Proxy mode, the Mode field display. Click to select the proxy mode:</p> <ul style="list-style-type: none"> <li>◦ Explicit</li> <li>◦ Transparent</li> </ul>
	<p>Explicit mode processes SSL/TLS traffic destined to a specific IP address and a specific port. On the client, you configure the proxy IP address and the port. The explicit SSL full proxy works as follows:</p> <ol style="list-style-type: none"> <li>1. The client connects to the configured proxy IP address and port and sends an HTTP Connect request.</li> <li>2. The SSL full proxy parses the HTTP Connect request and extracts the domain that the client wants to connect to. The proxy uses the domain</li> </ol>

Start Tls

☐ IMAP ☐ POP3 ☐ SMTP

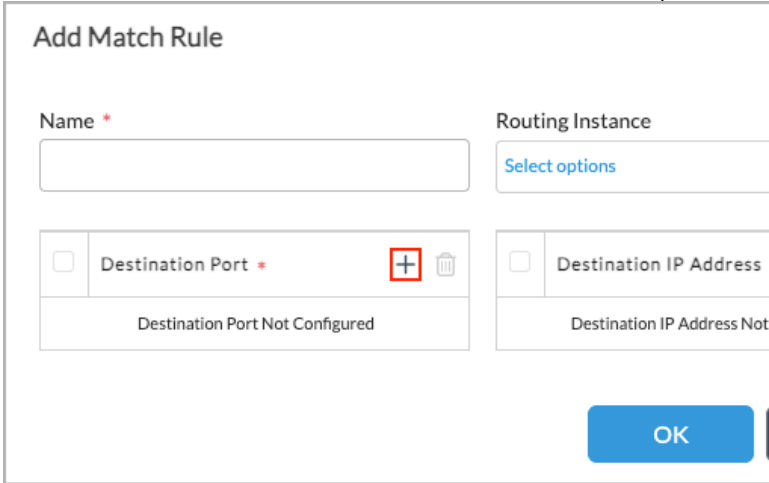
Mode

☐ Transparent ☒ Explicit

Match Rule + ⌵ ⌶ ⌷

<input type="checkbox"/>	Name
No Match Added	

	<p>and other Layer 3 and Layer 4 parameters to locate a decryption policy. If the proxy finds a decryption policy, it decrypts or bypasses the SSL connection based on the action in the policy. If there is no policy, decryption is bypassed.</p> <ol style="list-style-type: none"> <li>3. The SSL full proxy responds with a 200 OK message. When the proxy receives a client Hello message, if the policy decision was to decrypt, the SSL proxy responds with a server Hello message and the remainder of the handshake message between the client and the proxy is exchanged.</li> <li>4. After the handshake completes, the client does a GET or a POST on the connection.</li> <li>5. The proxy parses the HTTP request and extracts the domain name and port from the URL. The proxy then performs a DNS resolution of that domain and opens a connection towards the resolved IP address using the source IP address and port from the configured SNAT pool referenced in the HTTP proxy profile.</li> <li>6. When the connection is successful, the proxy initiates the SSL handshake with the server and then forwards the HTTP request to the server.</li> <li>7. All the other services in the service chain, such as PS/IDS and antivirus, examine the decrypted stream to look for any threats, and they may drop the packet based on the outcome of their examination.</li> </ol> <p>Transparent mode processes SSL/TLS traffic destined to any IP address but to a specific port. The transparent process works the same as the explicit process, except for the DNS resolution process. Because the destination IP address is the actual address of the server, the proxy skips DNS resolution, DNS resolution is done on the client, and the client opens the connection to the server IP address. The proxy uses the SNAT pool configured in the HTTPS proxy profile to perform source NATing.</p> <p>In the Match Rule table, select the rule containing the match conditions. To add a match condition rule, click the + Add icon. In the Add Match Rule popup window, enter information for the following fields.</p>
--	--

	 <ul style="list-style-type: none"> <li>◦ Name—Enter a name for the match rule.</li> <li>◦ Routing Instance—Select the routing instance in which to apply the rule.</li> <li>◦ Destination Port—Click the + Add icon, and enter the destination port to match.</li> <li>◦ Destination IP Prefix—Click the + Add icon, and enter the destination IP prefix to match.</li> </ul>
Trusted Certificate Database	Select the trusted certificate database to use to verify and confirm the authority of the server certificate.
CA Certificate	Select the certificate authority (CA) that issues the decryption server certificate. A CA is an entity that issues digital certificates to verify the ownership of a public key.
LEF Profile	Select a log export functionality (LEF) profile to use to capture SSL logs for the decryption profile. For information, see <a href="#">Configure Log Export Functionality</a> .
◦ Default Profile	Click to use the default LEF profile instead of the LEF profile selected in the previous field.
◦ LEF Log Level	If you select Default Profile, select the LEF log level.

7. Select the SSL Inspection tab, and then enter information for the following fields. For Releases 21.2.1 and earlier, these fields are on the main Add Decryption Profile popup window.

Add Decryption Profile

General

SSL Inspection

SSL Protocol

Advanced

OCSP

☐ Enabled

☐ Block Unknown Certificate

Response Timeout

5

Verify

--Select--

☐ CRL Check

☐ Fetch issuer using AIA issuer

Server Certificate Checks

Action for Expired Certificate

--Select--

Action for Untrusted Issuers

--Select--

☒ Restrict Certificate Extension

Unsupported Mode Checks

Action for Unsupported Cipher

--Select--

Min Supported Key Length

512

Action for Unsupported Key Length

--Select--

Action for Unsupported Version

--Select--

SNAT Pool

--Select--

☐ SNAT Pool Default

+ SNAT Pool

OK

Cancel

Field	Description
OCSP (Group of Fields)	For Releases 21.2.1 and later.
◦ Enabled	Click to enable server certificate verification using the Online Certificate Status Protocol (OCSP).
◦ Block Unknown Certificate	Click to block SSL sessions whose certificate status is unknown.
◦ Response Timeout	<p>Enter the timeout for an OCSP request.</p> <p><i>Default:</i> 5 seconds</p> <p><i>Value:</i> 0 through 255 seconds</p>
Verify	<p>Select the type of verification:</p> <ul style="list-style-type: none"> <li>◦ Client</li> <li>◦ Server</li> <li>◦ Server and Client</li> </ul>
CRL Check	Click to enable checking of the certificate revocation list (CRL). If enabled, the received server certificates are matched against the CRL. For more information, see <a href="#">Upload CRL Files</a> .
Fetch Issuer Using AIA Issuers	<p>(For Releases 22.1.2 and later.) Click to fetch intermediate certificates from the issuing certification authority. Authority Information Access (AIA) is an SSL certificate extension that contains information about the issuer of the certificate. If a server does not provide intermediate certificates, the certificates can be downloaded from the link contained in the AIA field.</p> <p>For this option to work, you must select a pool in the SNAT Pool field or you must click SNAT Pool Default.</p>
Server Certificate Checks (Group of Fields)	
◦ Action for Expired Certificate	Select the predefined or user-defined action to take when the server certificate expires. The following are

	<p>the predefined actions:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the decrypt session and generate an entry in the SSL log.</li> <li>◦ Allow—Allow the decrypt session without generating an entry in the SSL log.</li> <li>◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of a delayed response from the server or because a firewall blocked access to the website.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Action for Untrusted Issuers</li> </ul>	<p>Select the predefined or user-defined action to imply when the certificate is from an untrusted issuer. The following are the predefined actions:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the decrypt session and generate an entry in the SSL log.</li> <li>◦ Allow—Allow the decrypt session without generating an entry in the SSL log.</li> <li>◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to</li> </ul>



	determine whether this occurred because of a delayed response from the server or because a firewall blocked access to the website.
◦ Restrict Certificate Extension	Click to restrict certificate extensions.
Unsupported Mode Checks (Group of Fields)	
◦ Action for Unsupported Cipher	<p>Select the predefined or user-defined action to take when the decryption encounters an unsupported cipher:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the decrypt session and generate an entry in the SSL log.</li> <li>◦ Allow—Allow the decrypt session without generating an entry in the SSL log.</li> <li>◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of a delayed response from the server or because a firewall blocked access to the website.</li> </ul>
◦ Minimum Supported Key Length	Enter the minimum RSA key length, in bits. <i>Default:</i> 512 bits
◦ Action for Unsupported Key Length	<p>Select the action to take when the decryption encounters an unsupported key length:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the decrypt session and generate an entry in the SSL log.</li> <li>◦ Allow—Allow the decrypt session without generating an entry in the SSL log.</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of a delayed response from the server or because a firewall blocked access to the website.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Action for Unsupported Version</li> </ul>	<p>Select the action to take when the decryption encounters an unsupported CA version:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the decrypt session and generate an entry in the SSL log.</li> <li>◦ Allow—Allow the decrypt session without generating an entry in the SSL log.</li> <li>◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website.</li> <li>◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of a delayed response from the server or because a firewall blocked access to the website.</li> </ul>
SNAT Pool	Select an SNAT pool.
SNAT Pool Default	Click to have the selected SNAT pool be the default pool.

+ SNAT Pool	Click to create a new SNAT pool. For more information, see <a href="#">Configure SNAT Pools</a> .
-------------	---

8. (For Releases 21.2.1 and later.) Select the SSL Protocol tab, and enter information for the following fields. Note that if you do not select key exchange, encryption, and authentication algorithms, all algorithm are considered to be enabled for the selected cipher suites.

Add Decryption Profile

General
SSL Inspection
**SSL Protocol**
Advanced

Min Version
Max Version

TLS-1.1

▼

TLS-1.2

▼

Key Exchange Algorithms

☐ RSA
☐ ECDHE

Encryption Algorithms

☐ AES128-CBC
☐ AES128-GCM
☐ AES256-CBC
☐ AES256-GCM
☐ Camellia-256-CBC
☐ ChaCha20-Poly1305
☐ Seed CBC

Authentication Algorithms

☐ SHA
☐ SHA256
☐ SHA384

Cipher Suites

0 selected

▼

OK

Cancel

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)  
 Updated: Wed, 23 Oct 2024 08:18:18 GMT  
 Copyright © 2024, Versa Networks, Inc.

19

Field	Description
Minimum Version	<p>Select the minimum version of Transport Layer Security (TLS) that is supported. The minimum version must be the same as or earlier than the maximum version.</p> <ul style="list-style-type: none"> <li>◦ TLS 1.0</li> <li>◦ TLS 1.1</li> <li>◦ TLS 1.2</li> <li>◦ TLS 1.3</li> </ul>
Maximum Version	<p>Select the maximum version of TLS that is supported. The maximum version must be the same as or later than the minimum version. The options displayed depend on the version you select in the Minimum Version field. For example, if the minimum version is TLS 1.0, the options TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 are displayed. If the minimum version is TLS 1.2, the options TLS 1.2 and TLS 1.3 are displayed.</p>
Key Exchange Algorithms	<p>When you select minimum and maximum TLS versions and the version is not TLS 1.3, select one or more key exchange algorithms for the SSL connection:</p> <ul style="list-style-type: none"> <li>◦ ECDHE—Elliptic-curve Diffie–Hellman Key Exchange</li> <li>◦ RSA—Rivest–Shamir–Adleman algorithm</li> </ul>
Encryption Algorithms	<p>Select an encryption algorithm to use:</p> <ul style="list-style-type: none"> <li>◦ AES-128-CBC—AES CBC encryption algorithm with 128-bit key</li> <li>◦ AES-128-GCM—AES GCM encryption algorithm with 128-bit key</li> <li>◦ AES-256-CBC—AES CBC encryption algorithm with 256-bit key</li> <li>◦ AES-256-GCM—AES GCM encryption algorithm with 256-bit key</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Camellia-256-CBC—Camellia encryption algorithm with 256-bit key</li> <li>◦ Chacha20-Poly1305—ChaCha stream cipher and Poly1305 authenticator</li> <li>◦ Seed CBC—TLS RSA with seed CBC</li> </ul>
Authentication Algorithms	Click to have the selected LEF profile be the default LEF profile.
Cipher Suites	<p>Select a TLS cipher suite. If you select a cipher suite, it must be consistent with the selected key exchange, encryption, and authentication algorithms. If you do not configure cipher suites, all cipher suites matching the selected the key exchange, encryption, and authentication algorithms are selected by default.</p> <ul style="list-style-type: none"> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SH</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA25</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</li> <li>◦ TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA25</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</li> <li>◦ TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</li> <li>◦ TLS-RSA-WITH-AES-128-CBC-SH</li> <li>◦ TLS-RSA-WITH-AES-128-CBC-SHA256</li> <li>◦ TLS-RSA-WITH-AES-128-GCM-SHA256</li> <li>◦ TLS-RSA-WITH-AES-256-CBC-SHA</li> <li>◦ TLS-RSA-WITH-AES-256-CBC-SHA256</li> </ul>

	<ul style="list-style-type: none"> <li>◦ TLS-RSA-WITH-AES-256-GCM-SHA384</li> <li>◦ TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</li> <li>◦ TLS-RSA-WITH-SEED-CBC-SHA</li> </ul>
--	---

9. (For Releases 22.1.2 and later). Select the Advanced tab. The following screen displays.

10. Enter information for the following fields.

Field	Description
HTTP Header Profile	Select an HTTP header profile or click + Add New to create a new HTTP header profile. For more information, see <a href="#">Configure HTTP Header Profiles</a> .
Client Authentication (Group of Fields)	
<ul style="list-style-type: none"> <li>◦ Trusted Certificate Database for Client Certificate</li> </ul>	Select the trusted certificate database to use to verify and confirm the authority of the server certificate.

Field	Description
◦ Delegate Client Certificate	Select a delegate client certificate.
◦ Certificate Info Header Profile (Group of Fields)	Configure a profile for the certificate information header.
◦ Header	Enter a name for the header profile.
◦ Value	Select a value: <ul style="list-style-type: none"> <li>◦ Common Name</li> <li>◦ Issuer Distinguished Name</li> <li>◦ Subject Distinguished Name</li> <li>◦ Validity Not After</li> <li>◦ Validity Not Before</li> </ul>
◦ Name Option	If you select the values Issuer Distinguished Name or Subject Distinguished Name, enter a name for the header value.


11. Click OK.

---

## Configure an SSL Decryption Policy

You configure an SSL decryption policy to specify traffic that you want to decrypt.

To configure an SSL decryption policy:

- In Director view:
  - Select the Administration tab in the top menubar.
  - Select Appliance in the left menu bar.
  - Select a VOS device in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select an organization in the horizontal menu bar.
- Select Services > Next-Gen Firewall > Decryption > Policies in the left menu bar.
- Select the Decryption Policies tab and then click the  Add icon in the main pane. In the Add Decryption Policy popup window, enter information for the following fields.

