



## **Security Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12**

**First Published:** 2019-11-22

**Last Modified:** 2020-01-29

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





## CONTENTS

---

<b>CHAPTER 1</b>	<b>What's New for Cisco SD-WAN</b>	<b>1</b>
	What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r	<b>1</b>

---

<b>CHAPTER 2</b>	<b>Security Overview</b>	<b>5</b>
	Cisco SD-WAN Security Components	<b>5</b>
	Security Provided by NAT Devices	<b>6</b>
	Security for Connections to External Devices	<b>7</b>
	Control Plane Security Overview	<b>7</b>
	DTLS and TLS Infrastructure	<b>8</b>
	Control Plane Authentication	<b>9</b>
	Control Plane Encryption	<b>11</b>
	Control Plane Integrity	<b>12</b>
	Data Plane Security Overview	<b>12</b>
	Data Plane Authentication and Encryption	<b>13</b>
	Data Plane Integrity	<b>15</b>
	Carrying VPN Information in Data Packets	<b>18</b>
	Unified Threat Defense for Cisco SD-WAN	<b>18</b>
	Supported Platforms	<b>19</b>
	Restrictions	<b>20</b>

---

<b>CHAPTER 3</b>	<b>Configure Security Parameters</b>	<b>21</b>
	Configure Control Plane Security Parameters	<b>21</b>
	Configure DTLS on vManage	<b>22</b>
	Configure Data Plane Security Parameters	<b>23</b>
	Configure Allowed Authentication Types	<b>23</b>
	Change the Rekeying Timer	<b>24</b>

- Change the Size of the Anti-Replay Window 25
- VPN Interface IPsec 27
  - Create VPN IPsec Interface Template 27
  - Changing the Scope for a Parameter Value 27
  - Configure IPsec Tunnel Parameters 28
  - Configure Dead-Peer Detection 29
  - Configure IKE 30

---

**CHAPTER 4**

**Enterprise Firewall with Application Awareness 35**

- Overview of Enterprise Firewall with Application Awareness 35
- Restrictions for Enterprise Firewall 37
- Configure Firewall Policies 37
  - Configuration Components 39
- Create or Modify Lists 39
- Use the Policy Configuration Wizard 41
- Apply Policy to a Zone Pair 45
- Apply Security Policy to a Cisco IOS XE SD-WAN Device 46
- Monitor Enterprise Firewall 46
- Zone-Based Firewall Configuration Examples 47
- Firewall High-Speed Logging 50
  - Information About Firewall High-Speed Logging 50
    - Firewall High-Speed Logging Overview 50
    - NetFlow Field ID Descriptions 51
    - HSL Messages 55
  - How to Configure Firewall High-Speed Logging 61
    - Enabling Firewall High-Speed Logging Using vManage 61
    - Enabling High-Speed Logging for Global Parameter Maps 62
    - Enabling High-Speed Logging for Firewall Actions 63
- Configuration Examples for Firewall High-Speed Logging 64
  - Example: Enabling High-Speed Logging for Global Parameter Maps 64
  - Example: Enabling High-Speed Logging for Firewall Actions 65

---

**CHAPTER 5**

**Intrusion Prevention System 67**

- Overview of Intrusion Prevention System 67

Cisco SD-WAN IPS Solution	68
Configure and Apply IPS or IDS	68
Before you Begin	68
Configure Intrusion Prevention or Detection	68
Apply a Security Policy to a Device	71
Modify an Intrusion Prevention or Detection Policy	72
Delete an Intrusion Prevention or Detection Policy	72
Monitor Intrusion Prevention Policy	73
Update IPS Signatures	75

---

**CHAPTER 6****URL Filtering** 77

Overview of URL Filtering	77
Filtering Options	78
Category-Based Filtering	78
Reputation-Based Filtering	78
List-based Filtering	79
Configure and Apply URL Filtering	79
Before you Begin	79
Configure URL Filtering	79
Apply a Security Policy to a Device	83
Modify URL Filtering	84
Delete URL Filtering	84
Monitor URL Filtering	85

---

**CHAPTER 7****Advanced Malware Protection** 87

Overview of Advanced Malware Protection	87
Configure and Apply an Advanced Malware Policy	88
Before you Begin	88
Configure Threat Grid API Key	88
Configuring an Advanced Malware Protection Policy	89
Apply a Security Policy to a Device	91
Modify an Advanced Malware Protection Policy	92
Delete an Advanced Malware Protection Policy	93
Monitor Advanced Malware Protection	94

Troubleshoot Advanced Malware Protection	95
Rekey the Device Threat Grid API Key	95

---

**CHAPTER 8****SD-WAN Umbrella Integration 97**

Overview of Cisco SD-WAN Umbrella Integration	97
Restrictions for Umbrella Integration	100
Prerequisites for Umbrella Integration	100
Configure Umbrella API Token	100
Define Domain Lists	101
Configure Umbrella DNS Policy Using vManage	102
Apply DNS Umbrella Policy to an IOS XE Router	106
Monitoring Umbrella Feature	107
Umbrella Integration Using CLI	108
Umbrella show commands at FP Layer	115
Umbrella show commands at CPP Layer	116
Umbrella Data-Plane show commands	117
Troubleshooting the Umbrella Integration	119
DNS Security Policy Configuration	120

---

**CHAPTER 9****Security Virtual Image 123**

Install and Configure IPS/IDS, URL-F, or AMP Security Policies	123
Identify the Recommended Security Virtual Image Version	125
Upload the Cisco Security Virtual Image to vManage	126
Upgrade a Security Virtual Image	127

---

**CHAPTER 10****IPSec Pairwise Keys Overview 129**

Supported Platforms	129
Pairwise Keys	130
IPsec Security Association Rekey	130
Configure IPSec Pairwise Keys	130
Configure IPSec Pairwise Keys Using vManage	130
Configure Pairways Keys and Rekeying	131
Verify IPSec Pairwise Keys on Cisco XE SD-WAN Routers	132

---

**CHAPTER 11****Configure Single Sign-On 135**

Configure Single Sign-On using Okta 135

Enable an Identity Provider in vManage 135

Configure SSO on the Okta Website 136

Assign Users to the Application 138

Configure SSO for Active Directory Federation Services (ADFS) 138

Import Metadata File into ADFS 138

Add ADFS Relying Party Trust 140

Add ADFS Relying Party Trust Manually 140

---

**CHAPTER 12****Security CLI Reference 143**







# CHAPTER 1

## What's New for Cisco SD-WAN

This chapter describes what's new in Cisco SD-WAN for each release.

- [What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r, on page 1](#)

## What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r

This section applies to Cisco IOS XE SD-WAN devices.

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 SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

**Table 1: What's New for Cisco IOS XE SD-WAN Devices**

Feature	Description
<b>Getting Started</b>	
API Cross-Site Request Forgery Prevention	This feature adds protection against Cross-Site Request Forgery (CSRF) that occurs when using Cisco SD-WAN REST APIs. This protection is provided by including a CSRF token with API requests. You can put requests on an allowed list so that they do not require protection if needed. See <a href="#">Cross-Site Request Forgery Prevention</a> .
<b>Systems and Interfaces</b>	
IPv6 Support for NAT64 Devices	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN devices. See <a href="#">IPv6 Support for NAT64 Devices</a> .
Secure Shell Authentication Using RSA Keys	This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server. See SSH Authentication using vManage on Cisco XE SD-WAN Devices. See <a href="#">Configure SSH Authentication</a> .

Feature	Description
DHCP option support	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges. See <a href="#">Configure DHCP</a> .
Communication with an UCS-E Server	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template. See <a href="#">Create a UCS-E Template</a> .
<b>Bridging, Routing, Segmentation, and QoS</b>	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. See <a href="#">QoS on Subinterface</a> .
<b>Policies</b>	
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. See <a href="#">Configure and Monitor Packet Duplication</a> .
Control Traffic Flow Using Class of Service Values	This feature lets you control the flow of traffic into and out of a Cisco device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. See <a href="#">Configure Localized Data Policy for IPv4 Using Cisco vManage</a> .
Integration with Cisco ACI	The Cisco SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix-list and includes a VPN list to an SLA class that is provided by Cisco ACI. See <a href="#">Integration with Cisco ACI</a> .
Encryption of Lawful Intercept Messages	This feature encrypts lawful intercept messages between a Cisco IOS XE SD-WAN device and a media device using static tunnel information. See <a href="#">Encryption of Lawful Intercept Messages</a> .
<b>Security</b>	
High-Speed Logging for Zone-Based Firewalls	This feature allows a firewall to log records with minimum impact to packet processing. See <a href="#">Firewall High-Speed Logging</a> .
Self zone policy for Zone-Based Firewalls	This feature can help define policies to impose rules on incoming and outgoing traffic. See <a href="#">Apply Policy to a Zone Pair</a> in <a href="#">Use the Policy Configuration Wizard</a> .
Secure Communication Using Pairwise IPsec Keys	This feature allows private pairwise IPsec session keys to be created and installed for secure communication between IPsec devices and its peers. See <a href="#">IPsec Pairwise Keys Overview</a> .
<b>Network Optimization and High Availability</b>	

Feature	Description
TCP Optimization	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput. See <a href="#">TCP Optimization: Cisco XE SD-WAN Routers</a> .
Share VNF Devices Across Service Chains	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. See <a href="#">Share VNF Devices Across Service Chains</a> .
Monitor Service Chain Health	This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. See <a href="#">Monitor Service Chain Health</a> .
Manage PNF Devices in Service Chains	This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. See <a href="#">Manage PNF Devices in Service Chains</a> .
<b>Devices</b>	
Cisco 1101 Series Integrated Services Routers	Cisco SD-WAN capability can now be enabled on Cisco 1101 Series Integrated Services Routers.
<b>Commands</b>	
Loopback interface support for WAN (IPsec)	This feature allows you to configure a loopback transport interface on a Cisco IOS XE SD-WAN device for troubleshooting and diagnostic purposes. See the <a href="#">bind</a> command.





## CHAPTER 2

# 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:

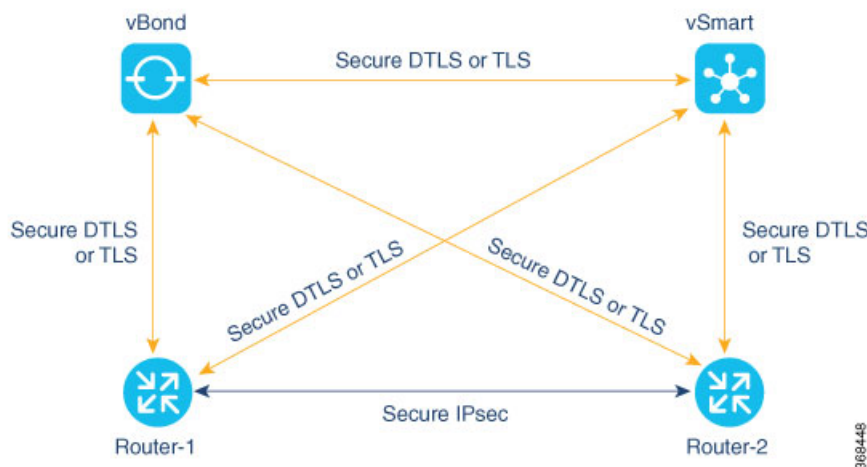
- [Cisco SD-WAN Security Components, on page 5](#)
- [Security Provided by NAT Devices, on page 6](#)
- [Security for Connections to External Devices, on page 7](#)
- [Control Plane Security Overview, on page 7](#)
- [Data Plane Security Overview, on page 12](#)
- [Unified Threat Defense for Cisco SD-WAN, on page 18](#)

## 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

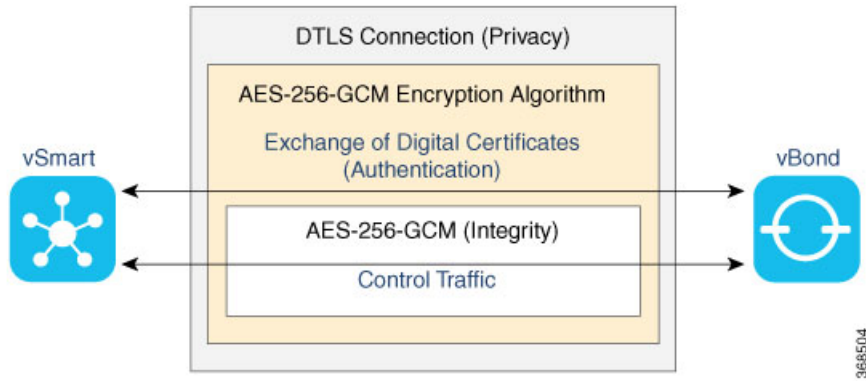
Cisco SD-WAN routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote user. The Cisco SD-WAN software supports IKE 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.

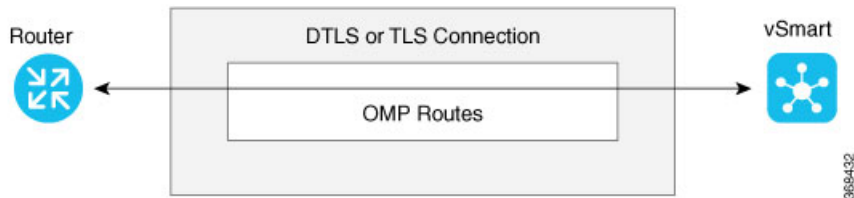
## DTLS and TLS Infrastructure

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.

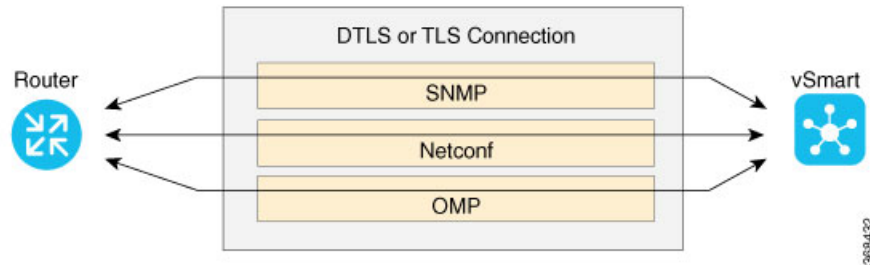
The Cisco SD-WAN software implements the standard version of DTLS with UDP, which is defined in RFC 6347 . DTLS for use with other protocols is defined in a number of other RFCs . For TLS, the Cisco SD-WAN software implements the standard version defined in RFC 5246.



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 `vd daemon` 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 router.

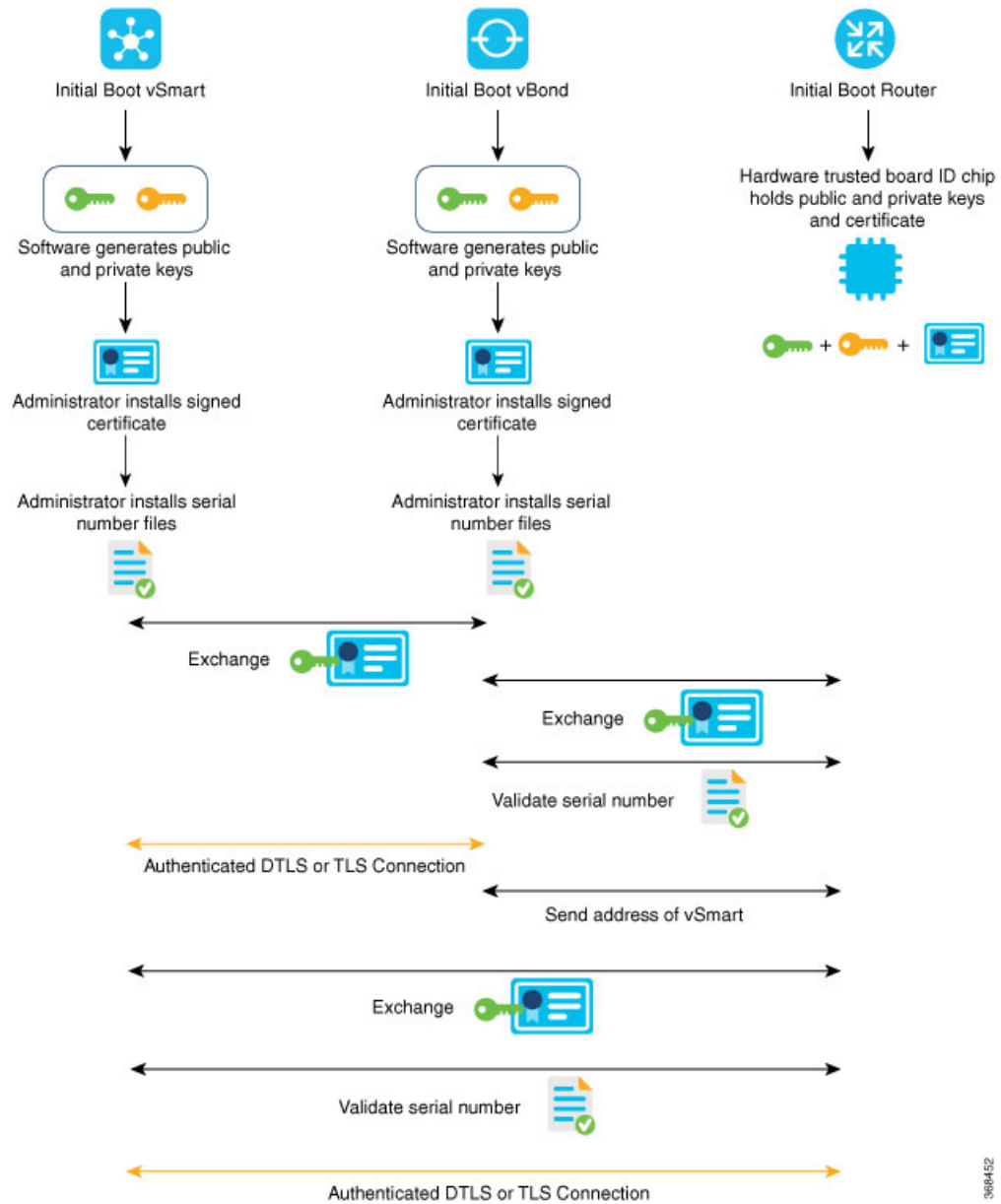
In addition to standard PKI components, the Cisco SD-WAN router serial numbers and the router chassis numbers are used in the authentication processes.

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.

To augment these standard PKI components, the Cisco SD-WAN software uses the router serial numbers in performing automatic router authentication. Specifically, it uses the router and vSmart serial numbers and the router chassis numbers. When a batch of routers is shipped, the manufacturer sends a text file that lists the serial numbers of the routers and the corresponding chassis numbers. For the vSmart controllers, when the network administrator receives the signed certificate, they should extract the serial numbers from the certificates and place them into a single text file, one serial number per line. Then the network administrator manually installs these two files. The file received from the manufacturer that lists all valid router serial and chassis numbers is uploaded and installed on vSmart 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.

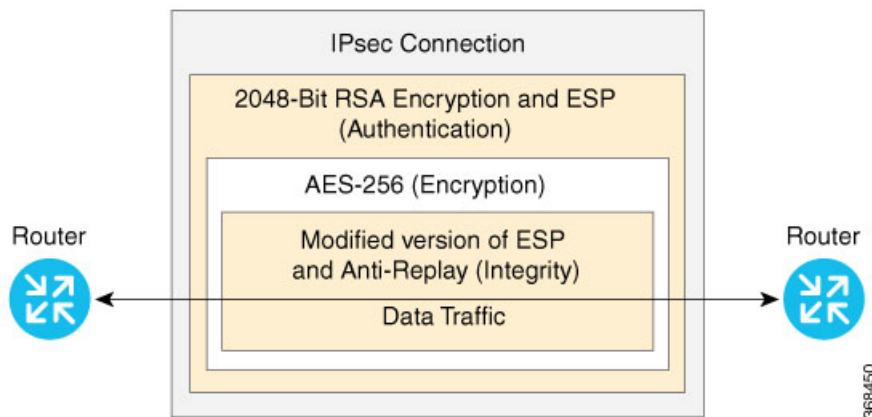


## Control Plane Encryption

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.

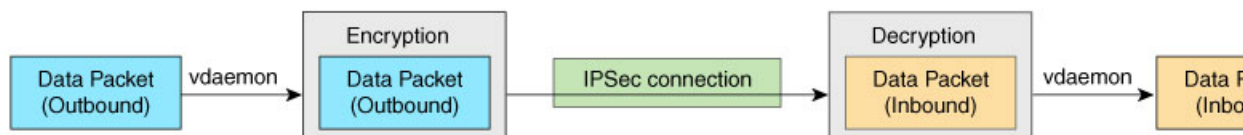
## Data Plane Security Overview

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 130.
  - 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.
- **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.

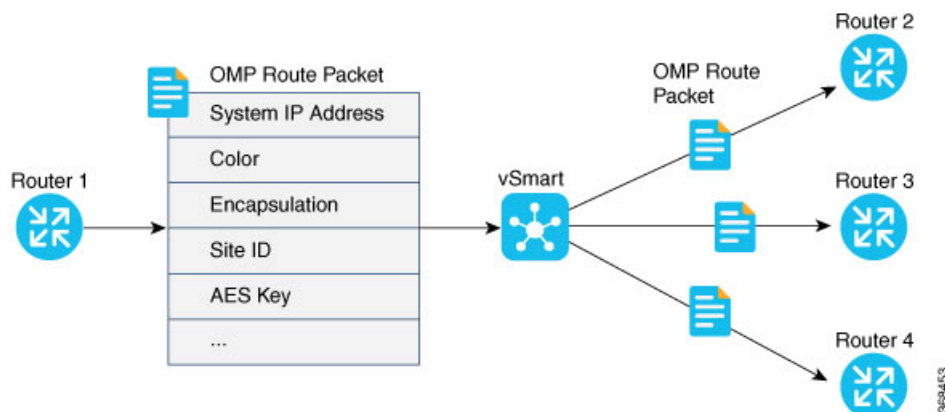
The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- 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 129



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.

