



Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.x

First Published: 2019-11-22

Last Modified: 2020-04-20

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Read Me First	1
CHAPTER 2	What's New in Cisco IOS XE (SD-WAN)	3
CHAPTER 3	Security Overview	5
	Cisco SD-WAN Security Components	5
	Security for Connections to External Devices	6
	Control Plane Security Overview	6
	DTLS and TLS Infrastructure	7
	Control Plane Authentication	8
	Control Plane Encryption	10
	Control Plane Integrity	11
	Data Plane Security Overview	11
	Data Plane Authentication and Encryption	12
	Data Plane Integrity	14
	Carrying VPN Information in Data Packets	17
	Unified Threat Defense for Cisco SD-WAN	17
	Supported Platforms	18
	Restrictions	19
	Security Provided by NAT Devices	20
CHAPTER 4	Configure Security Parameters	21
	Configure Control Plane Security Parameters	21
	Configure DTLS in Cisco vManage	22
	Configure Data Plane Security Parameters	23
	Configure Allowed Authentication Types	23

Change the Rekeying Timer	25
Change the Size of the Anti-Replay Window	26
VPN Interface IPsec	27
Create VPN IPsec Interface Template	27
Changing the Scope for a Parameter Value	28
Configure IPsec Tunnel Parameters	28
Configure Dead-Peer Detection	29
Configure IKE	30

CHAPTER 5
Enterprise Firewall with Application Awareness 35

Overview of Enterprise Firewall with Application Awareness	35
Restrictions	37
Configure Firewall Policies	37
Start the Security Policy Configuration Wizard	38
Create Rules	39
Create Rule Sets	40
Apply Policy to a Zone Pair	42
Create Policy Summary	43
Apply a Security Policy to a Device	44
Monitor Enterprise Firewall	44
Zone-Based Firewall Configuration Examples	45
Configure Port-Scanning Detection Using a CLI Template	48
Firewall High-Speed Logging	49
Information About Firewall High-Speed Logging	49
Firewall High-Speed Logging Overview	49
NetFlow Field ID Descriptions	50
HSL Messages	54
How to Configure Firewall High-Speed Logging	60
Enabling Firewall High-Speed Logging Using vManage	60
Enabling High-Speed Logging for Global Parameter Maps	61
Enabling High-Speed Logging for Firewall Actions	62
Configuration Examples for Firewall High-Speed Logging	63
Example: Enabling High-Speed Logging for Global Parameter Maps	63
Example: Enabling High-Speed Logging for Firewall Actions	64

Unified Security Policy	64
Restrictions for Unified Security Policy	64
Information About Unified Security Policy	65
Benefits of Unified Security Policy	65
Use Cases for Unified Security Policy	65
Configure Unified Security Policy	65
Create an Object Group	66
Create an Advanced Inspection Profile	66
Configure Firewall Policy and Unified Security Policy	67
Add a Zone Pair	69
Configure Umbrella DNS Policy Using Cisco vManage	69
Apply a Security Policy to a Device	70
Configure Unified Security Policy Using the CLI	71
Migrate a Security Policy to a Unified Security Policy	72
Monitor Unified Security Policy	72
Monitor Unified Security Policy Using the CLI	72
Configuration Example for Unified Security Policy	74
Configuration Example of an Application Firewall in a Unified Security Policy	75

CHAPTER 6

Configure Geolocation-Based Firewall Rules for Network Access 77

Overview of Geolocation-Based Firewall Rules	77
Prerequisites for Geo Object Groups	78
Restrictions for Geo Object Groups	79
Configure Geolocation-Based Firewall Rules	79
Configure Geolocation-Based Firewall Rules Using the CLI	81
Update the Geolocation Database Using the CLI	82
Verify Geolocation-Based Firewall Rules Using the CLI	82

CHAPTER 7

Intrusion Prevention System 87

Overview of Intrusion Prevention System	87
Cisco SD-WAN IPS Solution	88
Configure and Apply IPS or IDS	88
Before you Begin	88
Configure Intrusion Prevention or Detection	88

Apply a Security Policy to a Device	90
Modify an Intrusion Prevention or Detection Policy	91
Delete an Intrusion Prevention or Detection Policy	91
Monitor Intrusion Prevention Policy	92
Update IPS Signatures	92
Configure Intrusion Prevention System for Unified Security Policy	92

CHAPTER 8

URL Filtering 95

Overview of URL Filtering	96
Database Overview	96
Filtering Options	97
Category-Based Filtering	97
Reputation-Based Filtering	97
List-based Filtering	97
Cloud-Lookup	97
Configure and Apply URL Filtering	98
Before you Begin	98
Configure URL Filtering	98
Apply a Security Policy to a Device	100
Modify URL Filtering	101
Delete URL Filtering	101
Monitor URL Filtering	102
Configure URL Filtering for Unified Security Policy	102

CHAPTER 9

Advanced Malware Protection 105

Overview of Advanced Malware Protection	105
Configure and Apply an Advanced Malware Policy	106
Before you Begin	106
Configure Threat Grid API Key	106
Configuring an Advanced Malware Protection Policy	107
Apply a Security Policy to a Device	108
Modify an Advanced Malware Protection Policy	108
Delete an Advanced Malware Protection Policy	109
Monitor Advanced Malware Protection	109

Troubleshoot Advanced Malware Protection	109
Rekey the Device Threat Grid API Key	110
Configure Advanced Malware Protection for Unified Security Policy	110

CHAPTER 10

SSL/TLS Proxy for Decryption of TLS Traffic 113

Information about SSL/TLS Proxy	113
Overview of SSL/TLS Proxy	113
Role of Certificate Authorities in TLS Proxy	115
Supported Devices and Device Requirements	118
Supported Cipher Suites	119
Prerequisites for TLS Proxy	120
Limitations and Restrictions	120
Configure Cisco IOS XE SD-WAN Devices as TLS Proxy	120
Configure CA for TLS Proxy	122
Configure Enterprise CA	122
Configure Cisco vManage as CA	123
Configure Cisco vManage as Intermediate CA	123
Configure SSL Decryption	124
Apply a Security Policy to an XE SD-WAN Router	128
Upload a Subordinate CA Certificate to TLS Proxy	129
Verify Configuration	130
Monitor TLS Proxy Performance	131
Monitor TLS Proxy	131
Monitor SSL Decryption Statistics	132
Revoke and Renew Certificates	132
Revoke Enterprise CA Certificate	132
vManage as CA or vManage as Intermediate CA	133
Configure TLS/SSL Decryption Policy for Unified Security Policy	134
Configure TLS/SSL Profile for Unified Security Policy	136

CHAPTER 11

Cisco Umbrella Integration 139

Overview of Cisco SD-WAN Umbrella Integration	139
Restrictions for Umbrella Integration	141
Prerequisites for Umbrella Integration	142

Configure Umbrella API Token	142
Configure Cisco Umbrella Registration	143
Define Domain Lists	143
Configure Umbrella DNS Policy Using Cisco vManage	144
Attach DNS Umbrella Policy to Device Template	145
Umbrella Integration Using CLI	145
Umbrella show commands at FP Layer	150
Umbrella show commands at CPP Layer	151
Umbrella Data-Plane show commands	153
Troubleshooting the Umbrella Integration	155
DNS Security Policy Configuration	155
Monitor Umbrella Feature	157

CHAPTER 12
Integrate Your Devices With Secure Internet Gateways 159

Options to Integrate Your Devices with Secure Internet Gateways	160
Automatic Tunnels	161
Manual Tunnels	162
Configure Tunnels	162
Configure Automatic Tunnels Using Cisco vManage	162
Prerequisites	162
Create SIG Feature Template	162
Create SIG Credentials Template	164
Redirect Traffic to a SIG	165
Modify Service VPN Template	165
Create the SIG Device Template	165
Attach the SIG Template to Devices	166
Configure Manual Tunnels Using Cisco vManage	167
Configuring Manual Tunnels to an SIG	167
Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage	169
Troubleshoot Integrating Your Devices With Secure Internet Gateways	170
After Upgrading Cisco vManage Tunnels Fail	171

CHAPTER 13
Security Virtual Image 173

Identify the Recommended Security Virtual Image Version	173
---	-----

Upload the Cisco Security Virtual Image to Cisco vManage 174

Upgrade a Security Virtual Image 174

CHAPTER 14

IPsec Pairwise Keys 177

Supported Platforms 177

Pairwise Keys 178

IPsec Security Association Rekey 178

Configure IPsec Pairwise Keys 178

Configure IPsec Pairwise Keys Using Cisco vManage 178

Configure Pairwise Keys and Enable Rekeying on the CLI 179

Verify IPsec Pairwise Keys on a Cisco IOS XE SD-WAN Device 179

CHAPTER 15

Configure Single Sign-On 183

Configure Single Sign-On Using Okta 183

Enable an Identity Provider in Cisco vManage 183

Configure SSO on the Okta Website 184

Assign Users to the Application on the Okta Website 186

Configure SSO for Active Directory Federation Services (ADFS) 187

Import Metadata File into ADFS 187

Add ADFS Relying Party Trust 188

Add ADFS Relying Party Trust Manually 189

Configure SSO for PingID 190

Configure SSO on the PingID Administration Portal 191

Configure SSO for IDPs in Cisco vManage Cluster 193

CHAPTER 16

Cisco TrustSec Integration 195

Support for SGT Propagation with Cisco TrustSec Integration 195

SGT Propagation Using Inline Tagging 196

SGT Propagation in Cisco SD-WAN 196

Supported Platforms and NIMs 198

Limitations for SGT Propagation 199

Configure SGT Inline Tagging Using Cisco vManage 199

Configure SGT Inline Tagging Using CLI 201

View SGT Propagation Configuration 203

SGT Propagation Using SXP	203
Supported Platforms and NIMs	204
Propagate SGT Using SXP	205
SXP Reflectors	205
Configure SXP for Dynamic IP-SGT Binding Using Cisco vManage	206
Configure SXP for Dynamic IP-SGT Binding on the CLI	208
Configure Static IP-SGT Binding Using Cisco vManage	208
Configure TCP-AO Support for SXP	209
Configure TCP-AO Support for SXP on the CLI	211
Configure SXP Reflector using the CLI	211
SGACL for Cisco TrustSec	211
Download SGACL Policies to Cisco vEdge Devices	211
Download SGACL Policies using CLI	213
Configure Static SGACL Policies in Cisco vManage	213
SGT Enforcement	214
Configure SGT Enforcement at the Interface Level in Cisco vManage	214
Configuring SGT Enforcement at the Interface Level Using CLI	215
Monitor SXP Connections and SGT Enforcement	215

CHAPTER 17
Unified Threat Defense Resource Profiles 217

Supported Platforms	218
Configure Unified Threat Defense Resource Profiles	218
Configure the Unified Threat Defense Resource Profiles Using Cisco vManage	218
Verify Unified Threat Defense Resource Profiles	219

CHAPTER 18
Security CLI Reference 221



CHAPTER 1

Read Me First

Related References

- [Release Notes](#)
- [Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations](#)

User Documentation

- [Cisco IOS XE \(Cisco IOS XE SD-WAN Devices\)](#)
- [Cisco IOS XE \(SD-WAN\) Qualified Command Reference](#)
- [Cisco SD-WAN Command Reference](#)

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: [Cisco Profile Manager](#).
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit [Cisco Services](#).
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit [Cisco Devnet](#).
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, visit [Cisco Warranty Finder](#).
- To view open and resolved bugs for a release, access the [Cisco Bug Search Tool](#).
- To submit a service request, visit [Cisco Support](#).

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

What's New in Cisco IOS XE (SD-WAN)



Note

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

[What's New in Cisco IOS XE \(SD-WAN\) Release 17.x](#)



CHAPTER 3

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:

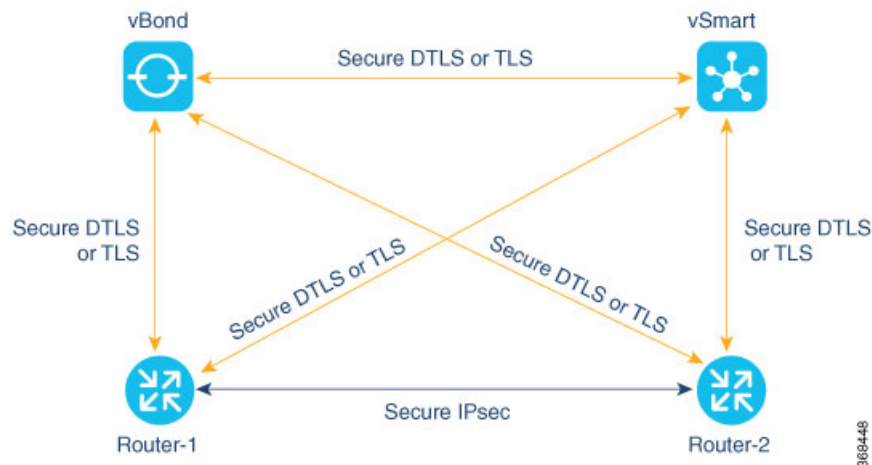
- [Cisco SD-WAN Security Components, on page 5](#)
- [Security for Connections to External Devices, on page 6](#)
- [Control Plane Security Overview, on page 6](#)
- [Data Plane Security Overview, on page 11](#)
- [Unified Threat Defense for Cisco SD-WAN, on page 17](#)
- [Security Provided by NAT Devices, on page 20](#)

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 for Connections to External Devices

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

Control Plane Security Overview

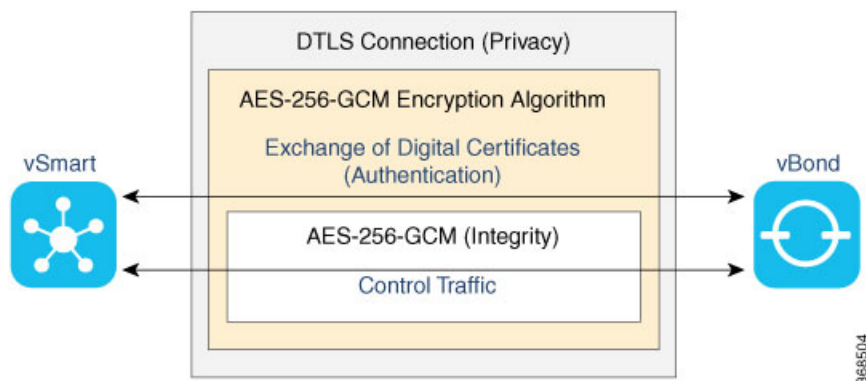
The control plane of any network determines the network topology and defines how to direct packets. In a traditional network, the control plane operations of building and maintaining routing and forwarding tables and directing packets towards their destination are handled by routing and switching protocols, which typically offer few or no mechanisms for authenticating devices or for encrypting routing updates and other control information. In addition, the traditional methods of providing security are manual and do not scale. For example, certificates are typically installed manually rather than in an automated fashion, and using preshared keys is not a 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 Secure Sockets Layer (SSL)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The Cisco 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 Cisco vBond Orchestrator, to Cisco vManage, and to other Cisco 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 the control traffic sent over the connections.

The privacy and encryption in the control plane, which is offered by DTLS and TLS, provide a safe and secure foundation for the other two security components, that is, 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, an authenticated encryption with associated data (AEAD) that provides encryption and integrity, which ensures that all the control and data traffic sent over the connections has not been tampered with.

Figure 1: Cisco SD-WAN Control Plane Overview



The following are the control plane security components, which function in the privacy provided by DTLS or TLS connections:

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

DTLS and TLS Infrastructure

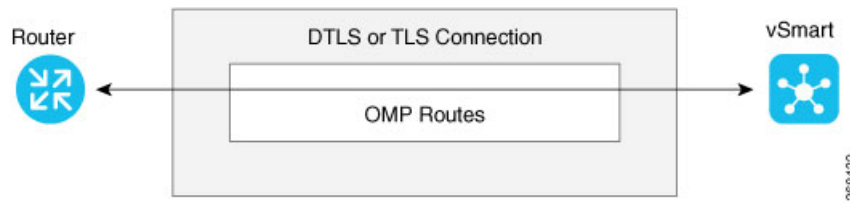
Security protocols derived from SSL provide the foundation for the Cisco SD-WAN control plane infrastructure.

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

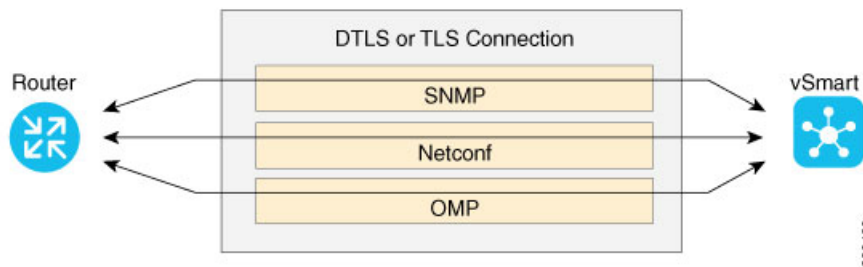
The control plane infrastructure can also be configured to run over TLS. This might be desirable in situations where the protections of TCP outweigh its issues. For example, firewalls generally offer better protection for TCP servers than for UDP servers.

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

software implements the standard version defined in RFC 5246. As described in the RFCs, Cisco SD-WAN uses DTLS and TLS versions 1.2.



In the Cisco SD-WAN architecture, the Cisco SD-WAN devices use DTLS or TLS as a tunneling protocol, which is an application-level (Layer 4) tunneling protocol. When the vSmart controllers, vBond orchestrators, Cisco vManages, and routers join the network, they create provisional DTLS or TLS tunnels between them as part of the device authentication process. After the authentication process completes successfully, the provisional tunnels between the routers and vSmart controllers, and those between the vBond orchestrators and vSmart controllers, become permanent and remain up as long as the devices are active in the network. It is these authenticated, secure DTLS or TLS tunnels that are used by all the protocol applications running on the Cisco SD-WAN devices to transport their traffic. For example, an OMP session on a router communicates with an OMP session on a vSmart controller by sending plain IP traffic through the secure DTLS or TLS tunnel between the two devices. The Overlay Management Protocol is the Cisco SD-WAN control protocol used to exchange routing, policy, and management information among Cisco SD-WAN devices, as described in Overlay Routing Overview.



A Cisco SD-WAN daemon running on each vSmart controller and router creates and maintains the secure DTLS or TLS connections between the devices. This daemon is called `vdaemon` and is discussed later in this article. After the control plane DTLS or TLS connections are established between these devices, multiple protocols can create sessions to run and route their traffic over these connections—including OMP, Simple Network Management Protocol (SNMP), and Network Configuration Protocol (Netconf)—without needing to be concerned with any security-related issues. The session-related traffic is simply directed over the secure connection between the routers and vSmart controllers.

Control Plane Authentication

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

- **Public keys**— These keys are generally known.
- **Private keys**— These keys are private. They reside on each Cisco SD-WAN router and cannot be retrieved from the router.

- **Certificates** signed by a root certification authority (CA)— The trust chain associated with the root CA needs to be present on all Cisco SD-WAN 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.

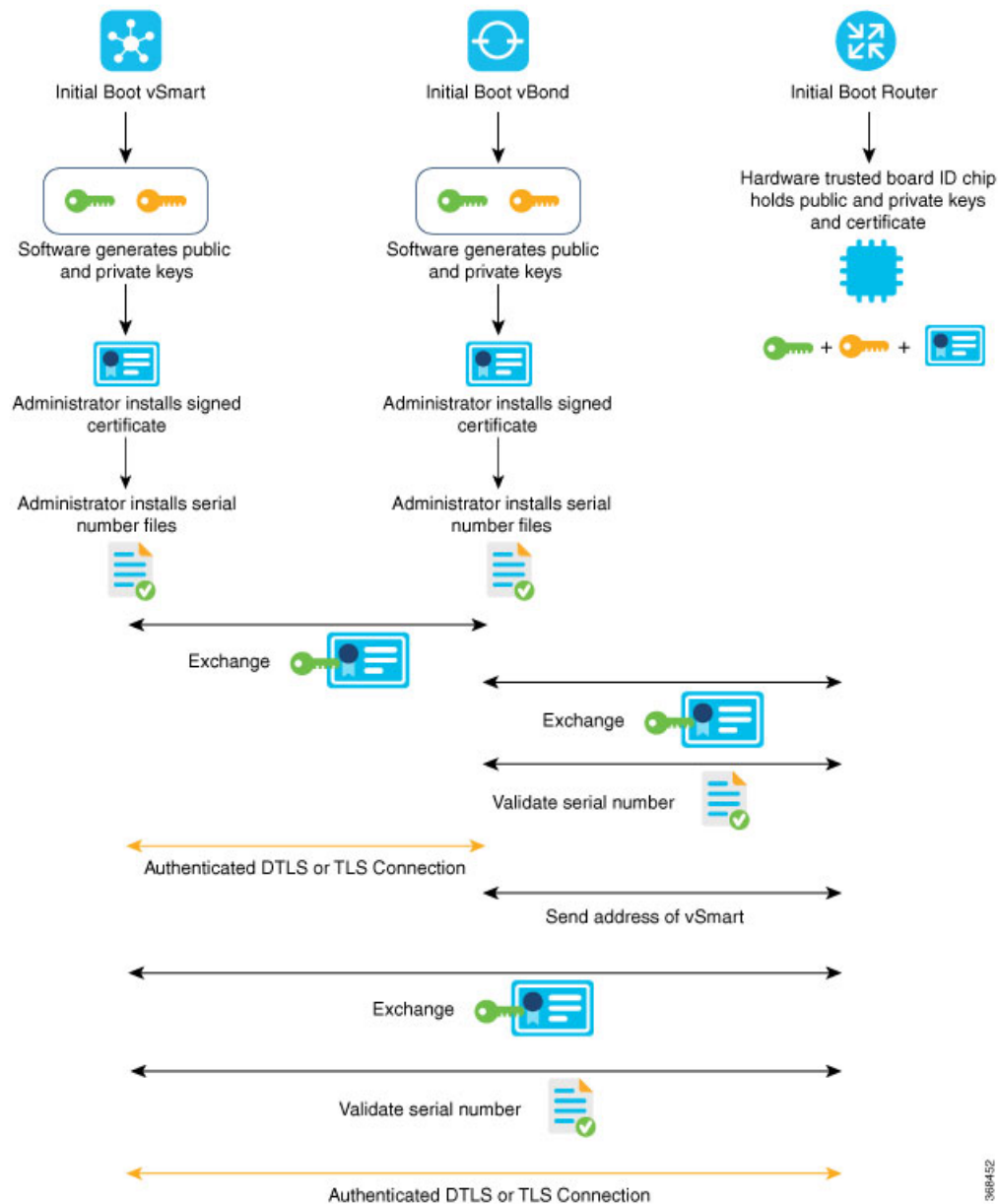
Let's first look at the PKI components that are involved in router authentication. On the Cisco XE SD-WAN router, the public and private keys and the certificates are managed automatically, by a hardware security chip that is built into the router called the Trust Anchor module (TAM). The TAM is a proprietary,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

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

When you place an order with Cisco using your Smart and Virtual Account, Cisco updates the Cisco Plug and Play (PNP) Portal with the chassis and certificate serial numbers of the devices that you purchased. You can then use Cisco vManage to sync the device information from the PNP portal using your Smart Account credentials. Alternatively, you can also download the trusted WAN Edge serial file from the PNP portal and upload it manually to Cisco vManage. Cisco vManage then broadcasts this information to the other controllers. Both the authorized serial number file and the file listing the vSmart serial numbers are uploaded and installed on vBond orchestrators. Then, during the automatic authentication process, as pairs of devices (routers and controllers) are establishing DTLS control connections, each device compares the serial numbers (and for routers, the chassis numbers) to those in the files installed on the router. A router allows a connection to be established only if the serial number or serial–chassis number combination (for a router) matches. Note that routers only make control connections to the controllers and not to other routers.

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.

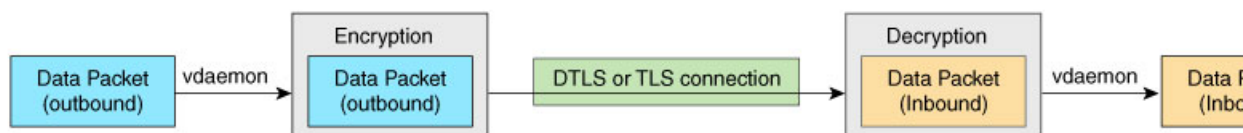


Control Plane Encryption

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: AES-GCM message digests, and public and private keys.

AES-GCM authenticated encryption provides high performance encryption that generates message digests (sometimes called simply digests) for each packet sent over a control plane connection. The receiver then generates a digest for the packet, and if the two match, the packet is accepted as valid. This encryption allows 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.

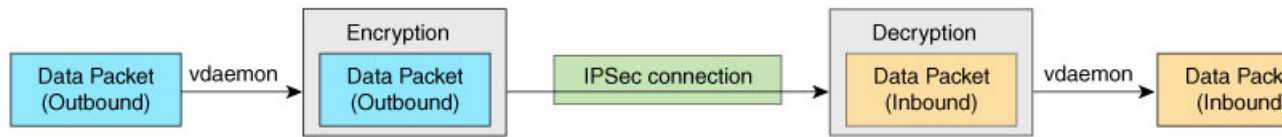
Data Plane Security Overview

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 can sniff the traffic, and 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 the devices are validated, and control traffic is encrypted and cannot be tampered with—you can be confident about 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, as shown in the figure, and described below.

Figure 2: Cisco SD-WAN Data Plane Overview



- **Authentication:** As mentioned, 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 Cisco vSmart Controller sends IPsec encryption keys to each edge device.

In the pairwise keys model, the Cisco vSmart Controller sends Diffie-Hellman public values to the edge devices, and they generate pairwise IPsec encryption keys using Elliptic-curve Diffie-Hellman (ECDH) and a P-384 curve. For more information, see [Pairwise Keys, on page 178](#).
 - 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 a 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, which is 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 antireplay 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 additional 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.

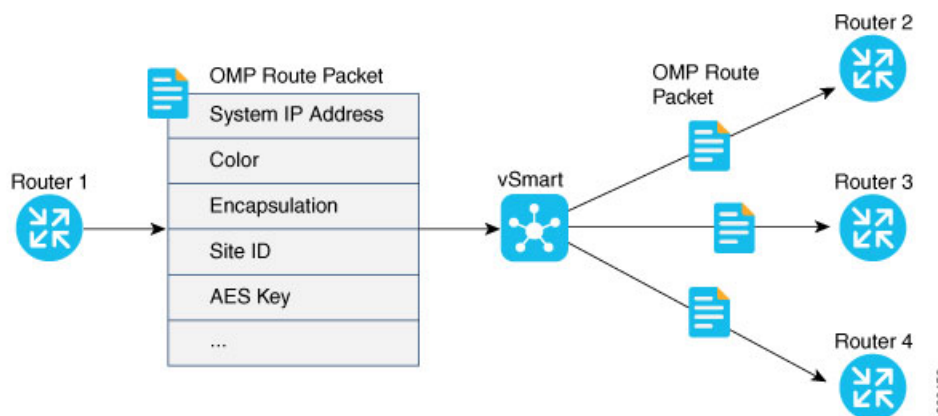
The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- 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](#), on page 177



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:

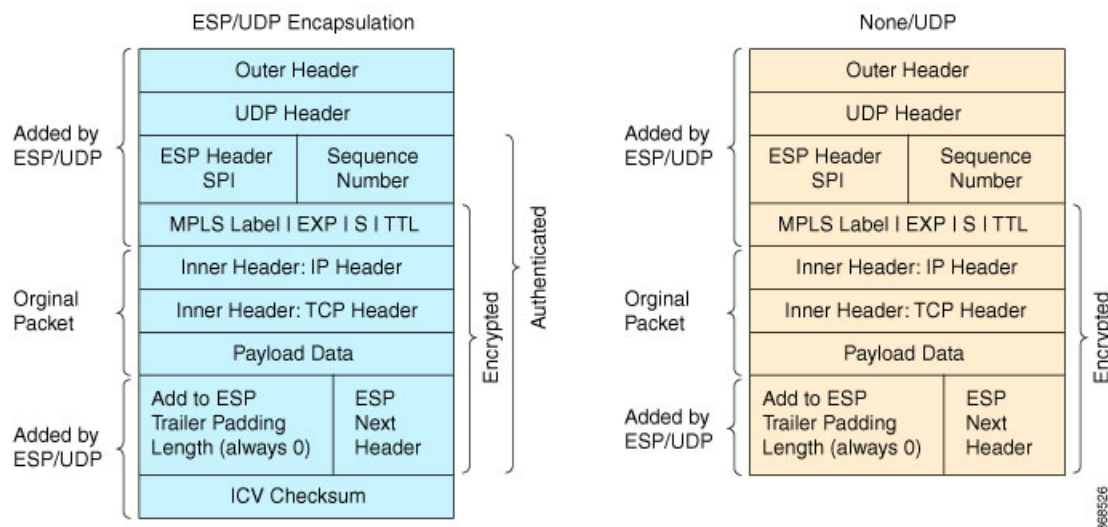
- ESP, which is a standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets. The modifications to ESP also protect the outer IP and UDP headers
- Modifications to ESP, which protect (via authentication) 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 hash calculation on the data packet's payload and inner header fields using AES-GCM and places the resultant hash (also called a digest) into a 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 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.