Add Decryption Policy

×

Name \*

Description

Tags

OK

Cancel

Field	Description
Name	Enter a name for the decryption policy.
Description	Enter a text description for the decryption policy.
Tags	Enter a keyword or phrase that allows you to filter the policy name. Tags are useful when you have many policies and want to view those that are tagged with a particular keyword.

6. Click OK.

## Configure an SSL Decryption Policy Rule

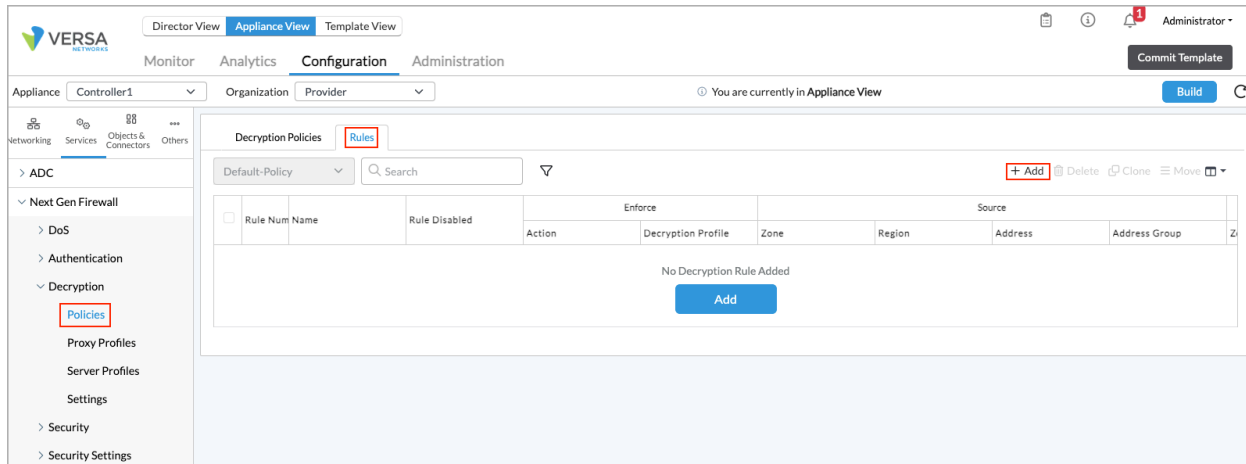
In an SSL decryption policy rule, you define the traffic of interest, and for matching traffic you define whether to decrypt the traffic, inspect the traffic, or both decrypt and inspect it.


When you configure SSL decryption for a tenant, the VOS device behaves as an SSL proxy, and it generates a TLS/SSL certificate for each HTTPS URL that the tenant tries to access (for example, `https://example.com`). The certificate allows the VOS device to inspect the data flow and take any necessary actions. To optimize the SSL proxy behavior, the VOS device uses the same generated public–private key pair for certificates issued across domains. This key pair is generated for each configured decryption profile, and hence is unique for each tenant.

To create the policy rule:



1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Services > Next-Gen Firewall > Decryption > Policies in the left menu bar.



5. Select the Rules tab and click the  Add icon in the main pane. The Add Decryption Rule popup window displays.
6. (For Releases 21.2.1 and later.) If you have already added one or more rules, the Configure Rule Order popup window displays.
  - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

**Add** [Close]

☒ Insert the rule last  
☐ Insert the rule top

Search Rule

1. test
---------

End of records

OK Cancel

- b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:

**Add** [Close]

☒ Insert the rule last  
☐ Insert the rule top  
☐ Insert the rule in specific placement

Search Rule

1. test
2. test1

End of records

OK Cancel

- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
- d. Click OK. The Add Decryption Rule popup window displays.
7. In the Add Decryption Rule screen, select the General tab and then enter information for the following fields.

Add Decryption Rule

General
Source
Destination
Headers/Schedule
URL
Users/Groups
Enforce

Name \*

Description
Tags

☐ Disable Rule

OK
Cancel

Field	Description
Name	Enter a name for the decryption policy rule
Description	Enter a text description for the decryption policy rule.
Tags	Enter a keyword or phrase that allows you to filter the rule name. This is useful when you have many rules and want to view those that are tagged with a particular keyword.
Disable Rule	Click to disable the decryption rule.

- Select the Source tab to define the source zone and the source address of the incoming (source) traffic to which the decryption policy rule applies. Enter information for the following fields.

Add Decryption Rule

General
Source
Destination
Headers/Schedule
URL
Users/Groups
Enforce

☐ Source Zone
+ New Zone
+

Source Zone Not Configured

☐ Source Address
+ New Address
+ New Address Group
+

Source Address Not Configured

☐ Custom Geo Circle
+

Custom Geo Circle Not Configured

☐ Region
+

Region Not Configured

☐ EIP Profiles
+ Add EIP Profile
+

EIP Profiles Not Configured

☐ State
+

State Not Configured

☐ City
+

City Not Configured




☐ Source Address Negate
☐ Source Location Negate

OK
Cancel

Note that in Releases 21.2 and earlier, the Source and Destination information was on the same tab.

The screenshot shows the 'Add Decryption Rule' dialog box with the 'Source/Destination' tab selected. The dialog is divided into two main columns for Source and Destination settings. Each column has a 'Zone' section and an 'Address' section. The 'Source Zone' and 'Destination Zone' sections each have a list of zones and a '+ New Zone' button. The 'Source Address' and 'Destination Address' sections each have a list of addresses and a '+ New Address' button. Below these sections are checkboxes for 'Source Address Negate' and 'Destination Address Negate'. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Description
Source Zone	Select the source zone to which to apply the rule to traffic coming from any interface in the specified zone.  Click the  Add icon to add more security zones.
Source Address	Select one or more source addresses to which to apply the decryption policy rule. Click the  Add icon to add more source addresses.
Custom Geographic Circle	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a custom geographic circle. A geographic circle consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. To configure a custom geographic circle, see <a href="#">Configure Custom Geographic Circles</a> .

Field	Description
Region	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a region. To create a region, see <a href="#">Create a Region</a> .
EIP Profiles	(For Releases 22.1.2 and later.) Click the  Add icon, and then select an endpoint information profile (EIP). To configure an EIP, click + Add EIP Profile. For more information, see <a href="#">Configure EIP Profiles</a> .
State	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a state.
City	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a city.
Source Address Negate	Click to select any source addresses except the configured source addresses.
Source Location Negate	Click to select any source locations except the configured source locations.

9. Select the Destination tab to define the destination zone and the destination address ;of the outgoing (destination) traffic to which the decryption policy rule applies. Enter information for the following fields.

Add Decryption Rule

General
Source
Destination
Headers/Schedule
URL
Users/Groups
Enforce

☐ Destination Zone
+ New Zone
+

Destination Zone Not Configured

☐ Destination Address
+ New Address
+ New Address Group
+

Destination Address Not Configured

☐ Custom Geo Circle
+

Custom Geo Circle Not Configured

☐ Region
+

Region Not Configured

☐ State
+







State Not Configured

☐ City
+

City Not Configured

☐ Destination Address Negate
☐ Destination Location Negate

OK
Cancel

Field	Description
Destination Zone	Select the destination zone to which to apply the decryption policy to traffic coming from all interfaces into a given zone. Click the  Add icon to add more security zones.
Destination Address	<p>Select one or more destination addresses to which to apply the decryption policy rule. Click the  Add icon to add more destination addresses.</p> <p>Note that for an explicit proxy, the destination address is the address on which the explicit proxy is configured. This means that configuring destination addresses for an explicit proxy is not effective.</p>
Custom Geographic Circle	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a custom geographic circle. ;A geographic circle consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. To configure a custom geographic circle, see <a href="#">Configure Custom Geographic Circles</a> .
Region	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a region. To create a region, see <a href="#">Create a Region</a> .
State	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a state.
City	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a city.
Destination Address Negate	<p>Click to select any destination addresses except the configured destination addresses.</p> <p>Note that for an explicit proxy, the destination address is the address on which the explicit proxy is</p>

Field	Description
	configured. This means that configuring destination addresses for an explicit proxy is not effective.
Destination Location Negate	Click to select any destination locations except the configured destination locations.

10. Select the Header/Schedule tab to define the IP header, services and schedule to which the decryption rule applies. Enter information for the following fields.

Add Decryption Rule

General
Source
Destination
**Headers/Schedule**
URL
Users/Groups
Enforce

IP

IP Version
--Select--
IP Flags
--Select--

DSCP

TTL
Condition
Greater than or equal to
Value (Max 255)

Others


Schedules
--Select--
+ Schedule

☐ Services
+ New Service

Services Not Configured

OK
Cancel

Field	Description
IP Version	Enter the IP version for which the decryption rule applies.
IP Flag	For IPv4, select how to fragment packets: <ul style="list-style-type: none"> <li>Don't Fragment</li> <li>More Fragment</li> </ul>
DSCP	Enter a differentiated service code point (DSCP) value to classify an IP packet is queued for forwarding.
TTL (Group of Fields)	
<ul style="list-style-type: none"> <li>Condition</li> </ul>	Select the TTL condition to use for the match. The TTL is the number of hops that a packet can travel before it is discarded and indicates the lifespan of a

Field	Description
	<p>packet. The condition can be one of the following boolean values:</p> <ul style="list-style-type: none"> <li>◦ Greater than or equal to—TTL value must be greater than or equal to the specified value to trigger the security access rule</li> <li>◦ Less than or equal to—TTL value must be less than or equal to the specified value to trigger the security access rule</li> <li>◦ Equal to—TTL value must be equal to the specified value to trigger the security access rule</li> </ul>
◦ Value (Max 255)	<p>Enter the value for the TTL.</p> <p><i>Range:</i> 1 through 255</p> <p><i>Default:</i> None</p>
Others (Group of Fields)	
◦ Schedules	Select a schedule to set the time and frequency at which the rule is in effect.
◦ + Schedule	Click to create a schedule. For more information, see <a href="#">Configure SD-WAN Policy</a> .
Services (Group of Fields)	
◦ Service List	Click the  Add icon to select one or more services to apply the decryption rule to the configured services.
◦ + Service	Click to create a service. For more information, see <a href="#">Configure SD-WAN Policy</a> .

11. Select the URL tab to configure match criteria for URL categories. Enter information for the following fields.



**Add Decryption Rule** ✕

General Source Destination Headers/Schedule **URL** Users/Groups Enforce

☐ URL Category
 + New URL Category +
✕

URL Category Not Configured

☐ URL Reputations
 + 
✕

Predefined Reputations Not Configured

**OK** **Cancel**

Field	Description
URL Category	Click the <b>+</b> Add icon to select one or more predefined/custom URL categories and apply the security access rule to the URL. For information, see <a href="#">Configure URL Files</a> .
Reputations	Click the <b>+</b> Add icon to select one or more predefined URL reputations and apply the security access rule to the URL. For more information, see <a href="#">View a Predefined URL Reputation</a> .

- Select the Users/Groups tab to define the users and user groups to which the rule applies. Enter information for the following fields.

**Add Decryption Rule** ✕

General Source Destination Headers/Schedule URL **Users/Groups** Enforce

Match Users:  ▼

User Group Profile:  ▼

☐ Local Database ☐ External Database

☐ Users
 + New Custom User +
✕



Users Not Configured

☐ Groups
 + New Custom Group +
✕

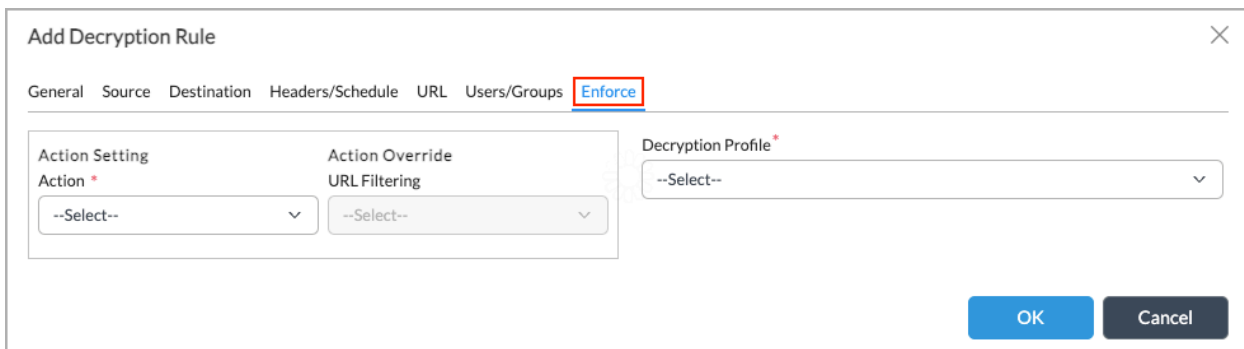
Groups Not Configured

**OK** **Cancel**

Field	Description
Match Users	Select the users to match: <ul style="list-style-type: none"> <li>Any—If you select to match any users, you cannot configure any other fields on this tab.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>Known—If you select to match known users, you cannot configure any other fields on this tab.</li> <li>Selected—If you select to match selected users, you can configure the other fields on this tab.</li> <li>Unknown—If you select to match unknown users, you cannot configure any other fields on this tab.</li> </ul>
User Group Profile	If you match selected users, select a user group profile to match users in a group.
Local Database	If you match selected users, click to create a local database to match users and user groups. Select these users and user groups in the Users and Groups fields.
External Database	If you match selected users, click to use an external database to match users and user groups. Select these users in the Users and Groups fields.
Users	If you match selected users, click the  Add icon and select a user. Select + New Custom User to add a user.
Groups	If you match selected users, click the  Add icon and select a user group. Select + New Custom Group to add a user group.

13. Select the Enforce tab to select the applications and URLs to which the decryption rule applies. Enter information for the following fields.