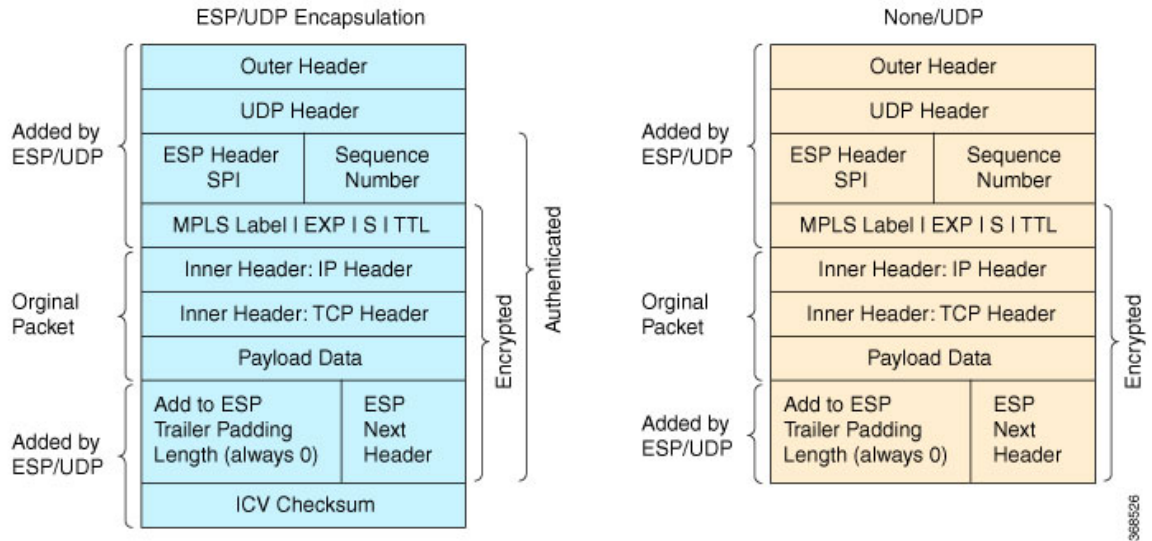
The first of these components, ESP, is the standard IPsec encryption protocol. ESP protects a data packet's payload and its inner IP header fields both by encryption, which occurs automatically, and authentication. For authentication, ESP performs a checksum calculation on the data packet's payload and 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



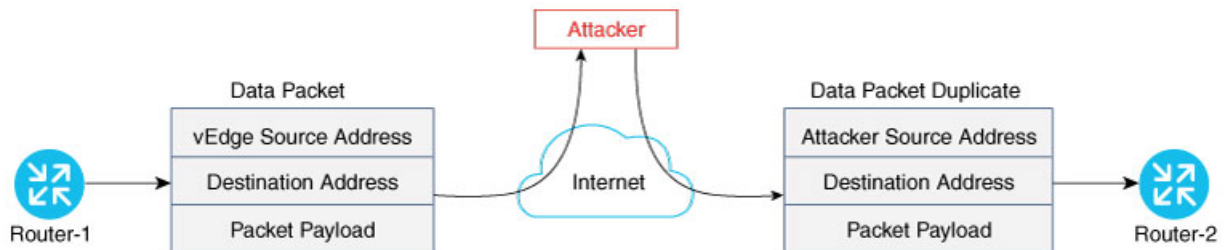
accepts packets whose checksums match. In the figure below, the center stack illustrates the encapsulation performed by the modified version of ESP. ESP again encrypts the inner headers, payload, MPLS label (if present), and ESP trailer fields, and now mimics AH by authenticating the entire packet—the 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.

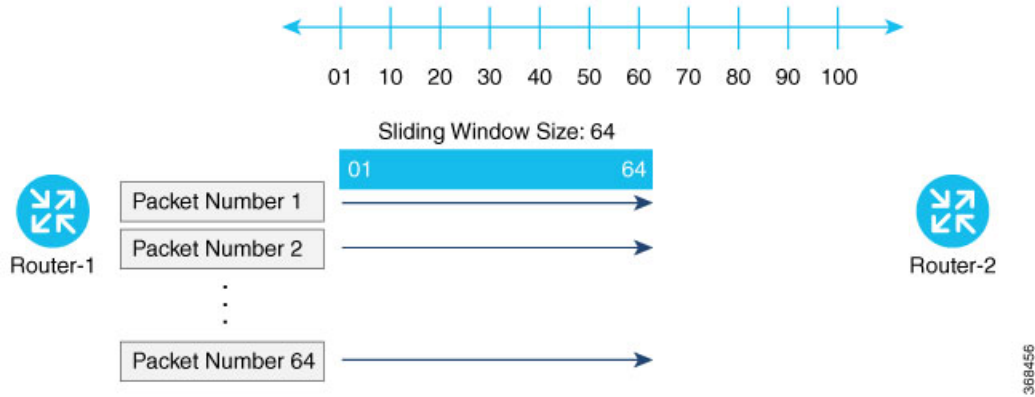
Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this 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 to the adversary unauthorized access to resources or services.



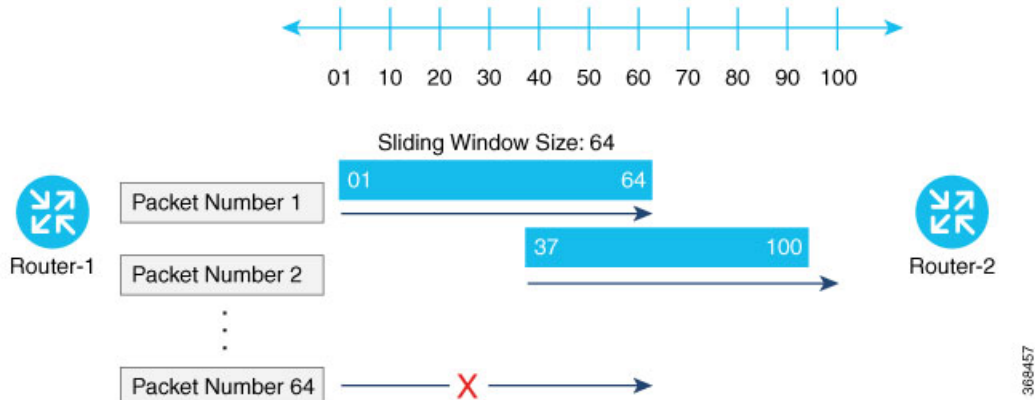
As a counter to such attacks, the Cisco SD-WAN overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender inserts a sequence number into each IPsec packet, and the destination checks the sequence number, accepting only packets with



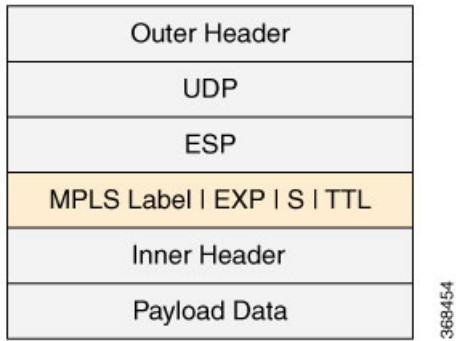
unique, non-duplicate sequence numbers. The second component is a sliding window, which defines a range of sequence numbers that are current. The sliding window has a fixed length. The destination accepts only packets whose sequence numbers fall within the current range of values in the sliding window, 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 2: Cisco SD-WAN SD-WAN Security Features**

Feature	Description
<a href="#">Enterprise Firewall with Application Awareness, on page 35</a>	A stateful firewall with NBAR2 application detection engine to provide application visibility and granular control, capable of detecting 1400+ applications.
<a href="#">Intrusion Prevention System, on page 67</a>	This system is backed by Cisco Talos signatures and are updated automatically. The Intrusion Prevention System is deployed using a security virtual image.

Feature	Description
<a href="#">URL Filtering, on page 77</a>	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.
<a href="#">Advanced Malware Protection, on page 87</a>	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.
<a href="#">SD-WAN Umbrella Integration, on page 97</a>	Cloud-delivered enterprise network security which provides users with a first line of defense against cyber security threats.

## 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 21](#)
- [Configure Data Plane Security Parameters, on page 23](#)
- [VPN Interface IPsec , on page 27](#)

## 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
```

PEER TYPE	PEER REMOTE	PEER PROTOCOL COLOR	PEER SYSTEM STATE	PEER IP UPTIME	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT
vedge	dtls		up	172.16.255.11	100	1	10.0.5.11	12346	10.0.5.11	12346
lte			up	0:07:48:58						
vedge	dtls		up	172.16.255.21	100	1	10.0.5.21	12346	10.0.5.21	12346
lte			up	0:07:48:51						
vedge	dtls		up	172.16.255.14	400	1	10.1.14.14	12360	10.1.14.14	12360
lte			up	0:07:49:02						
vedge	dtls		up	172.16.255.15	500	1	10.1.15.15	12346	10.1.15.15	12346
default			up	0:07:47:18						
vedge	dtls		up	172.16.255.16	600	1	10.1.16.16	12346	10.1.16.16	12346
default			up	0:07:41:52						
vsmart	tls		up	172.16.255.19	100	1	10.0.5.19	12345	10.0.5.19	12345
default			up	0:00:01:44						
vbond	dtls		up	-	0	0	10.1.14.14	12346	10.1.14.14	12346
default			up	0:07:49:08						

vSmart-2# **control connections**

PEER TYPE	PEER REMOTE	PEER PROTOCOL COLOR	PEER SYSTEM STATE	PEER IP UPTIME	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT
vedge	tls		up	172.16.255.11	100	1	10.0.5.11	12345	10.0.5.11	12345
lte			up	0:00:01:18						
vedge	tls		up	172.16.255.21	100	1	10.0.5.21	12345	10.0.5.21	12345
lte			up	0:00:01:18						
vedge	tls		up	172.16.255.14	400	1	10.1.14.14	12345	10.1.14.14	12345
lte			up	0:00:01:18						
vedge	tls		up	172.16.255.15	500	1	10.1.15.15	12345	10.1.15.15	12345
default			up	0:00:01:18						
vedge	tls		up	172.16.255.16	600	1	10.1.16.16	12345	10.1.16.16	12345
default			up	0:00:01:18						
vsmart	tls		up	172.16.255.20	200	1	10.0.12.20	23456	10.0.12.20	23456
default			up	0:00:01:32						
vbond	dtls		up	-	0	0	10.1.14.14	12346	10.1.14.14	12346
default			up	0:00:01:33						

## 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. The output shows that four vdaemon processes are running:

```
vManage# show control summary
```

INSTANCE	VBOND COUNTS	VMANAGE COUNTS	VSMART COUNTS	VEDGE COUNTS
0	2	0	2	7
1	2	0	0	5
2	2	0	0	5
3	2	0	0	4

To see the listening ports, use the **show control local-properties** command:

```
vManage# show control local-properties
```

```
organization-name      Cisco SD-WAN Inc Test
certificate-status      Installed
root-ca-chain-status   Installed

certificate-validity    Valid
certificate-not-valid-before May 20 00:00:00 2015 GMT
certificate-not-valid-after May 20 23:59:59 2016 GMT

dns-name                vbond.cisco.com
site-id                 5000
domain-id               0
protocol                dtls
tls-port                23456
...
...
...
number-active-wan-interfaces 1
```

		PUBLIC	PUBLIC	PRIVATE	PRIVATE					
ADMIN	OPERATION	LAST				VSMARTS	VMANAGES	COLOR	CARRIER	
INDEX	INTERFACE	IP	PORT	IP	PORT					
STATE	STATE	CONNECTION								
0	eth0	72.28.108.37	12361	172.16.98.150	12361	2	0	silver	default	
	up	up	0:00:00:08							

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 Data Plane Security Parameters

In the data plane, IPsec is enabled by default on all routers, and by default IPsec tunnel connections use a modified version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels. On the routers, you can change the type of authentication, the IPsec rekeying timer, and the size of the IPsec anti-replay window.

### 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:



**Note** The `sha1` in the configuration options is used for historical reasons. The authentication options indicate over how much of the packet integrity checking is done. They do not specify the algorithm that checks the integrity. The authentication algorithms supported by Cisco SD-WAN do not use SHA1.

- **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 15](#).

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:

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

The configuration looks like this:



```

security
  ipsec
    rekey seconds
  !

```

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
```

TLOC ADDRESS	TLOC COLOR	SPI	SOURCE IP	SOURCE PORT	KEY HASH
172.16.255.15	lte	256	10.1.15.15	12346	*****b93a

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
```

TLOC ADDRESS	TLOC COLOR	SPI	SOURCE IP	SOURCE PORT	KEY HASH
172.16.255.15	lte	257	10.1.15.15	12346	*****b93a

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.

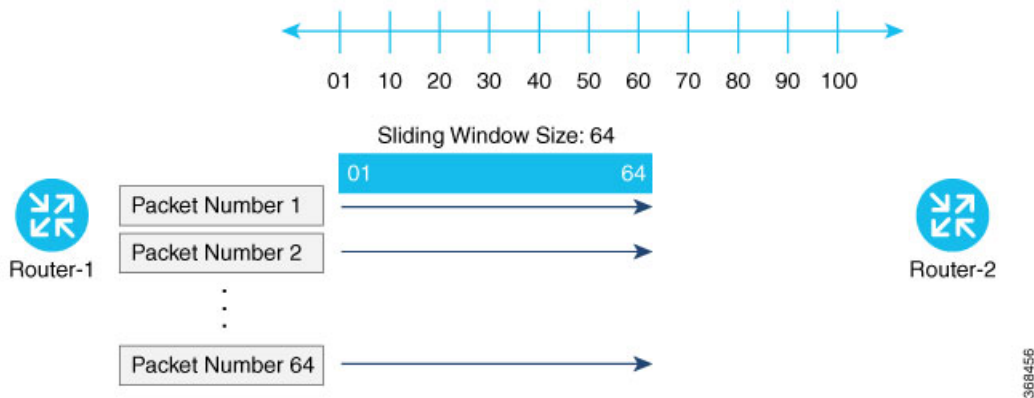
To stop using the old key immediately, issue the **request platform software sdwan security ipsec-rekey** command twice, in quick succession. This sequence of commands removes both SPI 256 and 257 and sets the SPI to 258. The router then uses the associated key of SPI 258. Note, however, that some packets 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
```

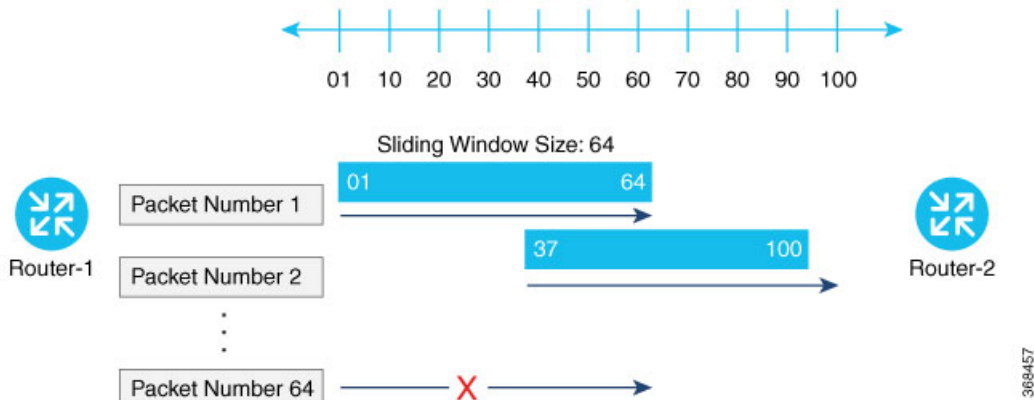
TLOC ADDRESS	TLOC COLOR	SPI	SOURCE IP	SOURCE PORT	KEY HASH
172.16.255.15	lte	258	10.1.15.15	12346	*****b93a

## 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:

Parameter Name	Description
 Device Specific	<p>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.</p> <p>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.</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
 Global	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

Once you have created and named the template, enter the following values. Parameters marked with an asterisk are required.

## Configure IPsec Tunnel Parameters

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

Parameter Name	Options	Description
<b>IPsec Rekey Interval</b>	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
<b>IKE Replay Window</b>	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
<b>IPsec Cipher Suite</b>	aes256-cbc-sha1 aes256-gcm null-sha1	Specify the authentication and encryption to use on the IPsec tunnel Default: aes256-gcm

Parameter Name	Options	Description
Perfect Forward Secrecy	<b>2</b> 1024-bit modulus <b>14</b> 2048-bit modulus <b>15</b> 3072-bit modulus <b>16</b> 4096-bit modulus <b>none</b>	Specify the PFS settings to use on the IPsec tunnel.  Select one of the following Diffie-Hellman prime modulus groups:  1024-bit – group-2 2048-bit – group-14 3072-bit – group-15 4096-bit – group-16 none –disable PFS.  <i>Default:</i> group-16

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:

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

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 3: Feature History*

Feature Name	Release Information	Description
SHA256 Support for IPsec Tunnels	Cisco IOS XE Release 17.2.1r	This feature adds support for <code>HMAC_SHA256</code> algorithms for enhanced security.

To configure IKE, click **IKE** and configure the following parameters:



**Note** 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, click **IPSEC** and configure the following parameters:

Parameter Name	Options	Description
<b>IKE Version</b>	<b>1</b> IKEv1 <b>2</b> IKEv2	Enter <b>1</b> to choose IKEv1. Enter <b>2</b> to choose IKEv2. <i>Default:</i> IKEv1

Parameter Name	Options	Description
<b>IKE Mode</b>	<b>Aggressive mode</b> <b>Main mode</b>	<p>For IKEv1 only, specify one of the following modes:</p> <ul style="list-style-type: none"> <li>• Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear.</li> <li>• Establishes an IKE SA session before starting IPsec negotiations.</li> </ul> <p><b>Note</b> For IKEv2, there is no mode.</p> <p><b>Note</b> IKE aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.</p> <p><i>Default:</i> Main mode</p>
<b>IPsec Rekey Interval</b>	3600 - 1209600 seconds	<p>Specify the interval for refreshing IKE keys.</p> <p><i>Range:</i> 1 hour through 14 days</p> <p><i>Default:</i> 14400 seconds (4 hours)</p>
<b>IKE Cipher Suite</b>	<b>3DES</b> <b>192-AES</b> <b>256-AES</b> <b>AES</b> <b>DES</b>	<p>Specify the type of authentication and encryption to use during IKE key exchange.</p> <p><i>Default:</i> 256-AES</p>
<b>IKE Diffie-Hellman Group</b>	<b>2</b> <b>14</b> <b>15</b> <b>16</b>	<p>Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.</p> <ul style="list-style-type: none"> <li>• 1024-bit modulus</li> <li>• 2048-bit modulus</li> <li>• 3072-bit modulus</li> <li>• 4096-bit modulus</li> </ul> <p><i>Default:</i> 4096-bit modulus</p>

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

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

### Change the IKE Version from IKEv1 to IKEv2

To change the IKE version, do the following:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature**, and then click **Add Template**.
3. Choose the device for which you are creating the template.
4. Click **Basic Configuration**.
5. Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.
6. Remove the ISAKMP profile from the IPsec profile.
7. 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.

---

8. 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.