In the Cisco SD-WAN solution, there are also modifications to ESP to enhance its behavior to cover more of the datagram. The modifications are similar to the way that AH works. 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 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

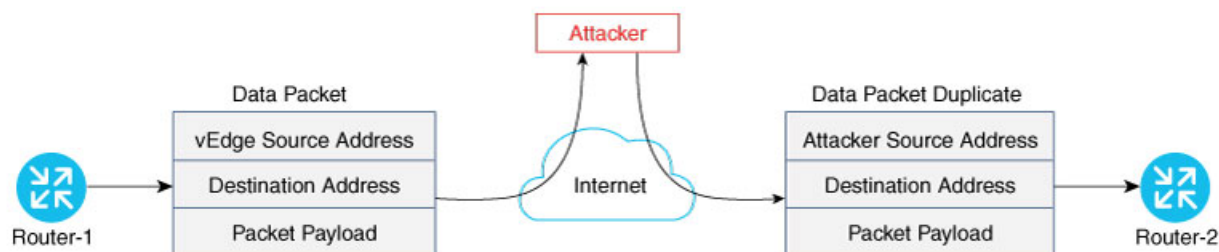
present), the original packet, and the ESP trailer—and places its calculated hash into the ICV checksum field at the end of the packet.

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.



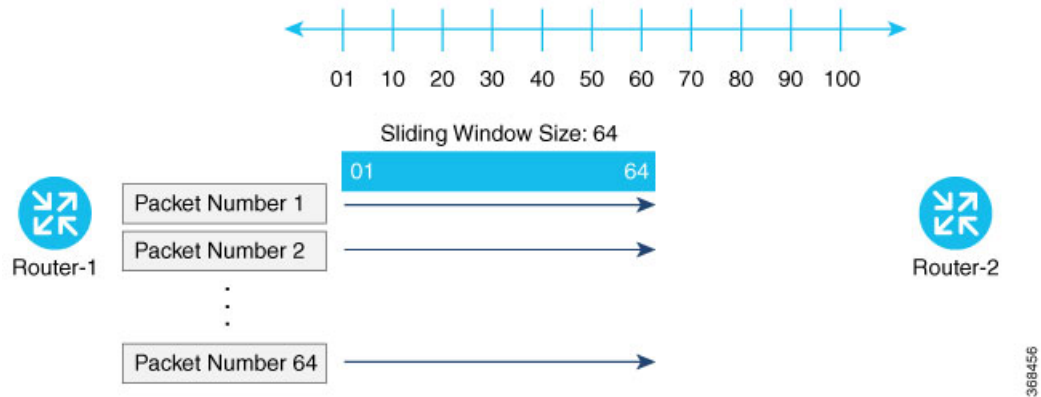
Note that Cisco SD-WAN devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the digest. Both are distributed as part of the TLOC properties for a router.

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.

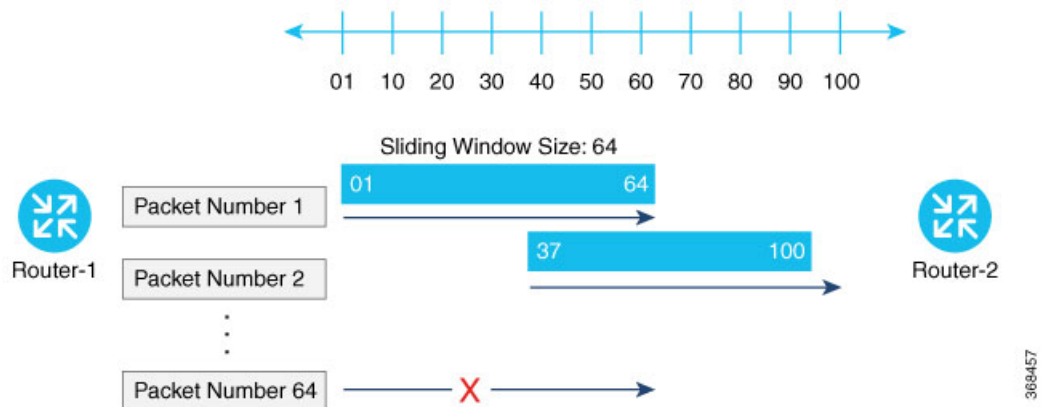


As a counter to such attacks, the Cisco SD-WAN overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender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

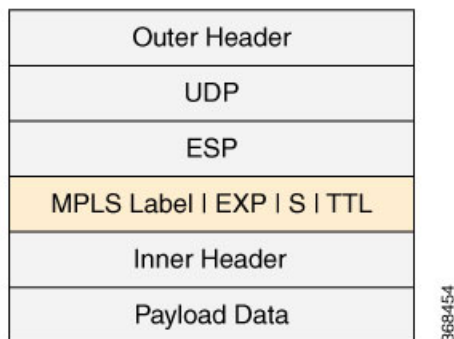
all others. A sliding window is used rather than accepting only packets whose sequence number is larger than the last known sequence number, because packets often do not arrive in order.



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.

Unified Threat Defense for Cisco SD-WAN

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

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

Cisco SD-WAN offers the following security features:

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

Feature	Description
Enterprise Firewall with Application Awareness, on page 35	A stateful firewall with NBAR2 application detection engine to provide application visibility and granular control, capable of detecting 1400+ applications.
Intrusion Prevention System, on page 87	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
URL Filtering, on page 95	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.
Advanced Malware Protection, on page 105	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.
Cisco Umbrella Integration, on page 139	Cloud-delivered enterprise network security which provides users with a first line of defense against cyber security threats.

Supported Platforms

For UTD 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 Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms

- Cisco Cloud Services Router 1000v series (CSR 1000v) on Amazon Web Services (AWS)
- Cisco Integrated Services Virtual Router
- Cisco Catalyst 8000V Edge Software

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 service 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.
- Cisco Catalyst 8200 Series Edge Platforms and Cisco Catalyst 8300 Series Edge Platforms must meet the following minimum requirements to support UTD:

- 8 GB DRAM
- 16 GB M.2 USB storage

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.



CHAPTER 4

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

vSmart-2# **control connections**

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

Configure DTLS in Cisco vManage

If you configure the Cisco 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 Cisco vManage. To display information about these processes and about the number of ports that are being forwarded, use the **show control summary** command shows that four vdaemon processes are running:

vManage# show control summary	VBOND	VMANAGE	VSMART	VEDGE
INSTANCE	COUNTS	COUNTS	COUNTS	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 Cisco 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 Cisco 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

Authentication Types in Cisco IOS XE Release 17.6.1a and Later

From Cisco IOS XE Release 17.6.1aCisco SD-WAN Release 20.6.1, the following integrity types are supported:

- **esp:** This option enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header.

- **ip-udp-esp:** This option enables ESP encryption. In addition to the integrity checks on the ESP header and the payload, the checks also include the outer IP and UDP headers.
- **ip-udp-esp-no-id:** This option is similar to ip-udp-esp, however, the ID field of the outer IP header is ignored. Configure this option in the list of integrity types to have the Cisco SD-WAN software ignore the ID field in the IP header so that the Cisco SD-WAN can work in conjunction with non-Cisco devices.
- **none:** This option turns integrity checking off on IPsec packets. We don't recommend using this option.

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

```
security ipsec integrity-type { none | ip-udp-esp | ip-udp-esp-no-id | esp }
```

Authentication Types Before Cisco IOS XE Release 17.6.1a

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 14](#).

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

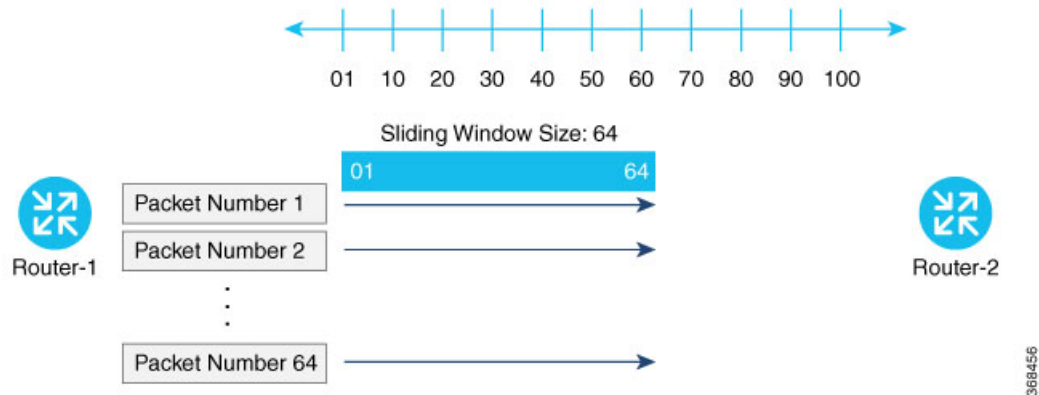
the SPI to 258. The router then uses the associated key of SPI 258. Note, however, that some packets will be dropped for a short period of time, until all the remote routers learn the new key.

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

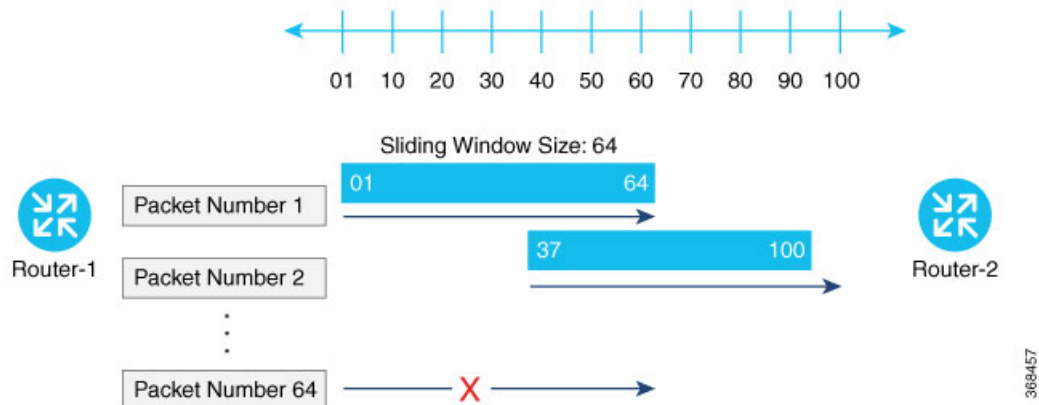
TLOC ADDRESS	TLOC COLOR	SPI	SOURCE IP	SOURCE PORT	KEY HASH
172.16.255.15	lte	258	10.1.15.15	12346	*****b93a

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, choose Configuration > Templates . |
| Step 2 | Click Feature . |
| Step 3 | Click Add Template . |
| Step 4 | Choose 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 Template Name , enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters. |
| Step 7 | In Template Description , 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 choose 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, click IPSEC and configure the following parameters:

Parameter Name	Options	Description
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
IKE Replay Window	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
IPsec Cipher Suite	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	2 1024-bit modulus 14 2048-bit modulus 15 3072-bit modulus 16 4096-bit modulus none	Specify the PFS settings to use on the IPsec tunnel. Choose 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: group-16</i>

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, click DPD 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 2: 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
IKE Version	1 IKEv1 2 IKEv2	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. <i>Default:</i> IKEv1
IKE Mode	Aggressive mode Main mode	For IKEv1 only, specify one of the following modes: <ul style="list-style-type: none"> Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear. Establishes an IKE SA session before starting IPsec negotiations. <p>Note For IKEv2, there is no mode.</p> <p><i>Default:</i> Main mode</p>

Parameter Name	Options	Description
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. <i>Range:</i> 1 hour through 14 days <i>Default:</i> 14400 seconds (4 hours)
IKE Cipher Suite	3DES 192-AES 256-AES AES DES	Specify the type of authentication and encryption to use during IKE key exchange. <i>Default:</i> 256-AES
IKE Diffie-Hellman Group	2 14 15 16	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. <ul style="list-style-type: none">• 1024-bit modulus• 2048-bit modulus• 3072-bit modulus• 4096-bit modulus <i>Default:</i> 4096-bit modulus
IKE Authentication	Configure IKE authentication.	
	Preshared Key	Enter the password to use with the preshared key.
	IKE ID for Local End Point	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
	IKE ID for Remote End Point	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 > 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.

CLI Equivalent for Changing the IKE Version



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

CLI Equivalents for IKEv1

ISAKMP CLI Configuration for IKEv1

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

IPsec CLI Configuration for IKEv1

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

Summary Steps

1. enable

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

CLI Equivalent for IKE2

```
crypto
 ikev2
   proposal proposal_name
     encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
     integrity {sha256 | sha384 | sha512}
     group {2 | 14 | 15 | 16}
   keyring ikev2_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 5

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, on page 37](#)
- [Configure Firewall Policies, on page 37](#)
- [Monitor Enterprise Firewall, on page 44](#)
- [Zone-Based Firewall Configuration Examples, on page 45](#)
- [Configure Port-Scanning Detection Using a CLI Template, on page 48](#)
- [Firewall High-Speed Logging, on page 49](#)
- [Unified Security Policy, on page 64](#)

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:

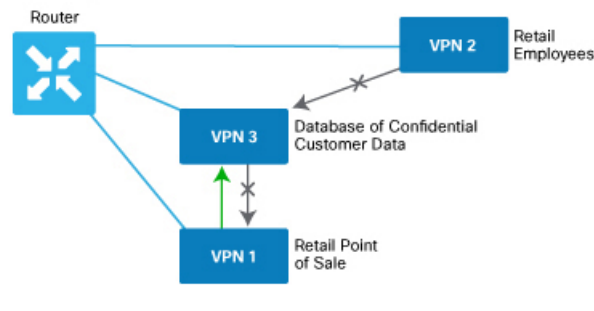
- **Source zone**—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- **Destination zone**—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- **Firewall policy**—A security policy, similar to a localized security 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, 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.



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.



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

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.

Restrictions

- You can configure up to 500 firewall rules in each security policy in Cisco vManage.
- For packets coming from Overlay to Service, the source VPN of the packet is defaulted to the destination VPN (service side VPN) for performing a Source Zone lookup when the actual source VPN cannot be determined locally on the branch. For example, a packet coming from VPN2 from the far end of a branch in a DC is routed through the Cisco SD-WAN overlay network to VPN1 of a branch router. In this case, if the reverse route lookup for the source IP does not exist on the branch VPN1, the source VPN for that packet is defaulted to the destination VPN (VPN1). Therefore, VPN1 to VPN1 Zone-pair firewall policy is applied for that packet. This behaviour is expected with policy-based routing configuration, and below are the examples of such a configuration.

Configuration	Command
Data policy: switching the VPN	<code>set-vpn</code>
Control policy and data policy: service chaining	<code>set service</code>

Configure Firewall Policies

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

Cisco vManage Firewall Configuration Procedure

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

- Create rules or rule sets – Create rules or sets of rules that you apply in the match condition of a firewall policy.

In Cisco vManage Release 20.4.1 and onwards, rule sets are supported. Rule sets are a method to easily create multiple rules with the same intent. Unlike rules, you can also reuse rule sets for multiple security policies. The configurations that Cisco vManage generates for configurations are smaller than for rules. For rules, a new class-map is generated for each rule. However, since rule sets use a common action (such as inspect, drop, or pass), a variety of rules are added to one class-map with multiple object-groups. When creating rules for the same source, destination, or intent, we recommend using rule sets.

Rules and rule sets can consist of the following conditions:

- Source data prefix(es) or source data prefix list(s).

- Source port(s) or source port list(s).
- Destination data prefix(es) or destination data prefix list(s).
- Destination port(s) or destination port list(s).



Note Destination ports or destination port lists cannot be used with protocols or protocol lists.

- Protocol(s) or protocol list(s).
 - Application lists.
- Define the order – Enter Edit mode and specify the priority of the conditions
 - Apply zone-pairs – Define the source and destination zones for the firewall policy.

You must configure all these components to create a firewall policy. .

Start the Security Policy Configuration Wizard

To start the policy configuration wizard:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Security Policy**.
3. Choose a security policy use-case scenario from one of the following:
 - Compliance.
 - Guest Access.
 - Direct Cloud Access.
 - Direct Internet Access.
 - Custom.
4. Click **Proceed**.
5. Click **Create Add Firewall Policy**.
6. Click **Create New**.

The Add Firewall Policy wizard is displayed.

Create Rules

Table 3: Feature History

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

Notes

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

Limitations

- Maximum number of fully qualified domain name (FQDN) patterns supported for a rule under firewall policy: 64
- Maximum number of entries for FQDN to IP address mapping supported in the database: 5000
- If a firewall policy uses an FQDN in a rule, the policy must explicitly allow DNS packets, or resolution will fail.
- Firewall policy does not support mapping multiple FQDN's to a single IP address.
- Only two forms of FQDN are supported: full name or a name beginning with an asterisk (*) wildcard.
Example: *.cisco.com

1. [Start the Security Policy Configuration Wizard](#)
2. In the **Name** field, enter a name for the policy.
3. In the **Description** field, enter a description for the policy.
4. Depending on your release of Cisco vManage, do one of the following:
 - Cisco vManage Release 20.4.1 and later releases:
 - a. Click **Add Rule/Rule Set Rule**.
 - b. Click **Add Rule**.
 - Cisco vManage Release 20.3.2 and earlier releases: click **Add Rule**.

The zone-based firewall configuration wizard opens.

5. Choose the order for the rule.
6. Enter a name for the rule.
7. Choose an action for the rule:

- **Inspect**
- **Pass**
- **Drop**

8. If you want matches for this rule to be logged, check the **Log** check box.
9. Configure one or more of the following.



Note For the following parameters, you can also enter defined lists or define a list from within the window.

Section	Description
Source Data Prefix(es)	IPv4 prefix(es) or prefix list(s) and/or domain names (FQDN) or list(s)
Source Port(s)	Source port(s) and/or list(s)
Destination Data Prefix(es)	IPv4 prefix(es) or prefix list(s) and/or domain names (FQDN) or list(s)
Destination Ports	Destination port(s) and/or list(s) Note Destination ports or destination port lists cannot be used with protocols or protocol lists.
Protocol(s)	Protocol(s) and/or list(s)
Application List(s)	Applications and/or list(s) Note If you chose an Application or Application Family List, you must choose at least one other match condition.

10. Click **Save** to save the rule.
11. (Optional) Repeat steps 4 to 10 to add more rules.
12. Click **Save Firewall Policy**.

Create Rule Sets

Table 4: Feature History

Feature Name	Release Information	Description
Support for Rule Sets	Cisco IOS XE Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to create sets of rules called rule sets. Rule sets are a method to create multiple rules that have the same intent. You can also re-use rule sets between security policies.

1. [Start the Security Policy Configuration Wizard](#)
2. Click **Add Rule/Rule Set Rule**. The zone-based firewall configuration wizard opens.
3. To add a rule set, click **Add Rule Set**.
4. Choose the order for the rule set.
5. Enter a name for the rule set.
6. Choose an action for the rule:
 - **Inspect**
 - **Pass**
 - **Drop**
7. If you want matches for this rule to be logged, check the **Log** check box.
8. Click + next to Rule Sets.
9. Choose from existing rule sets or create a new list by clicking + **New List**.
 - To choose from an existing rule: click the existing rule(s) and click **Save**.
 - To create a new rule:
 - a. Configure a rule using one or more of the following.

Section	Description
Source Data Prefix(es)	IPv4 prefix(es) or prefix list(s) and/or domain names (FQDN) or list(s)
Source Port(s)	Source port(s) and/or list(s)
Destination Data Prefix(es)	IPv4 prefix(es) or prefix list(s) and/or domain names (FQDN) or list(s)
Destination Ports	Destination port(s) and/or list(s) Note Destination ports or destination port lists cannot be used with protocols or protocol lists.
Protocol(s)	Protocol(s) and/or list(s)
Application List(s)	Applications and/or list(s) Note If you chose an Application or Application Family List, you must choose at least one other match condition.

- b. Click **Save** to save the rule.
 - c. (Optional) Add more rules by repeating steps 7 and 8.
10. Click **Save** to save the rule set.
11. Click + next to Application List To Drop.

12. Choose existing lists or create your own.
13. Click **Save**.
14. Review the rule set and click **Save**.
15. (Optional) Create additional rule sets or reorder the rule sets and/or rules if required.
16. Click **Save Firewall Policy**.

You can also create rule sets from outside the Security Policy Wizard as follows:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Lists**.
4. Click **Rule Sets**.
5. Click **New Rule Set**.
6. You can now choose from the various parameters such as source data prefix, port, protocol, and so on. Once you create your rule, click **Save Rule** to save the rule and add it to your rule set.
7. Create any additional rules that you want to add to your rule set.
8. After creating all the rules that you want for your rule set, click **Save Rule Set**.

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 chosen 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. For information see, [Start the Security Policy Configuration Wizard](#).
2. 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 ..., and choose the desired option.
9. Click **Next** to configure the next security block in the wizard. If you do want to configure other security features in this policy, click **Next** until the Policy Summary page is displayed.



Note When you upgrade to Cisco SD-WAN Release 20.3.3 and later releases from any previous release, traffic to and from a service VPN IPSEC interface is considered to be in the service VPN ZBFW zone and not a VPN0 zone. This could result in the traffic getting blackholed, if you allow traffic flow only between service VPN and VPN0 and not the intra service VPN.

You have to make changes to your ZBFW rules to accommodate this new behavior, so that the traffic flow in your system is not impacted. To do this, you have to modify your intra area zone pair to allow the required traffic. For instance, if you have a policy which has the same source and destination zones, you have to ensure the zone-policy allows the required traffic.

Create 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 49](#).

- 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 a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**.
3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.

The **Additional Templates** section is displayed.

6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click ... next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.



Note

If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco vManage, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Monitor Enterprise Firewall

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

To monitor Enterprise Firewall and view statistics:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Choose 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, choose **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. From the Cisco vManage menu, choose **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. Click **Data Prefix** in the left pane.
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. Click **Zones** in the left pane.
2. Click **New Zone List** in the right pane.
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 choose **Create New**.
2. Enter a name and description for the policy.
3. Click **Add Sequence** in the left pane.
4. Click **Add Sequence Rule** in the right pane.
5. Choose the desired match and action conditions.
6. Click **Same Match and Actions**.
7. Click **Default Action** in the left pane.
8. Choose 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 menu, choose the zone from which data traffic originates.
4. In the Destination Zone drop-down menu, choose 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.

Configure Port-Scanning Detection Using a CLI Template

Table 6: Feature History

Feature Name	Release Information	Description
Configure Port-Scanning Detection Using a CLI Template	Cisco IOS XE Release 17.4.1a Cisco vManage Release 20.4.1	This feature lets you configure port-scanning detection and apply a severity level (low, medium, or high) for identifying and classifying potential attacks using a CLI template.

Port scanning is a way of determining the open ports on a network, which receive and send data.

To configure port-scanning detection and include severity levels, use the following commands:

- **port-scan**
- **sense level**



Note

The **port-scan** command can detect, but not block possible port-scan attacks.

For more information on using these commands, see the **port-scan** and **sense level** commands in the [Cisco SD-WAN Command Reference Guide](#).

To detect port-scanning activity in your network, configure port-scanning detection on your device by copying and pasting in the configuration as a Cisco vManage CLI template. For more information on using CLI templates, see [Create a CLI Add-On Feature Template](#) in the Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x.

To generate port-scanning alerts, use Network Mapper (Nmap) commands. Nmap is an open-source tool for network scanning and discovery. For more information on Nmap command usage and installation, see <https://nmap.org/book/man.html>. Run the Nmap commands as an administrator:

1. After port-scanning detection is configured using a Cisco vManage CLI template, run the Linux Nmap commands from the device where port-scanning detection is configured.
2. After the Nmap commands are run, you can see the port-scanning alerts generated on the router by running the following Cisco IOS XE command:

```
Router# show utd engine standard logging events
```

3. From the Cisco vManage home page, chose **Monitor > Events** to see the port-scanning notifications.
4. To verify that the port-scanning configuration is applied on the router, use the following Cisco IOS XE **show** command:

```
Router# show utd engine standard config threat-inspection
```

```
Router# show utd engine standard config threat-inspection
UTD Engine Standard Configuration:
```

```
UTD threat-inspection profile table entries:
```

```
Threat profile: THREAT_INSP1
Mode: Intrusion Prevention
Policy: Security
Logging level: Informational
Port Scan:
Sense level: Medium
```

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 7: 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 8: NetFlow Field IDs

Field ID	Type	Length	Description
NetFlow ID Fields (Layer 3 IPv4)			
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
Flow ID Fields (Layer 4)			
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 ¹ 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

Field ID	Type	Length	Description
FW_TCP_ACK	185	4	TCP acknowledgment number
Flow ID Fields (Layer 7)			
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.
Flow Name Fields (Layer 7)			
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).
Flow ID Fields (Interface)			
FW_SRC_INTF_ID	10	2	Ingress SNMP ² ifIndex
FW_DST_INTF_ID	14	2	Egress SNMP ifIndex
FW_SRC_VRF_ID	234	4	Ingress (initiator) VRF ³ ID
FW_DST_VRF_ID	235	4	Egress (responder) VRF ID
FW_VRF_NAME	236	32	VRF name
Mapped Flow ID Fields (Network Address Translation)			
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
Status and Event Fields			
FW_EVENT	233	1	High level event codes <ul style="list-style-type: none"> • 0—Ignore (invalid) • 1—Flow created • 2—Flow deleted • 3—Flow denied • 4—Flow alert

Field ID	Type	Length	Description
FW_EXT_EVENT	35,001	2	Extended event code. For normal records the length is 2 byte, and 4 byte for optional records.
Timestamp and Statistics Fields			
FW_EVENT_TIME_MSEC	323	8	Time, in milliseconds, (time since 0000 hours UTC ⁴ 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
AAA Fields			
FW_USERNAME	40,000	20 or 64 depending on the template	AAA ⁵ user name
FW_USERNAME_MAX	40,000	64	AAA user name of the maximum permitted size
Alert Fields			
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
Miscellaneous			
FW_ZONEPAIR_ID	35,007	4	Zone pair ID
FW_CLASS_ID	51	4	Class ID

Field ID	Type	Length	Description
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
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"> • 0x01—Per box • 0x02—VRF • 0x03—Zone • 0x04—Class map • Other values are undefined
FW_EVENT_LEVEL_ID	33,004	4	Defines the identifier for the FW_EVENT_LEVEL field <ul style="list-style-type: none"> • If FW_EVENT_LEVEL is 0x02 (VRF), this field represents VRF_ID. • If FW_EVENT_LEVEL is 0x03 (zone), this field represents ZONE_ID. • If FW_EVENT_LEVEL is 0x04 (class map), this field represents CLASS_ID. • 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.
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

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

HSL Messages

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

Table 9: Syslog Messages and Their Templates

Message Identifier	Message Description	HSL Template
FW-6-DROP_PKT Type: Info	<p>Dropping %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u %s %s</p> <p>Explanation: Packet dropped by firewall inspection.</p> <p>%s: tcp/udp/icmp/unknown prot/L7 prot</p> <p>%s:interface</p> <p>%CA:%u ip/ip6 addr: port</p> <p>%s:%s: zone pair name/ class name</p> <p>%s "due to"</p> <p>%s: fw_ext_event name</p> <p>%u ip ident</p> <p>%s: if tcp, tcp seq/ack number and tcp flags</p> <p>%s: username</p>	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: l4/l7 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: l4/l7 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	<p>(target:class)-(%s:%s):New TCP connections to host %CA no longer blocked</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%CA: ip/ip6 addr</p>	<p>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</p>
FW-4-HOST_TCP_ALERT_ON Type: Warning	<p>"(target:class)-(%s:%s):Max tcp half-open connections (%u) exceeded for host %CA.</p> <p>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.</p> <p>%s:%s: zonepair name: class name</p> <p>%u: half open cnt</p> <p>%CA: ip/ip6 addr</p>	<p>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</p>

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 > 1 min blockout time</p> <p>%u: half open counter</p>	<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</p>
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>	<p>FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_ON</p>

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>	FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_OFF
FW-4-SESSIONS_MAXIMUM 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 => %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 => %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 [Start the Security Policy Configuration Wizard, on page 38](#).

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
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	parameter-map type inspect-global Example: Device(config)# parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.
Step 4	log dropped-packets Example: Device(config-profile)# log dropped-packets	Enables dropped-packet logging.
Step 5	log flow-export v9 udp destination <i>ip-address</i> port-number vrf <i>vrf-label</i> Example: 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.
Step 6	log flow-export template timeout-rate <i>seconds</i> Example: 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	end Example: 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	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	parameter-map type inspect <i>parameter-map-name</i> Example: Device(config)# parameter-map type inspect parameter-map-hsl	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect keyword, and enters parameter-map type inspect configuration mode.
Step 4	audit-trail on Example: Device(config-profile)# audit-trail on	Enables audit trail messages. You can enable audit-trail to a parameter map to record the start, stop, and duration of a connection or session, and the source and destination IP addresses.

	Command or Action	Purpose
Step 5	one-minute { <i>low number-of-connections</i> high <i>number-of-connections</i> } Example: 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.
Step 6	tcp max-incomplete host <i>threshold</i> Example: 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.
Step 7	exit Example: Device(config-profile)# exit	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
Step 8	policy-map type inspect <i>policy-map-name</i> Example: Device(config)# policy-map type inspect policy-map-hsl	Creates an inspect-type policy map and enters policy map configuration mode.
Step 9	class type inspect <i>class-map-name</i> Example: 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.
Step 10	inspect <i>parameter-map-name</i> Example: Device(config-pmap-c)# inspect parameter-map-hsl	(Optional) Enables stateful packet inspection.
Step 11	end Example: 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)# poliy-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
```

Unified Security Policy

Table 10: Feature History

Feature Name	Release Information	Description
Unified Security Policy	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to configure a single unified security policy for firewall and UTD security features such as IPS, Cisco URL Filtering, AMP, and TLS/SSL. Having a single unified security policy simplifies policy configuration and enforcement because firewall and UTD policies can be configured together in a single security operation rather than as individual policies.