Field	Description
Action (Required)	Select the action to take on the traffic:

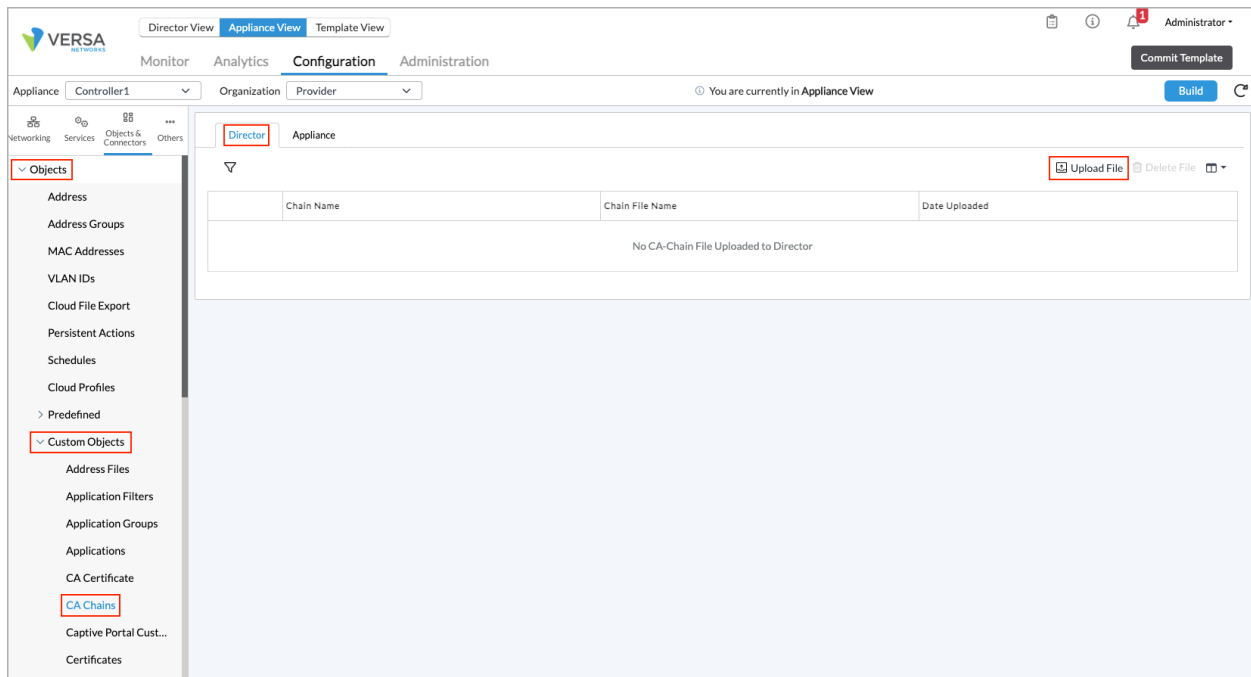
Field	Description
	<ul style="list-style-type: none"> <li>decrypt—Decrypt the traffic.</li> <li>no-decrypt—Do not decrypt the traffic.</li> </ul>
Action Override	If the action selected is decrypt, override the decryption action in a URL filtering profile. This URL filtering must be one in which decrypt bypass is enabled. With the action override, the decryption policy bypasses the URL filtering profile after the captive portal takes an Ask or Justify action before redirecting the user to the domain, and the profile is not decrypted.
<ul style="list-style-type: none"> <li>URL Filtering</li> </ul>	Select the URL filtering profile to which to apply the action override. Select + Add New to add a new URL filtering action override.
Decryption Profile (Required)	If the action you select is decrypt, select the decryption profile. Select + Add New to add a new decryption profile.

14. Click OK.

## Upload a Trusted CA Database

To upload a trusted CA database that verifies and confirms authority of the server certificate and to map it to a decryption profile:

- In Director view:
  - Select the Administration tab in the top menu bar.
  - Select Appliance in the left menu bar.
  - Select a VOS device in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select an organization in the horizontal menu bar.
- Select Objects & Connectors > Objects > Custom Objects > CA Chains in the left menu bar.
- Select the Director tab in the main pane.



6. Click the  Upload icon. The Upload CA Chain to Director popup window displays.

Upload CA Chain to Director

Chain Name \*

Chain File Name \*

Browse

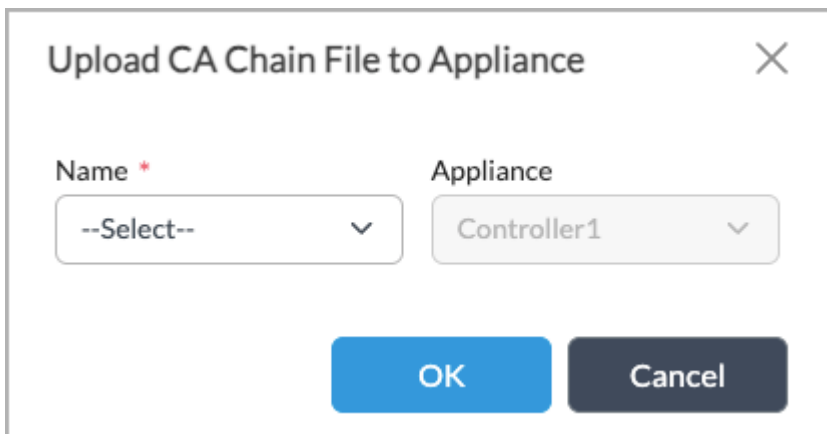
Note - Allowed file formats are .crt, .cer or .pem

OK

Cancel

7. In the Chain Name field, enter a name for the CA chain.
8. Click Browse and select the CA chain file to upload to Versa Director.
9. Click OK.
10. In the main CA Chain screen, select the Appliance tab.

11. Click the  Upload icon. The Upload CA Chain File to Appliance popup window displays.



12. In the Name field, select the name of the CA chain file.
13. In the Appliance field, select a VOS device.
14. Click OK to upload the CA chain file to the VOS device.

---

## Upload a CA Certificate

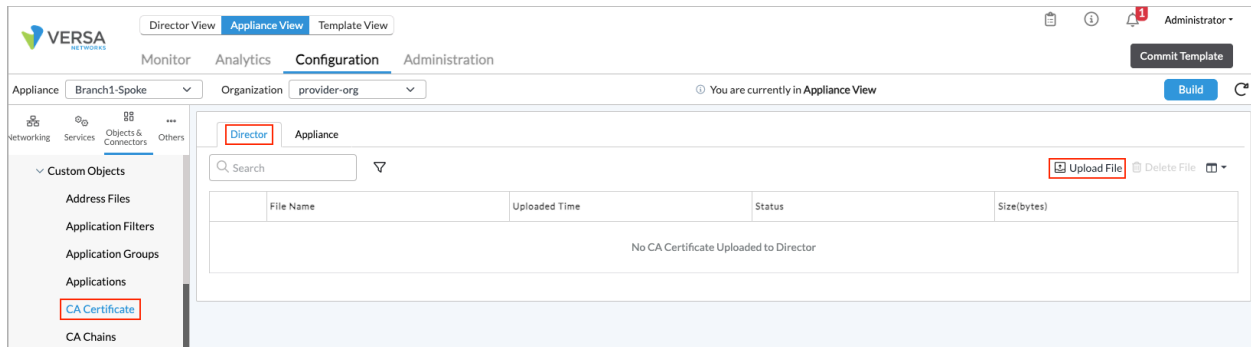
A certificate authority (CA) is an entity that issues digital certificates that are used to verify the ownership of a public key. The digital certificates allow a party to trust the signature that is made by a private key that corresponds to the certified public key.

After a VOS device requests a certificate from a CA server, the CA server issues the certificate. You then need to upload the certificate to the CA database so that it can be used for verification.

You can upload the CA certificate as a bundle of two files (zipped certificate and key), you can upload an existing CA file directly to a VOS device, or you can generate a new CA certificate on the VOS device. If you upload files, they must be in .zip format, and the key file must have the .key extension. The certificate file can have any file extension.

To upload a CA certificate:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Objects & Connectors > Objects > Custom Objects > CA Certificate in the left menu bar.
5. Select the Director tab in the main pane.



6. Click the  Upload File icon. The Upload CA Certificate to Director popup window displays.

### Upload CA Certificate to Director

File Name \*

Browse

CA Chain


--Select--

**Note :**

- The file to be uploaded need to be in .zip format. They will consist of 2 files a key and a certificate. The key file needs to have .key extension there is no restriction on the extension of the certificate file.
- CA Chain is Mandatory for 22.1 devices and above

OK

Cancel

7. Click Browse, and the select the name of the CA database file to upload.
8. In the CA Chain field, select a CA chain. In Releases 22.1 and later, you must select a CA chain.
9. Click OK.
10. In the main CA Certificate screen, select the Appliance tab.
11. Click the  Upload icon. The Upload CA Certificate to Appliance popup window displays.

Upload CA Certificate to Appliance

File Name \*

Appliance

Branch1-Spoke

CA Chain

Note - CA Chain is Mandatory for 22.1 devices and above

OK

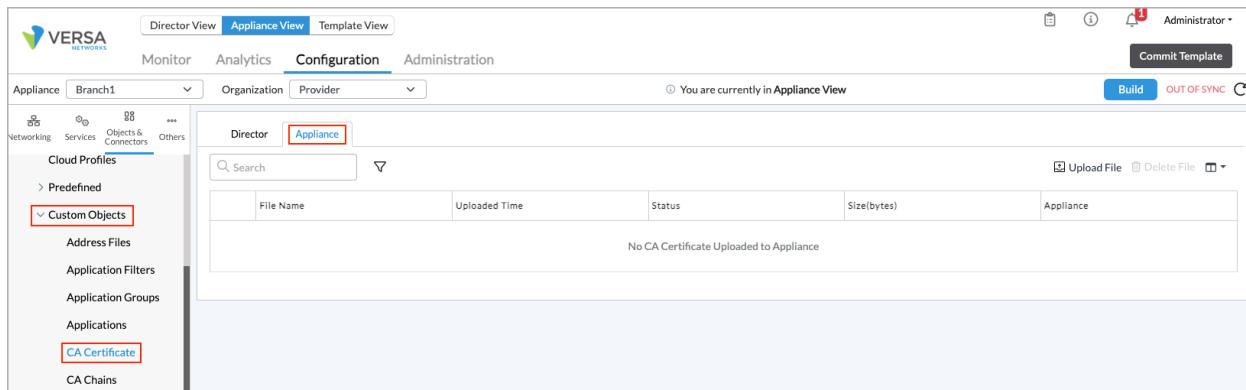
Cancel


12. In the Filename field, select the name of the CA certificate file.
13. In the Appliance field, select an appliance .
14. In the CA Chain field, select a CA chain. In Releases 22.1 and later, you must select a CA chain.
15. Click OK.

---

## Export a CA Certificate to a File

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Objects & Connectors > Objects > Custom Objects > CA Certificate in the left menu bar.
5. Select the Appliance tab in the main pane.



6. Select a Certificate from the list in the main pane.
7. Click the  Export icon.
8. Click OK.

## Upload CRL Files

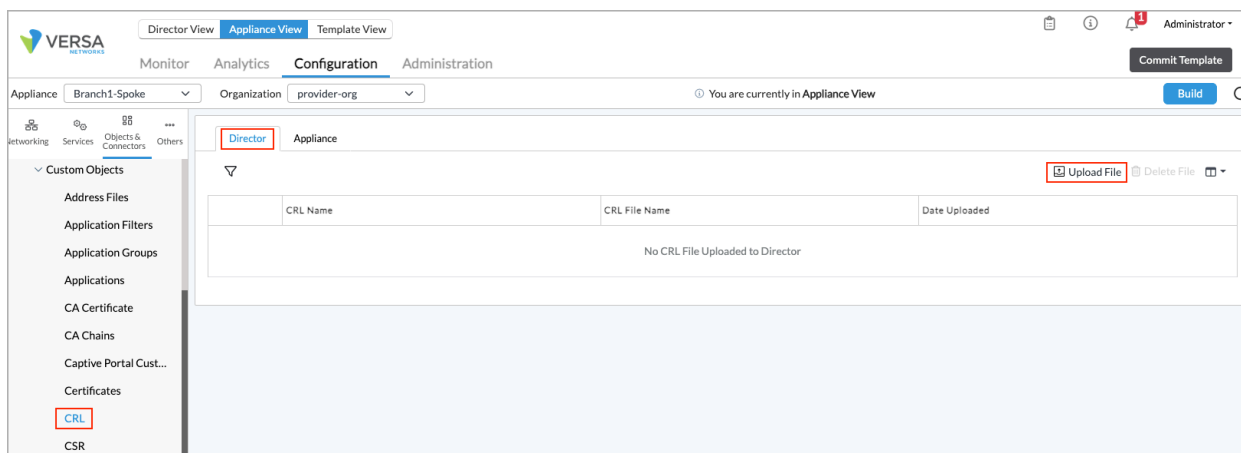
A certificate revocation list (CRL) is a cryptographically signed list of certificates that are revoked by a CA before their scheduled expiration date and should no longer be trusted. To validate the certificates in a CRL, you can upload a CRL file to a VOS device and enable CRL checking in an HTTP/HTTPS decryption profile. Enabling the CRL check ensures that a VOS device validates the server certificates received from SSL/TLS sessions against the CRL database.


You first upload the CRL file to the Director node, and then you upload it to the VOS device. To enable CRL checking in an HTTP/HTTPS decryption profile, see the section [Configure an SSL Decryption Profile](#), above.

To upload a CRL file to a Director node:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects> Custom Object> CRL in the left menu bar.





4. Select the Director tab in the horizontal menu bar.
5. Click the  Upload File icon, and in the Upload CRL to Director popup window, enter information for the following fields.

Upload CRL to Director

CRL Name \*

CRL File Name \*

Browse

Note - Allowed file format is .crl

OK

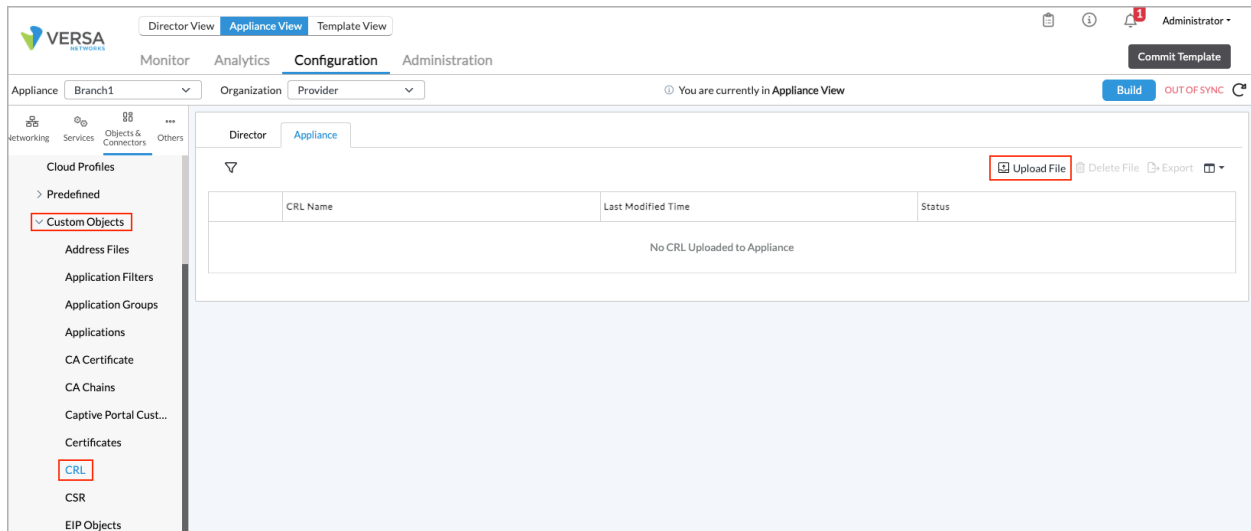
Cancel

Field	Description
CRL Name	Enter a name for the CRL.
CRL Filename	Click Browse to select the CRL file to upload to the Director node. The file must be in .crl format.

