CONTENTS

CHAPTER 1  What's New for Cisco IOS XE  1

CHAPTER 2  Security Overview  3

Cisco SD-WAN Security Components  3
Security Provided by NAT Devices  4
Security for Connections to External Devices  5
Control Plane Security Overview  5
  DTLS and TLS Infrastructure  6
  Control Plane Authentication  7
  Control Plane Encryption  9
  Control Plane Integrity  10
Data Plane Security Overview  10
  Data Plane Authentication and Encryption  11
  Data Plane Integrity  13
  Carrying VPN Information in Data Packets  15
Unified Threat Defense for Cisco SD-WAN  16
  Supported Platforms  16
  Restrictions  17

CHAPTER 3  Configure Security Parameters  19

Configure Control Plane Security Parameters  19
  Configure DTLS on vManage  20
Configure Data Plane Security Parameters  21
  Configure Allowed Authentication Types  21
  Change the Rekeying Timer  22
  Change the Size of the Anti-Replay Window  23
VPN Interface IPsec 25
  Create VPN IPsec Interface Template 25
Changing the Scope for a Parameter Value 25
Configure IPsec Tunnel Parameters 26
Configure Dead-Peer Detection 27
Configure IKE 27

CHAPTER 4

Enterprise Firewall with Application Awareness 33
  Overview of Enterprise Firewall with Application Awareness 33
Configure Firewall Policies 34
  Create or Modify Lists 35
  Use the Policy Configuration Wizard 36
  Apply a Security Policy to a Device 40
Zone-Based Firewall Configuration Examples 40
  Firewall High-Speed Logging 43
  Information About Firewall High-Speed Logging 44
    Firewall High-Speed Logging Overview 44
    NetFlow Field ID Descriptions 45
    HSL Messages 48
  How to Configure Firewall High-Speed Logging 55
    Enabling Firewall High-Speed Logging Using vManage 55
    Enabling High-Speed Logging for Global Parameter Maps 56
    Enabling High-Speed Logging for Firewall Actions 57
  Configuration Examples for Firewall High-Speed Logging 58
    Example: Enabling High-Speed Logging for Global Parameter Maps 58
    Example: Enabling High-Speed Logging for Firewall Actions 59

CHAPTER 5

Intrusion Prevention System 61
  Overview of Intrusion Prevention System 61
Cisco SD-WAN IPS Solution 62
Configure and Apply IPS or IDS 62
  Before you Begin 62
  Configure Intrusion Prevention or Detection 62
  Apply a Security Policy to a Device 65
CHAPTER 6

URL Filtering  71
Overview of URL Filtering  71
  Filtering Options  72
    Category-Based Filtering  72
    Reputation-Based Filtering  72
    List-based Filtering  73
  Configure and Apply URL Filtering  73
    Before you Begin  73
    Configure URL Filtering  73
    Apply a Security Policy to a Device  77
  Modify URL Filtering  77
  Delete URL Filtering  78
  Monitor URL Filtering  78

CHAPTER 7

Advanced Malware Protection  81
Overview of Advanced Malware Protection  81
Configure and Apply an Advanced Malware Policy  82
  Before you Begin  82
    Configure Threat Grid API Key  82
    Configuring an Advanced Malware Protection Policy  83
  Apply a Security Policy to a Device  85
  Modify an Advanced Malware Protection Policy  86
  Delete an Advanced Malware Protection Policy  87
  Monitor Advanced Malware Protection  87
  Troubleshoot Advanced Malware Protection  88
  Rekey the Device Threat Grid API Key  88

CHAPTER 8

SSL/TLS Proxy for Decryption of TLS Traffic  89
Information about SSL/TLS Proxy  89
<table>
<thead>
<tr>
<th>Chapter 9: Cisco Umbrella Integration</th>
<th>113</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Cisco SD-WAN Umbrella Integration</td>
<td>113</td>
</tr>
<tr>
<td>Restrictions for Umbrella Integration</td>
<td>115</td>
</tr>
<tr>
<td>Prerequisites for Umbrella Integration</td>
<td>116</td>
</tr>
<tr>
<td>Configure Umbrella API Token</td>
<td>116</td>
</tr>
<tr>
<td>Configure Cisco Umbrella Registration</td>
<td>116</td>
</tr>
<tr>
<td>Define Domain Lists</td>
<td>117</td>
</tr>
<tr>
<td>Configure Umbrella DNS Policy Using Cisco vManage</td>
<td>117</td>
</tr>
<tr>
<td>Attach DNS Umbrella Policy to Device Template</td>
<td>118</td>
</tr>
<tr>
<td>Umbrella Integration Using CLI</td>
<td>119</td>
</tr>
<tr>
<td>Umbrella show commands at FP Layer</td>
<td>124</td>
</tr>
<tr>
<td>Umbrella show commands at CPP Layer</td>
<td>125</td>
</tr>
</tbody>
</table>

| Overview of SSL/TLS Proxy | 89 |
| Role of Certificate Authorities in TLS Proxy | 91 |
| Supported Platforms and Platform Requirements | 94 |
| Supported Cipher Suites | 94 |
| Prerequisites for TLS Proxy | 95 |
| Limitations and Restrictions | 95 |
| Configure Cisco IOS XE SD-WAN Devices as TLS Proxy | 96 |
| Configure CA for TLS Proxy | 98 |
| Configure Enterprise CA | 98 |
| Configure Cisco vManage as CA | 99 |
| Configure vManage as Intermediate CA | 99 |
| Configure SSL Decryption | 100 |
| Apply a Security Policy to an XE SD-WAN Router | 104 |
| Upload a Subordinate CA Certificate to TLS Proxy | 104 |
| Verify Configuration | 106 |
| Monitor TLS Proxy Performance | 107 |
| Monitor TLS Proxy | 107 |
| Monitor SSL Decryption Statistics | 108 |
| Revoke and Renew Certificates | 110 |
| Revoke Enterprise CA Certificate | 110 |
| vManage as CA or vManage as Intermediate CA | 112 |

<p>| Restrictions for Umbrella Integration | 115 |
| Prerequisites for Umbrella Integration | 116 |
| Configure Umbrella API Token | 116 |
| Configure Cisco Umbrella Registration | 116 |
| Define Domain Lists | 117 |
| Configure Umbrella DNS Policy Using Cisco vManage | 117 |
| Attach DNS Umbrella Policy to Device Template | 118 |
| Umbrella Integration Using CLI | 119 |
| Umbrella show commands at FP Layer | 124 |
| Umbrella show commands at CPP Layer | 125 |</p>
<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Integrate With Secure Internet Gateways</th>
<th>133</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create the SIG Template</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Attach the SIG Template to Devices</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>Configure a GRE Tunnel from Cisco vManage</td>
<td>137</td>
</tr>
<tr>
<td></td>
<td>Configure an IPsec Tunnel from Cisco vManage</td>
<td>137</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11</th>
<th>Security Virtual Image</th>
<th>139</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identify the Recommended Security Virtual Image Version</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>Upload the Cisco Security Virtual Image to vManage</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>Upgrade a Security Virtual Image</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Verifying Your SVI Upgrade</td>
<td>142</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12</th>
<th>IPSec Pairwise Keys Overview</th>
<th>145</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supported Platforms</td>
<td>145</td>
</tr>
<tr>
<td></td>
<td>Pairwise Keys</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>IPsec Security Association Rekey</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>Configure IPSec Pairwise Keys</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>Configure IPSec Pairwise Keys Using Cisco vManage</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>Configure Pairways Keys and Rekeying</td>
<td>147</td>
</tr>
<tr>
<td></td>
<td>Verify IPSec Pairwise Keys on Cisco XE SD-WAN Routers</td>
<td>148</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13</th>
<th>Configure Single Sign-On</th>
<th>151</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure Single Sign-On using Okta</td>
<td>151</td>
</tr>
<tr>
<td></td>
<td>Enable an Identity Provider in vManage</td>
<td>151</td>
</tr>
<tr>
<td></td>
<td>Configure SSO on the Okta Website</td>
<td>152</td>
</tr>
<tr>
<td></td>
<td>Assign Users to the Application</td>
<td>154</td>
</tr>
<tr>
<td></td>
<td>Configure SSO for Active Directory Federation Services (ADFS)</td>
<td>154</td>
</tr>
<tr>
<td></td>
<td>Import Metadata File into ADFS</td>
<td>154</td>
</tr>
</tbody>
</table>
What's New for Cisco IOS XE

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco SD-WAN solution, see the Resolved and Open Bugs section in the Release Notes.

What's New in Cisco IOS XE Release Amsterdam 17.2.1r
Security Overview

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing. There are multiple problems with the traditional ways of securing networks, including:

- Very little emphasis is placed on ensuring the authenticity of the devices involved in the communication.
- Securing the links between a pair of devices involves tedious and manual setup of keys and shared passwords.
- Scalability and high availability solutions are often at odds with each other.

This chapter contains the following topics:

- Cisco SD-WAN Security Components, on page 3
- Security Provided by NAT Devices, on page 4
- Security for Connections to External Devices, on page 5
- Control Plane Security Overview, on page 5
- Data Plane Security Overview, on page 10
- Unified Threat Defense for Cisco SD-WAN, on page 16

Cisco SD-WAN Security Components

The Cisco SD-WAN solution takes a fundamentally different approach to security, basing its core design around the following precepts:

- Authentication—The solution ensures that only authentic devices are allowed to send traffic to one another.
- Encryption—All communication between each pair of devices is automatically secure, completely eliminating the overhead involved in securing the links.
- Integrity—No group keys or key server issues are involved in securing the infrastructure.

These three components—authentication, encryption, and integrity—are key to securing the Cisco SD-WAN overlay network infrastructure.
The topics on Control Plane Security Overview and Data Plane Security Overview examine how authentication, encryption, and integrity are implemented throughout the Cisco SD-WAN overlay network. The security discussion refers to the following illustration of the components of the Cisco SD-WAN network—the vSmart controller, the vBond orchestrator, and the routers. The connections between these devices form the control plane (in orange) and the data plane (in purple), and it is these connections that need to be protected by appropriate measures to ensure the security of the network devices and all network traffic.

**Security Provided by NAT Devices**

While the primary purpose of NAT devices is to allow devices with private IP addresses in a local-area network (LAN) to communicate with devices in public address spaces, such as the Internet, NAT devices also inherently provide a level of security, functioning as hardware firewalls to prevent unwanted data traffic from passing through the routers and to the LAN networks in the service-side networks connected to the router.

To enhance the security at branch sites, you can place the router behind a NAT device. The router can interact with NAT devices configured with the following Session Traversal Utilities for NAT (STUN) methods, as defined in RFC 5389:

- **Full-cone NAT, or one-to-one NAT**—This method maps an internal address and port pair to an external address and port. Any external host can send packets to LAN devices behind the router by addressing them to the external address and port.

- **Address-restricted cone NAT, or restricted-cone NAT**—This method also maps an internal address and port to an external address and port. However, an external host can send packets to the internal device only if the external address (and any port at that address) has received a packet from the internal address and port.

- **Port-restricted cone NAT**—This method is a stricter version of restricted-cone NAT, in which an external host can send packets to the internal address and port only if the external address and port pair has received a packet from that internal address and port. The external device must send packets from the specific port to the specific internal port.

- **Symmetric NAT**—With this method, each request from the same internal IP address and port to an external IP address and port is mapped to a unique external source IP address and port. If the same internal host sends a packet with the same source address and port but to a different destination, the NAT device creates a different mapping. Only an external host that receives a packet from an internal host can send a packet back. The routers support symmetric NAT only on one side of the WAN tunnel. That is, only one of the NAT devices at either end of the tunnel can use symmetric NAT. When a router operates behind a NAT device running symmetric NAT, only one of the NAT devices at either end of the tunnel can use symmetric NAT. The router that is behind a symmetric NAT cannot establish a BFD tunnel with...
a remote router that is behind a symmetric NAT, an address-restricted NAT, or a port-restricted NAT. To allow a router to function behind a symmetric NAT, you must configure the vManage and vSmart controller control connections to use TLS. DTLS control connections do not work through a symmetric NAT.

Security for Connections to External Devices

Cisco SD-WAN routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device. The Cisco SD-WAN software supports IKE version 2, which performs mutual authentication and establishes and maintains security associations (SAs). IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

Control Plane Security Overview

The control plane of any network is concerned with determining the network topology and defining how to direct packets. In a traditional network, the control plane operations of building and maintaining routing and forwarding tables and directing packets towards their destination are handled by routing and switching protocols, which typically offer few or no mechanisms for authenticating devices or for encrypting routing updates and other control information. In addition, the traditional methods for providing security are highly manual and do not scale. As examples, certificates are typically installed manually rather than in an automated fashion, and using preshared keys is not a very secure approach for providing device security.

The Cisco SD-WAN control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The vSmart controller, which is the centralized brain of the Cisco SD-WAN solution, establishes and maintains DTLS or TLS connections to all Cisco SD-WAN devices in the overlay network: to the routers, the vBond orchestrators, to Cisco vManage, and to other vSmart controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Cisco SD-WAN devices in the network, using the Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all control traffic sent over the connections.

The privacy and encryption in the control plane offered by DTLS and TLS provide a safe and secure foundation for the other two security components, authentication and integrity. To perform authentication, the Cisco SD-WAN devices exchange digital certificates. These certificates, which are either installed by the software or hard-coded into the hardware, depending on the device, identify the device and allow the devices themselves to automatically determine which ones belong in the network and which are imposters. For integrity, the DTLS or TLS connections run AES-256-GCM, a cryptographic secure hash algorithm which ensures that all control and data traffic sent over the connections has not been tampered with.
The following are the control plane security components, which function in the privacy provided by DTLS or TLS connections:

- **AES-256-GCM** algorithm provides encryption services.
- **Digital certificates** are used for authentication.
- **AES-256-GCM** is responsible for ensuring integrity.

## DTLS and TLS Infrastructure

Security protocols derived from SSL provide the foundation for the Cisco SD-WAN control plane infrastructure. The first is the DTLS protocol, which is a transport privacy protocol for connectionless datagram protocols such as UDP, provides the foundation for the Cisco SD-WAN control plane infrastructure. It is based on the stream-oriented Transport Layer Security (TLS) protocol, which provides security for TCP-based traffic. (TLS itself evolved from SSL.) The Cisco SD-WAN infrastructure design uses DTLS running over UDP to avoid some of the issues with TCP, including the delays associated with stream protocols and some security issues. However, because UDP performs no handshaking and sends no acknowledgments, DTLS has to handle possible packet re-ordering, loss of datagrams, and data larger than the datagram packet size.

The control plane infrastructure can also be configured to run over TLS. This might be desirable in situations where the protections of TCP outweigh its issues. For example, firewalls generally offer better protection for TCP servers than for UDP servers.

The Cisco SD-WAN software implements the standard version of DTLS with UDP, which is defined in RFC 6347. DTLS for use with other protocols is defined in a number of other RFCs. For TLS, the Cisco SD-WAN software implements the standard version defined in RFC 5246. As described in the RFCs, Cisco SD-WAN uses DTLS and TLS versions 1.2.

In the Cisco SD-WAN architecture, the Cisco SD-WAN devices use DTLS or TLS as a tunneling protocol, which is an application-level (Layer 4) tunneling protocol. When the vSmart controllers, vBond orchestrators, Cisco vManages, and routers join the network, they create provisional DTLS or TLS tunnels between them as part of the device authentication process. After the authentication process completes successfully, the provisional tunnels between the routers and vSmart controllers, and those between the vBond orchestrators and vSmart controllers, become permanent and remain up as long as the devices are active in the network. It is these authenticated, secure DTLS or TLS tunnels that are used by all the protocol applications running on the Cisco SD-WAN devices to transport their traffic. For example, an OMP session on a router communicates with an OMP session on a vSmart controller by sending plain IP traffic through the secure DTLS or TLS tunnel between the two devices. The Overlay Management Protocol is the Cisco SD-WAN control protocol used to exchange routing, policy, and management information among Cisco SD-WAN devices, as described in Overlay Routing Overview.
A Cisco SD-WAN daemon running on each vSmart controller and router creates and maintains the secure DTLS or TLS connections between the devices. This daemon is called vdaemon and is discussed later in this article. After the control plane DTLS or TLS connections are established between these devices, multiple protocols can create sessions to run and route their traffic over these connections—including OMP, Simple Network Management Protocol (SNMP), and Network Configuration Protocol (Netconf)—without needing to be concerned with any security-related issues. The session-related traffic is simply directed over the secure connection between the routers and vSmart controllers.

Control Plane Authentication

The Cisco SD-WAN control plane uses digital certificates with 2048-bit RSA keys to authenticate the Cisco SD-WAN routers in the network. The digital certificates are created, managed, and exchanged by standard components of the public key infrastructure (PKI):

- **Public keys**—These keys are generally known.
- **Private keys**—These keys are private. They reside on each Cisco SD-WAN router and cannot be retrieved from the router.
- **Certificates** signed by a root certification authority (CA)—The trust chain associated with the root CA needs to be present on all Cisco SD-WAN routers.

In addition to standard PKI components, the Cisco SD-WAN router serial numbers and the router chassis numbers are used in the authentication processes.

Let's first look at the PKI components that are involved in router authentication. On the Cisco XE SD-WAN router, the public and private keys and the certificates are managed automatically, by a hardware security chip that is built into the router called the Trust Anchor module (TAm). The TAm is a proprietary, tamper-resistant chip that features non-volatile secure storage for the Secure Unique Device Identifier (SUDI), as well as secure generation and storage of key pairs with cryptographic services including random number generation (RNG). When the routers are manufactured, this chip is programmed with a signed certificate. This certificate includes the router's public key, its serial number, and the router's private key. When the routers boot up and join the network, they exchange their certificates (including the router's public key and serial number) with other Cisco SD-WAN routers as part of the router authentication process. Note that the router's private key always remains embedded in the router's Trusted Board ID chip, and it is never distributed, nor can it ever be retrieved from the router. In fact, any brute-force attempt to read the private key causes the hardware security chip to fail, thereby disabling all access to the router.

For vSmart controllers, vBond orchestrators, and Cisco vManage systems, the public and private keys and the certificates are managed manually. When you boot these routers for the first time, the Cisco SD-WAN software generates a unique private key–public key pair for each software image. The public key needs to be signed by the CA root. The network administrator then requests a signed certificate and manually installs it and the certificate chains on the vSmart controllers, vBond orchestrators, and Cisco vManage systems. A
typical network might have only a small handful of vSmart controllers, vBond orchestrators, and Cisco vManages, so the burden of manually managing the keys and certificates on these routers is small.

When you place an order with Cisco using your Smart and Virtual Account, Cisco updates the Cisco Plug and Play (PNP) Portal with the chassis and certificate serial numbers of the devices that you purchased. You can then use Cisco vManage to sync the device information from the PNP portal using your Smart Account credentials. Alternatively, you can also download the trusted WAN Edge serial file from the PNP portal and upload it manually to Cisco vManage. Cisco vManage then broadcasts this information to the other controllers. Both the authorized serial number file and the file listing the vSmart serial numbers are uploaded and installed on vBond orchestrators. Then, during the automatic authentication process, as pairs of devices (routers and controllers) are establishing DTLS control connections, each device compares the serial numbers (and for routers, the chassis numbers) to those in the files installed on the router. A router allows a connection to be established only if the serial number or serial–chassis number combination (for a router) matches.

You can display the installed vSmart authorized serial numbers using the `show control valid-vsmarts` command on a vSmart controller and the `show orchestrator valid-vsmarts` command on a vBond orchestrator. You can also run `show sdwan control valid-vsmarts` on Cisco IOS XE SD-WAN devices. You can display the installed router authorized serial and chassis number associations using the `show control valid-vedges` command on a vSmart controller and the `show orchestrator valid-devices` command on a vBond orchestrator.

Now, let's look at how the PKI authentication components and the router serial and chassis numbers are used to authenticate router on the Cisco SD-WAN overlay network. When vSmart controllers, vBond orchestrators, and routers first boot up, they establish secure DTLS or TLS connections between the vSmart controllers and the routers. Over these connections, the devices authenticate each other, using the public and private keys, the signed certificates, and the routers serial numbers and performing a series of handshake operations to ensure that all the devices on the network are valid and not imposters. The following figure illustrates the key and certificate exchange that occurs when the Cisco SD-WAN devices boot. For details about the authentication that occurs during the bringup process, see Bringup Sequence of Events.
Control Plane Encryption

Control plane encryption is done by either DTLS, which is based on the TLS protocol, or TLS. These protocols encrypt the control plane traffic that is sent across the connections between Cisco SD-WAN devices to validate the integrity of the data. TLS uses asymmetric cryptography for authenticating key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

A single Cisco SD-WAN device can have DTLS or TLS connections to multiple Cisco SD-WAN devices, so vdaemon creates a kernel route for each destination. For example, a router would typically have one kernel route, and hence one DTLS or TLS connection, for each vSmart controller. Similarly, a vSmart controller would have one kernel route and one DTLS or TLS connection for each router in its domain.
Control Plane Integrity

The Cisco SD-WAN design implements control plane integrity by combining two security elements: SHA-1 or SHA-2 message digests, and public and private keys.

SHA-1 and SHA-2 are cryptographic hash functions that generate message digests (sometimes called simply digests) for each packet sent over a control plane connection. SHA-1 generates a 160-bit message digest. SHA-2 is a family that consists of six hash functions with digests that are 224, 256, 384, or 512 bits. The receiver then generates a digest for the packet, and if the two match, the packet is accepted as valid. Both SHA-1 and SHA-2 allow verification that the packet's contents have not been tampered with.

The second component of control plane integrity is the use of public and private keys. When a control plane connection is being established, a local Cisco SD-WAN device sends a challenge to a remote device. The remote device encrypts the challenge by signing it with its private key, and returns the signed challenge to the local device. The local device then uses the remote device’s public key to verify that the received challenge matches the sent challenge.

Then, once a control plane connection is up, keys are used to ensure that packets have been sent by a trusted host and were not inserted midstream by an untrusted source. The authenticity of each packet is verified through encryption and decryption with symmetric keys that were exchanged during the process of establishing the control connection.

Data Plane Security Overview

The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they could be sent through MPLS tunnels. If the routers in the Cisco SD-WAN overlay network were to send traffic over a public IP cloud, the transmission would be insecure. Anyone would be able to sniff the traffic, and it would be easy to implement various types of attacks, including man-in-the-middle (MITM) attacks.

The underlying foundation for security in the Cisco SD-WAN data plane is the security of the control plane. Because the control plane is secure—all devices are validated, and control traffic is encrypted and cannot be tampered with—we can be confident in using routes and other information learned from the control plane to create and maintain secure data paths throughout a network of routers.

The data plane provides the infrastructure for sending data traffic among the routers in the Cisco SD-WAN overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Cisco SD-WAN data plane implements the key security components of authentication, encryption, and integrity in the following ways:

- Authentication—As mentioned above, the Cisco SD-WAN control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:
  - In the traditional key exchange model, the vSmarts sends IPsec encryption keys to each edge device.
In the pairwise keys model, the vSmart sends Diffie-Hellman public values to the edge devices and they generate pairwise IPsec encryption keys using ECDH and a P-384 curve. For more information, see Pairwise Keys, on page 146.

- By default IPsec tunnel connections use a modified version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels.

- **Encryption**—A modified version of ESP protects the data packet's payload. This version of the protocol also checks the outer IP and UDP headers. Hence, this option supports an integrity check of the packet similar to the Authentication Header (AH) protocol. Data encryption is done using the AES-GCM-256 cipher.

  The standard ESP protocol protects the data packet’s payload, and the standard AH protocol protects both the payload and the non-mutable header fields. Key exchange encryption is done using the AES-256 cipher.

- **Integrity**—To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:
  - A modified version of the ESP protocol encapsulates the payload of data packets.
  - The modified version of ESP uses an AH-like mechanism to check the integrity of the outer IP and UDP headers. You can configure the integrity methods supported on each router, and this information is exchanged in the router’s TLOC properties. If two peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.
  - The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

### Data Plane Authentication and Encryption

During the bringup of the overlay, the Cisco vSmart Controller establishes the information for edge routers to send data to each other. However before a pair of routers can exchange data traffic, they establish an IPsec connection between them, which they use as a secure communications channel. Since the Cisco vSmart Controller has authenticated the devices, the devices do not further authenticate each other.

Control plane communications have allowed the edge device to have enough information to establish IPsec tunnels. Edge devices simply send data through the tunnels. There is no authentication step.

In a traditional IPsec environment, key exchange is handled by the Internet Key Exchange (IKE) protocol. IKE first sets up secure communications channels between devices and then establishes security associations (SAs) between each pair of devices that want to exchange data. IKE uses a Diffie-Hellman key exchange algorithm to generate a shared key that encrypts further IKE communication. To establish SAs, each device (n) exchanges keys with every other device in the network and creates per-pair keys, generating a unique key for each remote device. This scheme means that in a fully meshed network, each device has to manage $n^2$ key exchanges and $(n-1)$ keys. As an example, in a 1,000-node network, 1,000,000 key exchanges are required to authenticate the devices, and each node is responsible for maintaining and managing 999 keys.

The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- The handshaking required to set up the communications channels is both time consuming and resource intensive.
• The processing required for the key exchange, especially in larger networks, can strain network resources and can take a long time.

The Cisco SD-WAN implementation of data plane authentication and encryption establishes SAs between each pair of devices that want to exchange data, but it dispenses with IKE altogether. Instead, to provide a scalable solution to data plane key exchange, the Cisco SD-WAN solution takes advantage of the fact that the DTLS control plane connections in the Cisco SD-WAN overlay network are known to be secure. Because the Cisco SD-WAN control plane establishes authenticated, encrypted, and tamperproof connections, there is no need in the data plane to set up secure communications channels to perform data plane authentication.

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other routers in the network. In this way, the AES keys for all the routers are distributed across the network. Even though the key exchange is symmetric, the routers use it in an asymmetric fashion. The result is a simple and scalable key exchange process that uses the Cisco vSmart Controller.

In Cisco SD-WAN Release 19.2.x and Cisco IOS XE SD-WAN Release 16.12.x onwards, Cisco SD-WAN supports IPSec pairwise keys that provide additional security. When IPSec pairwise keys are used, the edge router generates public and private Diffie-Hellman components and sends the public value to the vSmart for distribution to all other edge devices. For more information, see IPSec Pairwise Keys Overview, on page 145.

If control policies configured on a vSmart controller limit the communications channels between network devices, the reachability advertisements sent by the vSmart controller contain information only for the routers that they are allowed to exchange data with. So, a router learns the keys only for those routers that they are allowed to communicate with.

To further strengthen data plane authentication and encryption, routers regenerate their AES keys aggressively (by default, every 24 hours). Also, the key regeneration mechanism ensures that no data traffic is dropped when keys change.

In the Cisco SD-WAN overlay network, the liveness of SAs between router peers is tracked by monitoring BFD packets, which are periodically exchanged over the IPsec connection between the peers. IPsec relays the connection status to the vSmart controllers. If data connectivity between two peers is lost, the exchange of BFD packets stops, and from this, the vSmart controller learns that the connection has been lost.