Restrictions for Unified Security Policy

- If an application is not recognized by first packet, it will attempt to match other criteria in your configuration to recognize the application and apply the corresponding action. If the application can be recognized within ten packets, a reclassification process takes place.
- Unified policy can have next-generation firewall rules with or without an associated advanced inspection profile. If a unified policy is created without an advanced inspection profile associated at rule level and global level and pushed to a device, you cannot directly associate an advanced inspection profile (at a rule level or a global level) by editing the unified policy. An error is displayed. As a workaround, you must remove the unified policy from all the associated device templates, and then edit the unified policy to add an advanced inspection profile. Thereafter, you can attach the unified policy to the device template along with container profile template.

- If you modify a **TLS** action to a **Decrypt** action in the advanced inspection profile of an already deployed security policy, you must ensure that there is a **TLS/SSL Decryption** policy chosen in the **Policy Summary** page.

Information About Unified Security Policy

A unified security policy is a method of configuring a security policy that combines all the security features such as firewall, Cisco Intrusion Prevention System (IPS), Cisco URL Filtering, Advanced Malware Protection (AMP), and TLS/SSL Decryption together into a single policy.

When you create a unified security policy, you configure a firewall action (Inspect, Pass, or Drop), and also add a security inspection action, (also called as United Threat Defense (UTD) action) as part of an advanced inspection profile. If the firewall action is **Inspect**, an advanced inspection profile can be attached to a rule. An advanced inspection profile is a combination of the security features IPS, Cisco URL Filtering, AMP, and TLS/SSL Decryption. An advanced inspection profile must be created first, and then attached to a policy at a rule level or a device level.

After a unified security policy is created, it must be attached to a zone pair and pushed to the device for implementation.

You have the following options to choose from when you configure a unified policy:

- You can create a new unified security policy. For information, see [Configure Unified Security Policy](#) , on page 65
- You can continue using the existing security policy where you create separate policies for each feature. For information, see [Configure Firewall Policies](#).
- You can migrate from an existing security policy to a unified security policy. For information, see [Migrate a Security Policy to a Unified Security Policy](#), on page 72.

Benefits of Unified Security Policy

- Simplifies policy configuration where you have a single way of configuring a security policy for all the traffic passing through the device.
- Prevents reclassification of traffic for each security feature.

Use Cases for Unified Security Policy

With unified security policy:

- You can apply a combination of security inspection policies (firewall, IPS, Cisco URL Filtering, and AMP) to an application (HTTP, TFTP, Telnet, or SMTP) going from a specific source to a destination.
- A single unified security policy simplifies policy configuration and enforcement because firewall and UTD policies can be configured together in a single security operation rather than as individual policies.

Configure Unified Security Policy

Perform the following tasks to create a unified security policy:

- [Create an Object Group](#)
- [Create an Advanced Inspection Profile](#)
- [Configure Firewall and Unified Security Policy](#)
- [Add a Zone Pair](#)
- [Apply a Security Policy to a Device](#)

Create an Object Group

An object group is a set of filters that are used in a rule. You can create an object group and then attach it to a rule you are creating, or reuse it across different rules.

When you create a rule, you have the option to either attach an object group, or apply the individual filters directly to a rule. If you choose to attach an object group, the individual filters are unavailable. You must create an object group first, and then attach the object group to a rule. A new object group can also be created while you are creating a new rule.

To create a new object group, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Lists**.
4. Click **Object Group** in the left pane.
5. Click **New Object Group**.
6. In the **Object Group Name** field, enter a name for the object group.
7. In the **Description** field, enter a description for the object group.
8. Set the filters to include in this object group.
9. Click **Save**.

Create an Advanced Inspection Profile

An advanced inspection profile is a security inspection profile that includes Cisco UTD security features such as IPS, URLF, AMP, TLS Action, and TLS/SSL Decryption. After you create an advanced inspection profile, you must attach the advanced inspection profile to a policy at a rule level or a device level. You can attach up to 16 advanced inspection profiles per unified security policy. Using the advanced inspection profiles in a policy helps you create a unified security policy that has the capability of a firewall and the UTD functionality, all in the same policy.

To create an advanced inspection profile, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **Advanced Inspection Profile** in the left pane.

5. Click **New Advanced Inspection Profile**.
6. In the **Profile Name** field, enter a name for the advanced inspection profile.
7. In the **Description** field, enter a description for the advanced inspection profile.
8. In the **Intrusion Prevention** field, choose an intrusion prevention policy to add to the advanced inspection profile. The policies that you create in the unified mode determine which policies are available. For information, see [Configure Intrusion Prevention System for Unified Security Policy, on page 92](#)
9. In the **URL Filtering** field, choose a Cisco URL Filtering policy to add to the advanced inspection profile. The Cisco URL Filtering policies that you create in the unified mode determine which policies are available. For information, see [Configure URL Filtering for Unified Security Policy, on page 102](#).
10. In the **Advanced Malware Protection** field, choose an advanced malware protection policy to add to the advanced inspection profile. The advanced malware protection policies that you create in the unified mode determine which policies are available. For information, see [Configure Advanced Malware Protection for Unified Security Policy, on page 110](#)
11. Click a TLS action.
12. If you choose **Decrypt** as a TLS action, you can choose a TLS/SSL Decryption profile to add to the advanced inspection profile. The TLS/SSL Decryption profiles that you create in the unified mode determine which policies are available. For information, see [Configure TLS/SSL Profile for Unified Security Policy, on page 136](#).
13. Click **Save** to save the advanced inspection profile.

Configure Firewall Policy and Unified Security Policy

To configure a firewall policy and a unified security policy, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Unified Security Policy**.
3. Click **Add NG Firewall Policy**.
4. Click **Create New**.
5. In the **Name** field, enter a name for the policy.
6. In the **Description** field, enter a description for the policy.
7. Depending on your Cisco vManage release, do one of the following:
 - For Cisco vManage Release 20.4.1 and later releases:
 - a. Click **Add Rule**.
 - b. Click **Add Rule with Rule Sets**.
 - For Cisco vManage Release 20.3.2 and earlier releases, click **Add Rule**.
8. From the **Order** drop-down list, choose the order for the rule .
9. Enter a name for the rule.
10. From the **Action** drop-down list, choose an action for the rule.

- **Inspect**
- **Pass**
- **Drop**

11. If you want the matches for this rule to be logged, check the **Log** check box.
12. Choose an advance inspection profile to attach to the policy. This field is available only if you have chosen the action rule as **Inspect**. If you have created an advance inspection profile, this field lists all the advance inspection profiles that you have created. Choose an advance inspection profile from the list. For information on creating an advance inspection profile, see [Create an Advanced Inspection Profile, on page 66](#).
13. Click **Source**, and choose one of the following options:
 - **Object Group:** Click this option to use an object group for your rule.
To create a new object group, click **New Object Group List**. Set the filters for matching, and then click **Save**. For information on creating an object group, see [Create an Object Group, on page 66](#).
 - **Filters Types:** You can choose from IPv4 prefixes, prefix lists, fully qualified domain names (FQDN), lists or Geo Location.
14. Click **Save**.
15. Click **Destination**, and choose one of the following options:
 - **Object Group:** Click this option to use an object group for your rule.
To create a new object group, click **New Object Group List**. Set the filters for matching, and then click **Save**. For information on creating an object group, see [Create an Object Group, on page 66](#).
 - **Filters Types:** You can choose from IPv4 prefixes, prefix lists, fully qualified domain names (FQDN), lists or Geo Location.
16. Click **Save**.
17. Click **Protocol** to configure a protocol for the rule.
18. Click **Application List** to configure a list of applications you want to include in the rule. An application is subject to inspection, dropped, or allowed to pass based on the application list you configure, and the other filters that you set for the rule.

**Note**

From Cisco IOS XE Release 17.6.1a, and Cisco vManage Release 20.6.1, the applications are attached directly to the rule the way other filters are. If configured as part of access control lists (ACLs), they are attached to a class-map along with the source and destination.

19. Click **Save** to save the rule.
20. (Optional) Repeat Step 7 to Step 19 to add more rules.
21. Click **Save Unified Security Policy**.

22. Click **Add Zone Pair** to apply the policy to a zone pair. For information, see [Add a Zone Pair, on page 69](#).
23. To edit or delete a unified security policy, click ..., and choose an option.
24. Click **Next** to configure the next security block in the wizard in which have the option to configure DNS Security. For more information, see [Configure Umbrella DNS Policy Using vManage](#).
25. Click **Next**.
The **Policy Summary** page is displayed.
26. In the **Policy Summary** page, you have the option to attach an advance inspection profile at a device level. This implies, all the rules in the device that match the traffic to be inspected will be subjected to the advanced inspection profile.



Note An advanced inspection profile that is attached at a rule level is preferred over an advanced inspection profile attached at a device level. If the rule does not have advanced inspection profile attached, and if the action is **Inspect**, then the advanced inspection profile that is attached at the device level will be effective in the policy.

27. (Optional) Choose a TLS/SSL Decryption policy. This field is visible if you have configured a TLS action in the advanced inspection profile.
28. Click **Save Policy** to save the unified security policy.
29. Apply the security policy to a device. For more information, see [Apply a Security Policy to a Device](#).

Add a Zone Pair

To add a zone pair to a policy:

1. In the **Add NG Firewall Policy** page, click **Add Zone-Pairs**.
2. In the **Source Zone** drop-down list, choose the zone that is the source of the data packets.
3. In the **Destination Zone** drop-down list, 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, but not both.

4. Click + icon to create a zone pair.
5. Click **Save**.

Configure Umbrella DNS Policy Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** wizard, click **Direct Internet Access**.
4. Click **Proceed**.

5. Click **Next** until you reach the **DNS Security** page.
6. From the **Add DNS Security Policy** drop-down list, choose one of the following:
 - **Create New:** A **DNS Security - Policy Rule Configuration** wizard is displayed. Continue to Step 7.
 - **Copy from Existing:** Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
7. If you are creating a new policy using the **Create New** option, the **DNS Security - Policy Rule Configuration** wizard is displayed.
8. Enter a policy name in the **Policy Name** field.
9. The **Umbrella Registration Status** displays the status of the API Token configuration.
10. Click **Manage Umbrella Registration** to add a token, if you have not added one already.
11. Click **Match All VPN** to keep the same configuration for all the available VPNs and continue with Step 13.
 Or click **Custom VPN Configuration** if you need to add target service VPNs to your policy. A **Target VPNs** window appears, and continue with Step 12.
12. To add target service VPNs, click **Target VPNs** at the top of the window.
13. Click **Save Changes** to add the VPN.
14. From the **Local Domain Bypass List** drop-down list, choose the domain bypass.
15. Configure **DNS Server IP** from the following options:
 - **Umbrella Default**
 - **Custom DNS**
16. Click **Advanced** to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
17. Click **Save DNS Security Policy**.
 The **Configuration > Security** window is displayed, and the DNS policy list table includes the newly created DNS Security Policy.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**.
3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.
 The **Additional Templates** section is displayed.
6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.

7. Click **Create** to apply the security policy to a device.
8. Click ... next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.



Note If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco vManage, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Configure Unified Security Policy Using the CLI

This section provides CLI configurations to configure unified security policy.

1. Attach an advanced inspection profile to a unified security policy:

```
Device# config-transaction
Device(config)# parameter-map type inspect name
Device(config)# utd-policy utd advance inspection profile-name
```

2. Attach an application to a unified security policy:

```
Device# config-transaction
Device(config)# policy-map type inspect policy-map
Device(config-pmap)# class type inspect class-map
Device(config-pmap-c)# inspect parameter-map
```

3. Attach an advanced inspection profile to a unified security policy at a device level:

```
Device# config-transaction
Device(config)# parameter-map type inspect-global
Device(config-profile)# utd-policy utd-aip-name-def
```

4. Apply a zone pair to a unified security policy:

```
Device# config-transaction
Device(config)# zone-pair security pair source src-zone destination dst-zone
Device(config-sec-zone-pair)# service-policy type inspect policy-map
```

5. Configure unified security policy:

```
Device# config-transaction
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# policy policy-name
Device(config-utd-mt-policy)# threat-inspection profile ips_profile
```

```
Device(config-utd-mt-policy)# web-filter url profile urlf_profile
Device(config-utd-mt-policy)# file-inspection profile file_insp_profile
Device(config-utd-mt-policy)# tls-decryption profile tls_dec_profile
```

Migrate a Security Policy to a Unified Security Policy

From Cisco IOS XE Release 17.6.1a and Cisco vManage Release 20.6.1, Cisco SD-WAN supports unified security policy. You can migrate your existing firewall and other security policies to a unified security policy by copying the policies. While copying a security policy to a unified policy, all the zone pairs that are attached to the policy, and the applications added to **Application List to Drop** list are removed. You will have to reattach the zone pair and reconfigure the application list for the newly copied policy.

To migrate your security policy to a unified security policy:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Unified Security Policy**.
3. Click **Add NG Firewall Policy**.
4. Click **Copy from Existing NG Firewall Policy**.
5. Click **Copy**.



Note

Existing security policies cannot be migrated to a unified security policy as is. You must create an advanced inspection profile and then attach it to the relevant rules in the policy. Alternatively, you can add an existing advanced inspection profile at the device level in **Policy Summary** page and further optimize it.

Monitor Unified Security Policy

You can monitor the unified policies you created using Cisco vManage.

1. From the Cisco vManage menu, choose **Monitor > Network**.
2. Click the host name of the device you want to monitor.
3. In the left pane, under **Security Monitoring**, choose a security feature.

Depending on what you choose, the details are displayed.

Monitor Unified Security Policy Using the CLI

Example 1

The following is a sample output from the **show utd unified-policy** command. This example displays a unified policy configuration.

```
Device# show utd unified-policy
Unified Policy is enabled
```

```
Config State : MT Config Sync Complete
Bulk download Timer State : Stopped
Messages sent in current transaction: 0
Config download queue size: 0
UTD TLS-decryption dataplane policy is enabled
```

Example 2

The following is a sample output from the **show utd engine standard config** command. This example displays the Unified Threat Defense (UTD) configuration.

```
Device# show utd engine standard config
TD Engine Standard Configuration:

Unified Policy: Enabled

URL-Filtering Cloud Lookup: Enabled

URL-Filtering On-box Lookup: Disabled

File-Reputation Cloud Lookup: Disabled

File-Analysis Cloud Submission: Disabled

UTD TLS-Decryption Dataplane Policy: Enabled

Flow Logging: Disabled

UTD VRF table entries:
Policy: uni-utd
Threat Profile: uips

VirtualPortGroup Id: 1

UTD threat-inspection profile table entries:
Threat profile: uips
```

```
Mode: Intrusion Prevention
```

```
Policy: Balanced
```

```
Logging level: Error
```

```
UTD threat-inspection whitelist profile table entries:
```

```
UTD threat-inspection whitelist profile table is empty
```

```
UTD web-filter profile table entries
```

```
UTD web-filter profile table is empty
```

```
UTD TLS-Decryption profile table entries
```

```
UTD TLS-Decryption profile table is empty
```

```
UTD File analysis table entries
```

```
UTD File analysis profile table is empty
```

```
UTD File reputation table entries
```

```
UTD File reputation profile table is empty
```

Example 3

The following is a sample output from the **show platform hardware qfp active feature utd config** command. This example shows the UTD datapath configuration and status.

```
Device# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: disabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst id 0 feat id 4 fo id 4 chunk id 17
  Max flows: 55000
```

Configuration Example for Unified Security Policy

Example

The following example shows a configured unified security policy:

```

Device# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: disabled
  Unified-policy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 3 fo id 3 chunk id 16
  Max flows: 165000
  SN Health: channel: Threat Defense : Green
  SN Health: channel: Service : Down

Flow-logging Information:
-----
  State : disabled

Context Id: 0, Name: Global domain Security Context

  Ctx Flags: (0x50001)
  Engine: Standard
  State : Enabled
  SN Redirect Mode : Fail-open, Divert
  Threat-inspection: Not Enabled
  Domain Filtering : Not Enabled
  URL Filtering : Not Enabled
  File Inspection : Not Enabled
  All Interfaces : Not Enabled
  TLS action : Not specified

Context Id: 2, Name: 2 : 2

  Ctx Flags: (0xc50001)
  Engine: Standard
  State : Enabled
  SN Redirect Mode : Fail-open, Divert
  Threat-inspection: Not Enabled
  Domain Filtering : Not Enabled
  URL Filtering : Enabled
  File Inspection : Not Enabled
  All Interfaces : Enabled
  TLS action : Do-not-Decrypt

```

Configuration Example of an Application Firewall in a Unified Security Policy

Example

The following example shows how to configure the match criterion for a class map on the basis of a specified protocol for application firewall.

In this configuration example, if an application is not recognized by the first packet, it will not match either **seq-1** or **seq-11**. It will use a default action. You must specify an L3 or L4 class if you do not want to use the default action path.

An application that is not recognized by the first packet will match **seq-21** and use the corresponding action defined there. If the application can be recognized within ten packets, reclassification of packets takes place.

In this example, if the application is outlook, it will match **seq-1**. For reclassification, if the application is gmail, reclassification results in matching **FW1-seq-1-cm**.

```

Device(config)# policy-map type inspect FW1
Device(config-pmap)# class type inspect FW1-seq-1-cm
Device(config-pmap-c)# inspect AIP_1-pmap
!
Device(config-pmap)# class type inspect FW1-seq-11-cm
Device(config-pmap-c)# drop
!
Device(config-pmap)# class type inspect FW1-seq-21-cm
Device(config-pmap-c)# inspect
!
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
!
!
Device(config)# class-map type inspect match-all FW1-seq-1-cm
Device(config-cmap)# match class-map MAIL_APP-GLOBAL-cm
Device(config-cmap)# match access-group name FW1-seq-Rule_1-acl!

Device(config)# class-map type inspect match-all FW1-seq-11-cm
Device(config-cmap)# match class-map STREAMING_APP-GLOBAL-cm
Device(config-cmap)# match access-group name FW1-seq-Rule_2-acl
!
Device(config)# class-map type inspect match-all FW1-seq-21-cm
Device(config-cmap)# match class-map FW1-sRule_3-14-cm
!
Device(config)# class-map match-any MAIL_APP-GLOBAL-cm
Device(config-cmap)# match protocol gmail
Device(config-cmap)# match protocol outlook-web-service
!
Device(config)# class-map match-any STREAMING_APP-GLOBAL-cm
Device(config-cmap)# match protocol netflix
Device(config-cmap)# match protocol youtube
!
Device(config)# class-map type inspect match-any FW1-sRule_3-14-cm
Device(config-cmap)# match protocol tcp
!
Device(config)# ip access-list extended FW1-seq-Rule_1-ac
Device(config-ext-nacl)# 11 permit object-group FW1-Rule_1-svc_ any any
!
Device(config)# ip access-list extended FW1-seq-Rule_2-acl
Device(config-ext-nacl)# 11 permit object-group FW1-Rule_2-svc_ any any
!
Device(config)# object-group service FW1-Rule_1-svc
Device(config-service-group)# ip
!
Device(config)# object-group service FW1-Rule_2-svc
Device(config-service-group)# ip
!

```



CHAPTER 6

Configure Geolocation-Based Firewall Rules for Network Access

Table 11: Feature History

Feature Name	Release Information	Description
Geolocation-Based Firewall Rules for Allowing or Denying Network Traffic Based on Geolocation	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	<p>This feature enables you to configure firewall rules for allowing or denying network traffic based on the source and destination location instead of IP addresses.</p> <p>This feature adds a new object group, geo, where you can specify countries and continents as objects in an Access Control List (ACL). An object group ACL simplifies policy creation in large networks, especially if the ACL changes frequently.</p> <p>New object-group and geo commands were added.</p>

- [Overview of Geolocation-Based Firewall Rules, on page 77](#)
- [Prerequisites for Geo Object Groups, on page 78](#)
- [Restrictions for Geo Object Groups, on page 79](#)
- [Configure Geolocation-Based Firewall Rules, on page 79](#)
- [Configure Geolocation-Based Firewall Rules Using the CLI, on page 81](#)
- [Update the Geolocation Database Using the CLI, on page 82](#)
- [Verify Geolocation-Based Firewall Rules Using the CLI, on page 82](#)

Overview of Geolocation-Based Firewall Rules

Geolocation-based firewall rules allow you to configure firewall rules for allowing or denying network traffic based on the specified source and destination locations.

A third-party database is used for geolocation-to-IP-address mapping. Use the **geo database update** command to update the geolocation database periodically to pick up the latest changes.

After you configure a geolocation-based firewall rule by specifying source and destination locations in Cisco vManage, the geolocation database is automatically enabled in the CLI. Alternatively, you can use the **geo database** command to enable the geolocation database.

For more information on the CLI commands, see [Cisco IOS XE SD-WAN Qualified Command Reference](#).

This feature adds a new object group **geo**, where you can specify countries and continents as objects to use in Access Control Lists (ACLs). The new geo object group is then used in the ACL to enable geolocation-based firewall rules.

The geo object group is a collection of the following types of objects:

- Three-letter country code objects
- Two-letter continent code objects

An object group can contain a single object or multiple objects. You can nest other geolocation object groups using the **group-object** command.


Note

You cannot configure nested geo object groups in Cisco vManage. You can configure nested geo object groups using only the CLI.

Data packets are classified using geolocation-based firewall rules instead of using IP addresses. When classifying the data packet, if a firewall rule has a geolocation-based filter, an IP address lookup occurs against the geolocation database to determine which country or continent is associated with the IP address.

Use-Case Scenario

A client (192.168.11.10) in a local area network (LAN) initiates traffic over Dedicated Internet Access (DIA) to a destination IP addresses belonging to France (FRA) and Germany (GBR). As per the security firewall policy, traffic to France should be inspected and that to Germany should be dropped.

Benefits of Geolocation-Based Firewall Rules

- You can restrict access to particular countries without needing to know the associated IP addresses for those countries.
- A geolocation can be a country, a continent, or a list containing both continents and countries.


Note

After you have chosen a continent in a security firewall rule, all IP addresses belonging to that particular continent code are inspected as part of the security firewall rule.

- You can add multiple geolocation lists or geolocations using a single policy.
- When you update a geo object group, all the policies that use that geo object group are automatically updated.

Prerequisites for Geo Object Groups

To associate a geo object with an ACL, the geo object group must be already defined with at least one object.

Restrictions for Geo Object Groups

- Empty geo object groups are not supported. Any empty geo object group is deleted in exiting global configuration mode. You cannot associate an empty object group with an ACL.



Note An empty geo object group is a geo object group that does not contain any references to countries. To empty a geo object group, you need to remove any references to countries within the geo object group.

- As long as a geo object group is in use inside the corresponding ACL or nested in another group, it can neither be deleted nor emptied.
- A geo object group can be associated only with extended IPv4 ACLs and not with IPv4 standard ACLs.

Configure Geolocation-Based Firewall Rules

To configure firewall rules, specify the source and destination locations in the security firewall policies in Cisco vManage.

There are two ways to configure geofiltering using Cisco vManage:

- Configure a geolocation list using **Configuration > Security > Custom Options**.
- Create or add a geolocation list or a geolocation to an existing firewall security policy.

Prerequisite: You must have an existing security policy for the second bullet item.



Note If you add a geolocation list, you cannot add a geolocation.
Conversely, if you add a geolocation, you cannot add a geolocation list.



Note You cannot configure both a fully qualified domain name (FQDN) and a geo as a source data prefix and as a destination data prefix.

Configure a Geolocation List Using Configuration > Security > Custom Options

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. From the **Custom Options** drop-down menu, choose **Lists**.
3. Click **Geo Location** in the left pane.
4. Click **New Geo Location List**.
5. Enter a name for the geolocation list.

6. Choose one or more geolocations from the drop-down menu.

**Note**

If you choose a continent, you cannot choose any of the countries that are part of the continent. If you want to choose a list of countries, choose the appropriate countries from the list.

7. Click **Add**.

Create a Geolocation List or Add a Geolocation to an Existing Security Firewall Policy

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Choose an existing security policy.
3. For the chosen policy, click **...**, and click **Edit**.
The **Edit Security Policy** window displays.
4. Click **Firewall**.
5. For the desired policy you want to modify, click **...** and click **Edit**.
The **Edit Firewall Policy** window displays.
6. Click **Add Rule/Rule Set Rule**.
7. From the drop-down menu, choose **Add Rule**.
The **New Firewall** window displays.
8. Click **Source Data Prefix** to add a source geolocation list or new geolocations.
9. From the **Geo Location List** drop-down menu, choose a previously configured geolocation list.
10. Alternatively, to create a new geolocation list, choose **New Geo Location**.
The **Geo Location List** dialog box displays.
 - a. In the **Geo Location List Name** field, specify a name for the geolocation list.
 - b. From the **Select Geo Location** drop-down menu, choose one or more locations.
 - c. Click **Save**.
11. From the **Geo Location** drop-down menu, choose one or more locations.
12. Click **Save**.
13. Click **Destination Data Prefix** to add a destination geolocation list or new geolocations.
14. Repeat Step 9 through Step 12.
15. Click **Save Firewall Policy** to save the security firewall rule.
16. Click **Save Policy Changes**.

Configure Geolocation-Based Firewall Rules Using the CLI

1. Enable the geolocation database:

```
Device(config)# geo database
```

2. View the status of the geodatabase:

```
Device# show geo status
Geo-Location Database is enabled
File in use       : geo_ipv4_db
File version      : 2134.ajkdbnakjsdn
Number of entries : 415278
```

3. View the contents of the geodatabase file:

```
Device# show geo file-contents info bootflash:geo_ipv4_db
File version      : 2134.ajkdbnakjsdn
Number of entries : 415278
```

4. Update the geodatabase for periodic updates:

```
Device# geo database update bootflash:geo_ipv4_db
```

Here, *geo_ipv4_db* is the name of the geodatabase file downloaded from the Cisco.com path and copied to the bootflash device or the hard disk.