6. Click OK.

To upload a CRL file to a VOS device:

1. If you are continuing from the previous section, skip to Step 4. Otherwise, in Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > CRL in the left menu bar.
4. Select the Appliance tab in the horizontal menu bar.



5. Click the  Upload File icon, and in the Upload CRL to Appliance popup window, enter information for the following fields.

The popup window titled 'Upload CRL to Appliance' contains two dropdown menus. The 'Name' dropdown is set to '--Select--' and the 'Appliance' dropdown is set to 'Branch1-Spoke'. At the bottom, there are 'OK' and 'Cancel' buttons.

Field	Description
Name	Select the name of a CRL file.
Appliance	Select the name of the VOS device to which to upload the CRL file.

6. Click OK.

## Configure SSL Server Profiles

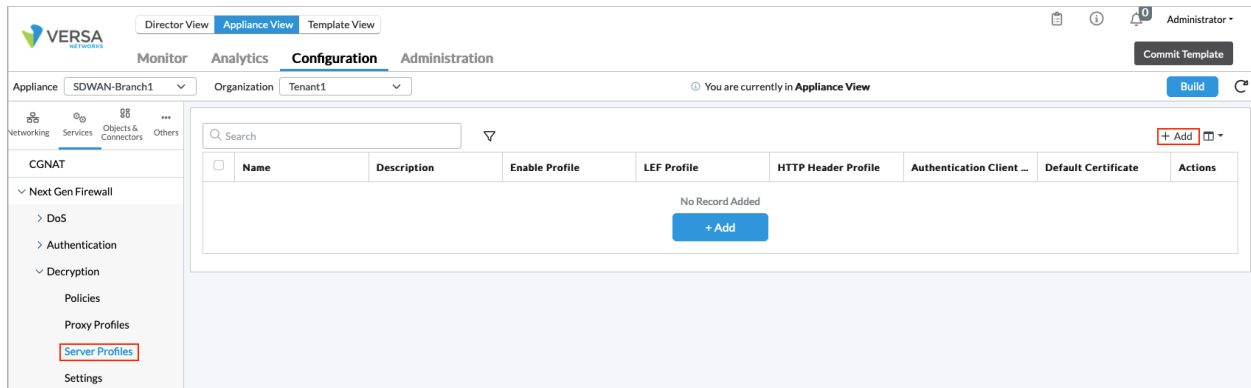
*For Releases 21.2.1 and later.*

You can configure SSL server profiles that are used for decryption by captive portal and Versa secure access. Server profiles are used to validate client certificates during certificate-based authentication. Server profiles are based on decryption profiles and use server certification instead of a CA certificate. Note that decryption policy evaluation is not performed for an SSL server profile.

In an SSL server profile, you can configure servers and import server certificates, and you can select a default server certificate. A default server certificate is used for authentication during the TLS handshake when the VOS device is establishing a connection if the first client message (the client Hello) does not contain a Server Name Indication (SNI). If you do not configure a default server certificate, and if the client Hello message does not contain an SNI, the session is closed. When an SNI is present in the initial client message, all the configured servers are evaluated in order, and the first match is used. A server matches when its hostname matches the domain pattern of the server. That server's server certificate is then used to establish connection.

To configure an SSL server profile:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Services > Next-Gen Firewall > Decryption > Server Profiles in the left menu bar.



5. Click the **+** Add icon. The Add Server Profile popup window displays.
6. Select the General tab, and then enter information for the following fields.

### Add Server Profile

General

SSL Protocol

HTTP Header Profile

Name \*

Description

☒ Enable Profile

☐ Support Session Ticket

Server

+ Add

Name

Actions

No Record Added

Match Rule \*

+ Add

Name

Actions

No Record Added

LEF Profile

LEF Log Level

---Please Select---

Alert

☐ Default Profile

SNAT Pool

---Please Select---

☐ SNAT Pool Default

**Client Authentication**

Trusted Certificate Database for Client Certificate  
---Please Select---

Default Server Certificate  
---Please Select---

CA Chain  
---Please Select---

**OCSP**

☐ Enabled ☐ Block Unknown Certificate


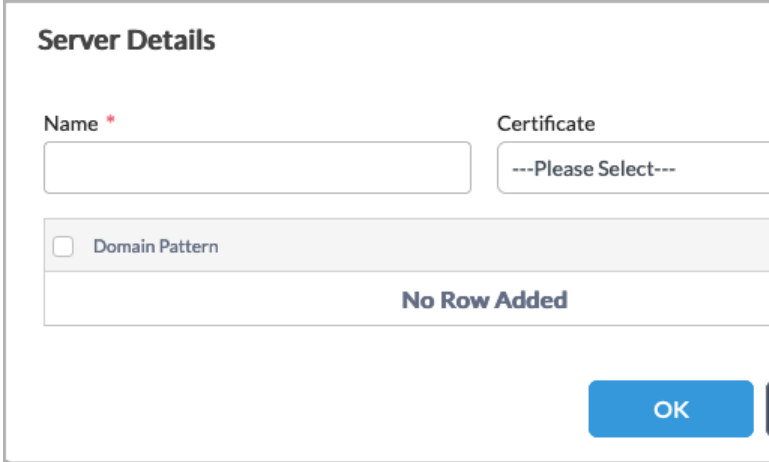


Response Timeout  
5

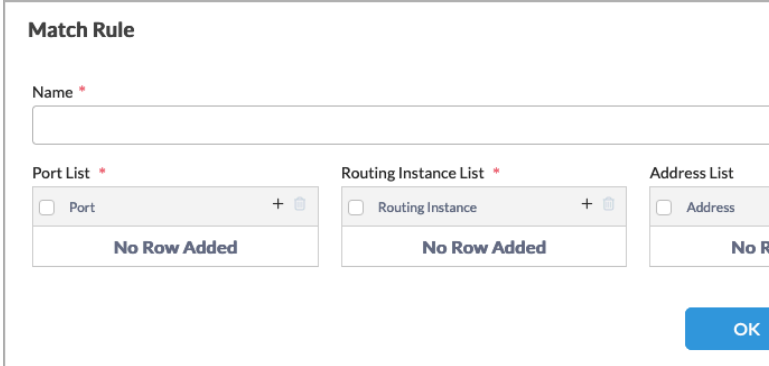



Verify  
---Please Select---

☐ Fetch issuer using AIA issuer

OK

Cancel

Field	Description
Name	Enter a name for the server profile.
Description	Enter a text description for the server profile.
Enable Profile	Click to enable the server profile.
Support Session Ticket	Click to enable a session that was created earlier.
Server (Group of Fields)	<p>Displays the names of the servers that are already configured. To add a server, click the  Add icon and in the Server Details popup window, enter information for the following fields.</p> 
◦ Name	Enter a name for the server.
◦ Certificate	Select a certificate to use to authenticate the server.
◦ Domain Pattern	Click the  Add icon to add a domain pattern for the server. When the hostname and domain pattern match, this server's server certificate is used for client connection.
Match Rule (Group of Fields)	<p>Displays the names of the match rules that are already configured. To add a rule, click the  Add icon and in the Match Rule popup window, enter information for the following fields.</p>

	
◦ Name	Enter a name for the match rule.
◦ Port List	Click the  Add icon to add a TCP port on which to listen for connections for the server profile.
◦ Routing Instance List	Click the  Add icon to add a routing instance for the server profile.
◦ Address List	Click the  Add icon to add an IP address on which to listen for connections for the server profile.
LEF Profile	Select a log export functionality (LEF) profile to use to capture logs for the server profile.
LEF Log Level	Select the log level to associate with the LEF profile
Default Profile	Click to use the default LEF profile instead of the LEF profile selected in the previous field. For more information, see <a href="#">Configure Log Export Functionality</a> .
SNAT Pool	Select the source NAT (SNAT) pool to use for OSCP requests. For more information, see <a href="#">Configure SNAT Pools</a> .
SNAT Pool Default	Click to make the selected SNAT pool the default pool.
Client Authentication (Group of Fields)	
◦ Trusted Certificate Database for Client Certification	Select a Trusted Certificate Database for Client Certification.

◦ Default Server Certificate	Select the default certificate to use when the client message does not contain an SNI.
◦ CA Chain	Select the certificate authority (CA) chain for the server certificate. For more information, see <a href="#">Configure CA Certificates, Key File, and CA Chains</a> .
OCSP (Group of Fields)	
◦ Enabled	Click to enable server certificate verification using the Online Certificate Status Protocol (OCSP).
◦ Block Unknown Certificate	Click to block SSL sessions whose certificate status is unknown.
◦ Response Timeout	Enter the timeout for an OCSP request.  <i>Default:</i> 5 seconds  <i>Value:</i> 0 through 255 seconds
◦ Verify	
Fetch Issuer Using AIA Issuers	(For Releases 22.1.2 and later.) Click to fetch intermediate certificates from the issuing certification authority. Authority Information Access (AIA) is an extension in SSL certificates that contains information about the issuer of the certificate. If a server does not provide intermediate certificates, you can download the certificates from the link contained in the AIA field.

7. Select the SSL Protocol tab, and enter information for the following fields. Note that if you do not select key exchange algorithms, encryption algorithms, and authentication algorithms, all algorithm are considered to be enabled for the selected cipher suites.



Add Server Profile

General

SSL Protocol

HTTP Header Profile

Min Version

TLS-1.1

Max Version

TLS-1.2

Key Exchange Algorithms

Encryption Algorithms

Authentication Algorithms

☐ RSA

☐ ECDHE

☐ AES-128-CBC

☐ AES-128-GCM

☐ AES-256-CBC

☐ AES-256-GCM

☐ Camellia-256-CBC

☐ ChaCha20-Poly1305

☐ Seed CBC

☐ SHA

☐ SHA256

☐ SHA384

Cipher Suites

Select Option

OK

Cancel

Field	Description
Minimum Version	<p>Select the minimum version of the Transport Layer Security (TLS) protocol that is supported. The minimum version must be the same as or earlier than the maximum version.</p> <ul style="list-style-type: none"> <li>◦ TLS 1.0</li> <li>◦ TLS 1.1</li> <li>◦ TLS 1.2</li> <li>◦ TLS 1.3</li> </ul>
Maximum Version	<p>Select the maximum version of the TLS protocol that is supported. The maximum version must be the same as or later than the minimum version. The options displayed depend on the version you select in the Minimum Version field. For example, if the minimum version is are TLS 1.0, the options TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 are displayed. If the minimum version is TLS 1.2, the options TLS 1.2 and TLS 1.3 are displayed.</p>
Key Exchange Algorithms	<p>When you select minimum and maximum TLS protocol versions and the version is not TLS 1.3, select one or more key exchange algorithms for the SSL connection:</p> <ul style="list-style-type: none"> <li>◦ ECDHE—Elliptic-Curve Diffie–Hellman Key Exchange</li> <li>◦ RSA—Rivest–Shamir–Adleman algorithm</li> </ul>
Encryption Algorithms	<p>Select an encryption algorithm to use:</p> <ul style="list-style-type: none"> <li>◦ AES-128-CBC—AES CBC encryption algorithm with 128-bit key</li> <li>◦ AES-128-GCM—AES GCM encryption algorithm with 128-bit key</li> <li>◦ AES-256-CBC—AES CBC encryption algorithm with 256-bit key</li> <li>◦ AES-256-GCM—AES GCM encryption algorithm with 256-bit key</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Camellia-256-CBC—Camellia encryption algorithm with 256-bit key</li> <li>◦ Chacha20-Poly1305—ChaCha stream cipher and Poly1305 authenticator</li> <li>◦ Seed CBC—TLS RSA with seed CBC</li> </ul>
Authentication Algorithms	Click to have the selected LEF profile be the default LEF profile.
Cipher Suites	<p>Select a TLS cipher suite. If you select a cipher suite, it must be consistent with the selected key exchange, encryption, and authentication algorithms. If you do not configure cipher suites, all cipher suites matching the selected the key exchange, encryption, and authentication algorithms are selected by default.</p> <ul style="list-style-type: none"> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</li> <li>◦ TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</li> <li>◦ TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</li> <li>◦ TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</li> <li>◦ TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</li> <li>◦ TLS-RSA-WITH-AES-128-CBC-SHA</li> <li>◦ TLS-RSA-WITH-AES-128-CBC-SHA256</li> <li>◦ TLS-RSA-WITH-AES-128-GCM-SHA256</li> <li>◦ TLS-RSA-WITH-AES-256-CBC-SHA</li> <li>◦ TLS-RSA-WITH-AES-256-CBC-SHA256</li> </ul>

	<ul style="list-style-type: none"> <li>◦ TLS-RSA-WITH-AES-256-GCM-SHA384</li> <li>◦ TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</li> <li>◦ TLS-RSA-WITH-SEED-CBC-SHA</li> </ul>
--	---

8. Select the HTTP Header Profile tab.

The screenshot shows the 'Add Server Profile' dialog box. The 'General' tab is selected, and the 'HTTP Header Profile' sub-tab is highlighted with a red box. Below the sub-tab, there is a dropdown menu labeled 'HTTP Header Profile' with the text '---Please Select---'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Note that in Releases 22.1.1 and earlier, the Add Server Profile screen did not contain the HTTP Header Profile tab.

The screenshot shows the 'Add Server Profile' dialog box with the 'General' tab selected. The dialog contains several fields and sections:
 

- Name** and **Description** text input fields.
- LEF Profile** dropdown menu with '---Please Select---' and checkboxes for **Default** and **Support Session Ticket**.
- Authentication Certificate**, **Default Server Certificate**, and **CA Chain** dropdown menus, all with '---Please Select---'.
- OCSP** section with a checkbox for **Enabled**, a checkbox for **Block Unknown Certificate**, a **Response Timeout** input field with the value '5', and a **Source NAT Pool** dropdown menu with '---Please Select---'.
- Server** and **Match Rule** sections, each containing a table with a 'Name' header and a 'No Record Added' message. Both sections have pagination controls showing '1 of 1' and a '25' dropdown.
- OK** and **Cancel** buttons at the bottom right.