---




---

**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_string
profile ikev2_profile_name
match identity remote address ip_address
authentication {remote | local} pre-share
keyring local ikev2_keyring_name
lifetime 120-86400
```



## CHAPTER 4

# 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 35](#)
- [Restrictions for Enterprise Firewall, on page 37](#)
- [Configure Firewall Policies, on page 37](#)
- [Create or Modify Lists, on page 39](#)
- [Use the Policy Configuration Wizard, on page 41](#)
- [Apply Policy to a Zone Pair, on page 45](#)
- [Apply Security Policy to a Cisco IOS XE SD-WAN Device, on page 46](#)
- [Monitor Enterprise Firewall, on page 46](#)
- [Zone-Based Firewall Configuration Examples, on page 47](#)
- [Firewall High-Speed Logging, on page 50](#)

## 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:

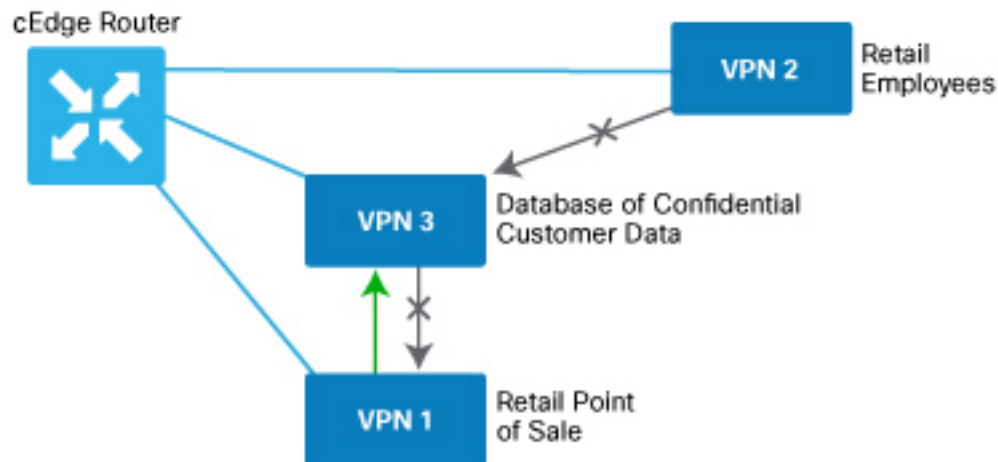
- **Source zone**—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- **Destination zone**—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- **Firewall policy**—A security policy, similar to a localized security 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. When a session is inspected, you do not need to create a service-policy that matches the return traffic.
- Pass—Allow the packet to pass to the destination zone without inspecting the packet's header at all. When a flow is passed, no sessions are created. For such a flow, you must create a service-policy that will match and pass the return traffic.

The following figure shows a simple scenario in which three VPNs are configured on a router. One of the VPNs, VPN 3, has shared resources that you want to restrict access to. These resources could be printers or confidential customer data. For the remaining two VPNs in this scenario, only users in one of them, VPN 1, are allowed to access the resources in VPN 3, while users in VPN 2 are denied access to these resources. In this scenario, we want data traffic to flow from VPN 1 to VPN 3, but we do not want traffic to flow in the other direction, from VPN 3 to VPN 1.



818878



**Note** From Cisco IOS XE SD-WAN Release 16.12.2r and onwards, vManage does not show ZBFW statistics for classes that are without any value. If the statistics are "zero" for any of the configured sequences, these are not shown on the device dashboard for zone-based firewall.

### Application Firewall

The Application Firewall blocks traffic based on applications or application-family. This application-aware firewall feature provides the following benefits:

- Application visibility and granular control
- Classification of 1400+ layer 7 applications
- Blocks traffic by application or application-family

You can create lists of individual applications or application families. A sequence that contains a specified application or application family list can be inspected. This inspect action is a Layer 4 action. Matching applications are blocked/denied.

The router provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall. Service NAT support is added for FTP ALG on the client and not on the FTP Server.



---

**Note** The Application Firewall is valid only for Cisco IOS XE SD-WAN devices.

---

## Restrictions for Enterprise Firewall

You can configure up to 200 rules for firewalls in Cisco vManage.

## Configure Firewall Policies

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.

### Configuration Components

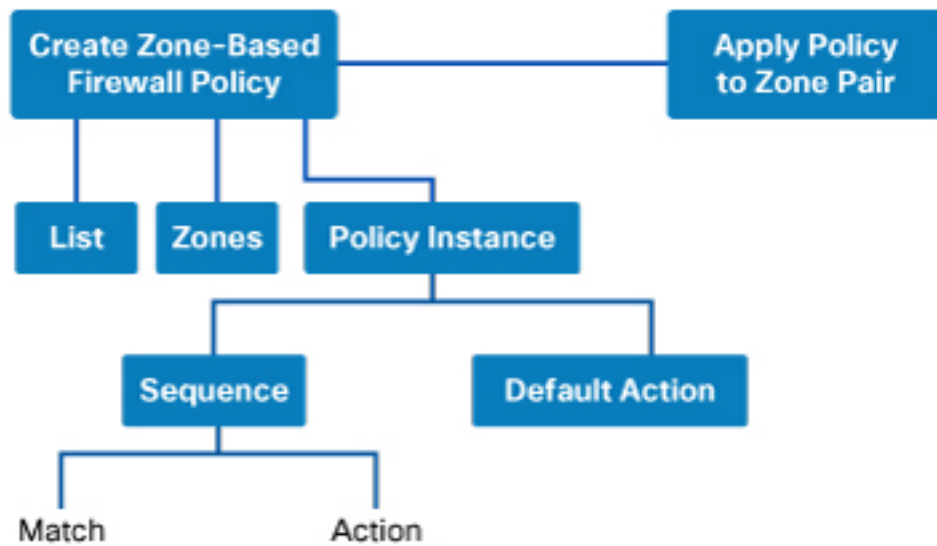
For firewall policies, you configure zones and a policy to apply to those zones.

Each zone consists of one or more VPNs in the overlay network. You define a source zone, which identifies the VPNs from which data traffic originates, and a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered (ordered) sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken and policy evaluation on that packet stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the policy sequences, you define a default action to be taken on the packet.

The following figure illustrates the configuration components for firewall policies:



968896

To create an application firewall policy, you include the following components in the configuration for a XE SD-WAN Router:

Component	Description	vManage Configuration	CLI Configuration Command
Lists	Groupings of related items that you reference in the match portion of the firewall policy configuration.	Configuration ► Security ► Custom Options ► Lists ► Application Configuration ► Security ► Custom Options ► Lists ► Zones	<b>policy lists</b>
Firewall policy	Container for a firewall policy.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy	<b>policy zone-based-policy</b>
Numbered sequences of match–action pairs	Sequences establish the order in which the policy components are applied.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule	<b>policy zone-based-policy sequence</b>
Application Match parameters	Conditions that packets must match to be considered for a security policy.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule ► Match ► Application/Application Family List	<b>policy zone-based-policy sequence match app-list</b>
Actions	For a sequence that contains an application or application family list, packets can be inspected. Matching applications are blocked/denied.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule ► Actions ► Inspect	<b>policy zone-based-policy sequence action inspect</b>

Component	Description	vManage Configuration	CLI Configuration Command
Default action	Action to take if a packet matches none of the match parameters in any of the sequences. By default, non matching packets are dropped.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule ► Actions	<b>policy zone-based-policy default-action drop</b>
Apply firewall policy to a zone pair	For a firewall policy to take effect, you include it in the definition of a zone pair.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Apply Policy	<b>policy zone-pair</b>

### General vManage Configuration Procedure

To configure firewall policies, use the vManage 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.

## Configuration Components

UTD security policy components consist of the following:

- Intrusion prevention policy—Protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.
- URL filtering policy—Allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on lists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blocked list, a custom blocked page is displayed or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the allowed list, the traffic is allowed without further URL filtering inspection.

## Create or Modify Lists

To create an application firewall policy, you include the following components in the configuration for a XE SD-WAN Router:

Component	Description	vManage Configuration	CLI Configuration Command
Lists	Groupings of related items that you reference in the match portion of the firewall policy configuration.	Configuration ► Security ► Custom Options ► Lists ► Application Configuration ► Security ► Custom Options ► Lists ► Zones	<b>policy lists</b>
Firewall policy	Container for a firewall policy.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy	<b>policy zone-based-policy</b>
Numbered sequences of match-action pairs	Sequences establish the order in which the policy components are applied.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule	<b>policy zone-based-policy sequence</b>
Application Match parameters	Conditions that packets must match to be considered for a security policy.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule ► Match ► Application/Application Family List	<b>policy zone-based-policy sequence match app-list</b>
Actions	For a sequence that contains an application or application family list, packets can be inspected. Matching applications are blocked/denied.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule ► Actions ► Inspect	<b>policy zone-based-policy sequence action inspect</b>
Default action	Action to take if a packet matches none of the match parameters in any of the sequences. By default, non matching packets are dropped.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Add Firewall Policy ► Sequence Rule ► Actions	<b>policy zone-based-policy default-action drop</b>
Apply firewall policy to a zone pair	For a firewall policy to take effect, you include it in the definition of a zone pair.	Configuration ► Security ► Add Security Policy ► <Scenario> ► Apply Policy	<b>policy zone-pair</b>

### 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.



List Type	Procedure
Application	<ol style="list-style-type: none"> <li>1. In the left pane, click <b>Application</b>.</li> <li>2. Click <b>New Application List</b>.</li> <li>3. Enter a name for the list.</li> <li>4. Select individual applications or application families.</li> <li>5. Click <b>Add</b>.</li> </ol>
Data Prefix	<ol style="list-style-type: none"> <li>1. In the left pane, click <b>Data Prefix</b>.</li> <li>2. Click <b>New Data Prefix List</b>.</li> <li>3. Enter a name for the list.</li> <li>4. Enter one or more IP prefixes.</li> <li>5. Click <b>Add</b>.</li> </ol>
Zones	<ol style="list-style-type: none"> <li>1. In the left pane, click <b>Zones</b>.</li> <li>2. Click <b>New Zone List</b>.</li> <li>3. Enter a name for the zone list.</li> <li>4. In the Add VPN field, enter the number or numbers of the VPN in the zone. Separate numbers with commas.</li> <li>5. Click <b>Add</b>.</li> </ol>

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

This article provides procedures for configuring firewall policies on XE SD-WAN Routers. You 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

1. Click the **Add Firewall Policy** drop-down.
2. To create a new firewall policy
  - a. Select **Create New**.
  - b. Enter a name and description for the policy.
  - c. Go to Step 4.
3. 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.

Otherwise, click **Next** to move to the next security block in the configuration wizard.

4. In the left pane, click **Sequence Rule** to create a single sequence in the firewall policy. The Match tab is selected by default.
5. Click a match condition:
  - Source Data Prefix
  - Source Port
  - Destination Data Prefix
  - Destination Port

- Protocol
- Application/Application Family List

6. Enter the values for the match condition.




---

**Note** If you selected an **Application** or **Application Family List**, you must select at least one other match condition.

---

7. Click the **Actions** tab.

8. Enter the action or actions to take if the traffic matches.




---

**Note** If a match condition contains an **Application** or **Application Family List**, the action must be **Inspect**. This inspect action is a Layer 4 action. The action for a specific application is block/deny.

---

9. Click **Save Match** and **Actions** to save match-action pair.

10. Repeat Steps 4 through 9 to add match–action pairs to the firewall policy.

11. To rearrange match–action pairs in the policy, drag them to the desired position.

12. To edit, copy, or delete a sequence rule, in the right pane, click the edit, copy, or delete icon to the right of the sequence rule.

13. If no packets match any of the policy sequence rules, the default action is to drop the packets. To change the default action:

- Click the **Pencil** icon.
- Change the default action to Inspect or Pass.
- Click **Save Match** and **Actions**.

### Apply Policy to a Zone Pair

*Table 4: Feature History*

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco IOS XE SD-WAN Release 16.12.1b	This feature can help define policies to impose rules on incoming and outgoing traffic.

- At the top of the page, click **Apply Zone-Pairs**.
- In the Source Zone field, select the zone that is the source of the data packets.
- In the Destination Zone field, select the zone that is the destination of the data packets.




---

**Note** 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.
  - Intrusion Prevention
  - URL Filtering
  - DNS Security

### 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:




---

**Note** For more information on HSL, see [Firewall High-Speed Logging Overview, on page 50](#).

---

- 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 configure an audit trail, enable the Audit Trail option. This option is only applicable for rules with an Inspect action.
6. Click **Save Policy** to save the security policy.

# Apply Policy to a Zone Pair

Table 5: Feature History

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco IOS XE SD-WAN Release 16.12.1b	This feature allows you to define firewall policies for incoming and outgoing traffic between a self zone of an edge router and another zone. When a self zone is configured with another zone, the traffic in this zone pair is filtered as per the applied firewall policy.



**Note** For IPSEC overlay tunnels in Cisco SD-WAN, if a self zone is selected as a zone pair, firewall sessions are created for SD-WAN overlay BFD packets if inspect action is configured for UDP.

However, for GRE overlay tunnels, if you chose a self zone as a zone pair with the inspect action of protocol 47, firewall sessions are created only for TCP, UDP, ICMP packets; but not BFD packets.



**Warning** Control connections may be impacted when you configure drop action from self-zone to VPN0 and vice versa. This applies for DTLS/TLS, BFD packets, and IPsec overlay tunnel.

To apply policy to a zone pair:

1. Create security policy using Cisco vManage. See <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-firewall-17.html#c-use-the-policy-configuration-wizard-17>
2. At the top of the page, click **Apply Zone-Pairs**.
3. In the **Source Zone** field, choose the zone that is the source of the data packets.
4. In the **Destination Zone** field, choose the zone that is the destination of the data packets.



**Note** You can choose self zone for either a source zone or a destination zone, not both.

5. Click the plus (+) icon to create a zone pair.
6. Click **Save**.
7. At the bottom of the page, click **Save Firewall Policy** to save the policy.
8. To edit or delete a firewall policy, click the **More Actions** icon in the right pane to the far right of the policy, and select the desired option.
9. Click **Next** to configure the next security block in the wizard.
  - Intrusion Prevention

- URL Filtering
- DNS Security

## Apply Security Policy to a Cisco IOS XE SD-WAN Device

To apply a security policy to an Cisco IOS XE SD-WAN device:

1. In Cisco vManage, 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 Cisco IOS XE SD-WAN devices.
  - 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).

## Monitor Enterprise Firewall

You can monitor Enterprise Firewall by using the statistics created for the firewall.

To monitor Enterprise Firewall and view statistics:

1. Cisco vManage, navigate to **Monitor** > **Network**.
2. Select a device from the list of devices.

- Under the Security Monitoring pane on the left, click **Firewall**. Here you can view the statistics for all the firewall policies created.

You can view the statistics either for a specified time range, hourly, daily, weekly, or for a customized period. To customize the time period, select **Custom** and then click on the calendar icon to input the start date and time followed by the end date and time.

## 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:

Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
TCP and UDP	10.0.0.1 172.16.0.1 192.168.0.1 255.255.0.0	200	209.165.200.225 209.165.202.129	300	drop

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

- Enable privileged EXEC mode. If prompted, enter your password.

```
Device> enable
```

- Enter global configuration mode:

```
configure transaction
```

- Create the inspect parameter map:

```
Device(config)# parameter-map type inspect-global
multi-tenancy
vpn zone security
alert on
log dropped-packets
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:

1. Select **Configuration > Security**.
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.

**Table 6: Feature History**

Feature Name	Release Information	Feature Description
Firewall High-Speed Logging	Cisco IOS XE SD-WAN Release 16.12.1b	This feature allows a firewall to log records with minimum impact to packet processing.

This module describes how to configure HSL for zone-based policy firewalls.

## 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 7: NetFlow Field IDs*

Field ID	Type	Length	Description
<b>NetFlow ID Fields (Layer 3 IPv4)</b>			
FW_SRC_ADDR_IPV4	8	4	Source IPv4 address
FW_DST_ADDR_IPV4	12	4	Destination IPv4 address
FW_SRC_ADDR_IPV6	27	16	Source IPv6 address
FW_DST_ADDR_IPV6	28	16	Destination IPv6 address
FW_PROTOCOL	4	1	IP protocol value
FW_IPV4_IDENT	54	4	IPv4 identification
FW_IP_PROTOCOL_VERSION	60	1	IP protocol version
<b>Flow ID Fields (Layer 4)</b>			
FW_TCP_FLAGS	6	1	TCP flags
FW_SRC_PORT	7	2	Source port
FW_DST_PORT	11	2	Destination port
FW_ICMP_TYPE	176	1	ICMP <sup>1</sup> type value
FW_ICMP_CODE	177	1	ICMP code value
FW_ICMP_IPV6_TYPE	178	1	ICMP Version 6 (ICMPv6) type value
FW_ICMP_IPV6_CODE	179	1	ICMPv6 code value
FW_TCP_SEQ	184	4	TCP sequence number
FW_TCP_ACK	185	4	TCP acknowledgment number
<b>Flow ID Fields (Layer 7)</b>			

Field ID	Type	Length	Description
FW_L7_PROTOCOL_ID	95	2	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.
<b>Flow Name Fields (Layer 7)</b>			
FLOW_FIELD_L7_PROTOCOL_NAME	96	32	Layer 7 protocol name. Identifies the Layer 7 protocol name that corresponds to the Layer 7 protocol ID (FW_L7_PROTOCOL_ID).
<b>Flow ID Fields (Interface)</b>			
FW_SRC_INTF_ID	10	2	Ingress SNMP <sup>2</sup> ifIndex
FW_DST_INTF_ID	14	2	Egress SNMP ifIndex
FW_SRC_VRF_ID	234	4	Ingress (initiator) VRF <sup>3</sup> ID
FW_DST_VRF_ID	235	4	Egress (responder) VRF ID
FW_VRF_NAME	236	32	VRF name
<b>Mapped Flow ID Fields (Network Address Translation)</b>			
FW_XLATE_SRC_ADDR_IPV4	225	4	Mapped source IPv4 address
FW_XLATE_DST_ADDR_IPV4	226	4	Mapped destination IPv4 address
FW_XLATE_SRC_PORT	227	2	Mapped source port
FW_XLATE_DST_PORT	228	2	Mapped destination port
<b>Status and Event Fields</b>			
FW_EVENT	233	1	High level event codes <ul style="list-style-type: none"> <li>• 0—Ignore (invalid)</li> <li>• 1—Flow created</li> <li>• 2—Flow deleted</li> <li>• 3—Flow denied</li> <li>• 4—Flow alert</li> </ul>
FW_EXT_EVENT	35,001	2	Extended event code. For normal records the length is 2 byte, and 4 byte for optional records.
<b>Timestamp and Statistics Fields</b>			

Field ID	Type	Length	Description
FW_EVENT_TIME_MSEC	323	8	Time, in milliseconds, (time since 0000 hours UTC <sup>4</sup> January 1, 1970) when the event occurred (if the event is a microevent, use 324 and 325, if it is a nanoevent)
FW_INITIATOR_OCTETS	231	4	Total number of Layer 4 payload bytes in the packet flow that arrives from the initiator
FW_RESPONDER_OCTETS	232	4	Total number of Layer 4 payload bytes in the packet flow that arrives from the responder
<b>AAA Fields</b>			
FW_USERNAME	40,000	20 or 64 depending on the template	AAA <sup>5</sup> user name
FW_USERNAME_MAX	40,000	64	AAA user name of the maximum permitted size
<b>Alert Fields</b>			
FW_HALFOPEN_CNT	35,012	4	Half-open session entry count
FW_BLACKOUT_SECS	35,004	4	Time, in seconds, when the destination is shutdown or unavailable
FW_HALFOPEN_HIGH	35,005	4	Configured maximum rate of TCP half-open session entries logged in one minute
FW_HALFOPEN_RATE	35,006	4	Current rate of TCP half-open session entries logged in one minute
FW_MAX_SESSIONS	35,008	4	Maximum number of sessions allowed for this zone pair or class ID
<b>Miscellaneous</b>			
FW_ZONEPAIR_ID	35,007	4	Zone pair ID
FW_CLASS_ID	51	4	Class ID
FW_ZONEPAIR_NAME	35,009	64	Zone pair name
FW_CLASS_NAME	100	64	Class name
FW_EXT_EVENT_DESC	35,010	32	Extended event description

Field ID	Type	Length	Description
FLOW_FIELD_CTS_SRC_GROUP_TAG	34000	2	Cisco Trustsec source tag
FW_SUMMARY_PKT_CNT	35,011	4	Number of packets represented by the drop/pass summary record
FW_EVENT_LEVEL	33003	4	Defines the level of the logged event <ul style="list-style-type: none"> <li>• 0x01—Per box</li> <li>• 0x02—VRF</li> <li>• 0x03—Zone</li> <li>• 0x04—Class map</li> <li>• Other values are undefined</li> </ul>
FW_EVENT_LEVEL_ID	33,004	4	Defines the identifier for the FW_EVENT_LEVEL field <ul style="list-style-type: none"> <li>• If FW_EVENT_LEVEL is 0x02 (VRF), this field represents VRF_ID.</li> <li>• If FW_EVENT_LEVEL is 0x03 (zone), this field represents ZONE_ID.</li> <li>• If FW_EVENT_LEVEL is 0x04 (class map), this field represents CLASS_ID.</li> <li>• 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.</li> </ul>
FW_CONFIGURED_VALUE	33,005	4	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.
FW_ERM_EXT_EVENT	33,006	2	Extended event-rate monitoring code
FW_ERM_EXT_EVENT_DESC	33,007	N (string)	Extended event-rate monitoring event description string

<sup>1</sup> Internet Control Message Protocol

<sup>2</sup> Simple Network Management Protocol

<sup>3</sup> virtual routing and forwarding

<sup>4</sup> Coordinated Universal Time

<sup>5</sup> Authentication, Authorization, and Accounting

## HSL Messages

The following are sample syslog messages from Cisco SD-WAN IOS XE Router:

**Table 8: Syslog Messages and Their Templates**

Message Identifier	Message Description	HSL Template
FW-6-DROP_PKT Type: Info	Dropping %s pkt from %s %CA:%u => %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  %CA:%u ip/ip6 addr: port  %s:%s: zone pair name/ class name  %s "due to"  %s: fw_ext_event name  %u ip ident  %s: if tcp, tcp seq/ack number and tcp flags  %s: username	FW_TEMPLATE_DROP_V4 or FW_TEMPLATE_DROP_V6

Message Identifier	Message Description	HSL Template
FW-6-SESS_AUDIT_TRAIL_START Type: Info	<p>(target:class)-(%s:%s):Start %s session: initiator (%CA:%u) -- responder (%CA:%u) from %s %s %s</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%s: 14/17 protocolname</p> <p>%CA:%u ip/ip6 addr: port</p> <p>%s : interface</p> <p>%s : username</p> <p>%s : TODO</p> <p>Actual log:</p> <p>*Jan 21 20:13:01.078: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:125 TS:00000010570290947309 %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</p>	FW_TEMPLATE_START_AUDIT_V4 or FW_TEMPLATE_START_AUDIT_V6



Message Identifier	Message Description	HSL Template
FW-6-SESS_AUDIT_TRAIL Type: Info	<p>(target:class)-(%s:%s):Stop %s session: initiator (%CA:%u) sent %u bytes -- responder (%CA:%u) sent %u bytes , from %s %s</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%s: I4/I7 protocolname</p> <p>%CA:%u ip/ip6 addr: port</p> <p>%u bytes counters</p> <p>%s: interface</p> <p>%s : TODO</p> <p>Actual log:</p> <p>*Jan 21 20:13:15.889:            %IOSXE-6-PLATFORM: F0:            cpp_cp: CPP:00 Thread:036            TS:00000010585102587819            %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</p>	FW_TEMPLATE_STOP_AUDIT_V4 or FW_TEMPLATE_STOP_AUDIT_V6

Message Identifier	Message Description	HSL Template
FW-4-UNBLOCK_HOST Type: Warning	(target:class)-(%s:%s):New TCP connections to host %CA no longer blocked  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.  %s:%s: zonepair name: class name  %CA: ip/ip6 addr	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
FW-4-HOST_TCP_ALERT_ON Type: Warning	"(target:class)-(%s:%s):Max tcp half-open connections (%u) exceeded for host %CA.  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.  %s:%s: zonepair name: class name  %u: half open cnt  %CA: ip/ip6 addr	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

Message Identifier	Message Description	HSL Template
FW-2- BLOCK_HOST Type: Critical	<p>(target:class)-(%s:%s):Blocking new TCP connections to host %CA for %u minute%s (half-open count %u exceeded).</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%CA: ip/ip6 addr</p> <p>%u blockout min</p> <p>%s: s if &gt; 1 min blockout time</p> <p>%u: half open counter</p>	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_BLOCK_HOST
FW-4-ALERT_ON Type: Warning	<p>(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%s: "getting aggressive"</p> <p>%u/%u halfopen cnt/high</p> <p>%u: current rate</p>	FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_ON

Message Identifier	Message Description	HSL Template
FW-4-ALERT_OFF Type: Warning	<p>(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%s: "calming down"</p> <p>%u/%u halfopen cnt/high</p> <p>%u: current rate</p>	<p>FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_OFF</p>
FW-4-SESSIONS_MAXIMUM Type: Warning	<p>Number of sessions for the firewall policy on "(target:class)-(%s:%s) exceeds the configured sessions maximum value %u</p> <p>Explanation: The number of established sessions have crossed the configured sessions maximum limit.</p> <p>%s:%s: zonepair name: class name</p> <p>%u: max session</p>	FW_TEMPLATE_ALERT_MAX_SESSION

Message Identifier	Message Description	HSL Template
FW-6-PASS_PKT Type: Info	<p>Passing %s pkt from %s %CA:%u =&gt; %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u</p> <p>Explanation: Packet is passed by firewall inspection.</p> <p>%s: tcp/udp/icmp/unknown prot</p> <p>%s:interface</p> <p>%CA:%u src ip/ip6 addr: port</p> <p>%CA:%u dst ip/ip6 addr: port</p> <p>%s:%s: zonepair name: class name</p> <p>%s %s: "due to", "PASS action found in policy-map"</p> <p>%u: ip ident</p>	FW_TEMPLATE_PASS_V4 or FW_TEMPLATE_PASS_V6
FW-6-LOG_SUMMARY Type: Info	<p>%u packet%s %s from %s %CA:%u =&gt; %CA:%u (target:class)-(%s:%s) %s</p> <p>Explanation : Log summary for the number of packets dropped/passed</p> <p>%u %s: pkt_cnt, "s were" or "was"</p> <p>%s: "dropped"/ "passed"</p> <p>%s: interface</p> <p>%CA:%u src ip/ip6 addr: port</p> <p>%CA:%u dst ip/ip6 addr: port</p> <p>%s:%s: zonepair name: class name</p> <p>%s: username</p>	FW_TEMPLATE_SUMMARY_V4 or FW_TEMPLATE_SUMMARY_V6 with FW_EVENT: 3 - drop 4 - pass

## 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](#).

## 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

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>parameter-map type inspect-global</b> <b>Example:</b> Device(config)# parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.
<b>Step 4</b>	<b>log dropped-packets</b> <b>Example:</b> Device(config-profile)# log dropped-packets	Enables dropped-packet logging.
<b>Step 5</b>	<b>log flow-export v9 udp destination <i>ip-address port-number</i>vrf <i>vrf-label</i></b> <b>Example:</b> cEdge(config-profile)# log flow-export v9 udp destination 10.20.25.18 2055 vrf 1	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.
<b>Step 6</b>	<b>log flow-export template timeout-rate <i>seconds</i></b> <b>Example:</b> Device(config-profile)# log flow-export template timeout-rate 5000	Template timeout-rate is the interval (in seconds) at which the netflow template formats are advertised.