5. Create a geo object group:

```
Device(config)# object-group geo GEO_1
```

6. Add a continent to a geo group object:

```
Device(config-geo-group)# continent EU
```

7. Add a country to a geo group object:

```
Device(config-geo-group)# country GBR
```

8. View the geo object group:

```
Device# show object-group name Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
GEO object group Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
country GBR
```

9. View detailed country information:

```
Device# show platform hardware qfp active feature geo client alpha gbr
Country alpha code: gbr
Country numeric code: 826
GEO country info:
Country alpha code: gbr
Continent alpha code: eu
Continent numeric code: 5
Country ref count: 0
Country hit count: 13
```

10. Verify geodatabase status:

```
Device# show platform hardware qf active feature geo client stats
CPP client Geo DB stats
-----
Enable received      : 1
Modify received      : 0
```

```

Disable received          : 0
Enable failed            : 0
Modify failed            : 0
Disable failed           : 0
IPv4 table write failed   : 0
Persona write failed     : 0
Country table write failed : 0

```

11. View the geodatabase file and memory information:

```

Device# show platform hardware qf active feature geo client info
Geo DB enabled
DB in use
  File name: /usr/binos/conf/geo_ipv4_db
  Number of entries installed: 415278
  Version: 2134.ajkdbnakjsdn
  Datapath PPE Address: 0x00000000f0d3b070
  Size (bytes): 6644448
  Exmem Handle: 0x009dcf0709080003
Country table
  Datapath PPE Address: 0x00000000f04bcc60
  Size (bytes): 16000
  Exmem Handle: 0x009550c609080003

```

12. View geodatabase table memory information:

```

Device# show platform hardware qf active feature geo datapath memory
Table-Name  Address      Size
-----
Country DB  0xf04bcc60   1000
IPV4 DB     0xf0d3b070  415278

```

For more information on the CLI commands, see [Cisco IOS XE SD-WAN Qualified Command Reference](#).

Update the Geolocation Database Using the CLI

To ensure that you are using up-to-date geographical location data, we recommend that you update the geolocation database.

To download and update the geolocation database using the CLI:

1. Download the geolocation database from Cisco Software Central.
2. On the CLI, use Secure Copy Protocol (SCP) or TFTP to copy the geolocation database to your Cisco IOS XE SD-WAN device:

```
Device# copy scp: bootflash:
```

or

```
Device# copy tftp: bootflash:
```

Verify Geolocation-Based Firewall Rules Using the CLI

The following example shows how geo object groups are created for France and Germany:

```

platform inspect match-statistics per-filter
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
!

```

```

object-group geo Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
  country FRA
!
object-group network Zone1_to_Zone1-seq-Rule_1-network-src-og_
  host 192.168.11.10
!
object-group service Zone1_to_Zone1-seq-Rule_1-service-og_
  ip
!
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_ geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
!
ip access-list extended Zone1_to_Zone1-seq-Rule_2-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
  country GBR

```

The following example shows how a geo object group is defined under an extended ACL that is used in a security firewall class map:

```

ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_ geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
!
ip access-list extended Zone1_to_Zone1-seq-Rule_2-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
  country GBR
!
object-group network Zone1_to_Zone1-seq-Rule_1-network-src-og_
  host 192.168.11.10
!
object-group service Zone1_to_Zone1-seq-Rule_1-service-og_
  ip
!
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_ geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
!
ip access-list extended Zone1_to_Zone1-seq-Rule_2-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
  country GBR

```

The following example shows when a geolocation is chosen as part of a security firewall rule either in a source or a destination data prefix from Cisco vManage, the geodatabase is added by default. If a geolocation is removed, the geodatabase is removed from the rule.

```

class-map type inspect match-all Zone1_to_Zone1-seq-1-cm_
  match access-group name Zone1_to_Zone1-seq-Rule_1-acl_
!
class-map type inspect match-all Zone1_to_Zone1-seq-11-cm_
  match access-group name Zone1_to_Zone1-seq-Rule_2-acl_
!
policy-map type inspect Zone1_to_Zone1
  ! first
  class Zone1_to_Zone1-seq-1-cm_
    inspect
  !
  class Zone1_to_Zone1-seq-11-cm_
    drop
  !
  class class-default
    drop

```

```

!
parameter-map type inspect-global
  alert on
  log dropped-packets
  multi-tenancy
  vpn zone security
!
zone security Zone0
  vpn 0
!
zone security Zone1
  vpn 1
!
zone-pair security ZP_Zone1_Zone0_Zone1_to_Zone1 source Zone1 destination Zone0
  service-policy type inspect Zone1_to_Zone1
!
geo database

```

The following is a sample output of the **show policy-firewall config zone-pair** command used for validating geolocation configuration:

```

Device# show policy-firewall config zone-pair ZP_Zone1_Zone0_Zone1_to_Zone1

Zone-pair          : ZP_Zone1_Zone0_Zone1_to_Zone1
Source Zone        : Zone1
Destination Zone    : Zone0
Service-policy inspect : Zone1_to_Zone1
  Class-map : Zone1_to_Zone1-seq-1-cm_ (match-all)
  Match access-group name Zone1_to_Zone1-seq-Rule_1-acl_
Extended IP access list Zone1_to_Zone1-seq-Rule_1-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
Action : inspect
Parameter-map : Default
Class-map : Zone1_to_Zone1-seq-11-cm_ (match-all)
Match access-group name Zone1_to_Zone1-seq-Rule_2-acl_
Extended IP access list Zone1_to_Zone1-seq-Rule_2-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_2-service-og_ object-group
Zone1_to_Zone1-seq-Rule_2-network-src-og_geo-group Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
Action : drop log
Parameter-map : Default
Class-map : class-default (match-any)
Match any
Action : drop log
Parameter-map : Default

```

The following is a sample output of the **show policy-map type inspect zone-pair sessions** command used for verifying inspected and dropped traffic:

```

show policy-map type inspect zone-pair sessions
Zone-pair: ZP_Zone1_Zone0_Zone1_to_Zone1
Service-policy inspect : Zone1_to_Zone1

Class-map: Zone1_to_Zone1-seq-1-cm_ (match-all)
Match: access-group name Zone1_to_Zone1-seq-Rule_1-acl_
Inspect
Established Sessions
Session ID 0x0000000A (192.168.11.10:8)=>(2.10.1.1:14780) icmp SIS_OPEN.
Created 00:00:03, Last heard 00
Bytes sent (initiator:responder) [224:168]

Class-map: Zone1_to_Zone1-seq-11-cm_ (match-all)
Match: access-group name Zone1_to_Zone1-seq-Rule_2-acl_
Drop

```

```
13 packets, 1326 bytes
Class-map: class-default (match-any)
  Match: any
  Drop
    0 packets, 0 bytes
```




CHAPTER 7

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 87](#)
- [Cisco SD-WAN IPS Solution, on page 88](#)
- [Configure and Apply IPS or IDS, on page 88](#)
- [Modify an Intrusion Prevention or Detection Policy, on page 91](#)
- [Delete an Intrusion Prevention or Detection Policy , on page 91](#)
- [Monitor Intrusion Prevention Policy, on page 92](#)
- [Update IPS Signatures, on page 92](#)
- [Configure Intrusion Prevention System for Unified Security Policy, on page 92](#)

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 Cisco vManage](#).

Configure Intrusion Prevention or Detection

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

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
3. In Add Security Policy, choose 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** window displays.
6. Click the **Add Intrusion Prevention Policy** drop-down menu and choose **Create New** to create a new Intrusion Prevention policy. The Intrusion Prevention - Policy Rule Configuration wizard appears.

7. Click **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 menu. 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 menu. The following options are available:
 - **Detection**: Choose this option for intrusion detection mode
 - **Protection**: Choose this option for intrusion protection mode
11. (Optional) From **Advanced**, choose one or more existing IPS signature lists or create new ones as needed from the **Signature Whitelist** drop-down menu.

Choosing an IPS signature list allows the designated IPS signatures to pass through.

To create a new signature list, do the following:

 - a. Click **New Signature List** at the bottom of the drop-down. In **IPS Signature List Name**, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only).
 - b. In **IPS Signature**, enter signatures in the format *Generator ID:Signature ID*, separated with commas. You also can use **Import** to add a list from an accessible storage location.
 - c. Click **Save**.

You also can create or manage IPS Signature lists by choosing **Configuration > Security**, and then choosing **Lists** from **Custom Options**, and then choosing **Signatures**.

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 menu. 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. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**.
3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.

The **Additional Templates** section is displayed.

6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click ... next to the device template that you created.
9. Click **Attach Devices**.

10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.

**Note**

If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco vManage, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Modify an Intrusion Prevention or Detection Policy

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

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. In the Security window, click **Custom Options** drop-down menu and choose **Intrusion Prevention**.
3. For the policy you want to modify, click ... and choose **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. From the Cisco vManage menu, choose **Configuration > Security**.
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 ... and choose **Edit**.
The Policy Summary page is displayed.
 - b. Click **Intrusion Prevention**.
 - c. For the policy that you want to delete, click ... and choose **Detach**.
 - d. Click **Save Policy Changes**.
3. Delete the IPS or IDS policy as follows:
 - a. In the Security screen, click **Custom Options** drop-down menu and choose **Intrusion Prevention**.
 - b. For the policy that you want to delete, click ... and choose **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 Cisco vManage menu, choose **Monitor > Network**.
2. In the left panel, under **Security Monitoring**, Click **Intrusion Prevention**. The Intrusion Prevention wizard displays.
3. Click **By Severity** or **By Count** to designate how you want to display intrusion prevention information.

Update IPS Signatures

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



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

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

1. From the Cisco vManage menu, choose **Administration > Settings** 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.

Configure Intrusion Prevention System for Unified Security Policy

You can create an intrusion prevention policy specifically for use in a unified security policy. When created, intrusion prevention policy is included in the advanced inspection profile and applied to the unified security policy for implementation on Cisco IOS XE SD-WAN devices.

To configure an intrusion prevention system for a unified security policy, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.

2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **Intrusion Prevention** in the left pane.
5. Click **Add Intrusion Prevention Policy**, and choose **Create New**.
6. Click **Policy Mode** to enable the unified mode. This implies that you are creating an intrusion prevention policy for use in the unified security policy.



Note Target VPNs are not applicable for the intrusion prevention system used in a unified security policy.

7. Enter a policy name in the **Policy Name** field.
8. From the **Signature Set** drop-down list, choose a signature set that defines rules for evaluating traffic. 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**: Provides protection without a significant effect on system performance.
This signature set blocks vulnerabilities with a Common Vulnerability Scoring System (CVSS) score that is greater than or equal to 9. It also blocks (Common Vulnerabilities and Exposures) CVEs published in the last two years and have the following rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.
 - **Connectivity**: Less restrictive and provides 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**: Provides 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 have the following rule categories: Malware CNC, Exploit Kits, SQL Injection, blocked list, and App Detect Rules.
9. From the **Inspection Mode** drop-down list, choose an option:
 - **Detection**: Choose this option for intrusion detection mode.
 - **Protection**: Choose this option for intrusion protection mode.
10. (Optional) From **Advanced**, choose one or more existing IPS signature lists or create new ones, as needed, from the **Signature Whitelist** drop-down list.
Choosing an IPS signature list allows the designated IPS signatures to pass through.
To create a new signature list, do the following:
 - a. Click **New Signature List** at the bottom of the drop-down list.
 - b. In the **IPS Signature List Name** field, enter a list name of up to 32 characters (letters, numbers, hyphens, and underscores only).
 - c. In the **IPS Signature**, enter signatures in the format *Generator ID:Signature ID*, separated by commas. You also can click **Import** to add a list from an accessible storage location.

d. Click **Save**.

You also can create or manage IPS Signature lists by choosing **Configuration > Security** in the left pane, choosing **Lists** from **Custom Options** at the top-right corner of the window, and then choosing **Signatures** in the left pane.

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

11. (Optional) Click **Alert Log Level**, and choose one of the following options:

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

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

12. Click **Save Intrusion Prevention Policy**.



CHAPTER 8

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.



Note

A NAT direct internet access route is necessary to implement URL Filtering.

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.

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.

This section contains the following topics:

- [Overview of URL Filtering, on page 96](#)
- [Configure and Apply URL Filtering, on page 98](#)
- [Modify URL Filtering, on page 101](#)
- [Delete URL Filtering, on page 101](#)
- [Monitor URL Filtering, on page 102](#)
- [Configure URL Filtering for Unified Security Policy, on page 102](#)

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. Because the SSL/TLS session is still being established at the time it is determined the request should be blocked, the client is not expected to receive a HTTP response, whether it is the injected HTTP blocked page or redirect URL, which causes a protocol error to occur.

In Cisco SD-WAN, a HTTP response can be inserted into the HTTPS session if this traffic is routed through SSL/TLS proxy. The SSL/TLS session is allowed to establish in this case, and when the HTTP GET is received on the decrypted HTTPS session, the HTTP blocked page or redirect URL is injected and it is accepted by the client.

Database Overview

By default, WAN Edge routers do not download the URL database from the cloud.

To enable the URL database download:

- prior to Cisco vManage Release 20.5, you must set the **Resource Profile** to **High** in the App-hosting Security Feature Template.
- from Cisco vManage Release 20.5 onwards, you must enable **Download URL Database on Device** in the App-hosting Security Feature Template.

Additional memory is required to download the URL database.

If configured, WAN Edge routers download 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.

Filtering Options

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

Category-Based Filtering

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.

A URL may be associated with up to five different categories. If any of these categories match a configured blocked category, then the request will be blocked.

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.

Cloud-Lookup

The Cloud-Lookup feature is enabled by default and is used to retrieve the category and reputation score of URLs that are not available in the local database.

The category and reputation score of unknown URLs are returned as follows:

Name based URLs:

- Valid URL — corresponding category and reputation score is received.
- Unknown URL (new URL or unknown to the cloud) — category is 'uncategorized' and reputation score is 40
- Internal URLs with proper domain name (for example, internal.abc.com) — category and reputation score is based on the base domain name (abc.com from the example above).
- Completely internal URLs (for example, abc.xyz) — category is 'uncategorized' and reputation score is 40

IP based URLs:

- Public hosted IP — corresponding category and reputation score is received.
- Private IP like 10.◇, 192.168.◇ — category is 'uncategorized' and reputation score is 100
- Non-hosted/Non-routable IP — category is 'uncategorized' and reputation score is 40

The Cloud-Lookup score is different from the on-box database for these URLs (Unknown/Non-hosted/Non-routable/Internal URLs).

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 Cisco vManage](#).

Configure URL Filtering

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

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
3. In Add Security Policy, choose 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** window is displayed.
6. Click the **Add URL Filtering Policy** drop-down menu and choose **Create New** to create a new URL filtering policy. The URL filtering - Policy Rule Configuration wizard appears.
7. Click **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 one of the following options from the Web Categories drop-down:
 - **Block**: Block websites that match the categories that you choose.
 - **Allow**: Allow websites that match the categories that you choose.
10. Choose one or more categories to block or allow from the **Web Categories** list.
11. Choose a Web Reputation from the drop-down menu. The options are:
 - **High Risk**: Reputation score of 0 to 20.
 - **Suspicious**: Reputation score of 21 to 40.
 - **Moderate Risk**: Reputation score of 41 to 60.
 - **Low Risk**: Reputation score of 61 to 80.
 - **Trustworthy**: Reputation score of 81 to 100.
12. (Optional) From **Advanced**, choose one or more existing lists or create new ones as needed from the **Whitelist URL List** or **Blacklist URL List** drop-down menu.

**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** in the drop-down menu.
- 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 **Import** to add lists from an accessible storage location.
- d. Click **Save** when you are finished.

You also can create or manage URL lists. To do this:

- a. From the Cisco vManage menu, choose **Configuration > Security**.
- b. Choose **Lists** from the **Custom Options** drop-down menu.
- c. Choose **Whitelist URLs** or **Blacklist URLs** in the left pane.

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, choose 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. To edit the existing URL filtering policy, click **Custom Options** in the right-side panel of the Security wizard.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**.
3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.
The **Additional Templates** section is displayed.
6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click ... next to the device template that you created.

9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.

**Note**

If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco vManage, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Modify URL Flitering

To modify a URL Filtering policy, do the following:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. In the Security screen, click the **Custom Options** drop-down menu , choose **Policies/Profiles**, and then choose **URL Filtering**.
3. For the desired policy you want to modify, click ... and choose **Edit**.
4. Modify the policy as required and click **Save URL Filtering Policy**.

Delete URL Filtering

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

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. To detach the URL filtering policy from the security policy:
 - a. For the security policy that contains the URL filtering policy, click ... and click **Edit**.
The Policy Summary page is displayed.
 - b. Click **URL Filtering**.
 - c. For the policy that you want to delete, click ... and choose **Detach**.
 - d. Click **Save Policy Changes**.
3. To delete the URL filtering policy:
 - a. In the Security screen, click the **Custom Options** drop-down menu , choose **Policies/Profiles**, and then choose **URL Filtering**.
 - b. For the policy that you want to delete, click ... and click **Delete**.
 - 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 Cisco vManage menu, choose **Monitor > Network**, and then choose a device.
2. In the left pane, under Security Monitoring, click **URL Filtering**. The URL Filtering information displays in the right pane.
3. Click **Blocked**. The session count on a blocked URL appears.
4. Click **Allowed**. The session count on allowed URLs appears.

Configure URL Filtering for Unified Security Policy

You can create a URL filtering policy specifically for use in a unified security policy. After being created, the URL filtering policy is included in the advanced inspection profile and applied to the unified security policy for implementation on Cisco IOS XE SD-WAN devices.

To configure a URL filtering policy for a unified security policy, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **URL Filtering** in the left pane.
5. Click **Add URL Filtering Policy**, and choose **Create New**.
6. Click **Policy Mode** to enable the unified mode.

This implies that you are creating a URL filtering policy for use in the unified security policy.



Note

Target VPNs are not applicable for URL filtering used in a unified security policy.

7. Enter a policy name in the **Policy Name** field.
8. Choose one of the following options from **Web Categories**.
 - **Block**: Block websites that match the categories that you choose.
 - **Allow**: Allow websites that match the categories that you choose.
9. Choose one or more categories to block or allow from the **Web Categories** drop-down list.
10. Choose the **Web Reputation** from the drop-down list. The options are:
 - **High Risk**: The Reputation score is between 0 to 20.
 - **Suspicious**: The Reputation score is between 21 to 40.

- **Moderate Risk:** The Reputation score is between 41 to 60.
- **Low Risk:** The Reputation score is between 61 to 80.
- **Trustworthy:** The Reputation score is between 81 to 100.

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

**Note**

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

To create a new list, do the following:

- a. Click **New Whitelist URL List** or **New Blacklist URL List** in the drop-down list.
- 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 **URL** field, enter URLs to include in the list, separated by commas. You also can use **Import** to add lists from an accessible storage location.
- d. Click **Save**.

You also can create or manage URL lists by choosing **Configuration > Security**, and then choosing **Lists** from **Custom Options** top-right corner of the window, and then clicking **Whitelist URLs** or **Blacklist URLs** in the left pane.

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

12. (Optional) In the **Block Page Server** pane, choose an option to designate what happens when a user visits a URL that is blocked.

If you click **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 click **Redirect URL**, enter a URL to which users are redirected.

13. (Optional) In the **Alerts and Logs** pane, choose alert type option:
 - **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 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.
14. Configure the address of the external log server in the **Policy Summary** page.
15. Click **Save URL filtering Policy** to add an URL filtering policy.



CHAPTER 9

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 12: 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 105](#)
- [Configure and Apply an Advanced Malware Policy, on page 106](#)
- [Modify an Advanced Malware Protection Policy, on page 108](#)
- [Delete an Advanced Malware Protection Policy, on page 109](#)
- [Monitor Advanced Malware Protection, on page 109](#)
- [Troubleshoot Advanced Malware Protection, on page 109](#)
- [Rekey the Device Threat Grid API Key, on page 110](#)
- [Configure Advanced Malware Protection for Unified Security Policy, on page 110](#)

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 106](#)
- [Configure an Advanced Malware Policy](#)
- [Apply a Security Policy to a Device, on page 44](#)

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 Cisco vManage](#).
- To perform file analysis, you must configure the Threat Grid API Key as described in [Configure Threat Grid API Key](#)

**Note**

A NAT direct internet access route is necessary to apply Advanced Malware Protection Policy.

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 choose your account details.

- Step 2** Under your Account Details, an API key may already be visible if you've created one already. If you have not, click **Generate New API Key**.
- Your API key should then be visible under **User Details > API Key**.
- Step 3** From the Cisco vManage menu, choose **Configuration > Security**.
- Step 4** In the Security screen, click the **Custom Options** drop-down menu and choose **Threat Grid API Key**.
- Step 5** In the Manage Threat Grid API key dialog box, perform these steps:
- Choose a region from the **Region** drop-down menu.
 - 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** From the Cisco vManage menu, choose **Configuration > Security**.
- Step 2** Click **Add Security Policy**. The Add Security Policy wizard opens and various use-case scenarios display.
- Step 3** In Add Security Policy, choose **Direct Internet Access** and then click **Proceed**.
- Step 4** In the Add Security Policy wizard, click **Next** as needed to choose **Advanced Malware Protection**.
- Step 5** From **Advanced Malware Protection**, click **Add Advanced Malware Protection Policy** in the drop-down menu.
- Step 6** Choose **Create New**. The Add Advanced Malware Protection screen displays.
- Step 7** In the **Policy Name** field, enter a name for the malware policy. The name can be up to 128 characters and can contain only alphanumeric characters.
- Step 8** Ensure **Match All VPN** is chosen. Choose **Match All VPN** if you want to apply the policy to all the VPNs, or choose **Custom VPN Configuration** to input the specific VPNs.
- Step 9** From the **AMP Cloud Region** drop down menu, choose a global region.
- Step 10** From the **Alerts Log Level** drop down menu, choose 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](#).
- Note** File Analysis requires a separate Threat Grid license.
- Step 12** From the **TG Cloud Region** drop down menu, choose 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](#).
- Step 13** From the **File Types List** drop down menu, choose the file types that you want to be analyzed.

- Step 14** From the **Alerts Log Level** drop down menu, choose a severity level (Critical, Warning, or Info).
- Step 15** Click **Target VPNs** to choose the target service 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. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**.
3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.
The **Additional Templates** section is displayed.
6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click ... next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.



Note

If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco vManage, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Modify an Advanced Malware Protection Policy

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

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. In the Security screen, click the **Custom Options** drop-down menu, choose **Policies/Profiles**, and then choose **Advanced Malware Protection**.
3. For the desired policy you want to modify, click ... and choose **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. From the Cisco vManage menu, choose **Configuration > Security**.
2. Detach the AMP policy from the security policy as follows:
 - a. For the security policy that contains the AMP policy, click **...** and choose **Edit**.
The Policy Summary page is displayed.
 - b. Click **Advanced Malware Protection**.
 - c. For the policy that you want to delete, click **...** and choose **Detach**.
 - d. Click **Save Policy Changes**.
3. To delete the AMP policy, perform these steps:
 - a. In the Security screen, click the **Custom Options** drop-down menu, choose **Policies/Profiles**, and then choose **Advanced Malware Protection**.
 - b. For the policy that you want to delete, click **...** and choose **Delete**.
 - 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 Cisco vManage menu, choose Monitor > Network , and choose a device. |
| Step 2 | Under Security Monitoring, click Advanced Malware Protection in the left pane. |
-

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** From the Cisco vManage menu, choose **Maintenance > Security**.
 - Step 2** Click **Advanced Malware Protection**.
 - Step 3** Choose the device or devices that you want to rekey.
 - Step 4** Choose **Action > API Rekey**.
-

Configure Advanced Malware Protection for Unified Security Policy

You can create an advanced malware protection policy specifically for use in a unified security policy. When created, the advanced malware protection policy is included in the advanced inspection profile and applied to the unified security policy for implementation in Cisco IOS XE SD-WAN devices.

To configure advanced malware protection for a unified security policy, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **Advanced Malware Protection** in the left pane.
5. Click **Add Advanced Malware Protection Policy**, and choose **Create New**.
6. Click **Policy Mode** to enable the unified mode. This implies that you are creating an advanced malware protection policy for use in the unified security policy.



Note Target VPNs are not applicable for the advanced malware protection used in a unified security policy.

7. Enter a policy name in the **Policy Name** field.
8. From the **AMP Cloud Region** drop-down list, choose a global region.
9. From the **Alerts Log Level** drop-down list, choose 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.

10. Click **File Analysis** to enable Threat Grid file analysis.



Note Before you can perform Step 10, configure a threat grid API key as described in [Configure Threat Grid API Key](#).

File Analysis requires a separate Threat Grid license.

11. From the **TG Cloud Region** drop-down list, choose a global region.



Note Configure the Threat Grid API Key by clicking **Manage API Key** or as described in [Configure Threat Grid API Key](#).

From the **File Types List** drop-down list, choose the file types that you want to be analyzed.

12. From the **Alerts Log Level** drop-down list, choose a severity level (Critical, Warning, or Info).
13. Click **Save Advanced Malware Protection Policy**.



CHAPTER 10

SSL/TLS Proxy for Decryption of TLS Traffic

Table 13: Feature History

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

- [Information about SSL/TLS Proxy, on page 113](#)
- [Configure Cisco IOS XE SD-WAN Devices as TLS Proxy, on page 120](#)
- [Verify Configuration, on page 130](#)
- [Monitor TLS Proxy Performance, on page 131](#)
- [Revoke and Renew Certificates, on page 132](#)
- [Configure TLS/SSL Decryption Policy for Unified Security Policy, on page 134](#)
- [Configure TLS/SSL Profile for Unified Security Policy, on page 136](#)

Information about SSL/TLS Proxy

Overview of SSL/TLS Proxy



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

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

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

Benefits of TLS Proxy

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

Traffic Flow with TLS Proxy

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

This is how traffic flows when TLS proxy is enabled:

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

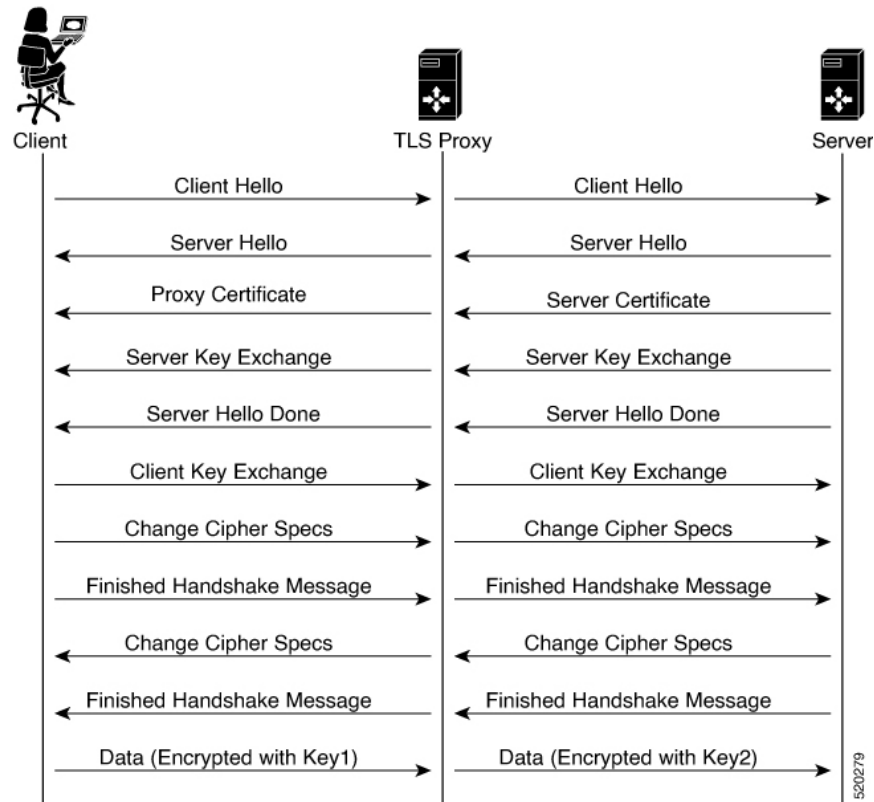


Note

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

The following image shows the TLS handshake process.