The IPsec software has no explicit SA idle timeout, which specifies the time to wait before deleting SAs associated with inactive peers. Instead, an SA remains active as long as the IPsec connection between two
routers is up, as determined by the periodic exchange of BFD packets between them. Also, the frequency with which SA keys are regenerated obviates the need to implement an implicit SA idle timeout.

In summary, the Cisco SD-WAN data plane authentication offers the following improvements over IKE:

- Because only $n+1$ keypaths are required rather than the $n^2$ required by IKE, the Cisco SD-WAN solution scales better as the network grows large.
- Keys are generated and refreshed locally, and key exchange is performed over a secure control plane.

## Data Plane Integrity

The following components contribute to the integrity of data packets in the Cisco SD-WAN data plane:

- **ESP**, which is a standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets. The modifications to ESP also protect the outer IP and UDP headers.
- Modifications to ESP, which protect (via authentication) the outer IP and UDP headers. This mimics the functionality of the AH protocol.
- Anti-replay, which is also part of the standard IPsec software suite, provides a mechanism to number all data packets and to ensure that receiving routers accept only packets with unique numbers.

The first of these components, ESP, is the standard IPsec encryption protocol. ESP protects a data packet’s payload and its inner IP header fields both by encryption, which occurs automatically, and authentication. For authentication, ESP performs a checksum calculation on the data packet’s payload and inner header fields and places the resultant hash (also called a digest) into a 12-byte HMAC-SHA1 field at the end of the packet. (A hash is a one-way compression.) The receiving device performs the same checksum and compares its calculated hash with that in the packet. If the two checksums match, the packet is accepted. Otherwise, it is dropped. In the figure below, the left stack illustrates the ESP/UDP encapsulation. ESP encrypts and authenticates the inner headers, payload, MPLS label (if present), and ESP trailer fields, placing the HMAC-SHA1 hash in the ICV checksum field at the end of the packet. The outer header fields added by ESP/UDP are neither encrypted nor authenticated.

A second component that contributes to data packet integrity is the modifications to ESP to mimic AH. This modification performs a checksum that includes calculating the checksum over all the fields in the packet—the payload, the inner header, and also all the non-mutable fields in the outer IP header. AH places the resultant HMAC-SHA1 hash into the last field of the packet. The receiving device performs the same checksum, and accepts packets whose checksums match. In the figure below, the center stack illustrates the encapsulation performed by the modified version of ESP. ESP again encrypts the inner headers, payload, MPLS label (if present), and ESP trailer fields, and now mimics AH by authenticating the entire packet—the outer IP and UDP headers, the ESP header, the MPLS label (if present), the original packet, and the ESP trailer—and places its calculated HMAC-SHA1 hash into the ICV checksum field at the end of the packet.

For situations in which data packet authentication is not required, you can disable data packet authentication altogether. In this case, data packets are processed just by ESP, which encrypts the original packet, the MPLS label (if present), and the ESP trailer. This scheme is illustrated in the right stack in the figure below.
Note that Cisco SD-WAN devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the HMAC-SHA1 digest. Both are distributed as part of the TLOC properties for a router.

Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this type of attack, an adversary tampers with the data traffic by inserting a copy of a message that was previously sent by the source. If the destination cannot distinguish the replayed message from a valid message, it may authenticate the adversary as the source or may incorrectly grant the adversary unauthorized access to resources or services.

As a counter to such attacks, the Cisco SD-WAN overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender inserts a sequence number into each IPsec packet, and the destination checks the sequence number, accepting only packets with unique, non-duplicate sequence numbers. The second component is a sliding window, which defines a range of sequence numbers that are current. The sliding window has a fixed length. The destination accepts only packets whose sequence numbers fall within the current range of values in the sliding window, and it drops all others. A sliding window is used rather than accepting only packets whose sequence number is larger than the last known sequence number, because packets often do not arrive in order.
When the destination receives a packet whose sequence number is larger than the highest number in the sliding window, it slides the window to the right, thus changing the range of valid sequences numbers it will accept. This scheme protects against an MITM type of attack because, by choosing the proper window size, you can ensure that if a duplicate packet is inserted into the traffic stream, its sequence number will either be within the current range but will be a duplicate, or it will be smaller than the lowest current value of the sliding window. Either way, the destination will drop the duplicate packet. So, the sequence numbering combined with a sliding window provide protection against MITM type of attacks and ensure the integrity of the data stream flowing within the IPsec connection.

### Carrying VPN Information in Data Packets

For enterprise-wide VPNs, Cisco SD-WAN devices support MPLS extensions to data packets that are transported within IPsec connections. The figure to the right shows the location of the MPLS information in the data packet header. These extensions provide the security for the network segmentation (that is, for the VPNs) that is needed to support multi-tenancy in a branch or segmentation in a campus. The Cisco SD-WAN implementation uses IPsec UDP-based overlay network layer protocol encapsulation as defined in RFC 4023. The security is provided by including the Initialization Vector (IV) at the beginning of the payload data in the ESP header. The IV value is calculated by the AES-256 cipher block chaining (CBC).
Unified Threat Defense for Cisco SD-WAN

The attack surface at branch locations continues to increase with local breakouts, especially with direct internet access. As a result, protecting the branch with right security capabilities is even more critical than before. Secure SD-WAN brings key security capabilities embedded natively in SD-WAN solution with cloud-based single-pane of management for both SD-WAN and security capabilities.

The security capabilities include enterprise firewall with application awareness, intrusion prevention systems with Cisco Talos signatures, URL-Filtering, and DNS/Web-layer Security. The security capabilities help customers achieve PCI compliance, segmentation, threat protection, content filtering and much more. With Cisco Umbrella DNS/Web-security layer, you get a layer of protection for all branch users from malware, botnets, phishing, and targeted online attacks.

Cisco SD-WAN offers the following security features:

*Table 1: Cisco SD-WAN SD-WAN Security Features*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Firewall with Application Awareness, on page 33</td>
<td>A stateful firewall with NBAR2 application detection engine to provide application visibility and granular control, capable of detecting 1400+ applications.</td>
</tr>
<tr>
<td>Intrusion Prevention System, on page 61</td>
<td>This system is backed by Cisco Talos signatures and are updated automatically. The Intrusion Prevention System is deployed using a security virtual image.</td>
</tr>
<tr>
<td>URL Filtering, on page 71</td>
<td>Enforces acceptable use controls to block or allow URLs based on 82 different categories and a web reputation score. The URL Filtering system is deployed using a security virtual image.</td>
</tr>
<tr>
<td>Advanced Malware Protection, on page 81</td>
<td>Global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches. It also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware. The Advanced Malware Protection system is deployed using a security virtual image.</td>
</tr>
<tr>
<td>Cisco Umbrella Integration, on page 113</td>
<td>Cloud-delivered enterprise network security which provides users with a first line of defense against cyber security threats.</td>
</tr>
</tbody>
</table>

**Supported Platforms**

For features that use the Security Virtual Image (Intrusion Prevention System, URL filtering, and Advanced Malware Protection), only the following platforms are supported:

- Cisco 4351 Integrated Services Router (ISR 4351)
- Cisco 4331 Integrated Services Router (ISR 4331)
• Cisco 4321 Integrated Services Router (ISR 4321)
• Cisco 4221X Integrated Services Router (ISR 4221X)
• Cisco 4431 Integrated Services Router (ISR 4431)
• Cisco 4451 Integrated Services Router (ISR 4451)
• Cisco 4461 Integrated Services Router (ISR 4461)
• Cisco Integrated Services Router 1111X-8P (C1111X-8P)
• Cisco Integrated Services Router 1121X-8PLTEP (C1121X-8PLTEP)
• Cisco Integrated Services Router 1121X-8PLTEPWY (C1121X-8PLTEPWY)
• Cisco Integrated Services Router 1126X-8PLTEP (C1126X-8PLTEP)
• Cisco Integrated Services Router 1127X-8PLTEP (C1127X-8PLTEP)
• Cisco Integrated Services Router 1127X-8PMLTEP (C1127X-8PMLTEP)
• Cisco Integrated Services Router 1161X-8P (C1161X-8P)
• Cisco Integrated Services Router 1161X-8PLTEP (C1161X-8PLTEP)
• Cisco Cloud Services Router 1000v series (CSR 1000v) on Amazon Web Services (AWS)
• Cisco Integrated Services Virtual Router

Restrictions

• ISR 1111X-8P does not support all of the IPS signatures because it does not support the pre-compiled rules of Snort.

• For Intrusion Prevention, URL-Filtering, and Advanced Malware Prevention (features that leverage the Security Virtual Image), the following restrictions apply:
  • ISR platforms must meet the following minimum requirements:
    • 8 GB flash memory
    • 8 GB DRAM

  • When you create a policy for these features, you must specify a target VPN. When you enable these features on a single VPN, the corresponding policy is applied to both traffic from and to the VPN. Note that this is when you specify one VPN and not a comma-separated list of VPNs.
    For example, if you applied the policy to a single VPN, say VPN 3, then the security policy is applied in both the following cases:
    • Traffic from VPN 3 to VPN 2.
    • Traffic from VPN 6 to VPN 3.

  • By default, when a policy is applied to VPN 0 (the global VPN) and enterprise tunnels are in VPN 0, all VPN traffic that uses the enterprise tunnels are not inspected. If you want the traffic of other VPNs to be inspected, you must explicitly specify the VPNs in the policy.
For example, in both the following cases, a VPN 0 security policy does not inspect traffic:

- Traffic originating from a service-side VPN (for example VPN 3) that is transmitted through the enterprise tunnel. This traffic is not inspected because VPN 3 is not explicitly specified in the policy.

- Traffic from the enterprise tunnel that is sent to the service-side VPN (for example VPN 3). This traffic is also not inspected because VPN 3 is not explicitly specified in the policy.

- You can enable these features on service and transport VPNs. This includes VPN 0.

- The VirtualPortGroup interface for data traffic for UTD uses the 192.0.2.0/30 IP address range. The use of the 192.0.2.0/24 subnet is defined in RFC 3330. vManage also automatically uses 192.0.2.1 and 192.0.2.2 for the data virtual private gateway in VPN 0 for UTD. You can modify this using a CLI template on vManage to configure the device. Due to this, you should not use these IP addresses on devices. Alternatively, you can change the routing configuration on the device to use a different IP address from the 192.0.2.0/24 subnet.
CHAPTER 3

Configure Security Parameters

This section describes how to change security parameters for the control plane and the data plane in the Cisco SD-WAN overlay network.

- Configure Control Plane Security Parameters, on page 19
- Configure Data Plane Security Parameters, on page 21
- VPN Interface IPsec, on page 25

Configure Control Plane Security Parameters

By default, the control plane uses DTLS as the protocol that provides privacy on all its tunnels. DTLS runs over UDP.

You can change the control plane security protocol to TLS, which runs over TCP. The primary reason to use TLS is that, if you consider the vSmart controller to be a server, firewalls protect TCP servers better than UDP servers.

You configure the control plane tunnel protocol on a vSmart controller:

vSmart(config)# security control protocol tls

With this change, all control plane tunnels between the vSmart controller and the routers and between the controller and vManage use TLS. Control plane tunnels to vBond orchestrators always use DTLS, because these connections must be handled by UDP.

In a domain with multiple vSmart controllers, when you configure TLS on one of the vSmart controllers, all control plane tunnels from that controller to the other controllers use TLS. Said another way, TLS always takes precedence over DTLS. However, from the perspective of the other vSmart controllers, if you have not configured TLS on them, they use TLS on the control plane tunnel only to that one vSmart controller, and they use DTLS tunnels to all the other vSmart controllers and to all their connected routers. To have all vSmart controllers use TLS, configure it on all of them.

By default, the vSmart controller listens on port 23456 for TLS requests. To change this:

vSmart(config)# security control tls-port number

The port can be a number from 1025 through 65535.

To display control plane security information, use the show control connections command on the vSmart controller. For example:

vSmart-2# show control connections
Configure DTLS on vManage

If you configure the vManage to use TLS as the control plane security protocol, you must enable port forwarding on your NAT. If you are using DTLS as the control plane security protocol, you do not need to do anything.

The number of ports forwarded depends on the number of vdaemon processes running on the vManage. To display information about these processes and about the number of ports that are being forwarded, use the `show control summary` command shows that four vdaemon processes are running:

```
vManage# show control summary
```

<table>
<thead>
<tr>
<th>INSTANCE</th>
<th>VBOND COUNTS</th>
<th>VMANAGE COUNTS</th>
<th>VSMART COUNTS</th>
<th>VEDGE COUNTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

To see the listening ports, use the `show control local-properties` command:
configure data plane security parameters

This output shows that the listening TCP port is 23456. If you are running vManage behind a NAT, you should open the following ports on the NAT device:

- 23456 (base - instance 0 port)
- 23456 + 100 (base + 100)
- 23456 + 200 (base + 200)
- 23456 + 300 (base + 300)

Note that the number of instances is the same as the number of cores you have assigned for the vManage, up to a maximum of 8.

configure allowed authentication types

By default, IPsec tunnel connections use a modified version of the Encapsulating Security Payload (ESP) protocol for authentication. To modify the negotiated authentication types, use the following command:

Device(config)# security ipsec authentication-type (ah-sha1-hmac | ah-no-id | sha1-hmac | )
By default, IPsec tunnel connections use AES-GCM-256, which provides both encryption and authentication. Configure each authentication type with a separate `security ipsec authentication-type` command. The command options map to the following authentication types, which are listed in order from most strong to least strong:

- `ah-sha1-hmac` enables encryption and encapsulation using ESP. However, in addition to the integrity checks on the ESP header and payload, the checks also include the outer IP and UDP headers. Hence, this option supports an integrity check of the packet similar to the Authentication Header (AH) protocol. All integrity and encryption is performed using AES-256-GCM.

- `ah-no-id` enables a mode that is similar to `ah-sha1-hmac`, however the ID field of the outer IP header is ignored. This option accommodates some non-Cisco SD-WAN devices, including the Apple AirPort Express NAT, that have a bug that causes the ID field in the IP header, a non-mutable field, to be modified. Configure the `ah-no-id` option in the list of authentication types to have the Cisco SD-WAN AH software ignore the ID field in the IP header so that the Cisco SD-WAN software can work in conjunction with these devices.

- `sha1-hmac` enables ESP encryption and integrity checking.

For information about which data packet fields are affected by these authentication types, see Data Plane Integrity, on page 13.

Cisco IOS XE SD-WAN devices and Cisco vEdge devices advertise their configured authentication types in their TLOC properties. The two routers on either side of an IPsec tunnel connection negotiate the authentication to use on the connection between them, using the strongest authentication type that is configured on both of the routers. For example, if one router advertises the `ah-sha1-hmac` and `ah-no-id` types, and a second router advertises the `ah-no-id` type, the two routers negotiate to use `ah-no-id` on the IPsec tunnel connection between them. If no common authentication types are configured on the two peers, no IPsec tunnel is established between them.

The encryption algorithm on IPsec tunnel connections is AES-256-GCM.

When the IPsec authentication type is changed, the AES key for the data path is changed.

### Change the Rekeying Timer

Before Cisco IOS XE SD-WAN devices and Cisco vEdge devices can exchange data traffic, they set up a secure authenticated communications channel between them. The routers use IPSec tunnels between them as the channel, and the AES-256 cipher to perform encryption. Each router generates a new AES key for its data path periodically.

By default, a key is valid for 86400 seconds (24 hours), and the timer range is 10 seconds through 1209600 seconds (14 days). To change the rekey timer value:

```bash
Device(config)# security ipsec rekey seconds
```

The configuration looks like this:
If you want to generate new IPsec keys immediately, you can do so without modifying the configuration of the router. To do this, issue the **request platform software sdwan security ipsec-rekey** command on the compromised router.

For example, the following output shows that the local SA has a Security Parameter Index (SPI) of 256:

```
Device# show sdwan ipsec local-sa
```

<table>
<thead>
<tr>
<th>TLOC ADDRESS</th>
<th>TLOC COLOR</th>
<th>SPI</th>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>KEY</th>
<th>HASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.255.15</td>
<td>lte</td>
<td>256</td>
<td>10.1.15.15</td>
<td>12346</td>
<td>*****b93a</td>
<td></td>
</tr>
</tbody>
</table>

A unique key is associated with each SPI. If this key is compromised, use the **request platform software sdwan security ipsec-rekey** command to generate a new key immediately. This command increments the SPI. In our example, the SPI changes to 257 and the key associated with it is now used:

```
Device# request platform software sdwan security ipsec-rekey
Device# show sdwan ipsec local-sa
```

<table>
<thead>
<tr>
<th>TLOC ADDRESS</th>
<th>TLOC COLOR</th>
<th>SPI</th>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>KEY</th>
<th>HASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.255.15</td>
<td>lte</td>
<td>257</td>
<td>10.1.15.15</td>
<td>12346</td>
<td>*****b93a</td>
<td></td>
</tr>
</tbody>
</table>

After the new key is generated, the router sends it immediately to the vSmart(s) using DTLS or TLS. The vSmart(s) send the key to the peer routers. The routers begin using it as soon as they receive it. Note that the key associated with the old SPI (256) will continue to be used for a short period of time, until it times out.

To stop using the old key immediately, issue the **request platform software sdwan security ipsec-rekey** command twice, in quick succession. This sequence of commands removes both SPI 256 and 257 and sets the SPI to 258. The router then uses the associated key of SPI 258. Note, however, that some packets will be dropped for a short period of time, until all the remote routers learn the new key:

```
Device# request platform software sdwan security ipsec-rekey
Device# request platform software sdwan security ipsec-rekey
Device# show sdwan ipsec local-sa
```

<table>
<thead>
<tr>
<th>TLOC ADDRESS</th>
<th>TLOC COLOR</th>
<th>SPI</th>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>KEY</th>
<th>HASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.255.15</td>
<td>lte</td>
<td>258</td>
<td>10.1.15.15</td>
<td>12346</td>
<td>*****b93a</td>
<td></td>
</tr>
</tbody>
</table>

### Change the Size of the Anti-Replay Window

IPsec authentication provides anti-replay protection by assigning a unique sequence number to each packet in a data stream. This sequence numbering protects against an attacker duplicating data packets. With anti-replay protection, the sender assigns monotonically increasing sequence numbers, and the destination checks these sequence numbers to detect duplicates. Because packets often do not arrive in order, the destination maintains a sliding window of sequence numbers that it will accept.
Packets with sequence numbers that fall to the left of the sliding window range are considered old or duplicates, and the destination drops them. The destination tracks the highest sequence number it has received, and adjusts the sliding window when it receives a packet with a higher value.

By default, the sliding window is set to 512 packets. It can be set to any value between 64 and 4096 that is a power of 2 (that is, 64, 128, 256, 512, 1024, 2048, or 4096). To modify the anti-replay window size, use the `replay-window` command, specifying the size of the window:

```
Device(config)# security ipsec replay-window
number
```

The configuration looks like this:

```
security
  ipsec
    replay-window number
  !
```

To help with QoS, separate replay windows are maintained for each of the first eight traffic channels. The configured replay window size is divided by eight for each channel.

If QoS is configured on a router, that router might experience a larger than expected number of packet drops as a result of the IPsec anti-replay mechanism, and many of the packets that are dropped are legitimate ones. This occurs because QoS reorders packets, giving higher-priority packets preferential treatment and delaying lower-priority packets. To minimize or prevent this situation, you can do the following:

- Increase the size of the anti-replay window.
- Engineer traffic onto the first eight traffic channels to ensure that traffic within a channel is not reordered.
VPN Interface IPsec

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65530, except for 512.

Cisco Cisco IOS XE SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE SD-WAN devices through Cisco vManage. In Cisco vManage, the system automatically maps the VPN configurations to VRF configurations.

Create VPN IPsec Interface Template

- **Step 1** From the Cisco vManage menu, select **Configuration > Templates**.
- **Step 2** Click **Feature**.
- **Step 3** Click **Add Template**.
- **Step 4** Select a Cisco IOS XE SD-WAN device from the list.
- **Step 5** From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.
- **Step 6** In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
- **Step 7** In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Changing the Scope for a Parameter Value

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (a ☑), and the default setting or value is shown. To change the default or to enter a value, click the **scope** drop-down to the left of the parameter field and select one of the following:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Icon](emoji) Device Specific | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template.  
When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. Upload the CSV file when you attach a device to a device template.  
To change the default key, type a new string and move the cursor out of the Enter Key box.  
Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
Configure Security Parameters

Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries IKE traffic, select the IPsec tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Rekey Interval</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 hour through 14 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3600 seconds</td>
</tr>
<tr>
<td>IKE Replay Window</td>
<td>64, 128, 256, 512, 1024,</td>
<td>Specify the replay window size for the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>2048, 4096, 8192</td>
<td>Default: 512</td>
</tr>
<tr>
<td>IPsec Cipher Suite</td>
<td>aes256-cbc-sha1</td>
<td>Specify the authentication and encryption to use on</td>
</tr>
<tr>
<td></td>
<td>aes256-gcm</td>
<td>the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>null-sha1</td>
<td>Default: aes256-gcm</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>2 1024-bit modulus</td>
<td>Specify the PFS settings to use on the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>14 2048-bit modulus</td>
<td>Select one of the following Diffie-Hellman prime</td>
</tr>
<tr>
<td></td>
<td>15 3072-bit modulus</td>
<td>modulus groups:</td>
</tr>
<tr>
<td></td>
<td>16 4096-bit modulus</td>
<td>1024-bit – group-2</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>2048-bit – group-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3072-bit – group-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4096-bit – group-16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none – disable PFS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: group-16</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI Equivalent

```
crypto
ipsec
profile ipsec_profile_name
    set ikev2-profile ikev2_profile_name
    set security-association
        lifetime (seconds 120-2592000 | kilobytes disable)
```
replay \{disable | window-size \{64 | 128 | 256 | 512 | 1024 | 4096 | 8192\}\}
set pfs group \{2 | 14 | 15 | 16 | none\}
set transform-set transform_set_name

**Release Information**

Introduced in Cisco vManage for Cisco IOS XE SD-WAN Release 16.11.x.

**Configure Dead-Peer Detection**

To configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable, select the DPD tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD Interval</td>
<td>Specify the interval for IKE to send Hello packets on the connection.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: Disabled</td>
</tr>
<tr>
<td>DPD Retries</td>
<td>Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 60</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**CLI Equivalent**

```
crypto
  ikev2
    profile ikev2_profile_name
      dpd 10-3600 2-60 \{on-demand | periodic\}
```

**Configure IKE**

**Table 2: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256 Support for IPSec Tunnels</td>
<td>Cisco IOS XE Release Amsterdam 17.2.1r</td>
<td>This feature adds support for HMAC_SHA256 algorithms for enhanced security.</td>
</tr>
</tbody>
</table>

To configure IKE, select the **IKE** tab and configure the following parameters:
When you create an IPsec tunnel on a Cisco IOS XE SD-WAN device, IKE Version 1 is enabled by default on the tunnel interface.

**IKE Version 1 and IKE Version 2**

To configure the IPsec tunnel that carries IKEv1 and IKEv2 traffic, select the **IPSEC** tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IKE Version</strong></td>
<td>1 IKEv1</td>
<td>Enter 1 to select IKEv1.</td>
</tr>
<tr>
<td></td>
<td>2 IKEv2</td>
<td>Enter 2 to select IKEv2.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong></td>
<td>IKEv1</td>
</tr>
<tr>
<td><strong>IKE Mode</strong></td>
<td>Aggressive mode</td>
<td>For IKEv1 only, specify one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>Main mode</td>
<td>• Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Establishes an IKE SA session before starting IPsec negotiations.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>For IKEv2, there is no mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong></td>
<td>Main mode</td>
</tr>
<tr>
<td><strong>IPsec Rekey Interval</strong></td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong></td>
<td>1 hour through 14 days</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong></td>
<td>14400 seconds (4 hours)</td>
</tr>
<tr>
<td><strong>IKE Cipher Suite</strong></td>
<td>3DES</td>
<td>Specify the type of authentication and encryption to use during IKE key exchange.</td>
</tr>
<tr>
<td></td>
<td>192-AES</td>
<td><strong>Default:</strong> 256-AES</td>
</tr>
<tr>
<td></td>
<td>256-AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DES</td>
<td></td>
</tr>
<tr>
<td><strong>IKE Diffie-Hellman Group</strong></td>
<td>2 14 15 16</td>
<td>Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1024-bit modulus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2048-bit modulus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3072-bit modulus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4096-bit modulus</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong></td>
<td>4096-bit modulus</td>
</tr>
</tbody>
</table>
Configure IKE

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Authentication</td>
<td>Configure IKE authentication.</td>
<td></td>
</tr>
<tr>
<td>Preshared Key</td>
<td>Enter the password to use with the preshared key.</td>
<td></td>
</tr>
<tr>
<td>IKE ID for Local End Point</td>
<td>If the remote IKE peer requires a local end point identifier, specify it.</td>
<td>Range: 1 through 64 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Tunnel's source IP address</td>
</tr>
<tr>
<td>IKE ID for Remote End Point</td>
<td>If the remote IKE peer requires a remote end point identifier, specify it.</td>
<td>Range: 1 through 64 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Tunnel's destination IP address</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**Change the IKE Version from IKEv1 to IKEv2**

To change the IKE version, do the following:

1. Select the **Basic Configuration** tab.
2. Use the `shutdown` parameter with the `yes` option (`yes shutdown`) to shut down the tunnel.
3. Remove the ISAKMP profile from the IPsec profile.
4. Attach the IKEv2 profile with the IPsec profile.

**Note**

Perform this step if you already have an IKEv2 profile. Otherwise, create an IKEv2 profile first.

5. Use the `shutdown` parameter with the `no` option (`no shutdown`) to start up the tunnel.

**Note**

You must issue the `shutdown` operations in two separate operations.

**CLI Equivalent for Changing the IKE Version**

**Note**

There is no single CLI for changing the IKE version. You need to follow the sequence of steps listed in the Change the IKE Version from IKEv1 to IKEv2 section.