	Command or Action	Purpose
Step 7	<b>end</b> <b>Example:</b> Device(config-profile)# end	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

## 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

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>parameter-map type inspect</b> <i>parameter-map-name</i> <b>Example:</b> Device(config)# parameter-map type inspect parameter-map-hsl	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the <b>inspect</b> keyword, and enters parameter-map type inspect configuration mode.
Step 4	<b>audit-trail on</b> <b>Example:</b> 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.

	Command or Action	Purpose
<b>Step 5</b>	<b>one-minute</b> { <i>low number-of-connections</i>   <b>high</b> <i>number-of-connections</i> } <b>Example:</b> Device(config-profile)# one-minute high 10000	Defines the number of new unestablished sessions that cause the system to start deleting half-open sessions and stop deleting half-open sessions.
<b>Step 6</b>	<b>tcp max-incomplete host</b> <i>threshold</i> <b>Example:</b> Device(config-profile)# tcp max-incomplete host 100	Specifies the threshold and blocking time values for TCP host-specific, denial of service (DoS) detection and prevention.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> Device(config-profile)# exit	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
<b>Step 8</b>	<b>policy-map type inspect</b> <i>policy-map-name</i> <b>Example:</b> Device(config)# policy-map type inspect policy-map-hsl	Creates an inspect-type policy map and enters policy map configuration mode.
<b>Step 9</b>	<b>class type inspect</b> <i>class-map-name</i> <b>Example:</b> Device(config-pmap)# class type inspect class-map-tcp	Specifies the traffic class on which an action is to be performed and enters policy-map class configuration mode.
<b>Step 10</b>	<b>inspect</b> <i>parameter-map-name</i> <b>Example:</b> Device(config-pmap-c)# inspect parameter-map-hsl	(Optional) Enables stateful packet inspection.
<b>Step 11</b>	<b>end</b> <b>Example:</b> Device(config-pmap-c)# end	Exits policy-map class configuration mode and returns to privileged EXEC mode.

## 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-profile)# 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 67](#)
- [Cisco SD-WAN IPS Solution, on page 68](#)
- [Configure and Apply IPS or IDS, on page 68](#)
- [Modify an Intrusion Prevention or Detection Policy, on page 72](#)
- [Delete an Intrusion Prevention or Detection Policy , on page 72](#)
- [Monitor Intrusion Prevention Policy, on page 73](#)
- [Update IPS Signatures, on page 75](#)

## 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 down 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](#)

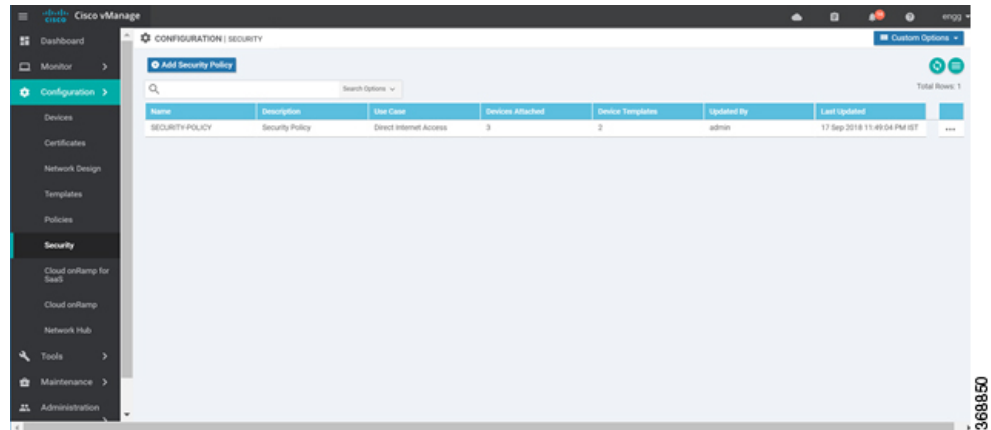
### Before you Begin

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](#).

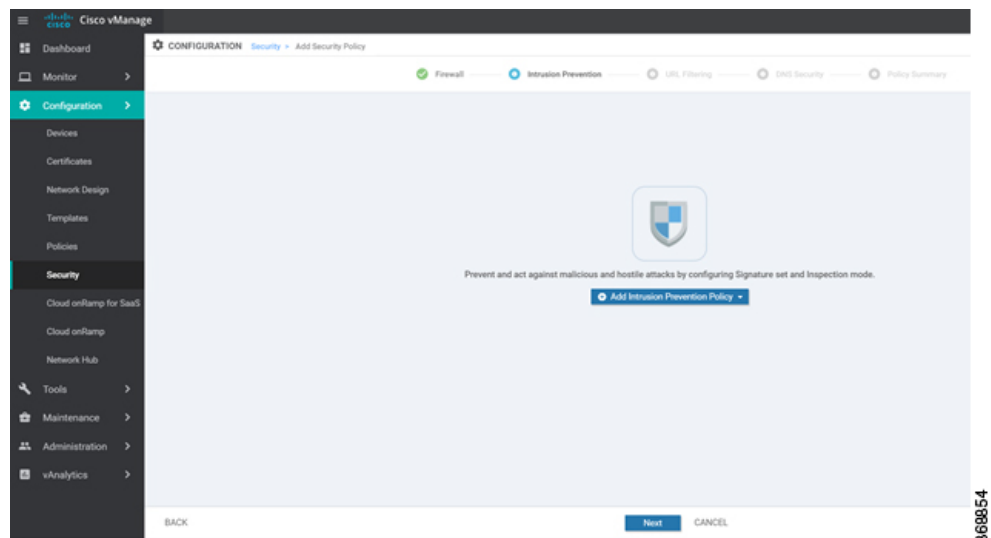
### Configure Intrusion Prevention or Detection

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 target service 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 lists or create new ones as needed from the **Signature Whitelist** drop-down.

Selecting an IPS signature list 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 list from an accessible storage location. Click **Save** when you are finished.

You also can create or manage IPS Signature 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 list 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

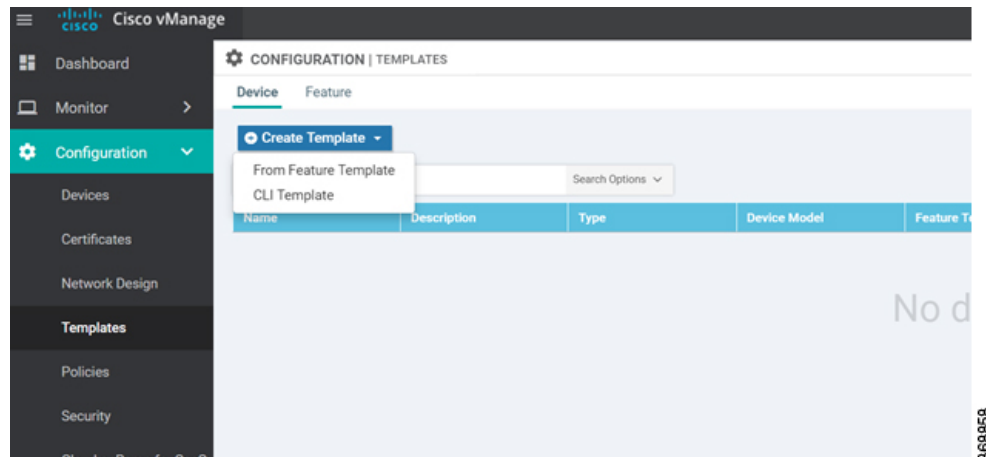
You must configure the address of the external log server in the Policy Summary page.

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.

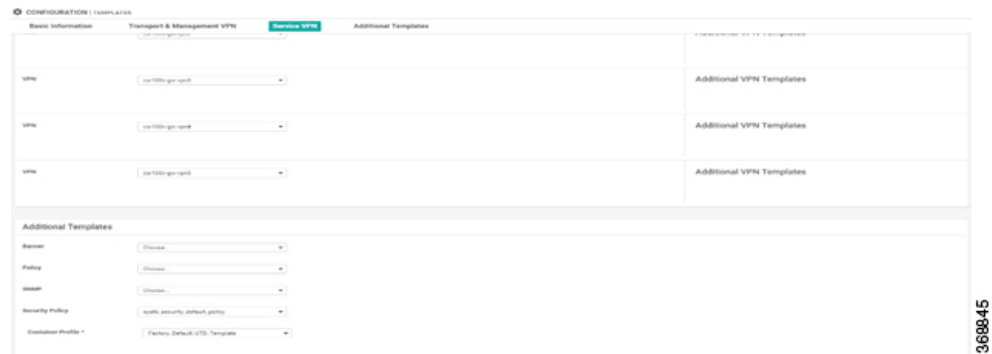
## Apply a Security Policy to a Device

To apply a security policy to a device:

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



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 IOS XE SD-WAN devices.
4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.

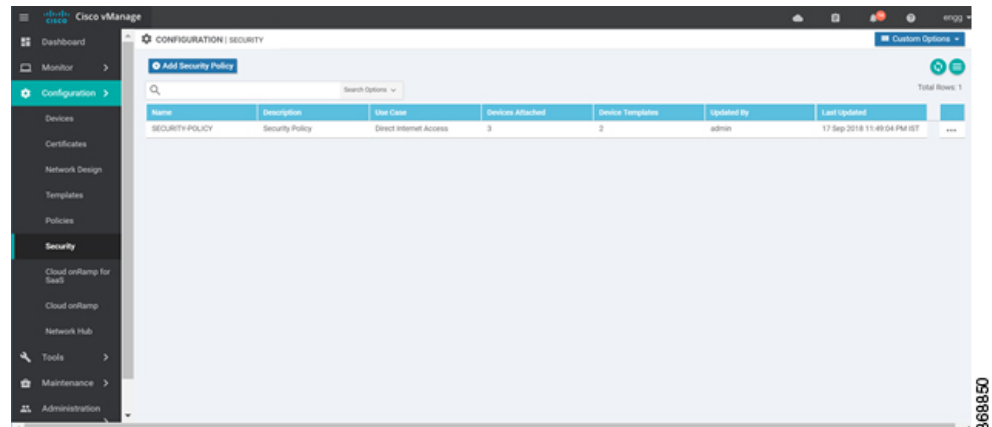


5. From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.
6. Click **Create** to apply the security policy to a device.

## Modify an Intrusion Prevention or Detection Policy

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

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



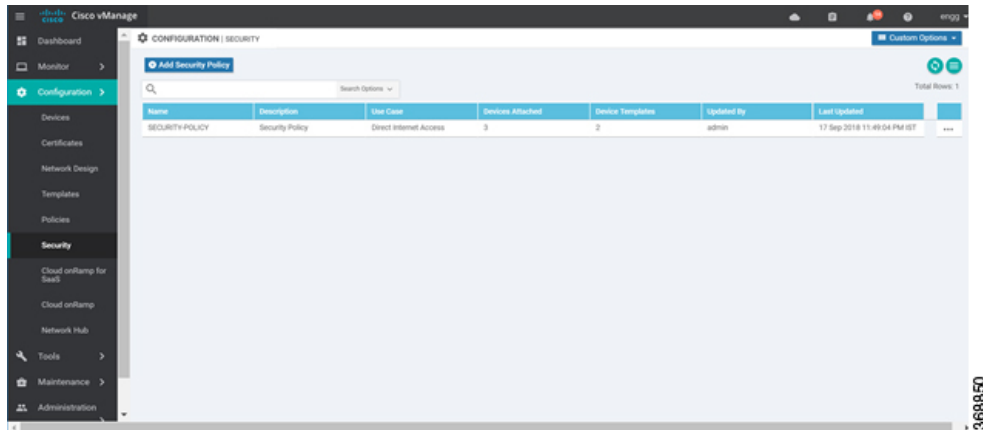
2. In the Security screen, click the **Custom Options** drop-down and select **Intrusion Prevention**.
3. For the policy that you want to modify, click the **More Actions** icon to the far right of the policy and select **Edit**.
4. Modify the policy as required and click **Save Intrusion Prevention 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.





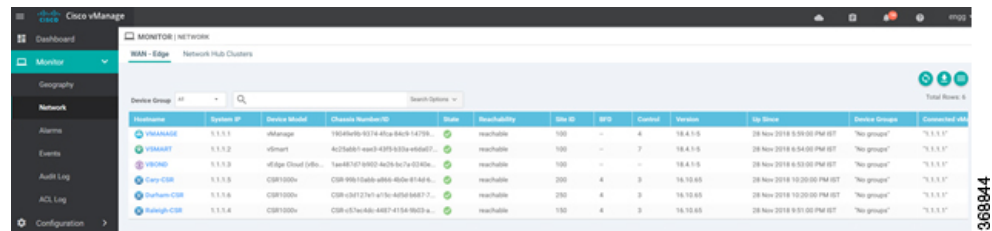
2. Detach the IPS or IDS policy from the security policy as follows:
  - a. For the security policy that contains the IPS or IDS policy, click the **More Actions** icon to the far right of the policy and select **Edit**.  
The Policy Summary page is displayed.
  - b. Click the **Intrusion Prevention** 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:
  - a. In the Security screen, click the **Custom Options** drop-down and select **Intrusion Prevention**.
  - 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 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:

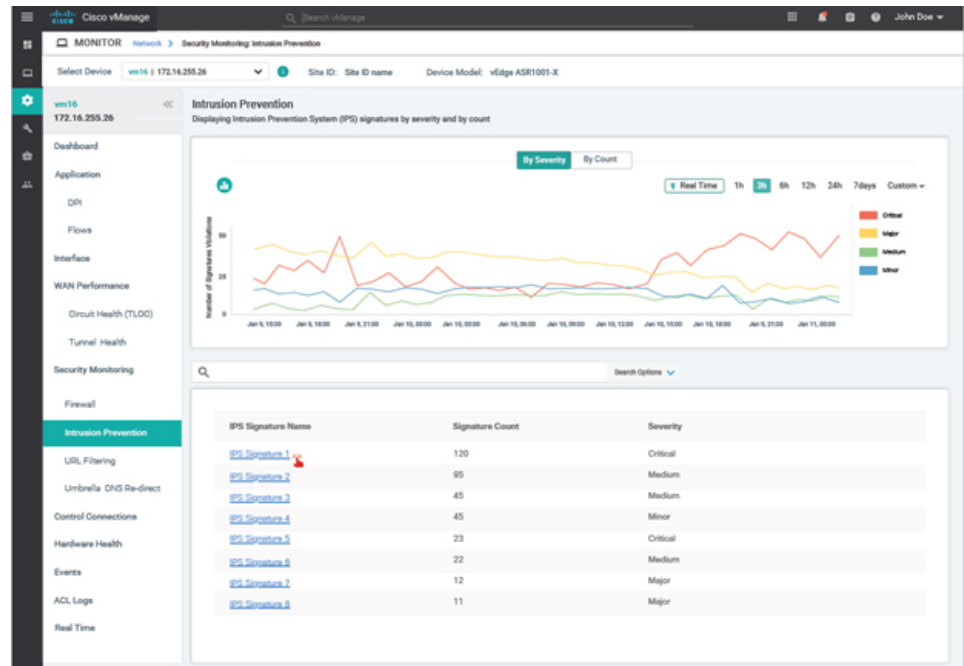
1. From the **Monitor** > **Network** screen, select a device.



Device Name	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	SPS	Control	Version	Last Sync	Device Group	Connected At
VWANASD	5.1.1.1	vManage	19024676-9374-45ca-86c9-14709...	OK	reachable	100	-	4	18.4.1.5	28 Nov 2018 5:59:00 PM IST	"No group"	"5.1.1.1"
VWANAT	5.1.1.2	vSmart	AC2246811-eac3-4378-833a-vb6d07...	OK	reachable	100	-	7	18.4.1.5	28 Nov 2018 6:54:00 PM IST	"No group"	"5.1.1.1"
VWANG	5.1.1.3	vEdge Cloud (S/W)	1ee48767-8902-4a29-bc7a-0340a...	OK	reachable	100	-	-	18.4.1.5	28 Nov 2018 6:53:00 PM IST	"No group"	"5.1.1.1"
Core-CDR	5.1.1.5	CSR1000v	CSR-995-10486-a856-846a-81442...	OK	reachable	200	4	3	18.10.85	28 Nov 2018 10:20:00 PM IST	"No group"	"5.1.1.1"
Spine-CDR	5.1.1.6	CSR1000v	CSR-v34727a1-a71e-4d5d-8a477...	OK	reachable	200	4	3	18.10.85	28 Nov 2018 10:20:00 PM IST	"No group"	"5.1.1.1"
Leaf-CDR	5.1.1.4	CSR1000v	CSR-v57a44b-44d7-4154-9052...	OK	reachable	100	4	3	18.10.85	28 Nov 2018 9:51:00 PM IST	"No group"	"5.1.1.1"

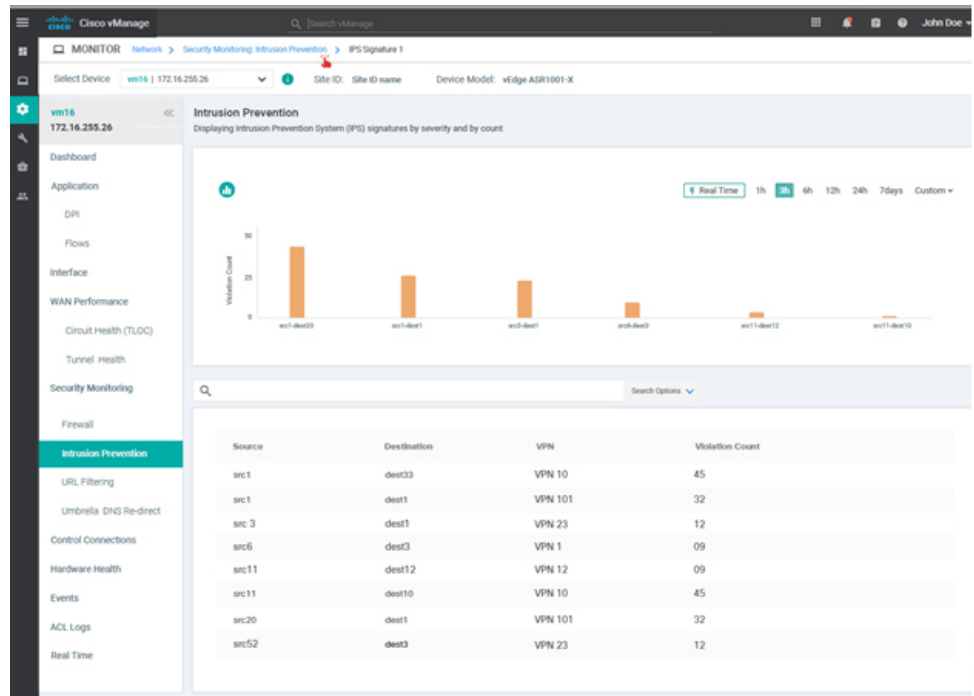
368844

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



368849

- 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
- cloudssso.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.

AS ADMINISTRATION | SETTINGS

Call Home	Disabled	View   Edit
Client Session Timeout	Disabled	View   Edit
Data Stream	Enabled	View   Edit
Tenancy Mode	Single Tenant	View   Edit
Statistics Configuration	Collection Interval: 30 minutes	View   Edit
Maintenance Window	Not Configured	Edit
Identity Provider Settings	Disabled	View   Edit
Statistics Database Configuration	Maximum Available Space: 243.7238 GB	View   Edit
Google Map API Key	Maps API Key: AIzaSyA1PwZuB1TnFLCE-5atpM0EuphV318	View   Edit
Software Install Timeout	Collection Interval: 60 minutes	View   Edit

**IPS Signature Update**

Enabled  Disabled

Username:

Password:

IPS Signature Download Interval (Range: 1 to 24 hrs)

Hours:  Minutes:

369856



## 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 77](#)
- [Configure and Apply URL Filtering, on page 79](#)
- [Modify URL Filtering, on page 84](#)
- [Delete URL Filtering, on page 84](#)
- [Monitor URL Filtering, on page 85](#)

## 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 displayed. URL Filtering will not decode any encoded URL before performing a lookup.

When there is no allowed 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




---

**Note** 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.




---

**Note** The URL Filtering database is periodically updated from the cloud in every 15 minutes.

---

### 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\foo\com` but also want to block other URLs such as `www\foo\abc` and `www\foo\xyz`, you can configure `www\foo\com` in the allowed list and `www\foo\` 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:

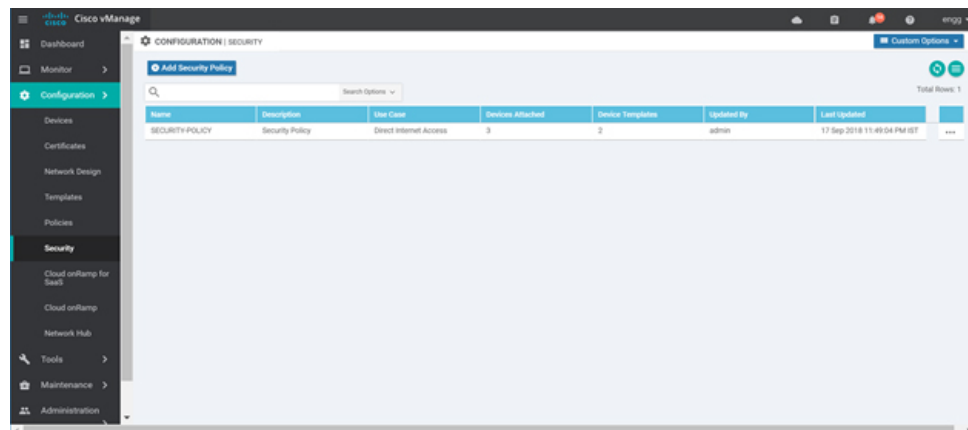
### Before you Begin

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](#).