9. Click in the HTTP Header Profile field, then select an HTTP header profile or click + Add New to create a new

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)

Updated: Wed, 23 Oct 2024 08:18:18 GMT

Copyright © 2024, Versa Networks, Inc.

HTTP header profile. If you click + Add New, the Add HTTP Header Profile screen displays. For more information, see [Configure HTTP Header Profiles](#).

10. Click OK to add the SSL server profile.

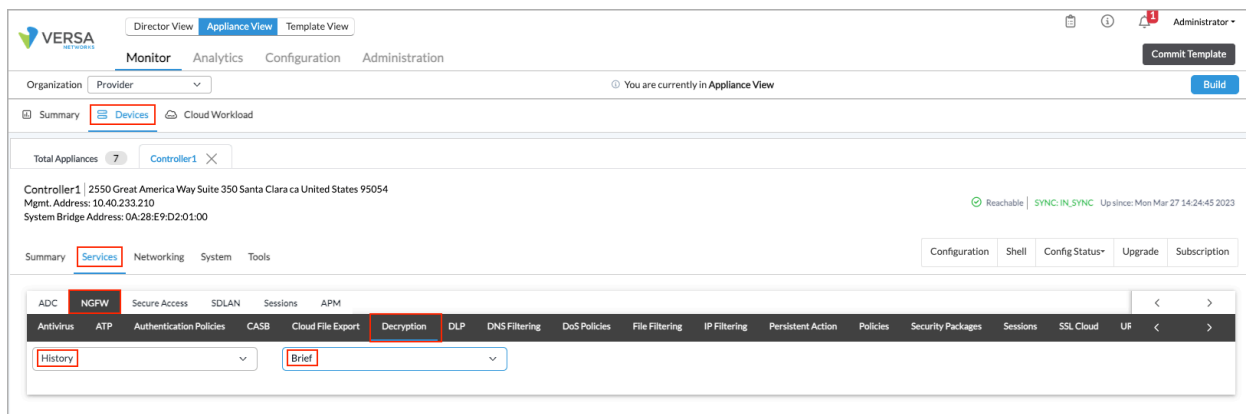
---

## View SSL Decryption History

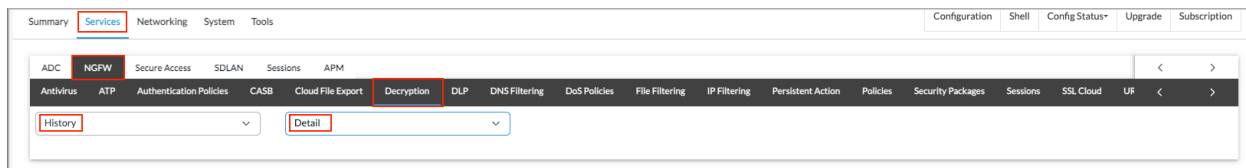
You can view brief and detailed history of SSL decryption profiles from the Monitoring tab.

To view information about SSL decryption profiles sessions:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a provider organization in the top submenu bar.
4. Select the Services tab, and then select NGFW > Decryption > History.
5. To display a brief history of SSL sessions, select Brief.



6. To display a detailed history of SSL sessions, select Detail.



To view SSL session history from the CLI, use the following commands:

- **show orgs org-services *tenant-name* security profiles decrypt history brief**

```
admin@versa-cli> show orgs org-services versa security profiles decrypt history brief
SRC          DST PROXY          DECRYPT
```

TIMESTAMP	SRC IP	PORT	DST IP	PORT	TYPE	RULE	PROFILE	ACTION
STARTTLS	HOSTNAME							
2020-12-17 11:59:07	192.168.10.23	42972	151.101.65.67	443	FORWARD	rule1	dp1	decrypt
false	edition.cnn.com							
2020-12-17 11:58:56	192.168.10.23	38983	157.240.2.35	443	FORWARD	rule1	dp1	decrypt
false	facebook.com							
2020-12-17 11:58:56	192.168.10.23	38983	157.240.2.35	443	FORWARD	rule1	dp1	decrypt
false	facebook.com							
2020-12-17 11:58:36	192.168.10.23	55336	172.217.164.110	443	FORWARD	rule1	dp1	decrypt
false	google.com							
2020-12-17 11:58:36	192.168.10.23	55336	172.217.164.110	443	FORWARD	rule1	dp1	decrypt
false	google.com							
2020-12-17 11:59:03	192.168.10.23	33837	151.101.1.67	443	FORWARD	rule1	dp1	decrypt
false	www.cnn.com							
2020-12-17 11:59:03	192.168.10.23	33837	151.101.1.67	443	FORWARD	rule1	dp1	decrypt
false	www.cnn.com							

• **show orgs org-services *tenant-name* security profiles decrypt history detail**

```

admin@versa-cli> show orgs org-services versa security profiles decrypt history detail
security profiles decrypt history detail "2020-12-17 11:59:07"
src-ip          192.168.10.23
src-port        42972
dst-ip          151.101.65.67
dst-port        443
proxy-type      FORWARD
rule            rule1
profile         dp1
decrypt-action   decrypt
starttls        false
hostname        edition.cnn.com
decrypt-bypass   false
action          NA
action-reason    NA
splice-state     Handshake
pub-key-len      2048
starttls-capability false
inward-tls-version TLSv1.2
inward-tls-cipher TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
inward-tls-state  "Handshake complete"
inward-last-tls-op Decrypt
inward-last-tls-op-status "Close notify"
inward-last-tls-op-error CLOSE_NOTIFY
outward-tls-version TLSv1.2
outward-tls-cipher TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
outward-tls-state  "Handshake complete"
outward-last-tls-op Decrypt
outward-last-tls-op-status Success
outward-last-tls-op-error UNUSED
security profiles decrypt history detail "2020-12-17 11:58:56"
src-ip          192.168.10.23
src-port        38983
dst-ip          157.240.2.35

```

```

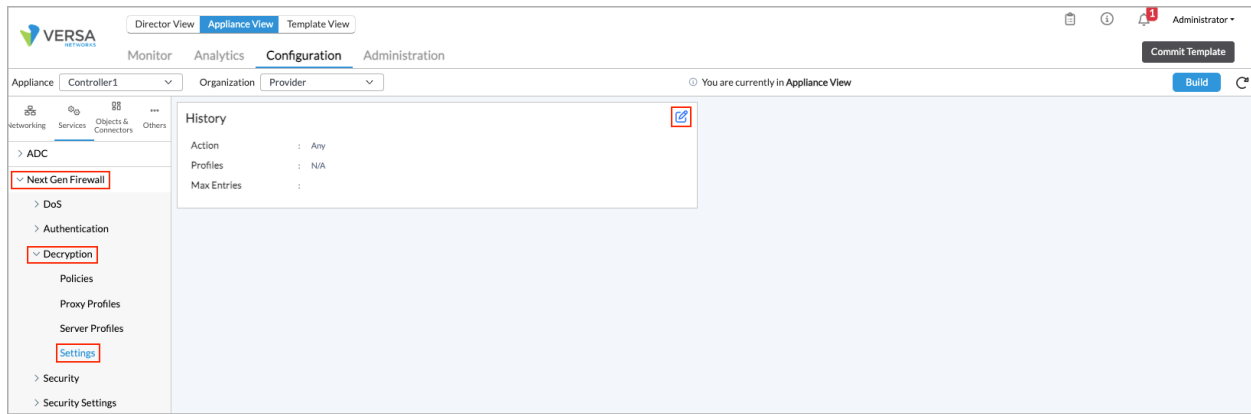
dst-port          443
proxy-type        FORWARD
rule              rule1
profile           dp1
decrypt-action    decrypt
starttls          false
hostname          facebook.com
decrypt-bypass    false
action            NA
action-reason     NA
splice-state      Handshake
pub-key-len       576
starttls-capability false
inward-tls-version TLSv1.2
inward-tls-cipher  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
inward-tls-state   "Handshake complete"
inward-last-tls-op Decrypt
inward-last-tls-op-status "Close notify"
inward-last-tls-op-error CLOSE_NOTIFY
outward-tls-version TLSv1.2
outward-tls-cipher  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
outward-tls-state   "Handshake complete"
outward-last-tls-op Decrypt
outward-last-tls-op-status Success
outward-last-tls-op-error UNUSED


```

To display the history of specific SSL decryption profiles in the Monitor tab, you configure history settings to select the desired profiles. You can display sessions that are either decrypted or not decrypted, and you can set the maximum number of entries to display.

To select the SSL decryption profiles sessions for which to display history:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Decryption > Settings in the left menu bar. The main pane displays the History pane.



4. Click the  Edit icon. In the Edit History popup window, enter information for the following fields.

The 'Edit History' popup window is displayed. It has a title bar with a close button (X). The window contains three form fields: 'Action' with a dropdown menu showing 'Any', 'Profiles' with a dropdown menu showing 'Select Option', and 'Max Entries' with a text input field containing '64'. At the bottom of the window are two buttons: 'OK' (blue) and 'Cancel' (dark grey).



Field	Description
Action	<p>Select the type of SSL session for which to display history:</p> <ul style="list-style-type: none"> <li>Decrypt—Display only sessions that are decrypted.</li> <li>No Decrypt—Display only sessions that are not decrypted.</li> </ul>
Profiles	Select the SSL decryption profiles for which to display session history.
Maximum Entries	<p>Enter the maximum number of entries to display in the session history in the Monitor tab.</p> <p><i>Value:</i> 1 through 128 <i>Default:</i> 64</p>

5. Click OK.

---

## Configure Secure Web Proxy

You can configure a VOS device to be an HTTP/HTTPS proxy, and you can define whether the proxy acts for some or all the HTTP or HTTPS requests that it receives.

You can configure the following types of HTTP/HTTPS proxy:

- Explicit proxy—Process SSL/TLS traffic destined to a specific IP address and a port.
- Web proxy—Type of explicit proxy that acts as an intermediary between the user and websites that they are visiting so that the websites see the IP address of the proxy, not the IP address of the user.
- Transparent proxy—Process the SSL/TLS traffic destined to any IP address but to a specific port.


---

## Configure an Explicit Proxy

An explicit proxy processes SSL/TLS traffic destined to a specific IP address and a specific port. To configure an explicit proxy, you configure the proxy IP address and port information on the client (browser), and then you configure explicit mode when you create an SSL decryption profile on the VOS device.

To configure an explicit HTTP/HTTPS proxy on a VOS device:

1. In Director view:

- a. Select the Administration tab in the top menu bar.
- b. Select Appliances in the left menu bar.
- c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Decryption > Proxy Profiles in the left menu bar.
4. Click the  Add icon in the main pane. The Add Decryption Profile popup window displays.

### Add Decryption Profile ✕

General

SSL Inspection

SSL Protocol

Advanced

Name \*

Description

Tags

☒ Enable Profile

☐ Support Session Ticket

☒ Use Extended Master Secret

Type \*

SSL Full Proxy

Trusted Certificate Database \*

default

CA Certificate \*

--Select--

LEF Profile

--Select--

☐ Default Profile





LEF Log Level

Alert


Mode

☐ Transparent
☒ Explicit

Match Rule

1




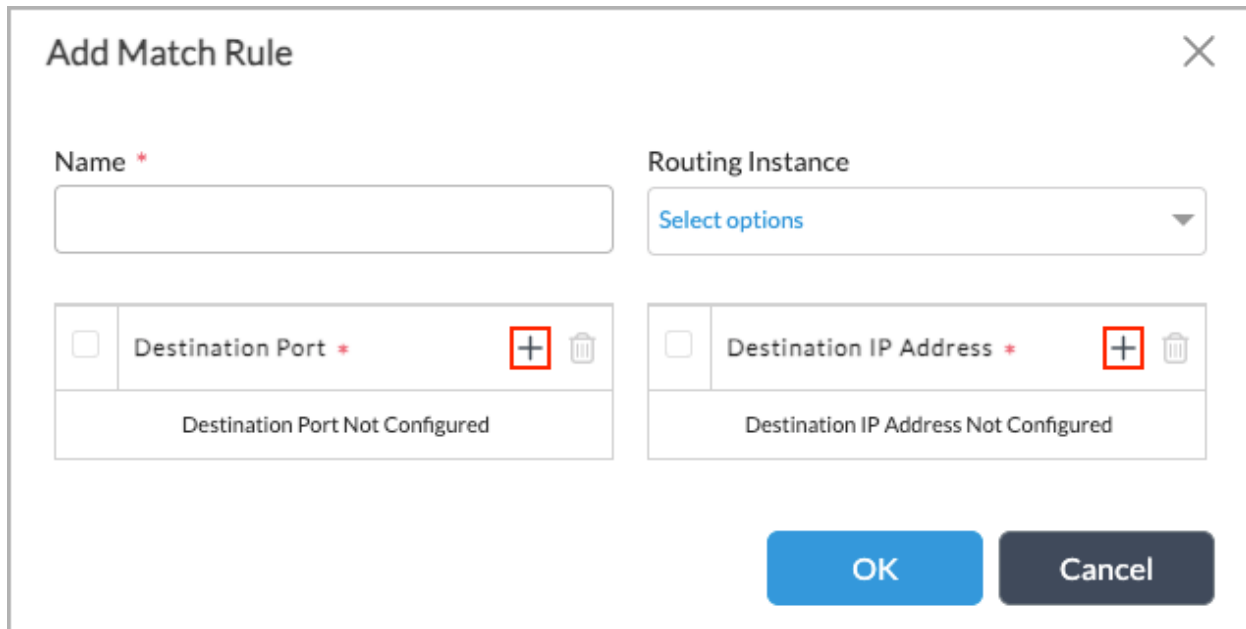
25

<input type="checkbox"/>	Name
No Match Added	

OK

Cancel



5. In the Type field, select SSL Full Proxy.
6. Under Mode, click Explicit.
7. In the Match Rule table, click the  Add icon. The Add Match Rule popup window displays.



The 'Add Match Rule' popup window contains the following elements:

- Title Bar:** 'Add Match Rule' with a close button (X) in the top right corner.
- Name:** A text input field with a red asterisk (\*) indicating it is required.
- Routing Instance:** A dropdown menu with 'Select options' and a downward arrow.
- Match Rule Table:** A table with two columns: 'Destination Port' and 'Destination IP Address'. Both columns have a red asterisk (\*) and a red box containing a plus sign (+) for adding new rules. Each row also has a trash icon for deleting the rule.
 

Destination Port	Destination IP Address
Destination Port Not Configured	Destination IP Address Not Configured
- Buttons:** 'OK' (blue) and 'Cancel' (dark grey) buttons at the bottom right.