Figure 3: TLS Handshake Process



520279

Role of Certificate Authorities in TLS Proxy

About Certificate Authorities (CAs)

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

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

How CA and TLS Proxy Work Together

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

CA Options for Configuring TLS Proxy

The following CA options are supported for configuring TLS proxy:

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

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

Enterprise CA

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

Table 14: Enterprise CA: Benefits and Limitations

Benefits	Limitations
<ul style="list-style-type: none"> • Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates • The client trust-store need not be updated • Provides a single location for managing all certificates issued • Certificates can be revoked and tracked through your own CA 	<ul style="list-style-type: none"> • Maintenance creates an administrative overload. • Manual certificate deployment is required for TLS proxy • Out-of-band management is required for tracking the usage and expiry of certificates • Requires manual re-issuance of expired proxy certificates • If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated

Enterprise CA with SCEP

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. If your CA supports SCEP, you can configure it to automate the certificate management process.

Table 15: Enterprise CA with SCEP: Benefits and Limitations

Benefits	Limitations
<ul style="list-style-type: none"> • Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates • The client trust-store need not be updated • Provides a single location for managing all certificates issued • Certificates can be revoked and tracked through your own CA • Certificate deployment to TLS Proxy can be automated 	<ul style="list-style-type: none"> • Maintenance creates an administrative overload. • If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated • Offers limited visibility through Cisco vManage • Enterprise CA have limited support for SCEP

vManage as CA

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

Table 16: vManage as CA: Benefits and Limitations

Benefits	Limitations
<ul style="list-style-type: none"> • Certificate deployment to proxy devices is automated • Certificates are reissued and revalidated before they expire • Certificates can be monitored, tracked, and validated through Cisco vManage 	<ul style="list-style-type: none"> • Cisco vManage certificate needs to be pushed to the client trust store

vManage as Intermediate CA: Benefits and Limitations

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

Table 17: vManage as Intermediate CA: Benefits and Limitations

Benefits	Limitations
<ul style="list-style-type: none"> • Certificate deployment to proxy devices is automated • Certificates are reissued and revalidated before they expire • The risk associated with certificates being compromised is limited as compromised proxy certificates are revoked • Certificates can be monitored, tracked, and validated through Cisco vManage • No other certificates, besides your enterprise CA certificate, need to be pushed to your client trust-store 	<ul style="list-style-type: none"> • Requires manual deployment • Maintaining two CAs causes administrative overload • Cisco vManage certificate usage is tracked through the enterprise CA • Deployment can be complex if your network has multiple Cisco vManage controllers for clustering or redundancy

Supported Devices and Device Requirements

The following devices support the SSL/TLS Proxy feature.

Table 18: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Release 17.2.1r	<ul style="list-style-type: none"> • Cisco 4331 Integrated Services Router (ISR 4331) • Cisco 4351 Integrated Services Router (ISR 4351) • Cisco 4431 Integrated Services Router (ISR 4431) • Cisco 4451 Integrated Services Router (ISR 4451) • Cisco 4461 Integrated Services Router (ISR 4461) • Cisco CSR 1000v Cloud Services Router (CSR1000v)
Cisco IOS XE Release 17.3.2	<ul style="list-style-type: none"> • Cisco Catalyst 8300 Series Edge Platforms
Cisco IOS XE Release 17.4.1a	<ul style="list-style-type: none"> • Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8200 Series Edge Platforms

Minimum Device Requirements

- The device must have a minimum of 8 GB of DRAM.
- The device must have a minimum of 8 vCPUs.

Supported Cipher Suites

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

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_SEED_CBC_SHA
- TLS_DHE_RSA_WITH_SEED_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Prerequisites for TLS Proxy

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

Limitations and Restrictions

- The TLS Proxy feature only supports TLS versions 1.0, 1.1, and 1.2. TLS version 1.3 is not supported and is downgraded to TLS version 1.2.
- Only RSA and its variant cipher suites are supported. ECDSA based cipher suites are not supported.
- Certificate Revocation List (CRL) check is not supported for server certificate validation. However, you can enable OCSP from Advanced Settings in SSL Decryption policy.
- OCSP stapling is not supported and must be explicitly disabled on the browser for the TLS session to be established.
- For branch-to-branch and branch-to-data center traffic scenarios that support service nodes, the SSL decryption security policy must be applied in a way that prevents the SSL flow from being inspected on both the devices.
- IPv6 traffic is not supported.
- TLS session resumption, renegotiation and client certificate authentication are not supported.
- If TLS proxy crashes, it takes up to two minutes for it to be ready to serve as proxy for TLS flows again. During this time, depending upon your security settings, the flows are either bypassed or dropped.

Configure Cisco IOS XE SD-WAN Devices as TLS Proxy

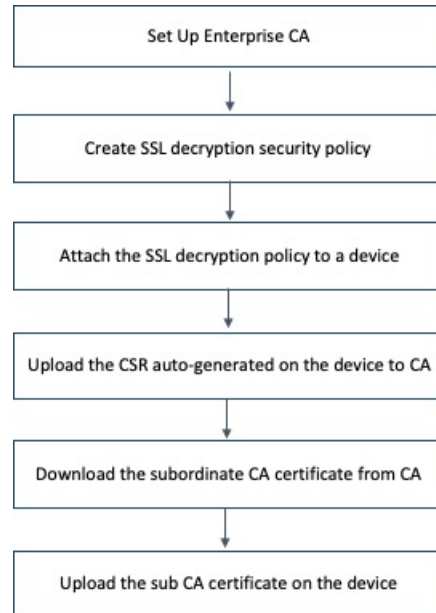
High-level Steps for Configuring a Device as TLS Proxy

1. Configure certificate authority (CA) for the TLS proxy: Enterprise CA, vManage as CA, or vManage as Intermediate CA.
2. The next step differs based on the CA option you configure. See the task flows in the following section for Enterprise CA, and vManage as CA and vManage as Intermediate CA.
3. Create and attach SSL decryption security policy to the device.

Task Flow: Set up TLS Proxy with Enterprise CA

If you configure Enterprise CA to enable TLS proxy on your devices, go through the following steps to complete the TLS proxy setup.

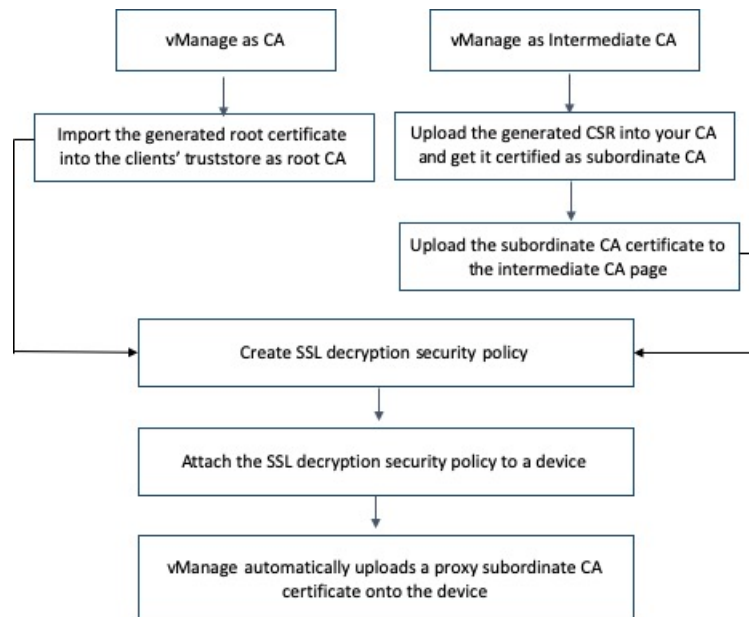
Figure 4: Use Enterprise CA to Configure TLS Proxy on a Device



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

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

Figure 5: Use vManage as CA or vManage as Intermediate CA to Configure TLS Proxy on a Device



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

Configure CA for TLS Proxy

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

Configure Enterprise CA

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

Prerequisites to Set up CA for SSL/TLS Proxy

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

Configure Enterprise CA

1. Download a CA certificate from your CA server in PEM or Base 64 format.
2. From the Cisco vManage menu, choose **Configuration > TLS/SSL Proxy**.
3. Choose **Enterprise CA**.
4. [Optional, but recommended] Check the Simple Certificate Enrollment Protocol (SCEP) check box.
 - a. Enter the SCEP server URL in the URL Base field.
 - b. [Optional] Enter the Challenge Password/Phrase if you have one configured.



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

5. To upload your PEM-encoded CA certificate, click **Select a file**.
OR
Paste the CA certificate in the Root Certificates box.
6. Verify that the fingerprint, which auto-populates after you upload the certificate, matches your CA.
7. Click **Save Certificate Authority**.



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

8. [Configure SSL Decryption](#)
9. [Apply a Security Policy to an XE SD-WAN Router](#)

10. [Upload a Subordinate CA Certificate to TLS Proxy, on page 129](#)

Configure Cisco vManage as CA

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

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

Prerequisites to Set up CA for SSL/TLS Proxy

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

1. From the Cisco vManage menu, choose **Configuration > TLS/SSL Proxy**.
2. Choose **vManage as CA**.



Note

Leave the Set vManage as Intermediate CA check box not checked if you want to set vManage as CA.

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



Note

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

8. Configure [Configure SSL Decryption](#) security policy.
9. [Configure SSL Decryption](#)
10. [Apply a Security Policy to an XE SD-WAN Router](#)

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

Configure Cisco vManage as Intermediate CA

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

When Cisco vManage is set as intermediate CA, your enterprise CA acts as the root CA and Cisco vManage is designated as the preferred intermediate CA to issue and manage subordinate CA certificates for a proxy

device. This option is suitable for enterprises that have their own internal CA but would like to use Cisco vManage to automate and manage certificate issuance and renewal.

1. From the Cisco vManage menu, choose **Configuration > TLS/SSL Proxy**.
2. Choose **vManage as CA**.
3. Check the **Set vManage as Intermediate CA** check box.
4. Upload the CA certificate using the **Select a file** option.
OR
Paste the content of the PEM-encoded CA certificate file in the Root Certificate text box.
5. Click **Next**.
6. Under the Generate CSR area, enter the requested details, and click **Generate CSR**.
The CSR field on the screen populates with the Certificate Signing Request (CSR).
7. Copy or download the CSR and upload it to the enterprise CA server to get it signed by the CA server as the subordinate CA certificate.

**Note**

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

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

**Note**

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

12. [Configure SSL Decryption](#)
13. [Apply a Security Policy to an XE SD-WAN Router](#)

When the SSL/TLS decryption security policy is attached to the device, Cisco vManage automatically issues a subordinate, proxy CA certificate and imports it on the device.

Configure SSL Decryption

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

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

For URL-based rules, note the following:

- A NAT direct internet access route is necessary to implement TLS/SSL decryption.
- You can set blocked list URLs to always be decrypted
- You can set allowed list URLs to never be decrypted.
- If a URL lookup to the cloud takes too long, the user can set one of the following:
 - Decrypt the traffic
 - Skip decryption for this traffic temporarily

To configure SSL decryption through a security policy, use the vManage security configuration wizard:

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

The New Decryption Rule window is displayed.

**Note**

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

10. Choose the order for the rule that you want to create.
11. In the **Name** field, enter the name of the rule.
12. You can choose to decrypt traffic based on source / destination which is similar to the firewall rules or applications which is similar to URL-Filtering rules.
 - If you choose Source / Destination, enter any of the following conditions:
 - Source VPNs
 - Source Networks
 - Source Ports
 - Destination VPNs
 - Destination Networks
 - Destination Port
 - Application/Application Family List
 - If you choose URLs, enter the following:
 - VPNs
 - TLS/SSL profile.
 - a. Enter a name for the profile.
 - b. Choose **Decrypt**, **No Decrypt** or **Pass Through**. Alternatively, you can choose multiple categories and set the action for all of them using the actions drop-down menu.
13. (Optional) To configure advanced settings such as server certificate checks, minimum TLS version, and so on, expand **Advanced Settings**



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

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

Field Name	Description	Options
Expired Certificate	Defines what the policy should do if the server certificate is expired	<ul style="list-style-type: none"> • Drop the traffic • Decrypt the traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted	<ul style="list-style-type: none"> • Drop the traffic • Decrypt the traffic

Field Name	Description	Options
Certificate Revocation Status	Defines whether Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate	Enabled or Disabled
Unknown Revocation Status	Defines what the policy should do, if the OCSP revocation status is <code>unknown</code>	<ul style="list-style-type: none"> • Drop the traffic • Decrypt the traffic

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

Field Name	Description	Options
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modulus	<ul style="list-style-type: none"> • 1024 bit RSA • 2048 bit RSA • 4096 bit RSA
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate in days.	
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support.	<ul style="list-style-type: none"> • TLS 1.0 • TLS 1.1 • TLS 1.2

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

Field Name	Description	Options
Unsupported Protocol Versions	Defines what the policy should do if an unsupported protocol version is detected.	<ul style="list-style-type: none"> • Drop the traffic • No Decrypt: The proxy does not decrypt this traffic.
Unsupported Cipher Suites	Defines what the policy should do if unsupported cipher suites are detected.	<ul style="list-style-type: none"> • Drop the traffic • No Decrypt: The proxy does not decrypt this traffic.
Failure Mode	Defines what the policy should do in the case of a failure.	<ul style="list-style-type: none"> • Close: Sets the mode as fail-close • Open: Sets the mode as fail-open.

Field Name	Description	Options
Certificate Bundle	Defines whether the policy should use the default CA certificate bundle or not	<p>You can choose or not choose this option. If you do not choose this option, the Custom Certificate Bundle option appears and you must upload a certificate by clicking Select a file.</p> <p>Note If you choose to use or update a custom certificate bundle for SSL decryption, ensure that the same certificate bundle is used across all devices in the network that have SSL decryption enabled.</p>

14. Click **Save TLS/SSL Decryption Policy**.
15. Click **Next**.
16. Enter Security Policy Name and Security Policy Description in the respective fields.
17. Click **Save Policy** to configure the Security policy.
18. To edit the existing SSL decryption policy, click **Custom Options** in the Security wizard.

Apply a Security Policy to an XE SD-WAN Router

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. If you are creating a new device template:
 - a. Click **Device**, and click **Create Template**.
 - b. From the Create Template drop-down menu, choose **From Feature Template**.
 - c. From the **Device Model** drop-down menu, choose one of the 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. Click **Device**, and click ... and click **Edit**.
 - b. Click **Additional Templates**. The screen scrolls to the Additional Templates section.
 - c. From the Policy drop-down menu, choose the name of a policy you have configured.
4. Click **Additional Templates** located directly beneath the Description field. The screen scrolls to the Additional Templates section.
 5. From the Security Policy drop-down menu, choose the name of the security policy you configured in the above procedure.
 6. Click **Create** (for a new template) or **Update** (for an existing template).

Upload a Subordinate CA Certificate to TLS Proxy



Note

This procedure is applicable only if you configure the Enterprise CA for TLS proxy.

Prerequisites to Generate a CSR from the TLS Proxy Device

1. [Configure Enterprise CA](#)
2. [Configure SSL Decryption](#)
3. [Apply a Security Policy to an XE SD-WAN Router](#)

Generate CSR and Upload Subordinate CA Certificate to TLS Proxy

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



Important

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

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

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

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

Verify Configuration

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

- **show sdwanrunning:** In Cisco vManage, run this command in **CLI mode** to verify if your configuration is applied.
- **show sdwan running-config:** In Cisco vManage, run this command by connecting to the device CLI through SSH.
- **show crypto pki status:** On your device CLI, run this command to verify that the PROXY-SIGNING-CA is present and configured correctly on the device.
- **show sslproxy statistics:** On your device CLI, run this command to view TLS proxy statistics.
- **show sslproxy status :** On your device CLI, run this command to verify whether TLS proxy was successfully configured and is enabled on Cisco vManage.

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

```
Configuration
-----
CA Cert Bundle           : /bootflash/vmanage-admin/sslProxyDefaultCAbundle.pem
CA TP Label              : PROXY-SIGNING-CA
Cert Lifetime            : 730
EC Key type              : P256
RSA Key Modulus          : 2048
Cert Revocation          : NONE
Expired Cert             : drop
Untrusted Cert           : drop
```

```

Unknown Status           : drop
Unsupported Protocol Ver  : drop
Unsupported Cipher Suites : drop
Failure Mode Action       : close
Min TLS Ver               : TLS Version 1.1

```

```

Status
-----

```

```

SSL Proxy Operational State : RUNNING
TCP Proxy Operational State : RUNNING
Clear Mode                  : FALSE

```

- **show platform hardware qfp active feature utd config:** On your device CLI, run this command to verify the UTD data plane configuration. For more information on this command, see the [Qualified Command Reference](#).
- **show sdwan running-configuration | section utd-tls-decrypt :** On your device CLI, run this command to verify the UTD data plane configuration.
- **show utd engine standard config:** On your device CLI, run this command to verify the UTD service plane configuration.
- **show utd engine standard status:** On your device CLI, run this command to verify the UTD service plane configuration.

Monitor TLS Proxy Performance

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

Monitor TLS Proxy

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

Monitor SSL Decryption Statistics

1. From the Cisco vManage menu, choose **Monitor > Network**.
2. Choose a device from the list of devices that displays.
3. Under the Security Monitoring pane, click **TLS/SSL Decryption** in the left pane.
4. The the right pane has the following options to choose from.
 - **Network Policy:** You can view the traffic information for an applied network policy.
 - **URL Policy:** You can view the traffic information of a URL policy.
 - **Time Range:** Choose to view the information for a specified time range (1h, 3h, 6h, and so on) or click **Custom** to define a time range.
5. Based on your choice, the information displays.

Additionally, from the Security Monitoring pane, you can also view information for other Security features such as Firewall, Intrusion Prevention, URL Filtering, and so on.

Revoke and Renew Certificates

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

Revoke Enterprise CA Certificate

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

Revoke and Renew Certificate

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



Note

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

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

Renew Certificate

1. From the Cisco vManage menu, choose **Configuration > Certificates**.
2. Click the **TLS Proxy**.
You will see a list of devices configured as CA.
3. Choose the device (configured as Enterprise CA) for which you want to revoke or revoke and renew the certificate.
4. Click **Renew Certificate**. A pop-up window opens.
5. Click **Yes** to continue with the renewal.
In the status column, the status of the certificate changes to **CSR_Generated**.
6. Click **Download CSR**.
A pop-up window opens. You can copy or download the CSR. Ensure that the certificate that you request is downloaded in PEM format.
7. On your CA server, request a certificate and upload or paste the CSR file you generated in the previous step.
8. Download the certificate issued by your CA in PEM format.



Important

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

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

9. Click **Upload Certificate**.
10. In the pop-up window that opens, upload or paste the PEM-encoded certificate that you generated from your CA server in step 9.
11. Click **Upload and Save**.

vManage as CA or vManage as Intermediate CA

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

1. From the Cisco vManage menu, choose **Configuration > Certificates**.
2. Click **TLS Proxy**.
You will see a list of devices configured as CA.

3. Choose the device.
4. Click **Revoke Certificate** or **Renew Certificate** to revoke or renew the certificate respectively.

Configure TLS/SSL Decryption Policy for Unified Security Policy

You can create a TLS/SSL Decryption policy specifically for use in a unified security policy. When created, the TLS/SSL Decryption policy is included in the advanced inspection profile and applied to the unified security policy for implementation on Cisco IOS XE SD-WAN devices.



Note Configuring a TLS/SSL Decryption policy is mandatory in a unified security policy, especially if you choose to use the TLS action as **Decrypt** while creating an advanced inspection profile.

To configure TLS/SSL Decryption for a unified security policy, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **TLS/SSL Decryption** in the left pane.
5. Click **Add TLS/SSL Decryption Policy**, and choose **Create New**.
6. Ensure that SSL Decryption is set to **Enabled**.
7. Click **Policy Mode** to enable the unified mode. This implies that you are creating a TLS/SSL Decryption policy for use in the unified security policy.
8. Enter a policy name in the **Policy Name** field.
9. (Optional) To configure advanced settings such as server certificate checks, minimum TLS version, and so on, expand **Advanced Settings**



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

- In **Server Certificate Checks**, configure the following:

Field Name	Description	Options
Expired Certificate	Defines what the policy should do if the server certificate has expired	<ul style="list-style-type: none"> • Drop the traffic by clicking Drop • Decrypt the traffic by clicking Decrypt

Field Name	Description	Options
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted	<ul style="list-style-type: none"> Drop the traffic by clicking Drop Decrypt the traffic by clicking Decrypt
Certificate Revocation Status	Defines whether Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate	Enabled or Disabled
Unknown Revocation Status	Defines what the policy should do, if the OCSP revocation status is unknown	<ul style="list-style-type: none"> Drop the traffic by clicking Drop Decrypt the traffic by clicking Decrypt

- In **Proxy Certificate Attributes**, configure the following:

Field Name	Description	Options
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modulus	<ul style="list-style-type: none"> 1024 bit RSA 2048 bit RSA 4096 bit RSA
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.	—
Minimum TLS Version Revocation Status	Sets the minimum version of TLS that the proxy should support.	<ul style="list-style-type: none"> TLS 1.0 TLS 1.1 TLS 1.2

- In **Unsupported Mode Checks**, configure the following:

Field Name	Description	Options
Unsupported Protocol Versions	Defines what the policy should do if an unsupported protocol version is detected.	<ul style="list-style-type: none"> Drop the traffic by clicking Drop Click No Decrypt so that the proxy does not decrypt this traffic.

Field Name	Description	Options
Unsupported Cipher Suites	Defines what the policy should do if unsupported cipher suites are detected.	<ul style="list-style-type: none"> • Drop the traffic by clicking Drop • Click No Decrypt so that the proxy does not decrypt this traffic.
Failure Mode	Defines what the policy should do in case of a failure.	<ul style="list-style-type: none"> • Close: Sets the mode as fail-close • Open: Sets the mode as fail-open.
Certificate Bundle	Defines whether the policy should use the default CA certificate bundle or not	You can choose or not choose this option. If you do not choose this option, the Custom Certificate Bundle option appears and you must upload a certificate by clicking Select a file .

10. Click **Save TLS/SSL Decryption Policy**.

Configure TLS/SSL Profile for Unified Security Policy

You can create a TLS/SSL profile specifically for use in a unified security policy. When created, the TLS/SSL profile is included in the advanced inspection profile and applied to the unified security policy for implementation on Cisco IOS XE SD-WAN devices.

To configure TLS/SSL Decryption for a unified security policy, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **TLS/SSL Profile** in the left pane.
5. Click **New TLS/SSL Profile**.
6. In **Profile Name**, enter the name of the profile.
7. Click **policy mode** to enable unified mode. This implies that you are creating a TLS/SSL profile for use in the unified security policy.
8. In the **Policy Name** field, enter the name of the policy.
9. Click **Decrypt**, **No Decrypt** or **Pass Through**. Alternatively, choose multiple categories and set the action for all of them using the **Actions** drop-down list.

10. Click **Save**.



CHAPTER 11

Cisco Umbrella Integration

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

- [Overview of Cisco SD-WAN Umbrella Integration, on page 139](#)
- [Restrictions for Umbrella Integration, on page 141](#)
- [Prerequisites for Umbrella Integration, on page 142](#)
- [Configure Umbrella API Token, on page 142](#)
- [Configure Cisco Umbrella Registration, on page 143](#)
- [Define Domain Lists, on page 143](#)
- [Configure Umbrella DNS Policy Using Cisco vManage, on page 144](#)
- [Attach DNS Umbrella Policy to Device Template, on page 145](#)
- [Umbrella Integration Using CLI, on page 145](#)
- [DNS Security Policy Configuration, on page 155](#)
- [Monitor Umbrella Feature, on page 157](#)

Overview of Cisco SD-WAN Umbrella Integration

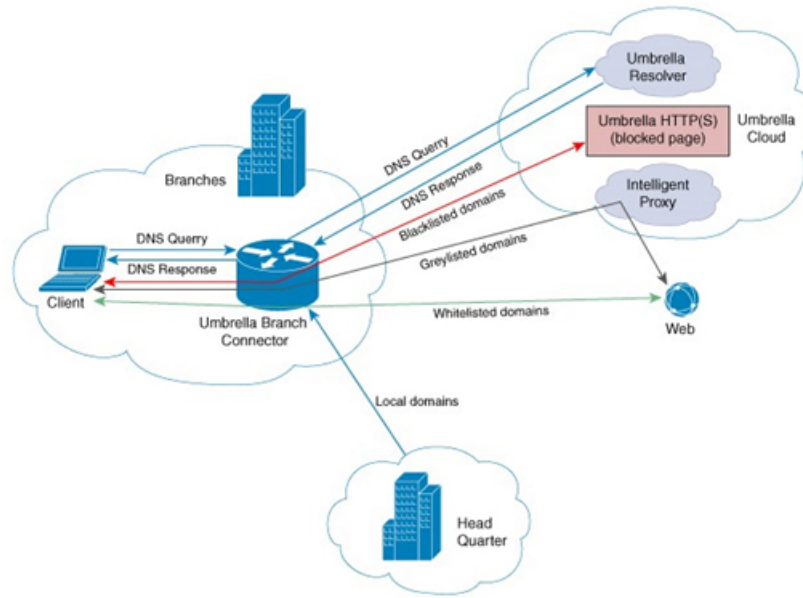
The Cisco SD-WAN Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through the device. When a host initiates the traffic and sends a DNS query, the Umbrella Connector in the device intercepts and inspects the DNS query. If the 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 6: Umbrella Cloud



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

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

Handling HTTP and HTTPs Traffic

With 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 7: 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.
- Data-policy based NAT and Umbrella DNS redirect interoperability is not supported. If NAT for internet bound traffic is configured through a data policy instead of a default NAT route in service VPN, for Umbrella DNS redirection, you must create a rule to match the DNS request and then set action as umbrella redirect. The data policy rule created for DNS redirect must be configured before the NAT rule in a sequence.

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. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options** to configure the Umbrella API.
3. Choose **Umbrella API Token**.
4. Enter token number in the **Umbrella Token** field.



Note Must be exactly 40 hexadecimal.

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

Configure Cisco Umbrella Registration

Table 19: Feature History

Feature Name	Release Information	Description
Auto-registration for Cisco Umbrella Cloud Services	Cisco IOS XE Release 17.2.1r	This feature adds the ability to register devices to Cisco Umbrella using the Smart Account credentials to automatically retrieve Umbrella credentials (organization ID, registration key, and secret). This offers a more automatic alternative to manually copying a registration token from Umbrella.

Use this procedure to configure Cisco Umbrella registration globally for all devices. The procedure retrieves the Umbrella registration parameters automatically.

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

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options** and choose **Umbrella Registration**.
3. In the **Manage Umbrella Registration** dialog box, use one of the following methods to register devices to Umbrella. The registration details are used globally.

- Cisco Umbrella Registration Key and Secret

- a. Click the **Get Keys** to retrieve Umbrella registration parameters automatically: Organization ID, Registration Key, and Secret.



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

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

- c. Click **Save Changes**.

- Cisco Umbrella Registration Token

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

Define Domain Lists

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Custom Options**, and choose **Lists** from the drop-down menu.

3. Choose **Domain** in the left pane.
4. Click **New Domain List** to create a new domain list or click the domain name, and click the pencil icon on the right side for an existing list.
5. Enter the **Domain List Name**, **Add Domain**, and click **Add** to create the list.

Configure Umbrella DNS Policy Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration > Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** wizard, click **Direct Internet Access**.
4. Click **Proceed**.
5. Click **Next** until you reach the **DNS Security** page.
6. From the **Add DNS Security Policy** drop-down list, choose one of the following:
 - **Create New:** A **DNS Security - Policy Rule Configuration** wizard is displayed. Continue to Step 7.
 - **Copy from Existing:** Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
7. If you are creating a new policy using the **Create New** option, the **DNS Security - Policy Rule Configuration** wizard is displayed.
8. Enter a policy name in the **Policy Name** field.
9. The **Umbrella Registration Status** displays the status of the API Token configuration.
10. Click **Manage Umbrella Registration** to add a token, if you have not added one already.
11. Click **Match All VPN** to keep the same configuration for all the available VPNs and continue with Step 13.