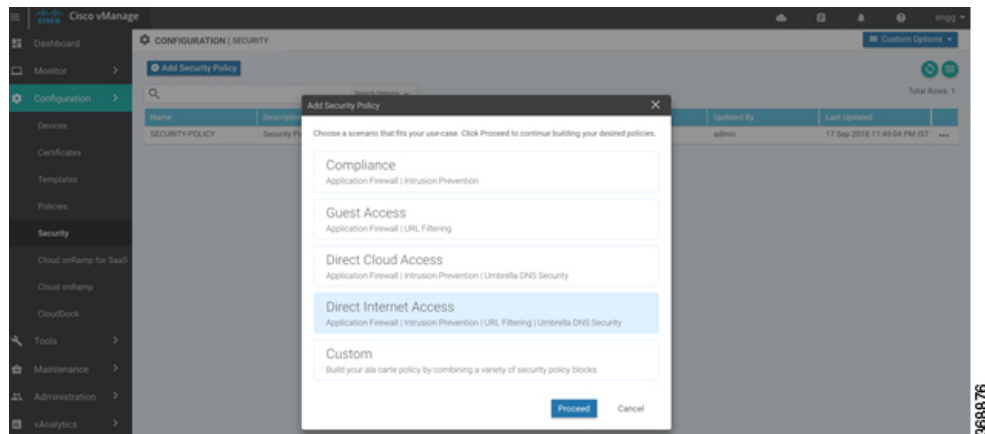
### Configure URL Filtering

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

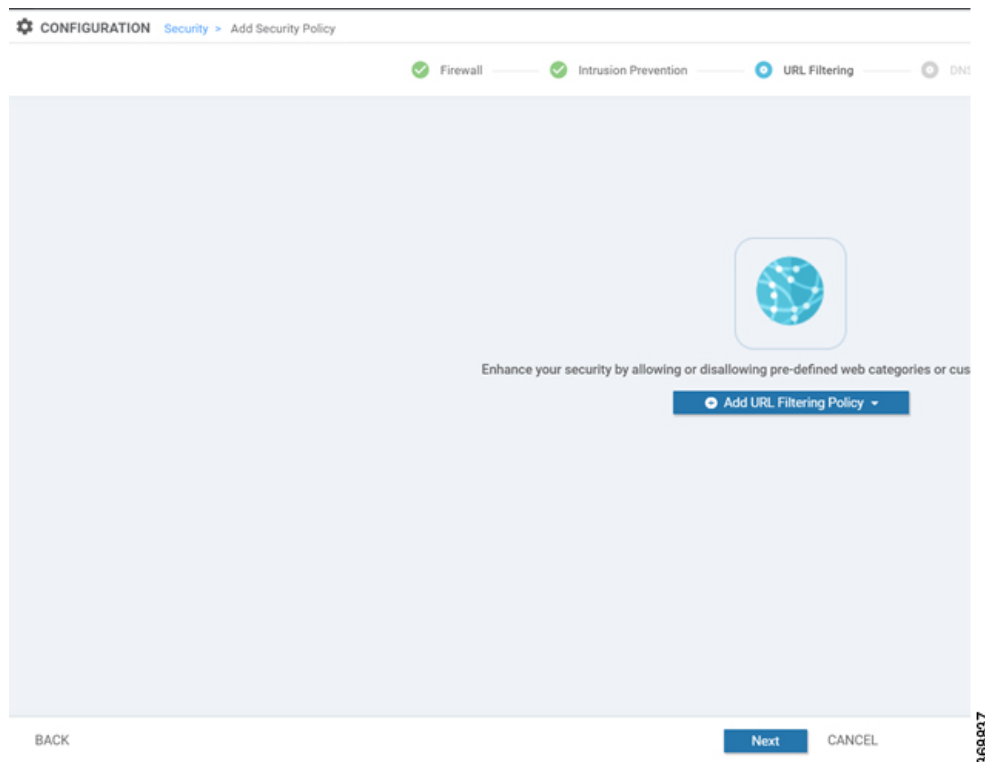
1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.



2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.

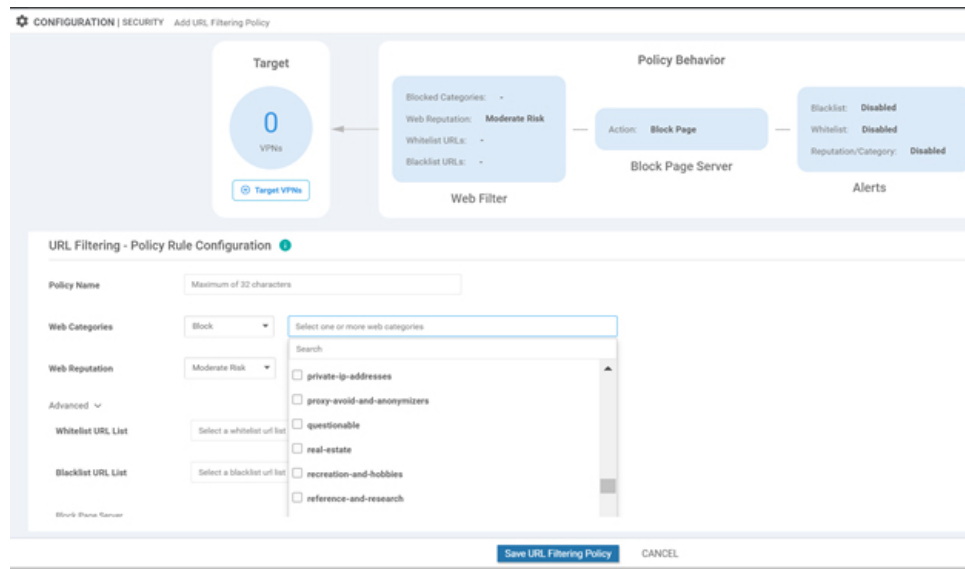


3. In Add Security Policy, select a scenario that supports URL filtering (**Guest Access, Direct Internet Access, or Custom**).
4. Click **Proceed** to add a URL filtering policy in the wizard.
5. In the **Add Security Policy** wizard, click **Next** until the **URL Filtering** screen is displayed.



6. Click the **Add URL Filtering Policy** drop-down and choose **Create New** to create a new URL filtering policy. The URL filtering - 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 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 0 to 40.
  - **Moderate Risk**: Reputation score of 0 to 60.
  - **Low Risk**: Reputation score of 0 to 80.
  - **Trustworthy**: Reputation score of 0 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.

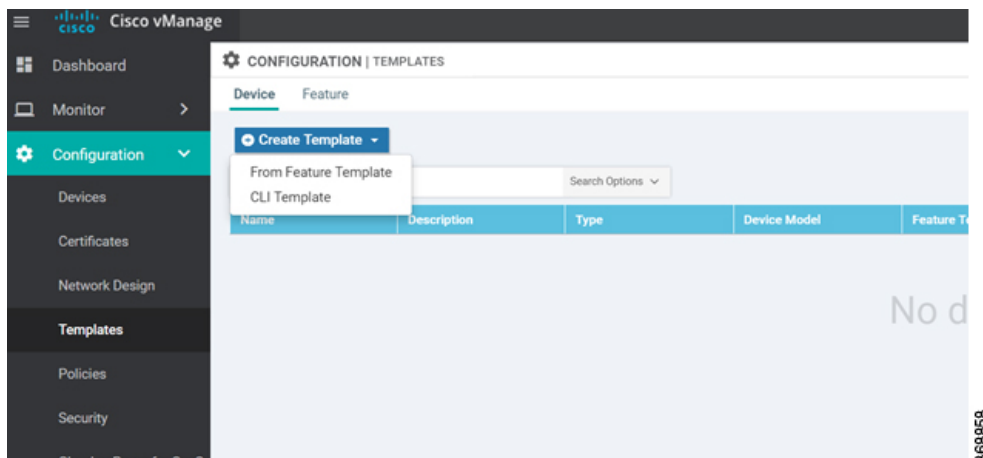


17. Click **Next** until the Policy Summary page is displayed.
18. Enter Security Policy Name and Security Policy Description in the respective fields.
19. If you enabled Alerts and Logs, in the Additional Policy Settings section you must specify the following:
  - External Syslog Server VPN: The syslog 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

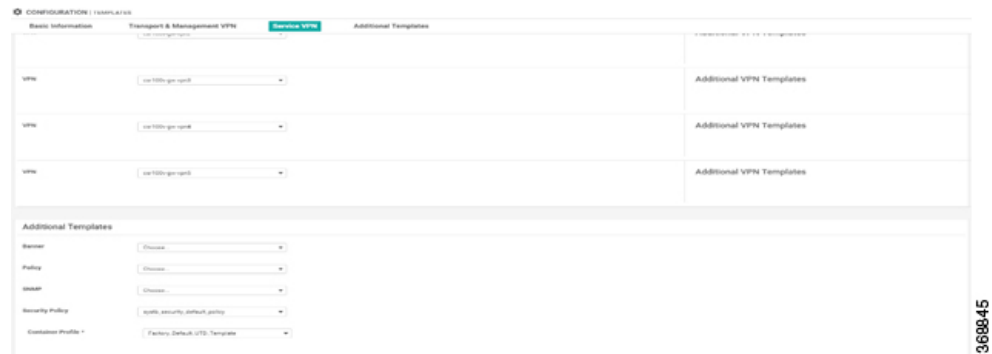
To apply a security policy to a device:

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



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 IOS XE SD-WAN devices.

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

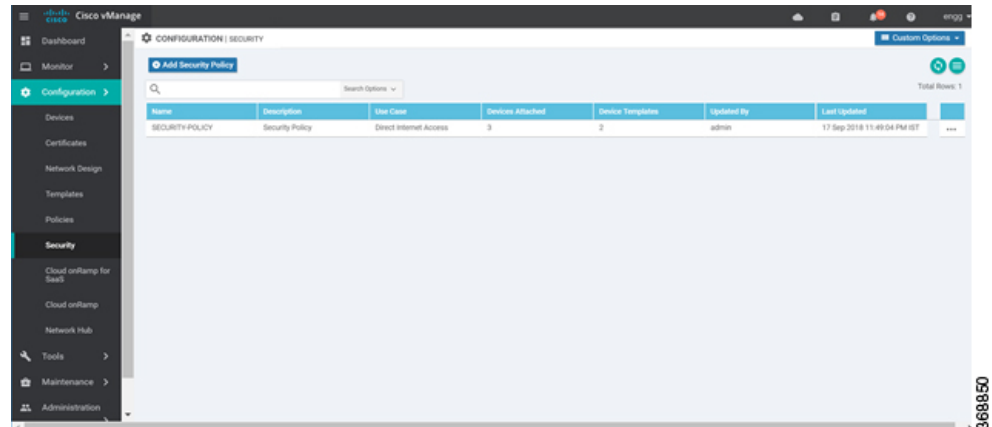


- From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.
- Click **Create** to apply the security policy to a device.

## Modify URL Filtering

To modify a URL Filtering policy, do the following:

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

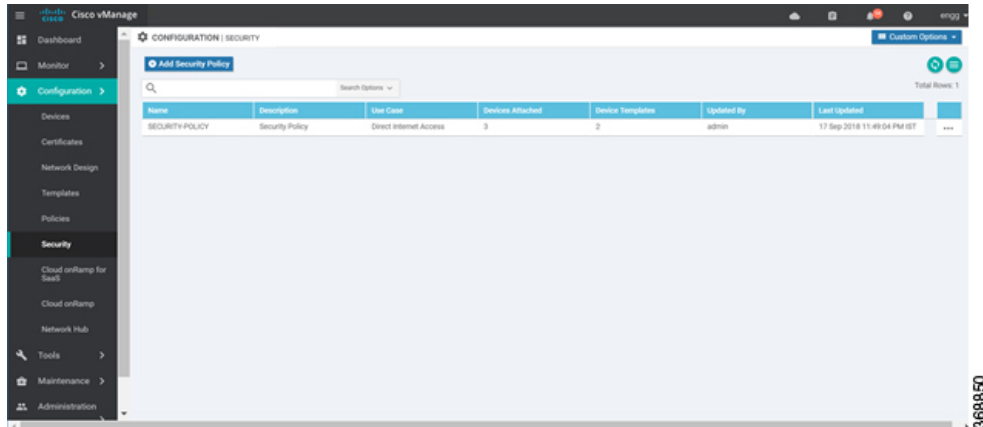


- In the Security screen, click the **Custom Options** drop-down and select **URL Filtering**.
- For the policy that you want to modify, click the **More Actions** icon to the far right of the policy and select **Edit**.
- Modify the policy as required and click **Save URL Filtering Policy**.

## Delete URL Filtering

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

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



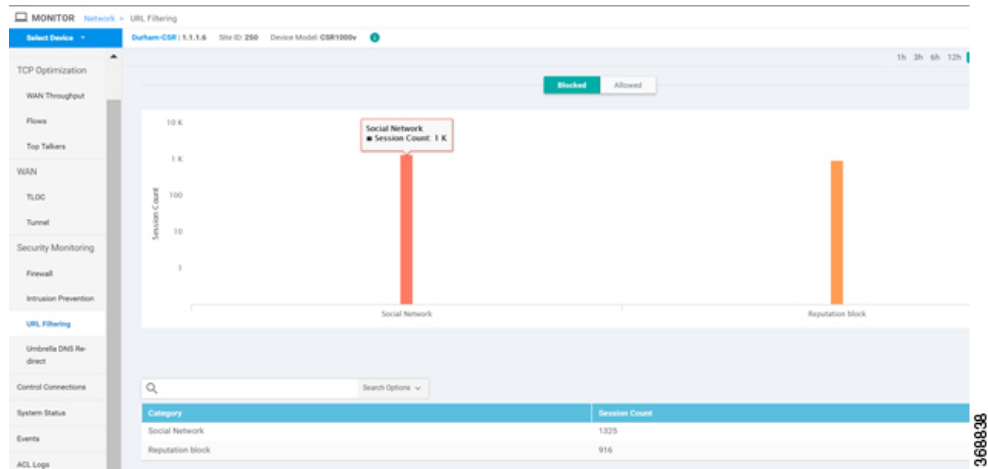
2. Detach the URL filtering policy from the security policy as follows:
  - a. For the security policy that contains the URL filtering policy, click the **More Actions** icon to the far right of the policy and select **Edit**.  
The Policy Summary page is displayed.
  - b. Click the **URL Filtering** 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

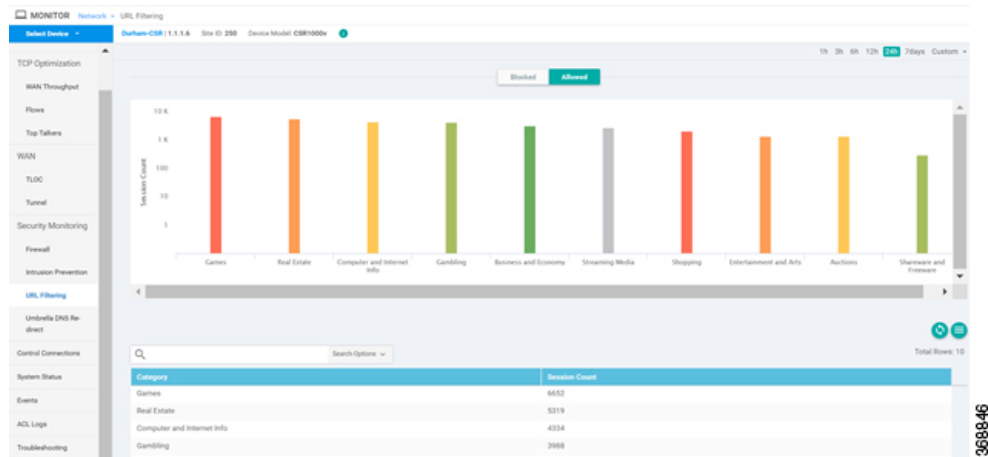
You can monitor the URL Filtering for a device by web categories using the following steps.

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.





## CHAPTER 7

# 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 9: Feature History**

Release	Description
Cisco SD-WAN 19.1	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.

- [Overview of Advanced Malware Protection, on page 87](#)
- [Configure and Apply an Advanced Malware Policy, on page 88](#)
- [Modify an Advanced Malware Protection Policy, on page 92](#)
- [Delete an Advanced Malware Protection Policy, on page 93](#)
- [Monitor Advanced Malware Protection, on page 94](#)
- [Troubleshoot Advanced Malware Protection, on page 95](#)
- [Rekey the Device Threat Grid API Key, on page 95](#)

## 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 88](#)
- [Configure and Apply an Advanced Malware Policy, on page 88](#)
- [Apply a Security Policy to a Device, on page 71](#)

### 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 88](#)

### Configure Threat Grid API Key

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

- 
- Step 1** Log into your Cisco AMP Threat Grid dashboard, and select your account details.
- Step 2** 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 > API Key.

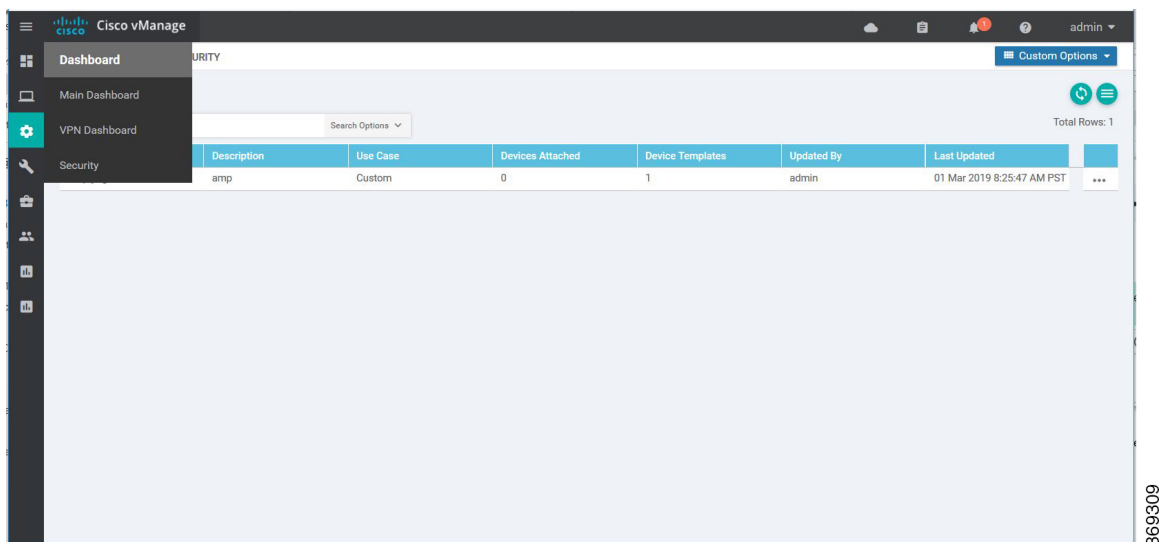


- Step 3** In Cisco vManage, select the **Configuration > Security** tab in the left side panel.
- Step 4** In the Security screen, click the **Custom Options** drop-down and select **Threat Grid API Key**.
- Step 5** In the Manage Threat Grid API key pop-up box, take these actions:
- Choose a region from the **Region** drop-down.
  - Enter the API key in the **Key** field.
  - Click **Add**.
  - Click **Save Changes**.

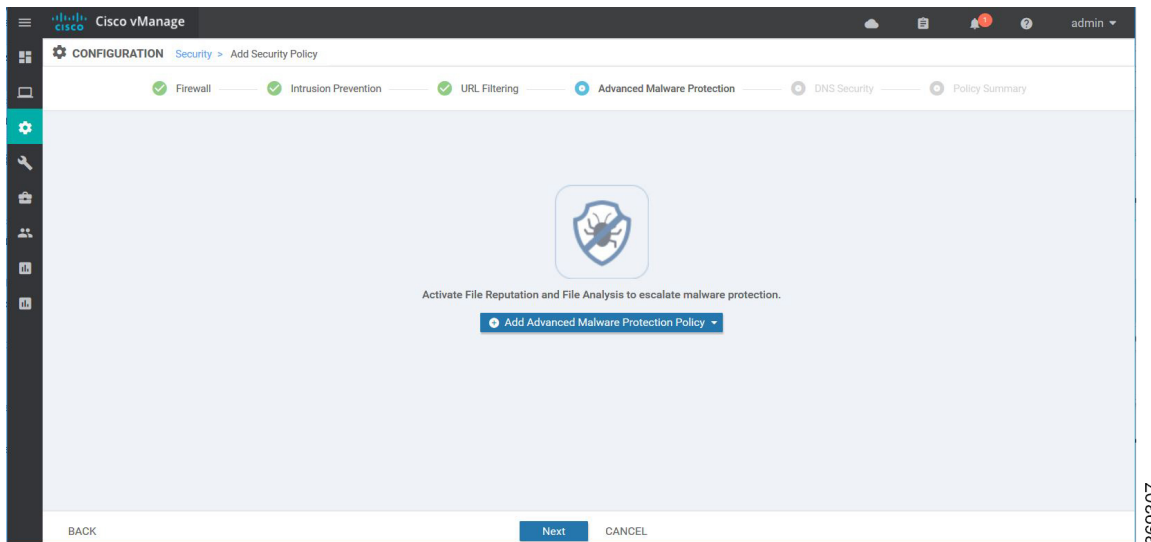
## Configuring an Advanced Malware Protection Policy

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.