8. In the Destination Port table, click the  Add icon, and then enter the port number to decrypt traffic originating from that port. The most common port number used for an explicit HTTP/HTTPS proxy is 3128.
9. In the Destination IP Address table, click the  Add icon, and then enter an IP address to decrypt traffic originating from that address.
10. Configure other decryption profile parameters. For more information, see [Configure an SSL Decryption Profile](#), above.
11. Click OK.

## Configure a Web Proxy

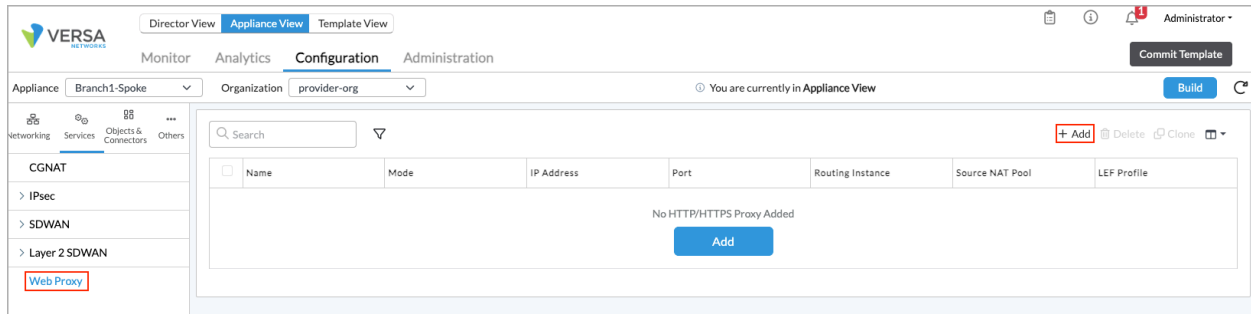
*For Releases 20.2 and later.*

You can configure a VOS device to be a web proxy, which is a type of explicit proxy. A web proxy acts as an intermediary between the user and websites that they are visiting so that the websites see and log the IP address of the proxy, not the IP address of the user. In this way, the web proxy allows the user to remain anonymous. A web proxy can also speed up browsing by caching webpage data.

To configure a web proxy:

1. In Director view:

- a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
  3. Select an organization in the horizontal menu bar.
  4. Select Services > Web Proxy in the left menu bar.



5. Click the **+** Add icon in the main pane. The Add HTTP/HTTPS Proxy popup window displays
6. Select the General tab, and then enter information for the following fields.

Add HTTP/HTTPS Proxy

General
Cookie Based User Identification
Rules

Name \*

Description

Mode \*

Explicit

IP Address \*

Port \*
+

Port Not Configured

Routing Instance

Select options

Provider Organization

--Select--

DNS Redirection Policy

--Select--

+ DNS Redirection Policy

Source NAT Pool

--Select--

+ SNAT Pool

☐ SNAT Pool Default

LEF Profile

--Select--

☒ Default Profile

Honour PBF


☐ Yes
☒ No

Parse Response

☐ Yes
☒ No

OK
Cancel

Field	Description
Name	Enter a name for the HTTP/HTTPS proxy.
Description	Enter a text description for the HTTP/HTTPS proxy.
Mode	Select Explicit. For more information about proxy modes, see <a href="#">Configure an SSL Decryption Profile</a> , above.

Field	Description
IP Address	Enter the IP address of the HTTP/HTTPS proxy.
Port	Click the  Add icon, and then enter the port number to use to connect to the proxy. The most common port number for an explicit HTTP/HTTPS proxy is 3128.
Routing Instance	Select the routing instance for the proxy to use to route traffic.
Source NAT Pool	Select the NAT pool for the explicit HTTP/HTTPS proxy to use.
LEF Profile	Select a LEF profile to use to record the SSL logs for the explicit HTTP/HTTPS proxy.
Default Profile	Click to use the default LEF profile instead of the LEF profile selected in the previous field. For more information, see <a href="#">Configure Log Export Functionality</a> .
Provider Organization	Select the organization to which the explicit HTTP/HTTPS proxy belongs.
DNS Redirection Policy	<p>Select a DNS redirection policy to use for DNS lookup of either the local breakout domain or FQDN of the proxy chain. For more information, see <a href="#">Configure DNS Proxy Profiles</a>.</p> <p>Note that if the next-generation firewall (NGFW) service is enabled, the redirection access policy must contain one rule with a source zone match condition that matches the host and with the action to allow self-generated DNS traffic. More information, see <a href="#">Configuration Example: Access Policy Rule To Allow DNS Traffic for NGFW</a>, in <a href="#">Configure File Filtering</a>.</p>
Honor PBF	Select whether to honor policy-based forwarding. If you click Yes, when you apply policy-based forwarding in a redirection rule in a DNS profile, proxy forwarding can also check SD-WAN policies to select the path for the DNS query and the onward connection to the application server. For more information, see <a href="#">Configure DNS Redirection Rules</a> .
Parse Response	Select whether to enable or disable HTTP/HTTPS parsing of the response. If you enable parsing of the

Field	Description
	response, the parsing responses are available as a counter in the secure web proxy VFP profile statistics.

7. Select the Cookie-Based User Identification tab, and then enter information for the following fields.

Add HTTP/HTTPS Proxy

General
Cookie Based User Identification
Rules

☒ Enabled

Authentication URL \*

Domain Cookie Name
Domain Cookie Validity

VERSA\_DCTX
86400

Validation Cookie Name
Validation Cookie Validity

VERSA\_DDCTX
60

☐ Block Session with No-Cookie
☐ Allow Cross Origin Requests

Whitelist

☐ Patterns
+

Patterns Not Configured

☐ URL Category List
+ New URL Category +

URL Category List Not Configured



OK
Cancel

Field	Description
Enabled	Click to enable cookie-based identification, which collects user information from cookies.
Authentication URL	Enter the URL of the central authentication server. Users are redirected to this server for authentication.
Domain Cookie Name	Enter the name of the cookie to use for storing user

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)

Updated: Wed, 23 Oct 2024 08:18:18 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	information for each domain.
Domain Cookie Validity	Enter how long the domain cookie is valid, in seconds. <i>Default:</i> 86400 seconds (24 hours)
Validation Cookie Name	Enter the name of the short-lived validation cookie to use to check the cookie status (whether it is enabled or disabled) on the user agent.
Validation Cookie Validity	Enter how long the validation cookie is valid, in seconds. <i>Default:</i> 60 seconds
Block Session with No Cookie	Click to block all sessions that do not have a cookie. If you do not click this field, all the sessions whose cookie is not set are allowed even without user identification.
Allow Cross-Origin Requests	Click to allow cross-origin requests. This option allows a user to request restricted resources on a webpage from a domain that is outside the domain that serves the resource.
Whitelist (Group of Fields)	Configure allow list information.
<ul style="list-style-type: none"> <li>Pattern</li> </ul>	Click the  Add icon to add domains that the user is allowed to access without user identification. Enter the pattern to use to match domain name; for example, <code>*+, *.google*</code> .
<ul style="list-style-type: none"> <li>URL Category</li> </ul>	Click the  Add icon to add a specific URL category to the allow list.

8. Select the Rules tab to configure proxy rules.



**Add HTTP/HTTPS Proxy** ✕

General Cookie Based User Identification **Rules**

+
🗑️
↕️
↑
↓
⌵
📅
🔍
<
1
>
25
▼

<input type="checkbox"/>	Name	Rule Mode	Rule Status
No Rules Added			

OK
Cancel

9. Click the  Add icon. The Add Rules popup window displays.

**Add Rules** ✕

**General** Match Enforce

Name \*

Monitor

--Select-- ▼

Rule Status

☐ Enabled
 ☒ Disabled

OK
Cancel

10. Select the General tab, and then enter information for the following fields.

Field	Description
Name	Enter a name for the rule.
Monitor	Select the monitor object for an IP address to associate with the rule. For more information, see <a href="#">Configure IP SLA Monitor Objects</a> .
Rule Status	Select the rule status: <ul style="list-style-type: none"> <li>◦ Disabled</li> <li>◦ Enabled</li> </ul>

11. Select the Match tab, and then enter information for the following fields.

Add Rules

General

Match

Enforce

Domain Pattern

Applications/URL

Domain Pattern

☐ Domain Pattern


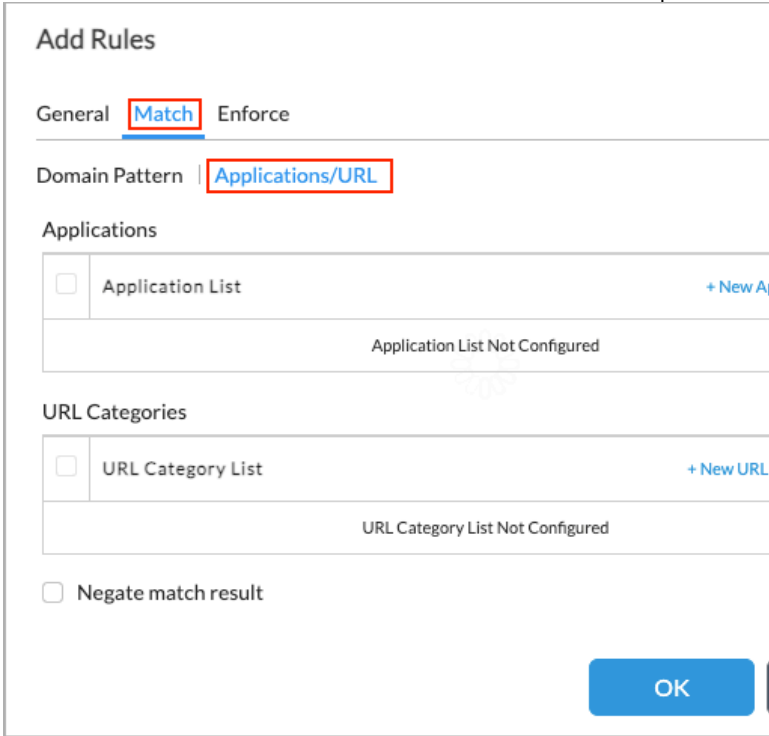


+

Domain Pattern Not Configured

☐ Negate match result

OK

Cancel

Field	Description
Domain Pattern (Tab)	
<ul style="list-style-type: none"> <li>Domain Pattern</li> </ul>	<p>Click the  Add icon to specify a pattern to use to match the domain name; for example, *.example.com. Requests are forwarded to the next proxy address and proxy port through the proxy routing instance only when the domain name of the proxy request matches the domain pattern.</p> <p>If you do not specify a pattern, proxy chaining is applied to all sessions.</p>
Negate Match Result	Select to negate the final match results. Any rule that matches the criteria is considered as a no-match.
Applications/URL (Tab)	
<ul style="list-style-type: none"> <li>Applications</li> </ul>	Click the  Add icon to select a predefined or a custom application.
<ul style="list-style-type: none"> <li>URL Categories</li> </ul>	Click the  Add icon to select a predefined or a custom URL category.

12. Select the Enforce tab, and then enter information for the following fields.

Add Rules

General

Match

Enforce

Rule Mode

☒ Proxy Chaining ☐ Local Breakout

Skip Local Breakout on DNS Failure

☒ Enabled ☐ Disabled

Proxy IP Address

Proxy Port \*

Honour PBF

☒ Enabled ☐ Disabled

FQDN

SNAT Pool

--Select--

+ SNAT Pool

OK

Cancel


Field	Description
Rule Mode (Group of Fields)	Click to select the proxy rule mode: <ul style="list-style-type: none"> <li>Local Breakout</li> <li>Proxy Chaining</li> </ul>
Proxy Chaining (Group of Fields)	Click to configure the proxy forwarding and match criteria and forward selected sessions to an external proxy. The VOS device acts as an intermediate proxy, and it supports virtual wire mode.
<ul style="list-style-type: none"> <li>Proxy IP Address</li> </ul>	Enter the address of the next proxy to which to send the forwarding request.
<ul style="list-style-type: none"> <li>Proxy Port</li> </ul>	Enter the port on the next proxy to which to send the forwarding request.
<ul style="list-style-type: none"> <li>SNAT Pool</li> </ul>	Select the SNAT pool for the explicit HTTP/HTTPS proxy to use.
<ul style="list-style-type: none"> <li>Honor PBF</li> </ul>	Click Enabled to honor policy-based forwarding. When honor policy-based forwarding is enabled, and when you apply policy-based forwarding in a redirection rule in a DNS profile, proxy forwarding can also check SD-WAN policies to select the path for the DNS query and the onward connection to the application server. For more information, see <a href="#">Configure DNS Redirection Rules</a> .
Local Breakout	Click to route internet traffic from the site directly to the internet.
<ul style="list-style-type: none"> <li>Skip Local Breakout on DNS Failure</li> </ul>	Click Enabled to not perform local breakout of traffic when DNS fails and instead route traffic to the proxy server.
<ul style="list-style-type: none"> <li>SNAT Pool</li> </ul>	Select the SNAT pool for the explicit HTTP/HTTPS proxy to use.
<ul style="list-style-type: none"> <li>Negate Match</li> </ul>	Select to negate the match results.