**CLI Equivalents for IKEv1**

**ISAKMP CLI Configuration for IKEv1**
crypto
    isakmp
        keepalive 60-86400 2-60 (on-demand | periodic)
        policy policy_num
            encryption [AES128-CBC-SHA1 | AES256-CBC-SHA1]
            hash [sha384 | sha256 | sha]
            authentication pre-share
            group {2 | 14 | 16 | 19 | 20 | 21}
        lifetime 60-86400
        profile ikev1_profile_name
            match identity address ip_address [mask]
            keyring keyring_name

IPsec CLI Configuration for IKEv1
profile ipsec_profile_name
    set transform-set transform_set_name
    set isakmp-profile ikev1_profile_name
    set security-association
        lifetime {kilobytes disable | seconds 120-2592000}
        replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
    set pfs group {14 | 16 | 19 | 20 | 21}
    keyring keyring_name
    pre-shared-key address ip_address [mask] key key_string
    ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac | esp-sha256-hmac] mode tunnel

Summary Steps
1. enable
2. configure terminal
3. crypto isakmp policy priority
4. encryption {des | 3des | aes | aes 192 | aes 256 }
5. hash {sha | sha256 | sha384 | md5 }
6. authentication {rsa-sig | rsa-encr | pre-share }
7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime seconds
9. exit
10. exit

CLI Equivalent for IKE2
crypto
    ikev2
        proposal proposal_name
            encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
            integrity {sha256 | sha384 | sha512}
            group {2 | 14 | 15 | 16}
        keyring idev2_keyring_name
        peer peer_name
            address tunnel_dest_ip [mask]
            pre-shared-key key key_string
        profile ikev2_profile_name
match identity remote address ip_address
authentication {remote | local} pre-share
keyring local ikev2_keyring_name
lifetime 120-86400
Enterprise Firewall with Application Awareness

Cisco’s Enterprise Firewall with Application Awareness feature uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

- Overview of Enterprise Firewall with Application Awareness, on page 33
- Configure Firewall Policies, on page 34
- Zone-Based Firewall Configuration Examples, on page 40
- Firewall High-Speed Logging, on page 43

Overview of Enterprise Firewall with Application Awareness

The Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

Zone configuration consists of the following components:

- Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- Firewall policy—a security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.
- Zone pair—a container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Matching flows that are accepted can be processed in two different ways:

- Inspect—The packet's header can be inspected to determine its source address and port.
**Configure Firewall Policies**

In Cisco vManage, you configure firewall policies from the **Configuration > Security** screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the router.
General Cisco vManage Configuration Procedure

To configure firewall policies, use the policy configuration wizard. The wizard is a UI policy builder that lets you configure policy components:

- **Create Lists**—Create lists that group together related items and that you call in the match condition of a firewall policy.
- **Firewall Policy**—Define the match and action conditions of the firewall policy.
- **Apply Configuration**—Define zone pairs.

You must configure all these components to create a firewall policy. If you are modifying an existing firewall, you can skip a component by clicking the **Next** button at the bottom of the screen. To return to a component, click the **Back** button at the bottom of the screen.

Create or Modify Lists

Create Lists

You create lists that group together related items and that you call in the match condition of a firewall policy. To create lists:

1. In vManage NMS, select the **Configure > Security** screen.
2. In the Title bar, click the **Custom Options** drop-down.
3. Select **Lists**. The Define Lists screen displays.
4. Select the list type to create. The following table describes the lists you can create for firewall policies.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>1. In the left pane, click <strong>Application</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>New Application List</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. Select individual applications or application families.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Data Prefix</td>
<td>1. In the left pane, click <strong>Data Prefix</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>New Data Prefix List</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. Enter one or more IP prefixes.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>
Use the Policy Configuration Wizard

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Zones     | 1. In the left pane, click Zones.  
            2. Click New Zone List.  
            3. Enter a name for the zone list.  
            4. In the Add VPN field, enter the number or numbers of the VPN in the zone. Separate numbers with commas.  
            5. Click Add. |

You can edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.

Use the Policy Configuration Wizard

**Table 3: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall FQDN Support</td>
<td>Cisco IOS XE Release Amsterdam 17.2.1r</td>
<td>This enhancement adds support to define a firewall policy using fully qualified domain names (FQDN), rather than only IP addresses. One advantage of using FQDNs is that they account for changes in the IP addresses assigned to the FQDN if that changes in the future.</td>
</tr>
</tbody>
</table>

This article provides procedures for configuring firewall policies on Cisco vManage to provision firewall policies to direct traffic between two zones, which are referred to as a source zone and a destination zone. Each zone consists of one or more VPNs in the overlay network.

In vManage NMS, you configure firewall policies from the Configuration > Security screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the XE SD-WAN Router.

**Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In vManage NMS, select the Configure > Security screen.
2. Click Add Security Policy.

The Add Security Policy configuration wizard opens, and various use-case scenarios display.

**Select a Use-Case Scenario**

In Add Security Policy, select a policy based on use-case scenarios, or build your own custom policy.

1. Select a security policy use-case scenario. The following table describes the use-case scenarios.
   - Compliance – Applies application firewall and intrusion prevention.
   - Guest Access – Applies application firewall and URL filtering.
   - Direct Cloud Access – Applies application firewall, URL filtering, and DNS Umbrella security.
• Direct Internet Access – Applies application firewall, intrusion prevention, URL filtering, and DNS Umbrella security.

• Custom – Build your own security policy by combining various security policy blocks.

2. Click **Proceed** to add a firewall policy in the wizard.

**Configure Firewall Policy**

**Notes**

• In the Cisco IOS XE Amsterdam 17.2 release, this procedure was updated to accommodate new functionality.

• The FQDN intended use is for matching standalone servers in data centers or a private cloud. When matching public URLs, the recommended match action is 'drop'. If you use 'inspect' for public URLs, you must define all related sub-urls/redirect-urls under the FQDN pattern.

**Limitations**

• Maximum number of fully qualified domain name (FQDN) patterns supported for a rule under firewall policy: 64

• Maximum number of entries for FQDN to IP mapping supported in the database: 5000

• If a firewall policy uses an FQDN in a rule, the policy must explicitly allow DNS packets, or resolution will fail.

• Firewall policy does not support mapping multiple FQDN's to a single IP.

• Only two forms of FQDN are supported: full name or a name beginning with an asterisk (*) wildcard.

  Example: *.cisco.com

1. Select **Configuration > Security**.

2. Click **Add Policy**. The zone-based firewall configuration wizard opens.

3. Click the **Add Firewall Policy** drop-down.

4. To create a new firewall policy
   a. Select **Create New**.
   b. Enter a name and description for the policy.
   c. Go to Step 4.

5. To import an existing zone-based firewall policy:
   a. Select **Copy from Existing**. The Copy from Existing Firewall Policy dialog box appears.
   b. From the Policy drop-down, select the policy to copy.
   c. In the Policy Name field, accept the default name (*policy_name_copy*) or enter a new name.
   d. In the Policy Description field, enter a description.
   e. Click **Copy**.
f. To modify the policy, click the **More Actions** icon to at the far right of the policy and select **Edit**. Go to Step 4.

6. Click **Add Rule**. In the **New Firewall Rule** window, enter a rule name and configure one or more of the following.

   **Note**
   
   For some options, it is possible to enter a defined list as a value, or to define a list from within the window.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Data Prefix</td>
<td>IPv4 prefixes and/or domain names (FQDN)</td>
</tr>
<tr>
<td>Source Port</td>
<td>Source ports</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>IPv4 prefixes and/or domain names (FQDN)</td>
</tr>
<tr>
<td>Destination Ports</td>
<td>Destination port</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol: select from a list, or enter a protocol.</td>
</tr>
<tr>
<td>Application List</td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you selected an Application or Application Family List, you must select at least one other match condition.</td>
</tr>
</tbody>
</table>

7. Set the Action for the rule as **Inspect**, **Pass**, or **Drop**.

8. Click **Save** to save the rule.

9. (Optional) Add additional rules.

10. Click **Save Firewall Policy**.

### Apply Policy to a Zone Pair

**Table 4: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self zone policy for Zone-Based</td>
<td>Cisco IOS XE SD-WAN Release 16.12.1b</td>
<td>This feature can help define policies to impose rules on incoming and outgoing traffic.</td>
</tr>
<tr>
<td>Firewalls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. At the top of the page, click **Apply Zone-Pairs**.

2. In the Source Zone field, select the zone that is the source of the data packets.

3. In the Destination Zone field, select the zone that is the destination of the data packets.
You can select the same zone for both source and destination. However, if the packet's source and destination use the same physical interface (resulting in U-turn traffic), a firewall session is not created and traffic passes.

4. Click the plus (+) icon to add zone pairs.

5. Click **Save**.

6. At the bottom of the page, click **Save Firewall Policy** to save the policy.

7. To edit or delete a firewall policy, in the right pane, click the **More Actions** icon to the far right of the policy and select the desired option.

8. Click **Next** to configure the next security block in the wizard or to proceed to the Policy Summary page.

**Policy Summary**

1. Enter a name for the security policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. Enter a description for the security policy. This field is mandatory.

3. (Optional) For Cisco IOS XE SD-WAN Release 16.12.x and onwards, to configure high-speed logging (HSL), enter the following details of the Netflow server that will listen for the Netflow event logs:

   a. In the VPN field, enter the VPN that the server is in.

   b. In the Server IP field, enter the IP address of the server.

   c. In the Port field, enter the port on which the server is listening.

4. If you configured an application firewall policy, uncheck the “Bypass firewall policy and allow all Internet traffic to/from VPN 0” check box in the Additional Security Policy Settings area.

5. (Optional) To prevent TCP SYN-flooding attacks that are a type of denial-of-service (DoS) attack, do the following:

   a. Enable the **TCP SYN Flood Limit** option.

   b. Specify a limit of the number of half-opened TCP sessions.

6. (Optional) To configure an audit trail, enable the Audit Trail option. This option is only applicable for rules with an Inspect action.

7. Click **Save Policy** to save the security policy.

For more information on HSL, see **Firewall High-Speed Logging Overview, on page 44.**
Apply a Security Policy to a Device

To apply a security policy to a device:

1. In vManage, select the **Configuration > Templates** screen.

2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template**.

3. From the **Device Model** drop-down, select one of the devices.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.

5. From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.

6. Click **Create** to apply the security policy to a device.

Zone-Based Firewall Configuration Examples

This topic provides an example of configuring a simple zone-based firewall using the CLI or vManage.
Setting Up an Inspection Firewall Policy

In this zone-based firewall configuration example, we have a scenario where a router is connected to an employee network and the internet.

We want to set up a firewall between the employee network and the internet to do the following:

- Enable stateful packet inspection for traffic between the employee network and the internet
- Log all packets dropped by the firewall
- Set Denial-of-Service thresholds
- Enable the following firewall rule:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP and UDP</td>
<td>10.0.0.1</td>
<td>200</td>
<td>209.165.200.225</td>
<td>300</td>
<td>drop</td>
</tr>
<tr>
<td></td>
<td>172.16.0.1</td>
<td></td>
<td>209.165.202.129</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>192.168.0.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>255.255.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The configuration consists of three sections:

- Define the zones.
- Define a firewall policy.
- Define the zone pair.
- Apply the zone-based firewall policy to the zone pair.

CLI Configuration

1. Enable privileged EXEC mode. If prompted, enter your password.
   
   Device> enable

2. Enter global configuration mode:
   
   configure transaction

3. Create the inspect parameter map:
   
   Device(config)# parameter-map type inspect-global
   multi-tenancy
   vpn zone security
   alert on
   log dropped-packets
   tcp syn-flood limit 2000
   max-incomplete tcp 2000

4. Create the employee zone:
   
   Device(config)# zone security employee
   vpn 1

5. Create the internet zone:
Device(config)# zone security internet
   vpn 0

6. Configure the object group for the source addresses:
Device(config)# object-group network employee_1
   host 10.0.0.1
   host 172.16.0.1
   192.168.0.1 255.255.0.0

7. Configure the object group for the destination addresses:
Device(config)# object-group network internet_1
   host 209.165.200.225
   host 209.165.202.129

8. Configure the object group for the ports:
Device(config)# object-group network svc
   tcp source eq 200 eq 300
   udp source eq 200 eq 300

9. Create the IP access-list:
Device(config)# ip access-list ext acl_1
   10 deny object-group svc object-group employee_1 object-group internet_1

10. Create the class map:
Device(config)# class-map type inspect match-all cmap_1
    match access-group name acl_1

11. Create the policy map that you want to add to the zone pair.
Device(config)# policy-map type inspect fw_policy1
    class cmap_1
    drop

12. Create the zone pair and link the policy map to it:
Device(config)# zone-pair security employee-inet source employee
destination internet
   service-policy type drop fw_policy1

vManage Configuration
To configure this zone-based firewall policy in vManage NMS:

2. Click Add Policy. The zone-based firewall configuration wizard opens.

Configure data prefix groups and zones in the Create Groups of Interest screen:
1. In the left pane, select Data Prefix.

2. In the right pane, click New Data Prefix List.

3. Enter a name for the list.

4. Enter the data prefix or prefixes to include in the list.

5. Click Add.

Configure zones in the Create Groups of Interest screen:
1. In the left pane, select **Zones**.
2. In the right pane, click **New Zone List**.
3. Enter a name for the list.
4. Enter the number of the zone or zones to include in the list. Separate numbers with a comma.
5. Click **Add**.
6. Click **Next** to move to Zone-Based Firewall in the zone-based firewall configuration wizard.

Configure zone-based firewall policies:

1. Click **Add Configuration**, and select **Create New**.
2. Enter a name and description for the policy.
3. In the left pane, click **Add Sequence**.
4. In the right pane, click **Add Sequence Rule**.
5. Select the desired match and action conditions.
6. Click **Same Match and Actions**.
7. In the left pane, click **Default Action**.
8. Select the desired default action.
9. Click **Save Zone-Based Policy**.

Click **Next** to move to the Apply Configuration in the zone-based firewall configuration wizard.

1. Enter a name and description for the zone-based firewall zone pair.
2. Click **Add Zone Pair**.
3. In the Source Zone drop-down, select the zone from which data traffic originates.
4. In the Destination Zone drop-down, select the zone to which data traffic is sent.
5. Click **Add**.
6. Click **Save Policy**. The **Configuration > Security** screen is then displayed, and the zone-based firewalls table includes the newly created policy.

**Firewall High-Speed Logging**

The Firewall High-Speed Logging feature supports the high-speed logging (HSL) of firewall messages by using NetFlow Version 9 as the export format.
Information About Firewall High-Speed Logging

Firewall High-Speed Logging Overview

Zone-based firewalls support high-speed logging (HSL). When HSL is configured, a firewall provides a log of packets that flow through routing devices (similar to the NetFlow Version 9 records) to an external collector. Records are sent when sessions are created and destroyed. Session records contain the full 5-tuple information (the source IP address, destination IP address, source port, destination port, and protocol). A tuple is an ordered list of elements.

HSL allows a firewall to log records with minimum impact to packet processing. The firewall uses buffered mode for HSL. In buffered mode, a firewall logs records directly to the high-speed logger buffer, and exports of packets separately.

A firewall logs the following types of events:

- Audit—Session creation and removal notifications.
- Alert—Half-open and maximum-open TCP session notifications.
- Drop—Packet-drop notifications.
- Pass—Packet-pass (based on the configured rate limit) notifications.
- Summary—Policy-drop and pass-summary notifications.

The NetFlow collector issues the `show platform software interface F0 brief` command to map the FW_SRC_INTF_ID and FW_DST_INTF_ID interface IDs to the interface name.

The following sample output from the `show platform software interface F0 brief` command shows that the ID column maps the interface ID to the interface name (Name column):

```
Device# show platform software interface F0 brief
Name     ID QFP_ID
GigabitEthernet0/2/0  16  9
GigabitEthernet0/2/1  17  10
GigabitEthernet0/2/2  18  11
GigabitEthernet0/2/3  19  12
```

Restrictions

- HSL is supported only on NetFlow Version 9 template.
- HSL is supported only on IPv4 destination and source IP addresses. IPv6 addresses are not supported.
- HSL supports only one HSL destination.

### NetFlow Field ID Descriptions

The following table lists NetFlow field IDs used within the firewall NetFlow templates:

**Table 6: NetFlow Field IDs**

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetFlow ID Fields (Layer 3 IPv4)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW_SRC_ADDR_IPV4</td>
<td>8</td>
<td>4</td>
<td>Source IPv4 address</td>
</tr>
<tr>
<td>FW_DST_ADDR_IPV4</td>
<td>12</td>
<td>4</td>
<td>Destination IPv4 address</td>
</tr>
<tr>
<td>FW_SRC_ADDR_IPV6</td>
<td>27</td>
<td>16</td>
<td>Source IPv6 address</td>
</tr>
<tr>
<td>FW_DST_ADDR_IPV6</td>
<td>28</td>
<td>16</td>
<td>Destination IPv6 address</td>
</tr>
<tr>
<td>FW_PROTOCOL</td>
<td>4</td>
<td>1</td>
<td>IP protocol value</td>
</tr>
<tr>
<td>FW_IPV4_IDENT</td>
<td>54</td>
<td>4</td>
<td>IPv4 identification</td>
</tr>
<tr>
<td>FW_IP_PROTOCOL_VERSION</td>
<td>60</td>
<td>1</td>
<td>IP protocol version</td>
</tr>
<tr>
<td><strong>Flow ID Fields (Layer 4)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW_TCP_FLAGS</td>
<td>6</td>
<td>1</td>
<td>TCP flags</td>
</tr>
<tr>
<td>FW_SRC_PORT</td>
<td>7</td>
<td>2</td>
<td>Source port</td>
</tr>
<tr>
<td>FW_DST_PORT</td>
<td>11</td>
<td>2</td>
<td>Destination port</td>
</tr>
<tr>
<td>FW_ICMP_TYPE</td>
<td>176</td>
<td>1</td>
<td>ICMP (^1) type value</td>
</tr>
<tr>
<td>FW_ICMP_CODE</td>
<td>177</td>
<td>1</td>
<td>ICMP code value</td>
</tr>
<tr>
<td>FW_ICMP_IPV6_TYPE</td>
<td>178</td>
<td>1</td>
<td>ICMP Version 6 (ICMPv6) type value</td>
</tr>
<tr>
<td>FW_ICMP_IPV6_CODE</td>
<td>179</td>
<td>1</td>
<td>ICMPv6 code value</td>
</tr>
<tr>
<td>FW_TCP_SEQ</td>
<td>184</td>
<td>4</td>
<td>TCP sequence number</td>
</tr>
<tr>
<td>FW_TCP_ACK</td>
<td>185</td>
<td>4</td>
<td>TCP acknowledgment number</td>
</tr>
<tr>
<td><strong>Flow ID Fields (Layer 7)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW_L7_PROTOCOL_ID</td>
<td>95</td>
<td>2</td>
<td>Layer 7 protocol ID. Identifies the Layer 7 application classification used by firewall inspection. Normal records use 2 bytes, but optional records use 4 bytes.</td>
</tr>
</tbody>
</table>

**Flow Name Fields (Layer 7)**
<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW_FIELD_L7_PROTOCOL_NAME</td>
<td>96</td>
<td>32</td>
<td>Layer 7 protocol name. Identifies the Layer 7 protocol name that corresponds to the Layer 7 protocol ID (FW_L7_PROTOCOL_ID).</td>
</tr>
</tbody>
</table>

### Flow ID Fields (Interface)

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_SRC_INTF_ID</td>
<td>10</td>
<td>2</td>
<td>Ingress SNMP ifIndex</td>
</tr>
<tr>
<td>FW_DST_INTF_ID</td>
<td>14</td>
<td>2</td>
<td>Egress SNMP ifIndex</td>
</tr>
<tr>
<td>FW_SRC_VRF_ID</td>
<td>234</td>
<td>4</td>
<td>Ingress (initiator) VRF ID</td>
</tr>
<tr>
<td>FW_DST_VRF_ID</td>
<td>235</td>
<td>4</td>
<td>Egress (responder) VRF ID</td>
</tr>
<tr>
<td>FW_VRF_NAME</td>
<td>236</td>
<td>32</td>
<td>VRF name</td>
</tr>
</tbody>
</table>

### Mapped Flow ID Fields (Network Address Translation)

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_XLATE_SRC_ADDR_IPV4</td>
<td>225</td>
<td>4</td>
<td>Mapped source IPv4 address</td>
</tr>
<tr>
<td>FW_XLATE_DST_ADDR_IPV4</td>
<td>226</td>
<td>4</td>
<td>Mapped destination IPv4 address</td>
</tr>
<tr>
<td>FW_XLATE_SRC_PORT</td>
<td>227</td>
<td>2</td>
<td>Mapped source port</td>
</tr>
<tr>
<td>FW_XLATE_DST_PORT</td>
<td>228</td>
<td>2</td>
<td>Mapped destination port</td>
</tr>
</tbody>
</table>

### Status and Event Fields

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
</table>
| FW_EVENT | 233 | 1 | High level event codes  
  - 0—Ignores (invalid)  
  - 1—Flow created  
  - 2—Flow deleted  
  - 3—Flow denied  
  - 4—Flow alert |
| FW_EXT_EVENT | 35,001 | 2 | Extended event code. For normal records the length is 2 byte, and 4 byte for optional records. |

### Timestamp and Statistics Fields

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_EVENT_TIME_MSEC</td>
<td>323</td>
<td>8</td>
<td>Time, in milliseconds, (time since 0000 hours UTC January 1, 1970) when the event occurred (if the event is a microevent, use 324 and 325, if it is a nanosecond)</td>
</tr>
</tbody>
</table>
### NetFlow Field ID Descriptions

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_INITIATOR_OCTETS</td>
<td>231</td>
<td>4</td>
<td>Total number of Layer 4 payload bytes in the packet flow that arrives from the initiator</td>
</tr>
<tr>
<td>FW_RESPONDER_OCTETS</td>
<td>232</td>
<td>4</td>
<td>Total number of Layer 4 payload bytes in the packet flow that arrives from the responder</td>
</tr>
</tbody>
</table>

#### AAA Fields

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_USERNAME</td>
<td>40,000</td>
<td>20 or 64 depending on the template</td>
<td>AAA user name</td>
</tr>
<tr>
<td>FW_USERNAME_MAX</td>
<td>40,000</td>
<td>64</td>
<td>AAA user name of the maximum permitted size</td>
</tr>
</tbody>
</table>

#### Alert Fields

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_HALFOPEN_CNT</td>
<td>35,012</td>
<td>4</td>
<td>Half-open session entry count</td>
</tr>
<tr>
<td>FW_BLACKOUT_SECS</td>
<td>35,004</td>
<td>4</td>
<td>Time, in seconds, when the destination is shutdown or unavailable</td>
</tr>
<tr>
<td>FW_HALFOPEN_HIGH</td>
<td>35,005</td>
<td>4</td>
<td>Configured maximum rate of TCP half-open session entries logged in one minute</td>
</tr>
<tr>
<td>FW_HALFOPEN_RATE</td>
<td>35,006</td>
<td>4</td>
<td>Current rate of TCP half-open session entries logged in one minute</td>
</tr>
<tr>
<td>FW_MAX_SESSIONS</td>
<td>35,008</td>
<td>4</td>
<td>Maximum number of sessions allowed for this zone pair or class ID</td>
</tr>
</tbody>
</table>

#### Miscellaneous

<table>
<thead>
<tr>
<th>Field ID</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_ZONEPAIR_ID</td>
<td>35,007</td>
<td>4</td>
<td>Zone pair ID</td>
</tr>
<tr>
<td>FW_CLASS_ID</td>
<td>51</td>
<td>4</td>
<td>Class ID</td>
</tr>
<tr>
<td>FW_ZONEPAIR_NAME</td>
<td>35,009</td>
<td>64</td>
<td>Zone pair name</td>
</tr>
<tr>
<td>FW_CLASS_NAME</td>
<td>100</td>
<td>64</td>
<td>Class name</td>
</tr>
<tr>
<td>FW_EXT_EVENT_DESC</td>
<td>35,010</td>
<td>32</td>
<td>Extended event description</td>
</tr>
<tr>
<td>FLOW_FIELD_CTS_SRC_GROUP_TAG</td>
<td>34000</td>
<td>2</td>
<td>Cisco Trustsec source tag</td>
</tr>
<tr>
<td>FW_SUMMARY_PKT_CNT</td>
<td>35,011</td>
<td>4</td>
<td>Number of packets represented by the drop/pass summary record</td>
</tr>
<tr>
<td>Field ID</td>
<td>Type</td>
<td>Length</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FW_EVENT_LEVEL</td>
<td>33003</td>
<td>4</td>
<td>Defines the level of the logged event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x01—Per box</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x02—VRF</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x03—Zone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0x04—Class map</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Other values are undefined</td>
</tr>
<tr>
<td>FW_EVENT_LEVEL_ID</td>
<td>33,004</td>
<td>4</td>
<td>Defines the identifier for the FW_EVENT_LEVEL field</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If FW_EVENT_LEVEL is 0x02 (VRF), this field represents VRF_ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If FW_EVENT_LEVEL is 0x03 (zone), this field represents ZONE_ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If FW_EVENT_LEVEL is 0x04 (class map), this field represents CLASS_ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• In all other cases the field ID will be 0 (zero). If FW_EVENT_LEVEL is not present, the value of this field must be zero.</td>
</tr>
<tr>
<td>FW_CONFIGURED_VALUE</td>
<td>33,005</td>
<td>4</td>
<td>Value that represents the configured half-open, aggressive-aging, and event-rate monitoring limit. The interpretation of this field value depends on the associated FW_EXT_EVENT field.</td>
</tr>
<tr>
<td>FW_ERM_EXT_EVENT</td>
<td>33,006</td>
<td>2</td>
<td>Extended event-rate monitoring code</td>
</tr>
<tr>
<td>FW_ERM_EXT_EVENT_DESC</td>
<td>33,007</td>
<td>N (string)</td>
<td>Extended event-rate monitoring event description string</td>
</tr>
</tbody>
</table>

1 Internet Control Message Protocol  
2 Simple Network Management Protocol  
3 virtual routing and forwarding  
4 Coordinated Universal Time  
5 Authentication, Authorization, and Accounting

**HSL Messages**

The following are sample syslog messages from Cisco SD-WAN IOS XE Router:
### Table 7: Syslog Messages and Their Templates

<table>
<thead>
<tr>
<th>Message Identifier</th>
<th>Message Description</th>
<th>HSL Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW-6-DROP_PKT</td>
<td>Dropping %s pkt from %s %CA:%u =&gt; %CA:%u (target:class)-(%s;%s) %s %s with ip ident %u %s %s Explanation: Packet dropped by firewall inspection. %s: tcp/udp/icmp/unknown prot/L7 prot %s: interface %s:%u ip/ip6 addr: port %s:%s: zone pair name/ class name %s &quot;due to&quot; %s: fw_ext_event name %u ip ident %s: if tcp, tcp seq/ack number and tcp flags %s: username</td>
<td>FW_TEMPLATE_DROP_V4 or FW_TEMPLATE_DROP_V6</td>
</tr>
</tbody>
</table>
### HSL Messages

<table>
<thead>
<tr>
<th>Message Identifier</th>
<th>Message Description</th>
<th>HSL Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW6SESS_AUDIT_TRAIL_START</td>
<td>(target:class)-(:%s:%s):Start %s session: initiator (%CA:%u) -- responder (%CA:%u) from %s %s</td>
<td>FW_TEMPLATE_START_AUDIT_V4 or FW_TEMPLATE_START_AUDIT_V6</td>
</tr>
</tbody>
</table>

Explanation: Start of an inspection session. This message is issued at the start of each inspection session and it records the source/destination addresses and ports.