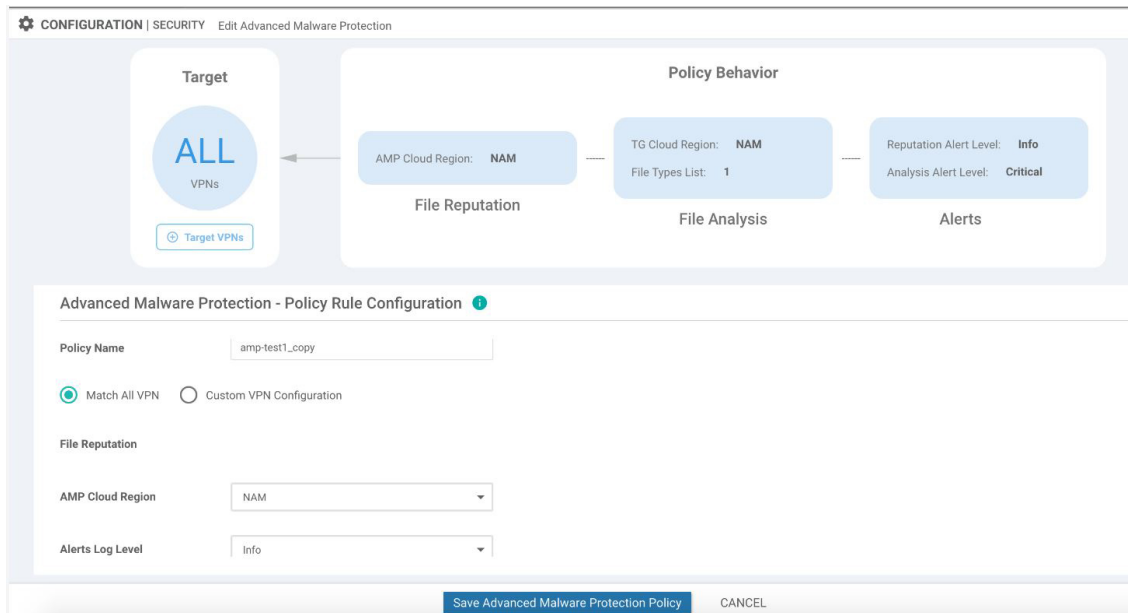


- Step 3** In Add Security Policy, select **Direct Internet Access** and then click **Proceed**.
- Step 4** In the Add Security Policy wizard, click **Next** as needed to select the **Advanced Malware Protection** tab.



369307

- 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.



369308

- 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 88.

Advanced Malware Protection - Policy Rule Configuration

File Analysis

TG Cloud Region: NAM

Threat Grid API Key: ✔ Configured [View API Key](#)

File Types List: All

Alerts Log Level: Critical

Save Advanced Malware Protec

Manage Threat Grid API Key

TG Cloud Region: NAM

Device Admin API Key: 1234890okjhgf34rqwe82821

TG Cloud Region: EU

Device Admin API Key: 1232w2828890okjhgf34r

Save Changes Cancel

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

369311

**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 88

**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**.

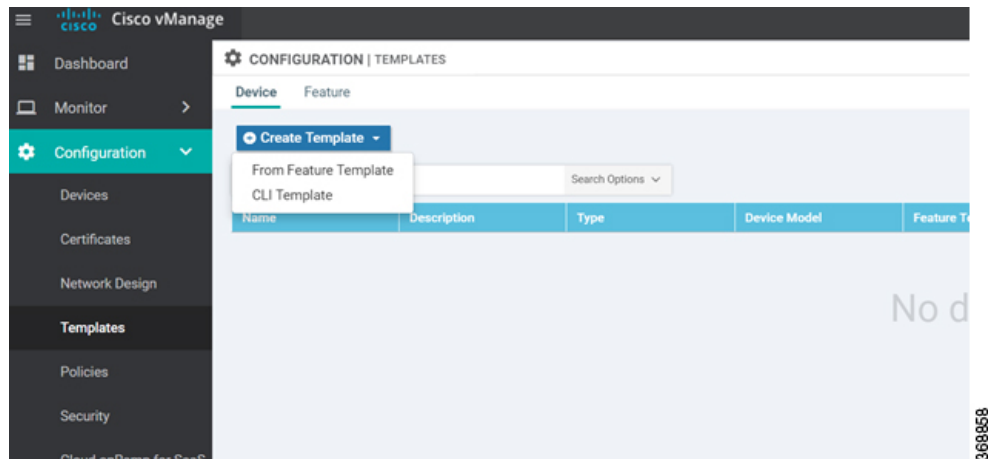
**Step 16** Click **Save Changes**. The Policy Summary screen displays.

**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 IOS XE SD-WAN devices.
4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.

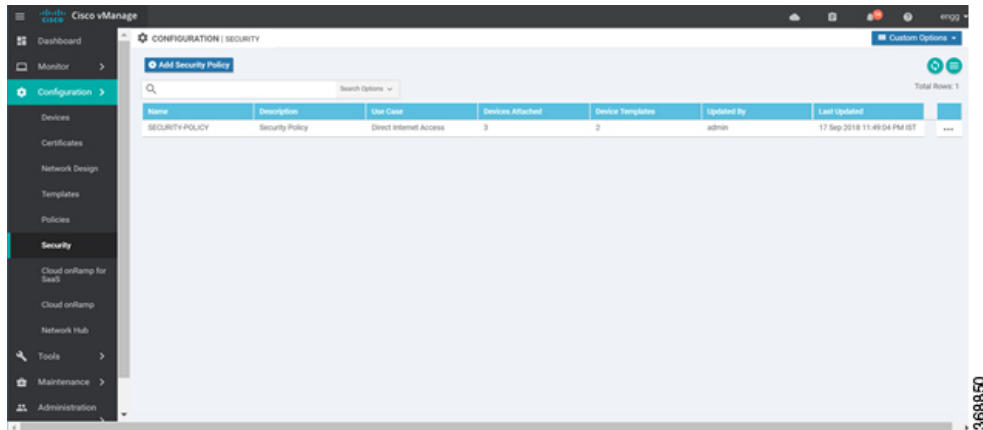


5. From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.
6. Click **Create** to apply the security policy to a device.

## 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.

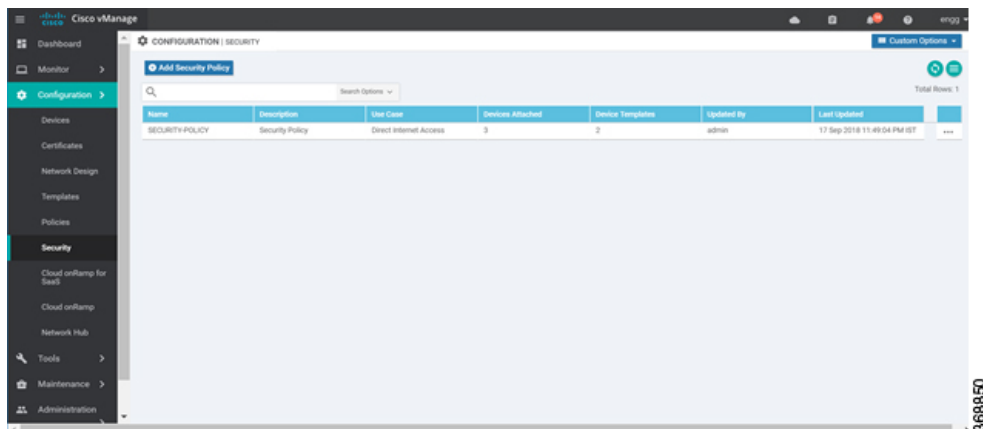


2. In the Security screen, click the **Custom Options** drop-down and select **Advanced Malware Protection**.
3. For the policy that you want to modify, click the **More Actions** icon to the far right of the policy and select **Edit**.
4. Modify the policy as required and click **Save Advanced Malware 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

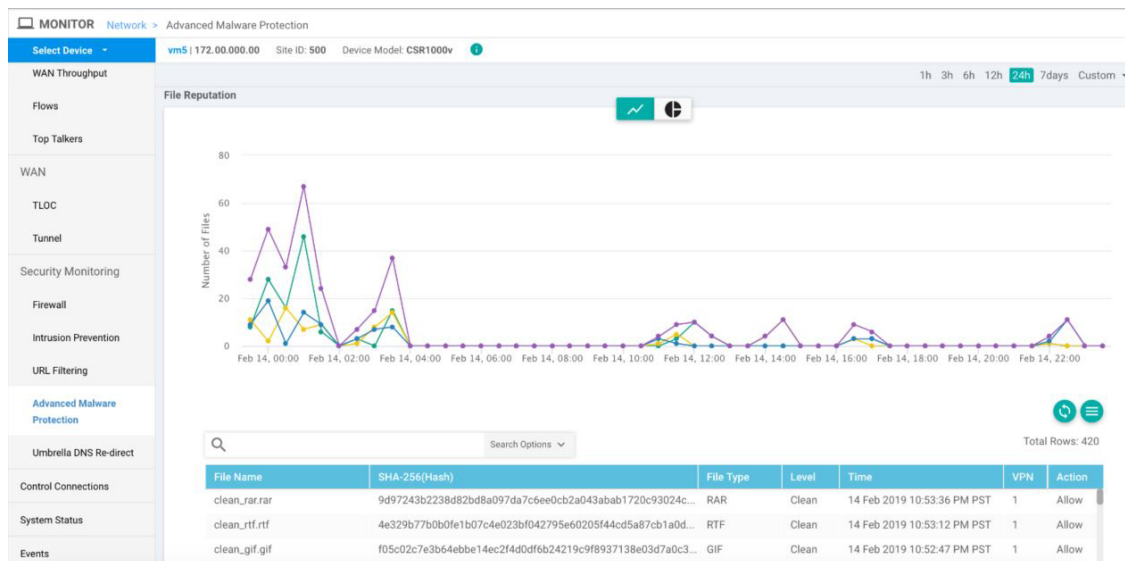
You can monitor Advanced Malware Protection from the Device Dashboard by using the following steps.

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

**Step 2** In the left panel, under Security Monitoring, select the **Advanced Malware Protection** tab.

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.



369310

# 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**.
-







## CHAPTER 8

# SD-WAN 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 97](#)
- [Restrictions for Umbrella Integration, on page 100](#)
- [Prerequisites for Umbrella Integration, on page 100](#)
- [Configure Umbrella API Token, on page 100](#)
- [Define Domain Lists, on page 101](#)
- [Configure Umbrella DNS Policy Using vManage, on page 102](#)
- [Apply DNS Umbrella Policy to an IOS XE Router, on page 106](#)
- [Monitoring Umbrella Feature, on page 107](#)
- [Umbrella Integration Using CLI, on page 108](#)
- [DNS Security Policy Configuration, on page 120](#)

## Overview of Cisco SD-WAN Umbrella Integration

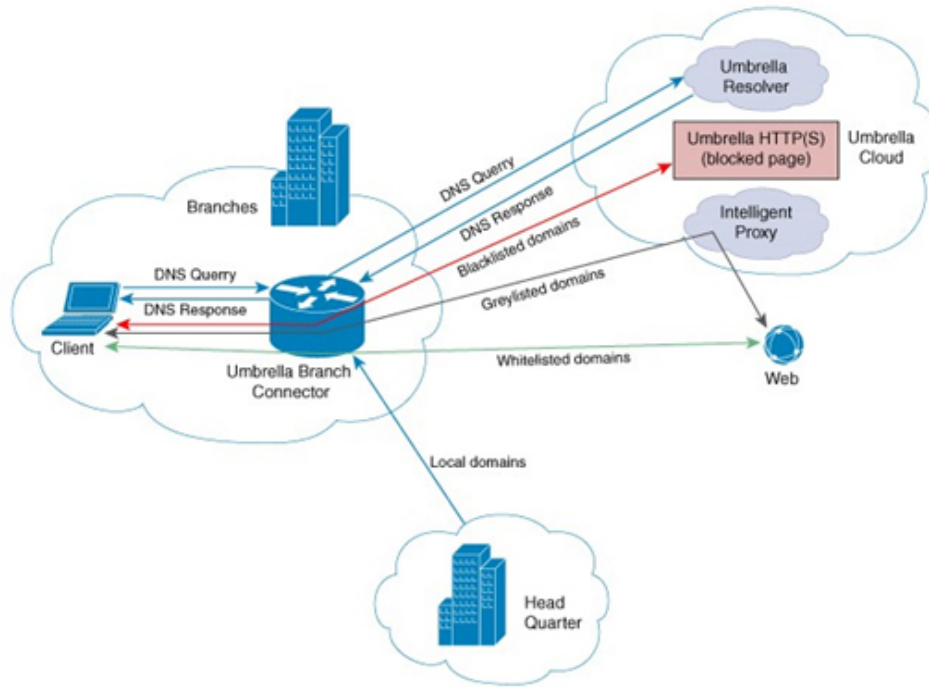
The Cisco SD-WAN Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through the device. When a host initiates the traffic and sends a DNS query, the Umbrella Connector in the device intercepts and inspects the DNS query. If the 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 1: Umbrella Cloud



368871

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 Cisco 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 allowedlisted 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 DNSCrypt 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 2: Umbrella Integration Topology**



## 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

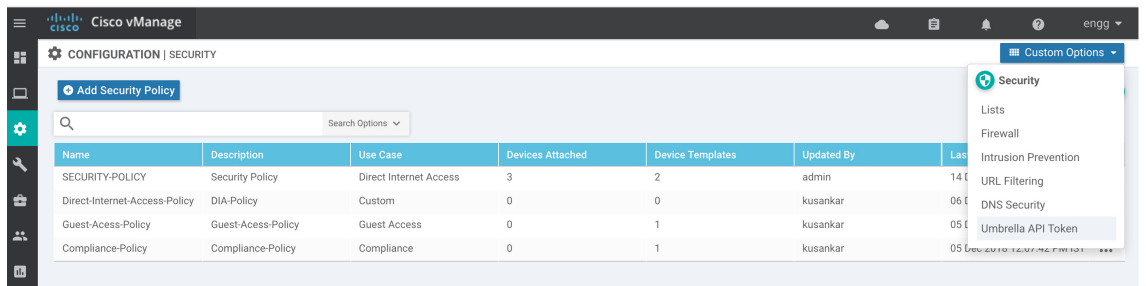
Before you configure the Umbrella Integration feature, ensure that the following are met:

- 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 NMS, select the **Configuration > Security tab > Custom Options** on the right side to configure the Umbrella API.
2. Select **Umbrella API Token**.



3. Enter token number in the **Umbrella Token** field.



**Note** Must be exactly 40 hexadecimal.

4. Click **Save Changes** to configure the Umbrella API Token.

## Define Domain Lists

To define Domain-List, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the **Configuration > Security tab > Custom Options** in the right side.



2. Click on **Lists** in the Custom Options drop-down.
3. Select **Domain** from the left pane.
4. Click on **New Domain List** to create a new domain list or select the domain name and click on pencil icon on the right side for the existing list.
5. Enter the **Domain List Name**, **Add Domain** and click **Add** to create the

- Application
- Data Prefix
- Domain
- Signatures
- Whitelist URLs
- Blacklist URLs
- Zones

+ New Domain List

Domain List Name

Add Domain

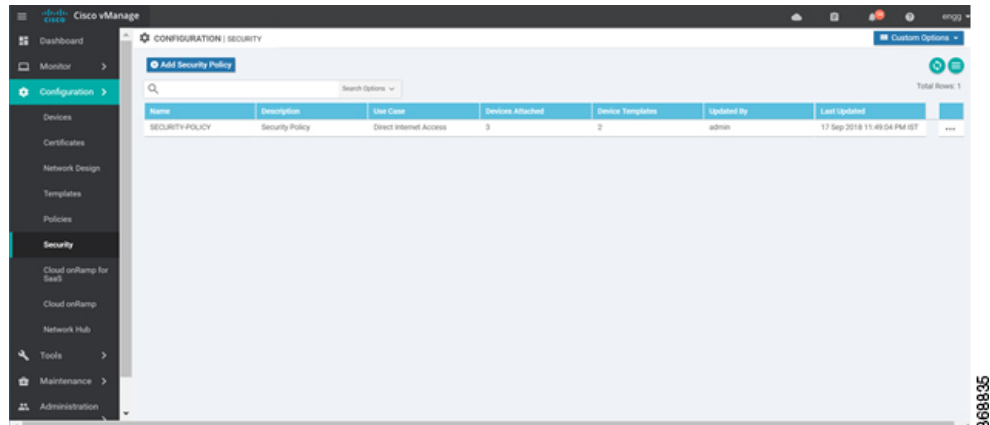
Example: cisco.com, \*.cisco.com, \*.cisco.com separated by commas. Should not start with '\*' or '+' and not more than 240 characters

Add
Cancel

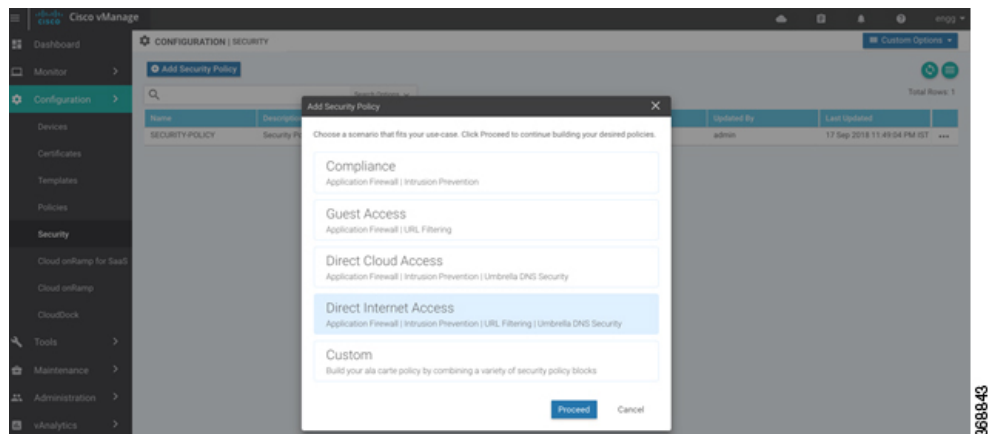
# Configure Umbrella DNS Policy Using vManage

To configure umbrella through DNS Security:

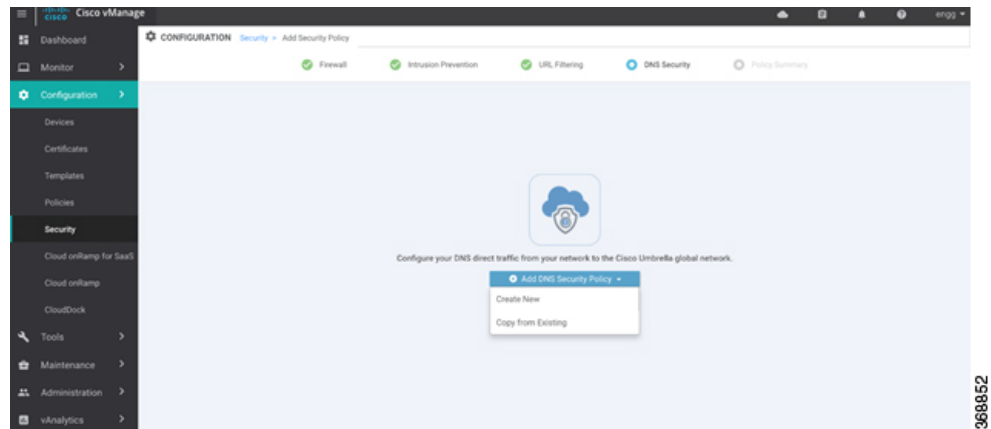
1. In Cisco vManage NMS, select the **Configuration** > **Security** tab in the left side panel.



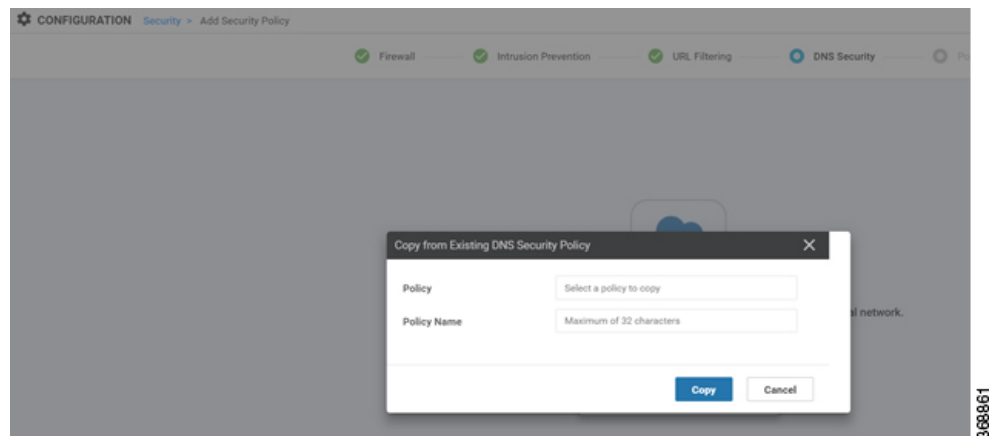
2. Click **Add Security Policy**. The Add Security Policy wizard appears.



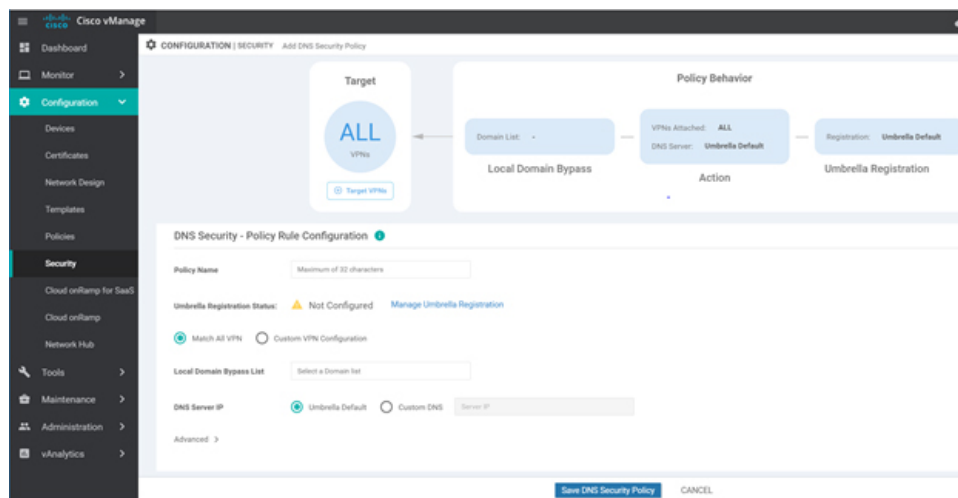
3. The Add Security Policy configuration wizard opens, and various use-case scenarios display.
4. In Add Security Policy, select **Direct Internet Access**.
5. Click **Proceed** to add an Umbrella DNS Security policy in the wizard.
6. In the Add Security Policy wizard, select **DNS Security** tab to create a new DNS Security policy.