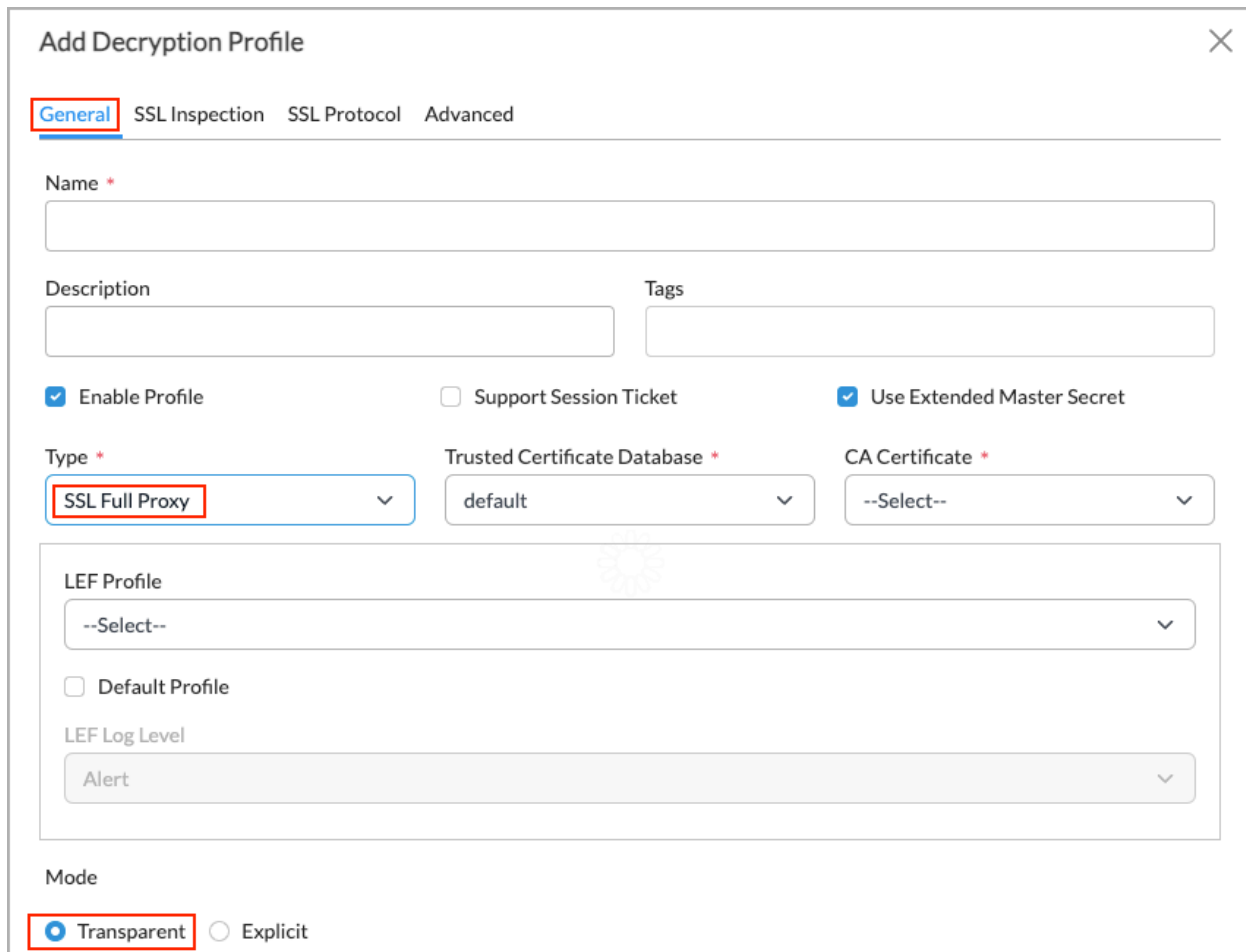
13. Click OK.

## Configure a Transparent Proxy

A transparent proxy processes SSL/TLS traffic that is destined to any IP address but to a particular port. The client (browser) performs DNS resolution and opens the connection to the server's IP address. To configure a transparent proxy, you configure explicit mode when you create an SSL decryption profile on a VOS device.

To configure a transparent explicit HTTP/HTTPS proxy:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Decryption > Profiles in the left menu bar.
4. Click the  Add icon in the main pane. Select the General tab in the Add Decryption Profile popup window.



The image shows the 'Add Decryption Profile' popup window. The 'General' tab is selected and highlighted with a red box. The 'Name' field is empty. The 'Description' and 'Tags' fields are also empty. The 'Enable Profile' checkbox is checked, 'Support Session Ticket' is unchecked, and 'Use Extended Master Secret' is checked. The 'Type' dropdown is set to 'SSL Full Proxy' and is highlighted with a red box. The 'Trusted Certificate Database' is set to 'default' and the 'CA Certificate' is set to '--Select--'. Below these, the 'LEF Profile' dropdown is set to '--Select--'. The 'Default Profile' checkbox is unchecked. The 'LEF Log Level' dropdown is set to 'Alert'. At the bottom, the 'Mode' section has 'Transparent' selected (highlighted with a red box) and 'Explicit' is unselected.

Match Rule

Toolbar: + (highlighted), trash, filter, left arrow, 1, right arrow, 25, dropdown arrow

<input type="checkbox"/>	Name
No Match Added	

Buttons: OK, Cancel

5. In the Type field, select SSL Full Proxy.
6. Under Mode, click Transparent.
7. In the Match Rule table, click the **+** Add icon. The Add Match Rule popup window displays.

Add Match Rule

Name \*

Routing Instance: Select options

<input type="checkbox"/>	Destination Port *	+ (highlighted)	trash
Destination Port Not Configured			
<input type="checkbox"/>	Destination IP Address *	+ (highlighted)	trash
Destination IP Address Not Configured			

Buttons: OK, Cancel

8. In the Destination Port table, click the **+** Add icon, and then enter the port number to use for the HTTP proxy. Common port numbers are 80 for an HTTP proxy and 443 for an HTTPS proxy.
9. In the Destination IP Prefix table, click the **+** Add icon, and then enter the IP address prefix to decrypt traffic originating from that address.
10. Configure other decryption profile parameters, as desired. For more information, see [Configure an SSL Decryption Profile](#), above.
11. Click OK.

To associate the decryption profile with a decryption rule:

1. Select the Configuration tab in the top menu bar of the Proxy Profiles dashboard screen.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)

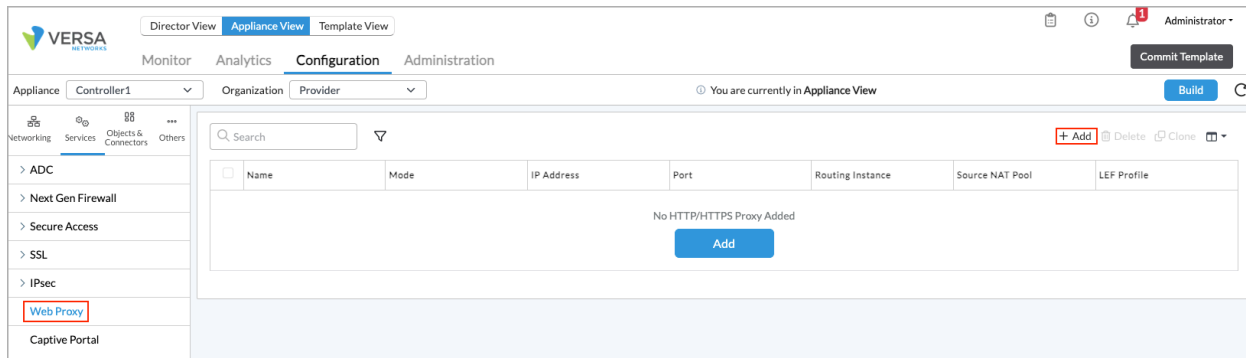
Updated: Wed, 23 Oct 2024 08:18:18 GMT

Copyright © 2024, Versa Networks, Inc.

2. Select Services > Next-Gen Firewall > Decryption > Policies in the left menu bar, and then select the Rules tab to associate the decryption profile with a decryption rule. For more information, see [Step 13](#) in [Configure an SSL Decryption Policy Rule](#), above.

To configure a transparent proxy for the web proxy service:

1. Select the Configuration tab in the top menu bar.
2. Select an organization in the horizontal menu bar.
3. Select Services > Web Proxy in the left menu bar.



4. Click the **+** Add icon in the main pane. The Add HTTP/HTTPS Proxy popup window displays.
5. Select the General tab, and then enter information for the following fields.



Add HTTP/HTTPS Proxy

General

Cookie Based User Identification

Rules

Name \*

0/127

Description

Mode \*

Transparent

IP Prefix

Port \*

+

Port Not Configured

Routing Instance

Select options

Provider Organization

--Select--

DNS Redirection Policy

--Select--

+ DNS Redirection Policy

Source NAT Pool

--Select--

+ SNAT Pool

☐ SNAT Pool Default

LEF Profile

--Select--

☒ Default Profile

Honour PBF

☐ Yes

☒ No

Parse Response

☐ Yes

☒ No


Parse Request

☐ Yes

☒ No

OK

Cancel

Field	Description
Name	Enter a name for the HTTP/HTTPS proxy.
Description	Enter a text description for the HTTP/HTTPS proxy.
Mode	Select Transparent. For more information, see <a href="#">Configure an SSL Decryption Profile</a> , above.
IP Prefix	Enter the IP address of the HTTP/HTTPS proxy.
Port	Click the  Add icon, and then enter the port number to use to connect to the proxy. The most common port number for an explicit HTTP/HTTPS proxy is 3128.
Routing Instance	Select the routing instance for the proxy to use to route traffic.
Provider Organization	Select the organization to which the transparent HTTP/HTTPS proxy belongs.
DNS Redirection Policy	Select a DNS redirection policy to use for DNS lookup of either the local breakout domain or FQDN of the proxy chain. For more information, see <a href="#">Configure DNS Proxy Profiles</a> .
Source NAT Pool	Select the NAT pool for the transparent HTTP/HTTPS proxy to use.
SNAT Pool Default	Click to use the default SNAT pool instead of the SNAT pool selected in the previous field.
LEF Profile	Select a LEF profile to use to record the SSL logs for the transparent HTTP/HTTPS proxy.
Default Profile	Click to use the default LEF profile instead of the LEF profile selected in the previous field. For more information, see <a href="#">Configure Log Export Functionality</a> .
Honor PBF	Select whether to honor policy-based forwarding. If you click Yes, when you apply policy-based forwarding in a redirection rule in a DNS profile, proxy forwarding can also check SD-WAN policies to select the path for the DNS query and the onward connection to the application server. For more information, see <a href="#">Configure DNS Redirection Rules</a> .
Parse Response	Select whether to enable or disable HTTP/HTTPS


	parsing of the response. If you enable parsing of the response, the parsing responses are available as a counter in the secure web proxy VFP profile statistics.
Parser Request	Select whether to enable or disable HTTP/HTTPS parsing of the request.

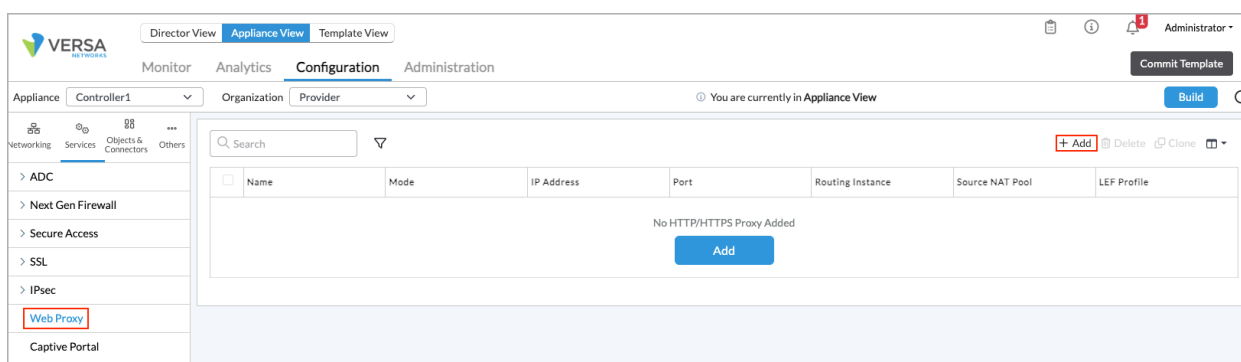
6. Click OK.
7. Configure your browser, setting the HTTP/HTTPS proxy port to the port configured in the decryption profile.

## Configure an Application Proxy

An application proxy serves as an intermediary between an application request from a client and the destination application server to obtain a requested service. When an application makes a request, the application proxy intercepts the request to the destination server and initiates its own request to the server. When the destination server responds to the request, the application proxy responds back to the client as if it were the destination server.

To configure an application proxy:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Services > Web Proxy in the left menu bar.
5. Click the  Add icon in the main pane.



6. In the Add HTTP/HTTPS Proxy popup window, select the General tab, and then enter information for the following fields.

Add HTTP/HTTPS Proxy

General
Cookie Based User Identification
Rules

Name \*

name

Description

Mode \*

App Proxy

IP Address \*

☐
Port \*

+

Port Not Configured

Routing Instance

Select options

Provider Organization

--Select--

DNS Redirection Policy

--Select--

+ DNS Redirection Policy

App Domain

Service Provider App Domain

Source NAT Pool

--Select--

+ SNAT Pool

☐
SNAT Pool Default

LEF Profile

--Select--

☒
Default Profile

Honour PBF

☐ Yes
☒ No

Parse Response

☐ Yes
☒ No

☐
Proxy App Certificates

+

Proxy App Certificates Not Configured

☐
Proxy Apps


+



Proxy Apps Not Configured

OK

Cancel

Field	Description
Name	Enter a name for the HTTP/HTTPS proxy.

Field	Description
Description	Enter a text description for the HTTP/HTTPS proxy.
Mode	Select App Proxy. For more information, see <a href="#">Configure an SSL Decryption Profile</a> , above.
IP Address	Enter the IP address of the HTTP/HTTPS application proxy.
Port	Click the  Add icon, and then enter the port number to use to connect to the proxy. The most common port number for an explicit HTTP/HTTPS proxy is 3128.
Routing Instance	Select the routing instance for the proxy to use to route traffic.
Provider Organization	Select the organization to which the explicit HTTP/HTTPS proxy belongs.
DNS Redirection Policy	<p>Select a DNS redirection policy to use for DNS lookup of either the local breakout domain or FQDN of the proxy chain. For more information, see <a href="#">Configure DNS Proxy Profiles</a>.</p> <p>Note that if the next-generation firewall (NGFW) service is enabled, the redirection access policy must contain one rule with a source zone match condition that matches the host and with the action to allow self-generated DNS traffic. More more information, see <a href="#">Configuration Example: Access Policy Rule To Allow DNS Traffic for NGFW</a>, in <a href="#">Configure File Filtering</a>.</p>
Application Domain	Enter the domain name of the application proxy. The application domain name is prepended to the replaced URLs in the response.
Service Provider Application Domain	Enter the service provider application domain name for the application proxy.
Source NAT Pool	Select the NAT pool for the explicit HTTP/HTTPS proxy to use.
LEF Profile	Select a LEF profile to use to record the SSL logs for the explicit HTTP/HTTPS proxy.

Field	Description
Default Profile	Click to use the default LEF profile instead of the LEF profile selected in the previous field. For more information, see <a href="#">Configure Log Export Functionality</a> .
Honor PBF	Select whether to honor policy-based forwarding. If you click Yes, when you apply policy-based forwarding in a redirection rule in a DNS profile, proxy forwarding can also check SD-WAN policies to select the path for the DNS query and the onward connection to the application server. For more information, see <a href="#">Configure DNS Redirection Rules</a> .
Parse Response	Select whether to enable or disable HTTP/HTTPS parsing of the response. If you enable parsing of the response, the parsing responses are available as a counter in the secure web proxy VFP profile statistics.
Proxy App Certificates	(For Releases 22.1.2 and later.) If you select application proxy mode, click the  Add icon, and then select a proxy application server certificate. The server certificates are used to create the implicit SSL server for application proxy.
Proxy Apps	(For Releases 22.1.2 and later.) If you select application proxy mode, click the  Add icon, and then select a proxy application. You can select multiple proxy applications.