Or click **Custom VPN Configuration** if you need to add target service VPNs to your policy. A Target VPNs window appears, and continue with Step 12.
12. To add target service VPNs, click **Target VPNs** at the top of the window.
13. Click **Save Changes** to add the VPN.
14. From the **Local Domain Bypass List** drop-down list, choose the domain bypass.
15. Configure **DNS Server IP** from the following options:
 - **Umbrella Default**
 - **Custom DNS**
16. Click **Advanced** to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
17. Click **Save DNS Security Policy**.

The **Configuration > Security** window is displayed, and the DNS policy list table includes the newly created DNS Security Policy.

Attach DNS Umbrella Policy to Device Template

1. From the Cisco vManage menu, choose **Configuration > Templates** screen.
2. Click **Device**, and choose **From Feature Template** from the Create Template drop-down menu.
3. From the Device Model drop-down menu, choose a device.
4. Click **Additional Templates**. The screen scrolls to the **Additional Templates** section.
5. From the Security Policy drop-down menu, choose the name of the Umbrella DNS Security Policy you configured in the above procedure.
6. Click **Create** to apply the Umbrella policy to a device template.

Umbrella Integration Using CLI

Configure the Umbrella Connector

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

To configure Umbrella Connector:

- Get the API token from the Umbrella portal.
- Define VRFs and each VRF can 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 Successfull 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:BB0D: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
DNSCrypt: 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
DNSCrypt: 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 DNSCrypt is disabled:

```

Device# show umbrella config
Umbrella Configuration
=====
Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
  1. 208.67.220.220
  2. 208.67.222.222
  3. 2620:119:53::53
  4. 2620:119:35::35

```

```

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

```

Display Umbrella Registration Details

The following example displays the device registration information:

```

Device# show sdwan umbrella device-registration
Device registration details
VRF      Tag      Status      Device-id29
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

```

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. *.amazon.com
03. *.salesforce.com

```

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
  DNSCrypt statistics:
    bypass pkt: 0
    clear sent: 0
    enc sent: 0
    clear rcvd: 0
    dec rcvd: 0
    pa err: 0
    enc lib err: 0
```

```
padding err: 0
nonce err: 0
flow bypass: 0
disabled: 0
flow not enc: 0
DCA statistics:
dca match success: 0
dca match failure: 0
```

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

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

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

```
Device# show platform hardware qfp active feature umbrella datapath runtime
udpflow_ageout: 5
ipv4_count: 2
ipv6_count: 2
ipv4_index: 0
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

CLI Command	Possible Completions	Description and possible input values
policy lists local-domain-list <name>		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

security umbrella		Configure Umbrella service related security properties.
	api-key	Config umbrella api-key. The value ranges from 1 to 64 characters.
	dnscrypt	Enable DNSCrypt while redirecting DNS requests to Umbrella.
	orgid	Config umbrella org id
	secret	Config umbrella secret. The value can be [0 6].
	token	Umbrella service registration token. The value ranges from 1 to 64 characters.

CLI Command	Possible Completions	Description and possible input values
vpn <number, range>	dns-redirect match-local-domain-to-bypass	List of domain name regular expression patterns
	dns-redirect umbrella	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
    dnscrypt
  !
exit
!
vpn matchAllVpn
  dns-redirect umbrella match-local-domain-to-bypass

```

DNS-Redirection with NAT

This example displays the centralized policy configuration for NAT with DNS redirection.

```

policy
data-policy DP1
  vpn-list VPN1
    sequence 1
      match
        dns request
      !
      action accept
        redirect-dns umbrella
      !
    !
  !

```

```
sequence 2
  action accept
  nat use-vpn 0
  !
  !
  default-action drop
  !
```

Monitor Umbrella Feature

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

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

1. From the Cisco vManage menu, choose **Monitor > Network**.
2. To choose a device, click the one of the devices listed under the Hostname column.
3. Under Security Monitoring, click **Umbrella DNS Re-direct** in the left pane. **Umbrella DNS Re-direct** displays the number of packets that are redirected to configured DNS server.
4. Click **Local Domain Bypass** to view the number of packets that are bypassed from DNS server.



CHAPTER 12

Integrate Your Devices With Secure Internet Gateways

Table 20: Feature History

Feature	Release Information	Description
Enable Layer 7 Health Check (Manual Tunnels)	Cisco IOS XE Release 17.2.1r Cisco SD-WAN Release 19.3.1	This features helps to maintain tunnel health by providing ability to load balance or failover tunnels. This feature is supported on Cisco IOS XE SD-WAN devices from Cisco IOS XE Release 17.2.1r and later releases.
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco IOS XE Release 17.4.1a Cisco vManage Release 20.4.1	<p>This feature allows you to use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. The application traffic is steered to a SIG based on a defined data policy and other match criteria.</p> <p>This feature also allows you to configure weights for multiple GRE/IPSEC tunnels for distribution of traffic among multiple tunnels. The traffic distribution enables you to balance the load among the tunnels. You can also configure the weights to achieve Equal-cost multi-path (ECMP) routing.</p>

Feature	Release Information	Description
Support for Zscaler Automatic Provisioning	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	This feature automates the provisioning of tunnels from Cisco SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose Zscaler in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning.

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

In Cisco IOS XE Release 17.2.1r and later, Cisco SD-WAN supports automatically tunneling to Cisco Umbrella as a SIG. In Cisco vManage Release 20.5.1, you can also automatically tunnel to Zscaler.

The Enable Layer 7 Health Check feature helps in maintaining tunnel health by providing tunnels the ability to failover. To use this feature, you must configure a tracker when creating your tunnel. The Direct Internet Access (DIA) traffic ingressing on SD-WAN service VPNs is tunneled to the Secure Internet Gateways (SIG) for securing enterprise traffic. All LAN/WIFI enabled enterprise client's traffic, based on routing, is forwarded to the SIG. For information on using the `tracker` command, see the [Cisco SD-WAN Command Reference Guide](#).

From Cisco vManage Release 20.4.1, all SIG workflow is consolidated under the Secure Internet Gateway feature template. You can use this template for both Cisco Umbrella and Third Party SIG providers.

- [Options to Integrate Your Devices with Secure Internet Gateways, on page 160](#)
- [Configure Tunnels, on page 162](#)
- [Troubleshoot Integrating Your Devices With Secure Internet Gateways, on page 170](#)

Options to Integrate Your Devices with Secure Internet Gateways

To integrate devices with a SIG, do one of the following:

- Automatic tunneling
- Manual tunneling

Automatic Tunnels

To use automatic tunneling, do the following:

1. Complete any prerequisites for the SIG. For more information, see [Prerequisites, on page 162](#).
2. Specify the details for the tunnel to the SIG by using the Cisco Security Internet Gateway (SIG) feature template.

In the template, define the parameters for the tunnels such as the interface name, the source interface, the SIG provider, and so on.
3. Specify the credentials of the SIG by using the SIG Credentials feature template.
4. Edit the Cisco VPN feature template that provides the service route for the devices to the internet.
5. Add a service route to the SIG in the Cisco VPN feature template.
6. Add feature templates to the device templates of the devices that should route traffic to the SIG.
7. Attach the device templates to the devices.

When you attach the device template, the device sets up an IPsec tunnel to the SIG and redirects traffic to it.

Using Cisco Umbrella

Use Cisco Umbrella as a SIG by choosing **Umbrella** as the SIG provider in the Cisco Security Internet Gateway (SIG) feature template, and then define IPSEC tunnels, and tunnel parameters. Use the SIG credentials feature template to specify the Umbrella Organization ID, Registration Key, and Secret.

For information on configuring automatic tunneling, see [Configure Automatic Tunnels Using Cisco vManage, on page 162](#).

Using Zscaler

In Cisco vManage Release 20.5.1, you can automatically tunnel to Zscaler Internet Access (ZIA) Public Service Edges using the Cisco Security Internet Gateway (SIG) feature template. ZIA Public Service Edges are secure internet gateways that can inspect and secure traffic from Cisco SD-WAN devices. The devices use Zscaler APIs to automatically create tunnels by doing the following:

1. Establish an authenticated session with ZIA.
2. Based on the IP address of the device, obtain a list of nearby data centres.
3. Provision the VPN credentials and location using ZIA APIs.
4. Using the VPN credentials and location, create an IPsec tunnel between the ZIA Public Service Edges and the device.

For information on configuring automatic tunneling, see [Configure Automatic Tunnels Using Cisco vManage, on page 162](#).

Manual Tunnels

With manual tunnels, you configure a GRE or IPSec using a SIG template tunnel to support any third-party SIG provider. Specify a tunnel destination to enable traffic flow. For more information on configuring manual tunnels, see [Configure Manual Tunnels Using Cisco vManage, on page 167](#).

From Cisco vManage Release 20.5.1, you can create tunnels to any SIG provider using the Cisco Secure Internet Gateway (SIG) feature template. Use the **generic** option in the feature template to provision IPSec or GRE tunnels to any SIG. When you create tunnels using this option, Cisco vManage does not automatically create the tunnel. To create the tunnel, manually configure the details of the tunnel for the SIG.

Configure Tunnels

Configure Automatic Tunnels Using Cisco vManage

Prerequisites

To configure automatic tunneling to a SIG, complete the following requisites:

- Cisco Umbrella: To configure Cisco vManage to connect Cisco Umbrella, you can do one of the following
 - If you want Cisco vManage to automatically get the API keys, specify Smart Account credentials in **Administration > Settings > Smart Account Credentials**. Your Cisco Smart Account is the account you use to log in to the Cisco Smart Software Manager (CSSM) portal. For more information, see [Information About Smart Licensing](#).
 - If you want to manually specify the API keys, generate **Umbrella Management** API keys as described [here](#).

Create SIG Feature Template

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature**.
3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under VPN, click **Cisco Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.
This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
This field is mandatory, and it can contain any characters and spaces.
8. In the Configuration pane, as the SIG Provider, choose **Umbrella** or **Zscaler**, or **Generic** or **Third Party** based on the SIG provider.

You can only choose Zscaler from Cisco vManage Release 20.5.1 and later releases.

9. For Cisco vManage Release 20.4.1 and earlier releases, click **Add Tunnel**.

10. Depending on your type of tunnel, do one of the following:

• **Cisco Umbrella or Zscaler**

Under Basic Settings, enter the following:

- a. In the **Interface Name** field, enter the name of your interface.
- b. In the **Description** field, enter a description of your interface.
- c. By default, the **Tracker** field is enabled to allow for load balancing and failing over the tunnel. If required, you can disable the tracker.
- d. In the **Tunnel Source Interface** field, enter the name of the source interface of the tunnel.
This interface should be the egress interface and is typically the Internet-facing interface.
- e. Choose a Data-Center.
- f. Click **Add**.

• **Generic or Third Party**



Note In Cisco vManage Release 20.5.1, the **Third Party** field is now called **Generic**

- a. In the **Tunnel Type** field, choose **ipsec** or **gre**.
- b. In the **Interface Name** field, enter the name of your interface.
- c. In the **Description** field, enter a description of your interface.
- d. In the **Source Type** field, choose **INTERFACE** or **IP**.
 - **INTERFACE**: enter the **Tunnel Source Interface** and **Tunnel Destination IP Address/FQDN(Ipsec)**.
 - **IP**: enter the **Tunnel Source IP Address, IPv4 Address** and **Tunnel Destination IP Address/FQDN**.
- e. If you are using an IPSec tunnel, also specify the **Preshared Key**.
- f. In the **Tunnel Source Interface** field, enter the name of the source interface of the tunnel.
This interface should be the egress interface and is typically the Internet-facing interface.
- g. Choose a Data-Center.
- h. Click **Add**.

11. (Optional) You can also add additional tunnels to act as a backup or secondary tunnel.

From Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, you can add up to eight tunnels.

12. To add the tunnel, click **Add**.

13. Depending on the tunnels you created, you can set the tunnels as Active and Backup in the High Availability pane. You can do the following:
 - a. For the Active tunnel, choose a tunnel.
 From Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, you can enter a weight (weight range 1-255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase your network bandwidth. If you enter the same weights, you can achieve Equal-cost multi-path routing (ECMP) load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel gets more priority for the flow of traffic.
 For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic will be load-balanced across both active tunnels in a 10:20 ratio.
 - b. Likewise, for the Backup tunnel, choose a tunnel as a secondary tunnel and then enter a Backup weight. Otherwise, choose **None**. If you choose **None**, there will be no backup tunnel to your SIG.
 You can create a maximum of four active and backup tunnel pairs.
14. (Optional) When using Umbrella or Zscaler as the SIG provider, the edge devices automatically identifies the closest data center to the device. To ensure that traffic is routed through specific data center, you can choose the primary and secondary data centers under advanced settings by doing the following:
 - a. For the **Primary Data-Center** field, choose **Global** from the drop-down list.
 - b. Choose the SIG provider data center through which to route traffic.
 - c. For the **Secondary Data-Center** field, choose **Global** from the drop-down list.
 - d. Choose the SIG provider data center through which to route traffic.
15. Click **Save**.

Create SIG Credentials Template

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature**.
3. Click **Add Template**.
4. Choose a device.
5. Under Other Templates, click **Cisco SIG Credentials**.
6. Depending on your SIG Provider, do one of the following:
 - Cisco Umbrella: under the Basic Details section, you can either automatically get the keys or manually specify the keys:
 - To automatically get the keys, click **Get Keys** to get the Organization ID, Registration Key, and Secret.



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

- To manually specify the keys, enter values for the **Organization ID**, **Registration Key**, and **Secret**. You can generate these values in your Umbrella account as described [here](#).



Note You must specify Umbrella Management API details in these fields.

7. Click **Save**.

Redirect Traffic to a SIG

You can redirect traffic to a SIG in two ways:

- Using Data Policy. For more information, see [Action Parameters](#) in the Policies Configuration Guide.
- Using the Service route to SIG. For more information, see [Modify Service VPN Template, on page 165](#)

Modify Service VPN Template

To ensure that the device connects to the SIG, you must modify the Cisco VPN template to include a service route to the SIG.

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature**.
3. For the Cisco VPN template of the device, click **Edit**.
4. Click **IPv4 Route**.
5. Click the delete icon on any existing IPv4 route to the internet.
6. Click **Service Route**.
7. Click **New Service Route**.
8. Enter a Prefix (for example, 10.0.0.0/8).
9. For the service route, ensure that **SIG** is chosen.
10. Click **Add**.
11. Click **Update**.

Create the SIG Device Template

To create a device template:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**, and click the **Create Template** drop-down menu, and choose **From Feature Template**.
3. From the **Device Model** drop-down menu, choose the type of device for which you are creating the template. Cisco vManage displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is chosen by default.
4. In the **Template Name** field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
5. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
6. Click **Transport & Management VPN**.
7. Under **Additional Cisco VPN 0 Templates**, click **Cisco Secure Internet Gateway**.
8. Click the **Cisco Secure Internet Gateway** drop-down menu.
9. Choose the template that you previously created.
10. Click **Additional Templates** or scroll down to the Additional Templates section.
11. Click the **Cisco SIG Credentials** drop-down menu.
12. Choose the template that you previously created.
13. Click **Create**. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Attach the SIG Template to Devices

To attach one or more devices to the device template:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device**, and choose the template that you created.
3. For the desired template, click ... and click **Attach Devices**.

The Attach Devices dialog box displays.

4. In the **Available Devices** column, choose a group and search for one or more devices, choose a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the **Selected Devices** column.
6. Click **Attach**.
7. If the template contains variables, enter the missing variable values for each device in one of the following ways:

- Enter the values manually for each device either in the table column or by clicking ... in the row and clicking **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
- Click **Import File** to upload a CSV file that lists all the variables and defines each variable value for each device.

8. Click **Update**.

Configure Manual Tunnels Using Cisco vManage

This section describes how to configure manual tunnels.

From Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1 all SIG related workflows for Automatic and Manual Tunnels have been consolidated into the SIG template.

If you are on Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, and onwards, we recommend configuring manual tunnels for GRE and IPSEC using the SIG template. See [Configuring Manual Tunnels to an SIG, on page 167](#).

If you are on a release-version prior to Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, see [Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage, on page 169](#)



Note

In release Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, the Layer 7 Health Check feature is only available if you use VPN Interface GRE/IPSEC templates, and not with SIG Templates for Umbrella or Third Party.

Configuring Manual Tunnels to an SIG

This section describes how to manually create a GRE or IPSEC tunnel from Cisco vManage to a third party service provider. Unlike automatic tunnels, configuring manual tunnels requires you to specify a tunnel destination to bring up the tunnels.

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature**.
3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under VPN, click **Cisco Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the feature template.
This field is mandatory, and it can contain any characters and spaces.
8. In the Configuration pane, choose **Third party** or **Generic**



Note In Cisco vManage Release 20.5.1, the **Third Party** field is now called **Generic**

9. Click **Add Tunnel**.

10. Under Basic Settings, enter the following:

- a. Choose a Tunnel type. Depending on the type of tunnel you choose, the corresponding fields display.
- b. In the **Interface Name** field, enter the name of your interface.
- c. Choose a Source Type.

Based on your choice the corresponding fields display:

- If you chose the Source Type as **Interface**, you enter the name of the source interface. This interface should be the egress interface and is typically the Internet-facing interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name.
 - If you chose the Source Type as **IP**, you enter the IP address of the tunnel source. In doing this, additional fields **IPv4 address** and **Tunnel Route-via Interface** display where you enter the tunnel interface's IP address and egress interface name.
- d. In the **Tunnel Destination IP Address/FQDN(Ipsec)** field, enter an IP address for the third-party destination tunnel.

11. Click **Add**.

Depending on the tunnels you created, the tunnel pairs (Active and Backup) display in the High Availability pane. You can do the following:

- a. For the Active tunnel, choose a tunnel. You can enter a weight (weight range 1-255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase your network bandwidth. If you enter the same weights, you can achieve Equal-cost multi-path routing (ECMP) load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel gets more priority for the flow of traffic.

For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic will be load-balanced across both active tunnels in a 10:20 ratio.

- b. Likewise, for the Backup tunnel, choose a tunnel as a secondary tunnel and then enter a Backup weight. Otherwise, click **None**. If you click **None**, there will be no backup tunnel to your SIG.

Likewise, for the Backup tunnel, choose a tunnel as a secondary tunnel and then enter a Backup weight. Otherwise, click **None**. If you click **None**, there will be no backup tunnel to your SIG.

You can create a maximum of four active and backup tunnel pairs.

12. Click **Save**.

Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage

Table 21: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco IOS XE Release 17.2.1r	This feature lets you manually configure a GRE tunnel by using the Cisco VPN Interface GRE template or an IPSec tunnel by using the Cisco VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.

Configure a GRE Tunnel from Cisco vManage

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

- Perform these actions to create a GRE template:
 - From the Cisco vManage menu, choose **Configuration > Templates**.
 - Click **Feature**, and then click **Add Template**.
 - Choose the type of device for which you are creating the template.
 - Choose the Cisco VPN Interface GRE template from the group of VPN templates.
 - In **Basic Configuration**, configure parameters as desired and then click **Save**.
- Perform these actions to create a GRE route:
 - Click **Feature**, and then click **Add Template**.
 - Choose the type of device for which you are creating the template.
 - Choose the Cisco VPN template in the group of VPN templates.
 - Click **GRE Route**.
 - Click **New GRE Route**.
 - Configure parameters as desired, and then click **Add**.
- Perform these actions to configure a device template for the GRE interface.
 - Click **Device**, and then click **...** and click **Edit** for the device template that you want to configure.
 - Click **Transport & Management VPN**.
 - From the Additional Cisco VPN 0 Templates list, choose the Cisco VPN Interface GRE template.
 - From the Cisco VPN Interface GRE drop-down menu, click **Create Template**.
 - Configure the templates as desired, and then click **Save**.

Configure an IPsec Tunnel from Cisco vManage

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

1. Perform these actions to create an IPsec template:
 - a. From the Cisco vManage menu, choose **Configuration > Templates**.
 - b. Click **Feature**, and click **Add Template**.
 - c. Choose the type of device for which you are creating the template.
 - d. Choose the Cisco VPN Interface IPsec template from the group of VPN templates.
 - e. In **Basic Configuration**, configure parameters as desired,
 - f. In **Advanced**, specify a name for your **Tracker**.
 - g. Click **Save**.
2. Perform these actions to create an IPSec route:
 - a. Click **Feature**, and, click **Add Template**.
 - b. Choose the type of device for which you are creating the template.
 - c. Choose the Cisco VPN template in the group of VPN templates.
 - d. Click **IPSEC Route**.
 - e. Click **New IPSEC Route**.
 - f. Configure parameters as desired, and then click **Add**.
3. Perform these actions to configure a device template for the IPsec interface.
 - a. Click **Device**, and click ... and choose **Edit** for the device template that you want to configure.
 - b. Click **Transport & Management VPN**.
 - c. From the Additional Cisco VPN 0 Templates list, choose the Cisco VPN Interface IPsec template.
 - d. From the Cisco VPN Interface IPsec drop-down menu, click **Create Template**.
 - e. Configure the templates as desired, and then click **Save**.

Troubleshoot Integrating Your Devices With Secure Internet Gateways

This section describes how to troubleshoot integrating your devices with Secure Internet Gateways.

After Upgrading Cisco vManage Tunnels Fail

After upgrading from Cisco vManage Release 20.3.1 to Cisco vManage Release 20.3.2, you may see failures when connecting from your devices to SIG services or when connecting standard IPSec tunnels to cloud security services.

Affected Feature Templates

- Cisco Secure Internet Gateway (SIG)
- Cisco VPN Interface IPSec (WAN)
- Cisco VPN Interface GRE

Description

By default, a tunnel created using the SIG template pushes the **tunnel vrf multiplexing** command. For VPN Interface IPSec templates, from the **Application** drop-down list, if you choose **Secure Internet Gateway**, the command is pushed. However, after you upgrade to Cisco vManage Release 20.3.2, your feature templates may remove the **tunnel vrf multiplexing** configuration. This causes your feature templates to fail when connecting to SIG services or other external services such as cloud security services.

Workaround

Depending on which feature template you want to update, do one of the following:

Cisco VPN Interface Feature Templates

1. In Cisco vManage, edit the template.
2. From the **Application** drop-down menu, choose **Secure Internet Gateway**.
3. Save the template.

All Affected Feature Templates

You can do one of the following:

- Manually add **tunnel vrf multiplexing** to the tunnel configuration using a CLI add-on feature template.
- In Cisco vManage, edit the existing template as follows:
 1. Modify a field, such as the description, that does not affect the configuration.
 2. Save the template.
 3. Push the template to the device.

Verification

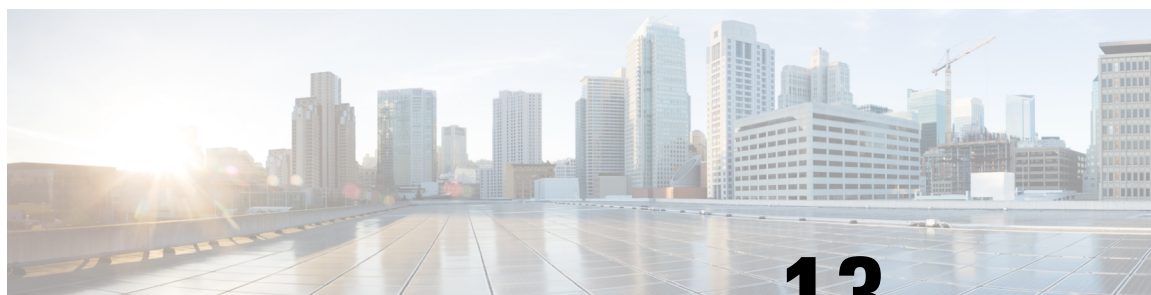
You can run the following command to verify that **tunnel vrf multiplexing** was added to your templates:

```
show sdwan running-config interface tunnelNumber
```

Example:

```
Device#sh sdwan running-config interface | begin Tunnel100001
interface Tunnel100001
```

```
no shutdown
ip unnumbered GigabitEthernet1
ip mtu 1400
tunnel source GigabitEthernet1
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing
exit
```



CHAPTER 13

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.

- [Identify the Recommended Security Virtual Image Version, on page 173](#)
- [Upload the Cisco Security Virtual Image to Cisco vManage, on page 174](#)
- [Upgrade a Security Virtual Image, on page 174](#)

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 device. To check this using Cisco vManage:

Step 1 From the Cisco vManage menu, choose **Monitor > Network**.

Step 2 Choose **WAN – Edge**.

Step 3 Choose the device that will run the SVI.

The System Status page displays.

Step 4 Scroll to the end of the device menu, and click **Real Time**.

The System Information page displays.

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

Step 6 The image name is displayed in the **Recommended Version** column. It should match the available SVI for your router from the Cisco downloads website.

Upload the Cisco Security Virtual Image to Cisco 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.

When a security policy is removed from Cisco IOS XE SD-WAN devices, the Virtual Image or Snort engine is also removed from the devices.

-
- Step 1** From the Software Download page for your router, locate the image **UTD Engine for IOS XE SD-WAN**.
 - Step 2** Click **download** to download the image file.
 - Step 3** From the Cisco vManage menu, choose **Maintenance > Software Repository**
 - Step 4** Choose **Virtual Images**.
 - Step 5** Click **Upload Virtual Image**, and choose 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.
 - 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 Cisco vManage menu, choose **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** From the Cisco vManage menu, choose **Maintenance > Software Upgrade**. The WAN Edge Software upgrade page displays.
 - Step 4** Choose the devices you want to upgrade, and check the check boxes in the leftmost column. When you have chosen one or more devices, a row of options display, as well as the number of rows you chose.
 - Step 5** When you are satisfied with your choices, choose **Upgrade Virtual Image** from the options menu. The Virtual Image Upgrade dialog box displays.
 - Step 6** For each device you have chosen, choose the correct upgrade version from the **Upgrade to Version** drop-down menu.

Step 7

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



CHAPTER 14

IPsec Pairwise Keys

Table 22: 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 you to create and install private pairwise IPsec session keys for secure communication between an IPsec device and its peers.

The IPsec pairwise keys feature implements controller-based key exchange protocol between a 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. The network devices, in turn, communicate with each other through a secure data plane.

A pair of IPsec session keys (one encryption key and one decryption key) are configured for each pair of local and remote transport locations (TLOC).

- [Supported Platforms, on page 177](#)
- [Pairwise Keys, on page 178](#)
- [IPsec Security Association Rekey, on page 178](#)
- [Configure IPsec Pairwise Keys, on page 178](#)

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. You use a controller to distribute keying material and policies between network devices. The devices generate private pairwise keys with each other.

IPsec devices share public keys from the Diffie-Hellman (DH) algorithm with the controllers. The controllers relay the DH public keys to authorized peers of the IPsec device as defined by the centralized policy.

Network devices create and install private pairwise IPsec session keys to secure communication with their peers.

IPsec Security Association Rekey

Every rekeying IPsec device generates a new Diffie-Hellman (DH) pair and 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 key and the DH public key 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 to the existing security association, and subsequently, to new security associations.

During a simultaneous rekey, up to four pairs of IPsec Security Associations (SAs) can be temporarily created. These four pairs converge on a single rekey of a device.

An IPsec device can initiate a rekey due to reasons such as the local time or a volume-based policy, or the counter result of a cipher counter mode initialization vector nearing completion.

When you configure a rekey on a local inbound security association, it triggers a peer outbound and inbound security association rekey. The local outbound security association rekey is initiated after the IPsec device receives the first packet with the new Security Parameter Index (SPI) from a peer.

**Note**

- A pairwise-key device can form IPsec sessions with both pairwise and nonpairwise devices.
- The rekeying process requires higher control plane CPU usage, resulting in lower session scaling.

Configure IPSec Pairwise Keys

Configure IPsec Pairwise Keys Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature**, and click **Add Template**.
3. From the **Device Model** drop-down menu, choose the type of device for which you are creating the template.
4. From **Basic Information**, click **Cisco Security** feature template.

5. From **Basic Configuration**, click **On** or **Off** from the **IPsec pairwise-keying** field.
6. Alternatively, enter the pairwise key specific to the device in the **Enter Key** field.
7. Click **Save**.

Configure Pairwise Keys and Enable Rekeying on the CLI

A pair of IPsec session keys is configured for each pair of local and remote transport locations.

