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

First Published: 2019-11-22

Last Modified: 2024-08-27

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 NONINFRINGEMENT 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.

CONTENTS

CHAPTER 1

Read Me First

Note

To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

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)

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.

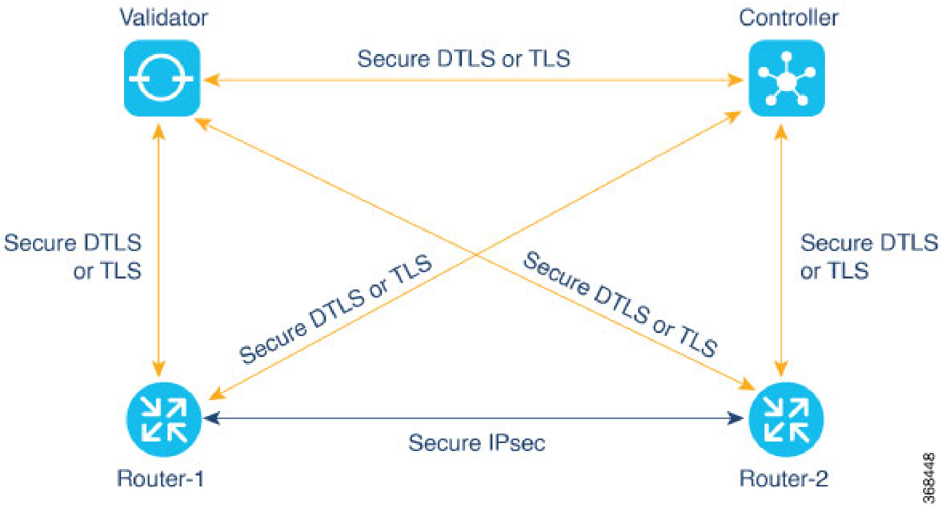
This chapter contains the following topics:

Cisco Catalyst SD-WAN Security Components

The Cisco Catalyst 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 Catalyst 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 Catalyst SD-WAN overlay network. The security discussion refers to the following illustration of the components of the Cisco Catalyst SD-WAN network—the Cisco SD-WAN Controller, the Cisco SD-WAN Validator, 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 Catalyst 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 Catalyst 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.

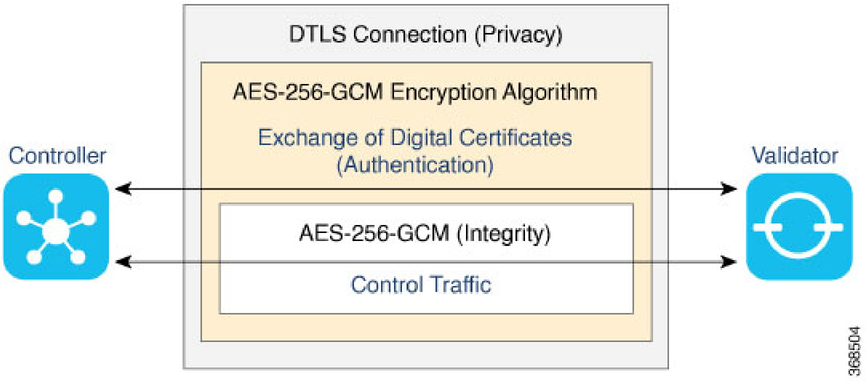
Control Plane Security Overview

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 Catalyst 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 SD-WAN Controller, which is the centralized brain of the Cisco Catalyst SD-WAN solution, establishes and maintains DTLS or TLS connections to all Cisco Catalyst SD-WAN devices in the overlay network—to the routers, the Cisco SD-WAN Validator, to Cisco SD-WAN Manager, and to other Cisco SD-WAN Controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Cisco Catalyst 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. For information about how Cisco SD-WAN Manager communicates with devices and controllers, see Cisco Catalyst SD-WAN Manager in the *Cisco Catalyst SD-WAN Getting Started Guide*.

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 Catalyst 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 Catalyst SD-WAN Control Plane Overview


DTLS Connection (Privacy)
AES-256-GCM Encryption Algorithm
Exchange of Digital Certificates (Authentication)
Controller
Validator
AES-256-GCM (Integrity)
Control Traffic
368504

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.

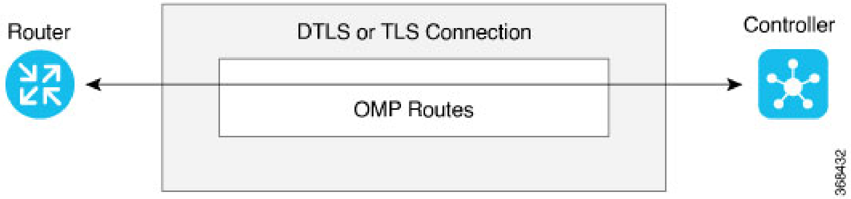
DTLS and TLS Infrastructure

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

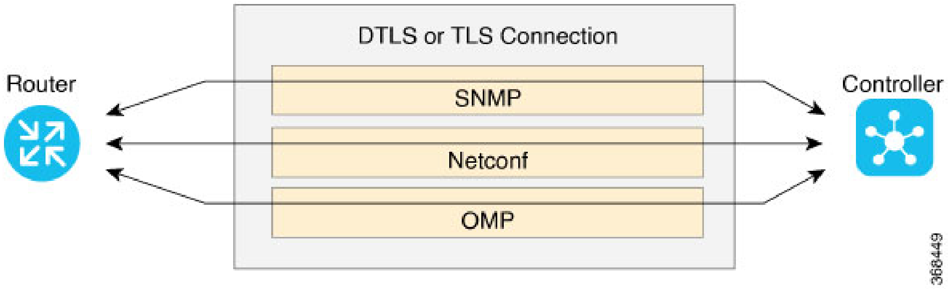
The first is the DTLS protocol, which is a transport privacy protocol for connectionless datagram protocols such as UDP, provides the foundation for the Cisco Catalyst SD-WAN control plane infrastructure. It is based on the stream-oriented Transport Layer Security (TLS) protocol, which provides security for TCP-based traffic. (TLS itself evolved from SSL.) The Cisco Catalyst 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 Catalyst 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 Catalyst SD-WAN software implements the standard version defined in RFC 5246. As described in the RFCs, Cisco Catalyst SD-WAN uses DTLS and TLS versions 1.2.



In the Cisco Catalyst SD-WAN architecture, the Cisco Catalyst SD-WAN devices use DTLS or TLS as a tunneling protocol, which is an application-level (Layer 4) tunneling protocol. When the Cisco SD-WAN Controller, Cisco SD-WAN Validator, Cisco SD-WAN Managers, 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 Cisco SD-WAN Controller, and those between the Cisco SD-WAN Validator and Cisco SD-WAN Controller, 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 Catalyst SD-WAN devices to transport their traffic. For example, an OMP session on a router communicates with an OMP session on a Cisco SD-WAN Controller by sending plain IP traffic through the secure DTLS or TLS tunnel between the two devices. The Overlay Management Protocol is the Cisco Catalyst SD-WAN control protocol used to exchange routing, policy, and management information among Cisco Catalyst SD-WAN devices, as described in Overlay Routing Overview.



A Cisco Catalyst SD-WAN daemon running on each Cisco SD-WAN 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 Cisco SD-WAN Controller.

Control Plane Authentication

The Cisco Catalyst SD-WAN control plane uses digital certificates with 2048-bit RSA keys to authenticate the Cisco IOS XE Catalyst SD-WAN devices 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 IOS XE Catalyst SD-WAN device and cannot be retrieved from the Cisco IOS XE Catalyst SD-WAN device.
- **Certificates** signed by a root certification authority (CA)— The trust chain associated with the root CA needs to be present on all Cisco IOS XE Catalyst SD-WAN devices.

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

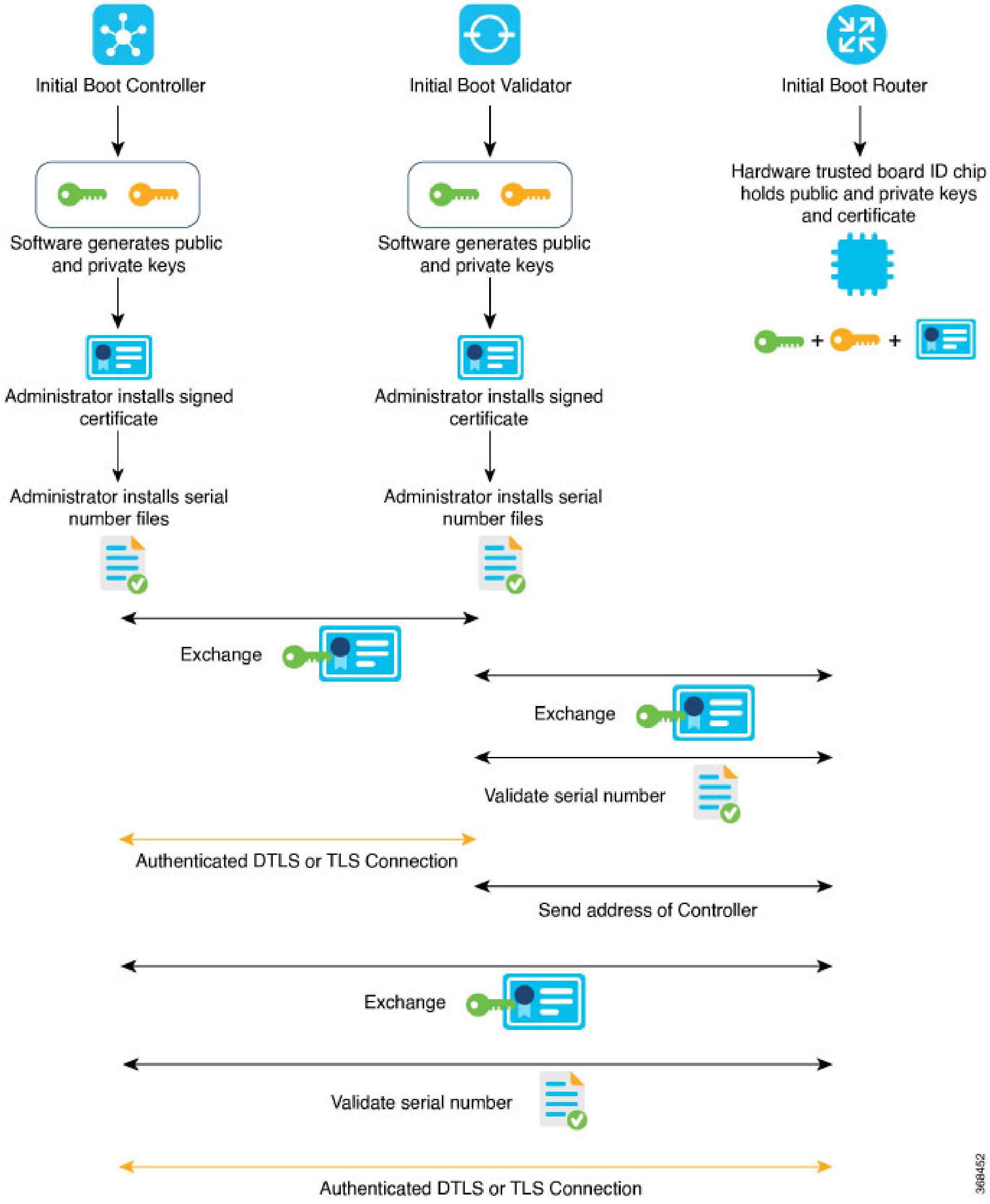
Let's first look at the PKI components that are involved in router authentication. On the Cisco IOS XE Catalyst SD-WAN device, the public and private keys and the certificates are managed automatically, by a hardware security chip that is built into the router called the Trust Anchor module (TAm). The 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 Catalyst 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 Cisco SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN Manager 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 Controller 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 Cisco SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN Manager systems. A typical network might have only a small handful of Cisco SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN Managers, 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 SD-WAN Manager 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 SD-WAN Manager. Cisco SD-WAN Manager then broadcasts this information to the other controllers. Both the authorized serial number file and the file listing the Cisco SD-WAN Controller serial numbers are uploaded and installed on Cisco Catalyst SD-WAN Validators. 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 Cisco SD-WAN Controller authorized serial numbers using the **show control valid-vsmarts** command on a Cisco SD-WAN Controller and the **show orchestrator valid-vsmarts** command on a Cisco Catalyst SD-WAN Validator. You can also run **show sdwan control valid-vsmarts** on Cisco IOS XE Catalyst SD-WAN devices. You can display the installed router authorized serial and chassis number associations using the **show control valid-vedges** command on a Cisco SD-WAN Controller and the **show orchestrator valid-devices** command on a Cisco Catalyst SD-WAN Validator.

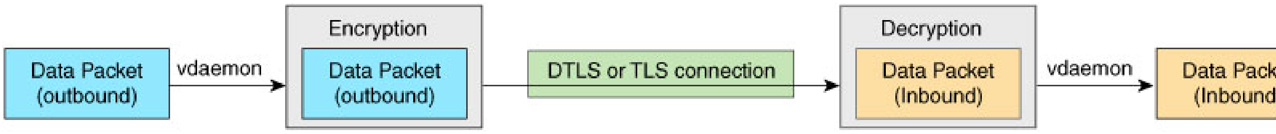
Now, let's look at how the PKI authentication components and the router serial and chassis numbers are used to authenticate router on the Cisco SD-WAN Controller overlay network. When Cisco SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and routers first boot up, they establish secure DTLS or TLS connections between the Cisco SD-WAN 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 Controller devices boot. For details about the authentication that occurs during the bringup process, see Bringup Sequence of Events.


Initial Boot Controller
Initial Boot Validator
Initial Boot Router
Software generates public and private keys
Software generates public and private keys
Hardware trusted board ID chip holds public and private keys and certificate
+
+
Administrator installs signed certificate
Administrator installs signed certificate
Administrator installs serial number files
Administrator installs serial number files
Exchange
Exchange
Validate serial number
Authenticated DTLS or TLS Connection
Send address of Controller
Exchange
Validate serial number
Authenticated DTLS or TLS Connection
368452

Control Plane Encryption

Control plane encryption is done by either DTLS, which is based on the TLS protocol, or TLS. These protocol encrypt the control plane traffic that is sent across the connections between Cisco Catalyst 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 Catalyst SD-WAN device can have DTLS or TLS connections to multiple Cisco Catalyst 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 Cisco SD-WAN Controller. Similarly, a Cisco SD-WAN Controller would have one kernel route and one DTLS or TLS connection for each router in its domain.



Control Plane Integrity

The Cisco Catalyst 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 Catalyst 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.

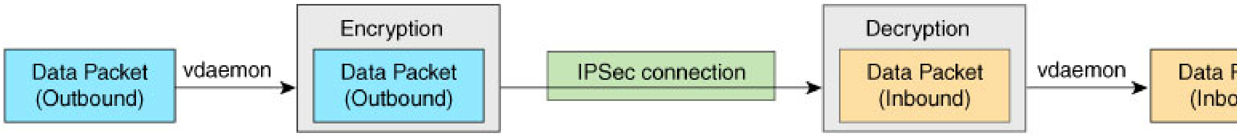
Data Plane Security Overview

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 Catalyst 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 Catalyst 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 Catalyst SD-WAN overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Cisco Catalyst 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 Catalyst SD-WAN Data Plane Overview



- Authentication: As mentioned, the Cisco Catalyst 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 Catalyst SD-WAN Controller sends IPsec encryption keys to each edge device.

    In the pairwise keys model, the Cisco SD-WAN 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 350.
  - By default, IPsec tunnel connections use an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels.
- Encryption: An enhanced 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:
  - An enhanced version of the ESP protocol encapsulates the payload of data packets.
  - The enhanced version of ESP uses an AH-like mechanism to check the integrity of the outer IP and UDP headers. You can configure the integrity methods supported on each router, and this information is exchanged in the router's TLOC properties. If two peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.
  - The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

Data Plane Authentication and Encryption

During the bringup of the overlay, the Cisco Catalyst SD-WAN 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 Catalyst SD-WAN 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.

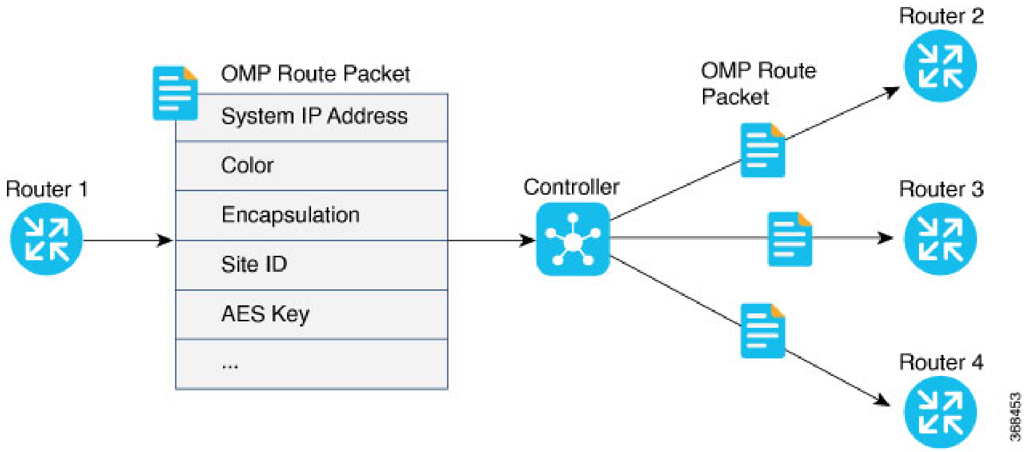
The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- 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 Catalyst 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 Catalyst SD-WAN solution takes advantage of the fact that the DTLS control plane connections in the Cisco Catalyst SD-WAN overlay network are known to be secure. Because the Cisco Catalyst 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 Catalyst 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 Cisco SD-WAN Controller in OMP route packets, which are similar to IP route updates. These packets contain information that the Cisco SD-WAN 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 Cisco SD-WAN 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 Catalyst SD-WAN Controller.

In Cisco SD-WAN Release 19.2.x and Cisco IOS XE SD-WAN Release 16.12.x onwards, Cisco Catalyst 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 Cisco SD-WAN Controller for distribution to all other edge devices. For more information, see IPsec Pairwise Keys, on page 349



If control policies configured on a Cisco SD-WAN Controller limit the communications channels between network devices, the reachability advertisements sent by the Cisco SD-WAN 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 Catalyst 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 Cisco SD-WAN Controllers. If data connectivity between two peers is lost, the exchange of BFD packets stops, and from this, the Cisco SD-WAN 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 Catalyst 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 Catalyst 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

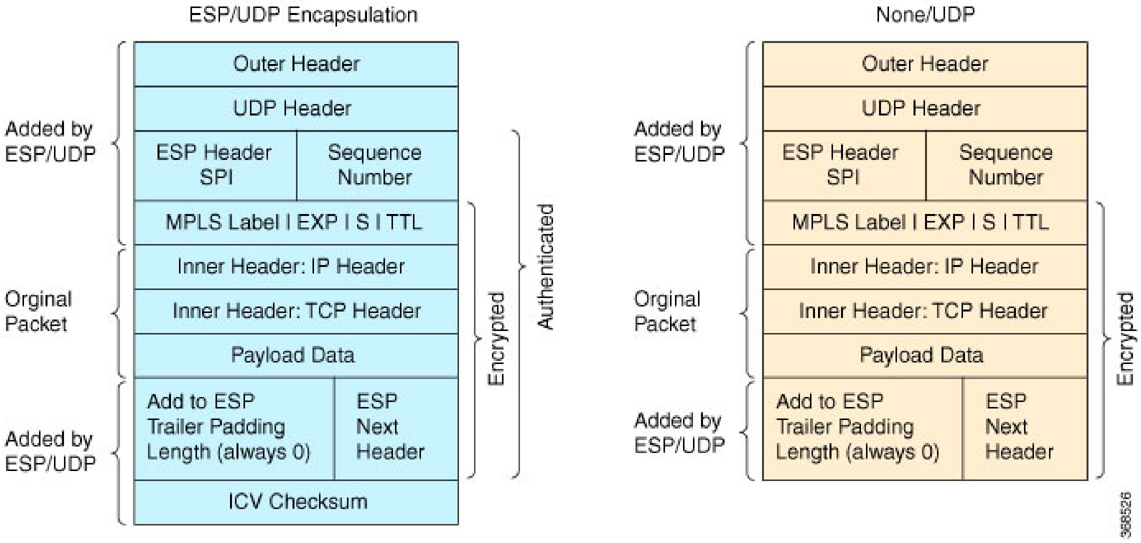
The following components contribute to the integrity of data packets in the Cisco Catalyst SD-WAN data plane:

- UDP – Encapsulate ESP within UDP packets per RFC 3948, UDP Encapsulation of IPsec ESP packets.
- 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. SDWAN complies with RFC 4303, IP Encapsulating Security Payload (ESP).
- Enhancements 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.

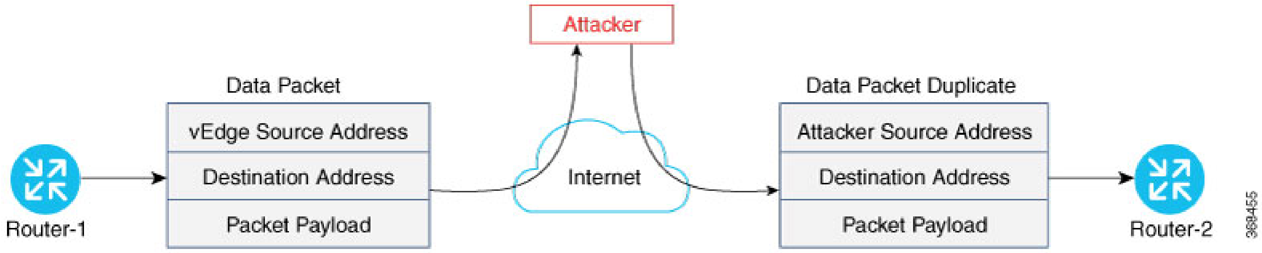
In the Cisco Catalyst SD-WAN solution, there are also enhancements to ESP to enhance its behavior to cover more of the datagram. These enhancements are similar to the way that AH works. This enhancement performs a checksum that includes calculating the checksum over all the fields in the packet—the payload, 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 enhanced 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.

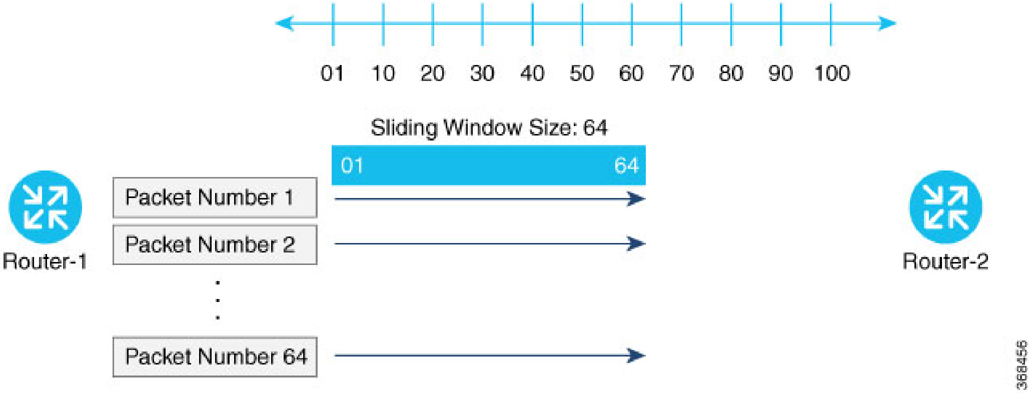


Note that Cisco Catalyst SD-WAN devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the digest. Both are distributed as part of the TLOC properties for a router.

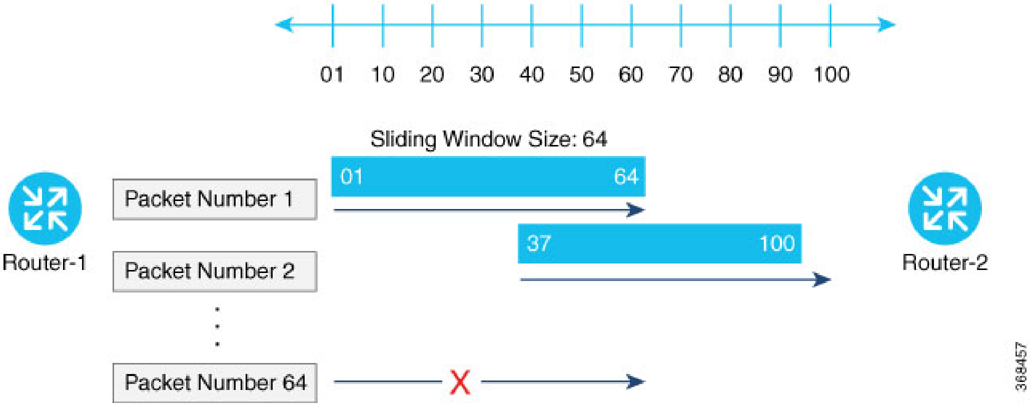
Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this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



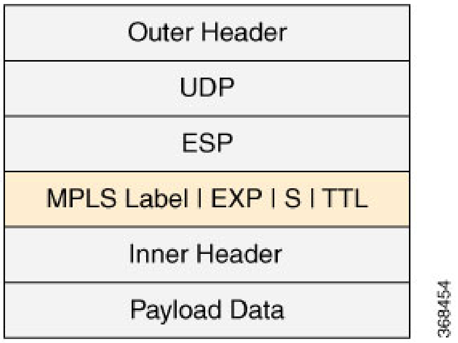
As a counter to such attacks, the Cisco Catalyst SD-WAN overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets.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

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

Feature	Description
Enterprise Firewall with Application Awareness, on page 44	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 143	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 159	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 169	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 203	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. Cisco SD-WAN Manager 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 Cisco SD-WAN Manager 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 and 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 Cisco SD-WAN Manager and Cisco SD-WAN 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 Catalyst SD-WAN overlay network.

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 Cisco SD-WAN Controller to be a server, firewalls protect TCP servers better than UDP servers.

You configure the control plane tunnel protocol on a Cisco SD-WAN Controller:

```
vSmart(config)# security control protocol tls
```

With this change, all control plane tunnels between the Cisco SD-WAN Controller and the routers and between the Cisco SD-WAN Controller and Cisco SD-WAN Manager use TLS. Control plane tunnels to Cisco Catalyst SD-WAN Validator always use DTLS, because these connections must be handled by UDP.

In a domain with multiple Cisco SD-WAN Controllers, when you configure TLS on one of the Cisco SD-WAN 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 Cisco SD-WAN Controllers, if you have not configured TLS on them, they use TLS on the control plane tunnel only to that one Cisco SD-WAN Controller, and they use DTLS tunnels to all the other Cisco SD-WAN Controllers and to all their connected routers. To have all Cisco SD-WAN Controllers use TLS, configure it on all of them.

By default, the Cisco SD-WAN 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 Cisco SD-WAN Controller. For example:

```
vSmart-2# show control connections

                                                            PEER                  PEER
PEER    PEER     PEER           SITE   DOMAIN  PEER         PRIVATE  PEER         PUBLIC
TYPE    PROTOCOL SYSTEM IP      ID     ID      PRIVATE IP   PORT     PUBLIC IP    PORT
REMOTE COLOR  STATE  UPTIME
------------------------------------------------------------------------------------------
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                  PEER
PEER     PEER     PEER           SITE   DOMAIN  PEER         PRIVATE  PEER         PUBLIC
TYPE     PROTOCOL SYSTEM IP      ID     ID      PRIVATE IP   PORT     PUBLIC IP    PORT
 REMOTE COLOR  STATE   UPTIME
------------------------------------------------------------------------------------------
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 SD-WAN Manager

If you configure the Cisco SD-WAN Manager 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 SD-WAN Manager. To display information about these processes and about and 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
INDEX INTERFACE IP           PORT   IP             PORT    VSMARTS  VMANAGES COLOR  CARRIER
  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 SD-WAN Manager 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 SD-WAN Manager, up to a maximum of 8.

Configure Security Parameters Using the Security Feature Template

Use the Cisco Security feature template for all Cisco IOS XE Catalyst SD-WAN devices. On the edge routers and on Cisco SD-WAN Validator, use this template to configure IPsec for data plane security. On Cisco SD-WAN Manager and Cisco SD-WAN Controller, use the Security feature template to configure DTLS or TLS for control plane security.

Configure Security Parameters

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

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

3. From the Devices list in the left pane, choose a device.

   The templates applicable to the selected device appear in the right pane.
4. Click **Cisco Security** to open the template.
5. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
6. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 2:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure Control Plane Security

Note The Configure Control Plane Security section is applicable to Cisco SD-WAN Manager and Cisco SD-WAN Controller only.

To configure the control plane connection protocol on a Cisco SD-WAN Manager instance or a Cisco SD-WAN Controller, choose the **Basic Configuration** area and configure the following parameters:

Table 3:

Parameter Name	Description
Protocol	Choose the protocol to use on control plane connections to a Cisco SD-WAN Controller: • DTLS (Datagram Transport Layer Security). This is the default. • TLS (Transport Layer Security)
Control TLS Port	If you selected TLS, configure the port number to use:*Range:* 1025 through 65535*Default:* 23456

Click **Save**

Configure Data Plane Security

Configure various data plane security parameters under the relevant areas of the template:

Table 4: Basic Configuration

Parameter Name	Description
Rekey Time	Specify how often a device changes the AES key used on its secure DTLS connection to the Cisco SD-WAN Controller. If OMP graceful restart is enabled, the rekeying time must be at least twice the value of the OMP graceful restart timer.*Range:* 10 through 1209600 seconds (14 days) *Default:* 86400 seconds (24 hours)
Replay Window	Specify the size of the sliding replay window. *Values:* 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets. *Default:* 512 packets
Extended Anti Replay	This is turned off by default. Click **On** to turn it on.
IPsec pairwise-keying	This is turned off by default. Click **On** to turn it on.

Table 5: Authentication Type

Parameter Name	Description
Authentication Type	Select the authentication types from the **Authentication List**, and click the arrow pointing right to move the authentication types to the **Selected List** column. Authentication types supported from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a: • **esp**: Enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header. • **ip-udp-esp:** Enables ESP encryption. In addition to the integrity checks on the ESP header and payload, the checks also include the outer IP and UDP headers. • **ip-udp-esp-no-id**: Ignores the ID field in the IP header so that Cisco Catalyst SD-WAN can work in conjunction with the non-Cisco devices. • **none**: Turns integrity checking off on IPSec packets. We don't recommend using this option. Authentication types supported in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and earlier: • **ah-no-id**: Enable an enhanced version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the packet's outer IP header. • **ah-sha1-hmac**: Enable AH-SHA1 HMAC and ESP HMAC-SHA1. • **none**: Select no authentication. • **sha1-hmac**: Enable ESP HMAC-SHA1. **Note** For an edge device running on Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or earlier, you may have configured authentication types using a **Cisco Security** template. When you upgrade the device to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, update the selected authentication types in the **Cisco Security** template to the authentication types supported from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a . To update the authentication types, do the following: 1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**. 2. Click **Feature Templates**. 3. Find the **Cisco Security** template to update and click … and click **Edit**. 4. Click **Update**. Do not modify any configuration. Cisco SD-WAN Manager updates the **Cisco Security** template to display the supported authentication types.

Key Chain and Key ID

To add a new key chain, click **New Key Chain** and specify the following:

Table 6: Key Chain

Parameter Name	Description
Keychain Name	Enter a name for the key chain
Key ID	Specify a key ID

Click **Save**.

Configure Data Plane Security Parameters

In the data plane, IPsec is enabled by default on all routers, and by default IPsec tunnel connections use an enhanced 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 Catalyst SD-WAN Release 17.6.1a and Later

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco 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 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 Catalyst SD-WAN software ignore the ID field in the IP header so that the Cisco Catalyst 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 an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication. To modify the negotiated interity types, use the following command:

When you change the authentication-type from CLI, the configuration change works well but the new authentication-change doesn't show in the running configuration. We recommend you to change the authentication type to integrity type from Cisco SD-WAN Manager during the template push.

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

Authentication Types Before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

By default, IPsec tunnel connections use an enhanced 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 Catalyst 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 Catalyst 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 Catalyst SD-WAN AH software ignore the ID field in the IP header so that the Cisco Catalyst SD-WAN software can work in conjunction with these devices.
- **sha1-hmac** enables ESP encryption and integrity checking.

For information about which data packet fields are affected by these authentication types, see Data Plane Integrity, on page 15.

Cisco IOS XE Catalyst 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.

For the unicast traffic, the encryption algorithm on IPSec tunnel connections is AES-256-GCM. From Cisco IOS XE SD-WAN Release 17.2.1r, the multicast traffic also supports AES-256-GCM encryption algorithm. You cannot modify the encryption algorithm choice made by the software.

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

Change the Rekeying Timer

Before Cisco IOS XE Catalyst 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

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

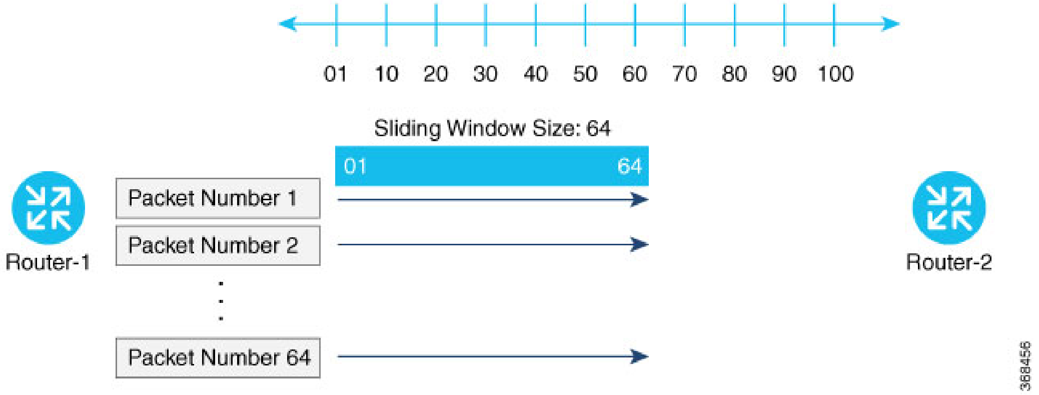
After the new key is generated, the router sends it immediately to the Cisco SD-WAN Controllers using DTLS or TLS. The Cisco SD-WAN Controllers send the key to the peer routers. The routers begin using it as soon as they receive it. Note that the key associated with the old SPI (256) will continue to 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.

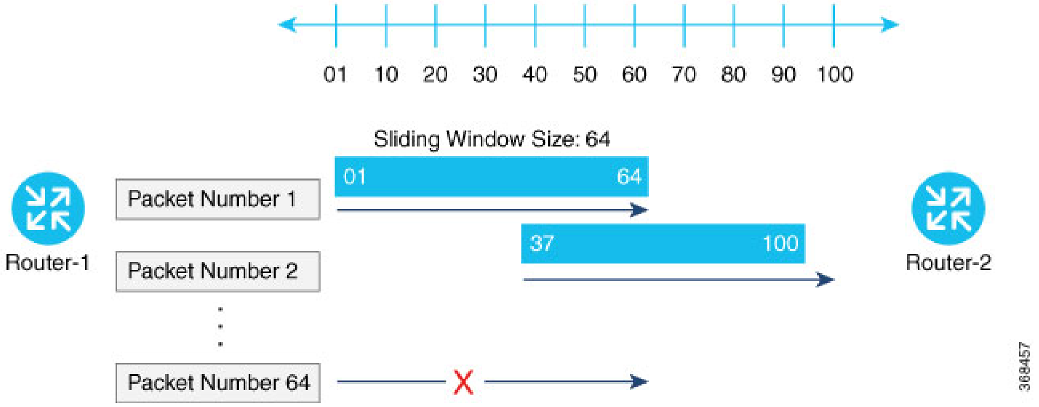
```
Device# request platform software sdwan security ipsec-rekey
Device# request platform software sdwan security ipsec-rekey
Device# show sdwan ipsec local-sa
                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
------------------------------------------------------------------------------
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 Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. In Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

In controller mode, only Route based IPSec tunnels are supported.

Create VPN IPsec Interface Template

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Choose a Cisco IOS XE Catalyst 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	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. Upload the CSV file when you attach a device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

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 Internet Key Exchange (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. *Default*: group-16

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, as part of the security hardening, the weaker ciphers are deprecated. As part of this change, the option to configure Diffie-Hellman (DH) groups 1, 2, and 5 is no longer supported. DH groups are used in IKE to establish session keys and are also available in IPsec as support for perfect forward secrecy.

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
```

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

Parameter Name	Description
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 7: Feature History

Feature Name	Release Information	Description
SHA256 Support for IPSec Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for `HMAC_SHA256` 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 Catalyst 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. *Default*: IKEv1 **Note** In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Parameter Name	Options	Description
IKE Mode	**Aggressive mode** **Main mode**	For IKEv1 only, specify one of the following modes: • Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear. • Establishes an IKE SA session before starting IPsec negotiations. **Note** For IKEv2, there is no mode. **Note** IKE aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen. *Default*: Main mode
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. *Range*: 1 hour through 14 days *Default*: 14400 seconds (4 hours)
IKE Cipher Suite	• AES 256 CBC SHA 256 • AES 256 CBC SHA 384 • AES 256 CBC SHA 512 • AES 256 CBC SHA 1 • AES 256 GCM • Nul SHA 256 • Nul SHA 384 • Nul SHA 512 • Nul SHA 1	Specify the type of authentication and encryption to use during IKE key exchange. *Default*: AES 256 CBC SHA 1

Parameter Name	Options	Description
IKE Diffie-Hellman Group	**2** **14** **15** **16**	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 1024-bit modulus • 2048-bit modulus • 3072-bit modulus • 4096-bit modulus *Default*: 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. *Range*: 1 through 64 characters *Default*: Tunnel's source IP address
	IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. *Range*: 1 through 64 characters *Default*: Tunnel's destination IP address

Note When you are pushing authentication from Cisco SD-WAN Manager, use the authentication string configured for the source and destination stations in double quotes as special characters are not supported. The string can be up to eight characters long.

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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and then click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Choose the device for which you are creating the template.
4. Click **Basic Configuration**.
5. Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.
6. Remove the ISAKMP profile from the IPsec profile.
7. Attach the IKEv2 profile with the IPsec profile.

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

8. Use the **shutdown** parameter with the **no** option (**no shutdown**) to start up the tunnel.

   Note You must issue the **shutdown** operations in two separate operations.

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

CLI Equivalents for IKEv1

ISAKMP CLI Configuration for IKEv1

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

IPsec CLI Configuration for IKEv1

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

Summary Steps

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

CLI Equivalent for IKE2

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

Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager	Cisco vManage Release 20.9.1	This feature allows you to disable weaker SSH algorithms on Cisco SD-WAN Manager that may not comply with certain data security standards.

Information About Disabling Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Cisco SD-WAN Manager provides an SSH client for communication with components in the network, including controllers and edge devices. The SSH client provides an encrypted connection for secure data transfer, based on a variety of encryption algorithms. Many organizations require stronger encryption than that provided by SHA-1, AES-128, and AES-192.

From Cisco vManage Release 20.9.1, you can disable the following weaker encryption algorithms so that an SSH client does not use these algorithms:

- SHA-1
- AES-128
- AES-192

Before disabling these encryption algorithms, ensure that Cisco vEdge devices, if any, in the network, are using a software release later than Cisco SD-WAN Release 18.4.6.

Note You cannot change the SSH KEX and cipher algorithms on the Cisco SD-WAN Controller and the Cisco Catalyst SD-WAN Validator through the CLI. It is only supported on Cisco SD-WAN Manager.

Benefits of Disabling Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Disabling weaker SSH encryption algorithms improves the security of SSH communication, and ensures that organizations using Cisco Catalyst SD-WAN are compliant with strict security regulations.

Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager Using CLI

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Choose the Cisco SD-WAN Manager device on which you wish to disable weaker SSH algorithms.
3. Enter the username and password to log in to the device.
4. Enter SSH server mode.