7. Click OK.

## Configuration Example for Decryption Bypass

The decrypt bypass option disables decryption of SSL traffic that matches the predefined captive portal actions for a URL filtering profile after captive portal redirection. The decryption policy decrypts SSL sessions to display only the captive portal response. After the captive portal action is performed, SSL decryption is bypassed, and users can directly access the URL.

The following example shows how to use a URL-filtering profile in which decrypt bypass is enabled in an SSL decryption policy. The configuration here displays a justify form when users try to access a social networking site (here, Facebook).

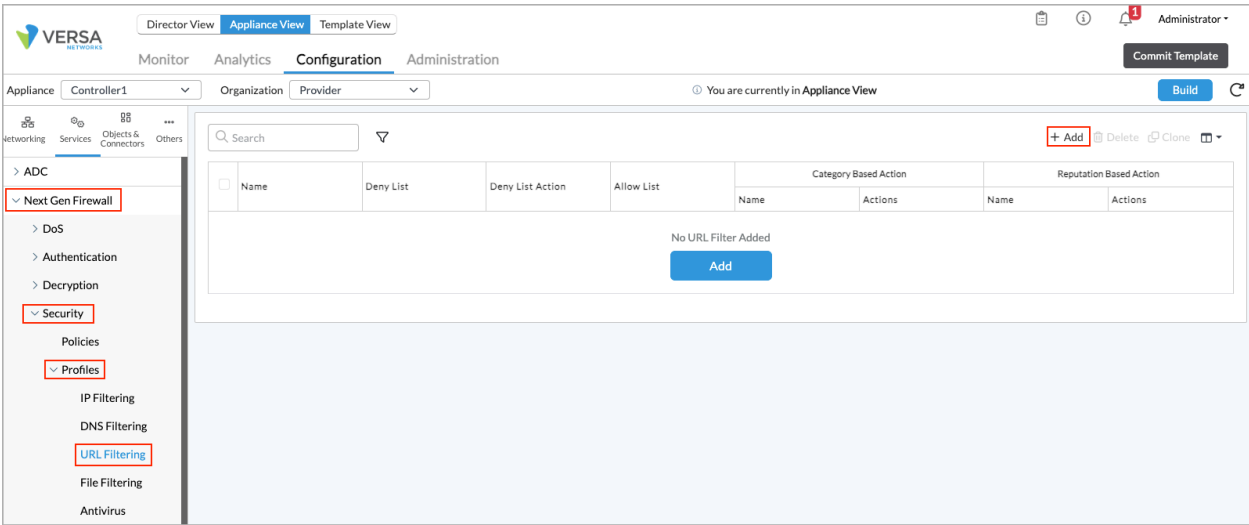
1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Click an appliance in the main pane. The view changes to Appliance view.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)

Updated: Wed, 23 Oct 2024 08:18:18 GMT

Copyright © 2024, Versa Networks, Inc.

- 2. Select the Configuration tab in the top menu bar.
- 3. Select Services > Next-Gen Firewall > Security > Profiles > URL Filtering.



- 4. Click the  Add icon. The Add URL Filter popup window displays.

Add URL Filter

Name \*
URLF\_Profile\_Social\_Networks

Description
Tags

Default Action
--Select--
☒ Decrypt Bypass
☐ Cloud Lookup State

LEF Profile
--Select--
☐ Default Profile

Deny List
Allow List
Category Based Action
Reputation Based Action

+
trash
filter
1
25

<input type="checkbox"/>	Name	Action
<input type="checkbox"/>	Category_Social_Media	justify

OK
Cancel

5. Add a URL-filtering profile with the following information. For more information, see [Configure URL Filtering](#).
  - a. In the Name field, enter a name for URL filter. In our example, the name is URLF\_Profile\_Social\_Networks.
  - b. Click the Decrypt Bypass checkbox to enable decryption bypass.
  - c. Select the Category-Based Action tab and add an action to justify access to social networking sites.
  - d. Click OK.
6. Go to Services > Next-Gen Firewall > Security > Policies, and then select the Rules tab.

Networking
Services
Objects & Connectors
Others

> ADC

Next Gen Firewall

DoS
Authentication
Decryption
Security
Policies
Profiles
Profile Groups
CASB Constraint
Security Settings

Access Policies
Rules

Default-Policy
Search
+ Add
Delete
Clone
Move

<input type="checkbox"/>	Rule Num	Name	Rule Disabled	Alias Name	Enforce	Services	Applications	URL Categories	U
					Actions	Security Profiles			
<input type="checkbox"/>	1	<a href="#">Allow-To-Analytics</a>	False		Allow		Custom: Analytics-Servi...		
<input type="checkbox"/>	2	<a href="#">Allow-From-CPE-Ports</a>	False		Allow		Custom: CPE-Ports, SN...		
<input type="checkbox"/>	3	<a href="#">Allow-ICMP</a>	False		Allow		Predefined: ICMP		
<input type="checkbox"/>	4	<a href="#">Deny-to-ControlNetZo...</a>	False		Deny				
<input type="checkbox"/>	5	<a href="#">Allow-All</a>	False		Allow				

Rows per page 25
Showing 1 - 5 of 5



7. Click the **+** Add icon.
8. In the Add Rule or Edit Rule popup window, add or edit a security access policy rule to apply to the URL-filtering profile. In our example, we update the rule named Justify\_Social\_Media\_Traffic. For more information, see [Configure Security Access Policy Rules](#).

Edit Rule - Justify\_Social\_Media-Traffic

General Source Destination Headers/Schedule **Applications/URL** Users/Groups Enforce

☐ Application List [+ New Application](#) [+ New Filter](#) [+ New Group](#) [+](#) [-](#)

Application List Not Configured

☐ URL Category List [+ New URL Category](#) [+](#) [-](#)

☐ **social\_network** [-](#)

☐ URL Reputations [+](#) [-](#)

Predefined Reputations Not Configured

**OK** **Cancel**

- a. Select the Applications/URL tab, click the **+** Add icon, and then select social\_network from the URL Category List.
- b. Select the Enforce tab.

**Edit Rule - Justify\_Social\_Media-Traffic**

General Source Destination Headers/Schedule Applications/URL Users/Groups **Enforce**

Actions | Log

Actions: ☐ Allow ☐ Deny ☐ Reject ☒ **Apply Security Profile**

Set-Type: ☒ Public ☐ Private ☐ None

Synced Flow: --Select-- Session Timeout (secs):  ☐ Send TCP Keep Alive at Session Timeout

☒ **Profiles** ☐ Profile Groups

☐ IP Filtering --Select-- 
 ☐ Antivirus --Select-- 
 ☐ File Filtering --Select--

☐ Vulnerability --Select-- 
 ☒ **URL Filtering** **URLF\_Profile\_Social\_Networks**   
 View URL-Filtering Profile

☐ DNS Filtering --Select-- 
 ☐ DLP Profile --Select--

☐ Predefined Vulnerability Profile Override --Select-- 
 ☐ CASB Profile --Select--

☐ ATP Profile --Select--

**OK** **Cancel**

- c. In the Actions field, select Apply Security Profile.
  - d. Click Profiles, and then select URL Filtering. Then select the profile you added, URLF\_Profile\_Social\_Networks, in Step 1. Note that in this profile, Decrypt Bypass is enabled.
9. Click OK.
  10. Upload a certificate, as described in [Upload a CA Certificate](#), above. When users try to access social networking sites, this certificate displays, along with the justify form.
  11. Add an SSL decryption profile, as described in [Configure an SSL Decryption Profile](#), above. In our example, the name of the decryption profile is Forward\_Proxy.

**Add Decryption Profile** ✕

**General** SSL Inspection SSL Protocol Advanced

Name \*

Description   
 Tags

☒ Enable Profile ☐ Support Session Ticket ☒ Use Extended Master Secret

Type \* Trusted Certificate Database \* CA Certificate \*

LEF Profile

☐ Default Profile

LEF Log Level

**OK** **Cancel**

- a. Add an SSL decryption policy rule in the Add Decryption popup window, as described in [Configure an SSL Decryption Policy Rule](#), above. In our example, the rule name is Justify\_Social\_Media\_Traffic.

**Add Decryption Rule** ✕

**General** Source Destination Headers/Schedule URL Users/Groups Enforce

Name \*

Description   
 Tags

☐ Disable Rule

**OK** **Cancel**

- b. Click OK.

## 12. Apply this rule to the SSL decryption rule that you created in Step 5.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_HTTP...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_HTTP...)

Updated: Wed, 23 Oct 2024 08:18:18 GMT

Copyright © 2024, Versa Networks, Inc.

- a. In the URL tab, select social\_network in the URL Category table.

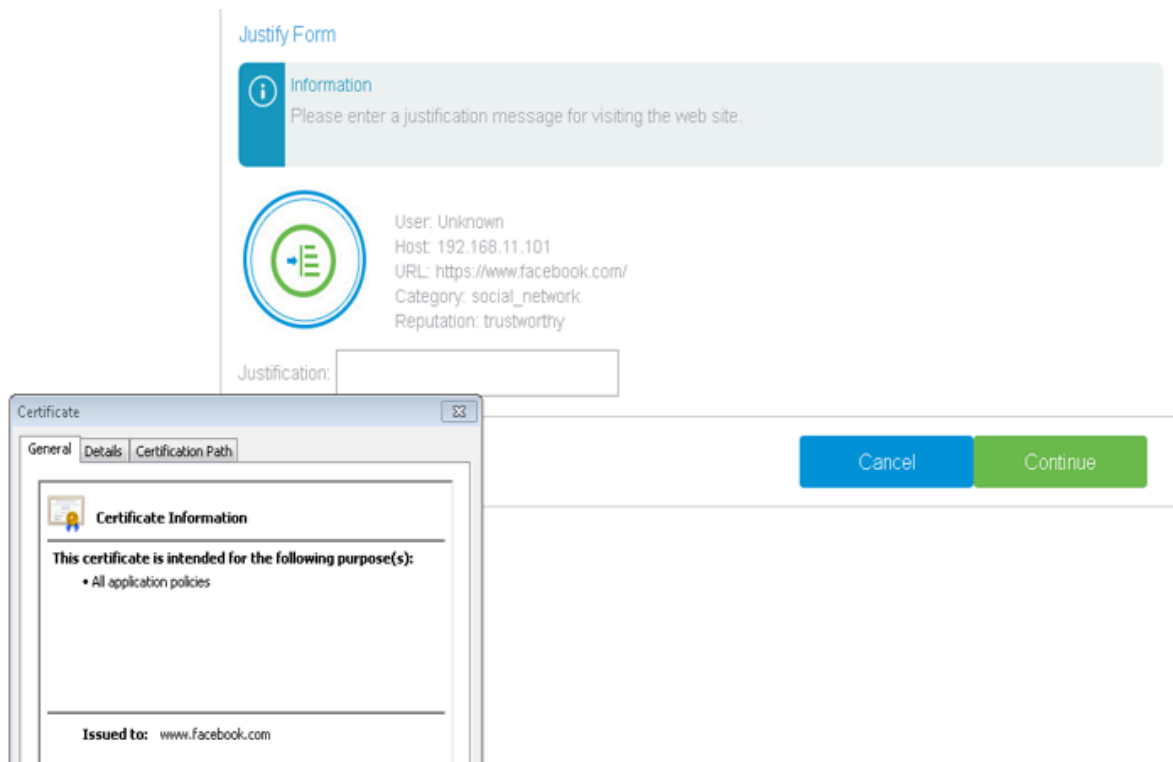
The screenshot shows the 'Add Decryption Rule' dialog box with the 'URL' tab selected. The 'URL Category' field has a dropdown menu with 'social\_network' selected. The 'URL Reputations' field is empty, showing 'Predefined Reputations Not Configured'. The 'OK' and 'Cancel' buttons are at the bottom right.

- b. In the Enforce tab:

- i. In the Action field, select decrypt.
- ii. In the Decryption Profile field, select the decryption profile you created in Step 5, here Forward\_Proxy.
- iii. In the URL Filtering field, select the URL filtering profile you created in Step 1, here URLF\_Profile\_Social\_Networks.

The screenshot shows the 'Add Decryption Rule' dialog box with the 'Enforce' tab selected. The 'Action' field is set to 'decrypt'. The 'Decryption Profile' field is set to 'Forward\_Proxy'. The 'URL Filtering' field is set to 'URLF\_Profile\_Social\_Networks'. The 'OK' and 'Cancel' buttons are at the bottom right.

13. Click OK.
14. When users try to access any social networking site, such as Facebook, the following justify form and CA certificate are displayed. To access Facebook, users must enter a justification and then click Continue.



To display the statistics for the SSL decryption profile called `Forward_Proxy`, issue the **show orgs organization name security profiles decrypt profile-stats decryption-profile-name** CLI command. The `ssl_pxy_bypass` field shows the number of times the decrypt bypass has been used in the decryption profile.

```
security profiles decrypt profile-stats Forward_Proxy
ssl_pxy_client_encrypt          0
ssl_pxy_client_decrypt         0
ssl_pxy_client_ptdata          0
ssl_pxy_server_encrypt         0
ssl_pxy_server_decrypt         0
ssl_pxy_server_ptdata          0
ssl_pxy_create                 0
ssl_pxy_strm                   0
ssl_pxy_drop                   0
ssl_pxy_url_match              0
ssl_pxy_url_decrypt            0
ssl_pxy_url_no_decrypt         0
ssl_pxy_bypass                 1
ssl_pxy_splice_failed          0
ssl_pxy_noprof_err             0
ssl_pxy_err                    0
ssl_alert_pxy_client_unexpected_message 0
ssl_alert_pxy_client_bad_record_mac     2
ssl_alert_pxy_client_decryption_failed  0
ssl_alert_pxy_client_record_overflow    0
ssl_alert_pxy_client_decompression_failure 0
ssl_alert_pxy_client_handshake_failure  0
```

```
ssl_alert_pxy_client_no_certificate      0
ssl_alert_pxy_client_bad_certificate     0
ssl_alert_pxy_client_unsupported_certificate 0
ssl_alert_pxy_client_certificate_revoked  0
ssl_alert_pxy_client_certificate_expired  0
```

---

## Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.2.1 adds support for CRL file uploading, SSL server profile configuration, setting the SSL encryption profile session cache history, displaying session history, validating a server certificate using OCSP, and configuring rule order for SSL decryption policy rules.
- Releases 22.1.2 renames the HTTP Header Insertion tab Advanced tab; adds support for proxy application certificates and proxy applications for web proxy.

---

## Additional Information

[Configure a DNS Proxy](#)

[Configure HTTP Header Profiles](#)

[Configure IP SLA Monitor Objects](#)

[Configure SNAT Pools](#)

[Configure URL Filtering](#)