7. Click the **Add DNS Security Policy** drop-down and select from the following options:
- Create New - A DNS Security - Policy Rule Configuration wizard appears and continue with Step 8.
  - Copy from Existing - A Copy from Existing DNS Security Policy wizard appears. Select a **Policy** from the drop-down and enter **Policy Name** and copy the policy to a device.

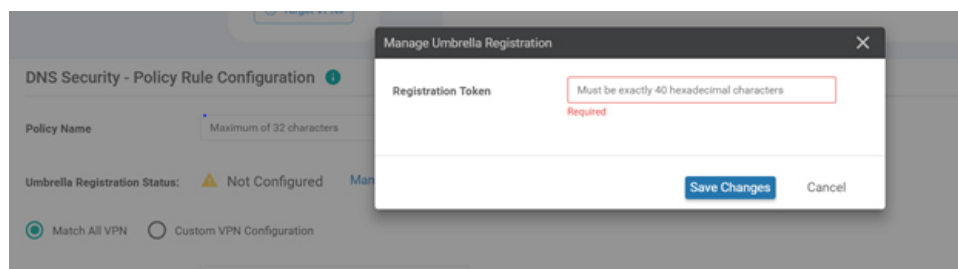


8. If you are creating a new policy using **Create New**, a DNS Security - Policy Rule Configuration wizard appears.



368863

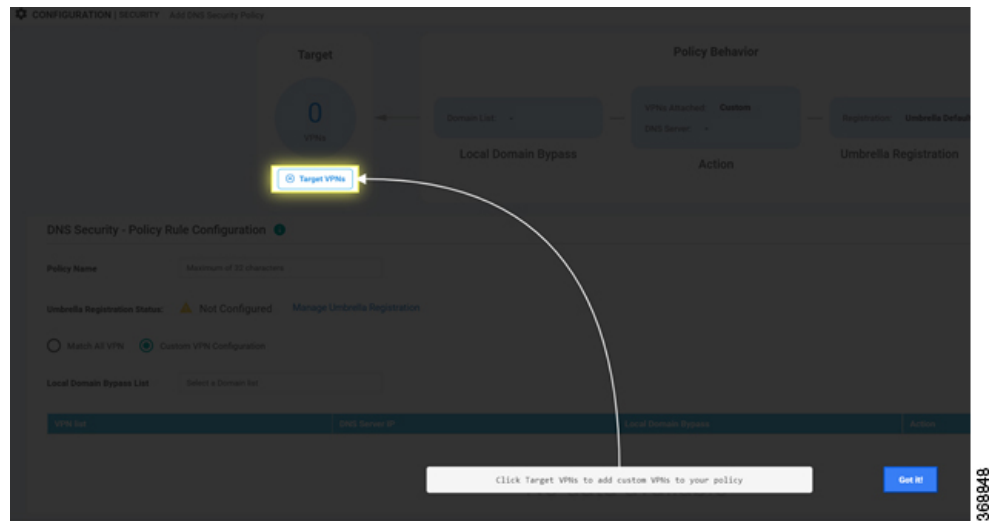
9. Enter a policy name in the **Policy Name** field.
10. The Umbrella Registration Status displays the status about the API Token configuration.
11. Click on **Manage Umbrella Registration** to add a token.



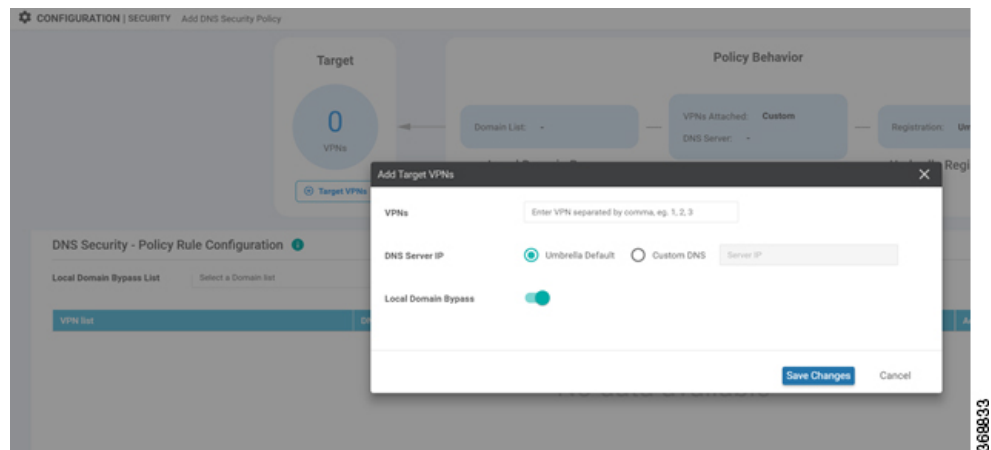
368867

12. Select **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.

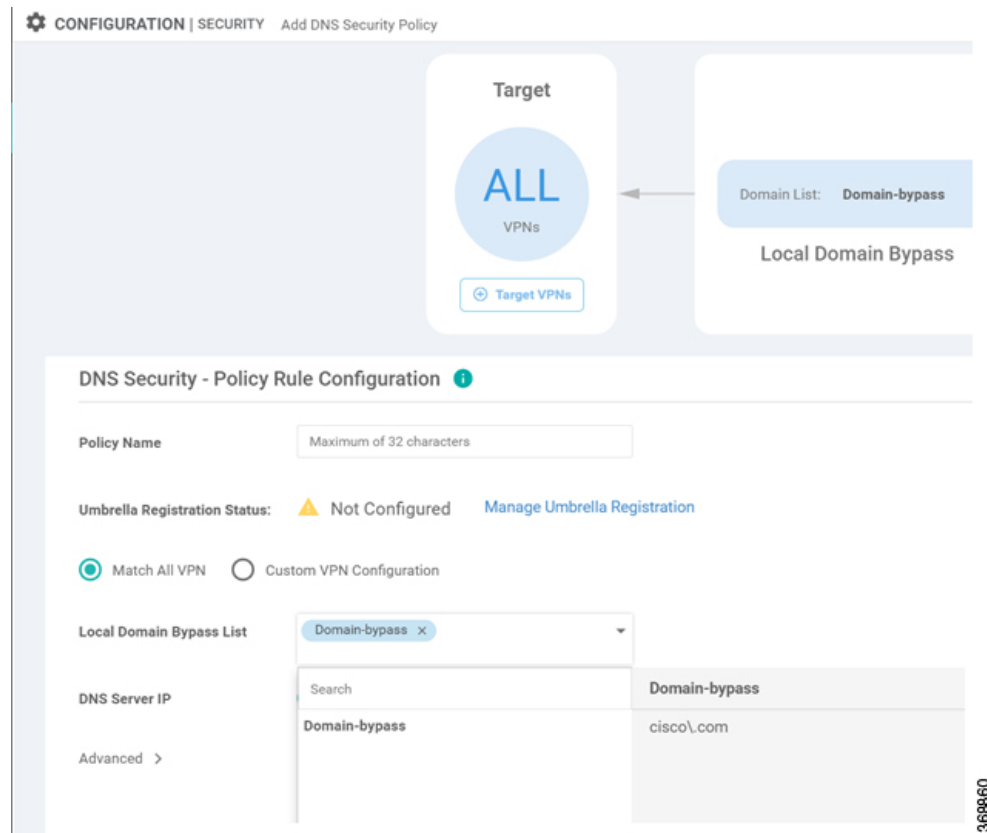




- To add target VPNs, click **Target VPNs** in the Add DNS Security Policy wizard.



- Click **Save Changes** to add the VPN.
- Select the domain bypass from the **Local Domain Bypass List** drop-down as shown.



368860

16. Configure the **DNS Server IP** from the following options:
  - Umbrella Default
  - Custom DNS
17. Click on the **Advanced** tab to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
18. Click **Save DNS Security Policy** to configure DNS Security policy. The **Configuration > Security** screen is then displayed, and the DNS Policy list table includes the newly created DNS Security Policy.

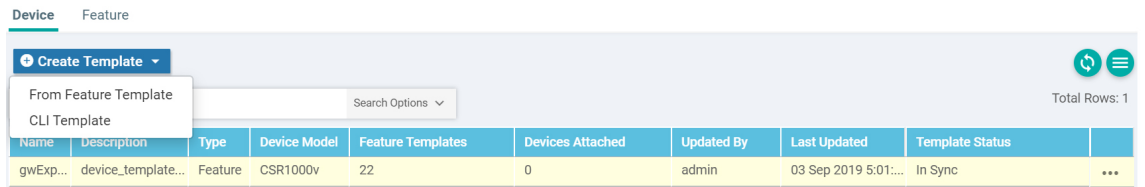


368834

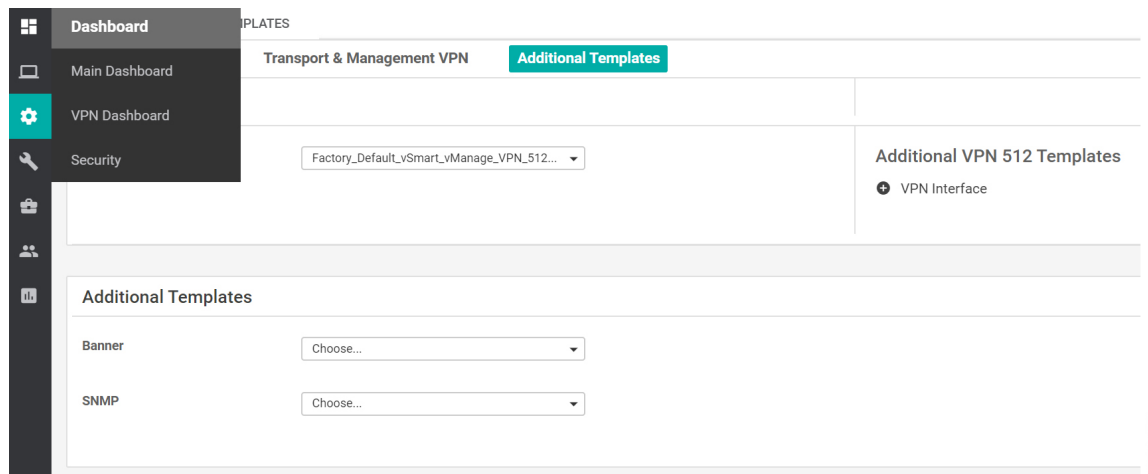
## Apply DNS Umbrella Policy to an IOS XE Router

To apply DNS Umbrella Policy:

1. In vManage NMS, select the **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, select one of the IOS XE devices.
4. Click the **Additional Templates** tab. The screen scrolls to the **Additional Templates** section.



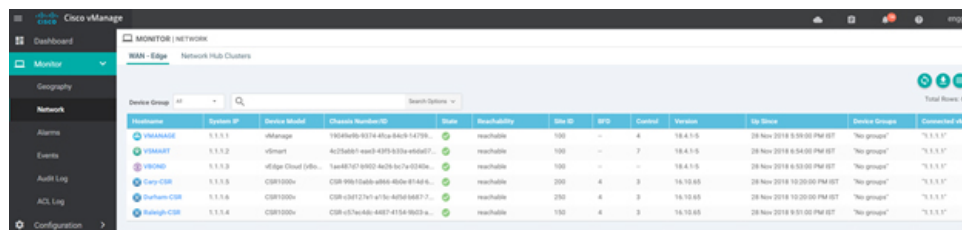
5. From the Security Policy drop-down, select the name of the Umbrella DNS Security Policy you configured in the above procedure.
6. Click **Create** to apply Umbrella policy to a device.

## Monitoring Umbrella Feature

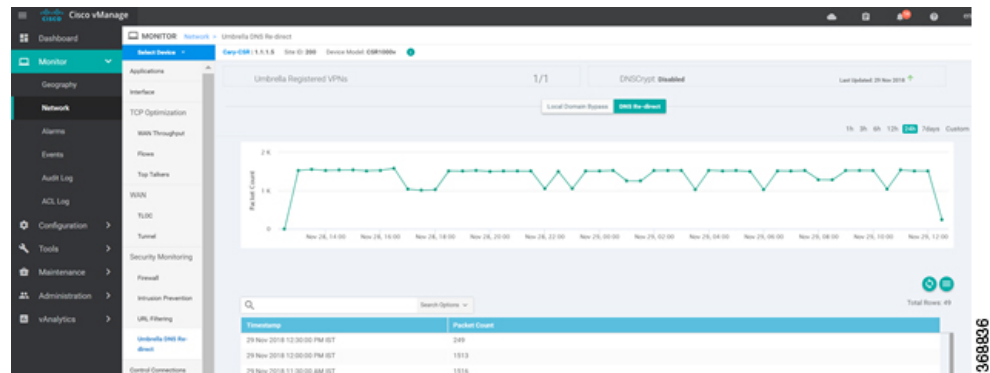
You can monitor the registered VPNs, DNSCrypt status, packet counts for required timestamps on a umbrella configured router using the following steps.

To monitor the status of Umbrella DNS Configuration on IOS XE device:

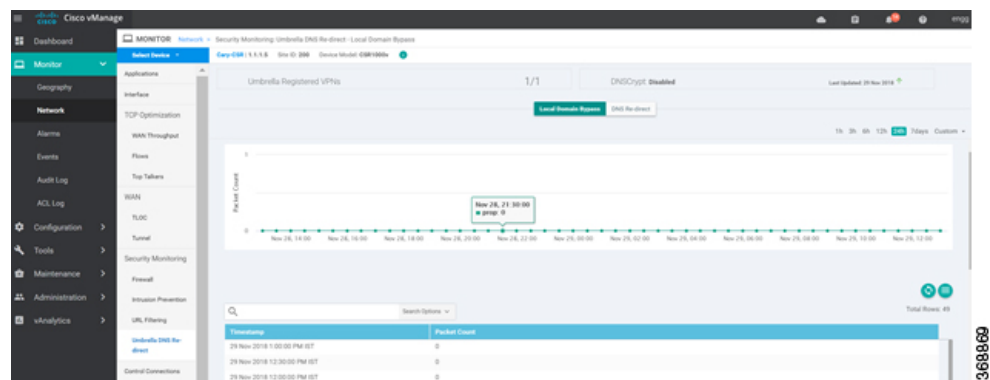
1. From the **Monitor > Network** screen, select an IOS XE device.



2. In the left panel, under Security Monitoring, select **Umbrella DNS Re-direct** tab. The Umbrella DNS Re-direct wizard displays showing how many packets are redirected to configured DNS server.



- Click on **Local Domain Bypass** to monitor the packet counts showing how many packets are bypassed to DNS server.



## 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 has 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-transaction
Device(config)# parameter-map type umbrella global
Device(config-profile)#?
```

```

parameter-map commands:
  dnscrypt      Enable DNSCrypt
  exit          Exit from parameter-map
  local-domain  Local domain processing
  no           Negative or set default values of a command
  public-key   DNSCrypt provider public key
  registration-vrf Cloud facing vrf
  resolver     Anycast address
  token        Config umbrella token
  udp-timeout  Config timeout value for UDP sessions
  vrf          Configure VRF

```

```

Per-VRF options are provided under VRF option:
Device(config)# parameter-map type umbrella global
Device(config-profile)#vrf 9
Device(config-profile-vrf)#?

```

```

vrf options:
  dns-resolver  DNS resolver address
  exit          Exit from vrf sub mode
  match-local-domain Match local-domain list(if configured)
  no           Negate a command or set its defaults

```

```

parameter-map type regex dns_bypass
pattern www.cisco.com
pattern .*amazon.com
pattern *.salesforce.com
!
parameter-map type umbrella global
token 648BF6139C379DCCFFBA637FD1E22755001CE241
local-domain dns_bypass
dnscrypt udp-timeout 5
vrf 9
    dns-resolver 8.8.8.8
    match-local-domain
vrf 19
    dns-resolver 8.8.8.8
    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:

VRF	dns-resolver	Match-local-domain (dns_bypass)
9	8.8.8.8	Yes
19	8.8.8.8	No
29	umbrella	Yes
39	umbrella	No



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

**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 .*amazon.com
Device(config)# pattern .*salesforce.com
```

**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

**B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79**

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
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successful 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)
Server Public Key     : 240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836

Client Secret Key Hash: 8A97:BBD0:A8BE:0263:F07B:72CB:BB21:330B:D47C:7373:B8C8:5F96:9F07:FEC6:BBFE:95D0

Client Public key      : 0622:C8B4:4C46:2F95:D917:85D4:CB91:5BCE:78C0:F623:AFE5:38BC:EF08:8B6C:BB40:E844

NM key Hash           : 88FC:7825:5B58:B767:32B5:B36F:A454:775C:711E:B58D:EE6C:1E5A:3BCA:F371:4285:5E3A

```

When disabled:

```

Device# show umbrella dnscrypt
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:
  dnscrypt
  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-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)# 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: AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
OrganizationID: 1882034
Local Domain Regex parameter-map name: NONE
DNSEncrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
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: 648BF6139C379DCCFFBA637FD1E22755001CE241
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_bypass
DNSEncrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

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 DNSEncrypt is disabled:
Device# show umbrella config
Umbrella Configuration

```



```

=====
Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_bypass
DNSEncrypt: 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
vpn29    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

```

### Configure Cisco Umbrella Using a CLI Device Template

For more information on using the CLI device template, see [Device Configuration-Based CLI Templates for Cisco IOS XE SD-WAN Devices](#).

This section provides example CLI configurations for Cisco Umbrella.

```

secure-internet-gateway
umbrella org-id <umbrella org id>
umbrella api-key <api key>
umbrella api-secret "<secret key>"

```

```

sdwan
interface Tunnel100001
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc
 source-interface GigabitEthernet0/0/0
 exit
 interface Tunnel100002
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference secondary-dc
 source-interface GigabitEthernet0/0/0
 exit

service sig vrf global
 ha-pairs
 interface-pair Tunnel100001 active-interface-weight 1 Tunnel100002 backup-interface-weight1

vrf definition <vrf#>
 address-family ipv4
 exit-address-family

interface Loopback<some value>
 no shutdown
 vrf forwarding <vrf#>
 ip address <IP Address> <mask>
 exit

interface Tunnel100001
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip clear-dont-fragment
 ip tcp adjust-mss 1300
 ip mtu 1400
 tunnel source GigabitEthernet<#/#/#>
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet<###> mandatory
 exit
interface Tunnel100002
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip clear-dont-fragment
 ip tcp adjust-mss 1300
 ip mtu 1400
 tunnel source GigabitEthernet<#/#/#>
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec2-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet<###> mandatory
 exit

crypto ikev2 policy policy1-global
 proposal p1-global

crypto ikev2 profile if-ipsec1-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 86400

crypto ikev2 profile if-ipsec2-ikev2-profile
 no config-exchange request

```

```

dpd 10 3 on-demand
dynamic
lifetime 86400

crypto ikev2 proposal p1-global
encryption aes-cbc-128 aes-cbc-256
group 14 15 16
integrity sha1 sha256 sha384 sha512

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256

crypto ipsec transform-set if-ipsec2-ikev2-transform esp-gcm 256

crypto ipsec profile if-ipsec1-ipsec-profile
set ikev2-profile if-ipsec1-ikev2-profile
set transform-set if-ipsec1-ikev2-transform
set security-association lifetime kilobytes disable
set security-association lifetime seconds 3600
set security-association replay window-size 512

crypto ipsec profile if-ipsec2-ipsec-profile
set ikev2-profile if-ipsec2-ikev2-profile
set transform-set if-ipsec2-ikev2-transform
set security-association lifetime kilobytes disable
set security-association lifetime seconds 3600
set security-association replay window-size 512

```

## 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
Dnscrypt: Enabled
Timeout:
-----
udp timeout: 5
OrgId :
-----
orgid : 1892929
Resolver config:
RESOLVER IP's
-----
208.67.220.220
208.67.222.222
2620:119:35::35
2620:119:53::53
Dnscrypt Info:
public_key:
A5:BA:18:C5:59:70:67:94:E5:37:38:33:06:F9:63:83:39:86:82:E4:00:F5:D8:BE:C1:AA:77:4A:4C:BA:64:00
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461

```

ProfileID	DeviceID	Mode	Resolver	Local-Domain	Tag
0		OUT		False	
4		IN	8.8.8.8	True	vpn9
1		IN	8.8.8.8	False	vpn19
2	010a9b2b0d5cb21f	IN	208.67.220.220	True	vpn29

```
3      010a1a2e1989da19  IN      208.67.220.220  False      vpn39
```

```
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.

```
+++ 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:
D9:2D:20:93:E8:8C:B4:BD:32:E6:A3:D1:E0:5B:7E:1A:49:C5:7F:96:BD:28:79:06:A2:DD:2E:A7:A1:F9:3D:7E
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 dnscrypt: 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 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
DNSEncrypt 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
ipv6_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 index: 0
-key[0]-
sn: 1517943461
ref cnt: 0
magic: 714e7a696d657555
Client Public Key:
A5BA:18C5:5970:6794:E537:3833:06F9:6383:3986:82E4:00F5:D8BE:C1AA:774A:4CBA:6400
NM Key Hash      :
16E6:DDC7:53BE:2929:1CDA:06AE:0BE2:C270:6E39:EAE7:F925:78FD:3599:2AB6:74C9:A59D
-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 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 171.168.1.7"
debug.opendns.com text = "flags 436 0 6040 39FF0000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 72.163.220.18:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"

```

## DNS Security Policy Configuration

### Domain List

Name	Entries	Reference Count	Updated By	Last Updated	Action
domain	cisco.com	1	admin	24 Apr 2019 8:03:54 PM PDT	

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



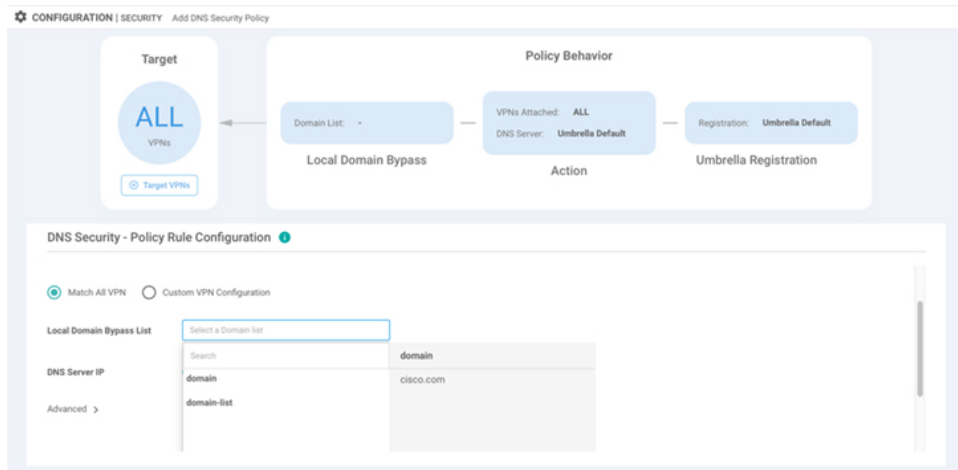
## Umbrella Registration

CLI Command	Possible Completions	Description and possible input values
<b>security umbrella</b>		Configure Umbrella service related security properties.
	<b>api-key</b>	Config umbrella api-key. The value ranges from 1 to 64 characters.
	<b>dnscrypt</b>	Enable DNSCrypt while redirecting DNS requests to Umbrella.
	<b>orgid</b>	Config umbrella org id
	<b>secret</b>	Config umbrella secret. The value can be [0   6].
	<b>token</b>	Umbrella service registration token. The value ranges from 1 to 64 characters.