```
vmanage# config terminal
vmanage(config)# system
vmanage(config-system)# ssh-server
```

5. Do one of the following to disable an SSH encryption algorithm:
   - Disable SHA-1:
     a. `vmanage(config-ssh-server)# no kex-algo sha1`
     b. `vmanage(config-ssh-server)# commit`

     The following warning message is displayed:

```
The following warnings were generated:
'system ssh-server kex-algo sha1': WARNING: Please ensure all your edges run code
 version > 18.4.6 which negotiates better than SHA1 with vManage. Otherwise those
 edges may become offline.
Proceed? [yes,no] yes
```

c. Ensure that any Cisco vEdge devices in the network are running Cisco SD-WAN Release 18.4.6 or later and enter **yes**.

- Disable AES-128 and AES-192:

a. `vmanage(config-ssh-server)# no cipher aes-128-192`

b. `vmanage(config-ssh-server)# commit`

The following warning message is displayed:

```
The following warnings were generated:
'system ssh-server cipher aes-128-192': WARNING: Please ensure all your edges
run code version > 18.4.6 which negotiates better than AES-128-192 with vManage.
 Otherwise those edges may become offline.
Proceed? [yes,no] yes
```

c. Ensure that any Cisco vEdge devices in the network are running Cisco SD-WAN Release 18.4.6 or later and enter **yes**.

Verify that Weak SSH Encryption Algorithms Are Disabled on Cisco SD-WAN Manager Using the CLI

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Select the Cisco SD-WAN Manager device you wish to verify.
3. Enter the username and password to log in to the device.
4. Run the following command:

```
show running-config system ssh-server
```

5. Confirm that the output shows one or more of the commands that disable weaker encryption algorithms:
   - no cipher aes-128-192
   - no kex-algo sha1

CHAPTER 5

Enterprise Firewall with Application Awareness

Enterprise Firewall with Application Awareness

Table 9: Feature History

Feature Name	Release Information	Feature Description
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW. IPv6 is supported for the following scenarios: • Creating firewall rules. For more information, see Create Rules, on page 48. • Creating firewall rulesets. For more information, see Create Rule Sets, on page 51. • Creating a unified security policy. For more information, see Unified Security Policy, on page 89. • Creating a identity based unified security policy. For more information, see Cisco Catalyst SD-WAN Identity-Based Firewall Policy, on page 115. • Firewall high speed logging. For more information, see Firewall High-Speed Logging, on page 74.
Match Traffic Using Custom Applications	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	Added support for matching traffic using a custom application in a custom-defined application list.

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

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.

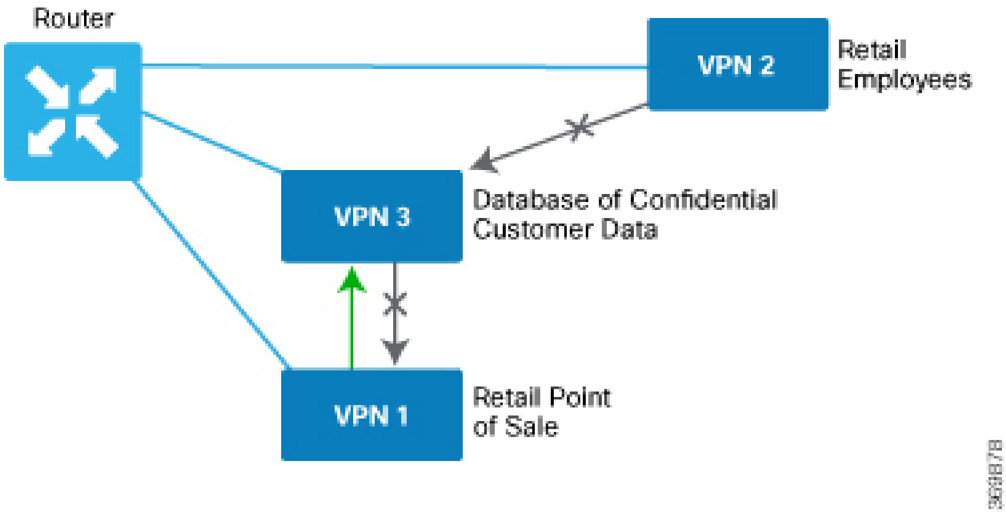
Zone configuration consists of the following components:

- 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 Catalyst SD-WAN Release 16.12.2r and onwards, Cisco Catalyst SD-WAN Manager 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 Catalyst 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 SD-WAN Manager.
- For packets coming from Overlay to Service side, 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 Catalyst 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 behavior is expected with policy-based routing configuration, and below are the examples of such a configuration.

Configuration	Command
Data policy: switching the VPN	`set-vpn`
Control policy and data policy: service chaining	`set service`

- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can configure geolocation and multiple list features in security policy on the edge devices. You can attach the security policy that has multiple list or geolocation feature enabled, only when the device is online with control connections up.

- The Application Layer Gateway (ALG) for L7 protocols causes traffic drop due to zone-based firewall inspection. If an application is running on a registered port which is assigned to another application, the traffic drops. For example, connection oriented syslog running on TCP port 514 which is assigned to another application drops. In such situations, disable application inspection or use a different port.
- Configuring service engine interfaces as a zone-member is not supported for releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a. You must disable ZBFW or configure zone for VPN0 to VPN1 to allow the traffic.
- (Cisco Catalyst SD-WAN Manager Release 20.13.1 and earlier) When creating a security policy do not match traffic using a user-defined application list that includes a user-defined custom application.

  From Cisco Catalyst SD-WAN Manager Release 20.14.1, using a user-defined application list that includes a user-defined custom application is supported. However, the custom application cannot use IPv6 addresses in its match criteria.

Configure Firewall Policies

In Cisco SD-WAN Manager, 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 SD-WAN Manager 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 SD-WAN Manager 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.

.

Start the Security Policy Configuration Wizard

To start the policy configuration wizard:

1. From the Cisco SD-WAN Manager 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 10: Feature History

Feature Name	Release Information	Description
Firewall FQDN Support	Cisco IOS XE Catalyst SD-WAN 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.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.

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 FQDNs 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
- If you choose the IP address type as IPv6 while creating a firewall rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list of Source Data Prefix(es). Additionally, Application Layer Gateway (ALG) is not supported for IPv6.

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 SD-WAN Manager, 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. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.
8. Choose an action for the rule:
   - **Inspect**
   - **Pass**
   - **Drop**
9. If you want matches for this rule to be logged, check the **Log** check box.

10. Configure one or more of the following fields.

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

Table 11: Firewall Rules

Field	Description
Source Data Prefixes	IPv4 prefixes or IPv6 prefixes or prefix lists and/or domain names (FQDN) or list(s). Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Source Data Prefixes** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list of Source Data Prefix(es). Additionally, Application Layer Gateway (ALG) is not supported for IPv6.
Source Port(s)	Source port(s) and/or lists
Destination Data Prefix(es)	IPv4 prefixes or prefix list(s) and/or domain names (FQDN) or list(s) Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Destination Data Prefix(es)** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list. Additionally, ALG is not supported for IPv6.
Destination Ports	Destination ports and/or lists **Note** Destination ports or destination port lists cannot be used with protocols or protocol lists.
Protocol(s)	Protocols and/or list(s)
Application List(s)	Applications and/or lists **Note** If you chose an Application or Application Family List, you must choose at least one other match condition. **Note** See the information about custom applications in Restrictions, on page 46.

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

Create Rule Sets

Table 12: Feature History

Feature Name	Release Information	Description
Support for Rule Sets	Cisco IOS XE Catalyst SD-WAN 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 reuse rule sets between security policies.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.

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. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.
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. Click + next to Rule Sets.
10. Choose from existing rule sets or click **+ New List** to create a new list.
    - To choose from an existing rule: click the existing rule(s) and click **Save**.
    - To create a new rule list **Cick + New List**.
      a. Configure a rule using one or more of the following fields.

Table 13: Firewall Rules

Field	Description
Source Data Prefix(es)	IPv4 prefixes or prefix lists and/or domain names (FQDN) or list(s) Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Source Data Prefixes** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list of Source Data Prefix(es). Additionally, Application Layer Gateway (ALG) is not supported for IPv6.
Source Port(s)	Source port(s) and/or list(s)
Destination Data Prefix(es)	IPv4 prefixes or prefix lists and/or domain names (FQDN) or list(s) Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Destination Data Prefix(es)** field displays the prefix options. **Note** If you choose the IP address type as IPv6 while creating the rule, FQDN, Identity (user and SGT) and geo filtering options are not available in this list. Additionally, ALG is not supported for IPv6.
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)	Protocols and/or lists
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. **Note** See the information about custom applications in Restrictions, on page 46.

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

c. (Optional) Add more rules by repeating steps 7 and 8.

11. Click **Save** to save the rule set.
12. Click + next to Application List To Drop.
13. Choose existing lists or create your own.
14. Click **Save**.
15. Review the rule set and click **Save**.
16. (Optional) Create additional rule sets or reorder the rule sets and/or rules if required.
17. Click **Save Firewall Policy**.

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

1. From the Cisco SD-WAN Manager 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. When 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 14: Feature History

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco IOS XE Catalyst 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 Catalyst 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 SD-WAN Manager. 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.

Configure Interface Based Zones and Default Zone

Table 15: Feature History

Feature Name	Release Information	Description
Configure Interface Based Zones and Default Zone	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to configure an interface-based firewall policy to control traffic between two interfaces or an interface-VPN-based firewall policy to control traffic between an interface and a VPN group. This feature also provides support for default zone where a firewall policy can be configured on a zone pair that consist of a zone and a default zone.

Restrictions for Interface Based Zones, Default Zone and Self Zone

- Port-channel does not support interface-based zone.
- Interface-based firewall policies and default zone can be configured only for unified security policies and on Cisco IOS XE Catalyst SD-WAN devices only.

  Interface types are not listed on the selected device model. You must manually enter the correct interface type and interface name for a device model.
- A default zone cannot be configured as both the source and the destination zone in a zone-pair.
- When the WAN interface is added to a zone, overlay traffic going over the WAN interface is not included for inspection. The corresponding tunnel interface created on the device must be added to a zone and a policy must be configured for the traffic flow.
- Interfaces belonging to different VPNs cannot be included in the same zone. Create separate zones for interfaces attached to each VPN.
- For Overlay traffic, tunnel interfaces corresponding to the physical interfaces must be used. For underlay traffic, you must add the physical interface as part of a zone. All other logical interfaces can be used as it is for the overlay traffic (for example ipsec1, gre1).
- When creating a zone-member interface, if the physical interface is not present on the device, then Cisco Catalyst SD-WAN Manager doesn't show any errors but this zone-member CLI is ignored. Ensure that there are no typos in the interface name when you enter it manually for the zone.
- When you define a class-map, you can specify an optional type. Generally, firewall uses class-map type inspect, but for application recognition, you can use a simple class-map with no type. If a class-map without a type is specified, then it requires NBAR to determine the application. NBAR is not run on traffic destined to the control plane (self zone) so the application cannot be determined. So, only class-map with a type of inspect should be used for zone pairs to or from the self zone.

Information About Interface Based Zones and Default Zone

Zone-based Firewall (ZBFW) is implemented by applying firewall policy to a zone pair. A zone pair allows users to specify a firewall policy between a source zone and a destination zone. From Cisco vManage Release 20.7.1, Cisco Catalyst SD-WAN supports interface-based ZBFW policy to restrict traffic between two interfaces. In addition, configuration of a default zone is supported.

Interface Based Zones

You configure ZBFW policy where you assign interfaces to zones, and apply inspection policies to traffic between the zones. For the same interface, there can be an interface-based policy and a VPN-based policy (where the interface is part of the VPN). In this case, the interface-based policy takes precedence over the VPN-based policy. In addition, an interface-based zone can also be paired with a VPN-based zone and vice versa.

Zones establish the security borders of your network. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. ZBFW's default policy between zones is deny all. If no policy is explicitly configured, all traffic between zones is blocked.

For VPN-based zones, on systems without a dedicated management interface, such as Aggregation Services Routers (ASRs), the management interface should be put into its own interface zone. The traffic going through the management port is combined with the general internet traffic. If you create a zone associated with VPN_0 and pairs it with self zone in zone-pair where the policy denies traffic, the traffic from the management port is also denied.

Default Zone

A default zone enables a firewall policy to be configured on a zone pair that consist of a zone and a default zone. You can configure a policy from a zone to a default zone, or vice versa. In Cisco Catalyst SD-WAN, any VPN or interface without an explicit zone assignment belongs to a default zone.

Rules For Traffic Flow Between Two Interfaces

- For source zones:
    - If an interface is assigned to a zone, then consider interface-zone as a source zone; or,
    - If a VPN is assigned to a zone, then consider VPN-zone as a source zone.
    - If neither the interface nor VPN is assigned to zones, then the default zone is considered as a source zone.
- For destination zones:
    - If interface is assigned to a zone, then consider interface-zone as a destination zone; or,
    - If VPN assigned to a zone, then consider VPN-zone as a destination zone.
    - If neither interface nor VPN is assigned to zones, then the default zone is considered as a destination zone.
- If a policy is configured for a zone pair of source zone and a destination zone which are based on the above rules, a zone-pair policy can be applied.
- If no policy is configured for the zone pair of source zoneand destination zone, packets are dropped.

- A default zone cannot be configured as both source and destination zone in a zone-pair.
- If one of the zone pair is default zone and the other is self zone, packets are passed without inspection by default unless default zone is explicitly provisioned.
- If only one of the zone pair is a default zoneand the other is not self zone, packets are dropped by default unless default zone is explicitly provisioned.

Benefits of Interface Based Zones and Default Zone

Interface-based zone policies offer flexibility and granularity for policy configuration. Different inspection policies can be applied to multiple host groups connected to the same interface.

Use Case for Interface Based Zones and Default Zone

- Configure ZBFW policy at an interface level instead of a zone level. You can apply a firewall policy from a source zone to a destination zone, where one of the zones, or both zones can be an interface-only zone.
- Configure a ZBFW policy when you have the source zone as interface type and the destination zone as a VPN type.
- Configure a ZBFW policy where different interfaces in the same VPN can be assigned to different zones.
- Enable the default zone policy for an interface and VPN.

Configure Interface Based Zones and Default Zone

To configure Interface Based Zones and Default Zones in Cisco SD-WAN Manager, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Unified Security Policy**.

   For information on configuring a unified security policy, see Configure Firewall and Unified Security Policy.

   After you have created a firewall policy, click to add a zone pair for the firewall policy.
3. In the **Add NG Firewall Policy** page, click **zoneBasedFW** to create a zone list.

   The **Zone List** page displays
4. Enter a name for the zone.
5. Click a zone type.

   You can choose to configure zones with zone type as **Interface** or as a **VPN**. Based on the zone type you choose, add the interfaces or VPNs to the zones.
6. Click **Save** to save the zone list.
7. In the **Add NG Firewall Policy** page, click **Add Zone-Pairs**.
8. In the **Source Zone** drop-down list, choose the zone that is the source of the data packets.
9. In the **Destination Zone** drop-down list, choose the zone that is the destination of the data packets.

Note Default zone appears in the drop-down list while selecting a zone as part of zone-pair. You can choose default zone for either a source zone or a destination zone, but not both.

10. Click + icon to create a zone pair.

11. Click **Save**.

You configure Interface Based Zones and Default Zone using a CLI device template in Cisco SD-WAN Manager. For information about using a device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices.

To configure Interface Based Zones and Default Zone using the CLI add-on feature template. For information on using the CLI Add-On template, see Create a CLI Add-On Feature Template.

Configure Interface Based Zones and Default Zone Using the CLI

This section provides example CLI configurations for Interface Based Zones and Default Zones.

VPN Zone to Interface Zone

```
object-group network nw192_13
 192.168.13.0 255.255.255.0
object-group service prot_ip
 ip
ip access-list extended acl_192_13
 10 permit object-group prot_ip object-group nw192_13 any
parameter-map type inspect-global
 vpn zone security
class-map type inspect match-any cm_192_13
 match access-group name acl_192_13
policy-map type inspect pm_192
 class type inspect cm_192_13
  inspect
 class class-default
 vpn zone security
zone security intf3
zone security vpn0
 vpn 0
zone-pair security int13_vpn0 source intf3 destination vpn0
 service-policy type inspect pm_192
interface GigabitEthernet3.103
   encapsulation dot1Q 103
   vrf forwarding 3
   ip address 172.16.13.2 255.255.255.0
   ip mtu 1496
   zone-member security intf3
```

VPN Zone to Default Zone

```
object-group network nw_rest
 192.138.12.0 255.255.255.0
 192.168.12.0 255.255.255.0
class-map type inspect match-any cm_rest
 match access-group name acl_rest
policy-map type inspect pm_rest
 class type inspect cm_rest
  inspect
 class class-default
!
ip access-list extended acl_rest
 20 permit object-group prot_ip object-group nw_rest any
zone security default
zone security vpn0
 vpn 0
zone-pair security v0_def source default destination vpn0
 service-policy type inspect pm_rest
```

Interface Zone to Default Zone

```
object-group network nw192_13
 192.168.13.0 255.255.255.0
object-group service prot_ip
 ip
ip access-list extended acl_192_13
 10 permit object-group prot_ip object-group nw192_13 any
parameter-map type inspect-global
 vpn zone security
class-map type inspect match-any cm_192_13
 match access-group name acl_192_13
policy-map type inspect pm_192
 class type inspect cm_192_13
  inspect
 class class-default
 vpn zone security
zone security intf3
zone security default
zone-pair security int13_def source intf3 destination default
 service-policy type inspect pm_192
 zone-member security intf3
interface GigabitEthernet3.103
 encapsulation dot1Q 103
 vrf forwarding 3
 ip address 172.16.13.2 255.255.255.0
 ip mtu 1496
 zone-member security intf3
```

Interface Zone to Default Zone and VPN Zone to Default Zone

This is applicable when a interface is attached to a zone, but VRF/VPN also has a zone configured.

```
object-group network nw192_11
 192.168.11.0 255.255.255.0
class-map type inspect match-any cm192_11
 match access-group name acl_192_11
policy-map type inspect pm192_11
 class type inspect cm192_11
  inspect
 class class-default
!
ip access-list extended acl_192_11
 10 permit object-group prot_ip object-group nw192_11 any
zone security intf1
zone-pair security intf1_def source intf1 destination default
 service-policy type inspect pm192_11
interface GigabitEthernet3.101
 encapsulation dot1Q 101
 vrf forwarding 1
 ip address 172.16.11.2 255.255.255.0
 ip mtu 1496
 zone-member security intf1
vm5#sh run | sec vpn1
```

```
zone security vpn1
 vpn 1
zone-pair security vpn1_def source vpn1 destination default
 service-policy type inspect pm192_11
```

Configuration Example for Interface Based Zones and Default Zones

```
object-group network TEST-Rule_1-nw-dstn_
 10.0.12.0 255.255.255.0
!
object-group service TEST-Rule_1-svc_
 icmp
 tcp
 udp
!
object-group network TEST-Rule_2-nw-dstn_
 192.168.0.0 255.255.0.0
!
object-group service TEST-Rule_2-svc_
 ip
!
class-map type inspect match-all TEST-seq-11-cm_
 match access-group name TEST-seq-Rule_2-acl_
class-map type inspect match-all TEST-seq-1-cm_
 match access-group name TEST-seq-Rule_1-acl_
!
policy-map type inspect optimized TEST-opt
 class type inspect TEST-seq-1-cm_
  inspect
 class type inspect TEST-seq-11-cm_
  inspect
 class class-default
  drop
!


zone security DIA_INTF
zone security SRC_INTF1
zone security VPN2
 vpn 2
zone security default
zone-pair security ZP_SRC_INTF1_DIA_INTF_TEST source SRC_INTF1 destination DIA_INTF
 service-policy type inspect TEST-opt
zone-pair security ZP_VPN2_VPN2_TEST source VPN2 destination VPN2
 service-policy type inspect TEST-opt
zone-pair security ZP_default_DIA_INTF_TEST source default destination DIA_INTF
 service-policy type inspect TEST-opt
interface GigabitEthernet1
zone-member security DIA_INTF
!
interface GigabitEthernet2
zone-member security DIA_INTF
!
interface GigabitEthernet3.101
zone-member security SRC_INTF1
```

Monitor Interface Based Zones and Default Zone Using the CLI

Example 1

The following is sample output from the **show policy-firewall config** command to validate a configured zone based firewall.

```
Zone-pair              : ZP_SRC_INTF1_DIA_INTF_TEST
Source Zone            : SRC_INTF1
  Member Interfaces:
    GigabitEthernet3.101
Destination Zone       : DIA_INTF
  Member Interfaces:
    GigabitEthernet1
    GigabitEthernet2
    GigabitEthernet4
Service-policy inspect : TEST-opt
  Class-map : TEST-seq-1-cm_ (match-all)
   Match access-group name TEST-seq-Rule_1-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : TEST-seq-11-cm_ (match-all)
   Match access-group name TEST-seq-Rule_2-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

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 74.

   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 SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Device Templates**.

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

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

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 SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices.
3. 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 the 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 template or Cisco SD-WAN Manager.

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`

Note By default, subnet 192.168.1.1/30 and 192.0.2.1/30 used for VPG0 and VPG1 (UTD) and 192.168.2.1/24 used for VPG2 (APPQOE) is configured through Cisco SD-WAN Manager. Use any RFC 1918 subnet for Transport and Service VPN configurations other than these netmask.

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.

Configure Zone-based Firewall Policy Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure zone-based firewall policy.

Note By default, subnet 10.168.1.1/30 and 10.0.2.1/30 used for VPG0 and VPG1 (UTD) and 10.168.2.1/24 used for VPG2 (APPQOE) is configured through Cisco SD-WAN Manager. Use any RFC 1918 subnet for Transport and Service VPN configurations other than these netmask.

1. Create the inspect parameter map.

```
parameter-map type inspect-global
multi-tenancy
vpn zone security
alert on
log dropped-packets
max-incomplete tcptimeout
```

2. Create an employee zone.

```
zone security employee
vpn vpn-id
```

3. Create an internet zone.

```
zone security internet
vpn vpn-id
```

4. Configure the object group for the source addresses.

```
object-group networkgroup-name
hostip address
hostip address
hostip address
```

5. Configure the object group for the destination addresses.

```
object-group networkgroup-name
hostip address
hostip address
```

6. Configure the object group for the ports.

```
object-group networkgroup-name
tcp source eqrangeeqrange
udp source eqrangeeqrange
```

7. Create the IP access-list.

```
ip access-list extname
10denyobject-groupgroup-name1object-groupgroup-name2object-groupgroup-name3
```

8. Create the class map.

```
class-map type inspect match-allclass-map-name
match access-group nameaccess-group-name
```

9. Create the policy map that you want to add to the zone pair.

```
policy-map type inspectpolicy-map-name
classclass-map-name
drop
```

10. Create the zone pair and link the policy map to it.

```
zone-pair securityzone-pair
namesourcesource-zone-namedestinationdestination-zone-name
service-policy type droppolicy-map-name
```

Cisco SD-WAN Manager Configuration

To configure this zone-based firewall policy in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager 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.

Optimize Traffic Flow and Firewall Security in Cisco Catalyst SD-WAN with Cisco IOS XE Catalyst SD-WAN Device and VRRP

This use case illustrates the importance of proper configuration in maintaining traffic symmetry and ensuring the proper functioning of a zone-based firewall in a network setup using Cisco IOS XE Catalyst SD-WAN devices and Virtual Router Redundancy Protocol (VRRP).

In a network setup where the switch, hub router, and firewall are located at the same site with the goal of protecting servers from malware, maintaining traffic symmetry is critical. This setup involves Cisco IOS XE Catalyst SD-WAN devices and VRRP to control and manage the traffic flow.

To ensure traffic symmetry where data packets follow the same path from the source to the destination and back, by correctly configuring Cisco IOS XE Catalyst SD-WAN devices using VRRP, and adjusting the priority settings in these devices, a user can control which Cisco IOS XE Catalyst SD-WAN device acts as the master (Hub 1) and which one serves as the backup (Hub 2). This setup allows for effective management of traffic flow and maintenance of traffic symmetry.

With the correct configuration and priority settings, traffic symmetry is achieved. This setup enables the zone-based firewall to function effectively as it can inspect both incoming and outgoing traffic on the same path.

To achieve traffic symmetry in these scenarios, we can take the following steps:

1. In the event of a TLOC interface failure, VRRP continues to direct traffic to Hub 1 because it is configured as a master. As a result all the traffic that is directed to Hub 1 will be dropped. To prevent this scenario, using VRRP tracking allows the master to automatically switch from Hub 1 to Hub 2 if a TLOC interface fails. This is similar to the requirement to shut down OMP when a VRRP interface fails, to avoid traffic loss.

2. When setting up remote policies for branch locations, it is important to ensure that the TLOC preferences are correctly configured within these policies to direct traffic toward the preferred hub, for example, Hub 1, which is also the master in the VRRP configuration. This helps maintain consistent routing and traffic flow to the intended primary hub.

Verify Zone-Based Firewall Configuration

Use the following CLI commands to verify zone-based configuration:

Verify Parameter Maps

The following is a sample output from the **show class-map type inspect** command:

```
Device# show class-map type inspect
 Class Map type inspect match-all seq_1-seq-11-cm_ (id 2)
   Match access-group name seq_1-seq-Rule_3-acl_

 Class Map type inspect match-all seq_1-seq-1-cm_ (id 1)
   Match access-group name seq_1-seq-rule1-v6-acl_
```

The following is a sample output from the **show policy-map type inspect** command:

```
Device#show policy-map type inspect
  Policy Map type inspect seq_1
    Class seq_1-seq-1-cm_
      Inspect
    Class seq_1-seq-11-cm_
      Inspect
    Class class-default
      Drop
```

View Zone Pairs

The following is a sample output from the **show zone-pair security** command:

```
Device#show zone-pair security
Zone-pair name ZP_zone1_zone1_seq_1 1
    Source-Zone zone1  Destination-Zone zone1
    service-policy seq_1
```

Verify Access List Configuration

The following is a sample output from the **show ipv6 access-list** command:

```
Device#show ipv6 access-list
IPv6 access list seq_1-seq-rule1-v6-acl_
    permit ipv6 object-group source_prefix object-group dest_prefix sequence 11
```

Verify Object Groups

The following is a sample output from the **show object-group** command:

```
Device#show object-group
V6-Network object group dest_prefix
 host 2001:DB8::1

Network object group dest_v4
 host 10.16.21.10

Service object group seq_1-Rule_3-svc_
 ip

Service object group seq_1-rule1-svc_
 ip

V6-Network object group source_prefix
 host 2001:DB8::1
```

```
Network object group source_v4
 host 10.16.11.10
```

For more information about the CLI commands, see Cisco IOS XE SD-WAN Qualified Command Reference.

Verify Zone-based Firewall Statistics

Use the following CLI commands to verify the result of zone-based firewall statistics:

View Zone-based Firewall Sessions

The following is a sample output from the **show sdwan zonebfwdp sessions** command:

```
Device#show sdwan zonebfwdp sessions

        SRC  DST                                                          TOTAL      TOTAL
                   UTD
SESSION                                                    SRC    DST                     SRC
  DST  VPN  VPN                                      NAT    INTERNAL  INITIATOR  RESPONDER
  APPLICATION  POLICY
ID       STATE  SRC IP               DST IP                PORT   PORT  PROTOCOL        VRF
  VRF  ID   ID   ZP NAME               CLASSMAP NAME    FLAGS  FLAGS      BYTES      BYTES
     TYPE         NAME
------------------------------------------------------------------------------------------
13       open    2001:DB8::1        2001:DB8::1  53247       80    PROTO_L7_HTTP  1       1
    1    1    ZP_zone1_zone1_seq_1  seq_1-seq-1-cm_  -      0         96         298990
               -
```

View Zone-Pair Statistics

The following is a sample output from the **show sdwan zbfw zonepair-statistics** command:

```
Device#show sdwan zbfw zonepair-statistics
zbfw zonepair-statistics ZP_zone1_zone1_seq_1
 src-zone-name zone1
 dst-zone-name zone1
 policy-name   seq_1
 fw-traffic-class-entry seq_1-seq-1-cm_
  zonepair-name                  ZP_zone1_zone1_seq_1
  class-action                   Inspect
  pkts-counter                   7236
  bytes-counter                  4573618
  attempted-conn                 9
  current-active-conn            0
  max-active-conn                1
  current-halfopen-conn          0
  max-halfopen-conn              1
  current-terminating-conn       0
  max-terminating-conn           0
  time-since-last-session-create 4373
  fw-tc-match-entry seq_1-seq-rule1-v6-acl_ 3
   match-type "access-group name"
  fw-tc-proto-entry 1
   protocol-name tcp
   byte-counters 4545768
   pkt-counters  7037
  fw-tc-proto-entry 4
   protocol-name icmp
   byte-counters 27850
   pkt-counters  199
  l7-policy-name                 NONE
 fw-traffic-class-entry seq_1-seq-11-cm_
  zonepair-name                  ZP_zone1_zone1_seq_1
  class-action                   Inspect
  pkts-counter                   4947
  bytes-counter                  3184224
  attempted-conn                 5
  current-active-conn            0
  max-active-conn                1
  current-halfopen-conn          0
  max-halfopen-conn              0
  current-terminating-conn       0
  max-terminating-conn           0
  time-since-last-session-create 4480
  fw-tc-match-entry seq_1-seq-Rule_3-acl_ 3
   match-type "access-group name"
  fw-tc-proto-entry 1
   protocol-name tcp
   byte-counters 3184224
   pkt-counters  4947
  l7-policy-name                 NONE
 fw-traffic-class-entry class-default
  zonepair-name                  ZP_zone1_zone1_seq_1
  class-action                   "Inspect Drop"
  pkts-counter                   11
  bytes-counter                  938
  attempted-conn                 0
  current-active-conn            0
  max-active-conn                0
  current-halfopen-conn          0
  max-halfopen-conn              0
  current-terminating-conn       0
  max-terminating-conn           0
  time-since-last-session-create 0
  l7-policy-name                 NONE
```

View Zone-Pair Drop Statistics

The following is a sample output from the **show sdwan zbfw drop-statistics** command:

```
Device#show sdwan zbfw drop-statistics
zbfw drop-statistics catch-all                 0
zbfw drop-statistics l4-max-halfsession        0
zbfw drop-statistics l4-too-many-pkts          0
zbfw drop-statistics l4-session-limit          0
zbfw drop-statistics l4-invalid-hdr            0
zbfw drop-statistics l4-internal-err-undefined-dir 0
zbfw drop-statistics l4-scb-close              0
zbfw drop-statistics l4-tcp-invalid-ack-flag   0
zbfw drop-statistics l4-tcp-invalid-ack-num    0
zbfw drop-statistics l4-tcp-invalid-tcp-initiator 0
zbfw drop-statistics l4-tcp-syn-with-data      0
zbfw drop-statistics l4-tcp-invalid-win-scale-option 0
zbfw drop-statistics l4-tcp-invalid-seg-synsent-state 0
zbfw drop-statistics l4-tcp-invalid-seg-synrcvd-state 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-too-old 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-win-overflow 0
zbfw drop-statistics l4-tcp-invalid-seg-pyld-after-fin-send 0
zbfw drop-statistics l4-tcp-invalid-flags      0
zbfw drop-statistics l4-tcp-invalid-seq        0
zbfw drop-statistics l4-tcp-retrans-invalid-flags 0
zbfw drop-statistics l4-tcp-l7-ooo-seg         0
zbfw drop-statistics l4-tcp-syn-flood-drop     0
zbfw drop-statistics l4-tcp-internal-err-synflood-alloc-hostdb-fail 0
zbfw drop-statistics l4-tcp-synflood-blackout-drop 0
zbfw drop-statistics l4-tcp-unexpect-tcp-payload 0
zbfw drop-statistics l4-tcp-syn-in-win         0
zbfw drop-statistics l4-tcp-rst-in-win         0
zbfw drop-statistics l4-tcp-stray-seg          0
zbfw drop-statistics l4-tcp-rst-to-resp        0
zbfw drop-statistics insp-pam-lookup-fail      0
zbfw drop-statistics insp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics insp-dstaddr-lookup-fail  0
zbfw drop-statistics insp-policy-not-present   0
zbfw drop-statistics insp-sess-miss-policy-not-present 0
zbfw drop-statistics insp-classification-fail  0
zbfw drop-statistics insp-class-action-drop    0
zbfw drop-statistics insp-policy-misconfigure  0
zbfw drop-statistics l4-icmp-too-many-err-pkts 0
zbfw drop-statistics l4-icmp-internal-err-no-nat 0
zbfw drop-statistics l4-icmp-internal-err-alloc-fail 0
zbfw drop-statistics l4-icmp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics l4-icmp-internal-err-dir-not-identified 0
zbfw drop-statistics l4-icmp-scb-close         0
zbfw drop-statistics l4-icmp-pkt-no-ip-hdr     0
zbfw drop-statistics l4-icmp-pkt-too-short     0
zbfw drop-statistics l4-icmp-err-no-ip-no-icmp 0
zbfw drop-statistics l4-icmp-err-pkts-burst    0
zbfw drop-statistics l4-icmp-err-multiple-unreach 0
zbfw drop-statistics l4-icmp-err-l4-invalid-seq 0
zbfw drop-statistics l4-icmp-err-l4-invalid-ack 0
zbfw drop-statistics l4-icmp-err-policy-not-present 0
zbfw drop-statistics l4-icmp-err-classification-fail 0
zbfw drop-statistics syncookie-max-dst         0
zbfw drop-statistics syncookie-internal-err-alloc-fail 0
zbfw drop-statistics syncookie-trigger         0
zbfw drop-statistics policy-fragment-drop      0
zbfw drop-statistics policy-action-drop        11
zbfw drop-statistics policy-icmp-action-drop   0
zbfw drop-statistics l7-type-drop              0
zbfw drop-statistics l7-no-seg                 0
zbfw drop-statistics l7-no-frag                0
zbfw drop-statistics l7-unknown-proto          0
zbfw drop-statistics l7-alg-ret-drop           0
zbfw drop-statistics l7-promote-fail-no-zone-pair 0
zbfw drop-statistics l7-promote-fail-no-policy 0
zbfw drop-statistics no-session                0
zbfw drop-statistics no-new-session            0
zbfw drop-statistics not-initiator             0
zbfw drop-statistics invalid-zone              18
zbfw drop-statistics ha-ar-standby             0
zbfw drop-statistics no-forwarding-zone        0
zbfw drop-statistics backpressure              0
zbfw drop-statistics zone-mismatch             0
zbfw drop-statistics fdb-err                   0
zbfw drop-statistics lisp-header-restore-fail  0
zbfw drop-statistics lisp-inner-pkt-insane     0
zbfw drop-statistics lisp-inner-ipv4-insane    0
zbfw drop-statistics lisp-inner-ipv6-insane    0
zbfw drop-statistics policy-avc-action-drop    0
zbfw drop-statistics l4-icmp-invalid-seq       0
zbfw drop-statistics l4-udp-max-halfsession    0
zbfw drop-statistics l4-icmp-max-halfsession   0
zbfw drop-statistics no-zone-pair-present      0
```

View Drop Statistics for Interfaces

The following is a sample output from the **show platform hardware qfp active statistic drop** command:

```
Device#show platform hardware qfp active statistic drop
Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                         Packets                  Octets
-------------------------------------------------------------------------
Disabled                                     3963                  439403
FirewallInvalidZone                            18                    1170
FirewallPolicy                                 11                     938
IpTtlExceeded                                  12                    1050
Ipv4NoAdj                                     151                    8456
Ipv4NoRoute                                   326                   46997
Ipv6EgressIntfEnforce                        4212                  897007
Ipv6NoAdj                                       6                     456
Ipv6NoRoute                                     3                     168
Nat64v6tov4                                     6                     480
SdwanImplicitAclDrop                         7033                  408502
UnconfiguredIpv6Fia                          1349                  147590
```

View Drop Counts

The following is a sample output from the **show platform hardware qfp active feature firewall drop all** command:

```
Device#show platform hardware qfp active feature firewall drop all
-------------------------------------------------------------------------------
Drop Reason                                                             Packets
-------------------------------------------------------------------------------
Invalid L4 header                                                             0
Invalid ACK flag                                                              0
Invalid ACK number                                                            0
Invalid TCP initiator                                                         0
SYN with data                                                                 0
Invalid window scale option                                                   0
Invalid Segment in SYNSENT                                                    0
Invalid Segment in SYNRCVD                                                    0
TCP out of window                                                             0
TCP window overflow                                                           0
TCP extra payload after FIN                                                   0
Invalid TCP flags                                                             0
Invalid sequence number                                                       0
Retrans with invalid flags                                                    0
TCP out-of-order segment                                                      0
SYN flood drop                                                                0
INT ERR:synflood h-tdl alloc fail                                             0
Synflood blackout drop                                                        0
TCP - Half-open session limit exceed                                          0
Too many packet per flow                                                      0
ICMP ERR PKT per flow exceeds                                                 0
Unexpect TCP pyld in handshake                                                0
INT ERR:Undefined direction                                                   0
SYN inside current window                                                     0
RST inside current window                                                     0
Stray Segment                                                                 0
RST sent to responder                                                         0
ICMP INT ERR:Missing NAT info                                                 0
ICMP INT ERR:Fail to get ErrPkt                                               0
ICMP INT ERR:Fail to get Statbk                                               0
ICMP INT ERR:direction undefined                                              0
ICMP PKT rcvd in SCB close st                                                 0
Missed IP hdr in ICMP packet                                                  0
ICMP ERR PKT:no IP or ICMP                                                    0
ICMP ERR Pkt:exceed burst lmt                                                 0
ICMP Unreach pkt exceeds lmt                                                   0
ICMP Error Pkt invalid sequence                                                0
ICMP Error Pkt invalid ACK                                                     0
ICMP Error Pkt too short                                                       0
Exceed session limit                                                           0
Packet rcvd in SCB close state                                                 0
Pkt rcvd after CX req teardown                                                 0
CXSC not running                                                               0
Zone-pair without policy                                                       0
Same zone without Policy                                                       0
ICMP ERR:Policy not present                                                    0
Classification Failed                                                          0
Policy drop:non tcp/udp/icmp                                                   0
PAM lookup action drop                                                         0
ICMP Error Packet TCAM missed                                                  0
Security policy misconfigure                                                   0
INT ERR:Get stat blk failed                                                    0
IPv6 dest addr lookup failed                                                   0
SYN cookie max dst reached                                                     0
INT ERR:syncook d-tbl alloc failed                                             0
SYN cookie being triggered                                                     0
Fragment drop                                                                  0
Policy drop:classify result                                                   11
ICMP policy drop:classify result                                               0
L7 segmented packet not allow                                                  0
L7 fragmented packet not allow                                                 0
L7 unknown proto type                                                          0
L7 inspection returns drop                                                     0
Promote fail due to no zone pair                                               0
Promote fail due to no policy                                                  0
Firewall Create Session fail                                                   0
Firewall No new session allow                                                  0
Not a session initiator                                                        0
Firewall invalid zone                                                         18
Firewall AR standby                                                            0
Firewall no forwarding allow                                                   0
Firewall back pressure                                                         0
Firewall LISP hdr restore fail                                                 0
Firewall LISP inner pkt insane                                                 0
Firewall LISP inner ipv4 insane                                                0
Firewall LISP inner ipv6 insane                                                0
Firewall zone check failed                                                     0
Could not register flow with FBD                                               0
Invalid drop event                                                             0
Invalid drop event                                                             0
Invalid drop event                                                             0
Invalid ICMP sequence number                                                   0
UDP - Half-open session limit exceed                                           0
ICMP - Half-open session limit exceed                                          0
AVC Policy drop:classify result                                                0
Could not aquire session lock                                                  0
No Zone-pair found                                                             0
```

For more information about the CLI commands, see Cisco IOS XE SD-WAN Qualified Command Reference.

Configure Port-Scanning Detection Using a CLI Template

Table 16: Feature History

Feature Name	Release Information	Description
Configure Port-Scanning Detection Using a CLI Template	Cisco IOS XE Catalyst SD-WAN 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 SD-WAN Manager 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 SD-WAN Manager 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. 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: Infomational
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 17: Feature History

Feature Name	Release Information	Feature Description
Firewall High-Speed Logging	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows a firewall to log records with minimum impact to packet processing.
Security Logging Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	With this feature you can configure up to four destination servers to export the syslogs, and an option to specify a source interface for high-speed logging (HSL). The IP addresses for the destination servers can be IPv4, IPv6, or both. For more information about configuring HSL, see Configure Firewall High-Speed Logging Using the CLI Template, on page 87. This feature allows you to configure up to four destination servers to export the syslogs, and an option to specify a source interface for high-speed logging (HSL). The IP addresses for the destination servers can be IPv4, IPv6, or both.

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 (like the NetFlow Version 9 records) to an external collector or destination servers.

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can configure up to four destination servers to export the syslogs to; the IP addresses for these destination servers can be IPv4, IPv6, or both. You also have the option to specify a source interface for HSL.

HSL allows a firewall to log records with minimum impact on 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.

  When sessions are created or destroyed, HSL netflow records are sent to the external netflow collector. Session records contain the 5-tuple information (the source IP address, destination IP address, source port, destination port, and protocol). A tuple is an ordered list of elements.

- 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.
- IPv6 HSL is not supported on tunnel interfaces.
- Unified Logging is not supported on IPv6 address type. For more information about unified logging, see Information About Unified Logging Security Connection Events, on page 109
- Cisco IOS XE Catalyst SD-WAN devices on Cisco IOS XE Catalyst SD-WAN Release 17.10.1a do not support IPv6 address or IPv6 HSL even if the device is running a Cisco vManage Release 20.11.1 version that supports IPv6 address or IPv6 HSL.

NetFlow Field ID Descriptions

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

Table 18: 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

Field ID	Type	Length	Description
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
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)			

Field ID	Type	Length	Description
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 • 0—Ignore (invalid) • 1—Flow created • 2—Flow deleted • 3—Flow denied • 4—Flow alert
FW_EXT_EVENT	35,001	2	Extended event code. For normal records the length is 2 byte, and 4 byte for optional records.
Timestamp and Statistics Fields			
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			

Field ID	Type	Length	Description
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
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 • 0x01—Per box • 0x02—VRF • 0x03—Zone • 0x04—Class map • Other values are undefined

Field ID	Type	Length	Description
FW_EVENT_LEVEL_ID	33,004	4	Defines the identifier for the FW_EVENT_LEVEL field • 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 IOS XE Catalyst SD-WAN device:

Table 19: Syslog Messages and Their Templates

Message Identifier	Message Description	HSL Template
FW-6-DROP_PKT Type: Info	Dropping %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u %s %s Explanation: Packet dropped by firewall inspection. %s: tcp/udp/icmp/unknown prot/L7 prot %s:interface %CA:%u ip/ip6 addr: port %s:%s: zone pair name/ class name %s "due to" %s: fw_ext_event name %u ip ident %s: if tcp, tcp seq/ack number and tcp flags %s: username	FW_TEMPLATE_DROP_V4 or FW_TEMPLATE_DROP_V6

Message Identifier	Message Description	HSL Template
FW-6-SESS_AUDIT_TRAIL_START Type: Info	(target:class)-(%s:%s):Start %s session: initiator (%CA:%u) -- responder (%CA:%u) from %s %s %s Explanation: Start of an inspection session. This message is issued at the start of each inspection session and it records the source/destination addresses and ports. %s:%s: zonepair name: class name %s: l4/l7 protocolname %CA:%u ip/ip6 addr: port %s : interface %s : username %s : TODO Actual log: *Jan 21 20:13:01.078: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP: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	FW_TEMPLATE_START_AUDIT_V4 or FW_TEMPLATE_START_AUDIT_V6

Message Identifier	Message Description	HSL Template
FW-6-SESS_AUDIT_TRAIL Type: Info	(target:class)-(%s:%s):Stop %s session: initiator (%CA:%u) sent %u bytes -- responder (%CA:%u) sent %u bytes , from %s %s Explanation: Per-session transaction log of network activities. This message is issued at the end of each inspection session, and it records the source/destination addresses and ports, and the number of bytes transmitted by the client and the server. %s:%s: zonepair name: class name %s: l4/l7 protocolname %CA:%u ip/ip6 addr: port %u bytes counters %s: interface %s : TODO Actual log: *Jan 21 20:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS: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	FW_TEMPLATE_STOP_AUDIT_V4 or FW_TEMPLATE_STOP_AUDIT_V6

Message Identifier	Message Description	HSL Template
FW-4-UNBLOCK_HOST Type: Warning	(target:class)-(%s:%s):New TCP connections to host %CA no longer blocked Explanation: New TCP connection attempts to the specified host are no longer blocked. This message indicates that the blocking of new TCP connection attempts to the specified host has been removed. %s:%s: zonepair name: class name %CA: ip/ip6 addr	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_UNBLOCK_HOST
FW-4-HOST_TCP_ALERT_ON Type: Warning	"(target:class)-(%s:%s):Max tcp half-open connections (%u) exceeded for host %CA. Explanation: Exceeded the max-incomplete host limit for half-open TCP connections. This message indicates that a high number of half-open connections is coming to a protected server, and this may indicate that a SYN flood attack is in progress. %s:%s: zonepair name: class name %u: half open cnt %CA: ip/ip6 addr	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_HOST_TCP_ALERT_ON

Message Identifier	Message Description	HSL Template
FW-2- BLOCK_HOST Type: Critical	(target:class)-(%s:%s):Blocking new TCP connections to host %CA for %u minute%s (half-open count %u exceeded). Explanation: Exceeded the max-incomplete host threshold for TCP connections. Any subsequent new TCP connection attempts to the specified host is denied, and the blocking option is configured to block all subsequent new connections. The blocking will be removed when the configured block time expires. %s:%s: zonepair name: class name %CA: ip/ip6 addr %u blockout min %s: s if > 1 min blockout time %u: half open counter	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_BLOCK_HOST
FW-4-ALERT_ON Type: Warning	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u Explanation : Either the max-incomplete high threshold of half-open connections or the new connection initiation rate has been exceeded. This error message indicates that an unusually high rate of new connections is coming through the firewall, and a DOS attack may be in progress. This message is issued only when the max-incomplete high threshold is crossed. %s:%s: zonepair name: class name %s: "getting aggressive" %u/%u halfopen cnt/high %u: current rate	FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_ON

Message Identifier	Message Description	HSL Template
FW-4-ALERT_OFF Type: Warning	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u Explanation: Either the number of half-open connections or the new connection initiation rate has gone below the max-incomplete low threshold. This message indicates that the rate of incoming new connections has slowed down and new connections are issued only when the max-incomplete low threshold is crossed. %s:%s: zonepair name: class name %s: "calming down" %u/%u halfopen cnt/high %u: current rate	FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_OFF
FW-4-SESSIONS_MAXIMUM Type: Warning	Number of sessions for the firewall policy on "(target:class)-(%s:%s) exceeds the configured sessions maximum value %u Explanation: The number of established sessions have crossed the configured sessions maximum limit. %s:%s: zonepair name: class name %u: max session	FW_TEMPLATE_ALERT_MAX_SESSION

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

How to Configure Firewall High-Speed Logging

Configure Firewall High-Speed Logging

To configure Firewall High-Speed Logging using Cisco SD-WAN Manager, follow the standard firewall Cisco SD-WAN Manager flow to create a firewall policy. For more information, see For more information on creating a firewall policy, see Configure Firewall Policy and Unified Security Policy.

You can configure HSL in the Policy Summary page. For more information about the policy summary page, see Create Unified Security Policy Summary.

Configure Firewall High-Speed Logging Using the CLI Template

Use the CLI templates to configure HSL. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

Enable 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.

1. Configure a global parameter map and enter into parameter-map type inspect configuration mode.

   ```
   Device(config)# parameter-map type inspect-global
   ```

2. Configure NetFlow event logging.

   HSL records provides the IP address and the port number of the log collector. UDP destination and port correspond to the IP address and the port on which the netflow server is listening for incoming packets.

   To configure Netflow event logging for IPv4, use the following command:

   ```
   log flow-export v9 udp destination ipaddress port port number vrf vrfid source
    interface-name
   ```

   To configure Netflow event logging for IPv6, use the following command:

   ```
   log flow-export v9 udpipv6-destination ipv6 address port port number vrf
   vrfid source interface-name
   ```

   Note From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can configure up to four destination servers to export the syslogs; the IP addresses for the destination servers can be IPv4, IPv6, or both. Optionally, you can specify a source interface for HSL. A source interface is used to determine where the logs originated from when they are collected into the destination servers.

3. Configure template timeout-rate interval (in seconds) at which the netflow template formats are advertised.

   ```
   log flow-export template timeout-rate seconds
   ```

Enable 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.

This procedure configures HSL for firewall actions.

1. Configure an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** keyword, and enters parameter-map type inspect configuration mode.

   ```
   Device(config)# parameter-map type inspect parameter-map-name
   ```

2. Enable 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.

   ```
   Device(config-profile)# audit-trail on
   ```

3. Define the number of new unestablished sessions that cause the system to start deleting half-open sessions and stop deleting half-open sessions.

   ```
   Device(config-profile)# one-minute {low number-of-connections | high
   number-of-connections}
   ```

4. Configure the threshold and blocking time values for TCP host-specific, denial of service (DoS) detection and prevention.

   ```
   Device(config-profile)# tcp max-incomplete host threshold
   ```

5. Create an inspect-type policy map and enters policy map configuration mode.

   ```
   policy-map type inspect policy-map-name
   ```

6. Configure the traffic class on which an action is to be performed and enters policy-map class configuration mode.

   ```
   class type inspect class-map-name
   ```

7. (Optional) Enables stateful packet inspection.

   ```
   inspect parameter-map-name
   ```

Configuration Examples for Firewall High-Speed Logging

Example: Enable High-Speed Logging for Global Parameter Maps

The following example shows how to enable logging of dropped packets or IPv4 and IPv6, and to log error messages in NetFlow Version 9 format to an external IP address:

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can configure up to four destination servers to export the syslogs to; the IP addresses for these destination servers can be IPv4, IPv6, or both.

```
configure terminal
 parameter-map type inspect-global
 log flow-export v9 udp destination 10.0.2.0 5000 vrf 1 source GigabitEthernet0/0/5
 log flow-export v9 udp ipv6-destination 2001:DB8::1 vrf 65528 source GigabitEthernet0/0/3
 log flow-export template timeout-rate 5000
 end
```

Example: Configure Firewall High-Speed Logging

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

```
configure terminal
parameter-map type inspect parameter-map-hsl
 audit trail on
 alert on
 one-minute high 10000
 tcp max-incomplete host 100
 exit
poliy-map type inspect policy-map-hsl
 class type inspect class-map-tcp
 inspect parameter-map-hsl
 end
```

Unified Security Policy

Table 20: Feature History

Feature Name	Release Information	Description
Unified Security Policy	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to configure a single unified security policy for firewall and Unified Threat Defense (UTD) security features such as IPS, Cisco URL Filtering, AMP, and TLS/SSL. Having a single unified security policy simplifies policy configuration and enforcement becuase firewall and UTD policies can be configured together in a single security operation rather than as individual policies.
Resource Limitations and Device-global Configuration Options	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to define resource limitation options such as idle timeout and session limits, and device-global options in the policy summary page to fine-tune a firewall policy behaviour after a firewall policy is implemented in Cisco Catalyst SD-WAN.

Feature Name	Release Information	Description
Security Logging Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	With this feature, you can export UTD logs to an external syslog server and specify the source interface from which the UTD syslog originates. For more information about UTD logging, see Create Unified Security Policy Summary, on page 98page.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW. You can create firewall rules or rulesets with IPv6 as the address type in a unified security policy. For more information, see Configure Firewall Policy and Unified Security Policy, on page 93.
IPv6 Support for UTD Policies	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature adds IPv6 support for UTD security features and Unified Logging. IPv6 support for UTD security feature includes configuration and inspection of IPv6 traffic, IPS, URL filtering, and AMP. The feature also adds IPv6 support for operational commands related to UTD.

Restrictions for Unified Security Policy

- First packet recognition:

  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.

- Advanced inspection profile:

  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.

- Decrypt action:

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.

- No IPv6 support for TLS proxy:

  The addition of IPv6 support in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a does not include IPv6 support for TLS proxy with security policy.

Note For voice traffic established with Session Initiation Protocol (SIP) or H.323, Cisco recommends bypassing UTD advanced inspection to avoid latency and ensure better voice quality.

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 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 92
- 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 firewall security policy to a unified NG firewall security policy only. For information, see Migrate a Security Policy to a Unified Security Policy, on page 102.

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 becuase 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 use 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 an object group, perform the following steps:

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 156
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 166.
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 175
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 202.
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 SD-WAN Manager 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 SD-WAN Manager 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. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.

11. From the **Action** drop-down list, choose an action for the rule.

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

12. If you want matches for this rule to be logged, check the **Log** check box.

    Note Cisco SD-WAN Manager supports log flow only at the rule level and not at the global level.

    Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1, you can choose the IP address type as IPv6.

13. Choose an advanced 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 advanced inspection profile, see Create an Advanced Inspection Profile, on page 92.

    Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1, you can choose the IP address type as IPv6.

14. Click **Source**, and choose one of the following options:

    - **Object Group**: 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 92.

    - **Type**: You can choose from IPv4 prefixes, IPv6 prefixes, prefix lists, fully qualified domain names (FQDN), lists, or Geo Location based on the IP address type that you choose.

    Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Type** field displays the prefix options.

15. Click **Save**.

16. 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 92.

    - **Type**: You can choose from IPv4 prefixes, IPv6 prefixes, prefix lists, fully qualified domain names (FQDN), lists, or Geo Location based on the IP address type that you choose.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Type** field displays the prefix options.

17. Click **Save**.

18. Click **Protocol** to configure a protocol for the rule.

19. 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 Catalyst SD-WAN 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.

Note See the information about custom applications in Restrictions, on page 46.

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

21. (Optional) Repeat Step 7 to Step 19 to add more rules.

22. Click **Save Unified Security Policy**.

23. Click **Add Zone Pair** to apply the policy to a zone pair. For information, see Add a Zone Pair, on page 96.

24. To edit or delete a unified security policy, click **...**, and choose an option.

25. 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 Cisco SD-WAN Manager, on page 96

26. Click **Next**.

    The **Policy Summary** page is displayed. For information on the **Policy Summary** page, see Create Unified Security Policy Summary.

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 SD-WAN Manager

1. From the Cisco SD-WAN Manager 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.
   - **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 the next step.
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.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

Table 21: DNS Security Policy

Field	Description
Add DNS Security Policy	From the **Add DNS Security Policy** drop-down list, select **Create New** to create a new DNS Security Policy policy. **Copy from Existing**: Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
Create New	Displays the DNS Security Policy wizard.
Policy Name	Enter a name for the policy.
Umbrella Registration Status	Displays the status of the API Token configuration.
Manage Umbrella Registration	Click **Manage Umbrella Registration** to add a token, if you have not added one already.
Match All VPN	Click **Match All VPN** to keep the same configuration for all the available VPNs.
Custom VPN Configuration	choose **Custom VPN Configuration** to input the specific VPNs.
Local Domain Bypass List	Choose the domain bypass.
DNS Server IP	Configure **DNS Server IP** from the following options: • **Umbrella Default** • **Custom DNS**
DNSCrypt	Enable or disable the DNSCrypt.
Next	Click **Next** to the policy summary page.

Create Unified Security Policy Summary

To complete creating a unified security policy, perform the following steps:

1. The **Policy Summary** page, enter a name for the unified 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 unified security policy. This field is mandatory.

3. Enter **TCP SYN Flood Limit** to configure the threshold of SYN flood packets per second for each destination address. Beyond this threshold, the TCP SYN Cookie is triggered. This number must be less than **Max Incomplete TCP Limit**.

4. Enter **Max Incomplete** timeout limits for the firewall policy. A **Max Incomplete** timeout limit protects firewall resources and keep these resources from being used up.

   - In the **TCP Limit** field, specify the Max TCP half-open sessions allowed on a device.
   - In the **UDP Limit** field, specify the Max UDP half-open sessions allowed on the device.
   - In the **ICMP Limit** field, specify the Max ICMP half-open sessions allowed on the device.

5. (Optional) For Cisco IOS XE Catalyst SD-WAN Release 16.12.2r and onwards, to configure high-speed logging (HSL), enter the following details of the Netflow server that will listen for the Netflow event logs.

   For more information on HSL, see Firewall High-Speed Logging Overview.

   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.

   d. In the **Source Interface** field, specify the interface for HSL.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can configure up to four destination servers to export the syslogs; the IP addresses for these destination servers can be IPv4, IPv6, or both. Optionally, you can specify a source interface for HSL.

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

7. Click **Unified Logging** to enable the unified logging feature.

Note To enable logging for a class or policy, check the **Log** check box for the rule in a policy.

8. Click **Session reclassify allow** to allow re-classification of traffic on policy change.

   Apply a policy to a set of devices, and then make changes to the security policy (adding, deleting, editing filters or rules) thereby effecting changes to existing flows as well. For example, if there are long-lived flows passing through the device, and if a change in the policy needs to be applied for those long-lived flows, use the **Session reclassify allow** to reclassify all the flows existing on the device based on the new firewall policy.

Note There is another kind of reclassification which is traffic driven. When FPM (First Packet Match) fails for an application, the traffic can hit a generalized L3/L4 rule if exists. After the application is fully recognized, the traffic is reclassified and hit the desired rule that deals with the specific application.

9. Click **ICMP unreachable allow** to allow ICMP unreachable packets to pass through.

10. Choose an advanced inspection profile.

    You have the option to attach an advance inspection profile at a device level. All the rules in the device that match the traffic to be inspected are inspected using the advance 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 is effective in the policy.

11. (Optional) Choose a TLS/SSL Decryption policy. This field is visible if you have configured a TLS action in the advanced inspection profile.

12. (Optional) Enter the following details to export the UTD logs to the external syslog server:

    - In the **VPN** field, enter the VPN that the syslog server is in.
    - In the **Server IP** field, enter the IP address of the syslog server.
    - From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, enter the interface name in the **Source Interface** field where the UTD syslogs should originate from.

13. Click **Save Policy** to save the unified security policy.

14. Apply the security policy to a device. For more information, see Apply a Security Policy to a Device.

Configure Resource Limitations and Device-global Configuration Options

The following sample configuration shows how to configure resource limitations and device-global configuration options:

```
Device# config transaction
Device(config)# parameter-map type inspect-global
Device(config-profile)# max-incomplete icmp 12
Device(config-profile)# max-incomplete udp 11
Device(config-profile)# max-incomplete tcp 10
Device(config-profile)# icmp-unreachable-allow
Device(config-profile)# session-reclassify-allow
Device(config-profile)# tcp syn-flood limit 5
Device(config-profile)# exit
```

Use the following command to display resource limitations and device-global configuration options on a Cisco IOS XE Catalyst SD-WAN device:

```
Device# show run | sec parameter-map
parameter-map type inspect-global
icmp-unreachable-allow
session-reclassify-allow
tcp syn-flood limit 5
alert on
max-incomplete tcp 10
max-incomplete udp 11
max-incomplete icmp 12
```

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

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

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

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
```

6. Enable UTD logging in a unified security policy:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all file-inspection
threat-inspection web-filtering
Device(config-utd-mt-global)# logging host host_IP [source-interface interface
name]
```

Note The **flow-logging all** command enables unified logging for all the UTD features. If you do not want to enable unified logging for all UTD features, choose the individual flow-logging options (**file-inspection**, **web-filtering**, **threat-inspection** .

Migrate a Security Policy to a Unified Security Policy

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, Cisco Catalyst SD-WAN supports unified security policy. You can migrate your existing firewall security policies to a unified NG firewall security only. While copying a security policy to a unified policy, all 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 SD-WAN Manager 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 IPS, URL, AMP and SSL/TLS security policies cannot be migrated to a unified security policy as is. You must create new unified policies separately and attach them to an advanced inspection profile. The advanced inspection profile can then be attached to the relevant rules in the unified NG firewall 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 SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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
```

Example 5

The following is a sample output from the **show platform hardware qfp active feature firewall drop** command that displays the Max Incomplete UDP after the limit is crossed.

```
Device# show platform hardware qfp active feature firewall drop
-------------------------------------------------------------------------------
Drop Reason                                                             Packets
-------------------------------------------------------------------------------
```

```
ICMP ERR Pkt:exceed burst lmt                                                  42
ICMP Unreach pkt exceeds lmt                                                  305
UDP - Half-open session limit exceed                                            2
```

Example 6

The following is a sample output from the **utd** command to verify UTD logging.

```
Device# show run | sec utd
parameter-map type inspect pm1
 utd-policy default
!
utd engine standard unified-policy
 threat-inspection profile default-threat
  threat protection
  policy security
 utd global
  logging host 10.1.1.1
  logging host 10.2.2.2 source-interface Loopback2
  logging host 10.3.3.3 source-interface GigabitEthernet3
 policy default
  threat-inspection profile default-threat
```

Example 7

The following is a sample output from the **show parameter-map type inspect-global** command to verify HSL configuration.

```
Device#show parameter-map type inspect-global
 parameter-map type inspect-global
  log flow-export v9 udp destination 10.10.0.2 5050
  log flow-export v9 udp destination 10.10.0.2 4040
  log flow-export v9 udp ipv6-destination 2001:DB8::1 source GigabitEthernet0/1/0
  log flow-export v9 udp ipv6-destination 2001:DB8::1
```

Configuration Example for Unified Security Policy

Example 1

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 based on a specific 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. Ensure to mention the order of the rule sequence because different ordering can end up with different results.

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-l4-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-l4-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
!
```

Unified Logging for Security Connection Events

Table 22: Feature History

Feature Name	Release Information	Description
Unified Logging for Security Connection Events	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature supports Unified Logging which is used to capture information about connection events across different security features at different stages during policy enablement and execution. With Unified Logging, you can have visibility to the log data for Zone-based Firewall and for Unified Threat Defense features such as IPS, URL-F and AMP to understand what traffic, threats, sites or malware were blocked, and the rules that blocked the traffic or sessions with the associated port, protocol or applications. Additionally, this feature also provides support for On-Demand Troubleshooting. On-Demand troubleshooting allows a user to view the connection events of inspect flows of traffic from a device within a configured period of time.

Prerequisites For Unified Logging for Security Connection Events

- Unified Logging can be used only with unified security policies.
- You must have configured a localized data policy, and enabled the **Netflow** and **Application** options in the policy.

Restrictions For Unified Logging for Security Connection Events

Unified Logging affects CPU performance and resource consumption for security connection events. Therefore, Unified Logging is not enabled by default in Cisco SD-WAN Manager. For this reason, we recommended you to only enable Unified Logging on specific devices for short periods.

Information About Unified Logging Security Connection Events

Unified Logging can be enabled for unified security policies to help you view the log data for security connection events. Security connection events contains log data of important information when a flow passes through various security features such as Zone-based Firewall (ZBFW), and Unified Threat Defense (UTD). The log data includes information about security policies and rules about traffic or sessions along with the associated port, protocol or applications.

Note As of Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, UTD TLS-Decryption events are not reported.

Flow data about ZBFW and UTD features is captured using Netflow. Netflow records the flow data to a JSON file which is used by Cisco SD-WAN Manager. The flow data can also be exported to an external Netflow collector. Exporters are assigned to flow monitors to export data from the flow monitor cache to a remote system such as a Netflow collector. Flow monitors can support more than one exporter. Each exporter can be customized to meet the requirements of the flow monitor or monitors in which it is used and the Netflow collector systems to which it is exporting data.

Cisco SD-WAN Manager displays the following data for the security connection events:

ZBFW

- Information about enforcement of ZBFW.
- Zone information (zone pair, source zone, and destination zone).
- Policy enforced on the connection flow.
- Action taken based on the policy on the connection flow (inspect).
- Status of Network Address Translation (NAT) or Port Address Translation (PAT) is enabled or not.

UTD

- Details of which UTD security features acted on a flow.
- Result of a security feature acting on a flow.
- Details of policy enforcement.

Comparison Between Unified Logging for Security Connection Events, ZBFW High Speed Logging and ZBFW Syslog

ZBFW supports high-speed logging (HSL). HSL allows ZBFW to log records with minimum impact to packet processing.

With HSL configured, ZBFW 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

For information about Firewall High-speed logging, see Firewall High-Speed Logging

In the case of Unified Logging, the log data consists of the following types:

Security Component	Event Type	Export ID (Pen:type)
ZBFW	• Zonepair ID • Source Zone ID • Dest Zone ID • Policy ID • Class ID • Proto • Action • Translated source IP Addr • Translated dest IP Addr • Translated source port • Translated dest port	• 9:2239 • 9:12464 • 9:12464 • 9:8236 • 9:8233 • 9:12466 • 9:12467 • 0:225 • 0:226 • 0:227 • 0:228
IPS	• Policy ID • Action • Priority • Generator ID • Signature ID • Classification ID	• 9:12479 • 9:12480 • 9:12487 • 9:12489 • 9:12488 • 9:12490
URL-F	• Policy ID • Action • Reason • Category • Reputation • URL Hash • App Name	• 9:12481 • 9:12482 • 9:12520 • 9:12492 • 9:12493 • 9:12491 • 9:12494

Security Component	Event Type	Export ID (Pen:type)
AMP	• Policy ID • Action • Disposition • File Type • File Name Hash • Malware Name Hash • File SHA	• 9:12484 • 9:12486 • 9:12495 • 9:12497 • 9:12498 • 9:12499 • 9:12494
FNF	• IPv4 SrcAddr • IPv4 DstAddr • IPv4 Protocol • Transport SrcPort • Transport DstPort • Routing VRF Service • IPv4 DSCP • Transport TCP Flags • Interface Input • Interface Output • Counter bytes long • Counter packets long • Timestamp absolute First • Timestamp absolute Last • Application Name • Flow end-reason	• 0:8 • 0:12 • 0:4 • 0:7 • 0:11 • 9:12434 • 0:195 • 0:6 • 0:10 • 0:14 • 0:1 • 0:2 • 0:152 • 0:153 • 0:95 • 0:136

Note Starting from Cisco IOS XE Release 17.9.1a, use the **policy ip visibility features** *ulogging* **enable** command to manually enable or disable the unified logging fields in flexible netflow (FNF). Use the **show sdwan policy cflowd-upgrade-status** command to check which features were enabled before the version upgrade. You have to manually control the features after a version upgrade using the disable or enable commands.

For more information, see policy ip visibility command page.

Note Unified Logging for security connection events and ZBFW HSL can be enabled together. If you choose to enable both these features, there will be a considerable impact on the performance.

On-Demand Troubleshooting

The On-Demand Troubleshooting feature allows a user to view detailed information about the flow of traffic from a device. A user can use this information for troubleshooting. For information, see On-Demand Troubleshooting.

Benefits of Unified Logging for Security Connection Events

- Provides a framework to log all security events in one place for ZBFW, IPS, URL-F, and AMP.
- Provides enhanced visibility to the log data for ZBFW, IPS, URL-F, and AMP.
- Provides flow-level detailed monitoring for ZBFW, IPS, URL-F, and AMP.

Use Cases For Unified Logging for Security Connection Events

You can view the log data for ZBFW, IPS, URL-F, and AMP to understand what traffic, threats, sites or malware were blocked, and the policy rules that blocked the traffic or sessions with the associated port, protocol or applications.

Configure Unified Logging for Security Connection Events

To configure Unified Logging for security connection events, perform the following steps:

1. Configure Localized Policy Using Cisco SD-WAN Manager.
2. Select the policy application check boxes for **Netflow** and **Application**. For information, see Configure Policy Settings.
3. Enable logging for a unified security policy. You can enable logging either at a rule level or at global level Configure Firewall and Unified Security Policy.

Note You can also use the CLI Add-on template for configure Unified Logging for security connection events. For more information, see Create a CLI Add-On Feature Template.

Configure Unified Logging for Security Connection Events Using the CLI

This section provides example CLI configurations to configure Unified Logging for ZBFW and UTD.

ZBFW

Use this configuration to enable Unified Logging for ZBFW at a global level.

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# log flow
```

UTD

Use this configuration to enable Unified Logging for all UTD features.

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all file-inspection threat-inspection
 web-filtering
Device(config-utd-mt-global)# logging host host_IP [source-interface Interface]
```

Note **flow-logging all** enables unified logging for all the UTD features. If you do not want to enable Unified Logging for all UTD features, choose the individual flow-logging options (**file-inspection**, **web-filtering**, **threat-inspection**.

Configure Netflow

Use this configuration to enable Netflow to export log data of ZBFW and UTD features to an external collector.

```
Device(config)# flow exporter exporter-name
Device(config-flow-exporter)# description description
Device(config-flow-exporter)# destination IP address
Device(config-flow-exporter)# export-protocol netflow-v9
Device(config-flow-exporter)# transport udp udp-port
```

Configuration Example for Unified Logging for Security Connection Events

ZBFW

This example shows the configuration of ZBFW and UTD for Unified Logging of security connection events.

Use this configuration to enable Unified Logging for ZBFW at a global level.

```
Device(config)# parameter-map type inspect-global
```

Use this configuration to enable Unified Logging for ZBFW at a rule level.

```
Device(config-profile)# log ?
flow Enable     flow/connection events for all security policies
flow-export     Configure inspect external logging parameters
```

Note Use **?** to view the options for Unified Logging for ZBFW at a rule level.

UTD

Use this configuration to enable Unified Logging for all UTD features.

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all file-inspection threat-inspection web-filtering
Device(config-utd-mt-global)# logging host 10.3.3.3 source-interface GigabitEthernet3
```

Note You can choose to use any of the UTD options if you do not want to enable Unified Logging for all UTD features.

Verify Unified Logging for Security Connection Events

The following is a sample output from the **show flow monitor sdwan_flow_monitor cache** command to verify Unified Logging configuration for security connection events.

```
IPV4 SOURCE ADDRESS:                     10.193.88.123
IPV4 DESTINATION ADDRESS:                         12.168.20.200
TRNS SOURCE PORT:                                 80
TRNS DESTINATION PORT:                            32964
IP VPN ID:                                        1000
IP PROTOCOL:                                      6
interface input:                                  Tu2000000001
interface output:                                 Gi3
counter bytes long:                               458
counter packets long:                             4
timestamp abs first:                              07:53:16.191
timestamp abs last:                               07:53:16.244
ulogging fw zp id:                                1
ulogging fw zone id array:                        1 2
ulogging fw class id:                             54049
ulogging fw policy id:                            29456
ulogging fw proto id:                             1
ulogging fw action:                               0
ulogging fw drop reason id:                       61
ulogging fw end flow reason:                      1
ulogging fw source ipv4 address translated:       10.1.1.1
ulogging fw destination ipv4 address translated:  20.1.1.1
ulogging fw source port translated:               0
ulogging fw destination port translated:          0
```

Monitor Unified Logging Security Connection Events

To view logged data for the security connection events in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click the device you want to monitor.
3. In the left pane, under **On-Demand Troubleshooting**, choose **Connection Events**. The connection details of the security connection events are displayed in the right pane.
4. Click **More Details** to view the log details for ZBFW and UTD features.

Note If you are using the **Connection Events** option for the first time, you need to enable On-Demand Troubleshooting. For information, see On-Demand Troubleshooting

Cisco Catalyst SD-WAN Identity-Based Firewall Policy

Table 23: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Identity-Based Firewall Policy	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature allows you to configure user identity-based firewall policies for unified security policies. Cisco Identity Services Engine (ISE) and Microsoft Active Directory Services are identity providers that authenticate and authorize device users in the network. When Cisco SD-WAN Manager and a Cisco Catalyst SD-WAN Controller establish a connection to Cisco ISE, information about user and user groups—that is, identity-mapping information—is retrieved from Cisco ISE. Identity-based policies are then distributed to Cisco IOS XE Catalyst SD-WAN devices. This identity mapping information is used while creating firewall policies.
Cisco Catalyst SD-WAN Identity-Based Firewall Policy Enhancement for SGT Integration	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Cisco Catalyst SD-WAN Identity-Based Firewall Policy Enhancement for SGT Integration feature is enhanced to support Security Group Tag (SGT) integration with Cisco ISE. SGTs are assigned in the network to simplify policy configuration across devices.
IPv6 Support for Zone-based Firewall	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW. You can create firewall rules or rulesets with IPv6 as the address type in a unified security policy. For more information, see Create Identity-Based Unified Security Firewall Policy, on page 122.

Information About Cisco Catalyst SD-WAN Identity-Based Firewall Policy

To configure identity-based firewall policies in Cisco Catalyst SD-WAN, the following components are used in Cisco Catalyst SD-WAN:

- Cisco ISE
- Microsoft Active Directory Services
- Cisco SD-WAN Manager
- Cisco SD-WAN Controller

Cisco ISE

Cisco ISE is an identity provider that is deployed on-premises to manage user identities and to provide services such as authentication, authorization, and accounting.

Microsoft Active Directory Services

Microsoft Active Directory Services is another identity provider that consists of identity and user group information. Cisco ISE interfaces with Microsoft Active Directory Services to receive user identity and user group information. For Cisco ISE to retrieve the identity information, Microsoft Active Directory Services must be integrated with Cisco ISE. A Microsoft Active Directory Services domain needs to be set up, and the domain information must be configured on Cisco ISE. For information on configuring Microsoft Active Directory Services on Cisco ISE, see AD Integration for Cisco ISE GUI and CLI Login.

Cisco SD-WAN Manager

A connection is required from Cisco SD-WAN Manager to Cisco ISE through Cisco pxGrid, to retrieve all the user and user group information. You can use the user and user group information to create security policies in Cisco SD-WAN Manager. Cisco SD-WAN Manager also configures the Cisco Catalyst SD-WAN Controllers so that they can communicate with ISE directly and then pull the user and user group information. When a user logs in or logs out, Cisco ISE tracks the login state and provides this information to the Cisco Catalyst SD-WAN Controller through Cisco pxGrid. Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller interface with the Cisco ISE pxGrid node to retrieve identity mapping information. See Configure Cisco ISE in Cisco SD-WAN Manager, on page 121, Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller, on page 120.

Cisco SD-WAN Controller

When the Cisco Catalyst SD-WAN Controller establishes a connection to Cisco ISE, it obtains the IP-to-username and user-to-user-group mappings from Cisco ISE and Cisco pxGrid. The Cisco Catalyst SD-WAN Controller subsequently pushes the identity mapping information containing IP-to-username to user-group mapping to the Cisco IOS XE Catalyst SD-WAN devices. The identity mapping information is used when creating firewall policies in Cisco SD-WAN Manager. For information on creating identity-based firewall policies, see Configure Cisco Catalyst SD-WAN Identity-Based Firewall Policy.

As of Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the following user identity scale numbers are supported on Cisco IOS XE Catalyst SD-WAN devices:

IP-User Sessions

- Cisco IOS XE Catalyst SD-WAN devices with 4GB of system memory or less can support a maximum of 10,000 ip-user sessions.

- Cisco IOS XE Catalyst SD-WAN devices with 8GB of system memory or greater can support a maximum of 100,000 ip-user sessions.

IP-SGT Bindings

- Cisco IOS XE Catalyst SD-WAN devices with 4GB of system memory or less can support a maximum of 10,000 bindings.
- Cisco IOS XE Catalyst SD-WAN devices with 8GB of system memory or greater can support a maximum of 100,000 bindings.

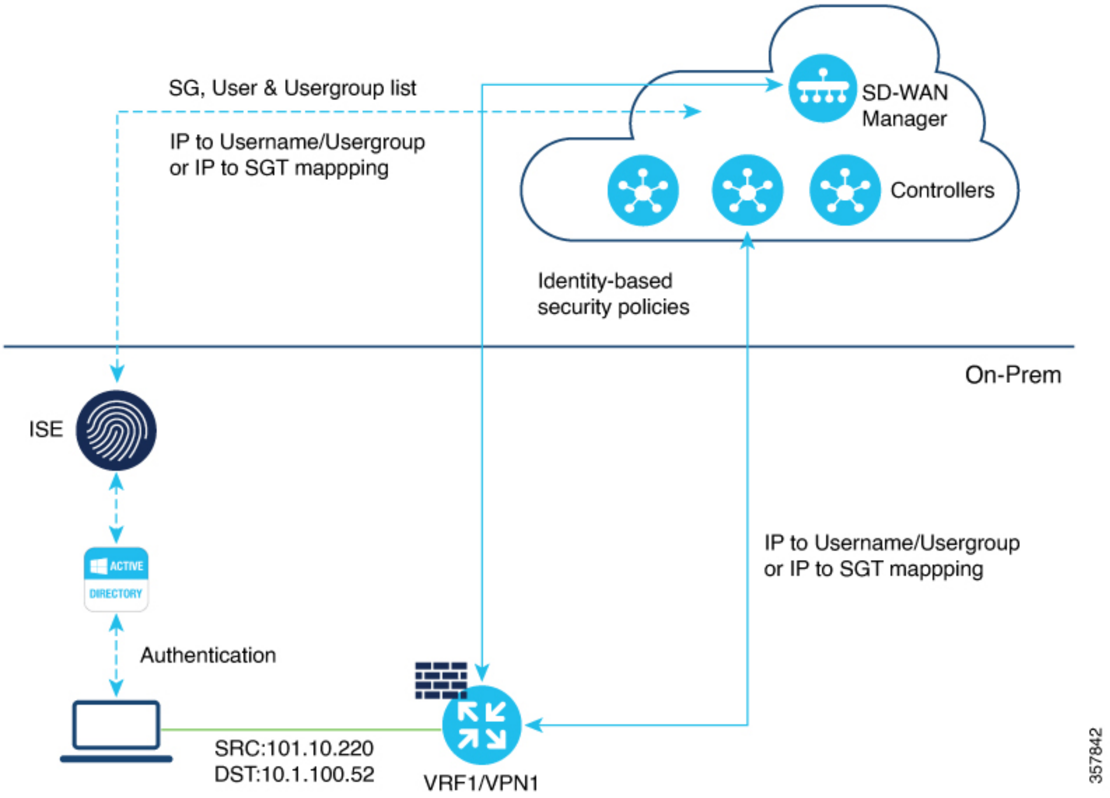
In order to provide connectivity of Cisco ISE with Cisco Catalyst SD-WAN Controller to push Cisco pxGrid service and integrate Cisco SD-WAN Manager with Cisco ISE,

- Cisco ISE version 3.2 supports only two Cisco Catalyst SD-WAN Controllers.
- Cisco ISE version 3.3 or later supports more than three Cisco Catalyst SD-WAN Controllers.

Architecture of Cisco Catalyst SD-WAN Identity-Based Firewall Policy

Figure 3: Cisco Catalyst SD-WAN Identity-Based Firewall Policy

This figure displays the identity information flow between Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco IOS XE Catalyst SD-WAN devices.



Management Plane

- Cisco SD-WAN Manager obtains the user and user group information from Cisco ISE and pxGrid.
- An administrator authors the security policies using the username and user group.
- Cisco SD-WAN Manager pushes these policies to the Cisco IOS XE Catalyst SD-WAN devices.

Controller Distribution

- A Cisco Catalyst SD-WAN Controller obtains the IP-to-username and user-to-user-group mappings from Cisco ISE and pxGrid when a user logs in. A session is created.
- The Cisco Catalyst SD-WAN Controller pushes the IP-to-username and user-to-user-group mappings to the Cisco IOS XE Catalyst SD-WAN devices.

Control Plane and Data Plane

- Cisco Catalyst SD-WAN Controller policies with username and user groups are provisioned through Cisco SD-WAN Manager, and pushed to a Cisco IOS XE Catalyst SD-WAN device.
- Cisco IOS XE Catalyst SD-WAN device learns the IP-to-username and user-to-user-group mappings.
- Cisco IOS XE Catalyst SD-WAN device receives flows and enforces the configured username and user-group-based policies.

Logging and Reporting

A Cisco IOS XE Catalyst SD-WAN device includes username information in the Cisco SD-WAN Manager logs and in the **show** command output.

Security Groups and SGTs

Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

A security group is a grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by a Cisco ISE administrator. As new users and devices are added to the Cisco TrustSec domain, the authentication server assigns these new entities to security groups. Cisco TrustSec assigns a unique 16-bit security group number whose scope is global within a Cisco TrustSec domain, to each security group. The number of security groups in the device is limited to the number of authenticated network entities.

After a device is authenticated, Cisco TrustSec tags any packet that originates from that device with a security group tag (SGT) that contains the security group number of the device. The tag appears in the packet's Cisco TrustSec header. The SGT is a single label that determines the privileges of the source within the entire enterprise.

An SGT is used in source or destination data prefixes in a firewall rule policy. Because the SGT contains the security group of the source, the tag can be referred to as the source SGT. The actual Cisco TrustSec packet tag does not contain the security group number of the destination device.

Benefits of Cisco Catalyst SD-WAN Identity-Based Firewall Policy

Firewall policies are created based on users and user groups, and not based on IP addresses. Therefore, policies do not have to be re-created even if there are changes in the IP addresses on the devices.

Prerequisites for Cisco Catalyst SD-WAN Identity-Based Firewall Policy

- Cisco Identity Services Engine (ISE) version must be 3.2 or later. Cisco ISE Release 3.2 and later support user and user-group-based policies and two Cisco Catalyst SD-WAN Controllers . Cisco ISE Release 3.1 supported only user-group-based policies with two Cisco Catalyst SD-WAN Controllers.
- Identity providers Cisco ISE and Microsoft Active Directory Services must be configured to provide user information. For information on configuring Microsoft Active Directory Services on Cisco ISE, see AD Integration for Cisco ISE GUI and CLI Login.
- In Cisco ISE, the option to allow password-based account creation for pxGrid Services must be enabled. This is necessary for connectivity from pxGrid to Cisco Catalyst SD-WAN Controller, becuase a Cisco Catalyst SD-WAN Controller uses a password-based mechanism to authenticate with pxGrid. Additionally, the API Service settings for External RESTful Services (ERS) and Open API must be enabled in Cisco ISE.
- Cisco Catalyst SD-WAN Controllers must be configured using a feature template.
- The fully qualified domain name (FQDN) for Cisco ISE must be resolvable from both Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller. Use an IP address to connect from Cisco SD-WAN Manager to Cisco ISE.
- If a connection from Cisco Catalyst SD-WAN Controller to Cisco ISE is established using a TLOC interface, you must add the **allow-service** *all* command to the implicit ACL configuration.
- PxGrid service must be enabled on Cisco ISE for a node.

Restrictions for Cisco Catalyst SD-WAN Identity-Based Firewall Policy

- Only one Cisco Catalyst SD-WAN node can connect to one Cisco ISE instance.
- For a multitenant setup, the Cisco ISE page is not available in Cisco SD-WAN Manager.
- Firewall rules can include only one identity list.
- A maximum of 16 user and user-group combinations can be selected in a single identity list.
- Rule sets, Object Group List, and Destination do not support identity list.
- One user can be tagged with up to eight user groups only.
- The maximum character length for a user name is up to 64 bytes, and 96 bytes for user group name.
- When a user-based identity policy is created, users must use the SAM-Account format to log in to Active Directory.
- The graceful restart timer value on a WAN edge device for the **omp graceful-restart timer** command should be greater than the timeout value for the **omp-connectivity-timeout** command on Cisco Catalyst SD-WAN Controller.

The following restrictions are applicable for Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a:

- Only one SGT list can be configured per firwall policy rule in each direction.
- SGT is not supported under ruleset or in object-group list.
- Only 8 SGTs are supported in an identity list.
- SGT in policy is supported only for unified policy.

Use Cases for Cisco Catalyst SD-WAN Identity-Based Firewall Policy

Firewall policies can be configured based on user groups, and user-based rules can be added to provide exceptions to the policies.

For example, an administrator can create a firewall policy that restricts users within a particular user group from accessing a specific website. But the administrator can create exceptions to that policy to allow specific users within the user group access to the website.

We recommend policies be configured based on user groups rather than users, and exceptions be created for specific users in a user group.

Configure Cisco Catalyst SD-WAN Identity-Based Firewall Policy

Perform the following tasks to create an identity-based unified security firewall policy:

1. Configure Cisco ISE for Microsoft Active Directory Services.
2. Configure PxGrid in Cisco ISE for connectivity to Cisco SD-WAN Controller.
3. Configure Cisco ISE in Cisco SD-WAN Manager.
4. Create an identity list.
5. Create an identity-based unified security firewall policy.

Configure Cisco ISE for Microsoft Active Directory Services

Microsoft Active Directory Services must be configured in Cisco ISE to fetch all the user and user group information. For information on configuring Microsoft Active Directory Services in Cisco ISE, see AD Integration for Cisco ISE GUI and CLI Login.

Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller

The **Allow password-based account creation** option for Cisco Platform Exchange Grid (pxGrid) services Services must be enabled in Cisco ISE. This is necessary for connectivity from pxGrid to the Cisco Catalyst SD-WAN Controller because the Cisco Catalyst SD-WAN Controller uses a password-based mechanism to authenticate with pxGrid. For information on configuring pxGrid in Cisco ISE, see pxGrid Settings.

Note Enable the ERS option by choosing **Administration** > **Settings** > **API Settings** > **API Service Settings** in ISE in order to enable pxGrid services for Cisco ISE connectivity to Cisco Catalyst SD-WAN Controller.

Configure Cisco ISE in Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Integration Management.**.
2. Click **Identity Services Engine**.
3. Click **Add Connection**. .

   The **Add ISE Server** window is displayed.
4. Specify an IP address in the **ISE Server IP address** field.
5. Enter a username and password to connect to Cisco ISE.
6. Choose the VPN over which connectivity to Cisco ISE must be established.
7. In the **ISE Server CA** pane, choose a file from your desktop or drag and drop to upload.

   Note You can download the Cisco ISE server certificate from Cisco ISE. For details on Cisco ISE certificates, see Generate Certificate Signing Request (CSR).
8. In the **PxGrid Server CA** pane, choose a file from your desktop or drag and drop to upload.

   Note You can download the PxGrid server certificate from Cisco ISE. For details on Cisco ISE certificates, see Generate Certificate Signing Request (CSR).
9. (Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1) In the **Feature Subscription** field, select the feature for which you want to retrieve the metadata information from Cisco ISE. The options are:
   - **User/User Groups**
   - **Security Group Tag (SGT)**
10. For **User/User Groups**, enter the **AD Joint Point** name and the **AD Domain** name, as defined in Cisco ISE.
11. Click **Submit**.

    A connection to Cisco ISE is initiated. An automatic template push to the Cisco SD-WAN Controller is initiated based on the username and password, Cisco ISE Server IP address, AD domain name, and VPN name. The Cisco SD-WAN Controller then connects to pxGrid using the pxGrid APIs, and opens a web socket connection.

    When the Cisco Catalyst SD-WAN Controller establishes a connection to Cisco ISE, information about user and user groups is retrieved from Cisco ISE and distributed to the Cisco IOS XE Catalyst SD-WAN devices.

    To view the list of users and user groups available in the corresponding domain, choose **Actions** > **View ISE Data**.

Create an Identity List

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.

2. Click **Custom Options**.

3. Click **Lists**.

4. Click **Identity**.

   Note If you have not completed the integration of Cisco ISE Controller with Cisco SD-WAN Manager, a message instructs you to complete the integration. After you complete this integration, the **Add an Identity list** link is displayed in **Identity List** window.

5. Click **Add an Identity list**.

6. Enter a name for the identity list.

7. Enter a description for the identity list.

8. (Minimum releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a)

   In the **Subscription Type** drop-down list, choose one of the following:

   - **User/ User Group**
   - **Security Group Tag (SGT)**

   Note You can configure either **User/ User Group** or **Security Group Tag (SGT)** at a given point, not both.

9. If you choose **Security Group Tag (SGT)**, select one or more SGTs and click **Add**.

   After you add the SGT identity list, you can use it in a unified security policy to create source-based or destination-based identity security firewall policies.

10. If you choose **User/User Groups**, select the user groups and click **Add**. If the user information is available, the **User Groups** list displays all the user groups. You can select a maximum of 16 user groups.

    After you add the identity list, you can use it in a unified security policy to create a user-identity-based security firewall policy.

Create Identity-Based Unified Security Firewall Policy

1. From the Cisco SD-WAN Manager 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. Click **Add Rule**.
8. From the **Order** drop-down list, choose the order for the rule .
9. Enter a name for the rule.
10. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type.
11. From the **Action** drop-down list, choose an action for the rule.
    - **Inspect**
    - **Pass**
    - **Drop**
12. (Optional) Check the **Log** check box if you want matches for this rule to be logged.

Note Cisco SD-WAN Manager supports log flow only at the rule level and not at the global level.

13. Choose an advanced 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 advanced inspection profile, this field lists all the advanced inspection profiles that you have created. Choose an advanced inspection profile from the list. For information on creating an advanced inspection profile, see Create an Advanced Inspection Profile.
14. Click **Source**, and choose **Identity** as the filter type
15. Click **Destination**, and choose one of the following options:
    - **Object Group**: 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 .
    - **Type**: You can choose from IPv4 prefixes, IPv6 prefixes, prefix lists, fully qualified domain names (FQDN), lists, or Geo Location based on the IP address type that you choose. When you configure SGT in the list, identity can be a filter type.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can choose an IP address type as IPv4 or IPv6. Based on the IP address type that you choose, the **Type** field displays the prefix options.

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 Catalyst SD-WAN Release 17.6.1a, and Cisco vManage Release 20.6.1, the applications are attached directly to a 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.

Note See the information about custom applications in Restrictions, on page 46.

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

20. Click **Save Unified Security Policy**.

21. Click **Add Zone Pair** to apply the policy to a zone pair. For information, see Add a Zone Pair.

22. To edit or delete a unified security policy, click **...**, and choose an option.

23. 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 Cisco SD-WAN Manager.

24. Click **Next**.

    The **Policy Summary** page is displayed. For information on this page, see Create Unified Security Policy Summary.

Configure Cisco Catalyst SD-WAN Identity-Based Firewall Policy Using a CLI Template

The following sections provide details about the tasks relating to configuring a connection to Cisco ISE, and creating a identity-based firewall policy using the CLI template.

Configure Cisco SD-WAN Controller to Connect to Cisco ISE Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides sample CLI configurations to configure a Cisco SD-WAN Controller to connect to Cisco ISE.

The following example shows how to configure a Cisco SD-WAN Controller connection to Cisco ISE:

```
identity
  pxgrid
    server-address <name>
    username <name>
    password <name>
    subscriptions {user-identity | sgt}
    domain-name <domain-name>
    vpn 0
```

Here is the complete configuration example that shows how to connect a Cisco SD-WAN Controller to Cisco ISE:

```
identity
 pxgrid
  server-address 10.27.216.141
  user-name      vIPtela_Inc_Regression_vsmart1644552134629
  password       $8$TVGuJQn$8$TVG
  subscriptions user-identity
  domain-name    SDWAN-IDENTITY.CISCO.COM
  vpn 0
 !
!
```

Configure Identity-Based Firewall Policy Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides sample CLI configurations to configure an identity-based firewall policy:

The following example shows how to configure an identity-based firewall policy:

```
class-map type inspect match-any cm3
    match identity user-group source Engineering
    match identity user-group source Security
    match identity user source Jim

class-map type inspect match-all cm4
    match access-group name <>
    match <application-class>
    match <protocol-class>
    match <identity-class-cm3>

policy-map type inspect pm1
    class type inspect cm4
         inspect
```

Here is the complete configuration example that shows how to configure an Cisco Catalyst SD-WAN identity-based firewall on a Cisco IOS XE Catalyst SD-WAN device.

```
class-map type inspect match-any TestID
 match identity source user-group "SDWAN-IDENTITY.CISCO.COM/Users/Domain Users"
class-map type inspect match-all visFW-seq-1-cm_
 match access-group name visFW-seq-Rule_1-acl_
class-map type inspect match-all visFW-seq-11-cm_
 match class-map TestID
 match access-group name visFW-seq-Rule_2-acl_

policy-map type inspect visFW
 class type inspect visFW-seq-1-cm_
  inspect
 class type inspect visFW-seq-11-cm_
  inspect
 class class-default
  drop
```

```
ip access-list extended visFW-seq-Rule_1-acl_
 11 permit object-group visFW-Rule_1-svc_ object-group visFW-Rule_1-nw-src_ any
ip access-list extended visFW-seq-Rule_2-acl_
 11 permit object-group visFW-Rule_2-svc_ any any

object-group network visFW-Rule_1-nw-src_
 10.1.1.0 255.255.255.0
object-group service visFW-Rule_1-svc_
 ip
object-group service visFW-Rule_2-svc_
 ip
 11 permit object-group visFW-Rule_1-svc_ object-group visFW-Rule_1-nw-src_ any
 11 permit object-group visFW-Rule_2-svc_ any any

 vpn zone security
zone security Zone23
 vpn 2
 vpn 3
zone security zone0
 vpn 0
zone-pair security ZP_Zone23_zone0_visFW source Zone23 destination zone0
 service-policy type inspect visFW
```

Monitor Cisco Catalyst SD-WAN Identity-Based Firewall Policy

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Click the Cisco SD-WAN Controller that you want to monitor.

3. Click **Real Time** in the left pane.

4. Choose one of the following options from the **Device Options** drop-down list to view IP-address-to- user mappings and username-to-user-group mappings.

   - **Idmgr User to Usergroup Bindings**
   - **Idmgr IP to User Bindings**
   - **Idmgr IP to SGT Bindings**

For unified security policies, you can view the log data for security connection events. These events contain log data of important information when a flow passes through various security features such as zone-based firewall (ZBFW) and unified threat defense (UTD). The log data includes information about security policies and rules about traffic or sessions, along with the associated port, protocol, or applications. See Monitor Unified Logging Security Connection Events.

Monitor Cisco Catalyst SD-WAN Identity-Based Firewall Using the CLI

The following is a sample output from the **show idmgr pxgrid-status** command executed on Cisco SD-WAN Controllers. The command output shows the Identity Manager status for pxGrid connections.

```
Device# show idmgr pxgrid-status

idmgr pxgrid-status default
```

```
-----------------------------------------
Identity Manager Tenant - default
-----------------------------------------
State                          Connection and subscriptions successful
Current event                  EVT-None
Previous event                 Session websocket create event
Session base URL               https://ise-sdwan-team.cisco.com:8910/pxgrid/mnt/sd
Session pubsub base URL        wss://ise-sdwan-team.cisco.com:8910/pxgrid/ise/pubsub
Session topic                  /topic/com.cisco.ise.session
UserGroups topic               /topic/com.cisco.ise.session.group
Websocket status               ws-connected
Last notification sent         Connection successful
Timestamp of recent session    2022-02-18T13:00:54.372-05:00
```

The following is a sample output from the **show idmgr user-sessions** command executed on Cisco SD-WAN Controllers. The command output shows the user sessions learned from ISE.

Note Enable **passive ID** under external identity source while adding Active Directory (AD) to Cisco ISE to see the user sessions from ISE and Cisco SD-WAN Manager.

```
Device# show idmgr user-sessions

USERNAME                            ADDRESS   TIMESTAMP                      STATE

------------------------------------------------------------------------------------------
TestUser0@SDWAN-IDENTITY.CISCO.COM  72.1.1.7  2022-02-18T13:00:54.372-05:00  Authenticated
```

The following is a sample output from the **show idmgr omp ip-user-bindings** command executed on Cisco SD-WAN Controller. The command output shows the ip-user session bindings sent to Overlay Management Protocol (OMP).

```
Device# show idmgr omp ip-user-bindings

IP                                            OMP UPDATE STATE
ADDRESS   USERNAME
-----------------------------------------------------------
10.1.1.7  TestUser0@SDWAN-IDENTITY.CISCO.COM  omp-updated
```

The following is a sample output from the **show idmgr omp user-usergroup-bindings** command executed on Cisco SD-WAN Controllers. The command output shows the user-user-group bindings sent to OMP.

```
Device# show idmgr omp user-usergroup-bindings

idmgr omp user-usergroup-bindings TestUser0@SDWAN-IDENTITY.CISCO.COM
 user-groups      "Unknown sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513 SDWAN-IDENTITY.CISCO.COM/Builtin/Users
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users "
 omp-update-state omp-updated
idmgr omp user-usergroup-bindings TestUser1@SDWAN-IDENTITY.CISCO.COM
 user-groups      "Unknown sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513 SDWAN-IDENTITY.CISCO.COM/Builtin/Users
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users "
 omp-update-state omp-updated
idmgr omp user-usergroup-bindings adsclient
 user-groups      "User Identity Groups:Employee User Identity Groups:TestUserGroup-1 null
 null "
 omp-update-state omp-updated
```

The following is a sample output from the **show uidp statistics** command executed on an edge device. The command output shows the UIDP statistics.

```
Device# show uidp statistics
---------------------------------------
 Add/Delete Stats
---------------------------------------
Total Users added            : 22
Total Usergroups added       : 12
Total SGT added              : 0
Total Users deleted          : 0
Total Usergroups deleted     : 0
Total SGT deleted            : 0
---------------------------------------
 Add/Delete Error Stats
---------------------------------------
 User add error              : 0
 Usergroup add error         : 0
 SGT add error               : 0
 User delete error           : 0
 Usergroups delete error     : 0
 SGT delete error            : 0
---------------------------------------
 Memory allocation error Stats
---------------------------------------
 ipvrf key list create error : 0
 Index list create error     : 0
 Memory allocation error     : 0
 Invalid binding event       : 0
-----------------------------------------------
 DB Add/Delete Bindings stats
-----------------------------------------------
 Total IP User binding added             : 341
 Total IP User binding delete            : 0
 Total IP User binding add error         : 0
 Total IP User binding delete error      : 0
 Total User Usergroups binding added        : 20
 Total User Usergroups binding deleted      : 0
 Total User Usergroups binding add error    : 0
 Total User Usergroups binding delete error : 0
```

The following is a sample output from the **show uidp user-group all** command executed on an edge device. The command output shows the UIDP user group information.

```
Device# show uidp user-group all
Total Usergroups : 12
-------------------------
SDWAN-IDENTITY.CISCO.COM/Builtin/Users
User Identity Groups:Employee
User Identity Groups:TestUserGroup-1
null
Unknown
sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users
cisco
eng
dev
mgmt
cEdge-identity#
cEdge-identity#sh uidp user-group us
cEdge-identity#sh uidp user ?
  all   Show all users info
  ip    Show user info by ip
  name  Show user info by user name
```

The following is a sample output from the **show uidp user ip** command executed on an edge device.

```
Device# show uidp user ip 10.1.1.7

User Info 1 : TestUser0@SDWAN-IDENTITY.CISCO.COM
cEdge-identity#sh uidp user name TestUser0@SDWAN-IDENTITY.CISCO.COM
------------------------------------------------------------------------------------------
User Id    User Name                            IP address
    VRF   Usergroup  Usergroup Name
------------------------------------------------------------------------------------------
1          TestUser0@SDWAN-IDENTITY.CISCO.COM   72.1.1.7
    0     1          SDWAN-IDENTITY.CISCO.COM/Builtin/Users

          5          Unknown

          6          sdwan-identity.cisco.com/S-1-5-32-545

          7          S-1-5-21-787885371-2815506856-1818290038-513

          8          SDWAN-IDENTITY.CISCO.COM/Users/Domain Users
```

The following is a sample output from the **show idmgr omp ip-sgt-bindings** command executed on a Cisco SD-WAN Controller. The command output shows the SGT information by IP address.