- %s:%s: zonepair name: class name
- %s: l4/l7 protocolname
- %CA:%u ip/ip6 addr: port
- %s: interface
- %s: username
- %s: TODO

Actual log:

```
*Jan 21 20:13:01.078: %IOSXE-6-PLATFORM:F0: cpp_cp:CPP:00Thread:125 TS:0000010570290947309 %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session: initiator (10.1.1.1:43365) -- responder (10.3.21.1:23) from FastEthernet0/1/0
```
<table>
<thead>
<tr>
<th>Message Identifier</th>
<th>Message Description</th>
<th>HSL Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW-6-SESS_AUDIT_TRAIL</td>
<td>(target:class)-(%s:%s):Stop %s session: initiator (%CA:%u) sent %u bytes -- responder (%CA:%u) sent %u bytes, from %s %s</td>
<td>FW_TEMPLATE_STOP_AUDIT_V4 or FW_TEMPLATE_STOP_AUDIT_V6</td>
</tr>
</tbody>
</table>

Explanation: Per-session transaction log of network activities. This message is issued at the end of each inspection session, and it records the source/destination addresses and ports, and the number of bytes transmitted by the client and the server.

- %s:%s: zonepair name: class name
- %s: l4/l7 protocolname
- %CA:%u ip/ip6 addr: port
- %u bytes counters
- %s: interface
- %s: TODO

Actual log:
*Jan 21 20:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP-00 Thread:036 TS:0000010585102587819 %FW-6-SESS_AUDIT_TRAIL: Stop tcp session: initiator (10.1.1.1:43365) sent 35 bytes -- responder (11.1.1.1:23) sent 95 bytes, from FastEthernet0/1/0
<table>
<thead>
<tr>
<th>Message Identifier</th>
<th>Message Description</th>
<th>HSL Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW-4-UNBLOCK_HOST</td>
<td>(target:class)-(%s:%s): New TCP connections to host %CA no longer blocked</td>
<td>FW TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW TEMPLATE ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW EXT ALERT_UNBLOCK_HOST</td>
</tr>
<tr>
<td>Type: Warning</td>
<td>Explanation: New TCP connection attempts to the specified host are no longer blocked. This message indicates that the blocking of new TCP connection attempts to the specified host has been removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>%s: zonepair name: class name %CA: ip/ip6 addr</td>
<td></td>
</tr>
<tr>
<td>FW-4-HOST_TCP_ALERT_ON</td>
<td>&quot;(target:class)-(%s:%s): Max tcp half-open connections (%u) exceeded for host %CA.</td>
<td>FW TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW TEMPLATE ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW EXT ALERT HOST_TCP_ALERT_ON</td>
</tr>
<tr>
<td>Type: Warning</td>
<td>Explanation: Exceeded the max-incomplete host limit for half-open TCP connections. This message indicates that a high number of half-open connections is coming to a protected server, and this may indicate that a SYN flood attack is in progress.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>%s: zonepair name: class name %u: half open cnt %CA: ip/ip6 addr</td>
<td></td>
</tr>
<tr>
<td>Message Identifier</td>
<td>Message Description</td>
<td>HSL Template</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>FW-2- BLOCK_HOST</td>
<td>Blocking new TCP connections to host %CA for %u minute %s (half-open count %u exceeded). Explanation: Exceeded the max-incomplete host threshold for TCP connections. Any subsequent new TCP connection attempts to the specified host is denied, and the blocking option is configured to block all subsequent new connections. The blocking will be removed when the configured block time expires. %s:%s: zonepair name: class name %CA: ip/ip6 addr %u blockout min %s: s if &gt; 1 min blockout time %u: half open counter</td>
<td>FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_eventid: FW_EXT_ALERT_BLOCK_HOST</td>
</tr>
<tr>
<td>FW-4-ALERT_ON</td>
<td>count (%u/%u) current rate: %u Explanation: Either the max-incomplete high threshold of half-open connections or the new connection initiation rate has been exceeded. This error message indicates that an unusually high rate of new connections is coming through the firewall, and a DOS attack may be in progress. This message is issued only when the max-incomplete high threshold is crossed. %s:%s: zonepair name: class name %s: &quot;getting aggressive&quot; %u/%u halfopen cnt/high %u: current rate</td>
<td>FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6 with fw_ext_event_id: FW_EXT_SESS_RATE_ALERT_ON</td>
</tr>
<tr>
<td>Message Identifier</td>
<td>Message Description</td>
<td>HSL Template</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| FW-4-ALERT_OFF            | (target:class)-(%s:%s):%s, count (%u+%u) current rate: %u
Explanation: Either the number of half-open connections or the new connection initiation rate has gone below the max-incomplete low threshold. This message indicates that the rate of incoming new connections has slowed down and new connections are issued only when the max-incomplete low threshold is crossed.
%s:%s: zonpair name: class name
%s: "calming down"
%u/%u halfopen cnt/high
%u: current rate                                                                                     | FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6 with fw_ext_event_id FW_EXT_SESS_RATE_ALERT_OFF |
| FW-4-SESSIONS_MAXIMUM     | Number of sessions for the firewall policy on "(target:class)-(%s:%s) exceeds the configured sessions maximum value %u
Explanation: The number of established sessions have crossed the configured sessions maximum limit.
%s:%s: zonpair name: class name
%u: max session                                                                                     | FW_TEMPLATE_ALERT_MAX_SESSION                                                                                                                        |
<table>
<thead>
<tr>
<th>Message Identifier</th>
<th>Message Description</th>
<th>HSL Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW-6-PASS_PKT</td>
<td>Passing %s pkt from %s %CA:%u =&gt; %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u</td>
<td>FW_TEMPLATE_PASS_V4 or FW_TEMPLATE_PASS_V6</td>
</tr>
<tr>
<td></td>
<td>Explanation: Packet is passed by firewall inspection. %s: tcp/udp/icmp/unknown prot %s: interface %CA:%u src ip/ip6 addr: port %CA:%u dst ip/ip6 addr: port %s:%s: zonepair name: class name %s %s: &quot;due to&quot;, &quot;PASS action found in policy-map&quot; %u: ip ident</td>
<td></td>
</tr>
<tr>
<td>FW-6-LOG_SUMMARY</td>
<td>%u packet%s %s from %s %CA:%u =&gt; %CA:%u (target:class)-(%s:%s) %s %s: &quot;dropped&quot;/ &quot;passed&quot; %s: interface %CA:%u src ip/ip6 addr: port %CA:%u dst ip/ip6 addr: port %s:%s: zonepair name: class name %s: username</td>
<td>FW_TEMPLATE_SUMMARY_V4 or FW_TEMPLATE_SUMMARY_V6 with FW_EVENT: 3 - drop 4 - pass</td>
</tr>
</tbody>
</table>

**How to Configure Firewall High-Speed Logging**

**Enabling Firewall High-Speed Logging Using vManage**

To enable Firewall High-Speed Logging using vManage, follow the standard firewall vManage flow. In the Policy Summary screen, you will see an option to enable Firewall High-Speed Logging. For more information, see Use the Policy Configuration Wizard, on page 36.
Enabling High-Speed Logging for Global Parameter Maps

By default, high-speed logging (HSL) is not enabled and firewall logs are sent to a logger buffer located in the Route Processor (RP) or the console. When HSL is enabled, logs are sent to an off-box, high-speed log collector. Parameter maps provide a means of performing actions on the traffic that reaches a firewall and a global parameter map applies to the entire firewall session table. Perform this task to enable high-speed logging for global parameter maps.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `parameter-map type inspect-global`
4. `log dropped-packets`
5. `log flow-export v9 udp destination ip-address port-number vrf vrf-label`
6. `log flow-export template timeout-rate seconds`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>parameter-map type inspect-global</code></td>
<td>Configures a global parameter map and enters parameter-map type inspect configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# parameter-map type inspect-global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>log dropped-packets</code></td>
<td>Enables dropped-packet logging.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-profile)# log dropped-packets</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>log flow-export v9 udp destination ip-address port-number vrf vrf-label</code></td>
<td>Enables NetFlow event logging and provides the IP address and the port number of the log collector. UDP destination and port correspond to the IP address and port on which the netflow server is listening for incoming packets.</td>
</tr>
<tr>
<td><strong>Example:</strong> cEdge(config-profile)# log flow-export v9 udp destination 10.20.25.18 2055 vrf 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>log flow-export template timeout-rate seconds</code></td>
<td>Template timeout-rate is the interval (in seconds) at which the netflow template formats are advertised.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-profile)# log flow-export template timeout-rate 5000</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling High-Speed Logging for Firewall Actions

Perform this task enable high-speed logging if you have configured inspect-type parameter maps. Parameter maps specify inspection behavior for the firewall and inspection parameter-maps for the firewall are configured as the inspect type.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. parameter-map type inspect parameter-map-name
4. audit-trail on
5. one-minute \{low number-of-connections | high number-of-connections\}
6. tcp max-incomplete host threshold
7. exit
8. policy-map type inspect policy-map-name
9. class type inspect class-map-name
10. inspect parameter-map-name
11. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
    enable
    Example:
    Device> enable | Enables privileged EXEC mode.
    Enter your password if prompted. |
| **Step 2**
    configure terminal
    Example:
    Device# configure terminal | Enters global configuration mode. |
| **Step 3**
    parameter-map type inspect parameter-map-name
    Example:
    Device(config)# parameter-map type inspect parameter-map-hsl | Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect keyword, and enters parameter-map type inspect configuration mode. |
| **Step 4**
    audit-trail on
    Example:
    Device(config-profile)# audit-trail on | Enables audit trail messages. You can enable audit-trail to a parameter map to record the start, stop, and duration of a connection or session, and the source and destination IP addresses. |
### Configuration Examples for Firewall High-Speed Logging

#### Example: Enabling High-Speed Logging for Global Parameter Maps

The following example shows how to enable logging of dropped packets, and to log error messages in NetFlow Version 9 format to an external IP address:

```
Device# configure terminal
Device(config)# parameter-map type inspect-global
Device(config)# log dropped-packets
Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000
Device(config-profile)# log flow-export template timeout-rate 5000
Device(config-profile)# end
```
Example: Enabling High-Speed Logging for Firewall Actions

The following example shows how to configure high-speed logging (HSL) for inspect-type parameter-map parameter-map-hsl.

```
Device# configure terminal
Device(config)# parameter-map type inspect parameter-map-hsl
Device(config-profile)# audit trail on
Device(config-profile)# alert on
Device(config-profile)# one-minute high 10000
Device(config-profile)# tcp max-incomplete host 100
Device(config-profile)# exit
Device(config)# policy-map type inspect policy-map-hsl
Device(config-pmap)# class type inspect class-map-tcp
Device(config-pmap-c)# inspect parameter-map-hsl
Device(config-pmap-c)# end
```
Example: Enabling High-Speed Logging for Firewall Actions
CHAPTER 5

Intrusion Prevention System

This feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco SD-WAN. It is delivered using a virtual image on Cisco IOS XE SD-WAN devices. This feature uses the Snort engine to provide IPS and IDS functionalities.

Snort is an open source network IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks. It can also perform protocol analysis, content searching or matching, and detect a variety of attacks and probes (such as buffer overflows).

- Overview of Intrusion Prevention System, on page 61
- Cisco SD-WAN IPS Solution, on page 62
- Configure and Apply IPS or IDS, on page 62
- Modify an Intrusion Prevention or Detection Policy, on page 66
- Delete an Intrusion Prevention or Detection Policy, on page 66
- Monitor Intrusion Prevention Policy, on page 67
- Update IPS Signatures, on page 68

Overview of Intrusion Prevention System

The IPS feature works in the network intrusion detection and prevention mode that provides IPS or IDS functionalities. In the network intrusion detection and prevention mode, the engine performs the following actions:

- Monitors network traffic and analyzes against a defined rule set.
- Performs attack classification.
- Invokes actions against matched rules.

Based on your requirements, you can enable Snort either in IPS or IDS mode. In IDS mode, the engine inspects the traffic and reports alerts, but does not take any action to prevent attacks. In IPS mode, in addition to intrusion detection, actions are taken to prevent attacks.

IPS the traffic and reports events to vManage or an external log server (if configured). External third-party monitoring tools, which supports Snort logs, can be used for log collection and analysis.
Cisco SD-WAN IPS Solution

The Snort IPS solution consists of the following entities:

- **Snort sensor**: Monitors the traffic to detect anomalies based on the configured security policies (that includes signatures, statistics, protocol analysis, and so on) and sends alert messages to the Alert/Reporting server. The Snort sensor is deployed as a security virtual image on the router.

- **Signature store**: Hosts the Cisco Talos signature packages that are updated periodically. vManage periodically downloads signature packages to the Snort sensors. You can modify the time interval to check for and download signature updates in Administration > Settings > IPS Signature Update.

- **Alert/Reporting server**: Receives alert events from the Snort sensor. Alert events generated by the Snort sensor can either be sent to vManage or an external syslog server or to both vManage and an external syslog server. vManage events can be viewed in Monitor > Events. No external log servers are bundled with the IPS solution.

Configure and Apply IPS or IDS

To configure and apply IPS or IDS to a Cisco IOS XE SD-WAN device, do the following:

- **Before you Begin**

- **Configure Intrusion Prevention or Detection**

- **Apply a Security Policy to a Device**

Before you Begin

Before you apply an IPS/IDS, URL Filtering, or Advanced Malware Protection policy for the first time, you must Upload the Cisco Security Virtual Image to vManage.

Configure Intrusion Prevention or Detection

To configure Intrusion Prevention or Detection through a security policy, use the vManage security configuration wizard:

1. In Cisco vManage, select the Configuration > Security tab in the left side panel.
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.

3. In Add Security Policy, select a scenario that supports intrusion prevention (**Compliance**, **Direct Cloud Access**, **Direct Internet Access**, or **Custom**).

4. Click **Proceed** to add an Intrusion Prevention policy in the wizard.

5. In the **Add Security Policy** wizard, click **Next** until the **Intrusion Prevention** screen is displayed.

6. Click the **Add Intrusion Prevention Policy** drop-down and choose **Create New** to create a new Intrusion Prevention policy. The Intrusion Prevention - Policy Rule Configuration wizard appears.

7. Click on **Target VPNs** to add the required number of VPNs in the Add Target VPNs wizard.

8. Enter a policy name in the **Policy Name** field.

9. Choose a signature set that defines rules for evaluating traffic from the **Signature Set** drop-down. The following options are available. Connectivity provides the least restrictions and the highest performance. Security provides the most restrictions but can affect system performance.
   - **Balanced**: Designed to provide protection without a significant effect on system performance.
This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 9. It also blocks CVEs published in the last two years and that have the following rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.

- Connectivity: Designed to be less restrictive and provide better performance by imposing fewer rules.

This signature set blocks vulnerabilities with a CVSS score of 10 and CVEs published in the last two years.

- Security: Designed to provide more protection than Balanced but with an impact on performance.

This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 8. It also blocks CVEs published in the last three years and that have the following rule categories: Malware CNC, Exploit Kits, SQL Injection, blocked list, and App Detect Rules.

10. Choose mode of operation from the Inspection Mode drop-down. The following options are available:

- Detection: Select this option for intrusion detection mode
- Protection: Select this option for intrusion protection mode

11. (Optional) From the Advanced tab, choose one or more existing IPS signature whitelist profile lists or create new ones as needed from the Signature Whitelist drop-down.

A whitelist allows the designated IPS signatures to pass through.

To create a new signature list, click New Signature List at the bottom of the drop-down. In the IPS Signature List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the IPS Signature field, enter signatures in the format Generator ID:Signature ID, separated with commas. You also can use the Import button to add a whitelist from an accessible storage location. Click Save when you are finished.

You also can create or manage IPS Signature Whitelist lists by selecting the Configuration > Security tab in the left side panel, choosing Lists from the Custom Options drop-down at the top right of the page, and then selecting Signatures in the left panel.

To remove an IPS Signature Whitelist from the Signature Whitelist field, click the X next to the list name in the field.

12. (Optional) Choose an alert level for syslogs from the Alert Log Level drop-down. The options are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

You must configure the address of the external log server in the Policy Summary page.
13. Click **Save Intrusion Prevention Policy** to add an Intrusion Prevention policy.
14. Click **Next** until the Policy Summary page is displayed
15. Enter Security Policy Name and Security Policy Description in the respective fields.
16. If you set an alert level when configuring the Intrusion Prevention policy, in the Additional Policy Settings section, you must specify the following:
   - External Syslog Server VPN: The syslog server should be reachable from this VPN.
   - Server IP: IP address of the server.
   - Failure Mode: **Open** or **Close**
17. Click **Save Policy** to configure the Security policy.
18. You can edit the existing Intrusion Prevention policy by clicking on **Custom Options** in the right-side panel of the **vManage > Configuration > Security** wizard.

### Apply a Security Policy to a Device

To apply a security policy to a device:

1. In vManage, select the **Configuration > Templates** screen.

   ![Image of vManage Configuration > Templates screen]

2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template**.
3. From the **Device Model** drop-down, select one of the devices.
4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.
5. From the Security Policy drop-down, select the name of the policy you configured in the previous procedure.

6. Click Create to apply the security policy to a device.

Modify an Intrusion Prevention or Detection Policy

To modify a intrusion prevention or detection policy, do the following:

1. In Cisco vManage, select the Configuration > Security tab in the left side panel.

2. In the Security screen, click the Custom Options drop-down and select Intrusion Prevention.

3. For the policy that you want to modify, click the More Actions icon to the far right of the policy and select Edit.

4. Modify the policy as required and click Save Intrusion Prevention Policy.

Delete an Intrusion Prevention or Detection Policy

To delete an intrusion prevention or detection policy, you must first detach the policy from the security policy:

1. In Cisco vManage, select the Configuration > Security tab in the left side panel.

2. Detach the IPS or IDS policy from the security policy as follows:
   a. For the security policy that contains the IPS or IDS policy, click the More Actions icon to the far right of the policy and select Edit.
      The Policy Summary page is displayed.
   b. Click the Intrusion Prevention tab.
   c. For the policy that you want to delete, click the More Actions icon to the far right of the policy and select Detach.
   d. Click Save Policy Changes.

3. Delete the IPS or IDS policy as follows:
In the Security screen, click the **Custom Options** drop-down and select **Intrusion Prevention**.

For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Delete**.

A dialog box is displayed.

Click **OK**.

### Monitor Intrusion Prevention Policy

You can monitor the Intrusion Prevention System (IPS) signature violations by severity and by count using the following steps.

To monitor the Signatures of IPS Configuration on IOS XE SD-WAN device:

1. From the **Monitor > Network** screen, select a device.

2. In the left panel, under **Security Monitoring**, select **Intrusion Prevention** tab. The Intrusion Prevention wizard displays.

3. Click **By Severity** or **By Count** to designate how you want to display intrusion prevention information.
Update IPS Signatures

IPS uses Cisco Talos signatures to monitor the network. Cisco recommends following this procedure to download the latest signatures.

**Note**

To download the signatures, vManage requires access to the following domains using port 443:

- api.cisco.com
- cloudsso.cisco.com
- dl.cisco.com
- dl1.cisco.com
- dl2.cisco.com
- dl3.cisco.com

1. In Cisco vManage, select the **Administration > Settings** tab in the left side panel to configure IPS Signature Update.

2. Click on **Edit** to **Enable/Disable** and provide your Cisco.com **Username** and **Password** details to save the Policy details as shown in the following screenshot.
CHAPTER 6

URL Filtering

The URL Filtering feature enables the user to provide controlled access to Internet websites or Intranet sites by configuring the URL-based policies and filters on the device. The user can configure the URL Filtering profiles to manage the web access. The URL Filtering feature is implemented using the security virtual image similar to the IPS feature.

URL Filtering can either allow or deny access to a specific URL based on:

• Allowed list and blocked list: These are static rules, which helps the user to either allow or deny URLs. If the same pattern is configured under both the allowed and blocked lists, the traffic is allowed.

• Category: URLs can be classified into multiple categories such as News, Social Media, Education, Adult and so on. Based on the requirements, user has the option to block or allow one or more categories.

• Reputation: Each URL has a reputation score associated with it. The reputation score range is from 0-100, and it is categorized as: high-risk (reputation score (0-20), suspicious (21-40), moderate-risk (41-60), low-risk (61-80), and trustworthy (81-100). Based on the reputation score of a URL and the configuration, a URL is either blocked or allowed.

This section contains the following topics:

• Overview of URL Filtering, on page 71
• Configure and Apply URL Filtering, on page 73
• Modify URL Filtering, on page 77
• Delete URL Filtering, on page 78
• Monitor URL Filtering, on page 78

Overview of URL Filtering

The URL Filtering feature enables the user to provide controlled access to Internet websites by configuring the URL-based policies and filters on the device.

The URL Filtering feature allows a user to control access to Internet websites by permitting or denying access to specific websites based on the category, reputation, or URL. For example, when a client sends a HTTP/HTTP(s) request through the router, the HTTP/HTTP(s) traffic is inspected based on the URL Filtering policies (allowed list/ blocked list, Category, and Reputation). If the HTTP/HTTP(s) request matches the blocked list, the HTTP(s) request is blocked by an inline block page response. If the HTTP/HTTP(s) request matches the allowed list, the traffic is allowed without further URL Filtering inspection.
For HTTPS traffic, the inline block page is not be displayed. URL Filtering will not decode any encoded URL before performing a lookup.

When there is no alloweed list or blocked list configured on the device, based on the category and reputation of the URL, traffic is allowed or blocked using a block page. For HTTP(s), a block page is not displayed and the traffic is dropped.

Filtering Options

The URL Filtering allows you to filter traffic using the following options:

Category-Based Filtering

By default, vManage does not download the URL database from the cloud. To enable the URL database download, you must set the Resource Profile to High in the Feature Template.

If configured, vManage downloads the URL database from the cloud. After the full database is downloaded from the cloud, if there are any updates to the existing database, the incremental updates will be automatically downloaded every 15 minutes. The complete database size is approximately 440 MB and the downloaded database should always synchronize with the cloud. The database will be invalid if the connection to the cloud is lost for more than 24 hours. The default URL category/reputation database only has a few IP address based records. The category/reputation look up occurs only when the host portion of the URL has the domain name. If the device does not get the database updates from the cloud, vManage ensures that the traffic designated for URL Filtering is not dropped.

Reputation-Based Filtering

In addition to category-based filtering, you can also filter based on the reputation of the URL. Each URL has a reputation score associated with it. The reputation score range is from 0-100 and it is categorized as:

- **High risk**: Reputation score of 0 to 20
- **Suspicious**: Reputation score of 21 to 40
- **Moderate risk**: Reputation score of 41 to 60
- **Low risk**: Reputation score of 61 to 80
- **Trustworthy**: Reputation score of 81 to 100

When you configure a web reputation in vManage, you are setting a reputation threshold. Any URL that is below the threshold is blocked by URL filtering. For example, if you set the web reputation to Moderate Risk in vManage, any URL that has a reputation score below than and equal to 60 is blocked.

Based on the reputation score of a URL and the configuration, a URL is either blocked or allowed.
List-based Filtering

List-based filtering allows the user to control access by permitting or denying access based on allowed or blocked lists. Here are some important points to note regarding these lists:

- URLs that are allowed are not subjected to any category-based filtering (even if they are configured).
- If the same item is configured under both the allowed and blocked list, the traffic is allowed.
- If the traffic does not match either the allowed or blocked lists, then it is subjected to category-based and reputation-based filtering (if configured).
- A user may consider using a combination of allowed and blocked pattern lists to design the filters. For example, if you want to allow `www.fo0.com` but also want to block other URLs such as `www.fo0.abc` and `www.fo0.xyz`, you can configure `www.fo0.com` in the allowed list and `www.fo0.` in the blocked list.

Configure and Apply URL Filtering

To configure and apply URL Filtering to a Cisco IOS XE SD-WAN device, do the following:

Before you Begin

Before you apply an IPS/IDS, URL Filtering, or Advanced Malware Protection policy for the first time, you must Upload the Cisco Security Virtual Image to vManage.

Configure URL Filtering

To configure URL Filtering through a security policy, use the vManage security configuration wizard:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
3. In Add Security Policy, select a scenario that supports URL filtering (Guest Access, Direct Internet Access, or Custom).
4. Click Proceed to add a URL filtering policy in the wizard.
5. In the Add Security Policy wizard, click Next until the URL Filtering screen is displayed.

7. Click on Target VPNs to add the required number of VPNs in the Add Target VPNs wizard.
8. Enter a policy name in the Policy Name field.
9. Choose one of the following options from the Web Categories drop-down:
   - **Block**—Block websites that match the categories that you select.
   - **Allow**—Allow websites that match the categories that you select.
10. Select one or more categories to block or allow from the Web Categories list.
11. Select the Web Reputation from the drop-down. The options are:
    - **High Risk**: Reputation score of 0 to 20.
    - **Suspicious**: Reputation score of 21 to 40.
    - **Moderate Risk**: Reputation score of 41 to 60.
    - **Low Risk**: Reputation score of 61 to 80.
- **Trustworthy**: Reputation score of 81 to 100.

12. (Optional) From the Advanced tab, choose one or more existing lists or create new ones as needed from the Whitelist URL List or Blacklist URL List drop-down.

**Note**

Items on the allowed lists are not subject to category-based filtering. However, items on the blocked lists are subject to category-based filtering. If the same item is configured under both the allowed and blocked lists, the traffic is allowed.

To create a new list, do the following:

a. Click **New Whitelist URL List** or **New Blacklist URL List** at the bottom of the drop-down.

b. In the URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only)

c. In the URL field, enter URLs to include in the list, separated with commas. You also can use the **Import** button to add lists from an accessible storage location.

d. Click **Save** when you are finished.

You also can create or manage URL lists by selecting the **Configuration > Security** tab in the left side panel, choosing **Lists** from the **Custom Options** drop-down at the top right of the page, and then selecting **Whitelist URLs** or **Blacklist URLs** in the left panel.

To remove a URL list from the URL List field, click the **X** next to the list name in the field.

13. (Optional) In the Block Page Server pane, choose an option to designate what happens when a user visits a URL that is blocked. Choose Block Page Content to display a message that access to the page has been denied, or choose Redirect URL to display another page.

If you choose Block Page Content, users see the content header “Access to the requested page has been denied.” in the Content Body field, enter text to display under this content header. The default content body text is “Please contact your Network Administrator.” If you choose Redirect URL, enter a URL to which users are redirected.
14. (Optional) In the Alerts and Logs pane, select the alert types from the following options:
   - **Blacklist**—Exports an alert as a Syslog message if a user tries to access a URL that is configured in the blocked URL List.
   - **Whitelist**—Exports an alert as a Syslog message if a user tries to access a URL that is configured in the allowed URL List.
   - **Reputation/Category**—Exports an alert as a Syslog message if a user tries to access a URL that has a reputation that is configured as blocked in the Web Reputation field or that matches a blocked web category.

   Alerts for allowed reputations or allowed categories are not exported as Syslog messages.

15. You must configure the address of the external log server in the Policy Summary page.

16. Click **Save URL filtering Policy** to add an URL filtering policy.

17. Click **Next** until the Policy Summary page is displayed.

18. Enter Security Policy Name and Security Policy Description in the respective fields.

19. If you enabled Alerts and Logs, in the Additional Policy Settings section you must specify the following:
   - **External Syslog Server VPN**: The syslog server should be reachable from this VPN.
   - **Server IP**: IP address of the server.
   - **Failure Mode**: **Open** or **Close**.