CLI Command	Possible Completions	Description and possible input values
<b>vpn &lt;number, range&gt;</b>	<b>dns-redirect match-local-domain-to-bypass</b>	List of domain name regular expression patterns

	<b>dns-redirect umbrella</b>	Bypass the dns redirect for entries in the local domain list  Use Umbrella as DNS redirect service.
--	------------------------------	---

### DNS-Security Policy with Domain List



```

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

```



## CHAPTER 9

# Security Virtual Image

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.

- [Install and Configure IPS/IDS, URL-F, or AMP Security Policies, on page 123](#)
- [Identify the Recommended Security Virtual Image Version, on page 125](#)
- [Upload the Cisco Security Virtual Image to vManage, on page 126](#)
- [Upgrade a Security Virtual Image, on page 127](#)

## Install and Configure IPS/IDS, URL-F, or AMP Security Policies

Installing and configuring IPS/IDS, URL-F, or AMP security policies require the following workflow:

Task 1: Create a Security Policy Template for IPS/IDS, URL-F, or AMP Filtering

Task 2: Create a Feature Template for Security App Hosting

Task 3: Create a Device Template

Task 4: Attach Devices to the Device Template

### Create a Security Policy Template

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** window, select your security scenario from the list of options.
4. Click **Proceed**.

### Create a Feature Template for Security App Hosting

The feature profile template configures two functions:

- **NAT:** Enables or disables Network Address Translation (NAT), which protects internal IP addresses when outside the firewall.

- **Resource Profile:** Allocates default or high resources to different subnets or devices.




---

**Note** A feature profile template, while not strictly required, is recommended.

---

To create a feature profile template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature Templates** and then click **Add Template**.




---

**Note** In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

---

3. From the **Select Devices** list, choose the devices that you want to associate with the template.
4. Under **Basic Information**, click **Security App Hosting**.
5. Enter **Template Name** and **Description**.
6. Under **Security Policy Parameters**, customize the security policy parameters if required.
  - Enable or disable the Network Address Translation (NAT) feature, based on your use case. By default, **NAT** is on.
  - Click the drop-down arrow to set boundaries for the policy. The default is **Default**.
    - Global:** Enables NAT for all devices attached to the template.
    - Device Specific:** Enables NAT only for specified devices. If you select **Device Specific**, enter the name of a device key.
    - Default:** Enables the default NAT policy for devices attached to the template.
  - Set **Resource Profile**. This option sets the number of snort instances to be used on a router. The default is **Low** that indicates one snort instance. **Medium** indicates two instances and **High** indicates three instances.
  - Click the drop-down arrow to set boundaries for the resource profile. The default is **Global**.
    - Global:** Enables the selected resource profile for all devices attached to the template.
    - Device Specific:** Enables the profile only for specified devices. If you select **Device Specific**, enter the name of a device key.
    - Default:** Enables the default resource profile for devices attached to the template.
7. Set **Download URL Database on Device** to **Yes** if you want to download the URL-F database on the device. In this case, the device looks up in the local database before trying the cloud lookup.
8. Click **Save**.

### Create a Device Template

To activate the policies you want to apply, you can create a device template that will push the policies to the devices that need them. The available options vary with the device type. For example, Cisco vManage devices

require a more limited subset of the larger device template. You will see only valid options for that device model.

To create a security device template, follow this example for vEdge 2000 model routers:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device Templates**, and then choose **Create Template > From Feature Template**.



---

**Note** In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

---

3. From the **Device Model** drop-down list, choose the device model.
4. From the **Device Role** drop-down list, choose the device role.
5. Enter **Template Name** and **Description**.
6. Scroll down the page to the configuration submenus that let you select an existing template, create a new template, or view the existing template. For example, to create a new System template, click **Create Template**.

#### Attach Devices to the Device Template

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device Templates**, and then choose **Create Template > From Feature Template**.



---

**Note** In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

---

3. In the row of the desired device template, click **...** and choose **Attach Devices**.
4. In the **Attach Devices** window, select the desired devices from the **Available Devices** list, and click the right-pointing arrow to move them to the **Selected Devices** list.
5. Click **Attach**.

## 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:

- 
- Step 1** From the vManage dashboard, select **Monitor > Network**.
  - Step 2** Choose **WAN – Edge**.
  - Step 3** Select the device that will run the SVI.  
The System Status page displays.
  - Step 4** Scroll to the bottom of the device menu, and click **Real Time**.

The System Information page displays.

**Step 5** Click the **Device Options** field, and select **Security App Version Status** from the menu list.

The screenshot shows the vManage interface for a device named 'pm3001' with IP '172.16.248.31' and Site ID '30003001'. The 'Device Options' dropdown menu is open, listing various status options. 'Security App Version Status' is highlighted. The background shows a table of properties and values.

Property	Value
Device groups	[No groups]
Domain ID	1
Hostname	pm3001
Last Updated	27 Mar 2019 11:35:04 AM F
Latitude	37.666684
Longitude	-122.777023
Personality	WAN Edge
Site ID	30003001
Timezone	PDT -0700
Vbond	172.71.10.2

**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.

The screenshot shows the vManage interface for a device named 'pm5' with IP '172.16.255.25' and Site ID '500'. The 'Device Options' dropdown menu is open, showing 'UTD Version Status'. Below the dropdown is a table with one row of data. The 'Recommended Version' column is circled in red.

Last Updated	Recommended Version	Supported Regex	Installed Version
26 Nov 2018 5:00:28 AM PST	1.0.7_SV2.9.11.1_XE16.10	*1\.\0\.\([0-9]+\)_SV(\.*)_XE16\.\10\$	1.0.7_SV2.9.11.1_XE16.10

## 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.

Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN / IOS XE SD-WAN Software- 16.10.2

Search...

Expand All Collapse All

Suggested Release >

Latest Release >

16.10.2

All Release >

16 >

Deferred Release >

16 >

### ISR 4000 Series IOS XE SD-WAN

Release 16.10.2

Related Links and Documentation  
[Release Notes for 16.10.2](#)

▲ Notifications

File Information	Release Date	Size	
Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.10.2.SPA.bin	11-Mar-2019	431.27 MB	↓ 🛒 📄
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.10.2.SPA.bin	11-Mar-2019	422.03 MB	↓ 🛒 📄
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.10.2.SPA.bin	11-Mar-2019	560.50 MB	↓ 🛒 📄
UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar	11-Mar-2019	75.33 MB	↓ 🛒 📄

369288

**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.

MAINTENANCE | SOFTWARE REPOSITORY

Software Images **Virtual Images**

Upload Virtual Image

369320

**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.

MAINTENANCE | SOFTWARE UPGRADE

WAN Edge Controller vManage

5 Rows Selected Upgrade Upgrade Virtual Image Activate Delete Available Software Set Default Version

Device Group All Search Options

	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability	Current Version	Available Versions
<input checked="" type="checkbox"/>	pm3003	172.16.248.33	ISR4331/K9-FDO21390B4E	30003003	ISR4331	reachable	16.10.1	16.10.85
<input checked="" type="checkbox"/>	pm3004	172.16.248.34	ISR4331/K9-FDO21390B56	30003004	ISR4331	reachable	16.10.1	16.10.85
<input checked="" type="checkbox"/>	pm3011	172.16.248.241	ASR1001-HX-JAE21450ATR	30003011	ASR1001-HX	reachable	16.10.1	16.10.85
<input checked="" type="checkbox"/>	pm3012	172.16.248.242	ASR1002-HX-JAE220107CS	30003012	ASR1002-HX	reachable	16.10.1	16.10.85
<input checked="" type="checkbox"/>	pm3015...	172.16.248.245	ISR-8c71e7e4-efa5-44ac-9193-...	30003015	ISRv	reachable	16.10.1	16.10.85

369290

- 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.

Virtual Image Upgrade

vManage  Remote Server - vManage

Security Application

Edge Base Image Version	Device Count	Current Version	Upgrade to Version
16.10.1	1	1.0.8_SV2.9.11.1_XE16.10	Select Select 1.7.9_SV2.9.11.1_XE16.10 1.0.8_SV2.9.11.1_XE16.10 Upgrade Cancel

369292

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





# CHAPTER 10

## IPSec Pairwise Keys Overview

*Table 10: Feature History*

Feature Name	Release Information	Description
Secure Communication Using Pairwise IPsec Keys	Cisco IOS XE SD-WAN Release 16.12.1b	This feature allows private pairwise IPsec session keys to be created and installed for secure communication between IPsec devices and its peers.

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 129](#)
- [Pairwise Keys , on page 130](#)
- [IPsec Security Association Rekey, on page 130](#)
- [Configure IPsec Pairwise Keys, on page 130](#)

## 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 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

---

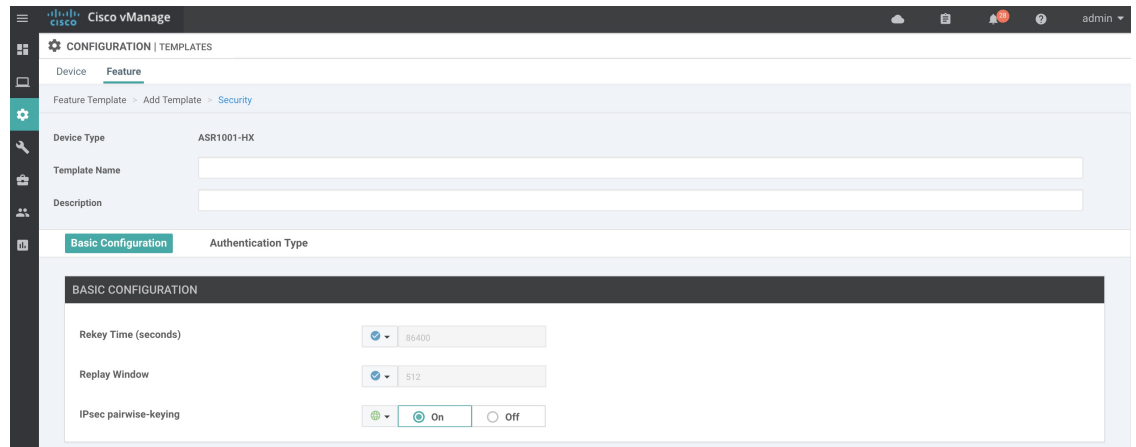
## Configure IPsec Pairwise Keys

### Configure IPsec Pairwise Keys Using vManage

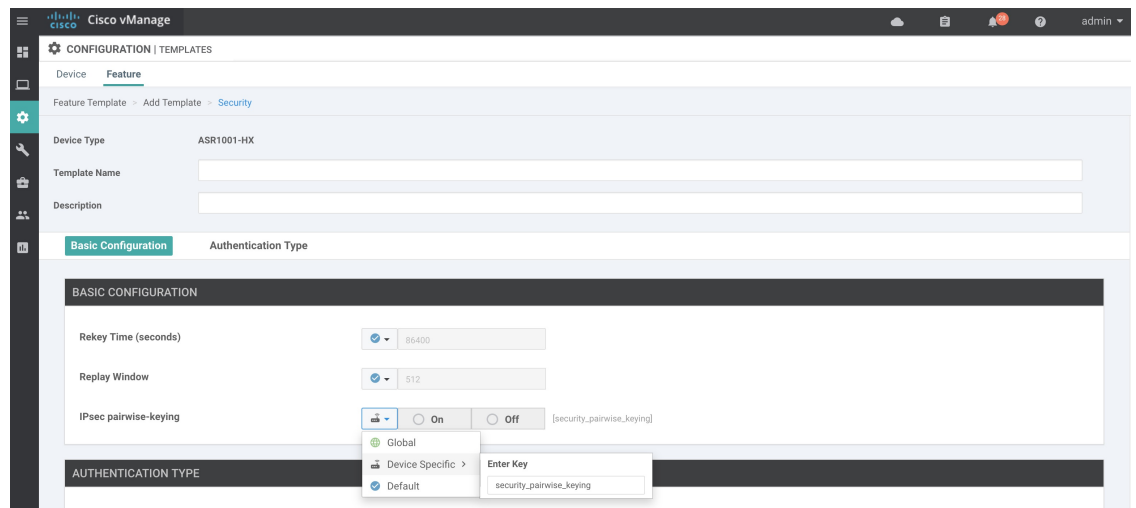
1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the **Feature** tab, click **Create Template**.
3. From the **Device Model** check box, select the type of device for which you are creating the template.
4. From the **Basic Information** tab, choose **Security** template.

- From the Basic Configuration tab, select On or Off from the IPsec Pairwise-Keying field..

**Figure 3: IPsec Pairwise Keying**



- Alternatively, enter the pairwise key specific to the device in the **EnterKey** field.



- 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
```



**Note** 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
```

SS	E-KEY	AH	REMOTE				SA	PKEY	NONCE	PKEY
SOURCE IP	Source Port	SOURCE IP	DEST	Port	LOCAL TLOC	ADDRESS	REMOTE TLOC	COLOR		
REMOTE TLOC	ADDRESS	REMOTE TLOC	COLOR	PWK-SPI	INDEX	ID	HASH	HASH	HASH	
HASH	AUTH									
10.168.11.3	12346	192.168.90.3	12346	10.1.0.2			lte			
10.1.0.1	privatel	000000	202	0	6668	17B0	F5A5			
true										
10.168.11.3	12346	192.168.92.6	12346	10.1.0.2			lte			
10.1.0.6	default	00A001	52	10	0ED6	AF12	0A09	8030		
true										
10.168.12.3	12346	192.168.90.3	12346	10.1.0.2			blue			
10.1.0.1	privatel	000000	205	0	6668	17B0	F5A5			
true										
10.168.12.3	12346	192.168.92.6	12346	10.1.0.2			blue			
10.1.0.6	default	00A001	55	10	0ED6	AF12	B9B7	BE29		
true										

Use the following command to verify inbound connection on IPSec Pairways Keys

```
Device# show sdwan ipsec pwk inbound-connections
```

DEST		LOCAL		LOCAL		SOURCE		REMOTE		REMOTE	
SA	PKEY	NONCE	PKEY	SS	D-KEY	AH	REMOTE	DEST IP			
PORT	TLOC	ADDRESS	TLOC	COLOR	PORT	TLOC	ADDRESS	TLOC	COLOR	PWK-SPI	
INDEX	ID	HASH	HASH	HASH	HASH	AUTH					
192.168.90.3	12346	5.1.0.2		lte		12346	10.168.11.3				
1	5605	70C7	17B0	F5A5	true	5.1.0.1	privatel			000000	2
192.168.92.6	12346	5.1.0.2		lte		12346	10.168.11.3				
1	5605	70C7	CCC2	C9E1	true	5.1.0.6	default			00100B	52
192.168.90.3	12346	5.1.0.2		blue		12346	10.168.12.3				
1	B9F9	5C75	17B0	F5A5	true	5.1.0.1	privatel			000000	5
192.168.92.6	12346	5.1.0.2		blue		12346	10.168.12.3				
1	B9F9	5C75	A0F8	7B6B	true	5.1.0.6	default			00100B	55

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

PKEY	NONCE	PKEY						SA
TLOC-ADDRESS	TLOC-COLOR	SOURCE-IP	SOURCE PORT	SPI	INDEX	ID		
5.1.0.2 70C7	lte	10.168.11.3	12346	257	6	1		5605
5.1.0.2 5C75	blue	10.168.12.3	12346	257	3	1		B9F9

```
Device# show platform hardware qfp active feature ipsec da spi
```

g_hash_idx	Flow id	QFP SA hdl	source IP dport SA ptr	sport dest IP crypto_hdl/old
1541	3	11	192.168.90.3 12346 0x312b84f0	12346 192.168.92.6
			0x0000000031fbfa80/0x0000000031fbd520	
6661	131	36	10.168.12.3 12346 0x312b9990	12346 192.168.92.6
			0x0000000031fbc9a0	
7429	117	6	10.168.11.3 12346 0x312b9300	12346 192.168.92.6
			0x0000000031fbd970/0x0000000031fbb580	

	System id	Wan int	Wan ip
Yubei-cedge	5102	Gi2.xxx	Sub 10.168.xxx
Yubei-tsn	5108	Gi0/0/1	192.168.92.8
Yubei-ovld	5106	Gi0/0/0	192.168.92.6
Yubei-lng	5107	Gi0/0/0	192.168.92.7
Yubei-utah	5104	Gi0/0/0	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]
```





## CHAPTER 11

# 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 135](#)
- [Configure SSO for Active Directory Federation Services \(ADFS\), on page 138](#)

## 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 11:*

Component	Value	Configuration
Response	Signed	
Assertion Signature	Signed	
Signature Algorithm	RSA-SHA256	
Digest Algorithm	SHA256	
Assertion Encryption	Encrypted	
Encryption Algorithm	AES256-CBC	
Key Transport Algorithm	RSA-OAEP	



Component	Value	Configuration
Encryption Certificate		<p><b>a.</b> Copy the encryption certificate from the metadata you downloaded.</p> <p><b>b.</b> Go to <a href="http://www.samltool.com">www.samltool.com</a> and click on <b>X.509 CERTS</b>, paste there. Click <b>Format X.509 Certificate</b>.</p> <p><b>c.</b> Make sure to remove the last empty line and then save the output (<b>X.509.cert with header</b>) into a text file <b>encryption.cer</b>.</p> <p><b>d.</b> 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.</p>
Enable Single Logout		Make sure this is checked.
Single Logout URL		Get from the metadata.
SP Issuer		Use the entityID from the metadata.
Signature Certificate		<p><b>a.</b> Obtain from the metadata. Format the signature certificate using <a href="http://www.samltool.com">www.samltool.com</a> as done above.</p> <p><b>b.</b> Save to a file, for example, <b>signing.cer</b> and upload.</p>
Authentication context class	X.509 Certificate	
Honor Force Authentication	Yes	
SAML issuer ID string	SAML issuer ID string	
Attribute Statements (optional)	Field: <b>Name</b>	Value: <i>Username</i>
	Field: <b>Name format (optional)</b>	Value: Unspecified
	Field: <b>Value</b>	Value: <i>user.login</i>
Group Attribute Statements (optional)	Field: <b>Name</b>	Value: Groups
	Field: <b>Name format (optional)</b>	Value: Unspecified
	Field: <b>Matches regex</b>	Value: .*




---

**Note** 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`.
5. Edit vManage Metadata file by deleting everything from **<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">** to **</ds:Signature>**.
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
5. Navigate to **`https://www.samltool.com/format_x509cert.php`**.
6. For **Signing certificate**, copy Signing certificate from “metadata” [everything between `<ds:X509Certificate>` and `</ds:X509Certificate>`].
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**.
2. Navigate to **Trust Relationships > Relying Party Trusts**.
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 ==
  "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-", ""));

```

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 `(?i)^SSO-` mentioned in **Step 19**.



---

**Note** Any active directory user who is NOT a member of these two groups, will only have **Basic** access to vManage.

---



## CHAPTER 12

# 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 12: Security Policy for UTD

CLI Template Configuration	Configuration on the Device
<pre> policy   zone internet     vpn 0   !   zone zone1     vpn 1   !   zone zone2     vpn 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     "&lt;![CDATA[&lt;h3&gt;Access" to the requested     page has been denied]]&gt;"       target-vpns    1     !   intrusion-prevention intrusion_policy     security-level  connectivity     inspection-mode protection     log-level      err     target-vpns    1     !   failure-mode      open   !   !   ! </pre>	



CLI Template Configuration	Configuration on the Device
	<pre> ip access-list extended fw_policy-seq-1-acl_      11 permit object-group fw_policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl     10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_     match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy     class fw_policy-seq-1-cm_         inspect ! class class-default     pass ! ! object-group service fw_policy-seq-1-service-og_     ip ! parameter-map type inspect-global     alert on     log dropped-packets     multi-tenancy     vpn zone security ! parameter-map type umbrella global     token A5EA676087BF66A42DC4F722C2AFD10D00256274     dnscrypt     vrf 1     dns-resolver                umbrella     match-local-domain-to-bypass ! ! zone security internet     vpn 0 ! zone security zone1     vpn 1 ! zone security zone2     vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet     service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2     service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0 </pre>

CLI Template Configuration	Configuration on the Device
	<pre> guest-interface 0   guest-ipaddress 192.168.1.2 netmask   255.255.255.252   !   app-vnic gateway1 virtualportgroup 1 guest-interface 1   guest-ipaddress 192.0.2.2 netmask   255.255.255.252   !   start   !   utd multi-tenancy   utd engine standard multi-tenancy   web-filter block page profile block-url_filter   text &lt;![CDATA[&amp;lt;h3&amp;gt;Access to the requested page has been denied&amp;lt;/h3&amp;gt;&amp;lt;p&amp;gt;Please contact your Network Administrator&amp;lt;/p&amp;gt;]]&gt;   !   web-filter url profile url_filter   categories block   games   !   block page-profile block-url_filter   log level error   reputation   block-threshold moderate-risk   !   ! threat-inspection profile intrusion_policy    threat protection   policy connectivity   logging level err   !   utd global   !   policy utd-policy-vrf-1   all-interfaces   vrf 1   threat-inspection profile intrusion_policy    web-filter url profile url_filter   exit   ! </pre>

### Security Monitoring Commands

- show control connections