```
Device# show idmgr omp ip-sgt-bindings

                  VPN       OMP UPDATE
IP PREFIX         ID   SGT  STATE
-------------------------------------
10.0.0.0/32        2    9    omp-updated
10.0.0.1/32        2    9    omp-updated
10.255.255.254/32  0    15   omp-updated
10.255.255.255/32  2    4    omp-updated
172.16.0.0/32      3    8    omp-updated
172.16.0.1/32      3    12   omp-updated
192.168.0.0/32     0    15   omp-updated
```

The following is a sample output from the **show cts role-based sgt-map all** command.

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

              VPN
IP Address     ID   SGT  Source
-------------------------------------
10.0.0.0       2    9    OMP
10.0.0.1       2    9    OMP
172.16.0.0     0    15   OMP
172.16.0.1     2    4    OMP
192.168.0.0    3    8    OMP

IP-SGT Active Bindings Summary
-------------------------------------
Total number of OMP bindings = 5
Total number of active bindings = 5
```

Troubleshooting Cisco Catalyst SD-WAN Identity-Based Firewall Policy

User Traffic is Dropped

Problem

User traffic is dropped when it must actually be allowed, based on the policy.

Possible Causes

This issue arises when there are errors while configuring user sessions. Use the **show** commands to verify the user session configuration both on the Cisco Catalyst SD-WAN Controller and on the Cisco IOS XE Catalyst SD-WAN device. See Monitor Cisco Catalyst SD-WAN Identity-Based Firewall Using the CLI to view the **show** commands used to the monitor identity-based firewall policy.

Solution

Ensure that the user session information is available on the device for policy enforcement.

Configuration Example for Cisco Catalyst SD-WAN Identity-Based Firewall

The following example shows how to configure connectivity from the Cisco Catalyst SD-WAN Controller to the Cisco ISE:

```
identity
 pxgrid
  server-address 10.27.216.141
  user-name      vIPtela_Inc_Regression_vsmart1644552134629
  password       $8$TVGurOH2PcGuJQnUUyDku5BkdBae5BpmIyBCqpv555U05MccrXQ97hQkkCaRNh6W
  subscriptions user-identity
  domain-name    SDWAN-IDENTITY.CISCO.COM
  vpn 0
 !
!
```

The following example shows how to configure a Cisco Catalyst SD-WAN identity-based firewall on a Cisco IOS XE Catalyst SD-WAN device:

```
class-map type inspect match-any TestID
 match identity source user-group "SDWAN-IDENTITY.CISCO.COM/Users/Domain Users"
class-map type inspect match-all visFW-seq-1-cm_
 match access-group name visFW-seq-Rule_1-acl_
class-map type inspect match-all visFW-seq-11-cm_
 match class-map TestID
 match access-group name visFW-seq-Rule_2-acl_

policy-map type inspect visFW
 class type inspect visFW-seq-1-cm_
  inspect
 class type inspect visFW-seq-11-cm_
  inspect
 class class-default
  drop

ip access-list extended visFW-seq-Rule_1-acl_
 11 permit object-group visFW-Rule_1-svc_ object-group visFW-Rule_1-nw-src_ any
ip access-list extended visFW-seq-Rule_2-acl_
 11 permit object-group visFW-Rule_2-svc_ any any
```

```
object-group network visFW-Rule_1-nw-src_
 10.1.1.0 255.255.255.0
object-group service visFW-Rule_1-svc_
 ip
object-group service visFW-Rule_2-svc_
 ip
 11 permit object-group visFW-Rule_1-svc_ object-group visFW-Rule_1-nw-src_ any
 11 permit object-group visFW-Rule_2-svc_ any any

 vpn zone security
zone security Zone23
 vpn 2
 vpn 3
zone security zone0
 vpn 0
zone-pair security ZP_Zone23_zone0_visFW source Zone23 destination zone0
 service-policy type inspect visFW
```

CHAPTER 6

Configure Geolocation-Based Firewall Rules for Network Access

Table 24: Feature History

Feature Name	Release Information	Description
Geolocation-Based Firewall Rules for Allowing or Denying Network Traffic Based on Geolocation	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	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. 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. New object-group and geo commands were added.

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 SD-WAN Manager, 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 SD-WAN Manager. 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 SD-WAN Manager.

There are two ways to configure geofiltering using Cisco SD-WAN Manager:

- 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 SD-WAN Manager 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 SD-WAN Manager 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 update the geolocation database using the CLI:

On the CLI, use Secure Copy Protocol (SCP) or TFTP to copy the geolocation database to your Cisco IOS XE Catalyst 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 SD-WAN Manager, 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

Table 25: Feature History

Feature Name	Release Information	Description
Snort Engine Version Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature adds support for Snort engine version 3, which is an upgrade from version 2.

This feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco Catalyst SD-WAN. It is delivered using a virtual image on Cisco IOS XE Catalyst 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

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 Cisco SD-WAN Manager 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 Catalyst 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. Cisco SD-WAN Manager periodically downloads signature packages to the Snort sensors. You can modify the time interval to check for and download signature updates in **Administration** > **Settings** > **IPS Signature Update** (in releases through Cisco vManage Release 20.9.1) or **Administration** > **Settings** > **UTD Snort Subscriber Signature** (in releases beginning with Cisco vManage Release 20.10.1).

Note Options for downloading UTD signature packages out of band from Cisco.com and uploading them to Cisco SD-WAN Manager or a remote server and options for custom signatures are available from Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

- Alert/Reporting server: Receives alert events from the Snort sensor. Alert events generated by the Snort sensor can either be sent to Cisco SD-WAN Manager or an external syslog server or to both Cisco SD-WAN Manager and an external syslog server. Cisco SD-WAN Manager 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 Catalyst 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 SD-WAN Manager.

Configure Intrusion Prevention or Detection

To configure Intrusion Prevention or Detection through a security policy, use the Cisco SD-WAN Manager security configuration wizard:

1. From the Cisco SD-WAN Manager 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 Cisco SD-WAN Manager menu, **Configuration** > **Security** wizard.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

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

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

Modify an Intrusion Prevention or Detection Policy

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

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 Cisco IOS XE Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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

Supported releases: Cisco SD-WAN Release 20.9.1 and earlier releases

IPS uses Cisco TALOS signatures to monitor the network. We recommend that you use the following procedure to download the latest signatures.

Note To download the signatures, Cisco Catalyst SD-WAN Manager requires access to the following domains using port 443:

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

1. From the Cisco SD-WAN Manager 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.

Update IPS Signatures and Custom Signature Rules

Table 26: Feature History

Feature Name	Release Information	Description
IPS Custom Signature and Offline Updates	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature lets you download IPS signature packages for the Intrusion Prevention System (IPS) out-of-band from Cisco SD-WAN Manager and upload these packages to Cisco SD-WAN Manager or a remote server. Cisco SD-WAN Manager then distributes these IPS signature packages to the devices on your network. This feature also lets you upload a custom signature rules file to Cisco SD-WAN Manager or a remote server, which Cisco SD-WAN Manager then distributes and appends to the existing IPS signature package rules.

Information About IPS Custom Signature and Offline Updates

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, if Cisco SD-WAN Manager does not have an internet connection, you can download IPS signature packages locally and either upload them directly to Cisco SD-WAN Manager or to a remote server or servers to which your devices have network access. Cisco SD-WAN Manager does not need to have network access to the remote servers. You also can append custom signature rules to the current Cisco TALOS signature rules file. This custom signature rules file can also be uploaded to Cisco SD-WAN Manager or to a remote server or servers to which your devices have network access.

The filename of an IPS signature package has the format shown in this example, where the numbers represent the Snort engine version and the version of the IPS signature package:
UTD-STD-SIGNATURE-29181-105-S.pkg

The first number is the Snort engine version and the second number is the version of the IPS signature package for the Snort engine. In this example, the filename represents the 105th release of the IPS signature package for the 2.9.18.1 Snort engine.

Prerequisites for IPS Custom Signature and Offline Updates

- To download the signatures, Cisco SD-WAN Manager requires access to the following domains using port 443:

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

- If you enable **IPS Signatures** and choose the **Remote Server** or **Local** option, you must download a separate IPS signature package for each Snort engine version that is used in your network.

  You can download the latest IPS signature packages for your Snort engines from the following page. The latest IPS signature package for each Snort engine is shown at the top left corner of this page.

  https://software.cisco.com/download/home/284389362/type/286285292/release/

  To determine the version of the Snort engine or engines that you are using, you can use the **show utd engine standard version** command or check the UTD package filename.

  For example, in the following output of the **show utd engine standard version** command, the Snort engine version number is 2.9.18.1, so you should use the latest 29181 IPS signature package release:

  ```
  Device# show utd engine standard version
  IOS-XE Recommended UTD Version: 1.0.6_SV2.9.18.1_XE17.9
  IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.9$
  ```

  Similarly, in the following UTD package filename, the Snort engine version number is 2.9.18.1, so again you should use the latest 29181 IPS signature package release:

secapp-utd.17.09.01a.1.0.6_SV**2.9.18.1**_XE17.9.x86_64.tar

- The IPS signature packages are updated approximately every 24 to 72 hours. If you enable **IPS Signatures** and choose the **Remote Server** or **Local** option, we recommend that you check for new IPS signature packages daily to ensure that the IPS signature packages that you are using are up to date.
- If you use an IPS signature package file on a remote sever and the filename that Cisco SD-WAN Manager points to includes the IPS signature package version, you must update the filename that Cisco SD-WAN Manager points to each time a new IPS signature package is uploaded to the remote server, for each Snort engine version used.

Configure IPS Custom Signature and Offline Updates

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

Use the procedure that this section describes to update IPS signatures and custom signature rules.

Before you begin, if you are using a remote server, we recommend that you perform either of the following actions for each Snort engine version that you are using to avoid needing to manually update the path in Cisco SD-WAN Manager each time a new IPS signature package is uploaded to the remote server:

- Remove the signature package version number (keeping the Snort engine version number) from the filename that Cisco SD-WAN Manager points to and override this filename on the remote server each time a new IPS signature package is uploaded for this Snort engine version.

  For example, rename UTD-STD-SIGNATURE-29181-105-S.pkg to UTD-STD-SIGNATURE-29181-S.pkg on the remote server and have Cisco SD-WAN Manager point to this filename. Then override this filename each time a new IPS signature package for the 2.9.18.1 Snort engine is uploaded to the remote server. Perform a similar action for each Snort engine version that is used.
- Use a symbolic link (symlink) on the remote server and update it to point to the latest IPS signature package each time a new IPS signature package is uploaded for a Snort engine version. In this case, have Cisco SD-WAN Manager point to this symbolic link.
- Every time you update the UTD signatures on Cisco IOS XE Catalyst SD-WAN devices, you must update the IPS signature package file on the remote server and on Cisco SD-WAN Manager.
- For a custom signature file, you must login to Cisco SD-WAN Manager and update the custom signature's file attributes, and these attributes are included in the UTD signature package metadata sent to the Cisco IOS XE Catalyst SD-WAN devices. This indicates that the custom signature file on the remote server has been updated and the file needs to be downloaded and applied on the device.

  For example, have a symbolic link called UTD-STD-SIGNATURE-29181-S.pkg that points to UTD-STD-SIGNATURE-29181-105-S.pkg on the remote server and have Cisco Catalyst SD-WAN Manager point to this symbolic link. Then update the file that this symbolic link points to each time a new IPS signature package for the 2.9.18.1 Snort engine is uploaded to the remote server. Perform a similar action for each Snort engine version that is used.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** in the **UTD Snort Subscriber Signature** row.

3. In the **IPS Signature Download Interval Hours** and **Minute** fields, enter how often Cisco SD-WAN Manager attempts to download new IPS signature packages from Cisco.com.

   This interval is also used for how often Cisco SD-WAN Manager has the devices attempt to download the latest IPS signature package or packages and custom signature rules file from Cisco SD-WAN Manager or the remote server or servers.

   You can enter an interval from 2 hours to 24 hours. The default interval is 24 hours.

4. To enable the IPS signature package update, enable the **IPS Signatures** option, then click one of the following radio buttons to specify how the IPS signature packages are distributed by Cisco SD-WAN Manager:

   - **Cisco.com**: Downloads IPS signature packages to Cisco SD-WAN Manager from Cisco.com, then causes the devices to download the IPS signature packages from Cisco SD-WAN Manager. This option requires that Cisco SD-WAN Manager has an internet connection.

     In the **Username** and **Password** fields, enter your Cisco Connection Online username and password.

   - **Remote Server**: Devices download the IPS signature packages from one or more remote servers over a local network connection, not from Cisco SD-WAN Manager. We recommend that you use this option to avoid Cisco SD-WAN Manager scaling issues.

     From the **Select Remote Server** drop-down list, choose a remote server (you can use the **Search** field to find a server), or click **Add Remote Server** to configure a new remote server.

     If you click **Add Remote Server**, perform these actions:

     a. Enter information for this server in the following fields:

Field	Description
Server Name	Name of the server
Server IP/DNS name	IP address or DNS hostname of the server
Select Protocol	Protocol that is used for the Cisco SD-WAN Manager network connection to the server (**FTP**, **HTTP**, or **SCP**)
Port	Port on the server that is used for access to the server
User ID	Username for access to the server
Password	Password for access to the server
Image location prefix:	Path to the folder that contains the IPS signature package
VPN	VPN used for access to the server, from 0 through 65527

     b. Click **Add** and choose the server from the **Select Remote Server** drop-down list.

     c. Click the **Remote Server Details** box that appears.

d. In the **IPS Signature Filename** field, enter the filename of the IPS signature package or the symbolic link to this IPS signature package that is on the remote server.

e. In the **IPS Signature Snort Version** field, enter the Snort engine version of the IPS signature package.

f. Click **Add**.

- **Local**: Uploads IPS signature packages from a local computer to Cisco SD-WAN Manager, then causes the devices to download the IPS signature packages from Cisco SD-WAN Manager.

  In the field that appears, click **Choose Files** and choose the IPS signature package, or drag and drop an IPS signature package. Then click **Add**.

5. (Optional) To change the IPS signature filename or Snort engine version for an IPS signature package on a remote server, perform the following actions.

Note If you are overwriting the filename or using a symbolic link for the file that Cisco SD-WAN Manager points to, you do not need to perform this step each time a new IPS signature package is uploaded to the remote server.

a. Under **IPS Signatures**, click **Remote Server**.

b. From the **Select Remote Server** drop-down menu, choose the server for which you want to update information.

c. Click the server in the **Remote Server Details** box that appears.

d. In the **IPS Signature Filename** field, enter the name of the IPS signature package file that is on the remote server.

e. In the **IPS Signature Snort Version** field, enter the Snort engine version of the IPS signature package.

f. Click **Add**.

6. To append custom signature rules to the current IPS signature package, enable **Custom Signature**, then click one of the following radio buttons to specify the location of the custom signature rules file.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, the Snort engine version has been upgraded from version 2 to version 3.

   The custom signature rules file must be a text file that contains rules in the appropriate Snort engine version rule format, be no larger than 1 MB, and have the .txt or .rules extension. Each rule should use the generator ID 1 or no generator ID (which defaults to 1), and the signature ID should be unique and greater than 1000000.

Note Cisco does not provide support for writing custom signatures or resolving issues with custom signatures and may request that you disable custom signatures before troubleshooting an issue.

Note Snort 2 and Snort 3 supported UTD versions cannot be used in combination with custom signatures since the custom signatures rules must either be in Snort 2 or Snort 3 format.

- **Remote Server**: Devices download the custom signature rules file from one or more remote servers over a local network connection, not from Cisco SD-WAN Manager. We recommend that you use this option to avoid Cisco SD-WAN Manager scaling issues.

  From the **Select Remote Server** drop-down list, choose a remote server(you can use the **Search** field to find a server), or click **Add Remote Server** to configure a new remote server.

  If you click **Add Remote Server**, perform these actions:

  a. Enter information for this server in the configuration fields. These fields are the same as the ones that are described for **Add Remote Server** in Step 4.

  b. Click **Add** and choose the server from the **Select Remote Server** drop-down list.

  c. Click the **Remote Server Details** box that appears.

  d. In the **Custom Signature Filename** field, enter the name of the custom signature rules file that is on the remote server.

  e. Click **Add**.

- **Local**: Uploads a custom signature rules file from a local computer to Cisco SD-WAN Manager, then causes the devices to download the custom signature rules file from Cisco SD-WAN Manager.

  In the field that appears, click **Choose Files** and choose the custom signature rules file, or drag and drop the custom signature rules file. Then click **Add**.

7. (Optional) To change the name of the custom signature rules file that is on a remote server, perform the following actions.

Note If you are overwriting the filename or using a symbolic link for the file that Cisco SD-WAN Manager points to, you do not need to perform this step each time a new custom signature rules file is uploaded to the remote server.

   a. Under **Custom Signature**, click **Remote Server**.

   b. From the **Select Remote Server** drop-down menu, choose the server for which you want to update information.

   c. Click the server in the **Remote Server Details** box that appears.

   d. In the **Custom Signature Filename** field, enter the name of the custom signature rules file that is on the remote server.

   e. Click **Add**.

8. If you are appending custom signature rules to the current IPS signature package, perform these actions to enable custom signatures for a security policy:

a. From the Cisco SD-WAN Manager window, choose **Configuration** > **Security**.

b. Choose **Custom Options** > **Policies/Profiles**.

c. In the left panel, click **Intrusion Prevention**.

d. For the desired policy, click **...** and choose **Edit**.

e. Under the **Advanced** options, enable **Custom Signature Set** for the custom rules to be appended.

Process Single Stream Large Session (Elephant Flow) by UTD

Introduction

This document describes why a single flow cannot consume the entire rated throughput of a Cisco Unified Threat Defense (UTD) deployment.

Background Information

The result of any bandwidth speed testing website, or the output of any bandwidth measurement tool (for example, iperf) might not exhibit the advertised throughput rating of a Cisco UTD deployment. Similarly, the transfer of a very large file over any transport protocol does not demonstrate the advertised throughput rating of a Cisco UTD deployment. It occurs because the UTD service does not use a single network flow in order to determine its maximum throughput.

Process Traffic by Snort

The underlying detection technology of the UTD service is Snort. A Cisco UTD deployment (router model and UTD resource profile) is rated for a specific rating based on the total throughput of all flows that goes through the UTD container. It is expected that the routers with UTD are deployed on a Corporate network, usually near the border edge and works with thousands of connections.

Depending on the UTD resource profile used, UTD uses load balancing of traffic to a number of different Snort processes. Ideally, the system load balances traffic evenly across all of the Snort processes. Snort needs to be able to provide proper contextual analysis for Next-Generation Firewall (NGFW), Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) inspection. In order to ensure Snort is most effective, all the traffic from a single flow is load balanced to one Snort instance. If all the traffic from a single flow was not balanced to a single Snort instance, the system could be evaded and the traffic would spilt in such a way that a Snort rule might be less likely to match or pieces of a file are not contiguous for AMP inspection. Therefore, the load balancing algorithm is based on the connection information that can uniquely identify a given connection.

Traffic is load balanced to Snort using a 3-tuple algorithm. The datapoints for this algorithm are:

- Source IP
- Destination IP
- VRF

Any traffic with the same source, destination, and VRF are load balanced to the same instance of Snort.

Total Throughput

The total throughput of a UTD deployment is measured based on the aggregate throughput of all the Snort instances that work to their fullest potential. Industry standard practices in order to measure the throughput are for multiple HTTP connections with various object sizes. For example, the Network Security Services (NSS) NGFW test methodology measures total throughput of the device with 44k, 21k, 10k, 4.4k, and 1.7k objects. These translate to a range of average packet sizes from around 1k bytes to 128 bytes because of the other packets involved in the HTTP connection.

Different types of traffic, network protocols, sizes of the packets along with differences in the overall security policy can all impact the observed throughput of the device.

Third Party Tool Test Result

When you test with any speed testing website, or any bandwidth measurement tool, such as, iperf, one large single stream TCP flow is generated. This type of large TCP flow is called an Elephant Flow. An Elephant Flow is a single session, relatively long running network connection that consumes a large or disproportionate amount of bandwidth. This type of flow is assigned to one Snort instance, therefore the test result displays the throughput of single Snort instance, not the aggregate throughput rating of the UTD deployment.

Remediations

Configure a unified security policy so that trusted traffic can be exempted from UTD inspection to avoid any latency during data transfer. For more information about configuring a unified security policy, see Unified Security Policy.

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 Catalyst SD-WAN devices.

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

1. From the Cisco SD-WAN Manager 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. The **Policy Mode** can only be set at time of creation and cannot be modified after the policy has been saved.

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

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 Catalyst 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, Cisco SD-WAN Manager 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 Cisco SD-WAN Manager, 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 Cisco SD-WAN Manager, 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).
- You can 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.

Note If you are using the *www* prefix in the allowed or blocked regex pattern, it can create a problem if the Server Name Indicator (SNI) returned in the client message doesn't match. For example, if you want to allow *www./foo./com* and SNI returns as *foo.com* only. We recommend not to include the *www* in the regex match.

For more information, see Regular Expression for URL Filtering and DNS Security, on page 471.

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 Catalyst 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 SD-WAN Manager.

Configure URL Filtering

To configure URL Filtering through a security policy, use the Cisco SD-WAN Manager security configuration wizard:

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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.

      You can use Look up URL or IP tool to validate how a website is classified using URL-Filtering feature. It only shows the output for the configured URL filtering alerts or events.

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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

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

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

Modify URL Flitering

To modify a URL Filtering policy, do the following:

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 Cisco IOS XE Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

    Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

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 Catalyst SD-WAN devices.

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

1. From the Cisco SD-WAN Manager 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 the advanced malware protection used in a unified security policy.
- You can enable Policy Mode only when creating advanced malware protection policies. You cannot configure the unified mode once the policy is saved.

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.

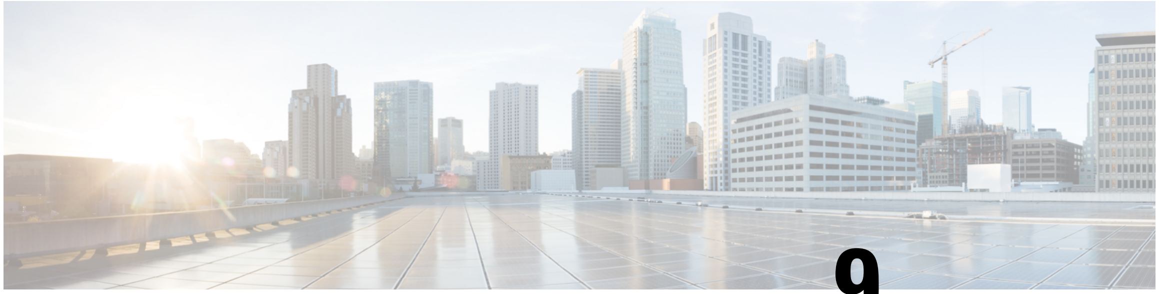
13. (Optional) In the **Alerts and Logs** pane, choose alert type option:

    - **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 Cisco Catalyst 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 27: Feature History

Release	Description
Cisco SD-WAN 19.1	Feature introduced. The Cisco Advanced Malware Protection (AMP) integration equips routing and Cisco Catalyst SD-WAN platforms to provide protection and visibility to cover all stages of the malware lifecycle.

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.

Note The maximum file size that will be inspected by AMP is 10 MB.

Note File Reputation supports the following file types: ACCDB, ALZ, AMF, AMR, ARJ, ASF, AUTORUN, BINARY_DATA, BINHEX, BMP, BZ, CPIO_CRC, CPIO_NEWC, CPIO_ODC, DICM, DMG, DMP, EGG, EICAR, ELF, EPS, FFMPEG, FLAC, FLIC, FLV, GIF, GZ, HLP, HWP, ICO, IMG_PCT, ISHIELD_MSI, ISO, IVR, JAR, JARPACK, JPEG, LHA, M3U, MACHO, MAIL, MAYA, MDB, MDI, MIDI, MKV, MNY, MOV, MP3, MP4, MPEG, MSCAB, MSCHM, MSOLE2, MSWORD_MAC5, MSZDD, MWL, NEW_OFFICE, NTHIVE, OGG, OLD_TAR, ONE, PCAP, PDF, PGD, PLS, PNG, POSIX_TAR, PSD, PST, RA, RAR, REC, REG, RIFF, RIFX, RIM, RMF, RPM, RTF, S3M, SAMI, SCRENC, SIS, SIT, SMIL, SWF, SYLKc, SYMANTEC, TIFF, TNEF, TORRENT, UUENCODED, VMDK, WAV, WEBM, WMF, WP, WRI, XLW, XPS, ZIP, ZIP_ENC, 7Z, 9XHIVE.

- 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. File Analysis supports a maximum file size of 10MB.

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 Catalyst SD-WAN device, do the following:

- Before you Begin, on page 171
- Configure an Advanced Malware Policy

- Apply a Security Policy to a Device, on page 61

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 SD-WAN Manager.
- 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 SD-WAN Manager 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 steos:

a) Choose a region from the **Region** drop-down menu.

b) Enter the API key in the **Key** field.

c) Click **Add**.

d) Click **Save Changes**.

Configuring an Advanced Malware Protection Policy

To configure an Advanced Malware Protection policy:

Step 1 From the Cisco SD-WAN Manager 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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

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

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

Modify an Advanced Malware Protection Policy

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

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager menu, choose **Monitor** > **Devices**, and choose a device.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 Catalyst SD-WAN devices.

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

1. From the Cisco SD-WAN Manager 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.
- You can enable Policy Mode only when creating advanced malware protection policies. You cannot configure the unified mode once the policy is saved.

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.

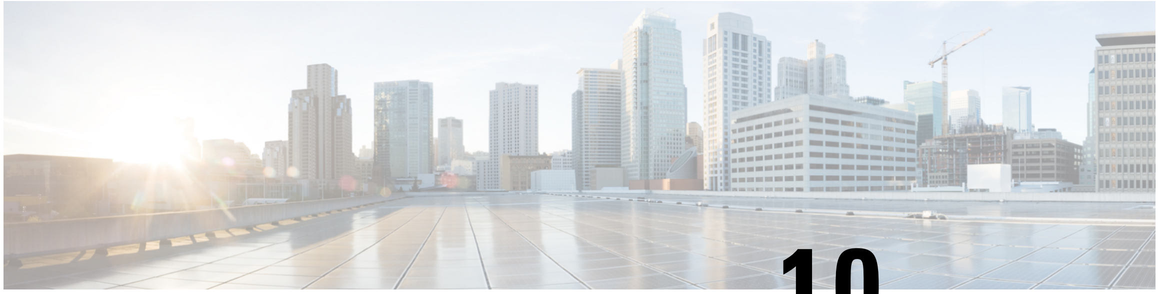
File Analysis requires a separate Threat Grid license.

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 28: Feature History

Feature Name	Release Information	Description
SSL/TLS Proxy	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	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. This feature is part of the Cisco Catalyst SD-WAN Application Quality of Experience (AppQoE) and UTD solutions.

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 polices 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.

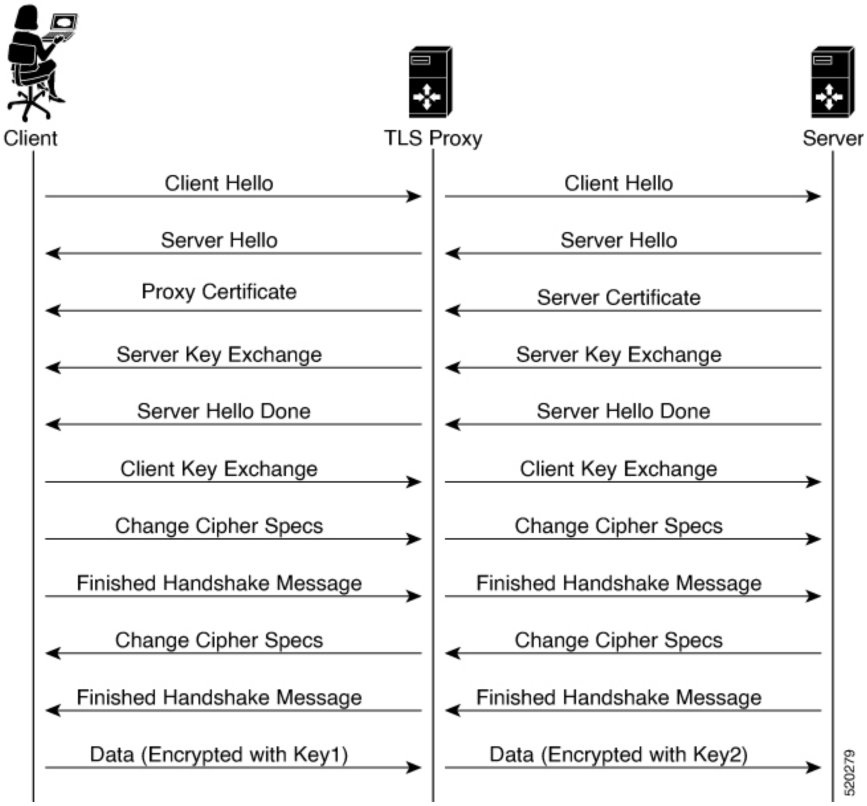
This is how traffic flows when TLS proxy is enabled:

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 4: TLS Handshake Process



Role of Certificate Authorities in TLS Proxy

About Certificate Authorities (CAs)

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

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

How CA and TLS Proxy Work Together

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

CA Options for Configuring TLS Proxy

The following CA options are supported for configuring TLS proxy:

- Enterprise CA
- Enterprise CA with SCEP Enabled
- Cisco SD-WAN Manager as CA
- Cisco SD-WAN Manager 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 SD-WAN Manager.

Table 29: Enterprise CA: Benefits and Limitations

Benefits	Limitations
• 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	• 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 30: Enterprise CA with SCEP: Benefits and Limitations

Benefits	Limitations
• 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	• 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 SD-WAN Manager • Enterprise CA have limited support for SCEP

Cisco SD-WAN Manager as CA

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

Table 31: Cisco SD-WAN Manager as CA: Benefits and Limitations

Benefits	Limitations
• Certificate deployment to proxy devices is automated • Certificates are reissued and revalidated before they expire • Certificates can be monitored, tracked, and validated through Cisco SD-WAN Manager	• Cisco SD-WAN Manager certificate needs to be pushed to the client trust store

Cisco SD-WAN Manager as Intermediate CA: Benefits and Limitations

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

Table 32: Cisco SD-WAN Manager as Intermediate CA: Benefits and Limitations

Benefits	Limitations
• 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 SD-WAN Manager • No other certificates, besides your enterprise CA certificate, need to be pushed to your client trust-store	• Requires manual deployment • Maintaining two CAs causes administrative overload • Cisco SD-WAN Manager certificate usage is tracked through the enterprise CA • Deployment can be complex if your network has multiple Cisco SD-WAN Manager controllers for clustering or redundancy

Supported Devices and Device Requirements

The following devices support the SSL/TLS Proxy feature.

Table 33: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	• 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 Catalyst SD-WAN Release 17.3.2	• Cisco Catalyst 8300 Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	• 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; 16 GB for Cisco Catalyst 8300 Series Edge Platforms.
- The device must have a minimum of 8 vCPUs.

Supported Cipher Suites

The TLS Proxy feature in Cisco Catalyst 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 Catalyst SD-WAN solution.

Note Cisco recommends enabling TLS decryption only for encrypted traffic (for example HTTPS, SFTP) by creating a specific rule in the NG firewall policy. Unencrypted traffic should not be subjected to TLS decryption.

Limitations and Restrictions

- Only RSA and its variant cipher suites are 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.
- When a Cisco public key (PKI) certificate is installed on a device, and you want to make changes to the certificate, detach the security template from the device template and push the device template to the device. This will remove the existing PKI certificate and configuration. After you have made changes to the PKI certificate, re-attach the security template and then push the device template to the device. This process updates the device for any the changes to the Cisco PKI certificate.
- 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 Catalyst SD-WAN Devices as TLS Proxy

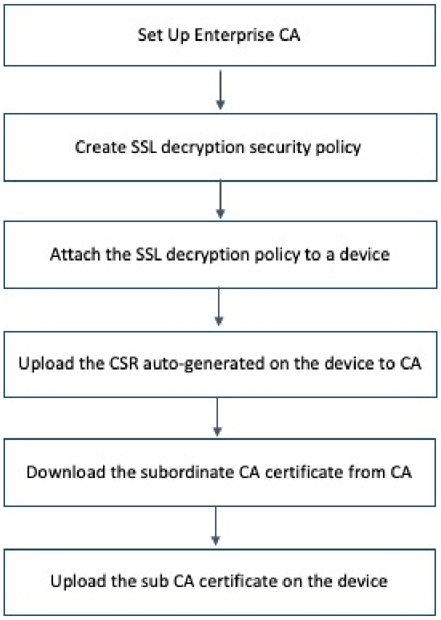
High-level Steps for Configuring a Device as TLS Proxy

1. Configure certificate authority (CA) for the TLS proxy: Enterprise CA, Cisco SD-WAN Manager as CA, or Cisco SD-WAN Manager 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 Cisco SD-WAN Manager as CA and Cisco SD-WAN Manager 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.

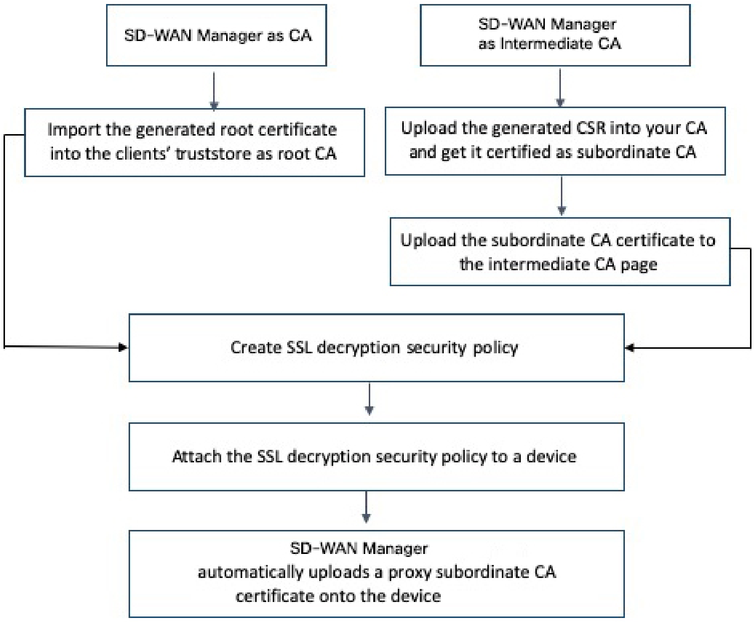
Figure 5: Use Enterprise CA to Configure TLS Proxy on a Device


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

Task Flow: of Set Up TLS Proxy with Cisco SD-WAN Manager as CA or Cisco SD-WAN Manager as Intermediate CA

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

Figure 6: Use Cisco SD-WAN Manager as CA or Cisco SD-WAN Manager as Intermediate CA to Configure TLS Proxy on a Device


SD-WAN Manager as CA
SD-WAN Manager as Intermediate CA
Import the generated root certificate into the clients' truststore as root CA
Upload the generated CSR into your CA and get it certified as subordinate CA
Upload the subordinate CA certificate to the intermediate CA page
Create SSL decryption security policy
Attach the SSL decryption security policy to a device
SD-WAN Manager automatically uploads a proxy subordinate CA certificate onto the device

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

Configure CA for TLS Proxy

Cisco SD-WAN Manager 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

- Time synchronization:

  To be able to configure CA certificates, ensure that the system time is synchronized for the CA server and the device seeking the certificate. See Configure NTP to learn how to coordinate and synchronize time across all devices in the Cisco Catalyst SD-WAN overlay network.

- Basic Constraint CA parameter for certificates:

  Ensure that the CA server is configured to issue certificates with the CA parameter of the X.509v3 Basic Constraints extension set to true.

Configure Enterprise CA

Note When configuring TLS/SSL proxy feature, trust point allows only two certificates; root certificate and certificate signed by root certificate. You cannot upload cert chain.

1. Download a CA certificate from your CA server in PEM or Base 64 format.
2. From the Cisco SD-WAN Manager 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 Cisco IOS XE Catalyst SD-WAN Device
10. Upload a Subordinate CA Certificate to TLS Proxy, on page 194

Configure Cisco SD-WAN Manager as CA

Configure Cisco SD-WAN Manager as CA to issue subordinate CA certificates to the proxy device at the edge of the network.

Use **SD-WAN as CA** if your enterprise does not have an internal CA. With this option, Cisco SD-WAN Manager 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 Cisco SD-WAN Manager as CA can be managed through Cisco SD-WAN Manager.

Prerequisites to Set Up CA for SSL/TLS Proxy

- Time synchronization:

  To be able to configure CA certificates, ensure that the system time is synchronized for the CA server and the device seeking the certificate. See Configure NTP to learn how to coordinate and synchronize time across all devices in the Cisco Catalyst SD-WAN overlay network.

- Basic Constraint CA parameter for certificates:

  Ensure that the CA server is configured to issue certificates with the CA parameter of the X.509v3 Basic Constraints extension set to true.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **TLS/SSL Proxy**.
2. Choose **SD-WAN as CA.**

Note Leave the **Set SD-WAN as Intermediate CA** check box not checked if you want to set Cisco SD-WAN Manager 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 Cisco SD-WAN Manager 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 SD-WAN Manager 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 Cisco IOS XE Catalyst SD-WAN Device

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

Configure Cisco SD-WAN Manager as Intermediate CA

Configure Cisco SD-WAN Manager as Intermediate CA to enable a TLS proxy device to use subordinate CA certificates issued by Cisco SD-WAN Manager.

When Cisco SD-WAN Manager is set as intermediate CA, your enterprise CA acts as the root CA and Cisco SD-WAN Manager 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 SD-WAN Manager to automate and manage certificate issuance and renewal.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **TLS/SSL Proxy**.
2. Choose **SD-WAN as CA.**
3. Check the **Set SD-WAN 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 SD-WAN Manager 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 SD-WAN Manager 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 Cisco IOS XE Catalyst SD-WAN Device

    When the SSL/TLS decryption security policy is attached to the device, Cisco SD-WAN Manager 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 Cisco SD-WAN Manager security configuration wizard:

1. From the Cisco SD-WAN Manager 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, Cisco SD-WAN Manager 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	• **Drop** the traffic • **Decrypt** the traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted	• **Drop** the traffic • **Decrypt** the traffic

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 `unknown`	• **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	• **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.	• **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.	• **Drop** the traffic • **No Decrypt**: The proxy does not decrypt this traffic.
Unsupported Cipher Suites	Defines what the policy should do if unsupported cipher suites are detected.	• **Drop** the traffic • **No Decrypt**: The proxy does not decrypt this traffic.
Failure Mode	Defines what the policy should do in the case of a failure.	• **Close**: Sets the mode as fail-close • **Open**: Sets the mode as fail-open.

Field Name	Description	Options
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**. **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.

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 Cisco IOS XE Catalyst SD-WAN Device

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. If you are creating a new device template:
   a. Click **Device Templates**, and click **Create Template**.

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

   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 Cisco IOS XE Catalyst SD-WAN Device

Generate CSR and Upload Subordinate CA Certificate to TLS Proxy

1. From the Cisco SD-WAN Manager 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=appqoe@cisco.com,cn=server-name,ou=AppQoE,o=CISCO,l=Blr,st=KA,c=IN
    Fingerprint MD5: 755C9485 DDACC0BD B5ED93E6 4E8A7DEB
    Fingerprint SHA1: 4D4380EA 07392044 6A5BF891 938AC610 C0C0AA6D
  Router General Purpose certificate configured:
    Subject Name:
     cn=sign
    Fingerprint MD5: 1956194E FEC057A3 8FE5BFA5 DD84662B
    Fingerprint SHA1: 864A8126 EBC780E2 D958AD86 93CB8923 3EF3B7FF
  State:
    Keys generated ............. Yes (General Purpose, non-exportable)
    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 SD-WAN Manager, run this command in CLI mode to verify if your configuration is applied.
- **show sdwan running-config**: In Cisco SD-WAN Manager, 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 SD-WAN Manager.

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

```
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 Qualifed 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 SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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 SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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, Cisco SD-WAN Manager as CA, and Cisco SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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 SD-WAN Manager 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**.

Cisco SD-WAN Manager as CA or Cisco SD-WAN Manager as Intermediate CA

If you have configured Cisco SD-WAN Manager as CA or Cisco SD-WAN Manager as Intermediate CA, follow the steps below to revoke or renew a certificate.

1. From the Cisco SD-WAN Manager 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 Catalyst 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 SD-WAN Manager 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 SD-WAN Manager 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. The **Policy Mode** can only be set at time of creation and cannot be modified after the policy has been saved.

- 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	• Drop the traffic by clicking **Drop** • Decrypt the traffic by clicking **Decrypt**
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted	• 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**	• 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	• **1024 bit RSA** • **2048 bit RSA** • **4096 bit RSA**
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.	—

Field Name	Description	Options
Minimum TLS Version Revocation Status	Sets the minimum version of TLS that the proxy should support.	• **TLS 1.0** • **TLS 1.1** • **TLS 1.2**

- 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.	• Drop the traffic by clicking **Drop** • Click **No Decrypt** so that the proxy does not decrypt this traffic.
Unsupported Cipher Suites	Defines what the policy should do if unsupported cipher suites are detected.	• Drop the traffic 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.	• **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**.
11. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
12. Edit the newly created policy.
13. Choose **NG Firewall**. Click **Add NG Firewall Policy** > **Create New.**
14. Click **Add Rule/Rule Set Rule**. In the **Action** field, click **Inspect**.
15. In the **Advanced Inspection Profile** field, select **New Advanced Inspection Profile List**. Set TLS Action to **Decrypt.**
16. Select the **TLS/SSL Decryption**.

17. Click **Save** in the Advanced Inspection Profile.
18. Click **Save** in the New Firewall Rule/Rule Set.
19. Click **Save Unified Security Policy**.
20. Choose **Policy Summary** and select the newly created TLS/SSL Decryption Policy.
21. Click **Save Policy Changes**.

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 Catalyst SD-WAN devices.

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

1. From the Cisco SD-WAN Manager 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**.

Note The **Policy Mode** can only be set at time of creation and cannot be modified after the policy has been saved.

CHAPTER 11

Cisco Umbrella Integration

The Cisco Catalyst 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.

Table 34: Feature History

Feature Name	Release Information	Description
Cisco Umbrella Scope Credentials	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS.

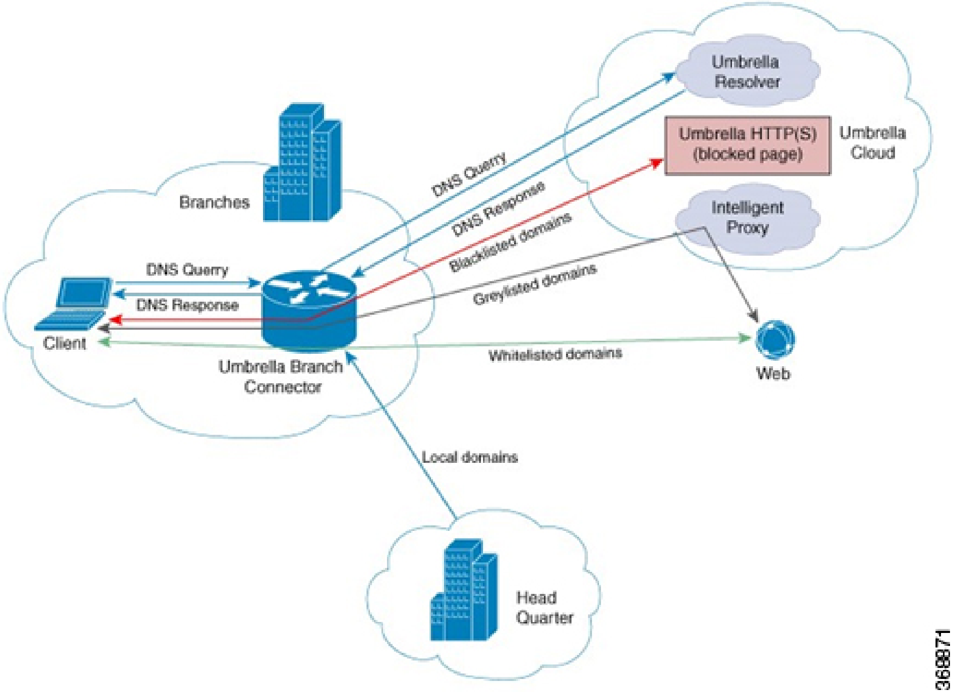
Overview of Cisco Catalyst SD-WAN Umbrella Integration

The Cisco Catalyst 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 7: 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 Catalyst 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.

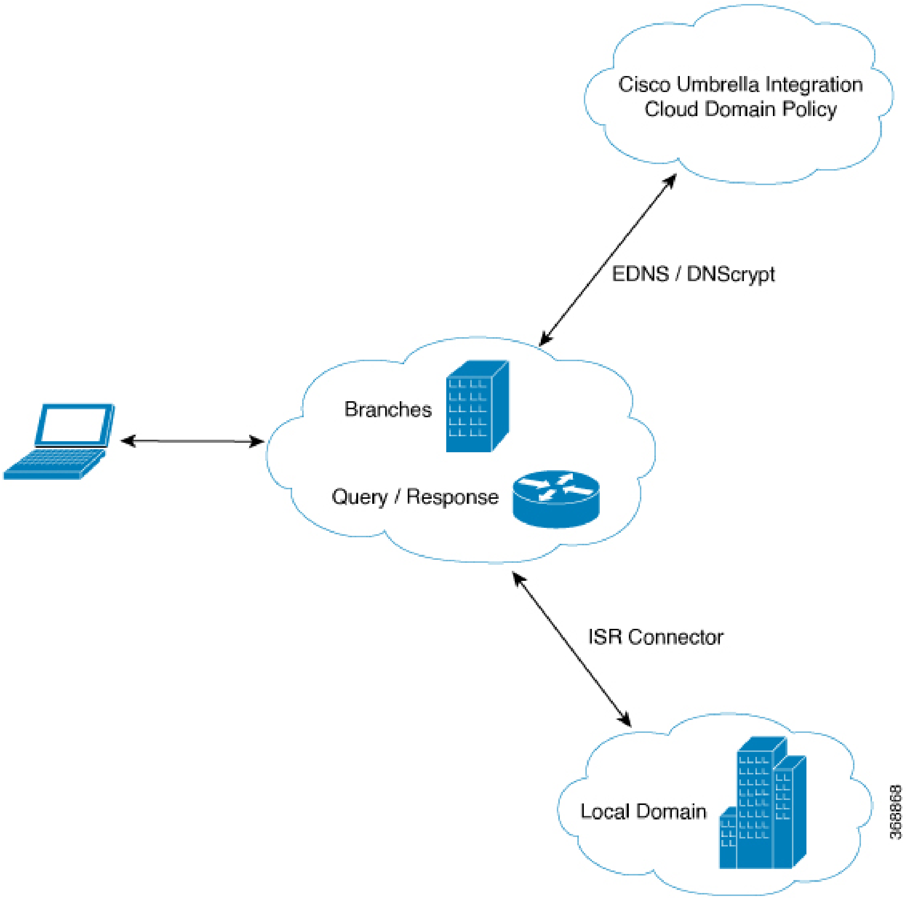
Encrypting the DNS Packet

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 8: 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.
- Umbrella redirection does not work with DNS sent over TCP. Only UDP is supported.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.
- The Cisco Umbrella configuration may enforce IP address restrictions for the Service VPN configurations. If you do not follow the guidelines, configuration may result in traffic loss. For additional information about Cisco Umbrella configuration, see Cisco Umbrella SIG User Guide.

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.
- Cisco Catalyst 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 SD-WAN Manager 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 35: Feature History

Feature Name	Release Information	Description
Auto-registration for Cisco Umbrella Cloud Services	Cisco IOS XE Catalyst SD-WAN 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 SD-WAN Manager 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 SD-WAN Manager uses the Smart Account credentials to connect to the Umbrella portal. The Smart Account credentials are configured in Cisco SD-WAN Manager 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.

Create Cisco Umbrella Scope Credentials

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Cloud Credentials** and select **Umbrella** as the provider.

3. Enter the following information, which is applicable to both Cisco Umbrella SIG and Cisco Umbrella DNS security:

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Scope Credentials	
API Key	Enter the Umbrella management API key.
Secret	Enter the Umbrella management API secret.

4. Click **Save**.

Define Domain Lists

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager

1. From the Cisco SD-WAN Manager 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.
   - **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 the next step.

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.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

Table 36: DNS Security Policy

Field	Description
Add DNS Security Policy	From the **Add DNS Security Policy** drop-down list, select **Create New** to create a new DNS Security Policy policy. **Copy from Existing**: Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
Create New	Displays the DNS Security Policy wizard.
Policy Name	Enter a name for the policy.
Umbrella Registration Status	Displays the status of the API Token configuration.
Manage Umbrella Registration	Click **Manage Umbrella Registration** to add a token, if you have not added one already.
Match All VPN	Click **Match All VPN** to keep the same configuration for all the available VPNs.

Field	Description
Custom VPN Configuration	choose **Custom VPN Configuration** to input the specific VPNs.
Local Domain Bypass List	Choose the domain bypass.
DNS Server IP	Configure **DNS Server IP** from the following options: • **Umbrella Default** • **Custom DNS**
DNSCrypt	Enable or disable the DNSCrypt.
Next	Click **Next** to the policy summary page.

Attach DNS Umbrella Policy to Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and choose **From Feature Template** from the Create Template drop-down menu.

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

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.

Upload Umbrella Root Certificates

Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1.

If edge devices in your Cisco Catalyst SD-WAN network require new Umbrella root certificates for Umbrella DNS security, you can upload an Umbrella root certificate bundle. The bundle contains a certificate for Cisco vEdge devices and a certificate for Cisco IOS XE Catalyst SD-WAN devices, in that order. After you upload the bundle, Cisco SD-WAN Manager pushes the appropriate certificates to the appropriate devices.

1. In the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** in the **Umbrella DNS Certificate** row.
3. Perform one of the following actions to enter the Umbrella root certificate bundle in the **Umbrella Root Certificate** field:

- Copy and paste the contents of the bundle. Ensure that the certificate for Cisco vEdge devices appears before the certificate for Cisco IOS XE Catalyst SD-WAN devices.
- Click **Select a File** and navigate to and select the bundle that you want.

4. Click **Save**.

Cisco SD-WAN Manager pushes the certificates to all devices that support an Umbrella root certificate.

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 Cisco Catalyst 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
```

For more information, see Regular Expression for URL Filtering and DNS Security, on page 471.