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

You must reboot the Cisco IOS XE SD-WAN device for the private-key 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 a Cisco IOS XE SD-WAN Device

Use the following command to verify the outbound connections for pairwise keys:

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

				REMOTE						SA	PKEY	NONCE	PKEY	
SS	E-KEY	AH		SOURCE IP	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 the inbound connections on IPsec pairwise keys:

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

Verify IPsec Pairwise Keys on a Cisco IOS XE SD-WAN Device

SOURCE													
DEST		LOCAL		LOCAL		REMOTE		REMOTE					
SA	PKEY	NONCE	PKEY	SS	D-KEY	AH							
		SOURCE IP					PORT			DEST IP			
	PORT	TLOC ADDRESS			TLOC COLOR		TLOC ADDRESS			TLOC COLOR		PWK-SPI	
INDEX	ID	HASH	HASH	HASH	HASH	AUTH							
<hr/>													
192.168.90.3							12346		10.168.11.3				
12346		10.1.0.2		lte			10.1.0.1			privatel		000000	
2	1	5605	70C7	17B0	F5A5	true							
192.168.92.6							12346		10.168.11.3				
12346		10.1.0.2		lte			10.1.0.6			default		00100B	
52	1	5605	70C7	CCC2	C9E1	true							
192.168.90.3							12346		10.168.12.3				
12346		10.1.0.2		blue			10.1.0.1			privatel		000000	
5	1	B9F9	5C75	17B0	F5A5	true							
192.168.92.6							12346		10.168.12.3				
12346		10.1.0.2		blue			10.1.0.6			default		00100B	
55	1	B9F9	5C75	A0F8	7B6B	true							

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

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

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	192.168.92.6	
			12346	0x312b84f0	0x00000115/0x00000114			
			0x0000000031fbfa80/0x0000000031fbd520					
6661	131	36	10.168.12.3			12346	192.168.92.6	
			12346	0x312b9990	0x0000b001/0x0000a001			
			0x0000000031fbe380/0x0000000031fbc9a0					
7429	117	6	10.168.11.3			12346	192.168.92.6	
			12346	0x312b9300	0x0000b001/0x0000a001			
			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 a Cisco IOS XE SD-WAN device:

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 IOS XE SD-WAN Devices

Use the following **debug** commands for debugging issues related to IPsec pairwise keys:

```
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 15

Configure Single Sign-On

This chapter describes how to configure single sign-on (SSO) for Cisco SD-WAN. Cisco SD-WAN supports SSO for the following identity providers (IdPs):

- Okta
- Active Directory Federation Services (ADFS)
- PingID
- [Configure Single Sign-On Using Okta, on page 183](#)
- [Configure SSO for Active Directory Federation Services \(ADFS\), on page 187](#)
- [Configure SSO for PingID, on page 190](#)
- [Configure SSO for IDPs in Cisco vManage Cluster, on page 193](#)

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).



Note

Cisco vManage no longer supports MD5 or SHA-1. All x.509 certificates handled by Cisco vManage need to use at least SHA-256 or a higher encryption algorithm.

Perform the following steps to configure SSO.

Enable an Identity Provider in Cisco vManage

To configure Okta SSO, use Cisco vManage to enable an identity provider and generate a Security Assertion Markup Language (SAML) metadata file:

1. From the Cisco vManage menu, chose **Administration** > **Settings**.
2. Click **Identity Provider Settings** and then click **Edit**.
3. Click **Enabled**.

4. Click **Click here to download the SAML metadata** and save the contents in a text file. This data is used for configuring Okta.
5. From the metadata that is displayed, make a note of the following information that you need for configuring Okta with Cisco 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 in to the Okta website.

**Note**

Each IdP application gets a customized URL from Okta for logging in to the Okta website.

2. Create a username using your email address.
3. To add Cisco vManage as an SSO application, from the Cisco vManage menu, click **Admin**.
4. Check the upper-left corner to ensure that it shows the **Classic UI** view on Okta.
5. If it shows **Developer Console**, click the down triangle to choose the **Classic UI**.
6. Click **Add Application** under **Shortcuts** to the right to go to the next window, and then click **Create New Application** on the pop-up window.
7. Choose **Web** for the platform, and choose **SAML 2.0** as the **Sign on Method**.
8. Click **Create**.
9. Enter a string as **Application name**.
10. (Optional): Upload a logo, and then click **Next**.
11. On the **SAML Settings for Single sign on URL** section, set the value to the **samlLoginResponse URL** from the downloaded metadata from Cisco vManage.
12. Check the **Use this for Recipient URL and Destination URL** check box.
13. 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 Cisco vManage site.
14. For **Default RelayState**, leave empty.
15. For **Name ID format**, choose **EmailAddress**.

16. For **Application username**, choose **Okta username**.
17. For **Show Advanced Settings**, enter the fields as indicated below.

Table 23: Fields for Show Advanced Settings

Component	Value	Configuration
Response	Signed	Not applicable
Assertion Signature	Signed	Not applicable
Signature Algorithm	RSA-SHA256	Not applicable
Digest Algorithm	SHA256	Not applicable
Assertion Encryption	Encrypted	Not applicable
Encryption Algorithm	AES256-CBC	Not applicable
Key Transport Algorithm	RSA-OAEP	Not applicable
Encryption Certificate	Not applicable	<ol style="list-style-type: none"> a. Copy the encryption certificate from the metadata you downloaded. b. Go to www.samltool.com and click X.509 CERTS, paste there. Click Format X.509 Certificate. c. Ensure to remove the last empty line and then save the output (X.509.cert with header) into a text file encryption.cer. d. Upload the file. Mozilla Firefox may not allow you to do the upload. Instead, you can use Google Chrome. You should see the certificate information after uploading to Okta.
Enable Single Logout		Ensure that this is checked.
Single Logout URL		Get from the metadata.
SP Issuer		Use the entityID from the metadata.
Signature Certificate		<ol style="list-style-type: none"> a. Obtain from the metadata. Format the signature certificate using www.samltool.com as described. b. Save to a file, for example, signing.cer and upload.
Authentication context class	X.509 Certificate	Not applicable

Component	Value	Configuration
Honor Force Authentication	Yes	Not applicable
SAML issuer ID string	SAML issuer ID string	Not applicable
Attribute Statements	Field: Name	Value: <i>Username</i>
	Field: Name format (optional)	Value: Unspecified
	Field: Value	Value: <i>user.login</i>
Group Attribute Statements	Field: Name	Value: Groups
	Field: Name format (optional)	Value: Unspecified
	Field: Matches regex	Value: <i>.*</i>

**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.

18. Click **Next**.
19. For **Application Type**, check **This is an internal app that we have created** (optional).
20. Click **Finish**. This brings you to the Okta application window.
21. Click **View Setup Instructions**.
22. Copy the IdP metadata.
23. In Cisco vManage, navigate to **Identity Provider Settings > Upload Identity Provider Metadata**, paste the IdP metadata, and click **Save**.
24. In addition to copy-and-pasting the contents of a file with IdP metadata, you can also upload a file directly using the **Select a file** option.

Assign Users to the Application on the Okta Website

To assign users to the application on the Okta website:

1. On the Okta application window, navigate to **Assignments > People > Assign**.
2. Choose **Assign to people** from the drop-down menu.
3. Click **Assign** next to the user(s) you chose and click **Done**.
4. To add a user, click **Directory > Add Person**.
5. Click **Save**.

Configure SSO for Active Directory Federation Services (ADFS)

Describes how to use Cisco vManage and ADFS to configure SSO.

The configuration of Cisco vManage to use ADFS as an IdP involves two steps:

- Step 1 - Import ADFS metadata to Cisco vManage.
- Step 2- Export Cisco vManage metadata to ADFS.

Step 2 can be further divided into:

- Edit and then import Cisco vManage metadata to ADFS.
- Set up ADFS manually using the information from Cisco vManage metadata.

Import Metadata File into ADFS

Step 1 - Import ADFS metadata to Cisco 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. From the Cisco vManage menu, choose **Administration > Settings > Identify Provider Settings > Enable** , and then upload **adfs_metadata.txt** to Cisco vManage .

Step 2 - Export Cisco 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 the Cisco vManage metadata file by deleting everything from `<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">` to `</ds:Signature>`.
6. Edit the Cisco vManage metadata file by deleting everything from `<md:KeyDescriptor use="encryption">` to `</md:KeyDescriptor>`.
7. Import the new modified Cisco 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 Cisco vManage.

Add ADFS Relying Party Trust

Before you begin

To add an ADFS relying party trust using Cisco vManage:

1. From the Cisco vManage menu, choose **Administration > Settings > Identify Provider Settings > Enable**.
2. Download the ADFS Metadata file, and upload it into Cisco 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. Choose **Enter data about the relying party manually**, and click **Next**.
6. Choose **Display name** and **Notes**, and then click **Next**.
7. Choose **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 WebSso 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. Choose **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 **Assurance Transform Rules**.
21. Click **Finish**.
22. Open **Properties** window of the newly created **Relying Party Trust**, and click **Signature**.
23. Click **Add**, and add the **Signing.cer** created in **Step 6**.
24. In the **Active Directory**, click **General**, 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 Cisco vManage.

Configure SSO for PingID

Cisco vManage supports PingID as an IdP. PingID is an identity management service for authenticating user identities with applications for SSO.

The configuration of Cisco vManage to use PingID as an IdP involves the following steps:

- Import (upload) IdP metadata from PingID to Cisco vManage.
- Download the Cisco vManage SAML metadata file to export to PingID.

Prerequisites:

1. In Cisco vManage, ensure that identity provider settings (**Administration Settings > Identity Provider Settings**) are set to **Enabled**.

2. Download the Cisco vManage SAML metadata file to export to PingID.

For more information on these procedures, see [Enable an Identity Provider in Cisco vManage](#). The steps are the same as for configuring Okta as an IdP.

Perform the following steps for configuring PingID.

Configure SSO on the PingID Administration Portal

To configure PingID:

1. Log in to the [PingID administration portal](#).
2. Create a username using your email address.
3. Click the **Applications**.
4. Click **Add Application** and choose **New SAML Application**.
In the **Application Details** section, **Application Name**, **Application Description**, and **Category** are all required fields.
For logos and icons, PNG is the only accepted graphics format.
5. Click **Continue to Next Step**.
The **Application Configuration** section appears.
6. Make sure that you choose **I have the SAML configuration**.
7. Under the **You will need to download this SAML metadata to configure the application** section, configure the following fields:
 - a. For **Signing Certificate**, use the drop-down menu, **PingOne Account Origination Certificate**.
 - b. Click **Download** next to **SAML Metadata** to save the PingOne IdP metadata into a file.
 - c. Later, you need to import the PingOne IdP metadata file into Cisco vManage to complete the SSO configuration.
 1. From the Cisco vManage menu, choose **Administration > Settings**.
 2. Click **Identity Provider Settings > Upload Identity Provider Metadata** to import the saved PingOne IdP metadata file into Cisco vManage.
 3. Click **Save**.
8. Under the **Provide SAML details about the application you are connecting to** section, configure the following fields:
 - a. For **Protocol Version**, click **SAMLv2.0**.
 - b. On **Upload Metadata**, click **Select File** to upload the saved Cisco vManage SAML metadata file to PingID.
PingID should be able to decode the metadata file and fill in the other fields.
 - c. Verify that the following fields and values are entered correctly.

Field	Value
Assertion Consumer Service (ACS)	<vManage_URL>/samlLoginResponse
Entity ID	IP address of Cisco vManage
Single Logout Endpoint	<vManage_URL>/samlLogoutResponse
Single Logout Binding Type	Redirect
Primary Verification Certificate	Name of the certificate
Encrypt Assertion	(Optional) If you do not encrypt the assertion, you might be prone to assertion replay attacks and other vulnerabilities.
Encryption Certification	Name of the certificate
Encryption Algorithm	(Optional) AES_256
Transport Algorithm	RSA_OAEP
Signing Algorithm	RSA_SHA256
Force Re-authentication	True

9. Click **Continue to Next Step**.
10. In the **SSO Attribute Mapping** section, configure the following fields:
 - a. Click **Add new attribute** to add the following attributes:
 1. Add **Application Attribute** as **Username**.
 2. Set **Identity Bridge Attribute or Literal Value Value** to **Email**.
 3. Check the **Required** box.
 4. Add another **Application Attribute** as **Groups**.
 5. Check the **Required** check box, and then click on **Advanced**.
 6. In the **IDP Attribute Name or Literal Value** section, click **memberOf**, and in **Function**, click **GetLocalPartFromEmail**.
 - b. Click **Save**.
11. Click **Continue to Next Step** to configure the **Group Access**.
12. Click **Continue to Next Step**.
13. Before clicking **Finish**, ensure that the settings are all correct.

Configure SSO for IDPs in Cisco vManage Cluster

1. Create three Cisco vManage single-tenant instances and associated configuration templates. See [Deploy Cisco vManage](#).
2. Create a Cisco vManage cluster consisting of three Cisco vManage instances. See the [Cluster Management](#) chapter in the *Cisco SD-WAN Getting Started Guide*.
3. Download SAML metadata based on the IDP from the first Cisco vManage instance, and save it into a file.
4. Configure SSO for Okta, ADFS, or PingID.
5. Note and save the SAML response metadata information that you need for configuring Okta, ADFS, or PingID with Cisco vManage.
6. In the first instance of Cisco vManage, navigate to **Administration > Settings > Identity Provider Settings > Upload Identity Provider Metadata**, paste the SAML response metadata information, and click **Save**.

When you log in to the Cisco vManage cluster now, the first instance of Cisco vManage redirects SSO using an IDP. The second and third instances of the cluster also redirect SSO using IDP.

If the first instance of Cisco vManage cluster or the application server isn't available, the second and third instances of the cluster try redirecting SSO using an IDP. However, the SSO login fails for the second and third instances of the Cisco vManage cluster. The only option available for accessing the second and third instances of the Cisco vManage cluster is by using the local device authentication, which is `/login.html`.



CHAPTER 16

Cisco TrustSec Integration

Table 24: Feature History

Feature Name	Release Information	Description
Support for SGT Propagation with Cisco TrustSec Integration	Cisco IOS XE Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables Cisco IOS XE SD-WAN edge devices to propagate Security Group Tag (SGT) inline tags that are generated by Cisco TrustSec-enabled switches in the branches to other edge devices in the Cisco SD-WAN network. While Cisco TrustSec-enabled switches does classification, propagation (inline SGT tagging) and enforcement on the branches, Cisco IOS XE SD-WAN devices carry the inline tags across the edge devices.

This chapter contains the following sections:

- [Support for SGT Propagation with Cisco TrustSec Integration, on page 195](#)
- [SGT Propagation Using Inline Tagging, on page 196](#)
- [SGT Propagation Using SXP, on page 203](#)
- [SGACL for Cisco TrustSec, on page 211](#)
- [SGT Enforcement, on page 214](#)
- [Monitor SXP Connections and SGT Enforcement, on page 215](#)

Support for SGT Propagation with Cisco TrustSec Integration

Cisco TrustSec is an end-to-end network infrastructure that provides a scalable architecture for the enforcement of role-based access control, identity-aware networking, and data confidentiality to secure the network and its resources. Cisco TrustSec uses Security Group Tag (SGT) to represent user and device groups. The switches, routers, and firewalls inspect these tags and enforce SGT-based traffic policies.

Cisco TrustSec is defined in three phases—classification, propagation, and enforcement. After traffic is classified, the SGT is propagated from where classification took place, to where enforcement action is invoked. This process is called propagation. Cisco TrustSec offers two types of SGT propagation, Inline tagging and Security Group Tag Exchange Protocol (SXP).

With inline tagging, a special Ethernet frame is used to propagate these SGTs between network hops where the policies are enforced based on the SGT policy. After the introduction of this feature, Cisco IOS XE

SD-WAN devices support propagation of SGT. See [Configure SGT Inline Tagging Using Cisco vManage, on page 199](#)

When Inline tagging is not used (or not possible), an SXP protocol can be used to dynamically exchange IP address binding to SGT between Cisco IOS XE SD-WAN devices. You can also manually configure IP address to SGT binding, statically, in Cisco vManage. See [SGT Propagation Using SXP, on page 203](#)

Enforcement of SGT is achieved using Security Group Access Control Lists (SGACL) where policies can be dynamically or statically configured and applied to the egress traffic on the network. See [SGT Enforcement, on page 214](#)

Benefits of Cisco TrustSec

- Provides secure access to network services and applications based on user and device identity.
- Applies policies across the network using tags instead of IP addresses.
- Enforces policies easily. SGT propagation simplifies network access and security operations with software-defined segmentation.
- Scales fast and enforces policies consistently across the network. SGT propagation helps streamline security policy management across domains.
- Reduces risk and segments devices without redesigning the network. You can easily manage access to enterprise resources and restrict lateral movement of threats with microsegmentation.

SGT Propagation Using Inline Tagging

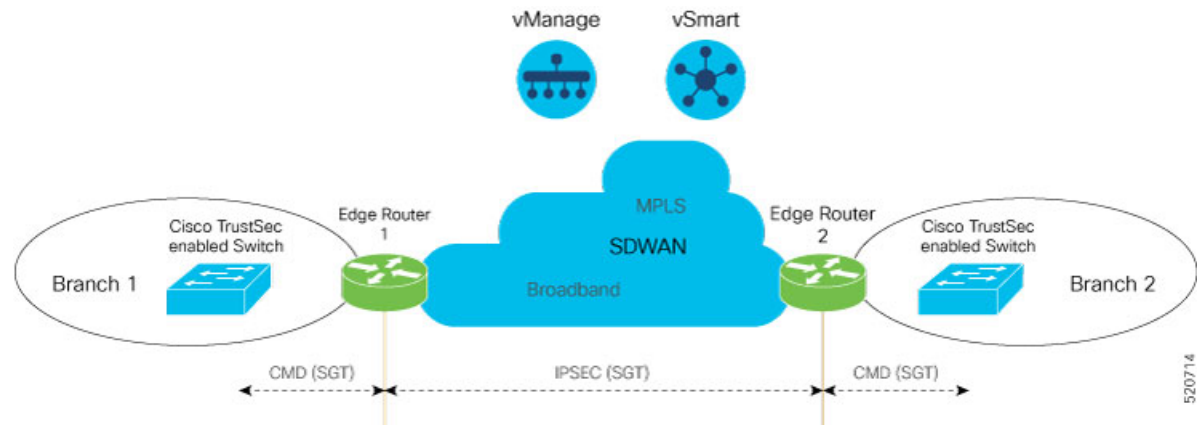
One of the SGT propagation methods is using Inline tagging where a special Ethernet frame is used to propagate these SGTs between network hops where the policies are enforced based on the SGT policy. For more information see, [SGT Propagation in Cisco SD-WAN, on page 196](#)

Prerequisites

- Branches must be equipped with Cisco TrustSec-enabled switches that are capable of handling SGT inline tagging.
- Cisco IOS XE SD-WAN devices running on Cisco IOS XE Release 17.3.1a and later.

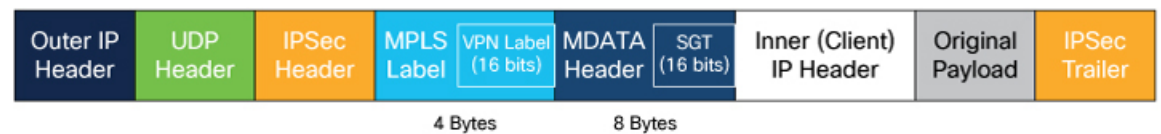
SGT Propagation in Cisco SD-WAN

The following image illustrates how SGT is propagated in Cisco SD-WAN from one branch to another.

Figure 8: SGT Propagation in Cisco SD-WAN

In this illustration, Branch 1 and Branch 2 are equipped with Cisco TrustSec-enabled switches, and these branches are connected to the Cisco IOS XE SD-WAN devices. The Cisco TrustSec switch in Branch 1 performs SGT Inline tagging in the Ethernet CMD frame toward Edge Router 1. Edge Router 1 then de-encapsulates the CMD frame, extracts the SGT, and propagates it over Cisco SD-WAN IPsec or GRE tunnels. The Edge Router 2 on Cisco SD-WAN extracts the SGT from Cisco SD-WAN, generates the Ethernet CMD frame, and copies the that is SGT received. The Cisco TrustSec switch on Branch 2 inspects the SGT, and looks it up against the destination SGT to determine if the traffic must be allowed or denied.

The following image is an illustration of SGT being carried through in an SD-WAN packet and an additional eight bytes of data is added to it.

Figure 9: SGT Propagation

The following table describes how SGT propagation between edge devices in the Cisco SD-WAN network varies based on the type of edge device and software release installed on the device.

Table 25: SGT Propagation with Cisco IOS XE SD-WAN Devices of Different Releases Interconnected in Cisco SD-WAN

Cisco IOS XE SD-WAN Device at Source	Cisco SD-WAN Device at Destination	Result
Cisco IOS XE Release 17.3.1a	Cisco IOS XE SD-WAN device with Cisco IOS XE Release 17.3.1a or later	<ul style="list-style-type: none"> Traffic with SGT is forwarded to the Cisco IOS XE SD-WAN device. If Cisco TrustSec is enabled on the Cisco IOS XE SD-WAN device, traffic with SGT along with the CMD header is forwarded to the switch. If Cisco TrustSec is not enabled on the Cisco IOS XE SD-WAN device, traffic without the SGT and CMD header is forwarded to the switch.
	Cisco IOS XE SD-WAN device with Cisco IOS XE Release Amsterdam 17.2.x and earlier.	Traffic without SGT is forwarded to the Cisco IOS XE SD-WAN device.
	Cisco vEdge device	Traffic without SGT is forwarded to the Cisco vEdge device.

Supported Platforms and NIMs

Supported Platforms

The following devices support propagation of SGT inline tagging. SGT propagation is supported only on the onboard WAN ports of these routers:

- Cisco 1100 Integrated Services Router
- Cisco CSR 1000v Series Cloud Services Router
- Cisco 4300 Integrated Services Router
- Cisco 4400 Integrated Services Router
- Cisco ASR 1001-X Router
- Cisco ASR 1001-HX Router
- Cisco ASR 1002-X Router
- Cisco ASR 1002-HX Router
- Cisco 5000 Series Enterprise Network Compute System
- Cisco Catalyst 8000V Router

- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Router

Supported NIMs

The following WAN NIMs are supported for Cisco 4000 Series Integrated Services Routers platforms:

- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- SM-X-4x1G-1x10G
- SM-X-6X1G

Limitations for SGT Propagation

- Enabling the **cts manual** command momentarily causes the interface to flap. Therefore, we recommend that you configure Cisco TrustSec manual on the Cisco IOS XE SD-WAN device before configuring it on the switch.
- If you are configuring subinterfaces on a Cisco IOS XE SD-WAN device, Cisco TrustSec must be enabled on the physical interface and on all the subinterfaces.
- Only devices on Cisco IOS XE Release 17.3.1a support propagation of SGT.
- Inline tagging is supported only on the L3 (WAN) ports of the Cisco IOS XE SD-WAN devices, and not on switch ports.
- For releases prior to Cisco IOS XE Release 17.3.3, Cisco SD-WAN multicast overlay traffic is not supported on interfaces enabled with the Cisco TrustSec feature.

Configure SGT Inline Tagging Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature > Add Template**.
3. Choose a Cisco IOS XE SD-WAN device from the list.
4. Choose one of the available Cisco VPN Interface templates, for example, **Cisco VPN Interface Ethernet**.
5. Enter a name and a description for the feature template.
6. Click **Tunnel**.

In the **CTS SGT Propagation** field, click **On** to enable SGT propagation for inline tagging. By default, this option is disabled.






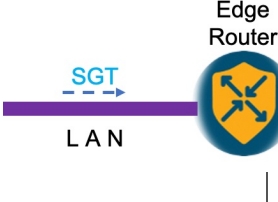
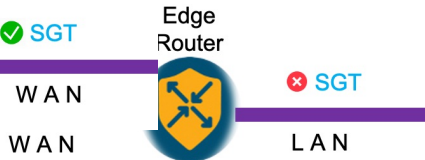

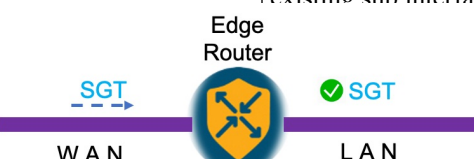
Note This is applicable to VPN0 tunnel interfaces only.

7. Click **TrustSec**.
8. Enable the Cisco TrustSec SGT propagation feature. By default, this feature is disabled.
9. To use the Cisco TrustSec SGT propagation feature, from the **Enable SGT Propagation** drop-down menu, choose **Global**, and then click **On**. Additional propagation options are displayed.
10. To propagate SGT in Cisco SD-WAN, set **Propagate** to **On**.

The following table displays the SGT propagation options, and the LAN to WAN and WAN to LAN behavior based on the option you choose for SGT propagation. The options are displayed in the following table and available to you only if you set the **Enable SGT Propagation** to **On**.

Table 26: SGT Propagation options

SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = On Security Group Tag = <SGT Value> Trusted = On	SGT is propagated from LAN to WAN. 	SGT is propagated from WAN to LAN. 	This is the most common configuration. Usually the SGT value
Propagate = On Security Group Tag = <SGT Value> Trusted = Off	SGT is propagated from LAN to WAN with a configured SGT value.	SGT is propagated from WAN to LAN. No effect to the incoming SGT.	Overrides the incoming SGT from LAN to WAN because Trusted is set to Off
Propagate = Off Security Group Tag = <SGT Value> Trusted = On	SGT is propagated from LAN to WAN. No effect to the incoming SGT.	SGT is not propagated from WAN to LAN. 	

SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = Off Security Group Tag = <SGT Value> Trusted = Off	SGT is propagated from LAN to WAN with a configured SGT value. 	SGT is not added to the LAN packets. SGT is not propagated. 	Overrides the incoming SGT from LAN to WAN because Trusted is set to Off .
Propagate = On	SGT propagated from LAN to WAN with SGT value. 	SGT is propagated from WAN to LAN with SGT value 0. 	This can be configured only on a physical interface if there are existing sub interfaces.

**Note**

Cisco 5000 Series Enterprise Network Compute System (ENCS) are configured differently.

On the Cisco 5000 series ENCS there are eight switch ports which are its LAN interfaces and two routing ports which are its WAN interfaces. Unlike all Edge devices for which all of the interfaces are identical, the ENCS LAN interfaces and WAN interfaces are different. When an ENCS 5000 series device is used as an Edge device for propagation of SGT, physically, the LAN interfaces must be connected to LAN side and the WAN interfaces must be connected to the WAN side of the network.

11. Click **Save**.
12. Configure the routing protocols using the vManage templates. You can choose to use any of the routing protocols. For BGP template, see [Configure BGP Using vManage Templates](#).
13. Attach the feature template to the device template.

Configure SGT Inline Tagging Using CLI

The following example shows SGT propagation configured on a Cisco IOS XE SD-WAN device. In this example:

- A network connection is established between a switch in the branch and a Cisco IOS XE SD-WAN device.
- Two VRF instances, and subinterfaces are configured on the Cisco IOS XE SD-WAN device.

- SGT propagation is enabled on the subinterfaces.
- SGT propagation is configured on the network using BGP.

```

! VRF 1
vrf definition 1
  rd 1:1
!

! VRF 2
vrf definition 2
  rd 1:2
!

! Link between switch and router
interface GigabitEthernet0/0/2
  no ip address
  no ip redirects
  negotiation auto
  ip mtu 1504
  mtu 1504
  cts manual
!

! sub-interface on VRF 1
interface GigabitEthernet0/0/2.2
  encapsulation dot1Q 2
  vrf forwarding 1
  ip address 77.27.9.2 255.255.255.0
  ip mtu 1500
  cts manual
  policy static sgt 2 trusted
!

! sub-interface on VRF 2
interface GigabitEthernet0/0/2.3
  encapsulation dot1Q 3
  vrf forwarding 2
  ip address 77.27.19.2 255.255.255.0
  ip mtu 1500
  cts manual
  policy static sgt 2 trusted
!