20. Click **Save Policy** to save the Security policy.

21. You can edit the existing URL filtering policy by clicking on **Custom Options** in the right-side panel of the **vManage > Configuration > Security** wizard.
**Apply a Security Policy to a Device**

To apply a security policy to a device:

1. In vManage, select the **Configuration > Templates** screen.

![Configuration > Templates screen](image1.png)

2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template**.

3. From the **Device Model** drop-down, select one of the devices.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.

![Additional Templates section](image2.png)

5. From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.

6. Click **Create** to apply the security policy to a device.

**Modify URL Filtering**

To modify a URL Filtering policy, do the following:

1. In Cisco vManage, select the **Configuration > Security** tab in the left side panel.

2. In the Security screen, click the **Custom Options** drop-down and select **URL Filtering**.
3. For the policy that you want to modify, click the More Actions icon to the far right of the policy and select Edit.

4. Modify the policy as required and click Save URL Filtering Policy.

Delete URL Filtering

To delete a URL filtering policy, you must first detach the policy from the security policy:

1. In Cisco vManager, select the Configuration > Security tab in the left side panel.

2. Detach the URL filtering policy from the security policy as follows:
   a. For the security policy that contains the URL filtering policy, click the More Actions icon to the far right of the policy and select Edit.
      The Policy Summary page is displayed.
   b. Click the URL Filtering tab.
   c. For the policy that you want to delete, click the More Actions icon to the far right of the policy and select Detach.
   d. Click Save Policy Changes.

3. Delete the URL filtering policy as follows:
   a. In the Security screen, click the Custom Options drop-down and select URL Filtering.
   b. For the policy that you want to delete, click the More Actions icon to the far right of the policy and select Delete.
      A dialog box is displayed.
   c. Click OK.

Monitor URL Filtering

You can monitor the URL Filtering for a device by web categories using the following steps.

To monitor the URLs that are blocked or allowed on an IOS XE SD-WAN device:

1. From the Monitor > Network screen, select a device.

2. In the left panel, under Security Monitoring, select the URL Filtering tab. The URL Filtering wizard displays.

3. Click on the Blocked tab, the session count on a blocked URL appears as shown in the following screenshot.
4. Click on the **Allowed** tab, the session count on allowed URLs appear as shown in the following screenshot.
Advanced Malware Protection

The Cisco Advanced Malware Protection (AMP) integration equips routing and SD-WAN platforms to provide protection and visibility to cover all stages of the malware lifecycle:

- Before: Hardening the network border with firewall rules
- During: Blocking malware based on File Reputation and IPS Signatures
- After:
  - Using File Notifications to represent breaches that occurred;
  - Retrospectively detecting malware and providing automatic reporting;
  - During: Blocking malware based on File Reputation and IPS Signatures
  - Using advanced file analysis capabilities for detection and deeper insight into unknown files in a network

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN 19.1</td>
<td>Feature introduced. The Cisco Advanced Malware Protection (AMP) integration equips routing and SD-WAN platforms to provide protection and visibility to cover all stages of the malware lifecycle.</td>
</tr>
</tbody>
</table>

Overview of Advanced Malware Protection

The Cisco Advanced Malware Protection is composed of three processes:
• File Reputation: The process of using a 256-bit Secure Hash Algorithm (SHA256) signature to compare the file against the Advanced Malware Protection (AMP) cloud server and access its threat intelligence information. The response can be Clean, Unknown, or Malicious. If the response is Unknown, and if File Analysis is configured, the file is automatically submitted for further analysis.

• File Analysis: The process of submitting an Unknown file to the Threat Grid (TG) cloud for detonation in a sandbox environment. During detonation, the sandbox captures artifacts and observes behaviors of the file, then gives the file an overall score. Based on the observations and score, Threat Grid may change the threat response to Clean or Malicious. Threat Grid’s findings are reported back to the AMP cloud, so that all AMP customers will be protected against newly discovered malware.

**Note**
File analysis requires a separate Threat Grid account. For information about purchasing a Threat Grid account, contact your Cisco representative.

• Retrospective: By maintaining information about files even after they are downloaded, we can report on files that were determined to be malicious after they were downloaded. The disposition of the files could change based on the new threat intelligence gained by the AMP cloud. This re-classification will generate automatic retrospective notifications.

**Configure and Apply an Advanced Malware Policy**

To configure and apply an Advanced Malware Policy to a Cisco IOS XE SD-WAN device, do the following:

- Before you Begin, on page 82
- Configure and Apply an Advanced Malware Policy, on page 82
- Apply a Security Policy to a Device, on page 40

**Before you Begin**

- Before you apply an IPS/IDS, URL filtering, or Advanced Malware Protection policy for the first time, you must [Upload the Cisco Security Virtual Image to vManage](#).
- To perform file analysis, you must configure the Threat Grid API Key as described in Configure Threat Grid API Key, on page 82

**Configure Threat Grid API Key**

To perform file analysis, you must configure your Threat Grid API key:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log into your Cisco AMP Threat Grid dashboard, and select your account details.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Under your Account Details, an API key may already be visible if you've created one already. If you haven't, click Generate New API Key. Your API key should then be visible under User Details &gt; API Key.</td>
</tr>
</tbody>
</table>
Step 3  In Cisco vManage, select the **Configuration > Security** tab in the left side panel.

Step 4  In the Security screen, click the **Custom Options** drop-down and select **Threat Grid API Key**.

Step 5  In the Manage Threat Grid API key pop-up box, take these actions:
   a) Choose a region from the **Region** drop-down.
   b) Enter the API key in the **Key** field.
   c) Click **Add**.
   d) Click **Save Changes**.

---

### Configuring an Advanced Malware Protection Policy

To configure an Advanced Malware Protection policy:

**Step 1**  In Cisco vManage, select the **Configuration > Security** tab in the left side panel.

**Step 2**  Click **Add Security Policy**. The Add Security Policy wizard opens and various use-case scenarios display.

![Add Security Policy](image)

**Step 3**  In Add Security Policy, select **Direct Internet Access** and then click **Proceed**.

**Step 4**  In the Add Security Policy wizard, click **Next** as needed to select the **Advanced Malware Protection** tab.
Step 5
In the Advanced Malware Protection tab, click the Add Advanced Malware Protection Policy drop-down.

Step 6
Select Create New. The Add Advanced Malware Protection screen displays.

Step 7
In the Policy Name field, enter a name for the malware policy. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8
Make sure that the Match All VPN button is selected. Select Match All VPN if you want to apply the policy to all the VPNs, or select Custom VPN Configuration to input the specific VPNs.

Step 9
From the AMP Cloud Region dropdown, select a global region.

Step 10
From the Alerts Log Level dropdown, select a severity level (Critical, Warning, or Info).

Note: Because the Info severity level generates multiple notifications and can affect system performance, this level should be configured only for testing or debugging and not for real-time traffic.

Step 11
Click File Analysis to enable Threat Grid (TG) file analysis.

Note: Before you can perform this step, configure a threat grid API key as described in Configure Threat Grid API Key, on page 82.
Note: File Analysis requires a separate Threat Grid license.

Step 12  From the **TG Cloud Region** dropdown, select a global region.

Note: Configure the Threat Grid API Key by clicking on Manage API Key or as described in Configure Threat Grid API Key, on page 82

Step 13  From the **File Types List** dropdown, select the file types that you want to be analyzed.

Step 14  From the **Alerts Log Level** dropdown, select a severity level (Critical, Warning, or Info).

Step 15  Click **Target VPNs** to select the target VPNs or all VPNs, and then click **Add VPN**.

Step 16  Click **Save Changes**. The Policy Summary screen displays.

Step 17  Click **Next**.

---

**Apply a Security Policy to a Device**

To apply a security policy to a device:

1. In vManage, select the **Configuration > Templates** screen.
2. In the Device tab, from the Create Template drop-down, select From Feature Template.

3. From the Device Model drop-down, select one of the devices.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the policy you configured in the previous procedure.

6. Click Create to apply the security policy to a device.

**Modify an Advanced Malware Protection Policy**

To modify an Advanced Malware Protection policy, do the following:

1. In Cisco vManage, select the Configuration > Security tab in the left side panel.

2. In the Security screen, click the Custom Options drop-down and select Advanced Malware Protection.

3. For the policy that you want to modify, click the More Actions icon to the far right of the policy and select Edit.

4. Modify the policy as required and click Save Advanced Malware Protection Policy.
Delete an Advanced Malware Protection Policy

To delete an Advanced Malware Protection policy, you must first detach the policy from the security policy:

1. In Cisco vManage, select the Configuration > Security tab in the left side panel.

2. Detach the AMP policy from the security policy as follows:
   a. For the security policy that contains the AMP policy, click the More Actions icon to the far right of the policy and select Edit.
      The Policy Summary page is displayed.
   b. Click the Advanced Malware Protection tab.
   c. For the policy that you want to delete, click the More Actions icon to the far right of the policy and select Detach.
   d. Click Save Policy Changes.

3. Delete the AMP policy as follows:
   a. In the Security screen, click the Custom Options drop-down and select Advanced Malware Protection.
   b. For the policy that you want to delete, click the More Actions icon to the far right of the policy and select Delete.
      A dialog box is displayed.
   c. Click OK.

Monitor Advanced Malware Protection

You can monitor Advanced Malware Protection from the Device Dashboard by using the following steps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Monitor &gt; Network screen, select a device.</td>
</tr>
<tr>
<td>2</td>
<td>In the left panel, under Security Monitoring, select the Advanced Malware Protection tab.</td>
</tr>
</tbody>
</table>

This tab shows the following:

- File Reputation – The graph or pie chart shows the total number of files transferred and how many are malicious, clean, or unknown. This tab area also includes a table with detailed information about each file that was inspected.
- File Retrospection – A table with detailed information about file retrospection events.
- File Analysis – A graph that shows the number of files that were uploaded to Threat Grid, and a table with detailed information about each file that was uploaded for analysis.
Troubleshoot Advanced Malware Protection

Malware in POP3 Account

If Cisco United Threat Defense (UTD) detects malware on a POP3 email server, UTD prevents email clients from downloading the email message with the malware, and then resets the connection between the email server and client. This prevents downloading any email after detection of the malware. Even later attempts to download email from the server fail if the problematic file remains on the server.

To resolve this, an administrator must remove the file(s) identified as malware from the server, to enable a new session between the server and client.

Rekey the Device Threat Grid API Key

To rekey the device Threat Grid API key from the Maintenance screen:

**Step 1**
In Cisco vManage, select the **Maintenance > Security** tab in the left side panel.

**Step 2**
Select the **Advanced Malware Protection** tab.

**Step 3**
Select the device or devices that you want to rekey.

**Step 4**
Select **Action > API Rekey**.
SSL/TLS Proxy for Decryption of TLS Traffic

Table 9: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL/TLS Proxy</td>
<td>Cisco IOS XE Release Amsterdam 17.2.1r</td>
<td>The SSL/TLS Proxy feature allows you to configure an edge device as a transparent SSL/TLS proxy. Such proxy devices can then decrypt incoming and outgoing TLS traffic to enable their inspection by Unified Thread Defense (UTD) and identify risks that are hidden by end-to-end encryption. This feature is part of the Cisco SD-WAN Application Quality of Experience (AppQoE) and UTD solutions.</td>
</tr>
</tbody>
</table>

- Information about SSL/TLS Proxy, on page 89
- Configure Cisco IOS XE SD-WAN Devices as TLS Proxy, on page 96
- Verify Configuration, on page 106
- Monitor TLS Proxy Performance, on page 107
- Revoke and Renew Certificates, on page 110

Information about SSL/TLS Proxy

Overview of SSL/TLS Proxy

Note

TLS is the successor of SSL. This document uses the term TLS to refer to both SSL and TLS.

Today more and more apps and data reside in the cloud. As a result, majority of internet traffic is encrypted. This may lead to malware remaining hidden and lack of control over security. The TLS proxy feature allows you to configure edge devices as transparent TLS proxy. This feature has been integrated with Cisco Unified Threat Defense (UTD).

TLS proxy devices act as man-in-the-middle (MitM) to decrypt encrypted TLS traffic traveling across WAN, and send it to (UTD) for inspection. TLS Proxy thus allows devices to identify risks that are hidden by end-to-end encryption over TLS channels. The data is re-encrypted post inspection before being sent to its final destination.
Benefits of TLS Proxy

- Monitoring of TLS traffic for any threats through transparent inspection
- Enforcement of security policies based on the inspection of the decrypted traffic
- Threat and malware protection for TLS traffic

Traffic Flow with TLS Proxy

A typical TLS handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). The clients and servers must trust these CAs in order to establish trust. TLS Proxy acts as MitM and runs a CA to issue proxy certificates for the connection dynamically.

This is how traffic flows when TLS proxy is enabled:

1. A TCP connection is established between the client and the proxy, and the proxy and the server.
2. If a decryption policy is enabled for the flow, a client Hello packet is sent to UTD to determine the decryption action.
3. Based on the UTD verdict, one of the following actions takes place:
   - **drop**: If the verdict is drop, the hello packet from the client is dropped and the connection is reset.
   - **do-not-decrypt**: If the verdict is do-not-decrypt, the hello packet bypasses TLS proxy.
   - **decrypt**: If the verdict is decrypt, the packet is forwarded to the client and goes through the following:
     a. TCP optimization for optimization of traffic
     b. Decryption of encrypted traffic through TLS proxy
     c. Threat inspection through UTD
     d. Re-encryption of decrypted traffic through TLS proxy

If there is a delay in determining the decrypt status of the flow, the UTD configuration for fail-decrypt is exercised.

The following image shows the TLS handshake process.
Figure 1: TLS Handshake Process

Role of Certificate Authorities in TLS Proxy

About Certificate Authorities (CAs)

A CA manages certificate requests and issue certificates to participating entities such as hosts, network devices, or users. A CA provides centralized identity management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate devices and individual users. In public key cryptography, such as the RSA encryption system, each device or user has a key-pair containing both a private key and a public key. The private key is kept secret and is known only to the owning device. The public key, however, can be known to everybody. The keys act as complements. Anything encrypted with one of the keys can be decrypted with the other. A signature is formed when data is encrypted with a sender’s private key. The receiver verifies the signature by decrypting the message with the sender’s public key. This process relies on the receiver having a copy of the sender’s public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

How CA and TLS Proxy Work Together

Once you configure a CA for TLS proxy, the CA issues signing certificates to the TLS proxy device. The device then securely stores the subordinate CA keys, and dynamically generates and signs the proxy certificates. The TLS proxy device then performs the following certification tasks:
CA Options for Configuring TLS Proxy

The following CA options are supported for configuring TLS proxy:

- Enterprise CA
- Enterprise CA with SCEP Enabled
- vManage as CA
- vManage as Intermediate CA

In the subsequent sections, we have listed the benefits and limitations of each of the supported CA options to help you make an informed decision about choosing the CA for TLS proxy.

Enterprise CA

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. For Enterprise CA that does not support Simple Certificate Enrollment Protocol (SCEP), manual enrollment is required. Manual enrollment involves downloading a Certificate Signing Request (CSR) for your device, getting it signed by your CA, and then uploading the signed certificate to the device through Cisco vManage.

Table 10: Enterprise CA: Benefits and Limitations

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates</td>
<td>• Maintenance creates an administrative overload.</td>
</tr>
<tr>
<td>• The client trust-store need not be updated</td>
<td>• Manual certificate deployment is required for TLS proxy</td>
</tr>
<tr>
<td>• Provides a single location for managing all certificates issued</td>
<td>• Out-of-band management is required for tracking the usage and expiry of certificates</td>
</tr>
<tr>
<td>• Certificates can be revoked and tracked through your own CA</td>
<td>• Requires manual re-issuance of expired proxy certificates</td>
</tr>
<tr>
<td></td>
<td>• If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated</td>
</tr>
</tbody>
</table>

Enterprise CA with SCEP

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. If your CA supports SCEP, you can configure it to automate the certificate management process.
**Table 11: Enterprise CA with SCEP: Benefits and Limitations**

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates</td>
<td>• Maintenance creates an administrative overload.</td>
</tr>
<tr>
<td>• The client trust-store need not be updated</td>
<td>• If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated</td>
</tr>
<tr>
<td>• Provides a single location for managing all certificates issued</td>
<td>• Offers limited visibility through Cisco vManage</td>
</tr>
<tr>
<td>• Certificates can be revoked and tracked through your own CA</td>
<td>• Enterprise CA have limited support for SCEP</td>
</tr>
<tr>
<td>• Certificate deployment to TLS Proxy can be automated</td>
<td></td>
</tr>
</tbody>
</table>

**vManage as CA**

Use this option if you don't have an enterprise CA and want to use Cisco vManage to issue trust certificates.

**Table 12: vManage as CA: Benefits and Limitations**

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Certificate deployment to proxy devices is automated</td>
<td>• Cisco vManage certificate needs to be pushed to the client trust store</td>
</tr>
<tr>
<td>• Certificates are reissued and revalidated before they expire</td>
<td></td>
</tr>
<tr>
<td>• Certificates can be monitored, tracked, and validated through Cisco vManage</td>
<td></td>
</tr>
</tbody>
</table>

**vManage as Intermediate CA: Benefits and Limitations**

Use this option if you have an internal enterprise CA, but would like to use Cisco vManage as intermediate CA to issue and manage subordinate CA certificates.
Table 13: vManage as Intermediate CA: Benefits and Limitations

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Certificate deployment to proxy devices is automated</td>
<td>• Requires manual deployment</td>
</tr>
<tr>
<td>• Certificates are reissued and revalidated before they expire</td>
<td>• Maintaining two CAs causes administrative overload</td>
</tr>
<tr>
<td>• The risk associated with certificates being compromised is limited as compromised proxy certificates are revoked</td>
<td>• Cisco vManage certificate usage is tracked through the enterprise CA</td>
</tr>
<tr>
<td>• Certificates can be monitored, tracked, and validated through Cisco vManage</td>
<td>• Deployment can be complex if your network has multiple Cisco vManage controllers for clustering or redundancy</td>
</tr>
<tr>
<td>• No other certificates, besides your enterprise CA certificate, need to be pushed to your client trust-store</td>
<td></td>
</tr>
</tbody>
</table>

Supported Platforms and Platform Requirements

The following platforms support the SSL/TLS Proxy feature.

- Cisco 4331 Integrated Services Router (ISR4331)
- Cisco 4351 Integrated Services Router (ISR4351)
- Cisco 4431 Integrated Services Router (ISR4431)
- Cisco 4451 Integrated Services Router (ISR4451)
- Cisco 4461 Integrated Services Router (ISR4461)
- Cisco CSR 1000v Cloud Services Router (CSR1000v)

Minimum Memory Requirements

- The platforms must have a minimum of 8 GB of DRAM.

Supported Cipher Suites

The TLS Proxy feature in Cisco SD-WAN supports the following cipher suites.

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_SEED_CBC_SHA
- TLS_DHE_RSA_WITH_SEED_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Prerequisites for TLS Proxy

- Flow symmetry is required for branches with dual routers.
- If you have multiple internet links, the flows must be pinned to only one of them. This ensures that the sites that require an SSL client have the same source IP address.
- TLS proxy devices and the clients must have their times in sync. See Configure NTP to learn how to synchronize all devices in the Cisco SD-WAN solution.

Limitations and Restrictions

- The TLS Proxy feature only supports TLS versions 1.0, 1.1, and 1.2. TLS version 1.3 is not supported and is downgraded to TLS version 1.2.
• Only RSA and its variant cipher suites are supported. ECDSA based cipher suites are not supported.

• Certificate Revocation List (CRL) check is not supported for server certificate validation. However, you can enable OCSP from Advanced Settings in SSL Decryption policy.

• OCSP stapling is not supported and must be explicitly disabled on the browser for the TLS session to be established.

• For branch-to-branch and branch-to-data center traffic scenarios that support service nodes, the SSL decryption security policy must be applied in a way that prevents the SSL flow from being inspected on both the devices.

• IPv6 traffic is not supported.

• TLS session resumption, renegotiation and client certificate authentication are not supported.

• If TLS proxy crashes, it takes up to two minutes for it to be ready to serve as proxy for TLS flows again. During this time, depending upon your security settings, the flows are either bypassed or dropped.

• For decrypted HTTPS traffic that is dropped, the block page is not displayed.

Configure Cisco IOS XE SD-WAN Devices as TLS Proxy

High-level Steps for Configuring a Device as TLS Proxy

1. Configure certificate authority (CA) for the TLS proxy: Enterprise CA, vManage as CA, or vManage as Intermediate CA.

2. The next step differs based on the CA option you configure. See the task flows in the following section for Enterprise CA, and vManage as CA and vManage as Intermediate CA.

3. Create and attach SSL decryption security policy to the device.

Task Flow: Set up TLS Proxy with Enterprise CA

If you configure Enterprise CA to enable TLS proxy on your devices, go through the following steps to complete the TLS proxy setup.
Figure 2: Use Enterprise CA to Configure TLS Proxy on a Device

- Set Up Enterprise CA
- Create SSL decryption security policy
- Attach the SSL decryption policy to a device
- Upload the CSR auto-generated on the device to CA
- Download the subordinate CA certificate from CA
- Upload the sub CA certificate on the device

Task Flow: of Set Up TLS Proxy with vManage as CA or vManage as Intermediate CA

If you configure up vManage as CA or vManage as Intermediate CA to enable TLS proxy on your devices, go through the following steps to complete the TLS proxy setup.

Figure 3: Use vManage as CA or vManage as Intermediate CA to Configure TLS Proxy on a Device

- vManage as CA
  - Import the generated root certificate into the clients’ truststore as root CA
- vManage as Intermediate CA
  - Upload the generated CSR into your CA and get it certified as subordinate CA
  - Upload the subordinate CA certificate to the intermediate CA page

- Create SSL decryption security policy
  - Attach the SSL decryption security policy to a device
  - vManage automatically uploads a proxy subordinate CA certificate onto the device

The subsequent topics provide a step-by-step procedure to complete the configuration of a Cisco IOS XE SD-WAN device as SSL/TLS Proxy.
Configure CA for TLS Proxy

Cisco vManage offers the following options to set up a CA.

Configure Enterprise CA

Configure Enterprise CA to issue subordinate CA certificates to the proxy device at the edge of the network.

Prerequisites to Set up CA for SSL/TLS Proxy

To be able to configure CA certificates, the CA server and the device seeking the certificate must have their time synchronized. See Configure NTP to learn how to coordinate and synchronize time across all devices in the Cisco SD-WAN overlay network.

Configure Enterprise CA

1. Download a CA certificate from your CA server in PEM or Base64 format.
2. In Cisco vManage, go to Configuration > TLS/SSL Proxy.
3. Select Enterprise CA.
   a. Enter the SCEP server URL in the URL Base field.
   b. [Optional] Enter the Challenge Password/Phrase if you have one configured.

Note

If Enterprise CA is configured with SCEP, the Enterprise SCEP CA server should be reachable from transport VPN (VPN 0).

5. Upload your PEM-encoded CA certificate by clicking the Select a file option next to Root Certificates.
   OR
   Paste the CA certificate in the Root Certificates Box.
6. Verify that the fingerprint, which auto-populates after you upload the certificate, matches your CA.
7. Click Save Certificate Authority.

Note

This step concludes configuring enterprise CA. However, you must complete steps 8, 9, and 10 to complete setting up the device as TLS proxy.

8. Configure SSL Decryption
9. Apply a Security Policy to an XE SD-WAN Router
10. Upload a Subordinate CA Certificate to TLS Proxy, on page 104
Configure Cisco vManage as CA

*Configure vManage as CA to issue subordinate CA certificates to the proxy device at the edge of the network.*

Use the vManage as CA option if your enterprise doesn’t have an internal CA. With this option, Cisco vManage is used as a root CA and is authorized to issue subordinate CAs to the proxy devices at the edge of the network. The certificates issued by vManage as CA can be managed through Cisco vManage.

**Prerequisites to Set up CA for SSL/TLS Proxy**

To be able to configure CA certificates, the CA server and the device seeking the certificate must have their time synchronized. See Configure NTP to learn how to coordinate and synchronize time across all devices in the Cisco SD-WAN overlay network.

1. In Cisco vManage, go to **Configuration > TLS/SSL Proxy**.
2. Select vManage as CA.

---

**Note**

Leave the Set vManage as Intermediate CA check-box unselected if you want to set vManage as CA.

3. Enter the requested details: Common Name, Organization, Organizational Unit, Locality, State/Province, Country Code, and Email.
4. Select the certificate validity period from the drop-down list.
5. Click **Save Certificate Authority**.
6. Click the **Download** option on the vManage as CA page to download the root certificate generated.
7. Import the downloaded certificate into your client's trustStore as a trusted root CA.

---

**Note**

This step concludes configuring Cisco vManage as CA. However, you must complete steps 8, 9, and 10 to complete setting up a device as TLS proxy.

8. Configure **Configure SSL Decryption** security policy.
9. **Configure SSL Decryption**
10. **Apply a Security Policy to an XE SD-WAN Router**

   When TLS/SSL decryption is applied to a Cisco IOS XE SD-WAN device, Cisco vManage automatically issues a subordinate CA for the proxy and imports it to the device.

---

### Configure vManage as Intermediate CA

*Configure vManage as Intermediate CA to enable a TLS proxy device to use subordinate CA certificates issued by Cisco vManage.*

When Cisco vManage is set as intermediate CA, your enterprise CA acts as the root CA and Cisco vManage is designated as the preferred intermediate CA to issue and manage subordinate CA certificates for a proxy device. This option is suitable for enterprises that have their own internal CA but would like to use Cisco vManage to automate and manage certificate issuance and renewal.
1. In Cisco vManage, go to Configuration > TLS/SSL Proxy.
2. Select vManage as CA.
3. Select the Set vManage as Intermediate CA check-box.
4. Upload the CA certificate using the Select a file option.
   OR
   Paste the content of the PEM-encoded CA certificate file in the Root Certificate text box.
5. Click Next.
6. Under the Generate CSR area, enter the requested details, and click Generate CSR.
   The CSR field on the screen populates with the Certificate Signing Request (CSR).
7. Copy or download the CSR and upload it to the enterprise CA server to get it signed by the CA server as the subordinate CA certificate.

**Note**
The process to get a CSR signed by a CA server may differ from one CA to another. Follow your standard procedure to get a CSR signed by your CA.

8. Click Next.
9. In the Intermediate Certificate text box, paste the content of the signed Cisco vManage certificate, and click Upload.
   OR
   Click the Select a file option and upload the CSR generated in the previous step, and click Upload.
10. Verify that the fingerprint, which auto-populates after you upload the CSR, matches your CA certificate.
11. Click Save Certificate Authority.

**Note**
This step concludes configuring Cisco vManage as intermediate CA. However, you must complete steps 12 and 13 to complete the configuration for setting up a device as TLS proxy.