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 dnscrypt** command and to re-enable DNSCrypt, use the **dnscrypt** 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 dnscrypt notifications:

```
Device# show sdwan umbrella dnscrypt
    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:BBD0:A8BE:0263:F07B:72CB:BB21:330B:D47C:7373:B8C8:5F96:9F07:FEC6:BBFE:95D0

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

          NM key Hash          : 88FC:7825:5B58:B767:32B5:B36F:A454:775C:711E:B58D:EE6C:1E5A:3BCA:F371:4285:5E3A
When disabled:
Device# show umbrella dnscrypt
       DNSCrypt: Not enabled
       Public-key: NONE
```

```
Sample configuration steps for dns-resolver and match-local-domain-to-bypass per vrf:
Router(config)# vrf definition 1
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# ?
Possible completions:
    dnscrypt
    local-domain
    public-key
    registration-vrf
    resolver
    token
    udp-timeout
    vrf
Router(config-profile)# vrf ?
This line doesn't have a valid range expression
Possible completions:
    <name:string, min: 1 chars, max: 32 chars>  1
Router(config-profile)# vrf 1
Router(config-profile-vrf)# ?
Possible completions:
    dns-resolver
    match-local-domain-to-bypass
Router(config-profile-vrf)# dns-resolver umbrella
Router(config-profile-vrf)# match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router(config)# vrf definition 2
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commitCommit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# vrf 2
Router(config-profile-vrf)# dns-resolver 8.8.8.8
Router(config-profile-vrf)# no match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router#sh umbrella config

Umbrella Configuration
========================
Token: AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
OrganizationID: 1882034
Local Domain Regex parameter-map name: NONE
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        : De
    vice Id recieved successfully
    WAN interface      : None
```

Configure Cisco Umbrella Using a CLI Device Template

For more information on using the CLI device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices.

This section provides example CLI configurations for Cisco Umbrella.

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

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

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


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

interface Loopback<some value>
no shutdown
```

```
  vrf forwarding <vrf#>
ip address <IP Address> <mask>
exit

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

crypto ikev2 policy policy1-global
  proposal p1-global

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

crypto ikev2 profile if-ipsec2-ikev2-profile
  no config-exchange request
 dpd 10 3 on-demand
  dynamic
  lifetime 86400

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

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

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

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

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

Umbrella show commands at FP Layer

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

```
Device# show platform software umbrella f0 config
+++ Umbrella Config +++
Umbrella feature:
------------------
Init: Enabled
Dnscrypt: Enabled
Timeout:
------------------
udp timeout: 5
OrgId :
------------------
orgid : 1892929
Resolver config:
RESOLVER IP's
---------------------
208.67.220.220
208.67.222.222
2620:119:35::35
2620:119:53::53
Dnscrypt Info:
public_key:
A5:BA:18:C5:59:70:67:94:E5:37:38:33:06:F9:63:83:39:86:82:E4:00:F5:D8:BE:C1:AA:77:4A:4C:BA:64:00
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461
ProfileID    DeviceID          Mode      Resolver     Local-Domain    Tag
------------------------------------------------------------------------------
     0                         OUT                    False
     4                         IN        8.8.8.8      True           vpn9
     1                         IN        8.8.8.8      False          vpn19
     2     010a9b2b0d5cb21f    IN     208.67.220.220  True           vpn29
     3     010a1a2e1989da19    IN     208.67.220.220  False          vpn39

The show platform software umbrella f0 local-domain displays the local domain list.
Device# show platform software umbrella f0 local-domain
01.  www.cisco.com
02.  .*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 39FF000000000000000"
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 SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose the **Monitor** > **Network**.

2. 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.

3. 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 37: Feature History

Feature	Release Information	Description
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	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. 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.
Support for Zscaler Automatic IPSec Tunnel Provisioning	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature automates the provisioning of tunnels from Cisco Catalyst 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.

Feature	Release Information	Description
SIG Integration Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	

Feature	Release Information	Description
		Source-Only Load Sharing: When you configure two or more active tunnels to a Secure Internet Gateway (SIG), different traffic flows from the same source IP address, with different destination public IP addresses, may be mapped to use different tunnels. With this feature, you can configure all traffic flows from a particular source IP address, irrespective of the destination IP address, to be routed to the SIG through only one of the active tunnels. **IPSec Tunnel Creation Improvements in an Active-Active Setup**: This feature ensures that when you provision an IPSec tunnel, the control and data traffic are sent through the same the physical interface toward the SIG endpoint. Pinning the control and data packets to the same physical interface removes a limitation that exists in previous releases. In previous releases, in certain situations, the control and data packets may be routed to the SIG endpoint through different physical interfaces. When the packets are routed in this way, one of the following scenarios occurs: • If the source is a physical interface, tunnel creation fails because the source IP address of the negotiation packets differs from the source IP address of the keepalive control packet. • If the source is a loopback interface, the source IP address of the data packets differs from the source IP address of the IPSec SA negotiated through the control packets. This difference causes the SIG endpoint to

Feature	Release Information	Description
		drop the data packets.
Layer 7 Health Check for Manual Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down.
Automatic GRE Tunnels to Zscaler	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, use the Secure Internet Gateway (SIG) feature template to provision automatic GRE tunnels to Zscaler SIGs. In earlier releases, the SIG template only supported the provisioning of automatic IPSec tunnels to Zscaler SIGs.
Global SIG Credentials Template	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, create a single global Cisco SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a Cisco SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global Cisco SIG Credentials template to the device template.
Monitor Automatic SIG Tunnel Status and Events	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	Monitor security events related to automatic SIG tunnels using the **Security Events** pane on the **Monitor** > **Security** page, and the **Events** dashboard on the **Monitor** > **Logs** page. Monitor automatic SIG tunnel status using the **SIG Tunnel Status** pane on the **Monitor** > **Security** page, and the **SIG Tunnels** dashboard on the **Monitor** > **Tunnels** page.

Feature	Release Information	Description
Configure SIG Tunnels in a Security Feature Profile	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	With this feature, create a Security feature profile and associate it with one or more configuration groups. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels. After configuring the feature, deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints.
Cisco Umbrella Multi-Org Support	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature supports management of multiple organizations through a single parent organization. With this feature, Cisco Catalyst SD-WAN Umbrella for SIG support security policy requirements for different regions of the SD-WAN network.
SLA Profile Support for Layer 7 Health Check	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This feature uses jitter and packet loss, in addition to latency in SLA metrics to determine the health of the tunnel.
Share Traffic Information with Cisco Security Service Edge	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Cisco SD-WAN Manager can share VPN and security group tag (SGT) information with Cisco Security Service Edge (SSE). This is called context information. SSE can apply different policies to traffic based on the context information of the traffic.

Cisco Catalyst SD-WAN edge devices support SD-WAN, routing, security, and other LAN access features that can be managed centrally. On high-end devices, you can enable all these features while providing the scale and performance required by large enterprises. However, on lower-end devices, enabling all the security features simultaneously can degrade performance. To avoid the performance degradation, integrate lower-end devices with Secure Internet Gateways (SIG) that do most of the processing to secure enterprise traffic. When you integrate a Cisco Catalyst SD-WAN edge device with a SIG, all client internet traffic, based on routing or policy, is forwarded to the SIG. In addition, the SIG can also protect roaming users, mobile users, and BYOD users. The Multi-security association (SA) Virtual Tunnel Interface (VTI) is not supported on Cisco Catalyst SD-WAN devices.

Options to Integrate Your Devices with Secure Internet Gateways

To integrate Cisco Catalyst SD-WAN edge devices with a SIG, you can use:

- Automatic tunnels
- Manual tunnels

Automatic Tunnels

Using the Cisco Secure Internet Gateway (SIG) feature template, you can provision automatic IPSec tunnels to Cisco Umbrella SIGs, or automatic IPSec or GRE tunnels to Zscaler SIGs.

Provision an automatic tunnel as follows:

1. Complete the following prerequisites for the SIG:
   a. Specify the address of one or more DNS servers.
   b. Enable the DNS lookup feature by using the **ip domain lookup** command on the Cisco IOS XE Catalyst SD-WAN device. For more information, see ip domain lookup.
   c. Ping the configured DNS name server. The DNS must be reachable using the VRF 65528.
   d. Automatic SIG tunnels use the first NAT outside WAN interface to connect to Umbrella or Zscaler. The DNS and the internet must be accessible through the same interface.
2. Specify Cisco Umbrella or Zscaler credentials using the Cisco SIG Credentials feature template.
3. Specify the details for the tunnel to the SIGs 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.
4. Edit the Cisco VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the Cisco VPN feature template.
5. Add feature templates to the device templates of the devices that should route traffic to the SIG.
6. Attach the device templates to the devices.

When you attach the device template, the device sets up tunnels to the SIGs and redirects traffic to it.

Note When a SIG Zscaler template is removed from a device template, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever the SIG template is removed from a device template.

Cisco Umbrella Integration

From Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Cisco vManage Release 20.2.1, 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 tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 238.

Cisco Umbrella Multi-Org Support

Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1

The Cisco Catalyst SD-WAN Umbrella for SIG support security policy requirements for different sub-regions of their SD-WAN network. This feature is supported for both DNS security policy and SIG templates.

Although Cisco Umbrella's individual dashboards can only support a single domain, the multi-org feature allows you to view and manage multiple domains or logically separate network segments from a particular dashboard. The multi-org setup is suitable for organizations that are highly distributed across different locations where networks are all connected, but where different regions require different security policies. The multi-org feature is also helpful for networks with more than one Active Directory (AD) domain, whether within an AD or logically separate domains.

Zscaler Integration

You can integrate Cisco Catalyst SD-WAN edge devices to Zscaler SIGs by provisioning automatic IPsec or GRE tunnels between the edge devices and the SIGs.

Automatic IPSec Tunnels: From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, you can provision automatic IPSec tunnels 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 Catalyst SD-WAN devices. The devices use Zscaler APIs to create IPSec 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.

Automatic GRE Tunnels: From Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, you can provision automatic GRE tunnels to Zscaler Internet Access (ZIA) Public Service Edges using the Cisco Security Internet Gateway (SIG) feature template. The devices use Zscaler APIs to create the GRE tunnels.

For information on configuring automatic tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 238.

Manual Tunnels

You can create a GRE or IPSec tunnel to a third-party SIG or a GRE tunnel to a Zscaler SIG by defining the tunnel properties in the Cisco Secure Internet Gateway (SIG) feature template.

Provision manual tunnels as follows:

1. 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.

2. Edit the Cisco VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the Cisco VPN feature template.

3. Add feature templates to the device templates of the devices that should route traffic to the SIG.

4. Attach the device templates to the devices.

When you attach the device template, the device sets up the defined IPSec or GRE tunnels to the SIG and redirects traffic to it.

Note When a SIG Zscaler template is removed from a device template, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever the SIG template is removed from a device template.

High Availability and Load Balancing

When you connect a Cisco Catalyst SD-WAN edge device to Cisco Umbrella, Zscaler, or a third-party SIG, you can connect the device to a primary data center and a secondary data center. Also, you can provision more than one tunnel to each data center.

Active Tunnels: You can provision up to four IPSec tunnels to the primary data center. These tunnels serve as active tunnels, and when two or more active tunnels are provisioned, the traffic toward the SIG is distributed among these tunnels, increasing the available bandwidth toward the SIG. From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, you can distribute the traffic equally among the active tunnels to achieve an equal-cost multi-path (ECMP) distribution, or assign different weights to the active tunnels so that some tunnels carry more traffic toward the SIG than the others.

Back-up Tunnels: You can provision up to four IPSec tunnels to the secondary data center, one for each active tunnel that you have provisioned to the primary data center. These tunnels to the secondary data center serve as back-up tunnels. When an active tunnel fails, the traffic toward the SIG is sent through the corresponding back-up tunnel. When you provision two or more back-up tunnels, the traffic toward the SIG is distributed among these tunnels, increasing the available bandwidth toward the SIG. From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, you can distribute the traffic equally among the back-up tunnels to achieve an ECMP distribution, or assign different weights to the back-up tunnels so that some tunnels carry more traffic toward the SIG than the others.

By provisioning two or more active tunnels and distributing the traffic among them, while not provisioning any back-up tunnels, you can create an active-active setup. By provisioning a back-up tunnel for each active tunnel, you can create an active-back-up setup.

Load Sharing Among Tunnels

When you connect a Cisco Catalyst SD-WAN edge device to a SIG and redirect internet-bound traffic to the SIG, any traffic from the branch that is destined for a public IP address passes through the SIG. If you have provisioned more than one tunnel to carry traffic to the SIG, Cisco Express Forwarding (CEF) may map different traffic flows from the same source IP address, and with different public IP address destinations, to different SIG tunnels.

Source-Only Load Sharing: From Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1, you can configure the traffic from a particular source IP address to be sent to the SIG over only one of the tunnels, irrespective of the destination public IP address. Cisco Express Forwarding (CEF) maps each source IP address to one of the tunnels, distributing traffic from different source IP addresses among the tunnels. For more information, see Configure Source-Only Load Sharing, on page 266.

Note This configuration does not create a sticky mapping between source IP addresses and tunnels to the SIG. If one or more of the tunnels are down, CEF maps source IP addresses to the remaining tunnels. During this mapping, traffic from a particular source IP address may be sent to the SIG over a tunnel that is different from the tunnel that was previously assigned.

Support for Layer 7 Health Check

You can monitor the health of tunnels towards the SIG using trackers attached to the tunnels. These trackers are used to automatically fail over to backup tunnels based on the health of the tunnel.

While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker with default values for failover parameters. However, you can also create customized trackers with failover parameter values that suit your SLA requirements.

In the case of manually created tunnels, create and attach the tracker.

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the tracker also uses jitter and packet loss in the calculation of tunnel health.

The following table summarizes tracker support for automatic and manual tunnels:

Tunnel Type	Default Tracker	Customized Tracker
Automatic IPSec Tunnels	Yes	Yes Minimum releases: Cisco IOS XE Release 17.6.2 and Cisco vManage Release 20.6.2
Automatic GRE Tunnels	Yes	Yes Minimum releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1

Tunnel Type	Default Tracker	Customized Tracker
Manual	No	Yes Minimum releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

The tunnel health is monitored as follows:

1. Based on the configuration in the System feature template, Cisco SD-WAN Manager creates a tracker according to the default or customized failover parameters that you define in the SIG template. This tracker uses VPN 65530. Cisco SD-WAN Manager reserves VPN 65530 for tracker VPNs.

2. The tracker resolves the IP address of the SIG service using VPN 0.

   For automatic tunnels to Cisco Umbrella or Zscaler, the tracker uses the following URLs to connect to the SIG:

   - Cisco Umbrella: http://service.sig.umbrella.com
   - Zscaler: http://gateway.*zscaler-cloud-url*/vpntest

3. The device sets up tunnels to the SIG.

4. For each tunnel, the device creates a named TCP socket that it uses to identify the tunnels.

5. The tracker monitors the health of the tunnel using HTTP probes. The tracker calculates the round-trip time (RTT) and compares it to the configured SLA parameters.

   From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the tracker also uses jitter and packet loss in the calculation of tunnel health.

6. For any tunnels that fail to receive a response within the interval and retransmit timers, or for any tunnels that exceed the latency threshold, the tunnel tracker status is marked down and the VPN routes pointing to this tunnel is marked standby. Crypto IKE stays up for the tunnel but the routes are withdrawn.

7. The device updates the routes for any service VPNs that are connected to the tunnel.

Related Topics

Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 242
Create Manual Tunnels Using Cisco SIG Feature Template, on page 257

Global SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

In Cisco vManage Release 20.8.x and earlier releases, you must create a Cisco SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) for each Cisco IOS XE Catalyst SD-WAN device model that you wish to connect to the SIG.

From Cisco vManage Release 20.9.1, create a single global Cisco SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) and attach the template to the required Cisco IOS XE Catalyst SD-WAN device s, irrespective of the device model. When you attach a Cisco SIG feature template that configures automatic SIG tunnels to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.

The Cisco IOS XE Catalyst SD-WAN devices of your organization connect to Cisco Umbrella or Zscaler using a common organization account with the SIG provider. As such, it is beneficial to configure the organization account credentials on the devices through a global template. When you modify the Cisco Umbrella or Zscaler credentials, update only one global template for the modified credentials to take effect on the attached Cisco IOS XE Catalyst SD-WAN devices.

Note After you upgrade Cisco SD-WAN Manager software from Cisco vManage Release 20.8.x or earlier to Cisco vManage Release 20.9.1 or later, the device-model-specific Cisco SIG Credentials templates created in Cisco vManage Release 20.8.x or earlier become read-only. The read-only status allows you to only view the configured credentials. To update the credentials configured in Cisco vManage Release 20.8.x or an earlier release, create a Cisco SIG Credentials template for the SIG provider.

If you try to create or modify a Cisco SIG feature template, Cisco SD-WAN Manager prompts you to create a global Cisco SIG Credentials template for the SIG provider.

Related Topics

Create Cisco Umbrella SIG Credentials Template, on page 238
Create Zscaler SIG Credentials Template, on page 240

Information About Cisco Umbrella Scope Credentials

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

You can generate new Cisco Umbrella credentials, also called as scope credentials, and use the same credentials for both Cisco Umbrella SIG and Cisco Umbrella DNS security configurations. The Cisco Umbrella scope credentials provide flexibility with the ability to customize API keys. You can create multiple API keys with tailored access control for each API key. For more information, see Cisco Umbrella SIG User Guide.

Use the **no use-v2-api** command to continue using legacy credentials while configuring Cisco Umbrella DNS Security.

Upgrade Scenarios

When you ...	And you ...	Then the result is ...
upgrade to Cisco Catalyst SD-WAN Manager Release 20.15.1	• upgrade edge devices to Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, and • configure Cisco Umbrella scope API keys	Cisco SD-WAN Manager automatically discovers and upgrades the Cisco Umbrella DNS and SIG configurations with the Cisco Umbrella scope API credentials.
upgrade to Cisco Catalyst SD-WAN Manager Release 20.15.1	have edge devices in the network running various releases of Cisco IOS XE	Cisco SD-WAN Manager uses both the Cisco Umbrella legacy and scope API credentials for Cisco Umbrella DNS and SIG configurations.

Restrictions for Devices With Secure Internet Gateways

- For Zscaler, GRE tunnel over TLOC extension is not supported.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Configure Tunnels

Configure Automatic Tunnels Using Cisco SD-WAN Manager

Prerequisites

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

- Cisco Umbrella: To configure automatic tunnels to Cisco Umbrella, you can do one of the following
  - For Cisco SD-WAN Manager to fetch the API keys, specify Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**. Your Cisco Smart Account is the account that you use to log in to the Cisco Smart Software Manager (CSSM) portal.
  - To manually specify the API keys, generate Umbrella Management API keys. See *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

    Specify the generated keys in the Cisco SIG Credentials template.
- Zscaler Internet Access (ZIA): To configure automatic tunnels to Zscaler, do the following:
  1. Create partner API keys on the ZIA Partner Integrations page.
  2. Add the Partner Administrator role to the partner API keys.
  3. Create a Partner Administrator.
  4. Activate the changes.

  For more information, see *Managing SD-WAN Partner Keys* on the Zscaler Help Center.

  Specify the generated keys in the Cisco SIG Credentials template.

Create Cisco Umbrella SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 242, on selecting Umbrella as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Cisco Umbrella SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 38: Cisco SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Umbrella Global Credentials
Description	(Read only) Global credentials for Umbrella

Configure Cisco Umbrella Credentials

1. In the **Basic Details** section, do one of the following:

   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:

     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

        Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

     b. Click **Get Keys**.

   - Enter Cisco Umbrella credentials:

Field	Description
SIG Provider	(Read only) Umbrella
Organization ID	Enter the Cisco Umbrella parent organization ID for your organization. For more information, see *Find Your Organization ID* in the Cisco Umbrella SIG User Guide.
Registration Key	Enter the Umbrella Management API Key. It is part of DNS security policy under unified security policy. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the Cloud Security API documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret.

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

Create Cisco Umbrella Scope Credentials

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

2. Click **Cloud Credentials** and select **Umbrella** as the provider.

3. Enter the following information, which is applicable to both Cisco Umbrella SIG and Cisco Umbrella DNS security:

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Scope Credentials	
API Key	Enter the Umbrella management API key.
Secret	Enter the Umbrella management API secret.

4. Click **Save**.

Create Zscaler SIG Credentials Template

Minimum release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 242, on selecting Zscaler as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Zscaler SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 39: Cisco SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Zscaler-Global-Credentials
Description	(Read only) Global credentials for Zscaler

1. In the **Basic Details** section, enter the Zscaler credentials:

Table 40: Zscaler Credentials

Field	Description
SIG Provider	(Read only) Zscaler
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help > Getting Started > Admin Portal > About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Username	Username of the SD-WAN partner account.

Field	Description
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help > Partner Integrations > Managing SD-WAN Partner Keys*.

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

Create Cisco SIG Credentials Template

Applicable releases: Cisco vManage Release 20.8.x and earlier releases.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **Other Templates**, click **Cisco SIG Credentials**.
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.
8. In **Basic Details** section, do the following:
   a. **SIG Provider**: Click **Umbrella** or **Zscaler**.
   b. For Cisco Umbrella, enter the following registration parameters or click **Get Keys** to have Cisco SD-WAN Manager fetch these parameters from the Cisco Umbrella portal.
      - **Organization ID**
      - **Child Org**
      - **Child Org List**
      - **Registration Key**
      - **Secret**

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

To fetch the parameters, Cisco SD-WAN Manager uses your Smart Account credentials to connect to the Cisco Umbrella portal. To manually enter the parameters, generate the values in your Umbrella account as described here.

c. For Zscaler, enter the following details:

Field	Description
Organization	The name of the organization in Zscaler cloud. To find this information in Zscaler, see **Administration** > **Company Profile**.
Child Org	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Enter the child organization information in the SIG template.
Child Org List	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Select the child org from the **Child Org List** drop-down list.
Partner base URI	This is the Zscaler Cloud API that Cisco SD-WAN Manager uses to connect to Zscaler. To find this information in Zscaler, see **Administration** > **API Key Management**.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	The partner API key. To find the key in Zscaler, see **Zscaler Cloud Administration** > **Partner Integrations** > **SD-WAN**.

9. Click **Save**.

Create Automatic Tunnels Using a Cisco SIG Feature Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **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 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the feature template.

8. (From Cisco vManage Release 20.9.1) **SIG Provider**: Click **Umbrella** or **Zscaler**.

   From Cisco vManage Release 20.9.1, on selecting **Umbrella** or **Zscaler** as the SIG provider, Cisco SD-WAN Manager prompts you to create the corresponding global SIG credentials template if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Cisco Umbrella or Zscaler SIG credentials template.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

9. To create one or more trackers to monitor tunnel health, do the following in the **Tracker** section:

Note From Cisco IOS XE Release 17.6.2 and Cisco vManage Relase 20.6.2 , you can create customized trackers to monitor the health of automatic tunnels. If you do not customize the SLA parameters, Cisco SD-WAN Manager creates a default tracker for the tunnel.

   a. **Source IP Address**: Enter a source IP address for the probe packets.

   b. Click **New Tracker**.

   c. Configure the following:

Table 41: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds.
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds

Field	Description
Multiplier	Enter the number of times the probes are resent before determining that a tunnel is down. **Note** When tunnel status changes continuously within a short period of time, the tunnel goes to the flapping state. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, to avoid flapping of tunnels, the tracker waits for the duration equal to the product of multiplier * interval to declare the status of the tunnel. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** The URL value passed to the endpoint-api-url configuration must resolve through DNS to an IPv4 address. Domains which resolve to an IPv6 address are currently not supported for the endpoint-api-url configuration.

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

10. To create tunnels, do the following in the **Configuration** section:

    a. (Cisco 20.8.x and earlier releases) **SIG Provider**: Click **Umbrella** or **Zscaler**.

    b. Click **Add Tunnel**.

    c. Under **Basic Settings**, configure the following:

Table 42: Basic Settings

Field	Description
Tunnel Type	Click **ipsec** or **gre**. **Note** Automatic GRE tunnels are supported from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 and only to Zscaler ZIA.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec template.
Description	Enter a description for the interface.

Field	Description
Tracker	By default, a tracker is attached to monitor the health of automatic tunnels to Cisco Umbrella or Zscaler. If you configured a customized tracker in step **8**, choose the tracker. **Note** From Cisco IOS XE Release 17.6.2 and Cisco vManage Relase 20.6.2, you can create customized trackers to monitor the health of automatic tunnels.

Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
	For releases before Cisco IOS XE Catalyst SD-WAN Release 17.13.1aCisco Catalyst SD-WAN Manager Release 20.13.1 and, and you have a Cellular or Dialer interface as the tunnel's source interface, the following workaround must be implemented.
	If you use a cellular interface as a tunnel source interface, you must modify your existing tunnel source interface configuration with the following configuration:
	`interface <interface name>`
	`no tunnel route-via <Interface> mandatory`
	Use the CLI add-on feature template to modify the tunnel configuration on the device. For more information on how to use a CLI add-on feature template, see , Create a CLI Add-On Feature Template.
	After you have modified the tunnel configuration, select the device template for which you want to apply the CLI add-on feature template, and push the configuration to the devices. For more information about attaching a device template to one or more devices, see Attach Template to Devices
	Note A SIG tunnel will be created for cellular interfaces only if a global VRF has only one transport interface. A SIG tunnel is not be created if a global VRF has multiple transport interfaces.

Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.

Field	Description
Source Public IP	Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. **Default**: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.

d. (Optional) Under **Advanced Options**, configure the following:

Table 43: General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10

Field	Description
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 44: IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 45: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM
Perfect Forward Secrecy	• Specify the PFS settings to use on the IPsec tunnel. • Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: None

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

11. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 46: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. 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 is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

12. (Optional) Modify the default configuration in the **Advanced Settings** section:

Table 47: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 48: Zscaler

Field	Description
Primary Data-Center	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels (Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1): Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Secondary Data-Center	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels (Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1): Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.

Field	Description
Zscaler Location Name	Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 (Optional) Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Refresh Time Unit	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: 0
Enable AUP	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Off
First Time AUP Block Internet Access	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Off
Force SSL Inspection	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Off
AUP Frequency	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: 0

13. Click **Save**.

Create Automatic Tunnels to Cisco Umbrella or Zscaler Using Policy Groups

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

You can create automatic tunnels to Cisco Umbrella or Zscaler using **Configuration** > **Policy Groups** > **Secure Internet Gateway**. For more information see, Configure a Secure Internet Gateway.

Configure Automatic Tunnels Using a CLI Add-On Template

We recommend the use of feature templates to configure automatic tunnels.

Configure a Tracker Using a CLI Add-On Template

For more information about using CLI add-on templates, see CLI Add-On Feature Templates.

Before You Begin

- A default tracker is available if the tunnel is created in Cisco Umbrella or Zscaler. You do not have to configure an endpoint tracker in this scenario.
- You can configure more than one endpoint tracker using the same CLI Add-On template.

Note By default, CLI templates execute commands in global config mode.

1. Configure the tracker name.

   endpoint-tracker *tracker name*

2. Configure the endpoint tracker using an API URL.

   endpoint-api-url *url-address*

3. Set an interval to determine the period between tracker probes.

   interval *interval-value*

4. Set a multiplier value.

   multiplier *multiplier-value*

5. Configure the tracker type.

   tracker-type interface

The following is a sample configuration example for configuring a tracker:

```
endpoint-tracker netflix

 endpoint-api-url http://www.netflix.com

 interval 20

 multiplier 1

 tracker-type interface

endpoint-tracker youtube

 endpoint-api-url http://www.youtube.com

 interval 20

 multiplier 1

 tracker-type interface
```

Configure a Tunnel Using CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

1. Enter the tunnel interface mode.

   interface Tunnel *interface-number*

2. Configure an IP unnumbered interface.

   ip unnumbered *source-interface-name*

3. Configure the endpoint tracker for tracking the status of an endpoint.

```
endpoint-tracker tracker-name
```

4. Configure the SLA profile for the tunnel interface.

   ```
   endpoint-tracker-sla-profile profile-name
   ```

5. Set the source address for the tunnel interface.

   ```
   tunnel source source-interface-name
   ```

6. Set the destination address for the tunnel interface.

   ```
   tunnel destination interface-ip-address
   ```

7. Specify the outgoing interface type for the tunnel transport.

   ```
   tunnel route-via interface-type mandatory
   ```

8. Enable path MTU discovery on the tunnel interface.

   ```
   tunnel path-mtu-discovery
   ```

9. Configure **tunnel vrf multiplexing**.

   This configuration allows multiple service VPNs to use the tunnel.

   ```
   tunnel vrf multiplexing
   ```

The following is a sample configuration example for configuring the tunnel:

```
interface Tunnel601

 ip unnumbered GigabitEthernet1

 endpoint-tracker youtube

 endpoint-tracker-sla-profile sla_mod

 tunnel source GigabitEthernet1

 tunnel destination 10.1.17.14

 tunnel route-via GigabitEthernet1 mandatory

 tunnel path-mtu-discovery

 tunnel vrf multiplexing
```

Configure an Endpoint Tracker SLA Profile for Layer 7 Health Check, Using a CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

1. Configure an SLA profile name.

   ```
   endpoint-tracker-sla-profile profile-name
   ```

2. Set the packet loss value as a percentage.

   The value can range from 0-100, with 10 being the default value.

   ```
   loss value
   ```

3. Set the latency value as milliseconds.

   The value can range from 1-10000, with 300 being the default value.

   latency *value*

4. Set the jitter value as milliseconds.

   The value can range from 1-10000, with 20 being the default value.

   jitter *value*

5. Set the SLA mode. You can choose one of the following modes:

   - Aggressive
   - Moderate
   - Conservative

   sla-mode *mode*

Note When SLA profile is configured in a manual tracker, the threshold from the endpoint tracker is used as the timeout value for HTTP probes.

The following is a sample configuration example for configuring an endpoint-tracker SLA profile with an aggressive sla-mode:

```
endpoint-tracker-sla-profile sla_agg

 loss 10

 latency 300

 jitter 80

 sla-mode aggressive
```

Configure a Service Route for SIG Using a CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

Configure a service route to the SIG Tunnel.

ip sdwan route vrf *vrf-range* **service sig**

The following is a sample configuration for configuring a service route for SIG:

```
ip sdwan route vrf 1 0.0.0.0/0 service sig
```

Configure High Availability Using a CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

1. Enter the HA pair mode.

   sdwan service sig vrf global
   ha-pairs

2. Define two tunnel interfaces for a high availability configuration.

   interface-pair *active-tunnel*[**active-interface-weight** *active-weight*] *backup-tunnel* [**backup-interface-weight** *backup-weight*]

3. Enter tunnel interface mode for the active tunnel.

   interface *active-tunnel*

4. Configure the tunnel options for the active tunnel.

   tunnel-options tunnel-set secure-internet-gateway-other source-interface *interface-name*

5. Enter tunnel interface mode for the backup tunnel.

   interface *backup-tunnel*

6. Exit tunnel interface mode.

   exit

7. Configure the tunnel options for the backup tunnel.

   tunnel-options tunnel-set secure-internet-gateway-other source-interface *interface-name*

8. Exit tunnel interface mode.

   exit

The following is a sample configuration for configuring high availability:

```
sdwan
 service sig vrf global
  ha-pairs
   interface-pair Tunnel601 active-interface-weight 1 Tunnel602 backup-interface-weight 1
 interface Tunnel601
  tunnel-options tunnel-set secure-internet-gateway-other source-interface GigabitEthernet1

 exit
 interface Tunnel602
  tunnel-options tunnel-set secure-internet-gateway-other source-interface GigabitEthernet2