! BGP configuration
router bgp 64005
  bgp log-neighbor-changes
  distance bgp 20 200 20
!
! BGP neighbor VRF 1
address-family ipv4 vrf 1
  network 77.27.9.0 mask 255.255.255.0
  redistribute connected
  redistribute static
  redistribute omp
  neighbor 77.27.9.1 remote-as 64006
  neighbor 77.27.9.1 activate
  neighbor 77.27.9.1 send-community both
exit-address-family
!
! BGP neighbor VRF 2
address-family ipv4 vrf 2
  redistribute connected
  redistribute static

```

```

redistribute omp
neighbor 77.27.19.1 remote-as 64006
neighbor 77.27.19.1 activate
neighbor 77.27.19.1 send-community both
exit-address-family
!
```

View SGT Propagation Configuration

To view Cisco TrustSec SGT Propagation configuration, follow these steps:

1. From the Cisco vManage menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time** in the left pane.
4. From **Device Options** drop-down list, choose **Interface TrustSec** to view SGT propagation configuration.

SGT Propagation Using SXP

Table 27: Feature History

Feature Name	Release Information	Description
SGT Propagation Using SXP and SGACL Enforcement	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	With this feature, Cisco IOS XE SD-WAN devices can exchange SGT over the overlay network using SXP. Use SXP when your hardware does not support Inline propagation of SGTs. This feature also extends support for SGACL enforcement on Cisco IOS XE SD-WAN devices by configuring SGACL policies.

You can use SXP to propagate SGTs across network devices if your hardware does not support inline tagging. Using Cisco Identity Services Engine (ISE), you can create an IP-to-SGT binding (Dynamic IP-SGT) and then download IP-SGT binding using SXP to a Cisco IOS XE SD-WAN device for propagation of the SGT over the Cisco SD-WAN network. See [Configure SXP for Dynamic IP-SGT Binding Using Cisco vManage, on page 206](#).

Alternatively, you have the option to manually configure IP-SGT binding (Static IP-SGT) and then push the configuration to a Cisco IOS XE SD-WAN device using a CLI Add-On template to propagate SGT over the Cisco SD-WAN network. See [Configure Static IP-SGT Binding Using Cisco vManage, on page 208](#).

Prerequisites

- You must enable Cisco TrustSec and propagation through SXP on the devices in a Cisco SD-WAN network.
- Cisco ISE version must be 2.6 or later.

Points to Consider

- Cisco ISE has a limit on the number of SXP sessions it can handle. Therefore, as an alternative, you can use SXP reflector for horizontal scaling.
- Static IP-SGT configuration is based on the CLI Add-On template and not using a Feature template in vManage.
- From Cisco IOS XE Release 17.5.1a, Cisco vManage Release 20.5.1, we recommend that you use an SXP reflector to establish an SXP peering with Cisco IOS XE SD-WAN devices. This is because when you use an SXP Reflector, the SXP filtering option ensures that only relevant IP-SGT bindings for the local service side networks are pushed down to the Cisco IOS XE SD-WAN device. Overlapping or remote entries coming through SXP can have an adverse effect on the Overlay routing. See [SXP Reflectors, on page 205](#)

Limitations for SGT Propagation Using SXP

- 802.1x-based SGT assignment is not supported.
- SGACL policies cannot be downloaded using HTTP.
- SXP filter is not supported.
- Static SGACLs using IPv6 is not supported through CLI or Cisco vManage.
- SGACL policies cannot be enforced on the ingress traffic, only on egress traffic in a Cisco SD-WAN network.
- The option to cache SGT is not available.
- An SXP connection with an IPv6 version is not supported.
- You cannot have overlapping of OMP routes for the prefixes bound to SGTs.
- SXP Node ID must be explicitly configured.
- Cisco TrustSec feature is not supported with Federal Information Processing Standard (FIPS) mode enabled. If FIPS mode is enabled, download of Protected Access Credential (PAC) key fails.

Supported Platforms and NIMs

Supported Platforms

The following devices support propagation of SGT using SXP. SGT propagation is supported only on the onboard WAN ports of these routers:

- Cisco 1000 Series Integrated Services Router
- Cisco 1100 Integrated Services Router (on L3 [WAN] ports)
- Cisco Integrated Services Virtual Router (on L3 [WAN] ports)
- Cisco CSR 1000v Series Cloud Services Router
- Cisco 4300 Integrated Services Router
- Cisco 4331 Integrated Services Router

- Cisco 4351 Integrated Services Router
- Cisco 4400 Integrated Services Router
- Cisco ASR 1001-X Router
- Cisco ASR 1001-HX Router
- Cisco ASR 1002-X Router
- Cisco ASR 1002-HX Router
- Cisco ASR 1006-X Router
- Cisco Catalyst 8000V Router
- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Router

Supported NIMs

The following WAN NIMs are supported on Cisco 4000 Series Integrated Services Routers platforms:

- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- SM-X-4x1G-1x10G
- SM-X-6X1G

Propagate SGT Using SXP

If hardware does not support SGT propagation through inline tagging, you can propagate SGT using SXP.

If a branch is equipped with Cisco TrustSec-enabled hardware, the branch is referred to as a TrustSec branch. You can propagate SGTs to a TrustSec branch through inline tagging. For information about Inline Tagging, see [SGT Propagation in Cisco SD-WAN, on page 196](#).

If a branch is not equipped with Cisco TrustSec-enabled hardware, the branch is referred to as a non-TrustSec branch. You can propagate SGT to a non-TrustSec branch using SXP.

In the case of a non-TrustSec branch, for SD-WAN ingress, a Cisco IOS XE SD-WAN device performs SGT tagging based on source IP address of the packet and IP-SGT binding dynamically learned from ISE using SXP or based on static IP-SGT binding configuration. For SD-WAN egress, the Cisco IOS XE SD-WAN device performs a destination SGT lookup based on the destination IP address using IP-SGT bindings (received through SXP or static configuration), and the SGT is determined. Policies for the SGT traffic on SD-WAN egress is enforced either by downloading SGACL policies from ISE or by configuring static SGACL policies.

SXP Reflectors

SXP reflectors are used when you need to have multiple connections to communicate information about IP-SGT bindings over a network. Because Cisco ISE has a limit on the number of SXP sessions it can handle,

as an alternative, you can use Cisco ASR1000 routers, with the SXP reflector functionality enabled for horizontal scaling between ISE and the Cisco IOS XE SD-WAN device.

You can configure an SXP connection to an SXP reflector the same way you configure an SXP connection to ISE. For information about configuring SXP reflector, see [Configure SXP Reflector using the CLI, on page 211](#).

We recommend an SXP reflector to establish SXP peering with Cisco IOS XE SD-WAN devices. When you use an SXP reflector, the SXP filtering configuration ensures that only relevant IP-SGT bindings for the local service-side networks are pushed down to the Cisco IOS XE SD-WAN devices. Overlapping or remote entries coming through an SXP can have an adverse effect on overlay routing.

Configure SXP for Dynamic IP-SGT Binding Using Cisco vManage

You can configure an SXP connection for downloading the IP-SGT binding from Cisco ISE to a Cisco IOS XE SD-WAN device.

To configure an SXP connection in Cisco vManage:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature > Add Template**.
3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **TrustSec**.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Enter the details for setting up an SXP connection:

Parameter Name	Description
Device SGT	Enter a value to configure the SGT for packets sent from a device. Range: 2 to 65519.
Credentials ID	Enter a TrustSec ID for the device. This ID must be the same as that in ISE and must not exceed 32 characters.
Credentials Password	Enter a TrustSec password for the device.
Enable Enforcement	Click On to enable at a global level. Click Off to disable SGT enforcement. Note You can enable this configuration either at a global level here, or at an interface level in step 8 of Configuring SGT Enforcement at an interface level in Cisco vManage, but not both.

8. Configure SXP for dynamic IP/SGT.

Parameter Name	Description
Enable SXP	Click On to enable an SXP connection on the device. When you enable SXP, you must enter a Node ID and a Node ID type. Note When you change a Node ID, you must first disable SXP and then push the template to the device. Then, you change the Node ID, and then push the template to the device again.
Source IP	Enter an IP address to set up a source IP address for SXP.
Password	Enter a default password for SXP.
Key Chain Name	Enter a name to configure the key chain for SXP.
Log Binding Changes	Click On to enable logging for IP-to-SGT binding changes.
Reconciliation Period (seconds)	Enter a time (in seconds) to configure the SXP reconciliation period. After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconciliation period timer starts. While the SXP reconciliation period timer is active, the Cisco TrustSec software retains the SGT mapping entries learned from the previous connection and removes the invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconciliation period to 0 seconds disables the timer and causes all the entries from the previous connection to be removed.
Retry Period (seconds)	Enter a time (in seconds) to configure the retry period for SXP reconnection.
Speaker Hold Time (seconds)	Enter time (in seconds) to configure the global hold-time period for a speaker device.
Minimum Listener Hold Time (seconds)	Enter a time (in seconds) to configure the minimum allowed hold-time period for a listener device.
Maximum Listener Hold Time (seconds)	Enter a time (in seconds) to configure the maximum allowed hold-time period for a listener device.
Node ID Type	Choose a node ID type.
Node ID	Enter a node ID. A node ID is used to identify the individual devices within the network.

9. Click **New Connection** to add a new SXP peer connection details.

Parameter Name	Description
Peer IP	Configure a peer IPv4 address for SXP.
Source IP	Configure a source IPv4 address for SXP.
Preshared Key	Choose a preshared key type.
Mode	Choose a connection mode. Local refers to the local device, and Peer refers to a peer device.
Mode Type	Choose a role for the device.

Parameter Name	Description
Minimum Hold Time	Enter time (in seconds) to configure the minimum hold time for the SXP connection.
Maximum Hold Time	Enter time (in seconds) to configure the maximum hold time for the SXP connection.
VPN ID	Enter a VPN or VRF ID for the SXP connection.



Note **Maximum Hold Time** and **Minimum Hold Time** can be configured only when you choose **Mode** as **Local** and **Mode Type** as **Listener**, or when **Mode** is **Peer** and **Mode Type** is **Speaker**.

Only **Minimum Hold Time** is configurable when **Mode** is **Local** and **Mode Type** is **Speaker** or when **Mode** is **Peer** and **Mode Type** is **Listener**.

Hold time cannot be configured if you choose **Mode Type** as **Both** (that is **Listener** and **Speaker**).

10. Click **Save** to save your configuration for an SXP connection.

Configure SXP for Dynamic IP-SGT Binding on the CLI

Set Up an SXP Connection

```
Device(config)# cts sgt 10
Device(config)# cts credentials id cEDGE4 password 6
RX^ASQVgffV^EOAeQWVZJVFQ_hcLDdgJJDevice(config)# cts credentials password cts_pwd
Device(config)# cts role-based enforcement
Device(config)#
```

Configure SXP for Dynamic IP/SGT Binding

```
Device(config)# cts sxp enable
Device(config)# cts sxp default source-ip 10.29.1.1
Device(config)# cts sxp default password 6 LZcdEUScdLSVZceMAJ_R[cJGb^NbWNLLC
Device(config)# cts sxp default key-chain key1
Device(config)# cts sxp log binding-changes
Device(config)# cts sxp reconciliation period 120
Device(config)# cts sxp retry period 60
Device(config)# cts sxp speaker hold-time 120
Device(config)# cts sxp listener hold-time 60 90
Device(config)#
```

Add a New SXP Peer Connection

```
Device(config)# cts sxp connection peer 10.201.1.2 source 10.29.1.1 password key-chain mode
local both vrf 1
```

Configure Static IP-SGT Binding Using Cisco vManage

To configure static IP-SGT, use the CLI add-on template in Cisco vManage

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature > Add Template**.
3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **CLI Add-On Template** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. In the **CLI Configuration** area, enter the following configuration:

```
cts role-based sgt-map vrf instance_name {ipv4_netaddress|ipv4_netaddress/prefix} sgt
sgt-number
cts role-based sgt-map vrf instance_name host {ipv4_hostaddress} sgt sgt-number
```
8. Click **Save** to save this configuration. This configuration can now be pushed to a Cisco IOS XE SD-WAN device for propagation of the SGT over a Cisco SD-WAN network.

Configure TCP-AO Support for SXP

Cisco TrustSec SXP peers exchange IP-SGT bindings over a TCP connection. TCP Authentication Option (TCP-AO) is used to guard against spoofed TCP segments in Cisco TrustSec SXP sessions between the peers. TCP-AO is resistant to collision attacks and provides algorithmic agility and support for key management.

To enable TCP-AO for an SXP connection, a TCP-AO key chain must be specified for the connection.

To establish an SXP peer connection with TCP-AO:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature > Add Template**.
3. Choose the device for which you are creating the template.
4. Under **BASIC INFORMATION** section, choose **Cisco Security** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Configure TCP-AO key chain and keys.

Parameter Name	Description
Keychain Name	Specify a TCP-AO key chain name. The key chain name can have a maximum of 256 characters.
Key ID	Specify a key identifier. Range: 0 to 2147483647.

Parameter Name	Description
Send ID	Specify the send identifier for the key. Range: 0 to 255.
Receiver ID	Specify the receive identifier for the key. Range: 0 to 255.
Include TCP Options	<p>This field indicates whether TCP options other than TCP-AO must be used to calculate Message Authentication Codes (MACs).</p> <p>A MAC is computed for a TCP segment using a configured MAC algorithm, relevant traffic keys, and the TCP segment data prefixed with a pseudoheader.</p> <p>When options are included, the content of all options is included in the MAC with TCP-AO's MAC field is filled with zeroed.</p> <p>When the options are not included, all options other than TCP-AO are excluded from all MAC calculations.</p>
Accept AO Mismatch	This field indicates whether the receiver must accept the segments for which the MAC in the incoming TCP-AO does not match the MAC that is generated on the receiver.
Crypto Algorithm	<p>Specify the algorithm to be used to compute MACs for TCP segments. You can choose one of these:</p> <ul style="list-style-type: none"> • aes-128-cmac • hmac-sha-1 • hmac-sha-256
Key String	<p>Specify the master key for deriving the traffic keys.</p> <p>The master keys must be identical on both the peers. If the master keys do not match, authentication fails and segments may be rejected by the receiver. Range: 0 to 80 characters.</p>
Send Lifetime Local	<p>Specify the time in seconds that is entered in Cisco vManage for which the key to be used in TCP-AO authentication is valid.</p> <p>Specify the start time in the local time zone. By default, the start time corresponds to UTC time. The end time can be specified in three ways—infinite (no expiry), duration (1 to 2147483646 sec), exact time – (either UTC or local).</p>
Accept Lifetime Local	<p>Specify the time in seconds that is entered in Cisco vManage for which the key to be accepted for TCP-AO authentication is valid.</p> <p>Specify the start time in the local time zone. By default, the start time corresponds to UTC time. The end time can be specified in three ways—infinite (no expiry), duration (1 to 2147483646 sec), exact time – (either UTC or local).</p>

**Note**

When you configure a key chain for an SXP connection, at least one key in the key chain must be configured with the current time. All keys in the key chain cannot be configured completely with a future time.

Configure TCP-AO Support for SXP on the CLI

```
Device(config)# key chain key1 tcp
Device(config-keychain)# key 1000
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Device(config-keychain-key)# key-string 6 _RPB[dVI]SO^BAOVNMKATgOZKMxFGXFTa
Device(config-keychain-key)# accept-lifetime local 18:00:00 Jan 12 2021 06:00:00 Jan 12 2022
Device(config-keychain-key)# send-lifetime local 18:00:00 Jan 12 2021 01:00:00 Jan 12 2022
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config)#
```

Configure SXP Reflector using the CLI

```
cts sxp filter-enable
cts sxp filter-list <device-name1>
  permit ipv4 <ip-address>
  deny ipv4 <ip-address>
  permit ipv6 <network-prefix>
  deny ipv6 <network-prefix>
cts sxp filter-list <device-name2>
  permit ipv4 <ip-address>
  deny ipv4 <ip-address>
  permit ipv6 <network-prefix>
  deny ipv6 <network-prefix>
cts sxp filter-group speaker <device-name1_spk>
  filter <device-name1>
  peer ipv4 <ip-address>
cts sxp filter-group speaker <device-name2_spk>
  filter <device-name1>
  peer ipv4 <ip-address>
!
```

SGACL for Cisco TrustSec

Security Group Access Control Lists (SGACLs) are a policy enforcement mechanism through which an administrator can control the operations performed by users based on the security group assignments and destination resources.

SGACL policies are configured in Cisco ISE and dynamically downloaded for enforcement to a Cisco IOS XE SD-WAN device using a RADIUS server. The downloaded SGACL policies override any conflicting locally defined policies. See [Download SGACL Policies to Cisco vEdge Devices, on page 211](#).

Alternatively, you have the option of configuring SGACL policies on Cisco vManage. The policies can be pushed to the Cisco IOS XE SD-WAN device using the CLI Add-On template. See [Configure Static SGACL Policies in Cisco vManage, on page 213](#).

Download SGACL Policies to Cisco vEdge Devices

When configured in Cisco ISE, SGACL policies can be downloaded dynamically from Cisco ISE to a Cisco IOS XE SD-WAN device using a RADIUS server.

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

3. Choose the device for which you are creating the template.
4. Under **Basic Information**, choose **Cisco AAA** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of the characters and spaces.
7. Click **Radius** to configure a connection to a RADIUS server. The following fields are displayed:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server.
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Range: 0 to 65535.
Accounting Port	Enter the UDP port that will be used to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 to 65535.
Timeout	Specify how long to wait to receive a reply from the RADIUS server before retransmitting a request. Range: 1 through 1000.
Retransmit Count	Specify how many times to search through the list of RADIUS servers while attempting to locate a server. Range: 1 through 1000.
Key Type	Click PAC as key type.
Key	Enter the key the Cisco IOS XE SD-WAN device passes to the RADIUS server for authentication and encryption. You can enter the key as a text string from—1 to 31 characters long,—and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.

8. Click **Radius Group** to add a new RADIUS group. The following fields are displayed:

Parameter Name	Description
Group Name	Displays the RADIUS group name. This field is automatically populated based on the VPN ID that you configure.
VPN ID	Enter a VPN ID.
Source Interface	Set the interface that will be used to reach the RADIUS server.
Radius Server	Choose an IP address for the RADIUS server.

9. Click **Radius COA** to configure the settings to accept change of authorization (CoA) requests from a RADIUS or other authentication server, and to act on requests to a connection to the RADIUS server.

Updated policies are downloaded to the Cisco IOS XE SD-WAN device when SGACL policies are modified on ISE and a CoA is pushed to the Cisco IOS XE SD-WAN device.

On clicking **Radius COA**, the following fields are displayed:

Parameter Name	Description
Client	Displays the RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests.
Domain Stripping	Configure domain stripping at the server group level. The stripping keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.
Port	Specify the RADIUS Dynamic Author port. <i>Range:</i> 0 to 65535

10. Click **TrustSec** to configure more details for authorization. The following details are displayed:

Parameter Name	Description
CTS Authorization List	Specify a name of a list for authentication, authorization, and accounting (AAA) servers.
Radius group	Choose a RADIUS server.

11. Click **Save**.

Download SGACL Policies using CLI

Configure a Radius Group Server

```
Device(config)# aaa group server radius radius-1
Device(config-sg-radius)# ip radius source-interface GigabitEthernet0/0/1.100
Device(config-sg-radius)# ip vrf forwarding 1
Device(config)#
```

Configure a Radius Server

```
Device(config)# aaa group server radius radius-1
Device(config-sg-radius)# server-private 10.251.1.1 auth-port 5 acct-port 5 timeout 5
retransmit 3 pac key 6 ebKQP0bGXfAKgRHQhbWe_ZXFTBCVgFOMg
Device(config)#
```

Configure a Radius CoA

```
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.251.1.1 vrf 1 server-key 6
gWTLbecJKOQcFcIbJNR[]WKP_g^TRacRF
Device(config-locsvr-da-radius)# domain stripping right-to-left
Device(config-locsvr-da-radius)# port 1
Device(config)#
```

Configure Other Details of Authorization

```
Device(config)# cts authorization list cts-mlist
Device(config)# aaa authorization network cts-mlist group radius-1
```

Configure Static SGACL Policies in Cisco vManage

To configure static SGACL policies, use the CLI Add-On template in Cisco vManage.

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature > Add Template**.
3. Choose the device for which you are creating the template.
4. Under **OTHER TEMPLATES** section, choose **CLI Add-On Template** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any of any characters and spaces.
7. In the CLI configuration area, enter the following configuration:

```
interface gigabitethernet 1/1/3
cts role-based enforcement
cts role-based sgt-map sgt 2
interface gigabitethernet 1/1/4
no cts role-based enforcement
[no] cts role-based permissions default ipv4 sgACL-name1 [sgACL-name2 [sgACL-name3 ...
sgACL-name16]]]
[no] cts role-based permissions from {source-sgt | unknown} to {dest-sgt | unknown} ipv4
sgACL-name1 [sgACL-name2 [sgACL-name3 ... sgACL-name16]]]
```

8. Click **Save**.

This configuration can now be pushed to the Cisco IOS XE SD-WAN device for enforcement of SGACL policies.

SGT Enforcement

SGACL policies configured on Cisco ISE, or configured using the CLI Add-On template can be applied and SGT enforced on egress traffic both globally (on all the interfaces) or on a specific interface.

You can enforce SGT at a global level in the TrustSec feature template. See [Configure SXP for Dynamic IP-SGT Binding Using Cisco vManage, on page 206](#).

Configure SGT Enforcement at the Interface Level in Cisco vManage

To enforce SGT using SGACL policies at the interface level in Cisco vManage:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature > Add Template**.
3. Choose the device for which you are creating the template.
4. Under **Basic Information**, choose **Cisco VPN Interface Ethernet** as the feature template.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 - 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.
7. Click **TrustSec**.
8. In the **Enable Enforcement** field, click **On** to enable SGT enforcement on a particular interface.



Note You can enable this configuration either at an interface level in this step, or a global level using the **Enable Enforcement** field in [Configuring SXP for Dynamic IP/SGT using vManage](#), but not both.

9. In the **Enter a SGT value** field, enter a value that can be used as a tag for enforcement .
10. Click **Save**.

Configuring SGT Enforcement at the Interface Level Using CLI

Use the following command to configure SGT enforcement:

```
Device(config)# interface <interface-type> <number>  
Device(config-if)# cts role-based enforcement
```

Monitor SXP Connections and SGT Enforcement

You can monitor an SXP connection and other SGT information in Cisco vManage, or the WAN edge device CLI.

Using Cisco vManage

To monitor SXP SGT information in Cisco vManage:

1. From the Cisco vManage menu, choose **Monitor> Network**.
2. Choose a device from the list of devices.
3. Click **Real Time** in the left pane.
4. Choose one of the following options from the **Device Options** drop-down list to monitor SXP and SGT information:
 - **TrustSec SXP Connections**
 - **TrustSec CTS PAC**
 - **TrustSec CTS Role Based SGT Map**
 - **TrustSec CTS Role Based SGT Permission**
 - **TrustSec CTS Role Based Counters**
 - **TrustSec CTS Role Based IPv6 Permission**
 - **TrustSec CTS Role Based IPv6 Counters**
 - **TrustSec CTS Environment Data**

- TrustSec CTS EnvData Radius Server



Note You can re-arrange the columns to view SXP and SGT information as per your preference by dragging the column title to the desired position. If you re-arrange the columns, we recommended the Source SGT and Destination SGT columns are set to your left hand side so that you can understand the bindings of a traffic flow.

Using CLI

Use the following commands to monitor SXP/SGT information using the CLI.

Table 28: SXP/SGT Commands

Commands	Description
show cts sxp connections	show SXP connections.
show cts role-based sgt-map	Displays role-based access control information (per VRF). (Both static and dynamic entries are shown.)
show cts role-based permissions	Displays the SGACL dynamic and static entries.
show cts role-based counters	Displays Security Group access control list (ACL) enforcement statistics.
show cts environment-data	Displays Cisco TrustSec environment data information.
show cts pac	Displays Cisco TrustSec PAC information.
show aaa server	Displays the AAA server status.
Show key chain	Displays key chain information.



Unified Threat Defense Resource Profiles

Table 29: Feature History

Feature Name	Release Information	Description
Configure Unified Threat Defense Resource Profiles	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	This feature lets you customize the amount of resources that Unified Threat Defense features use on a router. You can use larger resource profiles to process packets simultaneously. Simultaneously processing packets reduces the latency that security features can introduce to the packet processing of the device.

Unified Threat Defense features use the Snort engine to process packets. Snort is an open source network Intrusion Prevention System, capable of performing real-time traffic analysis and packet logging on IP networks. Unified Threat Defense deploys Snort as a single instance on the device to process packets. To improve performance, use the Security App Hosting feature template to allow Unified Threat Defense to use more resources.

You can use the Security App Hosting feature template to modify the resource profile as follows:

- **Deploy more instances of Snort:** When you enable Unified Threat Defense, the device sends each packet from the data plane to the service plane. Unified Threat Defense serially inspects each packet. Once inspected, Unified Threat Defense returns the packet to the data plane. Unified Threat Defense holds each packet to analyze it. These processes introduce latency to the flow of packets that affects the throughput of the device. To combat this latency, you can deploy more instances of Snort. With multiple instances of Snort available, Unified Threat Defense can simultaneously process multiple packets to reduce latency and increase throughput. This feature uses more systems resources.
- **Download URL databases to the devices:** This feature allows the URL Filtering feature of Unified Threat Defense to use a downloaded URL database on the device to find a URL. If the device downloads the database, Unified Threat Defense first uses the database on the device to find the URL. If a URL is not in the downloaded database, Unified Threat Defense connects to the Cloud for the URL information. This Cloud result is saved to a local cache for any subsequent requests to the same URL. This feature requires at least 16 GB bootflash and 16 GB RAM.
- [Supported Platforms, on page 218](#)

- [Configure Unified Threat Defense Resource Profiles](#) , on page 218
- [Verify Unified Threat Defense Resource Profiles](#), on page 219

Supported Platforms



Note

To download the database, the device must have at least 16 GB bootflash and 16 GB RAM.

Platform	Download Database Options	Supported Resource Profile
Cisco Integrated Services Routers (ISR) 1000 C1111	No	low
Cisco ISR1100X-4G	No	low
Cisco ISR1100X-6G	Yes	low
Cisco ISR 4221 and Cisco ISR 4321	No	low
Cisco Integrated Services Virtual Router (ISRv)	No	low
Cisco ISR4331, Cisco ISR4351, Cisco ISR4431 Cisco ISR4451, and Cisco ISR4461	Yes	low, medium, high
Cisco Catalyst 8000V	Yes	low
Cisco Catalyst 8200 Series Edge Platforms	Yes	low, medium, high
Cisco Catalyst 8300 Series Edge Platforms	Yes	low, medium, high
Cisco Catalyst 8500 Series Edge Platform C8500L-8S4X	Yes	low, medium, high

Configure Unified Threat Defense Resource Profiles

Configure the Unified Threat Defense Resource Profiles Using Cisco vManage

You can configure the Unified Threat Defense resource profiles using Cisco vManage by doing the following:

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Feature**.
3. Click **Add Template**.
4. Choose the device(s).
5. Click **Security App Hosting**.
6. Enter a template name and description.
7. Choose whether to enable or disable NAT. NAT is enabled by default.

To use Unified Threat Defense features that connect to the internet, you must enable NAT. For example, URL Filtering and Advanced Malware Protection connect to the internet to perform Cloud lookups. To use these features, enable NAT.

8. To download the URL database on the device, choose **Yes**.
9. To deploy more instances of Snort, choose one of the following resource profiles:
 - **Low**: This is the default profile.
 - **Medium**.
 - **High**.

When you specify a larger resource profile, the device deploys more Snort instances to increase throughput. The larger resource profiles also use more resources on the device. The number of Snort instances deployed by the device differs by platform and software release.

10. Click **Save**.
11. Add this template to the device template.
12. Attach the device template to the device.

Verify Unified Threat Defense Resource Profiles

To view the Unified Threat Defense resource profiles that you configured, run the following commands:

```
show app-resource package-profile
show run | section app-hosting appid utd
show app-hosting detail appid utd | section Activated profile name
```

To view the resource usage between activated resource profiles, run the following commands:

```
show platform software status control-processor brief
show platform hardware qfp active datapath utilization
show utd engine standard utilization cpu
show utd engine standard utilization memory
show app-hosting resource
```

To view the health of one or more Snort instances and the memory usage of UTD, run the following command:

```
show utd engine standard status
```




CHAPTER 18

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 30: 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 "<![CDATA[<h3>Access" to the requested page has been denied]]>" 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 <\![CDATA[&lt;h3>Access to the requested page has been denied&lt;/h3>&lt;p>Please contact your Network Administrator&lt;/p>]]> ! 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