12. Configure SSL Decryption
13. Apply a Security Policy to an XE SD-WAN Router
   When the SSL/TLS decryption security policy is attached to the device, Cisco vManage automatically issues a subordinate, proxy CA certificate and imports it on the device.

**Configure SSL Decryption**
The SSL decryption policy provides the following ways to divert traffic for decryption:

- Network-based rules: Diverts traffic on the basis of the source or destination IP address, port, VPNs, and application.
• URL-based rules: Decide whether to decrypt based on the URL category or reputation of the URL. The decision is made based on the Client Hello packet.

For URL-based rules, note the following:
• You can set blocked list URLs to always be decrypted
• You can set allowed list URLs to never be decrypted.
• If a URL lookup to the cloud takes too long, the user can set one of the following:
  • Decrypt the traffic
  • Skip decryption for this traffic temporarily

To configure SSL decryption through a security policy, use the vManage security configuration wizard:
1. In Cisco vManage, select the Configuration > Security tab in the left side panel.
2. Click Add Security Policy. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
3. In Add Security Policy, select a scenario that supports the TLS/SSL Decryption feature (Compliance, Guest Access, Direct Cloud Access, Direct Internet Access, or Custom).
4. Click Proceed to add an SSL decryption policy in the wizard.
5. • If this is the first time you're creating a TLS/SSL decryption policy, then you must create and apply a policy to the device before creating security policies that can use a security policy (such as Intrusion Prevention, URL Filtering, or Advanced Malware Protection). In the Add Security Policy wizard, click Next until the TLS/SSL Decryption screen is displayed.
   • If you want to use TLS/SSL decryption along with other security features such as Intrusion Prevention, URL Filtering, or Advanced Malware Protection, add those features as described in this book. Once you've configured those features, click Next until the TLS/SSL Decryption screen is displayed.
6. Click the Add TLS/SSL Decryption Policy drop-down and choose Create New to create a new SSL decryption policy. The TLS/SSL Decryption Policy Configuration wizard appears.
7. Ensure that SSL Decryption is Enabled.
8. In the Policy Name field, enter the name of the policy.
9. Click on Add Rule to create a rule.
   The New Decryption Rule window is displayed.

   **Note**
   For branch-to-branch and branch-to-data center traffic scenarios that support service nodes, the SSL decryption security policy must be applied in a way that prevents the SSL flow from being inspected on both the devices.
10. Select the order for the rule that you want to create.
11. In the Name field, enter the name of the rule.
12. You can choose to decrypt traffic based on source / destination which is similar to the firewall rules or applications which is similar to URL-Filtering rules.

   • If you select Source / Destination, enter any of the following conditions:
     • Source VPNs
     • Source Networks
     • Source Ports
     • Destination VPNs
     • Destination Networks
     • Destination Port
     • Application/Application Family List

   • If you select URLs, enter the following:
     • VPNs
     • TLS/SSL profile.
     a. Enter a name for the profile.
     b. Select Decrypt, No Decrypt or Pass Through. Alternatively, you can select multiple categories and set the action for all of them using the actions drop-down.

13. (Optional) To configure advanced settings such as server certificate checks, minimum TLS version, and so on, expand Advanced Settings

   Note: By default, vManage configures the default values for each advanced setting. If you change any of these settings, it may affect the behaviour of the decryption security policies.

   • Under the Server Certificate Checks section, you can configure the following:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
</table>
   | Expired Certificate      | Defines what the policy should do if the server certificate is expired | • Drop the traffic
                                       |                                        | • Decrypt the traffic |
   | Untrusted Certificate    | Defines what the policy should do if the server certificate is not trusted | • Drop the traffic
                                       |                                        | • Decrypt the traffic |
   | Certificate Revocation Status | Defines whether Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate | Enabled or Disabled |
### Options

- **Drop the traffic**
- **Decrypt the traffic**

### Description

- Defines what the policy should do, if the OCSP revocation status is unknown.

### Field Name

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
</table>
| Unknown Revocation Status | Defines what the policy should do, if the OCSP revocation status is unknown. | - Drop the traffic 
- Decrypt the traffic |

### Under the Proxy Certificate Attributes section, you can configure the following:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
</table>
| RSA Keypair Modules | Defines the Proxy Certificate RSA Key modulus | - 1024 bit RSA 
- 2048 bit RSA 
- 4096 bit RSA |
| Certificate Lifetime (in Days) | Sets the lifetime of the proxy certificate in days. | - TLS 1.0 
- TLS 1.1 
- TLS 1.2 |
| Minimum TLS Version Revocation Status | Sets the minimum version of TLS that the proxy should support. | - TLS 1.0 
- TLS 1.1 
- TLS 1.2 |

### Under the Unsupported Mode Checks section, you can configure the following:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
</table>
| Unsupported Protocol Versions | Defines what the policy should do if an unsupported protocol version is detected. | - Drop the traffic 
- No Decrypt: The proxy does not decrypt this traffic. |
| Unsupported Cipher Suites | Defines what the policy should do if unsupported cipher suites are detected. | - Drop the traffic 
- No Decrypt: The proxy does not decrypt this traffic. |
| Failure Mode | Defines what the policy should do in the case of a failure. | - Close: Sets the mode as fail-close 
- Open: Sets the mode as fail-open. |
| Certificate Bundle | Defines whether the policy should use the default CA certificate bundle or not | You can select or deselect this option. If you deselect this option, the Custom Certificate Bundle option appears and you must upload a certificate by clicking Select a file. |
14. Click Save TLS/SSL Decryption Policy.
15. Click Next.
16. Enter Security Policy Name and Security Policy Description in the respective fields.
17. Click Save Policy to configure the Security policy.
18. You can edit the existing SSL decryption policy by clicking on Custom Options in the right-side panel of the vManage > Configuration > Security wizard.

**Apply a Security Policy to an XE SD-WAN Router**

1. In vManage NMS, select the Configuration > Templates screen.
2. If you are creating a new device template:
   a. In the Device tab, click Create Template.
   b. From the Create Template drop-down, select From Feature Template.
   c. From the Device Model drop-down, select one of the XE SD-WAN Routers.
   d. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.
3. If you are editing an existing device template:
   a. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   b. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
5. From the Security Policy drop-down, select the name of the security policy you configured in the above procedure.
6. Click Create (for a new template) or Update (for an existing template).

**Upload a Subordinate CA Certificate to TLS Proxy**

*Note* This procedure is applicable only if you configure the Enterprise CA for TLS proxy.
Prerequisites to Generate a CSR from the TLS Proxy Device

1. Configure Enterprise CA
2. Configure SSL Decryption
3. Apply a Security Policy to an XESD-WAN Router

Generate CSR and Upload Subordinate CA Certificate to TLS Proxy

1. In Cisco vManage, navigate to Configuration > Certificates.
2. Select TLS Proxy. The page shows a list of devices on which a CA certificate has been installed and the status of the certificates.
3. Select the device for which you want to generate CSR and click Download CSR at the top of the page. A pop-up window opens. You can copy or download the CSR. Ensure that the certificate that you request is downloaded in PEM format.
4. On your CA server, request a certificate and upload or paste the CSR file you generated in the previous step.
5. Download the certificate issued by your CA in PEM format.

Important

Ensure that the certificate you generate is a subordinate or an intermediate CA certificate. The procedure to generate a subordinate CA certificate may differ from one enterprise CA to another. The certificate generated in this step must have its constraint set as CA: TRUE.

Cisco IOS CA can’t be used for the TLS proxy feature as it doesn’t support generating a certificate with the constraint set as CA: TRUE.

6. Repeat steps 1 and 2.
7. Select the device and click Upload Certificate at the top of the page.
8. In the pop-up window that opens, upload or paste the PEM-encoded certificate that you generated from your CA server in step 5.
9. Click Upload and Save.
10. Verify that the certificate is installed on the device by running the command show crypto pki trustpoint PROXY-SIGNING-CA status on your device CLI.

Device# show crypto pki trustpoint PROXY-SIGNING-CA status
Trustpoint PROXY-SIGNING-CA:
   Issuing CA certificate configured:
      Subject Name:
         e=appqoe@cisco.com,cn=server-name,ou=AppQoE,o=CISCO,l=Blr,st=KA,c=IN
         Fingerprint MD5: 755C9485 DDACC0BD B5ED93E6 4E8A7DEB
         Fingerprint SHA1: 4D4380EA 07392044 6A5BF891 938AC610 C0C0AA6D
   Router General Purpose certificate configured:
      Subject Name:
         cn=sign
         Fingerprint MD5: 1956194E FEC057A3 8FE5BFA5 DD84662B
         Fingerprint SHA1: 864A8126 EBC780E2 D958AD86 93CB8923 3EF3B7FF
      State:
         Keys generated .............. Yes (General Purpose, non-exportable)
Verify Configuration

Use the following commands to verify the configuration for TLS proxy.

- **show sdwan running**: In Cisco vManage, run this command in **CLI mode** to verify if your configuration is applied.

- **show sdwan running-config**: In Cisco vManage, run this command by connecting to the device CLI through SSH.

- **show crypto pki status**: On your device CLI, run this command to verify that the PROXY-SIGNING-CA is present and configured correctly on the device.

- **show sslproxy statistics**: On your device CLI, run this command to view TLS proxy statistics.

- **show sslproxy status**: On your device CLI, run this command to verify whether TLS proxy was successfully configured and is enabled on Cisco vManage.

In the output below, **Clear Mode: FALSE** denotes that TLS proxy was successfully configured and enabled on Cisco vManage.

```
Configuration
-------------
CA Cert Bundle : /bootflash/vmanage-admin/sslProxyDefaultCAbundle.pem
CA TP Label : PROXY-SIGNING-CA
Cert Lifetime : 730
EC Key type : P256
RSA Key Modulus : 2048
Expired Cert : drop
Untrusted Cert : drop
Unknown Status : drop
 Unsupported Protocol Ver : drop
Unsupported Cipher Suites : drop
Failure Mode Action : close
Min TLS Ver : TLS Version 1.1

Status
------
SSL Proxy Operational State : RUNNING
TCP Proxy Operational State : RUNNING
Clear Mode : FALSE
```

- **show platform hardware qfp active feature utd config**: On your device CLI, run this command to verify the UTD data plane configuration

- **show sdwan running-configuration | section utd-tls-decrypt**: On your device CLI, run this command to verify the UTD data plane configuration

- **show utd engine standard config**: On your device CLI, run this command to verify the UTD service plane configuration

- **show utd engine standard status**: On your device CLI, run this command to verify the UTD service plane configuration
Monitor TLS Proxy Performance

This section describes how to monitor various parameters related to the performance of TLS proxy and TLS decryption.

Monitor TLS Proxy

1. Cisco vManage, navigate to Monitor > Network.
2. Select a device from the list of devices that displays.
3. Under the Application pane on the left, click SSL Proxy.
4. The upper part of the right pane has the following options to choose from.
   - **Traffic View**: From the drop-down menu, choose one of the following—All Policy Actions, Encrypted, Un-encrypted, Decrypted.
   - **Filter**: You have the option to filter the traffic statistics by VPN, TLOC, Remote TLOC, and Remote System IP.
   - **SSL Proxy View Format**: You can choose to view the SSL proxy information in form of a line graph, bar chart, or a pie chart.
   - **Time Range**: Choose to view the information for a specified time range (1h, 3h, 6h, and so on) or click Custom to define a time range.
5. Based on your selection, the information displays. For representation, we have only shown the information in form of a bar chart.

This example shows the data that the selected device encrypted and decrypted in the last 12 hours.

*Figure 4: SSL Proxy Information in a Bar Chart*

Additionally, on the SSL Proxy Monitoring page, the information is also displayed in tabular format below the bar chart.
Monitor SSL Decryption Statistics

1. Cisco vManage, navigate to Monitor > Network.

2. Select a device from the list of devices that displays.


4. The upper part of the right pane has the following options to choose from.
   - **Network Policy**: You can view the traffic information for an applied network policy.
   - **URL Policy**: You can view the traffic information of a URL policy.
   - **Time Range**: Choose to view the information for a specified time range (1h, 3h, 6h, and so on) or click Custom to define a time range.

5. Based on your selection, the information displays. For example, the network policy displays as in the following screenshot. This example shows the number of bytes that were transferred for the sequence rules 65535, 11, and 1.
Additionally, from the Security Monitoring pane, you can also view information for other Security features such as Firewall, Intrusion Prevention, URL Filtering, and so on. For example, the following image displays the Advanced Malware Protection page in the graph format:
Revoke and Renew Certificates

This section describes how to revoke and renew certificates issued by Enterprise CA, vManage as CA, and vManage as Subordinate CA.

Revoke Enterprise CA Certificate

Follow these steps to revoke, renew, or revoke and renew a certificate for a device configured as TLS proxy using Enterprise CA.

Revoke and Renew Certificate

1. In Cisco vManage, go to Configuration > Certificates.
2. Click the TLS Proxy tab at the top of the page.
   You will see a list of devices configured as CA.
3. Select the device (configured as Enterprise CA) for which you want to revoke or revoke and renew the certificate.
4. Click Revoke Certificate at the top of the page. A pop-up window opens.
5. From the drop-down menu, choose a reason for revoking the certificate. Select the check-box.
6. **Revoke:** To revoke the certificate, click the **Revoke** button. Beware that the revocation is permanent and cannot be rolled back. If you choose to revoke the certificate, no additional steps are required after this step.

---

**Note**

Revoking the certificate through Cisco vManage only removes the certificate from the device and invalidates the private key. You also need to revoke this certificate from your Enterprise CA.

---

**Revoke and Renew:** To revoke the existing certificate and upload a new one to replace it, click the **Revoke and Renew** button. To renew a certificate after revoking it, see steps 6-11 in the **Renew Certificate** section of this topic.

---

**Renew Certificate**

1. In Cisco vManage, go to **Configuration > Certificates**.

2. Click the **TLS Proxy** tab at the top of the page.

   You will see a list of devices configured as CA.

3. Select the device (configured as Enterprise CA) for which you want to revoke or revoke and renew the certificate.

4. Click **Renew Certificate** at the top of the page. A pop-up window opens.

5. Click **Yes** to continue with the renewal.

   In the status column, the status of the certificate changes to **CSR_Generated**.

6. Click **Download CSR** at the top of the page.

   A pop-up window opens. You can copy or download the CSR. Ensure that the certificate that you request is downloaded in PEM format.

7. On your CA server, request a certificate and upload or paste the CSR file you generated in the previous step.

8. Download the certificate issued by your CA in PEM format.

---

**Important**

Ensure that the certificate you generate is a subordinate or an intermediate CA certificate. The procedure to generate a subordinate CA certificate may differ from one enterprise CA to another. The certificate generated in this step must have its constraint set as **CA: TRUE**.

Cisco IOS CA can’t be used for the TLS proxy feature as it doesn’t support generating a certificate with the constraint set as **CA: TRUE**.

9. Click **Upload Certificate** at the top of the page.

10. In the pop-up window that opens, upload or paste the PEM-encoded certificate that you generated from your CA server in step 9.

11. Click **Upload and Save**.
vManage as CA or vManage as Intermediate CA

If you have configured vManage as CA or vManage as Intermediate CA, follow the steps below to revoke or renew a certificate.

1. In Cisco vManage, go to Configuration > Certificates.
2. Click the TLS Proxy tab at the top of the page.
   - You will see a list of devices configured as CA.
3. Select the device.
4. At the top of the page, click Revoke Certificate or Renew Certificate to revoke or renew the certificate respectively.
Cisco Umbrella Integration

The SD-WAN Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device. The security administrator configures policies on the Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). The router acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Umbrella cloud.

- Overview of Cisco SD-WAN Umbrella Integration, on page 113
- Restrictions for Umbrella Integration, on page 115
- Prerequisites for Umbrella Integration, on page 116
- Configure Umbrella API Token, on page 116
- Configure Cisco Umbrella Registration, on page 116
- Define Domain Lists, on page 117
- Configure Umbrella DNS Policy Using Cisco vManage, on page 117
- Attach DNS Umbrella Policy to Device Template, on page 118
- Umbrella Integration Using CLI, on page 119
- DNS Security Policy Configuration, on page 129
- Monitor Umbrella Feature, on page 130

Overview of Cisco SD-WAN Umbrella Integration

The Cisco SD-WAN Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through the device. When a host initiates the traffic and sends a DNS query, the Umbrella Connector in the device intercepts and inspects the DNS query. If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network. If it is for an external domain, it adds an Extended DNS (EDNS) record to the query and sends it to Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, Umbrella Cloud applies different policies to the DNS query.

The Umbrella Integration cloud, based on the policies configured on the portal and the reputation of the DNS Fully Qualified Domain Name (FQDN) may take one of the following actions:

- If FQDN is found to be malicious or blocked by the customized Enterprise Security policy, then the IP address of the Umbrella Cloud's blocked landing page is returned in the DNS response. This is called a blocked list action at Umbrella Cloud.

- If FQDN is found to be non-malicious, then the IP address of the content provider is returned in the DNS response. This is called a allowed list action at Umbrella Cloud.
If the FQDN is suspicious, then the intelligent proxy unicast IP addresses are returned in the DNS response. This is referred to as grey list action at Umbrella Cloud.

Figure 8: Umbrella Cloud

When the DNS response is received, the device forwards the response back to the host. The host will extract the IP address from the response and send the HTTP / HTTPS requests to this IP.

Note: The intelligent proxy option has to be enabled in the Umbrella dashboard for the Umbrella Resolver to return the intelligent proxy unicast IP addresses in the DNS response when an attempt is made to access the domains in the grey list.

Handling HTTP and HTTPS Traffic

With SD-WAN Umbrella Integration, HTTP and HTTPS client requests are handled in the following ways:

- If the Fully Qualified Domain Name (FQDN) in the DNS query is malicious (falls under blocked domains), Umbrella Cloud returns the IP address of the blocked landing page in the DNS response. When the HTTP client sends a request to this IP, Umbrella Cloud displays a page that informs the user that the requested page was blocked and the reason for blocking the page.

- If the FQDN in the DNS query is non-malicious (falls under allowed listed domains), Umbrella Cloud returns the IP address of the content provider. The HTTP client sends the request to this IP address and gets the desired content.

- If the FQDN in the DNS query falls under grey-listed domains, Umbrella Resolver returns the unicast IP addresses of intelligent proxy in the DNS response. All HTTP traffic from the host to the grey domain gets proxied through the intelligent proxy and undergo URL filtering.

One potential limitation in using intelligent proxy unicast IP addresses is the probability of the datacenter going down when the client is trying to send the traffic to the intelligent proxy unicast IP address. This is a scenario where a client has completed DNS resolution for a domain which falls under grey-listed domain and client’s HTTP(S) traffic is being sent to one of the obtained intelligent proxy unicast IP address. If that datacenter is down, then the client has no way of knowing it.
The Umbrella Connector does not act on the HTTP and HTTPS traffic. The connector does not redirect any web traffic or alter any HTTP/(S) packets.

**Encrypting the DNS Packet**

The DNS packet sent from the device to Umbrella Integration server must be encrypted if the EDNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, device decrypts the packet and forwards it to the host. You can encrypt DNS packets only when the DNSencrypt feature is enabled on the device.

The device uses the following Anycast recursive Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

**Figure 9: Umbrella Integration Topology**

![Umbrella Integration Topology](image)

**Restrictions for Umbrella Integration**

- If an application or host uses IP address directly instead of DNS to query domain names, policy enforcement is not applied.

- When the client is connected to a web proxy, the DNS query does not pass through the device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Umbrella portal.

- When the Umbrella Integration policy blocks a DNS query, the client is redirected to a Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Umbrella portal.

- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Umbrella cloud for further inspection.
• Only the IPv4 address of the host is conveyed in the EDNS option.
• A maximum of 64 local domains can be configured under bypass list, and the allowed domain name length is 100 characters.

Prerequisites for Umbrella Integration

Before you configure the Umbrella Integration feature, ensure that the following are met:

• The device has a security K9 license to enable Umbrella Integration.
• The device runs on the SD-WAN IOS XE 16.10 software image or later.
• SD-WAN Umbrella subscription license is available.
• The device is set as the default DNS server gateway and needs to ensure that the DNS traffic goes through the device.

Configure Umbrella API Token

To configure Umbrella API token:

1. In Cisco vManage, navigate to the Configuration > Security.
2. Click Custom Options on the right side to configure the Umbrella API.
3. Select Umbrella API Token.
4. Enter token number in the Umbrella Token field.
5. Click Save Changes to configure the Umbrella API Token.

Configure Cisco Umbrella Registration

Table 14: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-registration for Cisco Umbrella</td>
<td>Cisco IOS XE Release</td>
<td>This feature adds the ability to register devices to Cisco Umbrella using the Smart Account credentials to automatically retrieve Umbrella</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>Amsterdam 17.2.1r</td>
<td>credentials (organization ID, registration key, and secret). This offers a more automatic alternative to manually copying a registration token from Umbrella.</td>
</tr>
</tbody>
</table>
Use this procedure to configure Cisco Umbrella registration globally for all devices. The procedure retrieves the Umbrella registration parameters automatically.

When configuring individual policies, it is also possible to configure Umbrella registration, but it can be managed more flexibly using the following procedure:

1. In vManage, select Configuration > Security.
2. Click Custom Options and select Umbrella Registration.
3. In the Manage Umbrella Registration dialog box, use one of the following methods to register devices to Umbrella. The registration details are used globally.
   - Cisco Umbrella Registration Key and Secret
     a. Click the Get Keys button to retrieve Umbrella registration parameters automatically: Organization ID, Registration Key, and Secret.

   **Note** To automatically retrieve registration parameters, Cisco vManage uses the Smart Account credentials to connect to the Umbrella portal. The Smart Account credentials are configured in Cisco vManage under Administration > Settings > Smart Account Credentials.

   b. (Optional) If the Umbrella keys have been rotated and the details that are automatically retrieved are incorrect, enter the details manually.
   c. Click Save Changes.

   - Cisco Umbrella Registration Token
     (For legacy devices only) Enter a registration token (40 hexadecimal digits) provided by Umbrella.

**Define Domain Lists**

1. In Cisco vManage, select Configuration > Security
2. Click Custom Options button at the right and choose Lists from the drop-down options.
3. Choose Domain from the left pane.
4. Click New Domain List to create a new domain list or select the domain name and click the pencil icon on the right side for an existing list.
5. Enter the Domain List Name, Add Domain, and click Add to create the list.

**Configure Umbrella DNS Policy Using Cisco vManage**

1. In Cisco vManage, select Configuration > Security.
2. Click Add Security Policy.

4. Click Proceed.

5. Click Next until you reach the DNS Security tab.

6. Click the Add DNS Security Policy drop-down button and choose one of the following:
   - Copy from Existing: Choose a Policy from the drop-down, enter Policy Name and click Copy.

7. If you are creating a new policy using the Create New option, the DNS Security - Policy Rule Configuration wizard appears.

8. Enter a policy name in the Policy Name field.

9. The Umbrella Registration Status displays the status of the API Token configuration.

10. Click Manage Umbrella Registration to add a token, if you don't have one added.

11. Select the Match All VPN option if you need to keep the same configuration for all the available VPNs and continue with Step 13.
   Or select Custom VPN Configuration if you need to add target VPNs to your policy. A Target VPNs wizard appears.

12. To add target VPNs, click Target VPNs at the top of the page

13. Click Save Changes to add the VPN.

14. Choose the domain bypass from the Local Domain Bypass List drop-down list.

15. Configure the DNS Server IP from the following options:
   - Umbrella Default
   - Custom DNS

16. Click the Advanced tab to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.

17. Click Save DNS Security Policy. The Configuration > Security screen then displays, and the DNS Policy list table includes the newly created DNS Security Policy.

---

**Attach DNS Umbrella Policy to Device Template**

1. In Cisco vManage, select Configuration > Templates screen.

2. In the Device tab, select From Feature Template from the Create Template drop-down.

3. From the Device Model drop-down, choose a device.

4. Click Additional Templates. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down list, choose the name of the Umbrella DNS Security Policy you configured in the above procedure.

6. Click Create to apply the Umbrella policy to a device template.
Umbrella Integration Using CLI

Configure the Umbrella Connector

Communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a DigiCert root certificate which is auto installed on the router by default.

To configure Umbrella Connector:

- Get the API token from the Umbrella portal.
- Define VRFs and each VRF can have two options: DNS resolver and enabling local domain list.
  - Umbrella registration is done per VRF only if DNS resolver is configured as Umbrella.
  - Local domain bypass list is global and each VRF can enable or disable the local domain bypass list.
    If enabled, the DNS packet will be matched against the local domain list.

- Umbrella is a Direct Internet Access (DIA) feature, so NAT configuration is mandatory.

Sample configuration:

```
Device(config-profile)# vrf 9
Device(config-profile-vrf)# dns-resolver 8.8.8.8
Device(config-profile-vrf)# match-local-domain
Device(config)# parameter-map type umbrella global
Device(config)# token 648BF6139C379DCCFFBA637FD1E22755001CE241
Device(config)# local-domain dns_bypass
Device(config)# dns-resolver 8.8.8.8
Device(config)# udp-timeout 5
Device(config)# vrf 9
Device(config)# dns-resolver 8.8.8.8
Device(config)# vrf 19
Device(config)# dns-resolver 8.8.8.8
```

```
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.cisco.com
Device(config)# pattern www.amazon.com
Device(config)# pattern .*sales.abc.*
```

Security Configuration Guide, Cisco IOS XE Release 17
no match-local-domain
vrf 29
dns-resolver umbrella
match-local-domain
vrf 39
dns-resolver umbrella
no match-local-domain

The following table captures the per VRF DNS packet behavior:

<table>
<thead>
<tr>
<th>VRF</th>
<th>dns-resolver</th>
<th>Match-local-domain (dns_bypass)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>8.8.8.8</td>
<td>Yes</td>
</tr>
<tr>
<td>19</td>
<td>8.8.8.8</td>
<td>No</td>
</tr>
<tr>
<td>29</td>
<td>umbrella</td>
<td>Yes</td>
</tr>
<tr>
<td>39</td>
<td>umbrella</td>
<td>No</td>
</tr>
</tbody>
</table>

The VRFs must be preconfigured. For example, the VRFs 9, 19, 29, 39 are preconfigured in the above example.

**Note**

Sample NAT config for DIA internet connectivity:

ip access-list extended dia-nat-acl
10 permit ip any any
ip nat inside source list dia-nat-acl interface <WAN-facing-Interface> overload
“ip nat outside” MUST be configured under <WAN-facing-Interface>

**Configure the Device as a Pass-through Server**

You can identify the traffic to be bypassed using domain names. In the SD-WAN device, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the device matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

Device# config-transaction
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.cisco.com
Device(config)# pattern www.amazon.com
Device(config)# pattern .*sales.abc.*

**DNSCrypt, Resolver, and Public-key**

When you configure the device using the parameter-map type umbrella global command, the following values are auto-populated:

- DNSCrypt
- Public-Key

**Public-key**

Public-key is used to download the DNSCrypt certificate from Umbrella Integration cloud. This value is preconfigured to...
which is the public-key of Umbrella Integration Anycast servers. If there is a change in the public-key and if
you modify this command, then you have to remove the modified command to restore the default value. If
you modify the value, the DNSCrypt certificate download may fail.