 exit
```

Create Manual Tunnels Using Cisco SIG Feature Template

From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, all SIG related workflows for automatic and manual tunnels have been consolidated into the Cisco SIG template. If you are using Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, or later, use the Cisco SIG template to configure GRE or IPSec tunnels to a third-party SIG, or GRE tunnels to a Zscaler SIG.

For a software release earlier than Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, see *Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager*.

Layer 7 Health Check: The option to create trackers and monitor the health of manually created tunnels is available from Cisco IOS XE Release 17.8.1a, Cisco vManage Relase 20.8.1. In earlier releases, the Layer 7 Health Check feature is only available if you use VPN Interface GRE/IPSEC templates, and not with Cisco SIG templates.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **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 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (Optional) To create one or more trackers to monitor tunnel health, do the following in the Tracker section:

Note The option to create trackers and monitor tunnel health is available from Cisco IOS XE Release 17.8.1a, Cisco vManage Relase 20.8.1.

   a. **Source IP Address**: Enter a source IP address for the probe packets.

   b. Click **New Tracker**.

   c. Configure the following:

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.

Field	Description
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** Both HTTP and HTTPS API URLs are supported. SIG tunnel tracker configuration only supports HTTP even though the HTTPS option is available.

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To create tunnels, do the following in the **Configuration** section:

a. **SIG** Provider: Click **Generic**.

Cisco vManage Release 20.4.x and earlier: Click **Third Party**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Field	Description
Tunnel Type	Based on the type of tunnel you wish to create, click **ipsec** or **gre**.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template or the Cisco VPN Interface GRE feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec or GRE templates.
Description	(Optional) Enter a description for the interface.

Field	Description
Source Type	Click **INTERFACE**. Cisco IOS XE Catalyst SD-WAN devices, **INTERFACE** is the only supported **Source Type**.
Tracker	(Optional) Choose a tracker to monitor tunnel health. **Note** From Cisco IOS XE Release 17.8.1a and Cisco vManage Relase 20.8.1, you can create trackers to monitor tunnel health.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.

Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
	For releases before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, and you have a Cellular or Dialer interface as the tunnel's source interface, the following workaround must be implemented.
	If you use a cellular interface as a tunnel source interface, you must modify your existing tunnel source interface configuration with the following configuration:
	`interface <interface name>`
	`no tunnel route-via <Interface> mandatory`
	Use the CLI add-on feature template to modify the tunnel configuration on the device. For more information on how to use a CLI add-on feature template, see , Create a CLI Add-On Feature Template.
	After you have modified the tunnel configuration, select the device template for which you want to apply the CLI add-on feature template, and push the configuration to the devices. For more information about attaching a device template to one or more devices, see Attach Template to Devices
	Note A SIG tunnel will be created for cellular interfaces only if a global VRF has only one transport interface. A SIG tunnel is not be created if a global VRF has multiple transport interfaces.

Tunnel Destination IP Address/FQDN	Enter the IP address of the SIG provider endpoint.
Preshared Key	This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

d. (Optional) Under **Advanced Options**, configure the following:

Table 49: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Table 50: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 0 to 65535 seconds **Default**: 10

Field	Description
DPD Retries	Specify how many unacknowledged packets to send before declaring an IKE peer to be dead and then removing the tunnel to the peer. **Range**: 0 to 255 **Default**:3

Table 51: (Tunnel Type: ipsec) IKE

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. Choose one of the following: • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 16 4096-bit modulus
IKE ID for Local Endpoint	If the remote IKE peer requires a local end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's source IP address

Field	Description
IKE ID for Remote Endpoint	If the remote IKE peer requires a remote end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's destination IP address

Table 52: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: NULL SHA 512

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: Group-16 4096-bit modulus

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

10. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 53: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. 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 is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.

Field	Description
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

11. 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 264

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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device** .

3. Click **Create Template** and click **From Feature Template**.
4. From the **Device Model** drop-down list, choose the device model for which you are creating the template.

   Cisco SD-WAN Manager 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.

5. From the **Device Role** drop-down list, choose **SDWAN Edge**.
6. 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.

7. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.

8. Click **Transport & Management VPN**.
9. In the **Transport & Management VPN** section, under **Additional Cisco VPN 0 Templates**, click **Cisco Secure Internet Gateway**.
10. From the **Cisco Secure Internet Gateway** drop-down list, choose the Cisco SIG feature template that you created earlier.
11. Click **Additional Templates**.
12. In the **Additional Templates** section,

    a. Automatic tunneling:

       (Cisco vManage Release 20.8.x and earlier) From the **Cisco SIG Credentials** drop-down list, choose the relevant Cisco SIG Credentials feature template.

       (From Cisco vManage Release 20.9.1) Cisco SD-WAN Manager automatically chooses the applicable global Cisco SIG Credentials feature template based on the Cisco SIG feature template configuration.

Note If there are any changes to the SIG credentials, for these changes to take effect, you must first remove the SIG feature template from the device template and push the device template. Thereafter, re-attach the SIG feature template and then push the template to the device. For information on pushing the device template, see Attach the SIG Template to Devices.

    b. Manual tunneling: No need to attach a **Cisco SIG Credentials** template.

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 Template to Devices

To attach one or more devices to the device template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and choose the template that you created.

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

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 Source-Only Load Sharing

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1.

Create CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the devices for which you are creating the template.

5. Under **Select Template**, scroll down to the **OTHER TEMPLATES** section.
6. Click **CLI Add-On Template**.
7. **Template Name**: 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.
8. **Description**: Enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
9. Under **CLI CONFIGURATION**, enter the following command: **ip cef load-sharing algorithm src-only**
10. Click **Save**.

Add CLI Add-On Template to Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.
3. Find the device template to which you wish to add the CLI add-on feature template.
4. For the device template, click **...** and click **Edit**.
5. Scroll down to **Additional Templates**.
6. From the **CLI Add-On Template** drop-down list, choose the CLI add-on feature template that you created earlier.
7. Click **Update**.

Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager

Table 54: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco IOS XE Catalyst SD-WAN 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.

Note 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 using Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, or later, configure GRE or IPSec tunnels to a generic SIG, or GRE tunnels to a Zscaler SIG, using the SIG template.

Configure a GRE Tunnel from Cisco SD-WAN Manager

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

Note To configure a GRE tunnel from Cisco SD-WAN Manager, use the SIG Feature Template. For more information, see Create Manual Tunnels Using Cisco SIG Feature Template. The Cisco VPN Interface GRE template is no longer used to configure a tunnel to a SIG.

For releases prior to Cisco vManage Release 20.8.1, use the Cisco VPN Interface GRE template.

1. Perform these actions to create a GRE template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and then click **Add Template**.

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

   c. Choose the type of device for which you are creating the template.
   d. Choose the Cisco VPN Interface GRE template from the group of VPN templates.
   e. In **Basic Configuration**, configure parameters as desired and then click **Save**.

2. Perform these actions to create a GRE route:
   a. Click **Feature Templates**, and then click **Add Template**.

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

   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 **GRE Route**.
   e. Click **New GRE Route**.
   f. Configure parameters as desired, and then click **Add**.

3. Perform these actions to configure a device template for the GRE interface.
   a. Click **Device**, and then click **...**and click **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 GRE template.
   d. From the Cisco VPN Interface GRE drop-down menu, click **Create Template**.

e. Configure the templates as desired, and then click **Save**.

Configure an IPsec Tunnel from Cisco SD-WAN Manager

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

Note To configure a IPSec tunnel from Cisco SD-WAN Manager, use the SIG Feature Template. For more information, see Create Automatic Tunnels Using Cisco SIG Feature Template. The Cisco VPN Interface IPSec template is no longer used to configure a tunnel to a SIG.

For releases prior to Cisco vManage Release 20.8.1, use the Cisco VPN Interface IPsec template.

1. Perform these actions to create an IPsec template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and click **Add Template**.

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

   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 Templates**, and, click **Add Template**.

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

   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**.

Configure SIG Tunnels in a Security Feature Profile

From Cisco vManage Release 20.10.1 and Cisco IOS XE SD-WAN Release 17.10.1, configure SIG tunnels in a configuration group and deploy the configuration to redirect traffic to SIG endpoints.

To configure SIG tunnels and redirect traffic to SIG endpoints, do the following:

1. For automatic tunnels, configure SIG provider credentials.
2. Create a Security feature profile or choose an exiting Security feature profile and associate it with the configuration group.
3. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels.

   For automatic tunnels, if you've not configured the SIG provider credentials, you are prompted to do so when you configure the Secure Internet Gateway feature.
4. For desired service VPNs, redirect traffic to SIG using data policies or by adding service routes in the service VPN feature configuration.
5. Deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints and redirect traffic to the SIG.

Configure SIG Credentials

Before you create automatic SIG tunnels, configure Cisco Umbrella or Zscaler credentials to enable Cisco SD-WAN Manager to create the tunnels to Cisco Umbrella or Zscaler endpoints. If you do not configure the SIG credentials on the **Administration** > **Settings** page before you configure the Secure Internet Gateway feature in the Security feature profile, Cisco SD-WAN Manager prompts you to enter the credentials when you configure the the Secure Internet Gateway feature. After you have configured the SIG credentials, you can modify the credentials on the **Administration** > **Settings** page.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **Secure Internet Gateyway (SIG) Credentials** setting, click **Edit**.
3. Choose **Umbrella** or **Zscaler**.
4. For **Umbrella**, do one of the following:
   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:

     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

b. Click **Get Keys**.

Cisco SD-WAN Manager obtains the following details:

- Organization ID
- Registration Key
- Secret

- Enter Cisco Umbrella credentials:

Table 55: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

5. For **Zscaler**, configure the following:

Table 56: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help > Getting Started > Admin Portal > About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.

Field	Description
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

6. Click **Save**.

Associate Security Feature Profile with a Configuration Group

Before you begin: Create a configuration group if you haven't already done so. For more information on creating a configuration group, see Run the Create Configuration Group Workflow.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. In the **Feature Profiles - Unconfigured** area, find the **Security Profile** and click **Start Configuration**.
4. In the **Add Profile** slide-in pane, do one of the following:
   - Create a new Security feature profile:
     a. Click **Create new**.
     b. Enter a unique **Name** and an optional **Description** for the profile.
     c. Click **Save**.
   - Choose an existing Security feature profile:
     a. Click **Choose existing**.
     b. Select an existing Security feature profile. Click the radio button adjacent to the profile name.
     c. Click **Save**.

   The Security feature profile is listed under **Associated Profiles**.

Configure Secure Internet Gateway Feature

Before you begin: Create or edit a configuration group and associate the Security feature profile with it.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. Under **Associated Profiles**, find the Security feature profile and expand the profile.
4. Click **Add Feature**.
5. In the **Add Feature** slide-in pane, from the drop-down list, choose the **Secure Internet Gateway** feature.
6. Configure the following details:

Table 57: Name, Description, and SIG Provider

Field	Description
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	(Optional) Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
SIG Provider	Click one of the following: • **Umbrella**: Configure automatic tunnel to Cisco Umbrella SIG. If you've not configured Umbrella credentials, Cisco SD-WAN Manager prompts you to configure the credentials: **Click here to add Umbrella credentials**. Click, and in the **Add Umbrella Credentials** dialog box, enter the details mentioned in Table 58: Cisco Umbrella Credentials, on page 273 and click **Add**. • **Zscaler**: Configure automatic tunnel to Zscaler SIG. If you've not configured Zscaler credentials, Cisco SD-WAN Manager prompts you to configure the credentials: **Click here to add Zscaler credentials**. Click, and in the **Add Zscaler Credentials** dialog box, enter the details mentioned in Table 59: Zscaler Credentials, on page 274 click **Add**. • **Generic**: Configure manual tunnel to a SIG endpoint.

Table 58: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

Table 59: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help > Getting Started > Admin Portal > About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help > Partner Integrations > Managing SD-WAN Partner Keys*.

7. To create tunnels, click **Configuration** and do the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. Enter the value when you add a device to the configuration group. To change the default key, type a new string and move the cursor out of the **Enter Key** box.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices.

a. Click **Add Tunnel**.

b. In the **Add Tunnel** dialog box, under **Basic Settings** configure the following:

Table 60: Basic Settings

Field	Description
Tunnel Type	Umbrella: (Read only) **ipsec** Zscaler: Click **ipsec** or **gre**. Generic: Click **ipsec** or **gre**.
Interface Name (1..255)	Enter the interface name.
Description	Enter a description for the interface.

Field	Description
Tracker	By default, a tracker is attached to monitor the health of tunnels. Alternatively, you can create a customized tracker as described in step **7** and choose the tracker.

Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
	For releases before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, and you have a Cellular or Dialer interface as the tunnel's source interface, the following workaround must be implemented.
	If you use a cellular interface as a tunnel source interface, you must modify your existing tunnel source interface configuration with the following configuration:
	`interface <interface name>`
	`no tunnel route-via <Interface> mandatory`
	Use the CLI add-on feature template to modify the tunnel configuration on the device. For more information on how to use a CLI add-on feature template, see , Create a CLI Add-On Feature Template.
	After you have modified the tunnel configuration, select the device template for which you want to apply the CLI add-on feature template, and push the configuration to the devices. For more information about attaching a device template to one or more devices, see Attach Template to Devices.
	Note A SIG tunnel will be created for cellular interfaces only if a global VRF has only one transport interface. A SIG tunnel is not be created if a global VRF has multiple transport interfaces.

Source Public IP	(Automatic GRE tunnels to Zscaler only) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. **Default**: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.

Field	Description
Tunnel Destination IP Address/FQDN	(Manual tunnels only) Enter the IP address of the SIG provider endpoint.
Preshared Key	(Manual tunnels only) This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

c. (Optional) Under **Advanced Options**, configure the following:

Table 61: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Table 62: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Field	Description
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 63: (Tunnel Type: ipsec) IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1

Field Name	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 64: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM

Field	Description
Perfect Forward Secrecy	• Specify the PFS settings to use on the IPsec tunnel. • Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: None

d. Click **Add**.

8. To create one or more trackers to monitor tunnel health, click **Tracker** and do the following:

   a. **Source IP Address**: Enter a source IP address for the probe packets.

   b. Click **Add Tracker**.

   c. In the **Add Tracker** dialog box, configure the following:

Table 65: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds.
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3

   d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

   a. Click **Add Interface Pair**.

   b. In the **Add Interface Pair** dialog box, configure the following:

Table 66: High Availability Parameters

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. 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 is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

   c. Click **Add**.

   d. To add more active and back-up tunnel pairs, repeat sub-step **a** to sub-step **c**.

10. (Optional) To configure advanced settings for Cisco Umbrella or Zscaler, click **Advanced Settings** and configure the following:

Table 67: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 68: Zscaler

Field	Description
Primary Datacenter	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.

Field	Description
Secondary Datacenter	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Zscaler Location	(Optional) Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Display Time Unit	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Off
Refresh Time Unit	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help* > *Traffic Forwarding* > *Location Management* > *Configuring Locations*. **Default**: 0

11. Click **Save**.

Redirect Traffic to SIG Using Service VPN Feature

Configure a SIG service route for a service VPN to direct the VPN traffic to SIG.

Note Alternatively, you can also redirect traffic to SIG using Data Policy. For more information, see Action Parameters in the *Policies Configuration Guide*.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. Expand the **Service Profile**, and for the service VPN whose traffic you want to redirect traffic to SIG, click **...** and click **Edit Parcel**.
4. Remove any existing static IPv4 routes to the internet:
   a. Click **Route**.
   b. Under **IPv4 Static Route**, find any routes to the internet and click the delete icon to remove it.
5. Add SIG service route:
   a. Click **Service Route**.
   b. Click **Add Service Route**.

c. In the **Add Service Route** dialog box, configure the following:

Table 69: Service Route Parameters

Field	Description
Network Address	Enter the public IPv4 address.
Subnet Mask	Enter the subnet for the IPv4 address.
Service	Choose **SIG** from the drop-down list.
VPN	Enter the VPN over which to direct the traffic. Default: VPN 0

d. Click **Add**.

6. Click **Save**.

Next steps: Add Devices to Configuration Group and Deploy Devices.

Monitor SIG Events

Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage 20.9.1

Monitor security events related automatic SIG tunnels using the following Cisco SD-WAN Manager GUI components:

- **Security Events** pane on the **Monitor** > **Security** page
- **Events** dashboard on the **Monitor** > **Logs** page

Security Events

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Security**.

   The **Security Events** pane shows how many critical, major, and minor security events Cisco IOS XE Catalyst SD-WAN devices have reported to Cisco SD-WAN Manager during a specified time period. The information is displayed in a bar chart.

   Cisco IOS XE Catalyst SD-WAN devices notify security events to Cisco SD-WAN Manager using NETCONF. The security events include events related to automatic SIG tunnel creation.

2. (Optional) By default, the pane displays security event information for the past 24 hours. To modify the time period, hover the mouse pointer over **24 Hours** and choose a desired time period from the drop-down list.

3. (Optional) **View Details**: Click **View Details** to display the **Monitor** > **Logs** > **Events** page, with information filtered for the **Security** component.

Events Dashboard

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs**.

2. Click **Events**.

   Cisco SD-WAN Manager displays any events that WAN edge devices and controllers have notified in the past three hours.

3. Click **Filter** and configure the following:

Field	Description
Component	Choose the **Security** component.
Severity	Choose one or more of **Critical**, **Major**, and **Minor**. If you do not select specific severities, events of all three severites are displayed.
System IP	To view events notified by specific WAN edge devices, choose the system IP of the devices.
Event name	To view information about one or more specific SIG tunnel events, choose the corresponding event names. **Tip** To view Cisco Umbrella SIG tunnel events, search for events that have `ftm-tunnel` in the event name. To view Zscaler SIG tunnel events, search for events that have `ftm-zia` in the event name.

   Click **Apply**.

   If the target devices or controllers notified any of the chosen events, Cisco SD-WAN Manager displays information about the same.

4. (Optional) To modify the time range, click **3 hours**, select a time range, and click **Apply.**

   Cisco SD-WAN Manager displays event information for the modified time range.

5. (Optional) Click **Export** to download a CSV file containing the table data.

   The file is downloaded to your browser's default download location.

6. (Optional) Click on the gear icon adjacent to **Export** to display the **Table Settings** slide-in pane. Toggle the columns that you wish to display or hide and click **Apply**.

Monitor SIG/SSE Tunnels

Minimum supported releases for SIG: Cisco IOS XE Release 17.9.1a and Cisco vManage 20.9.1

Minimum supported releases for SSE: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

Monitor the status of automatic SIG/SSE tunnels using the following Cisco SD-WAN Manager GUI components:

- **SIG/SSE Tunnel Status** pane on the **Monitor** > **Security** page
- **SIG/SSE Tunnels** dashboard on the **Monitor** > **Tunnels** page

SIG/SSE Tunnel Status

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Security**.

   The **SIG/SSE Tunnel Status** pane shows the following information using a donut chart:

   - total number of SIG/SSE tunnels that are configured
   - the number of SIG/SSE tunnels that are up
   - the number of SIG/SSE tunnels that are down
   - the number of SIG/SSE tunnels that are in a degraded state (Degraded state indicates that the SIG tunnel is up but the Layer 7 health of the tunnel as detected by the tracker does not meet the configured SLA parameters. Therefore, the traffic is not routed through the tunnel.)

2. (Optional) Click a section of the donut chart to view detailed information about tunnels having a particular status.

   Cisco SD-WAN Manager displays detailed information about the tunnels in the **SIG/SSE Tunnels** dashboard.

3. (Optional) Click **All SIG/SSE Tunnels** to view the **SIG/SSE Tunnels** dashboard.

SIG/SSE Tunnels Dashboard

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.

2. Click **SIG/SSE Tunnels**.

   Cisco SD-WAN Manager displays a table that provides the following details about each automatic tunnel created to a Cisco Umbrella, Zscaler SIG or Cisco Secure Access:

Field	Description
Host Name	Host name of the Cisco IOS XE Catalyst SD-WAN device or edge device.
Site ID	ID of the site where the WAN edge device is deployed.
Tunnel ID	Unique ID for the tunnel defined by the SIG/SSE provider.
Transport Type	IPSec or GRE
Tunnel Name	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
HA Pair	Active or Backup
Provider	Cisco Umbrella or Zscaler or Cisco Secure Access

Field	Description
Destination Data Center	SIG/SSE provider data center to which the tunnel is connected. **Note** This feature is supported for Cisco Umbrella SIG endpoints and it is yet to be supported for Zscaler ZIA Public Service Edges.
Tunnel Status (Local)	Tunnel status as perceived by the device.
Tunnel Status (Remote)	Tunnel status as perceived by the SIG/SSE endpoint. **Note** This feature is supported for Cisco Umbrella SIG endpoints and it is yet to be supported for Zscaler ZIA Public Service Edges.
Events	Number of events related to the tunnel set up, interface state change, and tracker notifications. Click on the number to display an Events slide-in pane. The slide-in pane lists all the relevant events for the particular tunnel. **Note** If you delete an automatic SIG tunnel from a GRE or IPSec interface and later configure an automatic SIG tunnel from the same interface, the newly configured SIG tunnel has the same name as the tunnel that you deleted earlier. As a result, when you configure the new tunnel, you may see SIG-tunnel-related events that were historically reported for the tunnel that was deleted earlier, if these events are not yet purged. Before deleting a tunnel using a CLI template, remove any static route pointing to the tunnel. Add the static route after creating the tunnel again.
Tracker	Enabled or disabled during tunnel configuration.

3. (Optional) By default, the table displays information for the past 24 hours. To modify the time period, hover the mouse pointer over **24 Hours** and choose a desired time period from the drop-down list.

4. (Optional) To download a CSV file containing the table data, click **Export**.

   The file is downloaded to your browser's default download location.

5. (Optional) Hide or display table columns: Click on the gear icon adjacent to **Export** to display the **Table Settings** slide-in pane. Toggle the columns that you wish to display or hide and click **Apply**.

Monitor Automatic SIG Tunnels Using CLI

Automatic SIG Tunnels to Cisco Umbrella

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE Catalyst SD-WAN device to Cisco Umbrella, use the **show sdwan secure-internet-gateway umbrella tunnels** command.

The following is a sample output of the **show sdwan secure-internet-gateway umbrella tunnels** command:

```
Device# show sdwan secure-internet-gateway umbrella tunnels
                                                                                     API
 LAST
TUNNEL IF                                                                            HTTP
 SUCCESSFUL    TUNNEL
NAME         TUNNEL ID  TUNNEL NAME                             FSM STATE            CODE
 REQ           STATE
------------------------------------------------------------------------------------------
Tunnel17447  527398582  SITE10005SYS172x16x255x88IFTunnel17447  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22427  527398577  SITE10005SYS172x16x255x88IFTunnel22427  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22457  527398373  SITE10005SYS172x16x255x88IFTunnel22457  st-tun-create-notif  200
 rekey-tunnel  -
```

Automatic SIG Tunnels to Zscaler

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE Catalyst SD-WAN device to Zscaler SIG, use the **show sdwan secure-internet-gateway zscaler tunnels** command.

The following is a sample output of the **show sdwan secure-internet-gateway zscaler tunnels** command for automatic IPSec tunnels:

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

```
Device# show sdwan secure-internet-gateway zscaler tunnels


                        HTTP
TUNNEL IF                                                   TUNNEL
                                                                 LOCATION
                        RESP
NAME          TUNNEL NAME                                   ID        FQDN
                                        TUNNEL FSM STATE         ID        LOCATION FSM
STATE   LAST HTTP REQ     CODE
-------------------------------------------------------------------------------------------
Tunnel100001  site1820851800sys172x16x255x15ifTunnel100001  52615809
site1820851800sys172x16x255x15iftunnel100001@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
Tunnel100002  site1820851800sys172x16x255x15ifTunnel100002  52615814
site1820851800sys172x16x255x15iftunnel100002@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
```

The following is a sample output of the **show sdwan secure-internet-gateway zscaler tunnels** command for automatic GRE tunnels:

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

```
Device# show sdwan secure-internet-gateway zscaler tunnels

                       HTTP
TUNNEL IF                             TUNNEL        TUNNEL FSM      LOCATION
         LAST HTTP     RESP
NAME          TUNNEL NAME             ID      FQDN  STATE           ID        LOCATION FSM
 STATE   REQ           CODE
------------------------------------------------------------------------------------------
Tunnel100512  192.0.2.2_Tunnel100512  102489  n/a   gre-add-tunnel  46206485
location-init-state  activate-req  200
Tunnel100513  192.0.2.2_Tunnel100513  102489  n/a   gre-add-tunnel  46206485
location-init-state  activate-req  200
```

Automatic SIG Tunnels

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE Catalyst SD-WAN device, use the **show sdwan secure-internet-gateway tunnels** command.

The following is a sample output of the **show sdwan secure-internet-gateway tunnels** command:

```
Device# show sdwan secure-internet-gateway tunnels
TUNNEL IF     TUNNEL                                                  HA      DEVICE  SIG
   TRACKER              DESTINATION            TUNNEL
NAME          ID        TUNNEL NAME                                  PAIR    STATE   STATE
  STATE    SITE ID     DATA CENTER  PROVIDER  TYPE    TIMESTAMP
------------------------------------------------------------------------------------------
Tunnel100001  52615809  site1820851800sys172x16x255x15ifTunnel100001  Active  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
Tunnel100002  52615814  site1820851800sys172x16x255x15ifTunnel100002  Backup  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
```

Monitor Layer 7 Health Check SLA Metrics Using the CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

SLA Profile

To view information about the SLA profile that you have configured, from Cisco SD-WAN Manager use the **show endpoint-tracker sla-profile** command.

The following is a sample output of the **show endpoint-tracker sla-profile** command:

```
Device# show endpoint-tracker sla-profile

SLA Profile     SLA mode            cfg loss(%)     cfg latency(ms)  cfg jitter(ms)
sla_agg                  aggressive           10             300             80

sla_con                  conservative         10             300             80

sla_mod                  moderate             10             300             30
```

SLA Mode

To view information about the SLA mode that you have configured from Cisco SD-WAN Manager use the **show endpoint-tracker sla-mode** command.

The following is a sample output of the **show endpoint-tracker sla-mode** command:

```
Device# show endpoint-tracker sla-mode
SLA mode         Poll Interval(Secs)  Poll multiplier(buckets)     Dampening multiplier
   Dampening window(Secs)

=====================================================================================================
Aggressive   60            1                            1                         60

Moderate  120              1                            2                         240

Conservative   300         1                            3                         900
```

The command output shows the following:

- **Poll Interval**: Time period in seconds which defines a bucket of sample data.
- **Poll Multiplier**: Number of buckets to wait before checking the SLA status (Met or Violated).
- **Dampening Multiplier**: Number of extra buckets to wait before allowing an SLA status to change from Violated to Met, to avoid flapping conditions.

SLA Status

To view information about the SLA status use the **show endpoint-tracker sla-status** command.

The following is a sample output of the **show endpoint-tracker sla-status** command:

```
Device# show endpoint-tracker sla-status
Interface   Record name  SLA Profile    SLA Status   Loss(%) Latency(ms)  Jitter(ms)
Tunnel601            youtbue      sla_agg         Met          0       32          46

Tunnel602            netflix      sla_agg         Met          0       4           1
```

SLA Statistics

To view information about the SLA statistics use the **show endpoint-tracker sla-statistics** command.

The following is a sample output of the **show endpoint-tracker sla-statistics** command:

```
Device# show endpoint-tracker sla-statistics
Interface     Index    Loss(%)    Latency(ms)  Jitter(ms)
Tunnel602            0          0           3           0
```

Troubleshoot Integrating Your Devices With Secure Internet Gateways

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

After Upgrading Cisco SD-WAN Manager 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 SD-WAN Manager, 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 SD-WAN Manager, 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 tunnel Number
```

Example:

```
Device#sh sdwan running-config interface | begin Tunnel100001
interface Tunnel100001
 ip unnumbered GigabitEthernet1
 ip mtu 1400
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec2-ipsec-profile
exit
```

GRE Tunnel Creation Fails After You Restore Device Operation

Problem

If you have created an automatic GRE tunnel to a Zscaler SIG endpoint with a source public IP address, the device becomes inoperative due to an event such as a power outage or a maintenance activity. This issue is seen in Cisco IOS XE Catalyst SD-WAN Release 17.9.1a or Cisco IOS XE Catalyst SD-WAN Release 17.9.2a. When you make the device operational again and attempt to create an automatic GRE tunnel to the Zscaler with the same source public IP address, the tunnel creation fails. One of the following failure notifications appears in the **Events** dashboard on the **Monitor** > **Logs** page in the Cisco SD-WAN Manager menu:

- **add-static-ip-failure**
- **add-gre-tunnel-failure**

Alternatively, you can use the **show sdwan secure-internet-gateway zscaler tunnels** command to view the status of the tunnel along with an error code which indicates the reason for the failure of the tunnel creation.

Possible Causes

Tunnel creation fails because the source public IP address may exist on the Zscaler portal. This event occurs because the device didn’t clear the previous tunnels after becoming operational again.

Solution

Delete the existing source public IP address on the Zscaler portal by doing the following:

1. Remove the SIG feature template from the device in Cisco SD-WAN Manager.
2. From the Zscaler portal, choose **Administration** > **Location Management** and search for the location that is associated with the tunnel in the **Location** tab.
3. Click the **Edit** icon and delete the entry.
4. From the Zscaler portal, choose **Administration** > **Static IPs & GRE Tunnels** and locate the static IP address in the **Static IP** tab.
5. Click the **Edit** icon and delete the entry.
6. Attach the SIG template that you removed in the first step, back to the device. For more information about attaching the SIG template, see the section Attach the SIG Template to Devices.

IKE/IPsec Tunnel Failure with Cellular Interface

Note: This problem and solution applies for releases Cisco IOS XE Catalyst SD-WAN Release 17.13.1a or before.

Problem

An IKE/IPsec tunnel cannot be established when a cellular interface is used as the source interface.

Possible Causes

IKE/IPsec packets may be routed through the incorrect source interface.

Solution

When configuring SIG tunnels, especially over cellular interfaces, it's recommended to set the tunnel routing option to **preferred** rather than **mandatory**. Utilizing **preferred** avoids packet loss issues that have been observed when **mandatory** is selected as the routing option for cellular interface-based tunnels.

Here are a few example scenarios to consider when setting up SIG tunnels, particularly with cellular interfaces in the configuration:

1. Cisco IOS XE Catalyst SD-WAN Device with Single Cellular Interface.

   When a cellular interface is active, SIG tunnels will be established as soon as the cellular interface is up.

2. Cisco IOS XE Catalyst SD-WAN Device with Both Broadband and Cellular Interfaces.

   - If both Broadband and Cellular interfaces are active:
     - SIG tunnels will be active for the broadband interface.
     - SIG tunnels will also be active for the cellular interface; however, the cellular interface's IKE/IPsec packets will be routed through the broadband interface.
   - If the broadband interface is down but the cellular interface is up:
     - SIG tunnels for the broadband interface will not be active.
     - SIG tunnels for the cellular interface will remain active, and IKE/IPsec negotiation will occur over the cellular link, as expected.

3. Cisco IOS XE Catalyst SD-WAN Device with Dual Cellular Interfaces.

   - When both cellular interfaces (cellular interface 1 and cellular interface 2) are active:
     - SIG tunnels will be active for both interfaces.
   - When cellular interface 1 is down and cellular interface 2 interface is active:
     - SIG tunnels for cellular interface 1 will not be active, but its IKE/IPsec packets will be rerouted via cellular interface 2.
     - SIG tunnels for cellular interface 2 will continue to remain active.

Here is a sample configuration to address the issue with the IKE/IPsec tunnel not establishing when using the cellular interface as the source interface.

```
interface Tunnel16000001
 no shutdown
 ip unnumbered Cellular0/1/0
 ip mtu 1400
 tunnel source Cellular0/1/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via Cellular0/1/0 preferred
```

Share Traffic Information with Cisco Security Service Edge

Information About Sharing Traffic Information with Cisco Security Service Edge

Minimum Supported Releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

Information Sharing

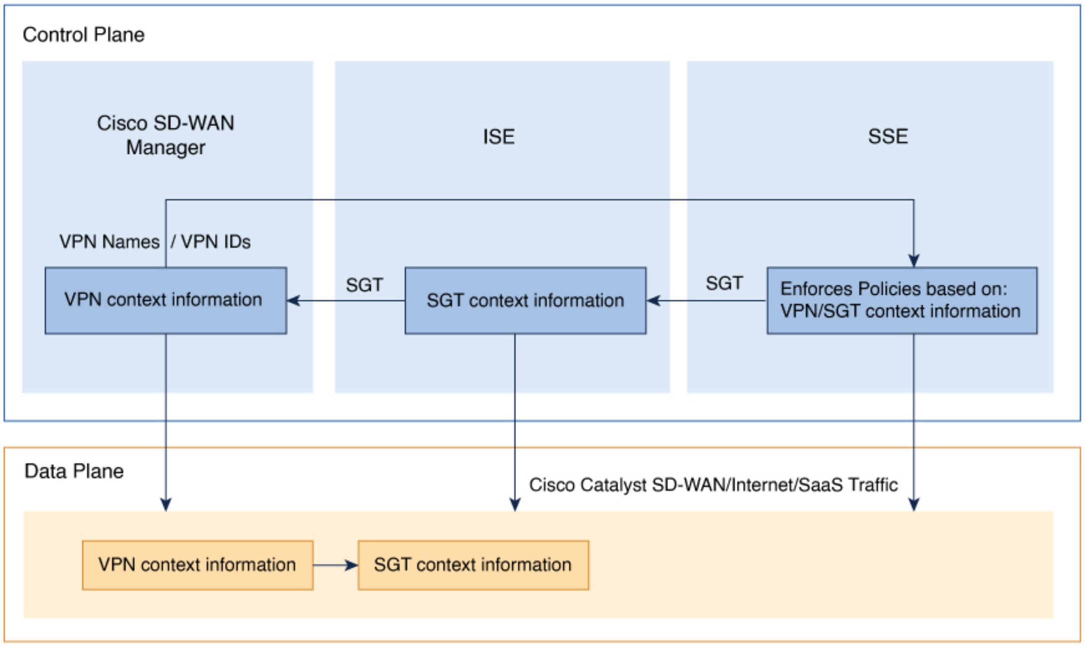
Cisco SD-WAN Manager shares VPN context information with Secure Service Edge (SSE). It provides SSE with VPN details, including VPN names and IDs. ISE shares SGT information with both Cisco SD-WAN Manager and SSE. SSE uses the VPN and SGT information to enforce specific security policies on traffic from Cisco Catalyst SD-WAN to internet and SaaS applications. These policies match source objects based on SGT or VPN for internet- and SaaS-bound traffic.

In the control plane, Cisco SD-WAN Manager shares VPN information with SSE but does not share SGT information. In the data plane, both VPN and SGT information are included in the traffic directed towards Cisco SSE.

Integration Requirements

Integrating ISE with the Cisco SD-WAN Manager is optional, but it is mandatory to configure the integration of ISE with SSE.

Figure 9: Cisco SD-WAN, SSE, and ISE Information Sharing



Prerequisites for Sharing Traffic Information with Cisco Security Service Edge

- **SSE Integration**

  Ensure SSE is integrated with both Cisco SD-WAN Manager and ISE. For more information, see Integrate Your Devices with Secure Service Edge.

- **API Credentials for SSE**

  Ensure that the API credentials for SSE has the necessary permissions, specifically write access, to manage identity-related information and enable context sharing.

- **Configure DNS on VPN0 Interface**

  Ensure DNS is configured on the VPN0 interface of the device for seamless connectivity between Cisco SD-WAN Manager and Cisco Secure Access.

- **Enable NAT on WAN and LAN Interfaces**

  Enable NAT on the WAN and LAN interfaces of the device to ensure proper address translation for both outbound and inbound traffic. This is crucial for maintaining seamless connectivity and proper routing of traffic through the network.

- **CLI Commands for SGT Sharing with SSE**

  To share SGT with SSE, use the following CLI commands as part of the CLI add-on template to fetch the SGT value:

  ```
  policy
   app-visibility
   flow-visibility
   ip visibility features
   ulogging enable
  ```

  For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Restrictions for Sharing Traffic Information with Cisco Security Service Edge

You cannot use CLI profiles to configure this feature.

Configure Sharing Traffic Information with Cisco Security Service Edge

Enable Context Sharing

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Credentials**.
2. Click **Context Sharing** to enable the context sharing in Cisco SD-WAN Manager.

Note Context sharing cannot be disabled after it is enabled.

Enable Context Sharing for VPN and SGT

Enable context sharing for VPN and SGT to allow Cisco IOS XE Catalyst SD-WAN devices to share context information with SSE.

From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Add Secure Service Edge (SSE)**.

Field	Description
VPN	Enable sharing of VPN information with SSE.
SGT	Enable sharing of SGT information with SSE.

Create SSE Policy Using Policy Group

For more information, see Configure a Secure Service Edge.

Verify Traffic Information Sharing with Cisco Security Service Edge

To check whether context sharing is active on a Cisco IOS XE Catalyst SD-WAN device, use the **show sse all** command.

In the following command, context sharing is enabled, and it is shown in bold.

```
Device# show sse all

***************************************
SSE Instance Cisco-Secure-Access
***************************************
Tunnel name : Tunnel16000001
Site id: 2432287619
Tunnel id: 634930903
SSE tunnel name: C8K-e28146f8-e524-46ff-a799-a95fc1a086da
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN | CONTEXT_SHARING_SGT
```

Monitor Traffic Information Sharing with Cisco Security Service Edge

Monitor SIG/SSE Tunnels

Use the security operations dashboard to monitor the status and performance of SSE tunnels.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Security**.

   The **SIG/SSE Tunnel Status** pane shows the following information using a donut chart:

   - Total number of SIG/SSE tunnels that are configured.
   - The number of SIG/SSE tunnels that are up and down.

- The number of SIG/SSE tunnels that are in a degraded state.

  Degraded state indicates that the SIG tunnel is up but the Layer 7 health of the tunnel as detected by the tracker does not meet the configured SLA parameters. Traffic is not routed through the tunnel.

2. (Optional) Click a section of the donut chart to view detailed information about tunnels having a particular status.

   Cisco SD-WAN Manager displays detailed information about the tunnels in the **SIG/SSE Tunnels** dashboard.

3. (Optional) Click **All SIG/SSE Tunnels** to view the **SIG/SSE Tunnels** dashboard.

View SSE Tunnels

View SSE tunnels to obtain granular information about each tunnel.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.
2. Click **SIG/SSE Tunnels**.

   Cisco SD-WAN Manager displays a table that provides the following details about each automatic tunnel created to a Cisco Umbrella, Zscaler SIG or Cisco Secure Access: For more information, see the section **SIG/SSE Tunnels Dashboard** in Monitor SIG/SSE Tunnels, on page 285.

View Context-Sharing Data

View context-sharing data by enabling context-sharing filters. These filters can help identify whether the context-sharing data (VPN and SGT) is enabled or disabled.

To enable context-sharing filters:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels** > **SIG/SSE Tunnels**.
2. Click on the gear icon to display the table settings slide-in pane.
3. Click to enable the context sharing filters to display detailed information about VPN and SGT context sharing in the table.

CHAPTER 13

Integrate Your Devices with Secure Service Edge

Table 70: Feature History

Feature	Release Information	Description
Cisco Secure Access Integration	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Cisco Secure Access is a cloud Security Service Edge (SSE) solution, that provides seamless, transparent, and secure Direct Internet Access (DIA). This feature supports Cisco Secure Access integration through policy groups in Cisco SD-WAN Manager.
Zscaler Integration	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature adds Zscaler integration with Cisco Catalyst SD-WAN as part of a simplified Security Service Edge (SSE) automation solution. You can provision both IPSec and GRE tunnels to Scaler using policy groups in Cisco SD-WAN Manager.
Zscaler Sub-Locations	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	With this feature you can configure one or more Zscaler sub-locations for a given location.

Information About Cisco Secure Access Integration

Cisco Secure Access is a cloud-based platform that provides multiple levels of defense against internet-based threats. From Cisco Catalyst SD-WAN Manager Release 20.13.1 Cisco Secure Access is integrated with Cisco Catalyst SD-WAN.

To configure Secure Service Edge (SSE), choose Cisco Secure Access as the provider in the SSE policy group in Cisco SD-WAN Manager. The SSE policy group defines IPSec tunnels and tunnel parameters. You can provision network tunnel groups in Cisco Secure Access and provide attributes to the edge devices that are needed to setup IPSec tunnels. For more information on network tunnel groups, see Manage Network Tunnel Groups.

Information About Zscaler Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can integrate Cisco Catalyst SD-WAN edge devices with Zscaler by provisioning automatic IPsec or GRE tunnels between the edge devices and the Security Service Edge (SSE) solution. Zscaler Internet Access (ZIA) inspects and secures traffic from Cisco Catalyst SD-WAN devices. The Cisco SD-WAN Manager uses Zscaler APIs to create the IPSec or GRE tunnels.

In the Zscaler integration the data center selection is based on the public IP address of the device. In the SSE configurations in Cisco SD-WAN Manager, if you enable the **Country** flag, the Zscaler APIs calls return the closest data centers within the country of the device. If there are no data centers in the country, Cisco SD-WAN Manager reports an error.

Information About Zscaler Sub-Locations

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

For a given Zscaler location, Cisco SD-WAN Manager supports one or more Zscaler sub-locations and their corresponding subnets. Using the IP addresses encapsulated within a GRE or IPSec tunnel of the sublocations, you can create new locations.

When you add a sub-location in Cisco SD-WAN Manager, the service automatically creates a default **Other** sub-location. You cannot rename the **Other** sub-location. The **Other** sub-location includes IP addresses that aren't already defined in any other sub-location.

Bandwidth Control

With the bandwidth control functionality, you can control bandwidth usage between a location and its sub-locations. You can provide a different bandwidth for sub-locations or use the parent locations settings. You can specify the upload and download bandwidths while creating a location. Any unused bandwidth from sub-locations remain available to the parent location.

Restrictions for Cisco Secure Access Integration

- Cisco SD-WAN Manager does not support API throttling to Cisco Secure Access.
- This feature cannot be configured through a CLI template. This feature can be configured using policy groups on Cisco SD-WAN Manager.
- After Cisco Secure Access integration with Cisco Catalyst SD-WAN, any changes made to the network tunnel group name in Cisco Secure Access dashboard are not reflected in Cisco SD-WAN Manager.

Restrictions for Zscaler Sub-Locations

- IP Addresses

  The sub-locations cannot have overlapping IP addresses within a location.

  The Sub-locations should support an individual IP address or a range of IP addresses. For example 10.0.0.2-10.0.0.25.

- Name

  The sub-location name should be unique.

Configure Tunnels to Cisco Secure Access or Zscaler Using Cisco SD-WAN Manager

Workflow for Cisco Secure Access or Zscaler Integration with Cisco Catalyst SD-WAN

Before You Begin

- Ensure that a configuration group is associated to the selected WAN edge devices and deployed.
- Configure the **IP domain lookup** command on the device.
- Configure the DNS server on Cisco SD-WAN Manager to connect to Cisco Secure Access or Zscaler.
- Add, modify or delete Zscaler sub-locations only from Cisco SD-WAN Manager and not from Zscaler portal. This ensures that the sub-location configurations between Cisco SD-WAN Manager and Zscaler are in sync.

Workflow for Cisco Secure Access or Zscaler Integration with Cisco Catalyst SD-WAN:

1. Create Cisco Secure Access or Zscaler credentials on the **Administrator** > **Settings** page.
2. Create automatic tunnels to Cisco Secure Access or Zscaler using **Configuration** > **Policy Groups**.
3. Redirect traffic to Cisco Secure Access or Zscaler using service routes or policy groups.

Create Cisco Secure Access Credentials

1. From **Configuration** > **Policy Groups** > **Add Secure Service Edge (SSE)** in Cisco SD-WAN Manager, select Cisco Secure Access as the provider.

2. Create the credentials in the **Administration > Settings** page. Click **Click here to add Cisco Secure Access Credentials** to create the Cisco Secure Access credentials.

   Enter Cisco Secure Access credentials:

Field	Description
Organization ID	Cisco Secure Access organization ID for your organization. For more information, see *Find Your Organization ID* in the Cisco Secure Access User Guide.
API Key	Cisco Secure Access API Key.
Secret	Cisco Secure Access API Secret.

   Click **Add**.

Create Zscaler Credentials

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.

2. Click **Add Secure Service Edge (SSE)** and select **Zscaler** as the provider.

3. Add the Zscaler credentials.

   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

   b. Click **Click here to add Zscaler Credentials** to create the Zscaler credentials.

   c. Enter the following information:

   Table 71: Zscaler Credentials

Field	Description
Organization ID	Name of the organization in Zscaler cloud. For more information, see *ZIA Help* > *Getting Started* > *Admin Portal* > *About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help* > *ZIA API* > *API Developer & Reference Guide* > *Getting Started*.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

Field	Description
Username	Username of the Cisco Catalyst SD-WAN partner account.
Password	Password of the Cisco Catalyst SD-WAN partner account.

d. Click **Add**.

Create Tunnels to Cisco Secure Access or Zscaler Using Policy Groups

You can create automatic tunnels to Cisco Secure Access or Zscaler using **Configuration > Policy Groups > Secure Service Edge**. For more information see, Configure Secure Service Edge.

When ...	Then for Cisco Secure Access ...	And for Zscaler ...
The deletion is initiated from Cisco SD-WAN Manager, the SSE Tunnel is not removed from the SSE dashboard.	You must manually delete the Remote Tunnel Group, which is the device Chassis ID (specific to Cisco Secure Access), from the SSE dashboard before provisioning it again from Cisco SD-WAN Manager.	If the location is not deleted, you must search for the given location in Zscaler and delete it.

Redirect Traffic to Cisco Secure Access or Zscaler

You can redirect traffic to a Cisco Secure Access or Zscaler in two ways:

- Using policy groups:

  1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.
  2. Add rules and set the action parameters to the policy to redirect traffic to the SSE instance. For more information, see Action Parameters in the *Policy Groups Configuration Guide*.

- Using service route:

  1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Service Profile**.
  2. Modify the service VPN parameters to ensure that the device connects to the SSE instance to include a service route to the SSE. For more information, see Service VPN in *Configuration Groups Configuration Guide*.

Monitor Security Service Edge Tunnels using CLI

To view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device, use the **show sse all** command.

```
Device# show sse all

***************************************
   SSE  Instance Cisco-Secure-Access
***************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access

Tunnel name : Tunnel15000002
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 44.241.136.173
Tunnel type: IPSEC
Provider name: Cisco Secure Access



*******************************************
   TUNNEL DB ALL
*******************************************

 Tun:Tunnel15000001 Instance:Cisco-Secure-Access (Id:2)
 Tun:Tunnel15000002 Instance:Cisco-Secure-Access (Id:2)

*******************************************
   SERVICE ROUTE LIST ALL
*******************************************
```

To view information about the GRE tunnels configured using Zscaler SSE provider on a Cisco Catalyst SD-WAN device, use the **show sse all** command.

```
Device# show sse all

***************************************
   SSE  Instance zScaler
***************************************
Tunnel name : Tunnel16000512
Site id: 2447182820
Tunnel id: 1299582
SSE tunnel name: site2447182820sys172x16x255x15Tunnel16000512
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 165.225.50.20
Tunnel type: GRE
Provider name: zScaler
Context sharing:  NA

Tunnel name : Tunnel16000513
Site id: 2447182820
```

```
Tunnel id: 1299582
SSE tunnel name: site2447182820sys172x16x255x15Tunnel16000513
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 104.129.198.174

Tunnel type: GRE
Provider name: zScaler
Context sharing:  NA



*******************************************
   TUNNEL DB ALL
*******************************************

 Tun:Tunnel16000512 Instance:zScaler (Id:2)
 Tun:Tunnel16000513 Instance:zScaler (Id:2)
```

To view information about the IPsec tunnels configured using Zscaler SSE provider on a Cisco Catalyst SD-WAN device, use the **show sse all** command.

```
Device# show sse all

***************************************
   SSE  Instance zScaler
***************************************

Tunnel name : Tunnel16000001
Site id: 2480190864
Tunnel id: 101989981
SSE tunnel name: site2480190864sys172x16x255x15Tunnel16000001
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 165.225.242.40
Tunnel type: IPSEC
Provider name: zScaler
Context sharing:  NA

Tunnel name : Tunnel16000002
Site id: 2480190864
Tunnel id: 101990028
SSE tunnel name: site2480190864sys172x16x255x15Tunnel16000002
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 104.129.198.179
Tunnel type: IPSEC
Provider name: zScaler
Context sharing:  NA



*******************************************
   TUNNEL DB ALL
*******************************************

 Tun:Tunnel16000001 Instance:zScaler (Id:2)
 Tun:Tunnel16000002 Instance:zScaler (Id:2)
```

```
*******************************************
   SERVICE ROUTE LIST ALL
*******************************************
Service Route    : 0.0.0.0/0 vrf_name:2
sse_list:
 Name:global

Service Route    : 0.0.0.0/0 vrf_name:3
sse_list:
 Name:global

Service Route    : 10.0.0.2/32 vrf_name:65528
sse_list:
 Name:zScaler

Service Route    : 0.0.0.0/0 vrf_name:1
sse_list:
 Name:zScaler
```

Monitor SIG/SSE Tunnels

Minimum supported releases for SIG: Cisco IOS XE Release 17.9.1a and Cisco vManage 20.9.1

Minimum supported releases for SSE: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

Monitor the status of automatic SIG/SSE tunnels using the following Cisco SD-WAN Manager GUI components:

- **SIG/SSE Tunnel Status** pane on the **Monitor** > **Security** page
- **SIG/SSE Tunnels** dashboard on the **Monitor** > **Tunnels** page

SIG/SSE Tunnel Status

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Security**.

   The **SIG/SSE Tunnel Status** pane shows the following information using a donut chart:

   - total number of SIG/SSE tunnels that are configured
   - the number of SIG/SSE tunnels that are up
   - the number of SIG/SSE tunnels that are down
   - the number of SIG/SSE tunnels that are in a degraded state (Degraded state indicates that the SIG tunnel is up but the Layer 7 health of the tunnel as detected by the tracker does not meet the configured SLA parameters. Therefore, the traffic is not routed through the tunnel.)

2. (Optional) Click a section of the donut chart to view detailed information about tunnels having a particular status.

   Cisco SD-WAN Manager displays detailed information about the tunnels in the **SIG/SSE Tunnels** dashboard.

3. (Optional) Click **All SIG/SSE Tunnels** to view the **SIG/SSE Tunnels** dashboard.

SIG/SSE Tunnels Dashboard

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.
2. Click **SIG/SSE Tunnels**.

   Cisco SD-WAN Manager displays a table that provides the following details about each automatic tunnel created to a Cisco Umbrella, Zscaler SIG or Cisco Secure Access:

Field	Description
Host Name	Host name of the Cisco IOS XE Catalyst SD-WAN device or edge device.
Site ID	ID of the site where the WAN edge device is deployed.
Tunnel ID	Unique ID for the tunnel defined by the SIG/SSE provider.
Transport Type	IPSec or GRE
Tunnel Name	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
HA Pair	Active or Backup
Provider	Cisco Umbrella or Zscaler or Cisco Secure Access
Destination Data Center	SIG/SSE provider data center to which the tunnel is connected. **Note** This feature is supported for Cisco Umbrella SIG endpoints and it is yet to be supported for Zscaler ZIA Public Service Edges.
Tunnel Status (Local)	Tunnel status as perceived by the device.
Tunnel Status (Remote)	Tunnel status as perceived by the SIG/SSE endpoint. **Note** This feature is supported for Cisco Umbrella SIG endpoints and it is yet to be supported for Zscaler ZIA Public Service Edges.

Field	Description
Events	Number of events related to the tunnel set up, interface state change, and tracker notifications. Click on the number to display an Events slide-in pane. The slide-in pane lists all the relevant events for the particular tunnel. **Note** If you delete an automatic SIG tunnel from a GRE or IPSec interface and later configure an automatic SIG tunnel from the same interface, the newly configured SIG tunnel has the same name as the tunnel that you deleted earlier. As a result, when you configure the new tunnel, you may see SIG-tunnel-related events that were historically reported for the tunnel that was deleted earlier, if these events are not yet purged. Before deleting a tunnel using a CLI template, remove any static route pointing to the tunnel. Add the static route after creating the tunnel again.
Tracker	Enabled or disabled during tunnel configuration.

3. (Optional) By default, the table displays information for the past 24 hours. To modify the time period, hover the mouse pointer over **24 Hours** and choose a desired time period from the drop-down list.

4. (Optional) To download a CSV file containing the table data, click **Export**.

   The file is downloaded to your browser's default download location.

5. (Optional) Hide or display table columns: Click on the gear icon adjacent to **Export** to display the **Table Settings** slide-in pane. Toggle the columns that you wish to display or hide and click **Apply**.

Troubleshooting Using Cisco SD-WAN Manager

You can troubleshoot provisioning errors or view the remote tunnel status using the audit logs. For more information, see View Audit Log Information.

CHAPTER 14

GRE Over IPsec Tunnels

Table 72: Feature History

Feature Name	Release Information	Description
GRE Over IPsec Tunnels Between Cisco IOS XE Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to set up GRE over IPsec tunnels with IKEv2 RSA-SIG authentication on Cisco IOS XE Catalyst SD-WAN devices in the controller mode to connect to Cisco IOS XE devices in the autonomous mode. This set up enables Cisco IOS XE Catalyst SD-WAN devices to use OSPFv3 as the dynamic routing protocol and multicast traffic across the WAN network. You can configure GRE over IPsec tunnels using the CLI device templates in Cisco SD-WAN Manager for Cisco IOS XE Catalyst SD-WAN devices.

GRE Over IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices

You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnels on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast(in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.

Prerequisites for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

To configure GRE over IPsec tunnels, use Internet Key Exchange Version 2 (IKEv2) protocol, and RSA Signature as the authentication method.

Restrictions for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

- IPv6 addresses for IPsec tunnel source are not supported.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.
- You cannot configure GRE Over IPsec tunnels between Cisco IOS XE devices using Cisco SD-WAN Manager GUI.

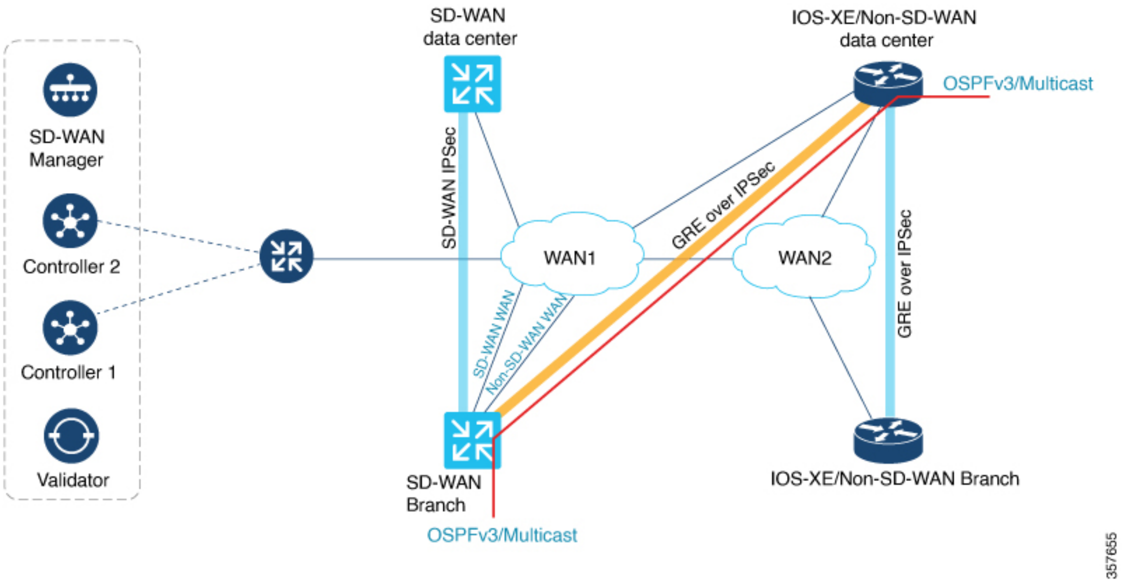
Benefits of GRE Over IPsec Tunnels Between Cisco IOS XE Devices

- Enables migration. You can either migrate to a Cisco Catalyst SD-WAN network or modify a device to support Cisco Catalyst SD-WAN.
- Provides a full mesh connection between a branch and data center, irrespective of whether the network is a Cisco Catalyst SD-WAN network or a non-SD-WAN network.
- Supports OSPFv3 and multicast traffic from a Cisco Catalyst SD-WAN enabled branch to a non-SD-WAN data center.

Use Case for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

In this sample topology, there are Cisco IOS XE devices that are located in different data centers and branches. Two Cisco IOS XE devices in the controller mode are located in the Cisco Catalyst SD-WAN network, one in a data center and another in a branch. The other two Cisco IOS XE devices in the autonomous mode are located in a non-SD-WAN network. A GRE over IPsec tunnel is configured to connect the Cisco IOS XE devices from the branch on the Cisco Catalyst SD-WAN network to the data center located in the non-SD-WAN network.

Note Ensure that the tunnel source is configured with the global VPN for the WAN side and the tunnel VRF configured with the service VPN for the Service side.



Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices

Configuring GRE over IPsec tunnels using Cisco SD-WAN Manager is a two-step process:

1. Install Certification Authentication.

   Import the pkcs12 file on the Cisco IOS XE Catalyst SD-WAN device using the **pki import** command. For information, see the **Install Certification Authentication** section in Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI .

2. Prepare the GRE over IPsec tunnel configurations (GRE, IPsec, IKEv2, PKI, OSPFv3 and Multicast) via the Cisco SD-WAN Manager CLI Template, and push it to the Cisco IOS XE Catalyst SD-WAN device. For information about using a device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices.

   See the **Configure GRE Over IPsec Tunnel** section in Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI for a sample configuration for use in the CLI template.

Note Note: Add the **crypto pki trustpoint** configuration command explicitly in the Cisco SD-WAN Manager CLI template.

Configure GRE Over IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices Using the CLI

This section provides example CLI configurations to configure GRE over IPsec tunnels for Cisco IOS XE Catalyst SD-WAN devices in the controller mode.

Install Certification Authentication

Import the pkcs12 file on the Cisco IOS XE Catalyst SD-WAN device using the **pki import** command.

```
Device# crypto pki import trustpoint_name pkcs12 bootflash:certificate_name
password cisco
```

Execute the **crypto pki trustpoint** command to reconfigure the Cisco IOS XE Catalyst SD-WAN device.

```
Device(config)# crypto pki trustpoint trustpoint_name
Device(ca-trustpoint)# enrollment pkcs12
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# rsakeypair trustpoint_name
```

Configure GRE over IPsec Tunnel

The following is a sample configuration example for configuring GRE over IPsec tunnel.

```
interface Tunnel100
 no shutdown
 vrf forwarding 11
 ip address 10.10.100.1 255.255.255.0
 ipv6 address 2001:DB8:0:ABCD::1
 ipv6 enable
 ospfv3 100 ipv4 area 0
 ospfv3 100 ipv6 area 0
 tunnel source GigabitEthernet4
 tunnel destination 10.0.21.16
 tunnel path-mtu-discovery
 tunnel protection ipsec profile ikev2_TP
exit
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 profile cisco
 authentication local rsa-sig
 authentication remote rsa-sig
 identity local dn
 match address local 10.0.20.15
 match fvrf any
 match identity remote any
 pki trustpoint TRUST_POINT_100
!
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16
 integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set transform-set-v4 esp-gcm 256
 mode transport/tunnel
!
crypto ipsec profile ikev2_TP
 set ikev2-profile cisco
 set pfs group16
 set transform-set transform-set-v4
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
!
crypto pki trustpoint TRUST_POINT_100
 enrollment pkcs12
 revocation-check none
 rsakeypair TRUST_POINT_100
```

Note The configurations for GRE over IPsec tunnels for Cisco IOS XE devices in the autonomous mode are the same as in the controller mode shown above.

Furthermore, the steps to install certification authentication for Cisco IOS XE devices in the autonomous mode is the same as in Cisco IOS XE Catalyst SD-WAN devices, and there is no requirement for you to reconfigure **crypto pki trustpoint** explicitly on the Cisco IOS XE devices in the autonomous mode.

Monitor GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI

Example 1

The following is sample output from the **show crypto pki certificates** command using the optional trustpoint-name argument and verbose keyword. The output shows the certificate of a device and the certificate of the CA. In this example, general-purpose RSA key pairs are previously generated, and a certificate is requested and received for the key pair.

```
Device# show crypto pki certificates verbose TRUST_POINT_100
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 31
  Certificate Usage: General Purpose
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    Name: ROUTER1
    cn=ROUTER1
    o=Internet Widgits Pty Ltd
    st=Some-State
    c=AU
  Validity Date:
    start date: 12:57:14 UTC Jul 24 2021
    end   date: 12:57:14 UTC Jul 22 2031
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: D0AD3252 586C0DB8 9F4EFC15 1D81AC5F
  Fingerprint SHA1: 6824ED1A C1405149 577CF210 C0BC83D1 8741F0D1
  X509v3 extensions:
    X509v3 Subject Key ID: E806DCF5 89698C43 97795999 4440D7F1 16F9827C
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:26 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_100
  Storage: nvram:CRDC#31.cer
  Key Label: TRUST_POINT_100
  Key storage device: private config

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Validity Date:
    start date: 13:41:14 UTC Feb 9 2018
    end   date: 13:41:14 UTC Feb 9 2038
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 5ECA97DB 97FF1B95 DFEEB8FB DAB6656F
  Fingerprint SHA1: 73A7E91E 3AB12ABE 746348E4 A0E21BE3 8413130C
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:23 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_ex TRUST_POINT_100
  Storage: nvram:CRDC#1CA.cer
```

Example 2

The following is sample output from the **show crypto ipsec sa** command to display the settings used by IPsec security associations.

```
Device# show crypto ipsec sa
interface: Tunnel100
    Crypto map tag: Tunnel100-head-0, local addr 10.0.20.15

   protected vrf: 11
   local  ident (addr/mask/prot/port): (10.0.20.15/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.0.21.16/255.255.255.255/47/0)
   current_peer 10.0.21.16 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2674, #pkts encrypt: 2674, #pkts digest: 2674
    #pkts decaps: 2677, #pkts decrypt: 2677, #pkts verify: 2677
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.20.15, remote crypto endpt.: 10.0.21.16
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet4
     current outbound spi: 0xDEFA0160(3740926304)
     PFS (Y/N): Y, DH group: group16

     inbound esp sas:
      spi: 0x32A84C67(849890407)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2057, flow_id: CSR:57, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime (sec): 2217
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y  replay window size: 512
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xDEFA0160(3740926304)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2058, flow_id: CSR:58, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime (sec): 2217
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y  replay window size: 512
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Example 3

The following example shows the **show crypto session detail** command output that displays the status information for active crypto sessions.

```
Device# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel100
Profile: cisco
Uptime: 03:59:01
Session status: UP-ACTIVE
Peer: 10.0.21.16 port 500 fvrf: (none) ivrf: 11
      Phase1_id: cn=ROUTER2,o=Internet Widgits Pty Ltd,st=Some-State,c=AU
      Desc: (none)
  Session ID: 1780
  IKEv2 SA: local 10.0.20.15/500 remote 10.0.21.16/500 Active
          Capabilities:U connid:1 lifetime:20:00:59
  IPSEC FLOW: permit 47 host 10.0.20.15 host 10.0.21.16
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1668 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
        Outbound: #pkts enc'ed 1665 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
```

Example 4

The following is sample output from the **show crypto key mypubkey rsa** command that displays the RSA public keys of your device.

```
Device# show crypto key mypubkey rsa
Key name: TRUST_POINT_100
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00B4E83F ABAE87DC DB7ACBB2 844F5FD6 FF2E9E02 DE49A302 D3D7884F 0B26EE6A
  D3D56275 4D733A4F 5D974061 CE8FB520 54276D6D 3B132C82 EB8A3C24 115F77F5
  C38740CE 1BBD89DB 3F766728 649B63FC 2C40C3AD 251656A1 BAF8341E 1736F03D
  0A0D15AF 0E9D3E94 4E2074C7 BA572CA3 95B3D664 916ADA74 281CDE07 B3DD0B42
  13289610 32E611AB 2B3B4EB6 0A3573B1 F097AC2A 3720961C 97597201 3CE8171C
  F02B99B4 3B7B718F 83E221E1 E172554D C2BEA127 93882766 A28C5E8C 4B83BDC5
  A161597D 2C3D8E13 3BE00D8F 02D0AD55 962DF402 599580A6 F049DBF4 045D751B
  A8932156 10B29D9F 037AB33F C1FC463D E59E014C 27660223 546A8B3A E6997713
  CF020301 0001
% Key pair was generated at: 00:22:51 UTC Oct 27 2021
```

CHAPTER 15

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

Table 73: Feature History

Feature Name	Release Information	Description
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices Over a Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.x	This feature allows you to configure an IPv6 GRE or IPsec tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a service VPN.
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices Over a Transport VPN	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature allows you to configure an IPv6 GRE or IPsec tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a transport VPN.

Information About IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third Party Devices

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

This feature allows you to configure an IPv6 GRE or IPSEC tunnel from Cisco IOS XE Catalyst SD-WAN devices to a third-party device over a service VPN or (from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a) a transport VPN. The following types are supported for a tunnel in a service VPN:

- IPv6 GRE tunnel over IPv4 underlay
- IPv6 GRE tunnel over IPv6 underlay
- IPsec IPv6 tunnel over IPv4 underlay
- IPsec IPv6 tunnel over IPv6 underlay

The following types are supported for a tunnel in a transport VPN:

- IPv6 GRE tunnel over IPv4 underlay
- IPv6 GRE tunnel over IPv6 underlay
- IPsec IPv6 tunnel over IPv4 underlay
- IPsec IPv6 tunnel over IPv6 underlay

Restrictions for IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

- Configuration methods:
  - Cisco IOS XE Catalyst SD-WAN Release 17.12.1a supports configuration in a service VPN by CLI template only.
  - Cisco IOS XE Catalyst SD-WAN Release 17.14.1a supports configuration in a service VPN by feature template and configuration groups.
  - Cisco IOS XE Catalyst SD-WAN Release 17.14.1a supports configuration in a transport VPN by CLI, feature template, and configuration groups.
- Dual stack:

  Dual stack is not supported for IPsec tunnels.
- Loopback interface:

  The interface name as loopback for tunnel source is not supported in the service VPN. When you use a loopback interface as a tunnel source, you must provide either an IPv4 or IPv6 address as the tunnel source field. You can provide an interface name as tunnel source field for the physical interface and sub-interface.
- NAT traversal:

  NAT traversal is not supported for IPsec tunnels with IPv6 underlay.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Supported Devices for IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

Table 74: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and later	• Cisco Catalyst 8200 Series Edge Platforms

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and later	• Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Edge Platforms • Cisco Catalyst 8000V Edge Software • Cisco ASR 1001-HX Router • Cisco ASR 1002-HX Router • Cisco ISR1100 Series Routers • Cisco 4461 Integrated Services Router

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Service VPN Using a CLI Template

Before You Begin

Configure a common source interface:

1. Enter interface configuration mode.

   ```
   interface GigabitEthernet1
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Set an IP address for the interface.

   ```
   ip address 209.165.200.225 255.255.255.0
   ```

4. Configure an IPv6 address.

   ```
   ipv6 address 2001:DB8:200::225/64
   ```

5. Exit the interface configuration mode.

   ```
   exit
   ```

Configure a loopback interface:

1. Configure a loopback interface.

   ```
   interface Loopback 0
   ```

2. Set an IP address for the interface.

   ```
   ip address 209.165.201.1 255.255.255.0
   ```

3. Configure an IPv6 address.

   ```
   ipv6 address 2001:DB8:201::1/64
   ```

4. Exit the interface configuration mode.

   ```
   exit
   ```

Here's the complete configuration example for configuring a common source interface.

```
interface GigabitEthernet5
 no shutdown
 ip address 209.165.202.129 255.255.255.0
 ipv6 address 2001:DB8:202::129/64
exit
interface Loopback0
 no shutdown
 ip address 209.165.201.1 255.255.255.0
 ipv6 address 2001:DB8:201::1/64
exit
```

Configure an IPv6 GRE Tunnel Over IPv4 Underlay

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Create an interface tunnel.

   ```
   interface Tunnel64
   ```

3. Enable the interface.

   ```
   no shutdown
   ```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

   ```
   vrf forwarding 1
   ```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

   ```
   ipv6 address 2001:DB8:64::1/64
   ```

6. Set the source address for the tunnel interface in interface configuration mode.

   ```
   tunnel source 209.165.202.129
   ```

7. Set the destination address for the GRE tunnel interface in interface configuration mode.

   ```
   tunnel destination 209.165.202.158
   ```

8. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet5 mandatory
   ```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over IPv4 underlay.

```
interface Tunnel64
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:64::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPv6 GRE Tunnel Over IPv6 Underlay

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Enter the tunnel interface mode.

   ```
   interface Tunnel66
   ```

3. Enable the interface.

   ```
   no shutdown
   ```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

   ```
   vrf forwarding 1
   ```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

   ```
   ipv6 address 2001:DB8:166::1/64
   ```

6. Set the source address for the tunnel interface in interface configuration mode.

   ```
   tunnel source 2001:DB8:15::15
   ```

7. Set the destination address for the GRE tunnel interface in interface configuration mode.

   ```
   tunnel destination 2001:DB8:15::16
   ```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

   ```
   tunnel mode gre ipv6
   ```

9. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet5 mandatory
   ```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over IPv6 underlay.

```
interface Tunnel66
 no shutdown
  vrf forwarding 1
  ipv6 address 2001:DB8:66::1/64
  tunnel source 2001:DB8:15::15
  tunnel destination 2001:DB8:15::16
  tunnel mode gre ipv6
  tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPsec IPv6 Tunnel Over IPv4 Underlay

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Enter the tunnel interface mode.

   ```
   interface Tunnel164
   ```

3. Enable the interface.

   ```
   no shutdown
   ```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

```
vrf forwarding 1
```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

   ```
   ipv6 address 2001:DB8:164::1/64
   ```

6. Set the source address for the tunnel interface in interface configuration mode.

   ```
   tunnel source 209.165.202.129
   ```

7. Set the destination address for the IPsec tunnel interface in interface configuration mode.

   ```
   tunnel destination 209.165.202.158
   ```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

   ```
   tunnel mode ipsec ipv4 v6-overlay
   ```

9. Associate the tunnel interface with an IPsec profile.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile164
   ```

10. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

    ```
    tunnel route-via GigabitEthernet5 mandatory
    ```

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over IPv4 underlay.

```
interface Tunnel164
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:164::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel mode ipsec ipv4 v6-overlay
 tunnel protection ipsec profile if-ipsec1-ipsec-profile164
 tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPsec IPv6 Tunnel Over IPv6 Underlay

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Enter the tunnel interface mode.

   ```
   interface Tunnel166
   ```

3. Enable the interface.

   ```
   no shutdown
   ```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

   ```
   vrf forwarding 1
   ```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

   ```
   ipv6 address 2001:DB8:166::1/64
   ```

6. Set the source address for the tunnel interface in interface configuration mode.

   ```
   tunnel source 2001:DB8:15::15
   ```

7. Set the destination address for the IPsec tunnel interface in interface configuration mode.

```
tunnel destination 2001:DB8:15::16
```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

   ```
   tunnel mode ipsec ipv6
   ```

9. Associate the tunnel interface with an IPsec profile.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile166
   ```

10. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

    ```
    tunnel route-via GigabitEthernet5 mandatory
    ```

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over IPv6 underlay.

```
interface Tunnel166
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:166::1/64
 tunnel source 2001:DB8:15::15
 tunnel destination 2001:DB8:15::16
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile if-ipsec1-ipsec-profile166
 tunnel route-via GigabitEthernet5 mandatory
```

Verify IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN devices and Third-Party Devices in Service VPN

The following is a sample output from the **show run interface** *type/number* command.

```
Device#show run interface tunnel 164
interface Tunnel164
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:164::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel mode ipsec ipv4 v6-overlay
 tunnel protection ipsec profile if-ipsec1-ipsec-profile164
 tunnel route-via GigabitEthernet5 mandatory
```

The following is a sample output from the **show adjacency tunnel164 internal** command.

```
Device#show adjacency tunnel164 internal
Protocol Interface                 Address
IPV6     Tunnel164                 point2point(7)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 14
                                   empty encap string
                                   P2P-ADJ
                                   Next chain element:
                                     IP adj out of GigabitEthernet5, addr 209.165.202.158
718424FDE3D8
                                     parent oce 0x718424FDE498
                                     frame originated locally (Null0)
                                   L3 mtu 1500
                                   Flags (0x5938C4)
                                   Fixup enabled (0x400000)
```

```
                                         IPSec tunnel
                                   HWIDB/IDB pointers 0x71842EA25C50/0x71842EA30E90
                                   IP redirect enabled
                                   Switching vector: IPv6 midchain adjacency oce
                                Post encap features: IPSEC Post-encap output classification
Protocol Interface                 Address
                                   Next-hop cannot be inferred
                                   IOSXE-RP Inject sbublock:
                                     pak transmitted 14
                                     last inject at 00:00:02 ago
                                   IP Tunnel stack to 209.165.202.158 in Default (0x0)
                                    nh tracking enabled: 209.165.202.158/32
                                    route-via enabled: GigabitEthernet5 (mandatory)
                                    IP adj out of GigabitEthernet5, addr 209.165.202.158
                                   Platform adj-id: 0xF80001D7, 0x0, tun_qos_dpidx:0
                                   Adjacency pointer 0x718424FDD8E8
                                   Next-hop unknown
```

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Transport VPN Using a CLI Template

The following sections describe procedures for configuring IPv6 GRE or IPsec tunnels over IPv4 and IPv6 overlay networks and underlay networks. Each of the tunnel configuration procedures includes as a prerequisite the procedure for configuring a common source interface.

Configure a Common Source Interface Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.

1. Enter interface configuration mode.

   ```
   interface GigabitEthernet1
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Set an IP address for the interface.

   ```
   ip address ip-address
   ```

4. Configure an IPv6 address.

   ```
   ipv6 address ip-address mask
   ```

5. Exit the interface configuration mode.

   ```
   exit
   ```

Here's the complete configuration example for configuring a common source interface.

```
interface GigabitEthernet1
 no shutdown
 ip address 209.165.202.129 255.255.255.0
 ipv6 address 2001:DB8:202::129/64
```

```
exit
interface Loopback0
 no shutdown
 ip address 209.165.201.1 255.255.255.0
 ipv6 address 2001:DB8:201::1/64
exit
```

Configure an IPv6 GRE Tunnel Over an IPv4 Overlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPv6 GRE Tunnel Over an IPv4 Overlay

1. Create an interface tunnel.

   ```
   interface Tunnel64
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ip-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the GRE tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel [route-via] GigabitEthernet-interface mandatory
   ```

7. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

8. Enable tunnel protection.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile64
   ```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over an IPv4 underlay.

```
interface Tunnel64
no shutdown
 vrf forwarding 1
 ipv6 address 2001:DB8:64::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
```

```
 tunnel protection ipsec profile if-ipsec1-ipsec-profile64
exit
```

Configure an IPv6 GRE Tunnel Over an IPv6 Overlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPv6 GRE Tunnel Over an IPv6 Overlay

1. Enter the tunnel interface mode.

   ```
   interface Tunnel66
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ipv6-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the GRE tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Set the encapsulation mode for the tunnel interface.

   ```
   tunnel mode gre ipv6
   ```

7. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet-interface mandatory
   ```

8. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

9. Enable tunnel protection.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile66
   ```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over an IPv6 underlay.

```
interface Tunnel66
 no shutdown
  ipv6 address 2001:DB8:66::1/64
  tunnel source 2001:DB8:15::15
  tunnel destination 2001:DB8:15::16
  tunnel mode gre ipv6
  tunnel route-via GigabitEthernet1 mandatory
  tunnel vrf multiplexing
```

```
tunnel protection ipsec profile if-ipsec1-ipsec-profile66
exit
```

Configure an IPsec IPv6 Tunnel Over an IPv4 Underlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPsec IPv6 Tunnel Over an IPv4 Underlay

1. Enter the tunnel interface mode.

   ```
   interface Tunnel164
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ipv6-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the IPsec tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Set the encapsulation mode for the tunnel interface.

   ```
   tunnel mode ipsec ipv4 v6-overlay
   ```

7. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet-interface mandatory
   ```

8. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

9. Associate the tunnel interface with an IPsec profile.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile164
   ```

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over an IPv4 underlay.

```
interface Tunnel164
no shutdown
 ipv6 address 2001:DB8:164::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel mode ipsec ipv4 v6-overlay
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
```

```
 tunnel protection ipsec profile if-ipsec1-ipsec-profile164
exit
```

Configure an IPsec IPv6 Tunnel Over an IPv6 Underlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPsec IPv6 Tunnel Over an IPv6 Underlay

1. Enter the tunnel interface mode.

   ```
   interface Tunnel166
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ipv6-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the IPsec tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Set the encapsulation mode for the tunnel interface.

   ```
   tunnel mode ipsec ipv6
   ```

7. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet-interface mandatory
   ```

8. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

9. Associate the tunnel interface with an IPsec profile.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile166
   ```

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over an IPv6 underlay.

```
interface Tunnel166
no shutdown
 ipv6 address 2001:DB8:166::1/64
 tunnel source 2001:DB8:15::15
 tunnel destination 2001:DB8:15::16
 tunnel mode ipsec ipv6
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec1-ipsec-profile166
```

```
exit
```

Verify IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in Transport VPN

Verify GRE Tunnel Protection

The following is a sample output from the **show run interface** *type/number* command.

```
Device#show run interface tunnel 64
interface Tunnel64
 no ip address
 ipv6 address 2001:DB8:64::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec-ipsec-profile64
end
```

The following is a sample output from the **show adjacency tunnel64 internal** command for a GRE tunnel.

```
Device#show adjacency tunnel64 internal
Protocol Interface                 Address
IPV6     Tunnel64                  point2point(11)
                                   14 packets, 1368 bytes
                                   epoch 0
                                   sourced in sev-epoch 1
                                   Encap length 24
                                   4500000000000000FF2F8363D1A5CA81
                                   D1A5CA9E000086DD
                                   P2P-ADJ
                                   Next chain element:
                                     IP adj out of GigabitEthernet1, addr 209.165.202.158
747CC8F3DD80
                                     parent oce 0x747CC8F3DE40
                                     frame originated locally (Null0)
                                   Fast adjacency enabled [OK]
                                   L3 mtu 1398
                                   Flags (0x5938CC)
                                   Fixup enabled (0x2)
                                         IP tunnel
                                   HWIDB/IDB pointers 0x747C5C618E90/0x747CC7B88190
                                   IP redirect enabled
Protocol Interface                 Address
                                   Switching vector: IPv6 midchain adjacency oce
                                Post encap features: IPSEC Post-encap output classification

                                   Next-hop cannot be inferred
                                   IOSXE-RP Inject sbublock:
                                     pak transmitted 14
                                     last inject at 00:00:44 ago
                                   IP Tunnel stack to 209.165.202.158 in Default (0x0)
                                    nh tracking enabled: 209.165.202.158/32
                                    route-via enabled: GigabitEthernet1 (mandatory)
                                    IP adj out of GigabitEthernet1, addr 209.165.202.158
                                   Platform adj-id: 0xF8000137, 0x0, tun_qos_dpidx:0
                                   Adjacency pointer 0x747CC8F3E870
                                   Next-hop unknown
```

The following is a sample output from the **show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host** command.

```
Device#show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host

VRF_IDX VRF_NAME Tbl_ID      Host_IP
   Flags   Tun_idx IFNAME         Tx_Pkts   Rx_Pkts
------------------------------------------------------------------------------------------
3       1        503316481   2001::3800:102
   0x1     65519   Tunnel64            29         29
```

Verify IPsec Tunnel

The following is a sample output from the **show run interface** *type/number* command.

```
Device#show run interface tunnel164
interface Tunnel164
 no ip address
 ipv6 address 2001:DB8:164::1/64
 tunnel source 209.165.202.129
 tunnel mode ipsec ipv4 v6-overlay
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec-ipsec-profile164
end
```

The following is a sample output from the **show adjacency tunnel164 internal** command for an IPsec tunnel.

```
Device#show adjacency tunnel164 internal
Protocol Interface                 Address
IPV6     Tunnel164                 point2point(11)
                                   14 packets, 1032 bytes
                                   epoch 0
                                   sourced in sev-epoch 3
                                   empty encap string
                                   P2P-ADJ
                                   Next chain element:
                                     IP adj out of GigabitEthernet1, addr 209.165.202.158
747CC8F3DD80
                                     parent oce 0x747CC8F3DE40
                                     frame originated locally (Null0)
                                   L3 mtu 1422
                                   Flags (0x5938C4)
                                   Fixup enabled (0x400000)
                                         IPSec tunnel
                                   HWIDB/IDB pointers 0x747CC265CEE0/0x747CC923AA98
                                   IP redirect enabled
                                   Switching vector: IPv6 midchain adjacency oce
                                Post encap features: IPSEC Post-encap output classification
Protocol Interface                 Address
                                   Next-hop cannot be inferred
                                   IOSXE-RP Inject sbublock:
                                     pak transmitted 14
                                     last inject at 00:01:32 ago
                                   IP Tunnel stack to 209.165.202.158 in Default (0x0)
                                    nh tracking enabled: 209.165.202.158/32
                                    route-via enabled: GigabitEthernet1 (mandatory)
                                    IP adj out of GigabitEthernet1, addr 209.165.202.158
                                   Platform adj-id: 0xF8000157, 0x0, tun_qos_dpidx:0
```

```
                                    Adjacency pointer 0x747CC91D9208
                                    Next-hop unknown
```

The following is a sample output from the **show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host** command for an IPsec tunnel.

```
Device#show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host

VRF_IDX VRF_NAME Tbl_ID      Host_IP
   Flags    Tun_idx IFNAME         Tx_Pkts   Rx_Pkts
-------------------------------------------------------------------------------------------
3       1        503316481   2001::3800:102
   0x1      65517   Tunnel164            1         1
```

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices Using a Feature Template

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure an IPv6 GRE or IPsec tunnel between Cisco IOS XE Catalyst SD-WAN devices and third-party devices in a service or transport VPN using a feature template.

The following sections describe the process of configuring the IPv6 GRE or IPsec tunnels between Cisco IOS XE Catalyst SD-WAN devices and third-party devices using a feature template.

Cisco VPN Interface GRE

Before you configure the GRE parameters, create the Cisco VPN Interface GRE template. To create the template using Cisco SD-WAN Manager feature templates, see "Navigate to the Template Screen and Name the Template" in Cisco VPN Interface GRE.

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, configure the following parameters:

Table 75: Basic Configuration

Field	Description
Shutdown*	Click **Off** to enable the interface.
Interface Name*	Enter the name of the GRE interface. Range: 1 through 255
Description	Enter a description of the GRE interface.
GRE Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
IPv4 Address	Enter an IPv4 address for the GRE tunnel.

Field	Description
IPv6 Address	Enter an IPv6 address for the GRE tunnel.
Source*	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. This address is on the local router. • **Tunnel Route-via Interface**: Enter the physical interface name to steer the GRE traffic through. • **Interface**: Enter the name of the source interface. • **Tunnel Source Interface**: Enter the physical interface that is the source of the GRE tunnel.
Destination*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. If this tunnel connects to a Secure Internet Gateway (SIG), specify the URL for the SIG.
GRE Destination IP Address*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
IP MTU	Specify the maximum MTU size of the IPv4 packets on the interface. Range: 576 through 1804 Default: 1500 bytes
Clear-ike mode-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IPv6 MTU	Specify the maximum MTU size of the IPv6 packets on the interface. Range: 1280 to 9976 bytes Default: 1500 bytes
IPv6 TCP MSS	Specify the maximum segment size (MSS) of IPv6 TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 40 to 1454 bytes Default: None

Table 76: DPD

Field	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3

Table 77: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Mode	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE Authentication	**Preshared Key**: Enter the preshared key (PSK) for authentication.

Field	Description
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

Table 78: IPsec

Field	Description
IPsec Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

Table 79: ACL

Field	Description
Rewrite Rule	Click **On** and specify the name of the rewrite rule to apply on the interface.

Field	Description
Ingress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.

Table 80: ADVANCED

Field	Description
Tracker	Enter the name of a tracker to track the status of GRE interfaces that connect to the internet.
Application	Specify that this tunnel connects to a SIG.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

Cisco VPN Interface IPsec

Before you configure the IPsec parameters, create the Cisco VPN Interface IPsec template. To create the template using Cisco SD-WAN Manager feature templates, see Create VPN IPsec Interface Template.

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, configure the parameters in the following section.

Table 81: Basic Configuration

Field	Options/Format	Description
Shutdown*	**Yes** / **No**	Click **No** to enable the interface; click **Yes** to disable.
Interface Name*	**ipsec** *number* (1…255)	Enter the name of the IPsec interface. *Number* can be from 1 through 255.
Description	Enter a description of the IPsec interface.	
IPsec Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **4o4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. • **6o4**: IPsec tunnel with IPv6 overlay and IPv4 underlay. • **6o6**: IPsec tunnel with IPv6 overlay and IPv6 underlay.	
IPv4 Address*	*ipv4 prefix/length*	Enter the IPv4 address of the IPsec interface.

Field	Options/Format	Description
Source *	Set the source of the IPsec tunnel that is being used for IKE key exchange:	
	IP Address	Based on the option you chose from the **IPsec Tunnel Mode** option, enter the IPv4 or IPv6 address for the overlay tunnel. Configure this address in **VPN 0**.
	Interface	Click and enter the name of the physical interface that is the source of the IPsec tunnel. Configure this interface in **VPN 0**. • If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name.

Field	Options/Format	Description
Destination*	Set the destination of the IPsec tunnel that is being used for IKE key exchange.	
	IPsec Destination IP Address/FQDN	Enter an IPv4 or IPv6 address that points to the destination.
	TCP MSS	Based on the IPv4 or IPv6 option you chose from the **IPsec Tunnel Mode** option, enter the maximum segment size (MSS) of the TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range for IPv4 TCP MSS: 500 to 1460 bytes Range for IPv6 TCP MSS: 40 to 1454 bytes Default: None
	Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport mode. Default: No
	IP MTU	Based on the option you chose from the **IPsec Tunnel Mode** option, enter the maximum transmission unit (MTU) size of the IPv4 MTU or IPv6 MTU packets on the interface. Range for IPv4 MTU: 68 through 9914 bytes Range for IPv6 MTU: 1280 to 9976 bytes Default: 1500 bytes
	Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Don't Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Don't Fragment bit and the Don't Fragment bit is set. For packets not requiring fragmentation, the Don't Fragment bit is not affected.

Table 82: DPD

Field	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

Table 83: IKE

Field	Description
IKE Version	Enter **1** to choose IKEv1. Enter **2** to choose IKEv2. Default: IKEv1
IKE Mode	For IKEv1 only, specify one of the following modes: • Aggressive mode: Negotiation is quicker, and the initiator and responder ID pass in the clear. • Main mode: Establishes an IKE SA session before starting IPsec negotiations. **Note** For IKEv2, there is no mode. **Note** We do not recommend using IKE aggressive mode with pre-shared keys. If it is necessary to use this mode, use a strong pre-shared key. Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Default: 256-AES

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 1024-bit modulus • 2048-bit modulus • 3072-bit modulus • 4096-bit modulus Default: 4096-bit modulus
IKE Authentication	Enter the password to use with the preshared key.
	If the remote IKE peer requires a local end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's source IP address
	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's destination IP address

Table 84: IPsec

Parameter Name	Options	Description
IPsec Rekey Interval	3600 to 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. From the drop-down list, 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 Default: group-16

Table 85: Advanced

Parameter Name	Description
Tracker	Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet.
Application	Specify that this tunnel connects to a SIG.

Configure IPv6 GRE or IPsec Tunnel Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Service VPN Using Configuration Groups

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure an IPv6 GRE tunnel between Cisco IOS XE Catalyst SD-WAN devices and third-party devices in a service VPN using configuration groups.

Before You Begin

Add the GRE or IPsec subfeature:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group name and choose **Edit**.
3. Click **Service Profile** to open it.
4. Click **…** adjacent to the **VPN** feature and choose **Add Sub-Feature**.
5. From the drop-down list, choose **GRE** or **IPsec**.
6. In the **Name** field, enter a name for the feature.
7. In the **Description** field, enter a description of the feature.

8. Configure the options described in the following section, as needed, and click **Save**.

After adding the subfeature, see the following sections to configure the IPv6 GRE or IPsec parameters for tunnels between Cisco IOS XE Catalyst SD-WAN devices and third-party devices using a feature template.

GRE

To configure the GRE parameters for a service VPN, see the GRE section in Service Profile.

IPsec

To configure the IPsec parameters for a service VPN, see the IPsec section in Service Profile.

Configure IPv6 IPsec Tunnel Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Transport VPN Using Configuration Groups

Before You Begin

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure an IPv6 IPsec tunnel between Cisco IOS XE Catalyst SD-WAN devices and third-party devices in a transport VPN using configuration groups.

Configure IPv6 IPsec Tunnel Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Transport VPN

1. Add the GRE or IPsec subfeature.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
   b. Click **…** adjacent to a configuration group name and choose **Edit**.
   c. Click **Transport & Management Profile** to open it.
   d. Click **…** adjacent to the **VPN0** feature and choose **Add Sub-Feature**.
   e. From the drop-down list, choose **GRE** or **IPsec**.
2. In the **Name** field, enter a name for the feature.
3. In the **Description** field, enter a description of the feature.
4. Configure the GRE or IPsec parameters as follows:
   - GRE: To configure the GRE parameters for a transport VPN, see the GRE section in Transport and Management Profile.
   - IPsec: To configure the IPsec parameters for a transport VPN, see the IPsec section in Transport and Management Profile.
5. Click **Save**.

CHAPTER 16

Security Virtual Image

Cisco SD-WAN Manager uses a Security Virtual Image to enable security features such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), and Advanced Malware Protection (AMP) on Cisco IOS XE Catalyst SD-WAN Devices. These features enable application hosting, real-time traffic analysis, and packet logging on IP networks. Once the image file is uploaded to the Cisco SD-WAN Manager Software Repository, you can create policy, profile, and device templates that will push the policies and updates to the correct devices automatically.

Before you use these features, you must first install and configure IPS/IDS, URL-F, or AMP security policies, and then upload the relevant Security Virtual Image to Cisco SD-WAN Manager. After upgrading the software on the device, you must also upgrade the Security Virtual Image.

This chapter describes how to perform these tasks.

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

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

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

Task 2: Create a Feature Template for Security App Hosting

Task 3: Create a Device Template

Task 4: Attach Devices to the Device Template

Create a Security Policy Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.

2. Click **Add Security Policy**.

3. In the **Add Security Policy** window, select your security scenario from the list of options.

4. Click **Proceed**.

Create a Feature Template for Security App Hosting

The feature profile template configures two functions:

- **NAT:** Enables or disables Network Address Translation (NAT), which protects internal IP addresses when outside the firewall.
- **Resource Profile:** Allocates default or high resources to different subnets or devices.

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

To create a feature profile template, follow these steps:

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

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

3. From the **Select Devices** list, choose the devices that you want to associate with the template.
4. Under **Basic Information**, click **Security App Hosting**.
5. Enter **Template Name** and **Description**.
6. Under **Security Policy Parameters**, customize the security policy parameters if required.
   - Enable or disable the Network Address Translation (NAT) feature, based on your use case. By default, **NAT** is on.
   - Click the drop-down arrow to set boundaries for the policy. The default is **Default**.

     Global: Enables NAT for all devices attached to the template.

     Device Specific: Enables NAT only for specified devices. If you select **Device Specific**, enter the name of a device key.

     Default: Enables the default NAT policy for devices attached to the template.
   - Set **Resource Profile**. This option sets the number of snort instances to be used on a router. The default is **Low** that indicates one snort instance. **Medium** indicates two instances and **High** indicates three instances.
   - Click the drop-down arrow to set boundaries for the resource profile. The default is **Global**.

     Global: Enables the selected resource profile for all devices attached to the template.

     Device Specific: Enables the profile only for specified devices. If you select **Device Specific**, enter the name of a device key.

     Default: Enables the default resource profile for devices attached to the template.
7. Set **Download URL Database on Device** to **Yes** if you want to download the URL-F database on the device. In this case, the device looks up in the local database before trying the cloud lookup.

8. Click **Save**.

Create a Device Template

To activate the policies you want to apply, you can create a device template that will push the policies to the devices that need them. The available options vary with the device type. For example, Cisco SD-WAN Manager devices require a more limited subset of the larger device template. You will see only valid options for that device model.

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

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

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

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

Attach Devices to the Device Template

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

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

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

Identify the Recommended Security Virtual Image Version

At times, you may want to check the recommended Security Virtual Image (SVI) release number for a given device. To check this using Cisco SD-WAN Manager:

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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 SD-WAN Manager

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 Catalyst 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 SD-WAN Manager menu, choose **Maintenance** > **Software Repository**

Step 4 Choose **Virtual Images**.

Step 5 Click **Upload Virtual Image**, and choose either **Manager** or **Remote Server – Manager**. The **Upload Virtual Image to Manager** 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 Catalyst SD-WAN device is upgraded to a new software image, the security virtual image must also be upgraded so that they match. If there is a mismatch in the software images, a VPN template push to the device will fail.

Note During the UTD Virtual image upgrade, the IPS signature file is installed with version 29.0C, which is the default packaging within the UTD tar container. 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 Cisco SD-WAN Manager* to download the recommended version of the SVI for your router. Note the version name.

Step 2 From the Cisco SD-WAN Manager 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 SD-WAN Manager 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 17

IPsec Pairwise Keys

Table 86: Feature History

Feature Name	Release Information	Description
Secure Communication Using Pairwise IPsec Keys	Cisco IOS XE Catalyst 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

The following platforms are supported for IPSec Pairwise Keys feature:

- Cisco IOS XE Catalyst 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 Catalyst SD-WAN Manager

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

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

3. From the **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 Catalyst 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 Catalyst 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    Source Port  SOURCE IP    DEST Port LOCAL TLOC ADDRESS  REMOTE TLOC COLOR
REMOTE TLOC ADDRESS   REMOTE TLOC COLOR      PWK-SPI  INDEX      ID      HASH   HASH   HASH
   HASH  AUTH
-----------------+--+----------------+---+------+------+-----+------+---+--+--+--+--+--+-+--
10.168.11.3   12346    192.168.90.3      12346    10.1.0.2                  lte
  10.1.0.1          private1          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          private1          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

                                          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
----------------+---+----------------+--+------+------+------+------+---+--+--+--+--+--+--+--
192.168.90.3                             12346    10.168.11.3
 12346    10.1.0.2          lte            10.1.0.1          private1          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          private1          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                         sport  dest IP
                               dport  SA ptr      spi/old              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-1ng       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 Catalyst 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 Catalyst 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 18

Configure Single Sign-On

Table 87: Feature History

Feature Name	Release Information	Description
Single Sign-On Using Azure Active Directory (AD)	Cisco vManage Release 20.8.1	This feature adds support for Azure Active Directory (AD) as an external identity provider (IdP) for single sign-on of Cisco SD-WAN Manager users. You can configure Azure AD as an external IdP using Cisco SD-WAN Manager and the Azure AD administration portal.
Configure Multiple IdPs for Single Sign-On Users of Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	With this feature, you can configure up to three IdPs for providing different levels of access for single sign-on users of Cisco SD-WAN Manager.

Information About Single Sign-On

This chapter describes how to configure single sign-on (SSO) for Cisco Catalyst SD-WAN.

Cisco Catalyst SD-WAN is generally compatible with SAML 2.0-compliant identity providers (IdPs), when configured according to industry standards. Cisco has tested and verified the following IdPs:

- Okta
- Active Directory Federation Services (ADFS)
- PingID

- Azure Active Directory (AD)

Note Because Cisco SD-WAN Manager supports the SAML2.0 standard, if you deploy an IdP other than those listed above and it does not work with Cisco SD-WAN Manager as expected, we recommend that you follow up with the IdP provider to troubleshoot the issue.

Note For Cisco vManage Release 20.3.x through Cisco vManage Release 20.11.x, and for Cisco Catalyst SD-WAN Manager Release 20.12.1 and later, use IdP SAML metadata with 2048-bit key signature certificate for SSO authentication because metadata with 1024-bit key signature certificate is not supported.

SSO enables secured access to multiple applications or websites with a single set of credentials. SSO requires the following components:

- Identity provider IdP: This system stores user data, maintains and supports the authentication mechanism, for example, Okta, ADFS, PingID, and Azure AD.
- Service provider: This system hosts the website or application of interest, for example, Cisco SD-WAN Manager.
- Users: People with a registered account with the IdP and the service provider.

To integrate IdPs with service providers, the SSO uses security assertion mark-up language (SAML). SAML is an XML-based communication standard that allows you to share identities among multiple organizations and applications.

The following steps describe the intergration of IdPs with service providers:

1. Whenever a network administrator tries to log in to a service provider using an IdP, the service provider first sends an encrypted message to the IdP.
2. The IdP decrypts the message and validates the credentials of the network administrator by comparing the information with the IdP's database.
3. After the validation, the IdP sends an encrypted message to the service provider. The service provider decrypts the message from the IdP, and the administrator is allowed to access the service provider.
4. In general, IdP and service provider exchange information based on predefined standards. This standard is a set of certificates called SAML.

After completing the above process, the administrator is redirected to the IdP portal. The administrator must enter IdP credentials to log in to Cisco SD-WAN Manager.

Note The privileges for a particular administrator are provided based on the information available about that administrator in the IdP's database.

Benefits of Single Sign-On

With a properly deployed SSO solution, you can do the following:

- Eliminate weak passwords for each cloud application
- Streamline the secured access process
- Provide one-click access to cloud applications

Prerequisites for Single Sign-On

- In Cisco SD-WAN Manager, ensure that the identity provider settings (**Administration Settings** > **Identity Provider Settings**) are set to **Enabled**.

  For more information on enabling identiy provider, see Enable an Identity Provider in Cisco SD-WAN Manager.

- Availability of SAML metadata files for configuring IdP and service provider.
- Cisco SD-WAN Manager requires access to an internet connection that doesn't have a firewall restriction for Cisco SD-WAN Manager to reach the SSO.

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 Beginning with Cisco vManage Release 20.3.1, Cisco SD-WAN Manager no longer supports MD5 or SHA-1. All x.509 certificates handled by Cisco SD-WAN Manager need to use at least SHA-256 or a higher encryption algorithm.

Perform the following procedures to configure SSO.

Enable an Identity Provider in Cisco SD-WAN Manager

To configure Okta SSO, use Cisco SD-WAN Manager to enable an identity provider and generate a Security Assertion Markup Language (SAML) metadata file.

From Cisco vManage Release 20.10.1, you can use **Add New IDP Settings** to configure up to three IdPs. For more information on integrating with multiple IdPs, see the chapter Configure Multiple IdPs.

1. From the Cisco SD-WAN Manager menu, choose **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 SD-WAN Manager:

   - **Entity ID**
   - **Signing certificate**
   - **Encryption certificate**
   - **Logout URL**
   - **Login URL**

Note Administrators can set up SSO using a single **Entity ID** only. Cisco SD-WAN Manager doesn't support more than one **Entity ID** while setting up SSO.

6. In the **Upload Identity Provider Metadata** section, click **Select a File** to upload the IdP metadata file.

7. Click **Save**.

Configure SSO on the Okta Website

Note This procedure involves a third-party website. The details are subject to change.

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 SD-WAN Manager as an SSO application, from the Cisco SD-WAN Manager 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 SD-WAN Manager.

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 SD-WAN Manager 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 88: 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	**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.

Component	Value	Configuration
Single Logout URL		Get from the metadata.
Service provider Issuer		Use the entityID from the metadata.
Signature Certificate		**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
Honor Force Authentication	Yes	Not applicable
SAML issuer ID string	SAML issuer ID string	Not applicable
Attribute Statements	Field: **Name**	Value: *Username*
	Field: **Name format (optional)**	Value: Unspecified
	Field: **Value**	Value: *user.login*
Group Attribute Statements	Field: **Name**	Value: Groups
	Field: **Name format (optional)**	Value: Unspecified
	Field: **Matches regex**	Value: **.***

Note It is mandatory to use the two strings, Username and Groups, exactly as shown above. Otherwise, you may be logged in with the default group of Basic.

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 SD-WAN Manager, 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

Note This procedure involves a third-party website. The details are subject to change.

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)

This section describes how to use Cisco SD-WAN Manager and ADFS to configure SSO.

The configuration of Cisco SD-WAN Manager to use ADFS as an IdP involves two steps:

- Step 1 - Import ADFS metadata to Cisco SD-WAN Manager.
- Step 2- Export Cisco SD-WAN Manager metadata to ADFS.

Step 2 can be further divided into:

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

Note There is no support for customized certificates for Cisco SD-WAN Manager SSO. If ADFS is configured, the signature and signing certificates are generated from the Cisco SD-WAN Manager metadata.

For more information on configuring ADFS, see Enable an Identity Provider in Cisco SD-WAN Manager. The steps are the same as for configuring Okta as an IdP.

Import Metadata File into ADFS

Note This procedure involves a third-party website. The details are subject to change.

Step 1 - Import ADFS Metadata to Cisco SD-WAN Manager:

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 SD-WAN Manager menu, choose **Administration** > **Settings** > **Identity Provider Settings** > **Enable**, and then upload **adfs_metadata.txt** to Cisco SD-WAN Manager.

   Step 2 - Export Cisco SD-WAN Manager Metadata to ADFS:

4. With **Identity Provider Settings** enabled, **Click here to download SAML metadata** and save the contents to a file, which is typically `192.168.1.15_saml_metadata.xml`.

5. After the SAML metadata is downloaded, verify that the signing certificate and the signature certificate are the same.

   a. If the signing certificate and the signature certificate are the same, proceed to Step 6 to edit the Cisco SD-WAN Manager metadata file.

   b. If the signing certificate and the signature certificate are not the same, use the signature certificate for the remaining steps, not the signing certificate.

6. Edit the Cisco SD-WAN Manager metadata file by deleting everything from **<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"**> to **</ds:Signature**>.

7. Edit the Cisco SD-WAN Manager metadata file by deleting everything from **<md:KeyDescriptor use="encryption"**> to **</md:KeyDescriptor**>.