DNSCrypt

DNSCrypt is an encryption protocol to authenticate communications between the device and the Umbrella
Integration. When the parameter-map type umbrella is configured and enabled by default on all WAN
interfaces. DNSCrypt gets triggered and a certificate is downloaded, validated, and parsed. A shared secret
key is then negotiated, which is used to encrypt the DNS queries. For every hour this certificate is automatically
downloaded and verified for an upgrade, a new shared secret key is negotiated to encrypt the DNS queries.

To disable DNSCrypt, use the no dnsencrypt command and to re-enable DNSCrypt, use the dnsencrypt command.

When the DNSCrypt is used, the DNS request packets size is more than 512 bytes. Ensure that these packets
are allowed through the intermediary devices; otherwise, the response may not reach the intended recipients.

Sample umbrella dnsencrypt notifications:

```
Device# show sdwan umbrella dnsencrypt
DNSCrypt: Enabled
Certificate Update Status:
  Last Successfully Attempt: 08:46:32 IST May 21 2018
Certificate Details:
  Certificate Magic : DNSC
  Major Version : 0x0001
  Minor Version : 0x0000
  Query Magic : 0x714E7A696D657555
  Serial Number : 1517943461
  Start Time : 1517943461 (00:27:41 IST Feb 7 2018)
  End Time : 1549479461 (00:27:41 IST Feb 7 2019)
When disabled:
Device# show umbrella dnsencrypt
DNSCrypt: Not enabled
  Public-key: NONE
```

```
Sample configuration steps for dns-resolver and match-local-domain-to-bypass per vrf:
Router(config)# vrf definition 1
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# ?
Possible completions:
  dnsencrypt
  local-domain
  public-key
  registration-vrf
  resolver
token
udp-timeout
vrf
Router(config-profile)# vrf ?
```
This line doesn't have a valid range expression
Possible completions:
<name:string, min: 1 chars, max: 32 chars> 1
Router(config-profile)# vrf 1
Router(config-profile-vrf)# ?
Possible completions:
dns-resolver
  match-local-domain-to-bypass
Router(config-profile-vrf)# dns-resolver umbrella
Router(config-profile-vrf)# match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router(config)# vrf definition 2
Router(config-ipv4)# exit-address-family ipv4
Router(config-ipv4)# exit
Router(config-profile-vrf)# parameter-map type umbrella global
Router(config-profile-vrf)# vrf 2
Router(config-profile-vrf)# dns-resolver 8.8.8.8
Router(config-profile-vrf)# no match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router#sh umbrella config
Umbrella Configuration
========================
Token: AAC1A2555C11B2B7968FF3AF27C2FB8F001CB7B2
OrganizationID: 1882034
Local Domain Regex parameter-map name: NONE
DNSCrypt: Enabled
UDP Timeout: 5 seconds
Resolver address:
  1. 208.67.220.220
  2. 208.67.222.222
  3. 2620:119:53::53
  4. 2620:119:35::35
Registration VRF: default
VRF List:
  1. VRF 1 (ID: 1)
     DNS-Resolver: umbrella
     Match local-domain-to-bypass: Yes
  2. VRF 2 (ID: 3)
     DNS-Resolver: 8.8.8.8
     Match local-domain-to-bypass: No

Verify the Umbrella Connector Configuration

Verify the Umbrella Connector configuration using the following commands:

Device# show umbrella config
Umbrella Configuration
------------------------
Token: 648BF6139C379DCFFBA637FD1E22755001CE241
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Enabled
UDP Timeout: 5 seconds
Resolver address:
1. 208.67.220.220
2. 208.67.222.222
3. 2620:119:53::53
4. 2620:119:35::35

Registration VRF: default
VRF List:
1. VRF 9 (ID: 4)
   DNS-Resolver: 8.8.8.8
   Match local-domain: Yes
2. VRF 19 (ID: 1)
   DNS-Resolver: 8.8.8.8
   Match local-domain: No
3. VRF 29 (ID: 2)
   DNS-Resolver: umbrella
   Match local-domain: Yes
4. VRF 39 (ID: 3)
   DNS-Resolver: umbrella
   Match local-domain: No

The output of VRF will have name and ID. The ID here is VRF ID:
Device# show vrf detail | inc VRF Id
VRF 19 (VRF Id = 1); default RD <not set>; default VPNID <not set>
VRF 29 (VRF Id = 2); default RD <not set>; default VPNID <not set>
VRF 39 (VRF Id = 3); default RD <not set>; default VPNID <not set>
VRF 9 (VRF Id = 4); default RD <not set>; default VPNID <not set>

When DNSCrypt is disabled:
Device# show umbrella config
Umbrella Configuration

Token: 64BF6139C379DCFFBA637FD1E22755001CE241
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
1. 208.67.220.220
2. 208.67.222.222
3. 2620:119:53::53
4. 2620:119:35::35

Registration VRF: default
VRF List:
1. VRF 9 (ID: 4)
   DNS-Resolver: 8.8.8.8
   Match local-domain: Yes
2. VRF 19 (ID: 1)
   DNS-Resolver: 8.8.8.8
   Match local-domain: No
3. VRF 29 (ID: 2)
   DNS-Resolver: umbrella
   Match local-domain: Yes
4. VRF 39 (ID: 3)
   DNS-Resolver: umbrella
   Match local-domain: No

Display Umbrella Registration Details

The following example displays the device registration information:
Device# show sdwan umbrella device-registration
Device registration details
VRF  Tag   Status      Device-id29
devicen29  200  SUCCESS  010a9b2b0d5cb21f39
vpn39  200  SUCCESS  010a1a2e1989da19
The following example displays the device registration information in detail:
Device# show umbrella deviceid detailed
Device registration details
1.29
Tag : vpn29
Device-id : 010a9b2b0d5cb21f
Description : Device Id recieved successfully
WAN interface : None
2.39
Tag : vpn39
Device-id : 010a1a2e1989da19
Description : Device Id recieved successfully
WAN interface : None

**Umbrella show commands at FP Layer**

The **show platform software umbrella f0 config** command displays all the local domains configured for Open DNS in the FP Layer.

Device# show platform software umbrella f0 config
+++ Umbrella Config +++
Umbrella feature:
------------------
Init: Enabled
Dnsencrypt: Enabled
Timeout: 5
------------------
udp timeout: 5
OrgId :
------------------
orgid : 1892929
Resolver config:
RESOLVER IP's
---------------------
208.67.220.220
208.67.222.222
208.67.119:35:35
208.67.119:35:35
Dnsencrypt Info:
public_key:
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461
ProfileID DeviceID Mode Resolver Local-Domain Tag
------------------------------------------------------------------------------
0 OUT False 8.8.8.8 True vpn9
1 IN 8.8.8.8 True vpn39
2 010a9b2b0d5cb21f IN 8.8.8.8 True vpn29
3 010a1a2e1989da19 IN 8.8.8.8 True vpn29

The **show platform software umbrella f0 local-domain** displays the local domain list.
Device# show platform software umbrella f0 local-domain
01. www.cisco.com
02. www.amazon.com
03. .*sales.abc.*
Umbrella show commands at CPP Layer

The show platform hardware qfp active feature umbrella client config command displays the configuration in CPP layer.

```plaintext
+++ Umbrella Config +++
Umbrella feature:
--------------
Init: Enabled
Dnscrypt: Enabled
Timeout:
----------
udp timeout: 5
Orgid:
-------
orgid: 1892929
Resolver config:
--------------
RESOLVER IP's
  208.67.220.220
  208.67.222.222
  2620:119:53::53
  2620:119:35::35
Dnscrypt Info:
--------------
public_key:
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461

Umbrella Interface Config:
--------------------------
11 GigabitEthernet4 :
  Mode : IN
  DeviceID : 010a9b2b0d5cb21f
  Tag : vpn29
10 GigabitEthernet3 :
  Mode : IN
  DeviceID : 0000000000000000
  Tag : vpn9
05 Null0 :
  Mode : OUT
06 VirtualPortGroup0 :
  Mode : OUT
07 VirtualPortGroup1 :
  Mode : OUT
08 GigabitEthernet1 :
  Mode : OUT
09 GigabitEthernet2 :
  Mode : OUT
12 GigabitEthernet5 :
  Mode : OUT

Umbrella Profile Deviceid Config:
----------------------------------
ProfileID: 0
  Mode : OUT
ProfileID: 1
  Mode : IN
  Resolver : 8.8.8.8
  Local-Domain: False
  DeviceID : 0000000000000000
  Tag : vpn19
```
ProfileID: 3
  Mode : IN
  Resolver : 208.67.220.220
  Local-Domain: False
  DeviceID : 010a1a2e1989da19
  Tag : vpn39

ProfileID: 4
  Mode : IN
  Resolver : 8.8.8.8
  Local-Domain: True
  DeviceID : 0000000000000000
  Tag : vpn9

ProfileID: 2
  Mode : IN
  Resolver : 208.67.220.220
  Local-Domain: True
  DeviceID : 010a9b2b0d5cb21f
  Tag : vpn29

Umbrella Profile ID CPP Hash:
----------------------------------------

VRF ID :: 1
  VRF NAME : 19
  Resolver : 8.8.8.8
  Local-Domain: False

VRF ID :: 4
  VRF NAME : 9
  Resolver : 8.8.8.8
  Local-Domain: True

VRF ID :: 2
  VRF NAME : 29
  Resolver : 208.67.220.220
  Local-Domain: True

VRF ID :: 3
  VRF NAME : 39
  Resolver : 208.67.220.220
  Local-Domain: False

Umbrella Data-Plane show commands

The show platform hardware qfp active feature umbrella datapath stats command displays the umbrella statistics in data plane.

Device# show platform hardware qfp active feature umbrella datapath stats

Umbrella Connector Stats:
  Parser statistics:
    parser unknown pkt: 0
    parser fmt error: 0
    parser count nonzero: 0
    parser pa error: 0
    parser non query: 0
    parser multiple name: 0
    parser dns name err: 0
    parser matched ip: 0
    parser opendns redirect: 0
    local domain bypass: 0
    parser dns others: 0
    no device id on interface: 0
    drop erc dnsencrypt: 0
    regex locked: 0
    regex not matched: 0
    parser malformed pkt: 0

Flow statistics:
feature object allocs : 0
feature object frees : 0
flow create requests : 0
flow create successful: 0
flow create failed, CFT handle: 0
flow create failed, getting FO: 0
flow create failed, malloc FO : 0
flow create failed, attach FO : 0
flow create failed, match flow: 0
flow create failed, set aging : 0
flow lookup requests : 0
flow lookup successful: 0
flow lookup failed, CFT handle: 0
flow lookup failed, getting FO: 0
flow lookup failed, no match : 0
flow detach requests : 0
flow detach successful: 0
flow detach failed, CFT handle: 0
flow detach failed, getting FO: 0
flow detach failed freeing FO : 0
flow detach failed, no match : 0
flow ageout requests : 0
flow ageout failed, freeing FO: 0
flow ageout failed, freeing FO: 0
flow ipv4 ageout requests : 0
flow ipv6 ageout requests : 0
flow update requests : 0
flow update successful: 0
flow update failed, CFT handle: 0
flow update failed, getting FO: 0
flow update failed, no match : 0

DNSCrypt statistics:
bypass pkt: 0
clear sent: 0
enc sent: 0
clear rcvd: 0
dec rcvd: 0
pa err: 0
enc lib err: 0
padding err: 0
nonce err: 0
flow bypass: 0
disabled: 0
flow not enc: 0
DCA statistics:
dca match success: 0
dca match failure: 0

The `show platform hardware qfp active feature umbrella datapath memory` command displays CFT information.

Device# show platform hardware qfp active feature umbrella datapath memory
==Umbrella Connector CFT Information==
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
==Umbrella Connector Runtime Information==
umbrella init state 0x4
umbrella dsa client handler 0x2

The `show platform hardware qfp active feature umbrella datapath runtime` command displays internal information. For example, key index used for DNSCrypt.

Device# show platform hardware qfp active feature umbrella datapath runtime
udpflow_ageout: 5
ipv4_count: 2
ipv6_count: 2
ipv4_index: 0
Umbrella IPv4 Anycast Address
IP Anycast Address0: 208.67.220.220
IP Anycast Address1: 208.67.222.222

Umbrella IPv6 Anycast Address
IP Anycast Address0: 2620:119:53:0:0:0:0:53
IP Anycast Address1: 2620:119:35:0:0:0:0:35

-DNSCrypt-
- key [0] -
  sn: 1517943461
  ref cnt: 0
  magic: 714e7a696d657555
- key [1] -
  sn: 0
  ref cnt: 0
  magic: 0000000000000000
  Client Public Key: 0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000
  NM Key Hash: 0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0000

Local domain 1
VPN-DEVICEID TABLE d7f37410

Clear Command
The clear platform hardware qfp active feature umbrella datapath stats command clears the Umbrella connector statistics in datapath.

Device# clear platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats Cleared

Troubleshooting the Umbrella Integration

Troubleshoot issues that are related to enabling the Umbrella Integration feature using these commands:

- debug umbrella device-registration
- debug umbrella config
- debug umbrella dnscrypt

Depending on the OS, run either of these two commands from the client device:

- The nslookup -type=txt debug.umbrella.com command from the command prompt of the Windows machine
- The nslookup -type=txt debug.umbrella.com command from the terminal window or shell of the Linux machine

nslookup -type=txt debug.opendns.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
  debug.opendns.com text = "server r6.mum1"
  debug.opendns.com text = "device 010A826AAB6C30"
  debug.opendns.com text = "organization id 1892929"
  debug.opendns.com text = "remoteip 171.168.1.7"
DNS Security Policy Configuration

### Domain List

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Possible Completions</th>
<th>Description and possible input values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy lists local-domain-list</code></td>
<td></td>
<td>List of domain name regular expression patterns</td>
</tr>
<tr>
<td><code>&lt;name&gt;</code></td>
<td></td>
<td>Domain name regular expression pattern string. For example, policy lists local-domain-list name as google.com.</td>
</tr>
</tbody>
</table>

### Umbrella Registration

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Possible Completions</th>
<th>Description and possible input values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>security umbrella</code></td>
<td></td>
<td>Configure Umbrella service related security properties.</td>
</tr>
<tr>
<td><code>api-key</code></td>
<td></td>
<td>Config umbrella api-key. The value ranges from 1 to 64 characters.</td>
</tr>
<tr>
<td><code>dnscrypt</code></td>
<td></td>
<td>Enable DNScrypt while redirecting DNS requests to Umbrella.</td>
</tr>
<tr>
<td><code>orgid</code></td>
<td></td>
<td>Config umbrella org id</td>
</tr>
<tr>
<td><code>secret</code></td>
<td></td>
<td>Config umbrella secret. The value can be [0</td>
</tr>
<tr>
<td><code>token</code></td>
<td></td>
<td>Umbrella service registration token. The value ranges from 1 to 64 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Possible Completions</th>
<th>Description and possible input values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpn &lt;number, range&gt;</code></td>
<td></td>
<td>List of domain name regular expression patterns</td>
</tr>
<tr>
<td><code>dns-redirect</code></td>
<td></td>
<td>Bypass the dns redirect for entries in the local domain list</td>
</tr>
<tr>
<td><code>match-local-domain-to-bypass</code></td>
<td></td>
<td>Use Umbrella as DNS redirect service.</td>
</tr>
<tr>
<td><code>dns-redirect umbrella</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DNS-Security Policy with Domain List

```
policy
lists
  local-domain-list domain-list
    google.com
  !
  exit
  !
  exit
  !
security
  umbrella
    dnscrypt
  !
  exit
  !
vpn matchAllVpn
dns-redirect umbrella match-local-domain-to-bypass
```

Monitor Umbrella Feature

You can monitor the registered VPNs, DNSCrypt status, packet counts for required timestamps on an Umbrella configured router using the following steps.

To monitor the status of Umbrella DNS Configuration on a device:

1. In Cisco vManage, select Monitor > Network.
2. To choose a device, click the one of the devices listed under the Hostname column.
3. In the left panel, under Security Monitoring, click Umbrella DNS Re-direct. The Umbrella DNS Re-direct tab displays the number of packets that are redirected to configured DNS server.
4. Click the Local Domain Bypass tab to view the number of packets that are bypassed from DNS server.
CHAPTER 10

Integrate With Secure Internet Gateways

Table 15: Feature History

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Automatic Tunneling to Secure Internet Gateways</td>
<td>Cisco IOS XE Release Amsterdam 17.2.1r</td>
<td>This feature allows you to integrate your routers with a Secure Internet Gateway to perform security processing and ensure that your device's performance is not affected by processing security rules.</td>
</tr>
</tbody>
</table>

SD-WAN branch routers can support SD-WAN, routing, security and other LAN access features that can be managed centrally. On high-end devices, all these features can be provided as well the required scale and performance for large enterprises. However, on lower-end devices not all security features can be enabled simultaneously without degrading performance. These routers can integrate with Secure Internet Gateways (SIG) which do the majority of the processing to secure enterprise traffic. When the SIG is set up, all LAN and WiFi client traffic, based on routing or policy, is forwarded to the SIG. In addition, the SIG can also protect roaming users, mobile users, and BYOD use-cases. On Cisco IOS XE SD-WAN devices, Cisco SD-WAN supports automatically tunneling to Cisco Umbrella as a SIG.

This chapter contains the following sections:

- Create the SIG Template, on page 133
- Attach the SIG Template to Devices, on page 136
- Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage, on page 136

Create the SIG Template

To create a device template:

1. Navigate to Configuration > Templates

2. In the Device tab, click the Create Template drop-down and select From Feature Template.

3. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

6. Click Transport & Management VPN.

7. Under the Additional Cisco VPN 0 Templates, click Cisco Secure Internet Gateway.

8. Select the Cisco Secure Internet Gateway drop-down.

9. If you have previously created a template that you want to use, select that template. If not, click Create Template.

The Add Template form for Cisco Secure Internet Gateway (SIG) is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining feature parameters.

10. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

11. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.

12. In the Configuration pane, as the SIG Provider, ensure that Umbrella is selected.

13. Under Basic Settings, enter the following:

   a. In the Interface Name and Source Interface fields, note the following

   Table 16:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value from 1 to 255, and apply that value to all devices.</td>
</tr>
</tbody>
</table>
### Create the SIG Template

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click Device Specific, the Enter Key box opens. This box displays the key, which is the unique string that identifies the parameter in a CSV file that you create. By default, the keys are as follows:  
• Interface Name: tunnel_if_name  
• Source Interface: tunnel_source_interface  
This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template.  
To change the default key, type a new string and move the cursor out of the Enter Key box. |

14. For Data-Center, select **Primary** or **Secondary**.

15. Click **Add** to add the tunnel.

16. If required, add additional tunnels.

17. In the High Availability pane, do the following:
   - For the Active tunnel, you must select one of the tunnels that you created.
   - For the Backup tunnel, you can either one of the tunnels that you created or **None**. If you select **None**, there will be no back up tunnel to your SIG.

18. Click **Additional Templates** or scroll down to the Additional Templates section.

19. Select the Cisco SIG Credentials drop-down.

20. If you have previously created a template that you want to use, select that template. If not, click **Create Template**.

   The Add Template form for Cisco SIG Credentials is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining feature parameters.

21. Under the Basic Details section, click **Get Keys** to get the Organization ID, Registration Key, and Secret.

   **Note**: To automatically retrieve registration parameters, Cisco vManage uses the Smart Account credentials to connect to the Cisco Umbrella portal. The Smart Account credentials are configured in Cisco vManage in **Administration > Settings > Smart Account Credentials**

22. Click **Save**.
23. For all other fields, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.

24. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

## Attach the SIG Template to Devices

To attach one or more devices to the device template:

1. In the Device tab, select the template that you created.

2. Click the More Actions icon to the right of the row and click Attach Devices. The Attach Devices dialog box opens with the Select Devices tab selected.

3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click Select All.

4. Click the arrow pointing right to move the device to the Selected Devices column on the right.

5. Click Attach.

6. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking the More Actions icon to the right of the row and clicking Edit Device Template. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click Import File in the upper right corner of the screen to upload a CSV file that lists all the variables and defines each variable's value for each device.

7. Click Update

## Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage

### Table 17: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Configuration for GRE Tunnels and IPsec Tunnels</td>
<td>Cisco IOS XE Release Amsterdam 17.2.1r</td>
<td>This feature lets you manually configure a GRE tunnel by using the Cisco VPN Interface GRE template or an IPSec tunnel by using the Cisco VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.</td>
</tr>
</tbody>
</table>
Configure a GRE Tunnel from Cisco vManage

This section describes how to manually create a GRE tunnel from Cisco vManage. This procedure lets you configure a GRE tunnel to a third-party vendor.

1. Perform these actions to create a GRE template:
   a. In Cisco vManage NMS, select the Configuration > Templates screen.
   b. In the Feature tab, click Add Template.
   c. Select the type of device for which you are creating the template.
   d. Select the Cisco VPN Interface GRE template from the group of VPN templates.
   e. In the Basic Configuration tab, configure parameters as desired, and then click Save.

2. Perform these actions to create a GRE route:
   a. In the Feature tab on the Templates screen, click Add Template.
   b. Select the type of device for which you are creating the template.
   c. Select the Cisco VPN template in the group of VPN templates.
   d. Select the GRE route tab.
   e. Click New GRE Route.
   f. Configure parameters as desired, and then click Add.

3. Perform these actions to configure a device template for the GRE interface.
   a. In the Device tab on the Templates screen, click More Options (…) and select Edit for the device template that you want to configure.
   b. Select the Transport & Management VPN tab.
   c. From the Additional Cisco VPN 0 Templates list on the right, select the Cisco VPN Interface GRE template.
   d. From the Cisco VPN Interface GRE drop-down, click Create Template.
   e. Configure the templates as desired, and then click Save.

Configure an IPsec Tunnel from Cisco vManage

This section describes how to manually create an IPsec tunnel from Cisco vManage. This procedure lets you configure an IPsec tunnel to a third-party vendor.

1. Perform these actions to create an IPsec template:
   a. In Cisco vManage NMS, select the Configuration > Templates screen.
   b. In the Feature tab, click Add Template.
   c. Select the type of device for which you are creating the template.
d. Select the Cisco VPN Interface IPsec template from the group of VPN templates.

e. In the Basic Configuration tab, configure parameters as desired, and then click **Save**.

2. Perform these actions to create an IPsec route:

   a. In the Feature tab on the Templates screen, click **Add Template**.
   
   b. Select the type of device for which you are creating the template.
   
   c. Select the Cisco VPN template in the group of VPN templates.
   
   d. Select the IPSEC route tab.
   
   e. Click **New IPSEC Route**.
   
   f. Configure parameters as desired, and then click **Add**.

3. Perform these actions to configure a device template for the IPsec interface.

   a. In the Device tab on the Templates screen, click More Options (…) and select **Edit** for the device template that you want to configure.
   
   b. Select the Transport & Management VPN tab.
   
   c. From the Additional Cisco VPN 0 Templates list on the right, select the Cisco VPN Interface IPsec template.
   
   d. From the Cisco VPN Interface IPsec drop-down, click **Create Template**.
   
   e. Configure the templates as desired, and then click **Save**.
vManage uses a Security Virtual Image to enable security features such as IPS, URL-Filtering, and AMP on Cisco IOS XE SD-WAN Devices. Before you use these features, you must upload the relevant Security Virtual Image to vManage. After upgrading the software on the device, you must also upgrade the Security Virtual Image.

This chapter describes how to perform these tasks.

- Identify the Recommended Security Virtual Image Version, on page 139
- Upload the Cisco Security Virtual Image to vManage, on page 140
- Upgrade a Security Virtual Image, on page 141

**Identify the Recommended Security Virtual Image Version**

At times, you may want to check the recommended Security Virtual Image (SVI) release number for a given router. To check this using vManage:

1. From the vManage dashboard, select Monitor > Network.
2. Choose WAN – Edge.
3. Select the device that will run the SVI.
   The System Status page displays.
4. Scroll to the bottom of the device menu, and click Real Time.
   The System Information page displays.
5. Click the Device Options field, and select Security App Version Status from the menu list.
Step 6 Note the image name in the Recommended Version column. It should match the available SVI for your router from the Cisco downloads website.

Upload the Cisco Security Virtual Image to vManage

Each router image supports a specific range of versions for a hosted application. For IPS/IDS and URL-Filtering, you can find the range of supported versions (and the recommended version) for a device on its Device Options page.
Step 1: From the Software Download page for your router, locate the image "UTD Engine for IOS XE SD-WAN."

Step 2: Click the download icon on the right-hand side of the window to download the image file.

Step 3: From the vManage dashboard, select Maintenance > Software Repository.

Step 4: Select Virtual Images from the top options.

Step 5: Click Upload Virtual Image, and select either vManage or Remote Server – vManage. The Upload Virtual Image to vManage window opens.

Step 6: Drag and drop, or browse to the image file and select it.

Step 7: Click Upload. When the upload completes, a confirmation message displays. The new virtual image displays in the Virtual Images Software Repository.

Upgrade a Security Virtual Image

When a Cisco IOS-XE SD-WAN router is upgraded to a new software image, the security virtual image must also be upgraded to match.

Note: If the IPS Signature Update option is enabled, the matching IPS signature package is automatically updated as a part of the upgrade. You can enable the setting from Administration > Settings > IPS Signature Update.
To upgrade the application hosting virtual image for a device, follow these steps:

**Step 1** Follow the steps in "Upload the Correct Cisco Security Virtual Image to vManage" to download the recommended version of the SVI for your router. Note the version name.

**Step 2** From the vManage menu, select **Maintenance > Software Repository > Virtual Images** to verify that the image version listed under the Recommended Version column matches a virtual image listed in the Virtual Images table.

**Step 3** Select **Maintenance > Software Upgrade**. The WAN Edge Software upgrade page displays.

**Step 4** Select the devices you want to upgrade by clicking the boxes in the leftmost column. When you have selected one or more devices, a row of options display, as well as the number of rows you selected.

**Step 5** When you are satisfied with your choices, select **Upgrade Virtual Image** from the options menu. The Virtual Image Upgrade dialog box opens.

**Step 6** For each device you selected, select the correct upgrade version from the **Upgrade to Version** drop-down list.

**Step 7** When you have selected an upgrade version for each device, click **Upgrade**. When the update completes, a confirmation message displays.

---

### Verifying Your SVI Upgrade

To verify your Security Virtual Image (SVI) upgrade:
Step 1  From the vManage menu, select Maintenance ► Software Upgrade.
Step 2  Locate an upgraded device in the device table.
Step 3  Scroll to the Available Services column on the far right of the device table.

<table>
<thead>
<tr>
<th>Default Version</th>
<th>Available Services</th>
<th>Up Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.10.68</td>
<td></td>
<td>30 Nov 2018 1:23:00 AM PST</td>
</tr>
<tr>
<td>99.99.999-1814</td>
<td>0</td>
<td>07 Aug 2018 6:45:00 AM PDT</td>
</tr>
<tr>
<td>99.99.999-1814</td>
<td>0</td>
<td>07 Aug 2018 6:44:00 AM PDT</td>
</tr>
<tr>
<td>99.99.999-1814</td>
<td>0</td>
<td>07 Aug 2018 6:45:00 AM PDT</td>
</tr>
</tbody>
</table>

Step 4  Click the linked number in the Available Services column. The Container Details popup displays.

Step 5  Verify that the device is running the updated image.
Verifying Your SVI Upgrade
IPSec Pairwise Keys Overview

**Table 18: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Communication Using Pairwise IPsec Keys</td>
<td>Cisco IOS XE SD-WAN Release 16.12.1b</td>
<td>This feature allows private pairwise IPSec session keys to be created and installed for secure communication between IPSec devices and its peers.</td>
</tr>
</tbody>
</table>

IPSec Pairwise Keys feature implements controller-based key exchange protocol between device and controller. Controller-based key exchange protocol is used to create a Gateway-to-Gateway VPN (RFC7018) in either a Full-Mesh Topology or Dynamic Full-Mesh Topology.

The network devices set up a protected control-plane connection to the controller. The controller distributes policies to network devices, which enables the network devices to communicate with each other through a secure data plane.

A pair of IPSec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

- Supported Platforms, on page 145
- Pairwise Keys, on page 146
- IPsec Security Association Rekey, on page 146
- Configure IPSec Pairwise Keys, on page 146

**Supported Platforms**

The following platforms are supported for IPSec Pairwise Keys feature:

- Cisco IOS XE SD-WAN devices
- Cisco vEdge devices
Pairwise Keys

Key exchange method combined with authentication policies facilitate pairwise key creation between two network devices. A controller is used to distribute keying material and policies between network devices, resulting in the devices generating private pairwise keys with each other.

IPSec devices share public values from Diffie-Hellman (DH) algorithm with the controllers. The controllers relay the DH public values to authorized peers of the IPSec device as defined by a centralized policy.

Network devices create and install private pairwise IPSec session keys to be used to secure communications with their peers.

IPsec Security Association Rekey

Every rekeying IPSec device generates a new DH pair and generates new IPSec security association pairs for each peer with which it is communicating. The new security association pairs are generated as a combination of the new DH private value and the DH public value of each each peer. The IPSec device distributes the new DH public value to the Controller, which forwards it to its authorized peers. Each peer continues to transmit on the existing security association until that peer starts transmitting on the new security associations.

During a simultaneous rekey up to four pairs of IPSec SAs may be temporarily created, and they converge on a single new set of IPSec SAs.

Any IPSec device may initiate a rekey due to reasons such as a local time or volume-based policy, or the counter result of a cipher counter mode Initialization Vector (IV) nearing completion.

When you configure a rekey on a local inbound security association, it triggers peer outbound and inbound security association rekey. The local outbound security association rekey is initiated after the IPSec device receives the first packet with new Security Parameter Index (SPI) from peer.

---

**Note**

A pairwise key edge device can form IPSec sessions with both pairwise and non-pairwise edge devices.

**Note**

The rekeying process requires higher control plane CPU usage, resulting in lower session scaling.

Configure IPSec Pairwise Keys

Configure IPSec Pairwise Keys Using Cisco vManage

1. In Cisco vManage, select the **Configuration ▶ Templates** screen.
2. In the **Feature** tab, click **Create Template**.
3. From the **Device Model** check box, select the type of device for which you are creating the template.
4. From the **Basic Information** tab, choose **Security** feature template.
5. From the **Basic Configuration** tab, select On or Off from the IPsec Pairwise-Keying field.

*Figure 10: IPSec Pairwise Keying*

6. Alternatively, enter the pairwise key specific to the device in the **Enter Key** field.

7. Click **Save**.

**Configure Pairways Keys and Rekeying**

A pair of IPSec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

The keys use AES-GCM-256 (AES_256_CBC for multicast) cipher to perform encryption. By default, a key is valid for 3600 seconds.

**Configure Pairwise Keys**

Use the following command to configure pairwise keys:

```
Device(config)# security ipsec pairwise-keying
```
On Cisco IOS XE SD-WAN Devices, you must reboot the device for the pairwise keys configuration to take effect.

**Configure Rekeying for IPSec Pairwise Keys**

Use the following command to configure rekeying for pairwise keys.

```
Device(config)# security ipsec pwk-sym-rekey
```

**Verify IPSec Pairwise Keys on Cisco XE SD-WAN Routers**

Use the following command to verify outbound connections for Pairwise Keys:

```
Device# show sdwan ipsec pwk outbound-connections
```

<table>
<thead>
<tr>
<th>SS</th>
<th>E-KEY</th>
<th>AH</th>
<th>SOURCE IP</th>
<th>Source Port</th>
<th>Source IP</th>
<th>DEST Port</th>
<th>LOCAL TLOC ADDRESS</th>
<th>REMOTE TLOC COLOR</th>
<th>PWK-SPI INDEX</th>
<th>ID HASH</th>
<th>HASH HASH HASH HASH AUTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.168.11.3</td>
<td>12346</td>
<td>192.168.90.3</td>
<td>12346</td>
<td>10.1.0.2</td>
<td>lte</td>
<td>10.1.0.1</td>
<td>private</td>
<td>000000</td>
<td>0</td>
<td>6668</td>
<td>17B0</td>
</tr>
<tr>
<td>10.168.11.3</td>
<td>12346</td>
<td>192.168.92.6</td>
<td>12346</td>
<td>10.1.0.2</td>
<td>lte</td>
<td>10.1.0.6</td>
<td>default</td>
<td>00A001</td>
<td>0</td>
<td>6668</td>
<td>17B0</td>
</tr>
<tr>
<td>10.168.12.3</td>
<td>12346</td>
<td>192.168.90.3</td>
<td>12346</td>
<td>10.1.0.2</td>
<td>blue</td>
<td>10.1.0.1</td>
<td>private</td>
<td>000000</td>
<td>0</td>
<td>6668</td>
<td>17B0</td>
</tr>
<tr>
<td>10.168.12.3</td>
<td>12346</td>
<td>192.168.92.6</td>
<td>12346</td>
<td>10.1.0.2</td>
<td>blue</td>
<td>10.1.0.6</td>
<td>default</td>
<td>00A001</td>
<td>0</td>
<td>6668</td>
<td>17B0</td>
</tr>
</tbody>
</table>

Use the following command to verify inbound connection on IPSec Pairways Keys:

```
Device# show sdwan ipsec pwk inbound-connections
```

<table>
<thead>
<tr>
<th>DEST IP</th>
<th>LOCAL PORT</th>
<th>LOCAL SS</th>
<th>LOCAL D-KEY</th>
<th>LOCAL AH</th>
<th>REMOTE PORT</th>
<th>REMOTE DEST IP</th>
<th>REMOTE PWK SPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.90.3</td>
<td>12346</td>
<td>5.1.0.2</td>
<td>lte</td>
<td>5.1.0.1</td>
<td>private</td>
<td>000000</td>
<td>2</td>
</tr>
<tr>
<td>192.168.92.6</td>
<td>12346</td>
<td>5.1.0.2</td>
<td>lte</td>
<td>5.1.0.6</td>
<td>default</td>
<td>00100B</td>
<td>52</td>
</tr>
<tr>
<td>192.168.90.3</td>
<td>12346</td>
<td>5.1.0.2</td>
<td>blue</td>
<td>5.1.0.1</td>
<td>private</td>
<td>000000</td>
<td>5</td>
</tr>
<tr>
<td>192.168.92.6</td>
<td>12346</td>
<td>5.1.0.2</td>
<td>blue</td>
<td>5.1.0.6</td>
<td>default</td>
<td>00100B</td>
<td>55</td>
</tr>
</tbody>
</table>
Device# show sdwan ipsec pwk local-sa

<table>
<thead>
<tr>
<th>PKEY</th>
<th>NONCE</th>
<th>PKEY</th>
<th>TLOC-ADDRESS</th>
<th>TLOC-COLOR</th>
<th>SOURCE-IP</th>
<th>SOURCE PORT</th>
<th>SPI</th>
<th>INDEX</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.0.2 lte</td>
<td>10.168.11.3</td>
<td>12346</td>
<td>257</td>
<td>6</td>
<td>1</td>
<td>5605</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70C7</td>
<td>5.1.0.2 blue</td>
<td>10.168.12.3</td>
<td>12346</td>
<td>257</td>
<td>3</td>
<td>1</td>
<td>B9F9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Device# show platform hardware qfp active feature ipsec da spi

<table>
<thead>
<tr>
<th>g_hash_idx</th>
<th>Flow id</th>
<th>QFP SA hdl</th>
<th>source IP</th>
<th>sport</th>
<th>dest IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1541 3 11</td>
<td>192.168.90.3</td>
<td>12346</td>
<td>192.168.92.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6661 6</td>
<td>10.168.11.3</td>
<td>12346</td>
<td>192.168.92.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7429 6</td>
<td>10.168.11.1</td>
<td>12346</td>
<td>192.168.92.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x000000000000fbd970/0x000000000000fbb580</td>
<td>12346</td>
<td>192.168.92.6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

System id Wan int Wan ip

Yubei-cedge 5102 Gi2.xxx Sub 10.168.xxx
Yubei-tns 5108 G10/0/1 192.168.92.8
Yubei-ovld 5106 G10/0/0 192.168.92.6
Yubei-ing 5107 G10/0/0 192.168.92.7
Yubei-utah 5104 G10/0/0 192.168.92.4
Yubei-vedge 5101 ge0/0 192.168.90.3

Use the following command to display IPSec pairwise keys information on Cisco IOS XE SD-WAN devices:

Device# show sdwan security-info

security-info authentication-type "AH_SHA1_HMAC SHA1_HMAC"
security-info rekey 86400
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Enabled
security-info pairwise-keying Enabled

Debug Commands on Cisco XE SD-WAN Devices

Use the following debug commands for debugging issues related to IPSec Pairwise Keys feature:

debug plat soft sdwan ftm pwk [dump | log]
debug plat soft sdwan ttm pwk [dump | log]
debug plat soft sdwan vdaemon pwk [dump | log]
Configure Single Sign-On

This chapter describes how to configure single sign-on for Cisco SD-WAN. Cisco SD-WAN supports single sign-on using Okta or Active Directory Federation Services (ADFS).

- Configure Single Sign-On using Okta, on page 151
- Configure SSO for Active Directory Federation Services (ADFS), on page 154

Configure Single Sign-On using Okta

Okta provides a secure identity management service that lets you connect any person with any application on any device using Single Sign-On (SSO).

Perform the following steps to configure SSO.

Enable an Identity Provider in vManage

To configure Okta SSO, you must use vManage to enable an identity provider and generate a SAML metadata file:

1. In vManage, click Administration > Settings > Identify Provider Settings > Edit.
2. Click Enabled.
3. Click Click here to download the SAML metadata and save the content in a file. This data will be used for configuring Okta.
4. In the metadata, note the following information that you will use to configure Okta with vManage:
   - Entity ID
   - Signing certificate
   - Encryption certificate
   - Logout URL
   - Login URL
Configure SSO on the Okta Website

To configure SSO on the Okta website:

1. Log on to the Okta website.
2. Create a username using your email address.
3. To add vManage as one SSO application, click on the Admin button on the upper right corner to go to the next page. Then check the upper left corner to make sure it shows the Classic UI view on Okta. If it shows the Developer Console, click on the down triangle to select the Classic UI.
4. Click on Add Application under Shortcuts to the right to go to the next page, and then click on Create New Application on the pop-up window. Select Web for the platform, and select SAML 2.0 as the Sign on Method. Click Create.
5. Give a string as Application name.
6. Optional: Upload a logo, and then click Next.
7. On SAML Settings for Single sign on URL section, set the value to the samlLoginResponse URL from the downloaded metadata from the vManage UI. Check the box Use this for Recipient URL and Destination URL.
8. Copy the entityID string and paste it in the Audience URI (SP Entity ID) field. The value can be an IP address or the name of the vManage site.
9. For Default RelayState, leave empty.
10. For Name ID format, select EmailAddress.
11. For Application username, select Okta username.
12. For Show Advanced Settings, enter the fields as indicated below.

\[Table 18:\]

<table>
<thead>
<tr>
<th>Component</th>
<th>Value</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>Assertion Signature</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>RSA-SHA256</td>
<td></td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>SHA256</td>
<td></td>
</tr>
<tr>
<td>Assertion Encryption</td>
<td>Encrypted</td>
<td></td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES256-CBC</td>
<td></td>
</tr>
<tr>
<td>Key Transport Algorithm</td>
<td>RSA-OAEP</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Value</td>
<td>Configuration</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption Certificate</td>
<td></td>
<td>a. Copy the encryption certificate from the metadata you downloaded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Go to <a href="http://www.samltool.com">www.samltool.com</a> and click on X.509 CERTS, paste there. Click Format X.509 Certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Make sure to remove the last empty line and then save the output (X.509.cert with header) into a text file encryption.cer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>d. Upload the file. Mozilla Firefox may not allow you to do the upload. Instead, you can use Google Chrome. You should see the certificate information after uploading to Okta.</td>
</tr>
<tr>
<td>Enable Single Logout</td>
<td>Make sure this is checked.</td>
<td></td>
</tr>
<tr>
<td>Single Logout URL</td>
<td>Get from the metadata.</td>
<td></td>
</tr>
<tr>
<td>SP Issuer</td>
<td>Use the entityID from the metadata.</td>
<td></td>
</tr>
<tr>
<td>Signature Certificate</td>
<td></td>
<td>a. Obtain from the metadata. Format the signature certificate using <a href="http://www.samltool.com">www.samltool.com</a> as done above.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Save to a file, for example, signing.cer and upload.</td>
</tr>
<tr>
<td>Authentication context class</td>
<td>X.509 Certificate</td>
<td></td>
</tr>
<tr>
<td>Honor Force Authentication</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SAML issuer ID string</td>
<td>SAML issuer ID string</td>
<td></td>
</tr>
<tr>
<td>Attribute Statements</td>
<td>Field: Name Value: Username</td>
<td></td>
</tr>
<tr>
<td>(optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field: Name format (optional) Value: Unspecified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field: Value Value: user.login</td>
<td></td>
</tr>
<tr>
<td>Group Attribute Statements</td>
<td>Field: Name Value: Groups</td>
<td></td>
</tr>
<tr>
<td>(optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field: Name format (optional) Value: Unspecified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field: Matches regex Value: .*</td>
<td></td>
</tr>
</tbody>
</table>
It is mandatory to use the two strings, Username and Groups, exactly as shown above. Otherwise, you may be logged in with the default group of Basic.

13. Click Next.
14. For Application Type, check This is an internal app that we have created (optional).
15. Click Finish. This brings you to the Okta application page.
16. Click on View Setup Instructions.
17. Copy the IDP metadata.
18. In the vManage UI, paste the IDP metadata in vManage using Identity Provider Settings > Upload Identity Provider Metadata, and click Save.

Assign Users to the Application

To assign users to the application on the Okta website:
1. On the Okta application page, navigate to Assignments > People > Assign.
2. Select Assign to people from the drop-down menu.
3. Click on Assign next to the user(s) you selected and click Done.
4. To add a user, click on Directory > Add Person > Save.

Configure SSO for Active Directory Federation Services (ADFS)

Describes how to use vManage and ADFS to configure Single Sign On (SSO).

The configuration of vManage to use ADFS as IDP involved two steps:

- Step 1 - Import ADFS metadata to vManage
- Step 2 - Export vManage metadata to ADFS

Step 2 can be further divided into:

- Edit and then import vManage metadata to ADFS
- Setup ADFS manually using the information from vManage metadata

Import Metadata File into ADFS

Step 1 - Import ADFS metadata to vManage:
1. Download the ADFS Metadata file, typically from the ADFS URL: https://<your ADFS FQDN or IP>/FederationMetadata/2007-06/FederationMetadata.xml
2. Save the file as `adfs_metadata.txt`.

3. On the vManage navigate to Admin > Settings > Identify Provider Settings > Enable, and then upload `adfs_metadata.txt` to vManage.

**Step 2 - Export vManage metadata to ADFS:**

4. With Identify Provider Settings enabled, Click here to download SAML metadata and save into a file, which is typically `192.168.1.15_saml_metadata.xml`.


6. Edit vManage Metadata file by deleting everything from `<md:KeyDescriptor use="encryption">` to `</md:KeyDescriptor>`.

7. Import the new modified vManage Metadata file into ADFS, and enter the `entityID` as **Display Name**.

8. Click Next until the end.

9. Open **Edit Claim Rule**, and add the following four new custom rules in the exact sequence:

   ```
   @RuleName = "sAMAccountName as Username" c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = {"Username"}, query = ";sAMAccountName;{0}", param = c.Value);
   @RuleName = "sAMAccountName as NameID" c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = {"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"}, query = ";sAMAccountName;{0}", param = c.Value);
   @RuleName = "Get User Groups and save in temp/variable" c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = {"http://temp/variable1"}, query = ";tokenGroups;{0}", param = c.Value);
   @RuleName = "Parse temp/variable1 and Send Groups Membership" c:[Type == "http://temp/variable1", Value =~ "(?i)^SSO-"] => issue(Type = "Groups", Value = RegExReplace(c.Value, "SSO-", ";"));
   ```

10. Verify the final result.

11. In the Active Directory, create the following two security groups: **SSO-Netadmin** and **SSO-Operator**.

---

**Note**

If you are using different naming convention for the two security groups, then you have to modify the Regular expression value "(?i)^SSO-" in the step above.

Any active directory users who are not members of the two groups will only have **Basic** access to vManage.
Add ADFS Relying Party Trust

Before you begin
To add ADFS relying party trust using vManage:

1. Navigate to Admin > Settings > Identify Provider Settings > Enable.
2. Download the ADFS Metadata file, and upload it into vManage. An example of a URL, https://<your ADFS FQDN or IP>/FederationMetadata/2007-06/FederationMetadata.xml.
3. Click here to download SAML metadata, and save into a file. An example of a saved file, 192.168.1.15_saml_metadata.xml.
4. Open the file with an XML editor, and check that the following information is available:
   - Entity ID
   - Signing certificate
   - Login URL
   - Logout URL
7. Navigate to www.samltool.com page, click X.509 CERTS > Format X.509 Certificate, and paste the copied content
8. Save the output (“X.509 cert with header”) into a text file “Signing.cer”. Remember to remove the last empty line.

Add ADFS Relying Party Trust Manually
To add ADFS relying party trust manually:

1. Launch AD FS 2.0 Management.
3. Click Action > Add Relying Party Trust.
4. Click Start.
5. Select Enter data about the relying party manually, and click Next.
6. Enter Display name and Notes, and then click Next.
7. Select AD FS 2.0 profile, and click Next.
8. Click Next to skip Configure Certificate page.
9. Click Enable support for the SAML 2.0 Webs So protocol.
10. Open a text editor, and open 10.10.10.15_saml_metadata.xml file.
11. Copy the value of the Location attribute for AssertionConsumerService, and paste it into the Relying party SAML 2.0 SSO service URL text box.

12. Click Next.

13. Copy the value of entityId attribute, and paste it into the Relying party trust identifiers text box.

14. Click Add, and click Next.

15. Click Next to skip Configure Multi-factor Authentication Now section.

16. Select Permit all users to access this relying party, and click Next.

17. Click Next to skip Ready to Add Trust section.

18. Click Close.

19. Open Edit Claim Rules window, and add the following four new custom rules in this order:

   - @RuleName = "sAMAccountName as Username" c:[Type ==
     Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = {"Username"},
     query = ";sAMAccountName;{0}"}, param = c.Value);
   - @RuleName = "sAMAccountName as NameID" c:[Type ==
     Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
     {"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"}, query =
     ";sAMAccountName;{0}"}, param = c.Value);
   - @RuleName = "Get User Groups and save in temp/variable" c:[Type ==
     Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types =
     {"http://temp/variable1"}, query = ";tokenGroups;{0}"}, param = c.Value);
   - @RuleName = "Parse temp/variable1 and Send Groups Membership" c:[Type ==
     "http://temp/variable1", Value =~ "(?i)^SSO-") => issue(Type = "Groups", Value =
     RegExReplace(c.Value, "SSO-", "")];

20. Open the Edit Claim Rules window, and verify that the rules display in the Assurance Transform Rules tab.

21. Click Finish.

22. Open Properties window of the newly created Relying Party Trust, and click the Signature tab.

23. Click Add, and add the Signing.cer created in Step 6.

24. In the Active Directory, click the General tab, and enter the following two security groups in the Group name text box:

   SSO-Netadmin
   SSO-Operator

Note If you use different naming convention for the two security groups, then you have to modify the Regular expression value for (?!)^SSO- mentioned in Step 19.
Any active directory user who is NOT a member of these two groups, will only have **Basic** access to vManage.
Security CLI Reference

CLI commands for configuring and monitoring security.

Security CLI Templates

The CLI Templates for Cisco IOS XE SD-WAN device features allows you to configure intent-based CLI templates for Cisco IOS XE SD-WAN devices using vManage. Intent-based CLI template refer to the command line interface configuration that are based on the vEdge device syntax. Using CLI templates, vManage enables pushing vEdge syntax-based commands to Cisco IOS XE SD-WAN devices in Cisco IOS XE syntax.
## Table 20: Security Policy for UTD

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy zone internet vnp 0 ! zone zone1 vnp 1 ! zone zone2 vnp 2 ! zone-pair ZP_zone1_internet_fw_policy source-zone zone1 destination-zone internet zone-policy fw_policy ! zone-pair ZP_zone1_zone2_fw_policy source-zone zone1 destination-zone zone2 zone-policy fw_policy ! zone-based-policy fw_policy sequence 1 match source-data-prefix-list subnet1 ! action inspect ! ! default-action pass ! zone-to-nozone-internet deny lists data-prefix-list subnet1 ip-prefix 10.0.10.0/24 ! ! url-filtering url_filter web-category-action block web-categories games block-threshold moderate-risk block text &quot;&lt;![CDATA[&lt;h3&gt;Access to the requested page has been denied]]&gt;&quot; target-vpns 1 ! intrusion-prevention intrusion_policy security-level connectivity inspection-mode protection log-level err target-vpns 1 ! failure-mode open !</td>
<td></td>
</tr>
</tbody>
</table>

"<! [CDATA[&lt;h3&gt;Access to the requested page has been denied]]&gt;" target-vpns 1
<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip access-list extended fw_policy-seq-1-acl</td>
</tr>
<tr>
<td></td>
<td>11 permit object-group</td>
</tr>
<tr>
<td></td>
<td>fw-policy-seq-1-service-og_ object-group</td>
</tr>
<tr>
<td></td>
<td>subnet1 any</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>ip access-list extended utd-nat-acl</td>
</tr>
<tr>
<td></td>
<td>10 permit ip any any</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class-map type inspect match-all</td>
</tr>
<tr>
<td></td>
<td>fw_policy-seq-1-cm_</td>
</tr>
<tr>
<td></td>
<td>match access-group name</td>
</tr>
<tr>
<td></td>
<td>fw_policy-seq-1-acl_</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>policy-map type inspect fw_policy</td>
</tr>
<tr>
<td></td>
<td>class fw_policy-seq-1-cm_</td>
</tr>
<tr>
<td></td>
<td>inspect</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>pass</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>object-group service</td>
</tr>
<tr>
<td></td>
<td>fw_policy-seq-1-service-og_</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>parameter-map type inspect-global</td>
</tr>
<tr>
<td></td>
<td>alert on</td>
</tr>
<tr>
<td></td>
<td>log dropped-packets</td>
</tr>
<tr>
<td></td>
<td>multi-tenancy</td>
</tr>
<tr>
<td></td>
<td>vpn zone security</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>parameter-map type umbrella global</td>
</tr>
<tr>
<td></td>
<td>token</td>
</tr>
<tr>
<td></td>
<td>A5EA676087BF66A42DC4F722C2AFD10D00256274</td>
</tr>
<tr>
<td></td>
<td>dns-encrypt</td>
</tr>
<tr>
<td></td>
<td>vrf 1</td>
</tr>
<tr>
<td></td>
<td>dns-resolver umbrella</td>
</tr>
<tr>
<td></td>
<td>match-local-domain-to-bypass</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>zone security internet</td>
</tr>
<tr>
<td></td>
<td>vpn 0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>zone security zone1</td>
</tr>
<tr>
<td></td>
<td>vpn 1</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>zone security zone2</td>
</tr>
<tr>
<td></td>
<td>vpn 2</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>zone-pair security</td>
</tr>
<tr>
<td></td>
<td>ZP_zone1_internet_fw_policy source zone1</td>
</tr>
<tr>
<td></td>
<td>destination internet</td>
</tr>
<tr>
<td></td>
<td>service-policy type inspect fw_policy</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>zone-pair security ZP_zone1_zone2_fw_policy</td>
</tr>
<tr>
<td></td>
<td>source zone1 destination zone2</td>
</tr>
<tr>
<td></td>
<td>service-policy type inspect fw_policy</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>app-hosting appid utd</td>
</tr>
<tr>
<td></td>
<td>app-resource package-profile cloud-low</td>
</tr>
<tr>
<td></td>
<td>app-vnic gateway0 virtualportgroup 0</td>
</tr>
<tr>
<td>CLI Template Configuration</td>
<td>Configuration on the Device</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>guest-interface 0</td>
<td>guest-ipaddress 192.168.1.2 netmask 255.255.255.252</td>
</tr>
<tr>
<td></td>
<td>! app-vnic gateway1 virtualportgroup 1</td>
</tr>
<tr>
<td></td>
<td>guest-interface 1 guest-ipaddress 192.0.2.2 netmask 255.255.255.252</td>
</tr>
<tr>
<td></td>
<td>! start</td>
</tr>
<tr>
<td></td>
<td>utd multi-tenancy utd engine standard multi-tenancy web-filter block page profile block-url_filter text &lt;![CDATA[&lt;h3&gt;Access to the requested page has been denied&lt;/h3&gt;&lt;p&gt;Please contact your Network Administrator&lt;/p&gt;]]&gt;</td>
</tr>
<tr>
<td></td>
<td>! web-filter url profile url_filter categories block games</td>
</tr>
<tr>
<td></td>
<td>! block page-profile block-url_filter log level error reputation block-threshold moderate-risk</td>
</tr>
<tr>
<td></td>
<td>! threat-inspection profile intrusion_policy threat protection policy connectivity logging level err</td>
</tr>
<tr>
<td></td>
<td>! utd global</td>
</tr>
<tr>
<td></td>
<td>! policy utd-policy-vrf-1 all-interfaces vrf 1 threat-inspection profile intrusion_policy</td>
</tr>
<tr>
<td></td>
<td>web-filter url profile url_filter exit</td>
</tr>
</tbody>
</table>

Security Monitoring Commands

- show control connections