8. Import the new modified Cisco SD-WAN Manager metadata file into ADFS, and enter the **entityID** as **Display Name**.

9. Click **Next** until the end.

10. 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-", ""));
```

11. Verify the final result.

12. 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 SD-WAN Manager.

Add ADFS Relying Party Trust

Before you begin

To add an ADFS relying party trust using Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Identity Provider Settings** > **Enable**.
2. Download the ADFS Metadata file, and upload it into Cisco SD-WAN Manager. 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 the contents to 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 the **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

Note This procedure involves a third-party website. The details are subject to change.

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 Webs So protocol**.
10. Open a text editor, and open the **10.10.10.15_saml_metadata.xml** file.
11. Copy the vale 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 the **entityID** attribute, and paste it into the **Relying party trust identifiers** text box.
14. Click **Add**, and click **Next**.
15. Click **Next** to skip to the **Configure Multi-factor Authentication Now** section.
16. Choose **Permit all users to access this relying party**, and click **Next**.
17. Click **Next** to skip to the **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 the **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 a 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 SD-WAN Manager.

Configure SSO for PingID

Cisco SD-WAN Manager supports PingID as an IdP. PingID is an identity management service for authenticating user identities with applications for SSO.

The configuration of Cisco SD-WAN Manager to use PingID as an IdP involves the following steps:

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

Prerequisites:

1. In Cisco SD-WAN Manager, ensure that identity provider settings (**Administration Settings** > **Identity Provider Settings**) are set to **Enabled**.
2. Download the Cisco SD-WAN Manager SAML metadata file to export to PingID.

   For more information on these procedures, see Enable an Identity Provider in Cisco SD-WAN Manager. 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

Note This procedure involves a third-party website. The details are subject to change.

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 SD-WAN Manager to complete the SSO configuration.
      1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
      2. Click **Identity Provider Settings** > **Upload Identity Provider Metadata** to import the saved PingOne IdP metadata file into Cisco SD-WAN Manager.
      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 SD-WAN Manager 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)	<Cisco SD-WAN Manager_URL>/samlLoginResponse
Entity ID	IP address of Cisco SD-WAN Manager
Single Logout Endpoint	<Cisco SD-WAN Manager_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	False

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 SD-WAN Manager Cluster

1. Create three Cisco SD-WAN Manager single-tenant instances and associated configuration templates. See Deploy Cisco SD-WAN Manager.
2. Create a Cisco SD-WAN Manager cluster consisting of three Cisco SD-WAN Manager instances. See the Cluster Management chapter in the *Cisco Catalyst SD-WAN Getting Started Guide*.
3. Download SAML metadata based on the IDP from the first Cisco SD-WAN Manager 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 SD-WAN Manager.
6. In the first instance of Cisco SD-WAN Manager, 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 SD-WAN Manager cluster now, the first instance of Cisco SD-WAN Manager redirects SSO using an IDP. The second and third instances of the cluster also redirect SSO using IDP.

If the first instance of Cisco SD-WAN Manager 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 SD-WAN Manager cluster. The only option available for accessing the second and third instances of the Cisco SD-WAN Manager cluster is by using the local device authentication, which is "/login.html".

Note If you log in by using the local device authentication, the **SAML Login** page appears when you log out.

Note When the token is expired for IDP login, refresh the browser or open the SSO in the new tab.

Configure Single Sign-On Using Azure AD

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

The configuration of Cisco SD-WAN Manager to use Azure AD as an IdP involves the following steps:

1. Export Cisco SD-WAN Manager metadata to Azure AD. For details, see Export Cisco SD-WAN Manager Metadata to Azure AD.
2. Configure SSO using Azure AD and import Azure AD metadata to Cisco SD-WAN Manager. For details, see Configure Single Sign-On Using Azure AD and Import Azure AD Metadata to Cisco SD-WAN Manager.

Export Cisco SD-WAN Manager Metadata to Azure AD

1. From the Cisco SD-WAN Manager menu, choose **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.

Configure Single Sign-On Using Azure AD and Import Azure AD Metadata to Cisco SD-WAN Manager

Note This procedure involves a third-party website. The details are subject to change.

1. Log in to the Azure AD portal.
2. Create an enterprise application in Azure services.

   An enterprise application integrates Azure AD with Cisco SD-WAN Manager. To create a new application, you must use the **Non-gallery application**.
3. Upload the SAML metadata file that you downloaded from Cisco SD-WAN Manager.
4. In the Azure AD portal, in the section for configuring attributes and claims, configure the following:
   a. Create a new claim for the emailaddress attribute, configuring the field values as follows:

Field	Value to enter
Name	emailaddress
Namespace	(Leave this undefined, which is the default.)
Name format	(Leave this undefined, which is the default.)
Source	Attribute
Source attribute	user.mail

   b. Create a new claim for the groups attribute, configuring the field values as follows:

Field	Value to enter
Name	Groups
Namespace	(Leave this undefined, which is the default.)
Name format	(Leave this undefined, which is the default.)
Source	Attribute
Source attribute	netadmin

c. Create a new claim for the username attribute, configuring the field values as follows:

Field	Value to enter
Name	Username
Namespace	(Leave this undefined, which is the default.)
Name format	(Leave this undefined, which is the default.)
Source	Attribute
Source attribute	user.userprincipalname

d. Modify the existing “Unique User Identifier (Name ID)” claim, as follows:

Field	Value to enter
Name identifier format	Email address
Source	Attribute
Source attribute	user.userprincipalname

5. Download the federation metadata XML (Azure AD metadata) file.
6. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
7. Choose **Identity Provider Settings** > **Upload Identity Provider Metadata** to import the saved Azure AD metadata file into Cisco SD-WAN Manager.
8. Click **Save**.

Verify Single Sign-On Using Azure AD

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

1. Log in to the Azure AD portal.
2. View the log of the authorized SSO logins.

Integrate with Multiple IdPs

The following sections provide information about integrating with multiple IdPs.

Information About Integrating with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

With this feature, you can now configure more than one IdP per tenant in Cisco SD-WAN Manager. This feature supports both single-tenant and multitenant environments.

You can configure up to three IdPs per tenant and a maximum of three IdPs per the provider.

The following fields are added in Cisco SD-WAN Manager **Administration** > **Settings** > **Identity Provider Settings** for configuring multiple IdPs:

- **Add New IDP Settings**
- **IDP Name**
- **Domain**

You can also edit or delete an IdP name and domain name.

For more information on configuring multiple IdPs, see Configure Multiple IdPs.

Benefits of Integrating with Multiple IdPs

- Enables end users to allocate different user access for different functions in the organization
- Provides high level of security and meets compliance requirements
- Reduces operational costs

Restrictions for Integrating with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

- You can configure only three IdPs in a single-tenant deployment and three IdPs per tenant in a multitenancy deployment.

Use Cases for Integrating with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

The following are potential use cases for integrating with multiple IdPs:

- An end user (tenant) requires different types of user access for employees versus contractors.
- An end user requires different types of user access for different functions within the organization.
- An end user requires access to the same IdP, but has a different email address.

Configure Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

The following workflow is for configuring multiple IdPs. For more information on enabling an IdP, see Enable an Identity Provider in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings** and choose **Edit**.
3. Click **Add New IDP Settings**.

Note: After three IdPs are configured, the **Add New IDP Settings** option is no longer displayed.

4. Click the toggle button to switch between enabling and disabling IdP settings while retaining the existing configuration.

5. Click **IDP Name** and enter a unique name for your IdP.

   Examples:

   - **okta**
   - **idp1**
   - **provider**
   - **msp**

   You can configure a maximum of three IdPs.

Note: You cannot map the same domain to multiple IdPs, but you can use the same IdP for multiple domains.

6. Click **Domain** and enter a unique domain name for your IdP, for example, okta.com.

   If the domain name already exists, Cisco SD-WAN Manager generates an error message.

   Alternatively, you can enter a wildcard (*) in the domain name field making it the default domain. If a default domain is configured, you can log in to a domain with your user ID without requiring you to enter an user ID in the email address format (xyz@mystore.com).

Note: Only one of the IDPs can be configured as a default IDP.

7. In the **Upload Identity Provider Metadata** section, upload the SAML metadata file you downloaded from your IdP.

8. Click **Save**.

9. After you configure a new IdP name, domain, and sign out of your current Cisco SD-WAN Manager session, you are redirected to a unified SAML login page.

10. In the unified SAML login page, if you require local authentication, remove the **login.html** portion of the URL. This redirects you to the local authentication page.

11. In the unified SAML login page, enter the SSO credentials for your IdP.

Note: You are redirected to the unified SAML login page each time you access Cisco SD-WAN Manager after configuring a new IdP name and domain.

Verify Integration with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings** and then click **View**.
3. Verify the configured IdP and the corresponding domain.

Troubleshooting Integration with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

For troubleshooting integration issues with multiple IdPs, you can access the log files at:

- `/var/log/nms/vmanage-server.log` is the log file for enabling and disabling IdP.
- `/var/log/nms/vmanage-sso.log` is the SSO-specific log file.

CHAPTER 19

Configure Port Security

Table 89: Feature History Table

Feature Name	Release Information	Description
Port Security Support for Switchports on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	The feature allows you to configure switchports on Edge platforms with switching modules to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port.

Supported Devices for Port Security

Cisco ISR4000 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules:

- ISR4461
- ISR4451
- ISR4351
- ISR4331

Cisco C8300 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules:

- C8300-1N1S-6T
- C8300-1N1S-4T2X
- C8300-2N2S-6T
- C8300-2N2S-4T2X

Information About Port Security

You can use the port security feature to configure switch ports on routing platforms, to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

The secure addresses are included in an address table in one of these ways:

- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- You can configure several addresses and allow the rest to be dynamically configured.

Note If the port shuts down, all dynamically learned addresses are removed.

- You can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

Enable *sticky learning* to configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration. To enable sticky learning, enter the **switchport port-security mac-address sticky** command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the configuration, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

Restrictions for Port Security

- Secure port and static MAC address configuration are mutually exclusive.

Note **switchport port-security** and **switchport port-security mac-address sticky** configuration commands are validated. There are other port-security commands available, but we recommend not to use them for Cisco SD-WAN Release 20.3.1.

Configure Port Security Using the CLI

Configure Port Security on an Interface

To restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port, perform this task:

1. Enters physical interface mode for configurations, for example **`gigabitethernet 1/0/1`**.

   ```
   Device(config)# interface interface_id
   ```

2. Enables port security on the interface.

   ```
   Device(config-if)# switchport port-security
   ```

3. (Optional) Enable sticky learning on the interface.

   ```
   Device(config-if)# switchport port-security mac-address sticky
   ```

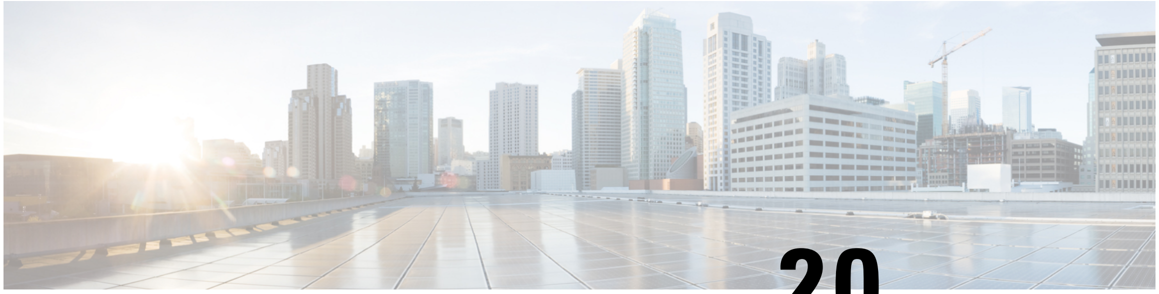
4. Returns to privileged EXEC mode.

   ```
   Device(config-if)# end
   ```

Configuration Example

The following example shows how to configure a secure MAC address on GigabitEthernet 1/0/1:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# end
```



CHAPTER 20

Cisco TrustSec Integration

Table 90: Feature History

Feature Name	Release Information	Description
Support for SGT Propagation with Cisco TrustSec Integration	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables Cisco IOS XE Catalyst 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 Catalyst SD-WAN network. While Cisco TrustSec-enabled switches do classification, propagation (inline SGT tagging) and enforcement on the branches, Cisco IOS XE Catalyst SD-WAN device devices carry the inline tags across the edge devices.
Enhanced SGACL Logging	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This feature enhances SGACL logging capability on Cisco IOS XE Catalyst SD-WAN devices by utilizing High Speed Logging (HSL). HSL offers a more efficient and scalable method for logging security events, ideal for high-traffic network environments.

This chapter contains the following sections:

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 Catalyst SD-WAN devices support propagation of SGT. See Configure SGT Inline Tagging Using Cisco SD-WAN Manager, on page 383

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 Catalyst SD-WAN devices. You can also manually configure IP address to SGT binding, statically, in Cisco SD-WAN Manager. See SGT Propagation Using SXP, on page 388

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 403

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 Catalyst SD-WAN, on page 380

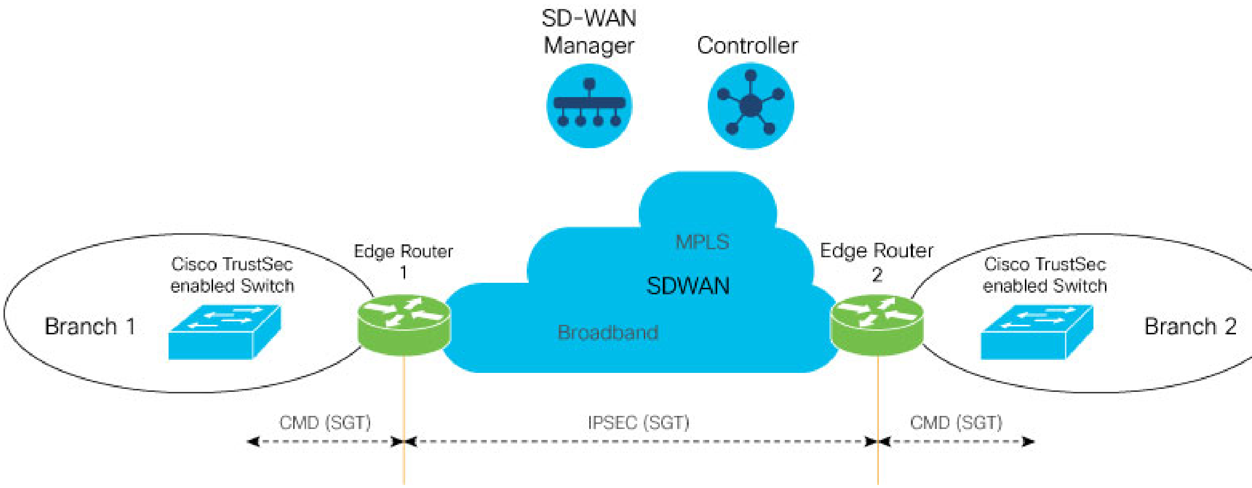
Prerequisites

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

SGT Propagation in Cisco Catalyst SD-WAN

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

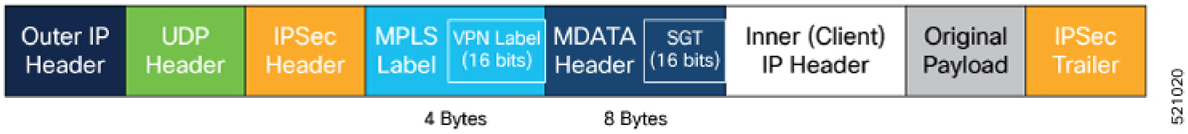
Figure 10: SGT Propagation in Cisco Catalyst SD-WAN



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 Catalyst 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 Catalyst SD-WAN IPSec or GRE tunnels. The Edge Router 2 on Cisco Catalyst SD-WAN extracts the SGT from Cisco Catalyst 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 Cisco Catalyst SD-WAN packet and an additional eight bytes of data is added to it.

Figure 11: SGT Propagation



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

Table 91: SGT Propagation with Cisco IOS XE Catalyst SD-WAN Devices of Different Releases Interconnected in Cisco Catalyst SD-WAN

Cisco IOS XE Catalyst SD-WAN Device at Source	Cisco Catalyst SD-WAN Device at Destination	Result
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Cisco IOS XE Catalyst SD-WAN device with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a or later	• Traffic with SGT is forwarded to the Cisco IOS XE Catalyst SD-WAN device. • If Cisco TrustSec is enabled on the Cisco IOS XE Catalyst 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 Catalyst SD-WAN device, traffic without the SGT and CMD header is forwarded to the switch.
	Cisco IOS XE Catalyst SD-WAN device with Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x and earlier.	Traffic without SGT is forwarded to the Cisco IOS XE Catalyst 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:

- 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

The following WAN NIMs are supported on Cisco Catalyst 8200 Router and Cisco Catalyst 8300 Router platforms:

- C-NIM-2T
- C-NIM-1M
- C-NIM-1X

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 Catalyst SD-WAN device before configuring it on the switch.
- You cannot enable Cisco TrustSec by using the **cts manual** command on port-channel sub-interfaces.
- If you are configuring subinterfaces on a Cisco IOS XE Catalyst SD-WAN device, Cisco TrustSec must be enabled on the physical interface and on all the subinterfaces.
- Ony devices on Cisco IOS XE Catalyst SD-WAN Release 17.3.1a support propagation of SGT.
- Inline tagging is supported only on the L3 (WAN) ports of the Cisco IOS XE Catalyst SD-WAN devices, and not on switch ports.
- For releases prior to Cisco IOS XE Release 17.3.3, Cisco Catalyst SD-WAN multicast overlay traffic is not supported on interfaces enabled with the Cisco TrustSec feature.

Configure SGT Inline Tagging Using Cisco SD-WAN Manager

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

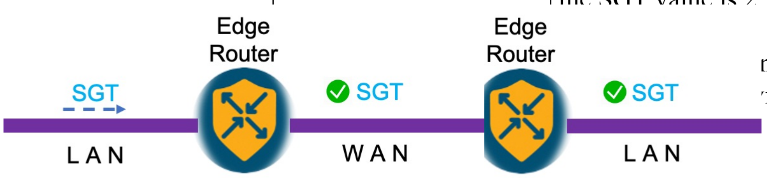
Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

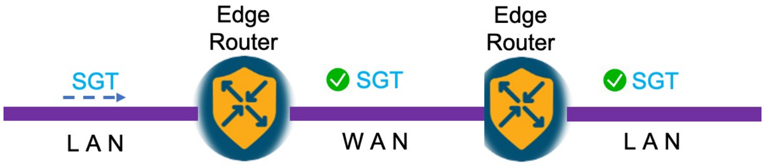
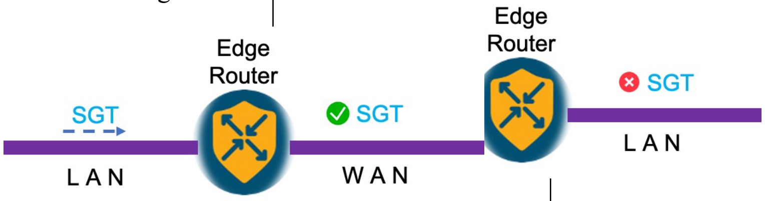
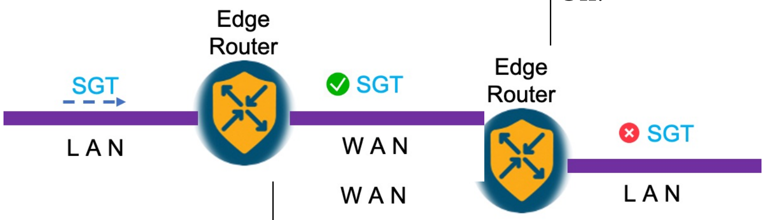
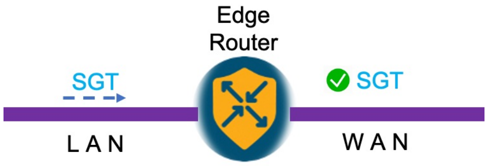
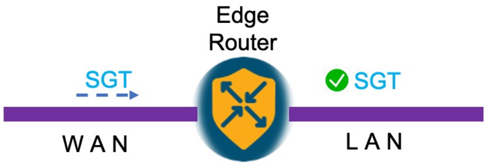
3. Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
4. Choose one of the available Cisco VPN Interface templates, for example, **Cisco VPN Interface Ethernet** .
5. Enter a name and a description for the feature template.
6. To enable SGT propagation, use the following options:
   - For Transport interface (VPN 0):
     a. Click **Tunnel**.
     b. In the **CTS SGT Propagation** field, click **On** to enable SGT propagation for inline tagging. By default, this option is disabled.
   - For service-side interface (VPN x):
     a. Click **TrustSec**.
     b. From the **Enable SGT Propagation** drop-down list, choose **Global**, and then click **On**. Additional propagation options are displayed.
     c. To propagate SGT in Cisco Catalyst 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 92: 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 is 2 n ices



SGT Propagation Options	LAN to WAN	WAN to LAN	Notes
Propagate = On **Security Group Tag** = <SGT Value> **Trusted** = Off	SGT is propagated from LAN to WAN with a configured SGT value.  Edge Router SGT LAN ✓ SGT WAN Edge Router ✓ SGT LAN	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.  Edge Router SGT LAN ✓ SGT WAN Edge Router ✗ SGT LAN	SGT is not propagated from WAN to LAN.	
Propagate = Off **Security Group Tag** = <SGT Value> **Trusted** = Off	SGT is propagated from LAN to WAN with a configured SGT value.  Edge Router SGT LAN ✓ SGT WAN Edge Router WAN ✗ SGT LAN	SGT is not added to the LAN packets. SGT is not propagated to	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

- Enterprise Network Compute System (ENCS) LAN and WAN ports allow propagation of SGT tags on its physical ports. The LAN interfaces must be connected to the LAN side and the WAN interfaces must be connected to the WAN side of the network. You must deploy Cisco Catalyst 8000V router or Integrated Services Virtual router to process the tagging.

7. Click **Save**.

8. Configure the routing protocols using the Cisco SD-WAN Manager templates. You can choose to use any of the routing protocols. For BGP template, see Configure BGP Using Cisco SD-WAN Manager templates.

9. 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 Catalyst SD-WAN device . In this example:

- A network connection is established between a switch in the branch and a Cisco IOS XE Catalyst SD-WAN device.
- Two VRF instances, and subinterfaces are configured on the Cisco IOS XE Catalyst 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 SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager 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 93: Feature History

Feature Name	Release Information	Description
SGT Propagation Using SXP and SGACL Enforcement	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	With this feature, Cisco IOS XE Catalyst 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 Catalyst 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 Catalyst SD-WAN device for propagation of the SGT over the Cisco Catalyst SD-WAN network. See Configure SXP for Dynamic IP-SGT Binding Using Cisco SD-WAN Manager, on page 390.

Alternatively, you have the option to manually configure IP-SGT binding (Static IP-SGT) and then push the configuration to a Cisco IOS XE Catalyst SD-WAN device using a CLI Add-On template to propagate SGT over the Cisco Catalyst SD-WAN network. See Configure Static IP-SGT Binding Using Cisco SD-WAN Manager, on page 393.

Prerequisites

- You must enable Cisco TrustSec and propagation through SXP on the devices in a Cisco Catalyst 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 Cisco SD-WAN Manager.
- From Cisco IOS XE Catalyst SD-WAN 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 Catalyst 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 Catalyst SD-WAN device. Overlapping or remote entries coming though SXP can have an adverse effect on the Overlay routing. See SXP Reflectors, on page 390

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 SD-WAN Manager.
- SGACL policies cannot be enforced on the ingress traffic, only on egress traffic in a Cisco Catalyst 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.
- Cisco TrustSec feature is not supported for more than 24K SGT Policies in controller mode.

Supported Platforms and NIMs

Supported Platforms

The following devices support propagation of SGT using SXP:

- 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 Catalyst SD-WAN, on page 380.

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 Catalyst 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 Catalyst 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 Catalyst 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 396.

We recommend an SXP reflector to establish SXP peering with Cisco IOS XE Catalyst 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 Catalyst 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 SD-WAN Manager

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

To configure an SXP connection in Cisco SD-WAN Manager:

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

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

3. 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 SD-WAN Manager, 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.

Parameter Name	Description
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.
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^EOAeQWVZ]VFQ_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 SD-WAN Manager

To configure static IP-SGT, use the CLI add-on template in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates** and then click **Add Template**.

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

3. 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 Catalyst SD-WAN device for propagation of the SGT over a Cisco Catalyst 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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

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

3. 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.
Send ID	Specify the send identifier for the key. Range: 0 to 255.

Parameter Name	Description
Receiver ID	Specify the receive identifier for the key. Range: 0 to 255.
Include TCP Options	This field indicates whether TCP options other than TCP-AO must be used to calculate Message Authentication Codes (MACs). 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. When options are included, the content of all options is included in the MAC with TCP-AO's **MAC field** is filled with zeroed. When the options are not included, all options other than TCP-AO are excluded from all MAC calculations.
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	Specify the algorithm to be used to compute MACs for TCP segments. You can choosese one of these: • **aes-128-cmac** • **hmac-sha-1** • **hmac-sha-256**
Key String	Specify the master key for deriving the traffic keys. 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.
Send Lifetime Local	Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be used in TCP-AO authentication is valid. 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).
Accept Lifetime Local	Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be accepted for TCP-AO authentication is valid. 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).

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(onfig-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 Catalyst SD-WAN device using a RADIUS server. The downloaded SGACL policies override any conflicting locally defined policies. See Download SGACL Policies to Cisco IOS XE Catalyst SD-WAN devices, on page 396.

Alternatively, you have the option of configuring SGACL policies on Cisco SD-WAN Manager. The policies can be pushed to the Cisco IOS XE Catalyst SD-WAN device using the CLI Add-On template. See Configure Static SGACL Policies in Cisco SD-WAN Manager, on page 399.

Download SGACL Policies to Cisco IOS XE Catalyst SD-WAN devices

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

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

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

3. 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 followin 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 Catalyst 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 Catalyst SD-WAN device when SGACL policies are modified on ISE and a CoA is pushed to the Cisco IOS XE Catalyst 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. *Range:* 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 ebKQPObGXfAKgRHQhbWe_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 SD-WAN Manager

To configure static SGACL policies, use the CLI Add-On template in Cisco SD-WAN Manager.

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

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

3. 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 | from |
[source-sgt] | to | [dest-sgt]]}
[no] cts role-based permissions {[ default | from | [source-sgt] | to | [dest-sgt]]}
```

8. Click **Save**.

   This configuration can now be pushed to the Cisco IOS XE Catalyst SD-WAN device for enforcement of SGACL policies.

Enhanced SGACL Logging

Information About Enhanced SGACL Logging

SGACL logging records actions that are taken by SGACLs to enforce security rules. It captures details about network traffic events, including whether traffic was allowed or blocked based on SGACL policies.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, SGACL logging on Cisco IOS XE Catalyst SD-WAN devices utilizes HSL. The enhanced SGACL logging using HSL offers a more efficient and scalable method for logging security events, which is beneficial in high-traffic network environments.

When SGACLs enforce security rules and generate log entries, these entries are stored as Cisco SYSLOG messages on the Cisco IOS XE Catalyst SD-WAN device. You can view these log messages by using the **show logging** command on the Cisco IOS XE Catalyst SD-WAN device.

Configure Enhanced SGACL Logging Using CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure enhanced SGACL logging.

1. Configure role-based access control with Cisco TrustSec by mapping IP addresses to SGTs, enabling enforcement, and defining SGACL permissions.

```
cts role-based sgt-map vrf vrf-value ip-address sgt SGT-value
cts role-based enforcement
cts role-based permissions from source-sgt to dest-sgt role-based-acl-name
```

2. Configure permissions for IPv4 traffic, and enable logging for TCP traffic.

```
ip access-list role-based role-based-access-list-name
 sequence-number permit tcp log-input
 sequence-number permit icmp
 sequence-number permit ip
```

3. Configure permissions for IPv6 traffic, and enable logging for UDP traffic.

```
ipv6 access-list role-based role-based-acl-name
 sequence sequence-number permit icmp
 sequence sequence-number permit udp log
 sequence sequence-number permit tcp
 sequence sequence-number permit ipv6
```

Note The log message that is produced is identical whether the **log** or the **log-input** command is used.

Here's the complete configuration example for SGACL logging for IPv4 traffic. In this example, the role-based access list named 'PERMIT' allows TCP traffic with logging enabled, while permitting ICMP and IP traffic without logging.

```
cts role-based sgt-map vrf 1 10.2.2.2 sgt 600
cts role-based enforcement
cts role-based permissions from 500 to 600 PERMIT
ip access-list role-based PERMIT
 20 permit tcp log-input
 30 permit icmp
 40 permit ip
```

Here's the complete configuration example for SGACL logging for IPv6 traffic. In this example, the role-based access list named 'PERMIT_IPv6' allows UDP traffic with logging enabled, while permitting ICMP, TCP and IPv6 traffic without logging.

```
cts role-based sgt-map vrf 1 10.2.2.2 sgt 600
cts role-based enforcement
cts role-based permissions from 500 to 600 ipv6 PERMIT_IPv6

ipv6 access-list role-based PERMIT_IPv6
 sequence 20 permit icmp
 sequence 30 permit udp log
 sequence 40 permit tcp
 sequence 50 permit ipv6
```

Note The Enhanced SGACL Logging feature can log a maximum of 512 unique traffic flows across all protocols, such as TCP, UDP, and ICMP. Flows exceeding this limit are not logged.

Verify Enhanced SGACL Logging

The following is a sample output from the **show platform hardware qfp active feature acl dp hsl configuration** command. This output displays the configuration for SGACL with HSL as set up on the device.

```
Device# show platform hardware qfp active feature acl dp hsl configuration
ACL DP HSL Config:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE

SGACL HSL Setup:
Handle Session/Instance: 127/63
Version: 9
Dest Type: 3
HSL Enable: TRUE
HSL BackPressure Enable: FALSE
Base Memory Addr: <0xpXXXX>
Memory Size (bytes): 147560
Max Records: 1024
Record Threshold: 256
Memory Threshold (bytes): 32768
Record Timeout (ms): 512
Export Timeout (ms): 4
MTU Size (bytes): 1450
Template Refresh Timer: 0
Template Refresh Packets: 0
Source Id: 0x404”
Max Record Size (bytes): 104
```

The following is a sample output from the **show platform hardware qfp active feature acl control** command. This output displays whether SGACL logging is enabled or disabled. In this example, SGACL logging is enabled.

```
Device# show platform hardware qfp active feature acl control
Stats Poll Period: 0
Stats Entry Size: 16
Ha Init: 1
Fm Ready: 0
IPv4 Logging Threshold: 2147483647
IPv4 Logging Interval: 0
IPv6 Logging Threshold: 350000
IPv6 Logging Interval: 0
Maximum Aces Per Acl: 256000
Stats Update size: 180
Maximum Entries: 0
Maximum Entries per Classifier: 0
Result Bit Size: 0
Result Start Bit Pos: 0
Maximum Profiles: 0
Maximum Blocks per Profile: 0
Device Select: 0
Maximum Tree Depth: 0
Dimention: 0
Number Cuts: 0
HSL Support: TRUE // sgacl hsl logging is enabled
HSL Force Disable: FALSE
```

The following is a sample output from the **show platform hardware qfp active feature acl dp hsl statistics** command. In this example, the output displays the logging statistics for SGACL HSL from the device.

```
Device# show platform hardware qfp active feature acl dp hsl statistics
Router#show platform hardware qfp active feature acl dp hsl statistic
ACL DP HSL Statistics:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE

SGACL Export Statistics
-----------------------
Records sent (to HSL): 2
Records dropped (before HSL): 0
Record alloc failures: 0
Records dropped flag: Off
Records sent (by HSL): 0
Records dropped (by HSL): 0
HSL packets dropped flag: Off
HSL buffer flow-on (count): 0

SGACL HSL Statistics
--------------------
Records exported: 2
Packets exported: 2
Bytes exported: 168
Dropped records: 0
Dropped packets (inc. Punt drops): 0
Dropped bytes: 0
```

Configuration Example for Enhanced SGACL Logging

This example illustrates how role-based access control and SGACL logging are configured on a Cisco IOS XE Catalyst SD-WAN device.

```
aaa authorization network cts-mlist group radius-1
cts authorization list cts-mlist
cts credentials id admin password 6 LFAZFNeZSWRhSFQX[[_abNQU[_EGLdcdd
cts sxp default source-ip 10.20.25.16
cts sxp node-id interface GigabitEthernet5
!
interface Tunnel1
 ip unnumbered GigabitEthernet1
ipv6 unnumbered GigabitEthernet1
 cts manual
 tunnel source GigabitEthernet1
 tunnel mode sdwan
!
cts role-based sgt-map vrf 1 10.2.2.2 sgt 600
cts role-based enforcement
cts role-based permissions from 500 to 600 PERMIT
!
ip access-list role-based PERMIT
 10 permit ip log
 20 permit tcp log-input
 30 permit icmp


ipv6 access-list role-based PERMIT_IPv6
 sequence 20 permit icmp
 sequence 30 permit udp log
 sequence 40 permit tcp
 sequence 50 permit ipv6

.
```

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 SD-WAN Manager, on page 390.

Configure SGT Enforcement at the Interface Level in Cisco SD-WAN Manager

To enforce SGT using SGACL policies at the interface level in Cisco SD-WAN Manager:

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

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

3. 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 Cisco SD-WAN Manager, 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 SD-WAN Manager, or the WAN edge device CLI.

Using Cisco SD-WAN Manager

To monitor SXP SGT information in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager 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**

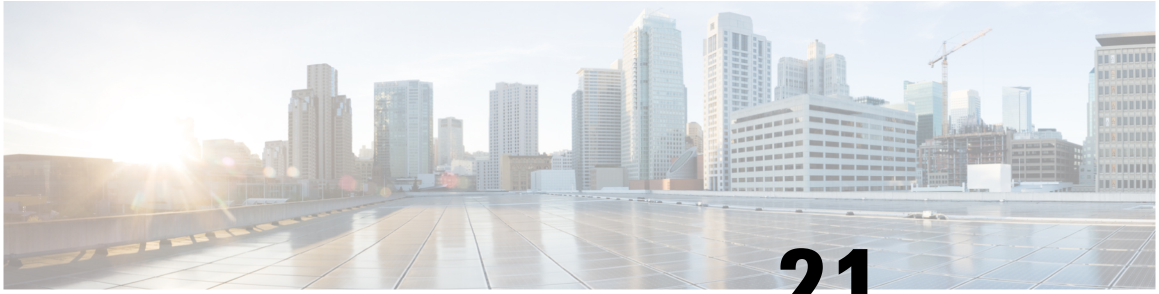
Note You can re-arrange the columns to view SXP and SGT information as per your preference by dragging the column title to the desired position. If you re-arrange the columns, we recommended the Source SGT and Destination SGT columns are set to your left hand side so that you can understand the bindings of a traffic flow.

Using CLI

Use the following commands to monitor SXP/SGT information using the CLI.

Table 94: 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.



CHAPTER 21

OMP Prefixes for IP-SGT Binding

Table 95: Feature History

Feature Name	Release Information	Description
OMP Prefixes for IP-SGT Binding	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	The OMP routes are typically present in the IOS RIB. The OMP routes aren't present in the IOS FIB containing entries that map destination IP addresses to next-hop IP addresses. The IOS FIB operates independently of the control plane, receiving the forwarding instructions from a centralized Cisco SD-WAN Controller instead of consuming the OMP routes from the IOS RIB. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the OMP prefixes get added to the IOS FIB which improves IP-SGT binding.

Information About OMP Prefixes for IP-SGT Binding

The Overlay Management Protocol (OMP) routes refer to the routes learned and exchanged by OMP in a network overlay architecture. OMP is a routing protocol used in Cisco Catalyst SD-WAN environments that dynamically establishes and manages overlay networks. The Overlay networks are virtual networks created on top of an existing physical network infrastructure.

OMP is a proprietary protocol running on Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Controllers and shares routing information such as the virtual network addresses, next-hop information, and any policy or quality-of-service requirements to Cisco IOS XE Catalyst SD-WAN devices from Cisco SD-WAN Controllers.

IOS Forwarding Information Base (FIB) is a data structure used by Cisco IOS to store information about how to forward packets in a network. The FIB contains entries that map destination IP addresses to next-hop IP addresses, allowing routers to efficiently determine where to send packets based on their destination. The FIB is used in the forwarding process to make forwarding decisions and gets updated dynamically as the network topology changes. While the IOS FIB handles the forwarding decisions for IP packets in the physical network, the OMP routes establishe and maintains connectivity within the virtual overlay network. Therefore, the IOS FIB entries don't contain OMP routes, or the need for OMP route information didn't arise until the introduction of Security Group Tag (SGT) propagation with Cisco TrustSec Integration in Cisco IOS XE Catalyst SD-WAN Release 17.3.1a. For more information, see SGT propagation with Cisco TrustSec Integration.

Note Adding the OMP routes in IOS FIB is mandatory for SGT binding because it allows for the enforcement of security policies based on SGTs in a network.

In the SD-WAN mode, the OMP routes are present in the Routing Information Base (IOS RIB). In Cisco IOS, IOS RIB stands for a database residing in the memory of a Cisco router or switch. The IOS RIB contains information about routes learned from different routing protocols, static routes, and directly connected networks. In the SD-WAN mode, the control plane handles the packet forwarding. The IOS RIB stores all the routes learned during packet transfer, while the control plane stores the packet forwarding information.

The OMP routes aren't downloaded directly into the IOS FIB from the IOS RIB because of the way Cisco Catalyst SD-WAN architecture handles routing and forwarding. The IOS FIB is designed to work independently of the control plane. It doesn't directly consume the routes from the IOS RIB. Instead, it receives forwarding instructions from a centralized Cisco SD-WAN Controller. The Cisco IOS XE Catalyst SD-WAN devices receive these forwarding instructions from the Cisco SD-WAN Controller and program their local forwarding tables, which could include the IOS FIB. Therefore, while the OMP routes exist in the IOS RIB, they aren't directly downloaded into the IOS FIB. Instead, the Cisco SD-WAN Controller determines the appropriate forwarding paths and instructs the devices accordingly. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, OMP prefixes get added to the IOS FIB. Cisco Catalyst SD-WAN considers the route with OMP prefixes as a **CTS route**. The CTS route contains the OMP prefix, the length, and the associated SGT value. When the OMP prefixes get added to the OMP routes, it means that the OMP routes are now associated with specific IP address prefixes, further strengthening the IP-SGT binding.

Restrictions of OMP Prefixes for IP-SGT Binding

- In the autonomous mode, the IP-SGT binding allows for the enforcement of multicast route policies using the Security Group Access Control List (SGACL). However, starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the ability to add OMP prefixes to IP-SGT binding for multicast routes is no longer supported.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the support for adding OMP prefixes to IP-SGT binding is not available on SD-WAN OMP routes and SD-WAN NAT routes, which are the two types of SD-WAN routes for Direct Internet Access (DIA).
- Adding OMP prefixes to IP-SGT binding is not supported on multitenant Cisco IOS XE Catalyst SD-WAN devices.

Benefits of OMP Prefixes for IP-SGT Binding

- In Cisco TrustSec, switches, routers, and firewalls examine Security Group Tags (SGTs) to classify user/device groups and enforce traffic policies. When it comes to Cisco IOS XE Catalyst SD-WAN egress, the Cisco IOS XE Catalyst SD-WAN device maps the destination IP address to a SGT mapping and performs a lookup for the destination SGT. These mappings can be received through Security Group Exchange Protocol (SXPs), OMP, or static configuration. Once the SGT is identified, the Cisco IOS XE Catalyst SD-WAN device enforces Security Group Access Control Lists (SGACLs) using downloaded or static SGACLs. The enforcement can occur at the branch site or the data center (DC) headend, depending on the deployment configuration. The SGACL ensures that traffic complies with the designated policies associated with the corresponding SGT, enhancing network security and control.

  Adding OMP prefixes to the SGTs enforces SGT based security policies to the overlay traffic.This can be enforced at a branch or at the headend. The SGT based security policy can be enforced on the DIA traffic. Adding OMP prefixes to the SGTs enables binding to the overlay prefixes as well.

- With OMP prefixes in the IOS FIB, the forwarding instructions received from the centralized Cisco SD-WAN Controller can be more accurate and specific, resulting in optimized routing and improved network performance.

- Adding the OMP prefixes provides greater flexibility in managing and controlling traffic within the Cisco Catalyst SD-WAN environment, enabling efficient utilization of network resources.

- The current FIB infrastructure allows OMP and CTS route information to exist together in routing entries. This information is accessible to the shim layer through the HW-API interface.

Configure OMP Prefixes for IP-SGT Binding Using Cisco SD-WAN Manager

The following are the three ways to configure OMP prefixes for IP-SGT Binding using Cisco SD-WAN Manager.

- Use SXP to propagate SGTs across network devices if your hardware does not support inline tagging. Using Cisco Identity Services Engine (ISE), create an IP-to-SGT binding (Dynamic IP-SGT) and download IP-SGT binding using SXP to a Cisco IOS XE Catalyst SD-WAN device for propagation of SGT over the Cisco Catalyst SD-WAN network. See Configure SXP for Dynamic IP-SGT Binding Using Cisco SD-WAN Manager.

- Alternatively, there's an option to manually configure IP-SGT binding (Static IP-SGT) and then push the configuration to a Cisco IOS XE Catalyst SD-WAN device using a CLI Add-On template to propagate SGT over the Cisco Catalyst SD-WAN network. See Configure Static IP-SGT Binding Using Cisco SD-WAN Manager.

Note Ensure that you enter the right **Peer IP** address and **Source IP** while creating a new SXP connection.

Note For more information on the SGT propagation options using Cisco SD-WAN Manager , and the LAN to WAN and WAN to LAN behavior see, SGT Propagation options.

- When the Cisco SD-WAN Controller establishes a connection to Cisco ISE, it obtains the IP-to-username and user-to-user-group mappings from Cisco ISE and Cisco pxGrid. The Cisco SD-WAN Controller subsequently pushes the identity mapping information containing IP-to-username to user-group mapping to the Cisco IOS XE Catalyst SD-WAN devices. The identity mapping information is used when creating firewall policies in Cisco SD-WAN Manager. For information on creating identity-based firewall policies, see Configure Cisco SD-WAN Identity-Based Firewall Policy.

Monitor OMP Prefixes for IP-SGT Binding Using the CLI

Monitor the Next-hop info

The command **show ip cef vrf detail** displays detailed information about the Cisco Express Forwarding (CEF) table for a specific Virtual Routing and Forwarding (VRF) instance. When OMP routes are advertised, they include next-hop information that indicates the IP address of the remote system from which the OMP route was learned. This next-hop information helps in determining the path to reach the destination network.

The following is a sample output from the **show ip cef vrf detail** command:

```
Device# show ip cef vrf 1 172.16.255.112/32 detail
172.16.255.112/32, epoch 0, flags [SDWAN], per-destination sharing
  Covered dependent prefixes: 1
    notify cover updated: 1
  nexthop 172.16.255.11 Sdwan-system-intf
  nexthop 172.16.255.21 Sdwan-system-intf
```

The example displays the OMP route containing the next-hop information attached with a remote system IP along with a SD-WAN flag set. By flagging routes as SD-WAN routes, the network infrastructure can distinguish them from other types of routes and treat them differently based on the requirements and policies of the Cisco Catalyst SD-WAN deployment.

Monitor the CTS Route Inheriting the OMP Route

The CTS routes that inherit OMP routes will include next-hop information indicating the IP address of the remote system from which the OMP route information was learned. This next-hop information helps routers determine the path to reach the destination network associated with the CTS route. The CTS routes that inherit the OMP routes will also have the SD-WAN flag set. The SD-WAN flag indicates that these routes are part of the SD-WAN infrastructure and are specifically designated for use within the Cisco Catalyst SD-WAN framework. The inherited flag is set to true for the CTS routes. The inherited flag signifies that the CTS route inherits the route information from the OMP route. It indicates that the CTS route is derived from the OMP route and carries forward the properties of the original OMP route.

The following is a sample output from the **show ip cef vrf detail**

```
Device# show ip cef vrf 1 10.2.2.0/24 detail
10.2.2.0/24, epoch 0, flags [cover dependents, SDWAN]
  Covered dependent prefixes: 1
```

```
    notify cover updated: 1
  nexthop 172.16.255.11 Sdwan-system-intf

vm5#show run | i cts
cts role-based sgt-map vrf 1 10.2.2.1 sgt 10

vm5#show ip cef vrf 1 10.2.2.1/32 detail
10.2.2.1/32, epoch 0, flags [subtree context, SDWAN]
  SC owned,sourced: FIB_SC: RBAC - [SGT 10 S D]
  1 IPL source [active source]
    Dependent covered prefix type inherit, cover 10.2.2.0/8
  recursive via 10.2.2.0/24
    nexthop 172.16.0.0 Sdwan-system-intf
```

Note The CTS routes that inherit OMP routes will have Internet Protocol Layer (IPL) as the source. This indicates that the route information originates from the IP layer of the network protocol stack.

Monitor the OMP Route Inheriting the CTS Route

Monitor the OMP route inheriting the CTS route using **show ip route vrf**.

The following is a sample output from the **show ip route vrf** command:

```
Device#  show ip route vrf 1 10.2.2.0
Routing Table: 1
Routing entry for 10.2.2.0/24
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via ospf 1
  Advertised by ospf 1 subnets
  Last update from 172.16.0.0 on Sdwan-system-intf, 00:33:31 ago
  Routing Descriptor Blocks:
  * 172.16.255.11 (default), from 172.16.255.11, 00:33:31 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
Device#  show run | i cts
cts role-based sgt-map vrf 1 10.2.0.0/16 sgt 16

Device#  sho ip cef vrf 1 10.2.2.0/24 detail
10.2.2.0/24, epoch 0, flags [cover dependents, subtree context, SDWAN]
  Covered dependent prefixes: 1
    notify cover updated: 1
  SC inherited: FIB_SC: RBAC - [SGT 16 S D]
  nexthop 172.16.0.0 Sdwan-system-intf
```

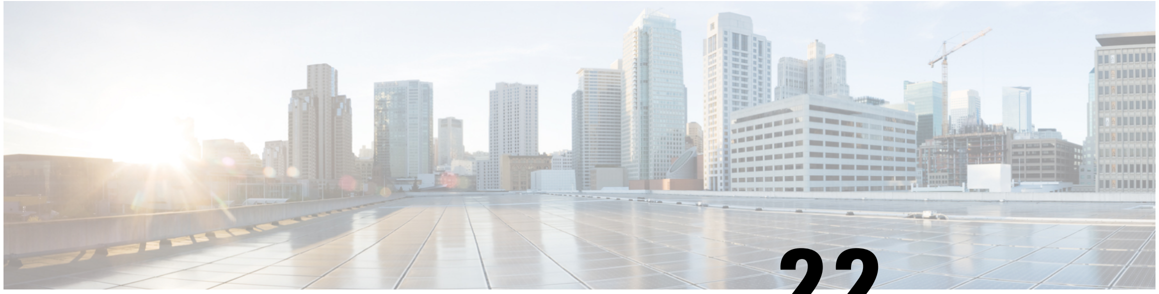
Monitor the Prefix Sourced Both from OMP and CTS Routes

When an exact prefix is sourced from both the OMP and CTS routes, the resulting route will have the next-hop information from OMP and SGT tag info from the CTS route.

The following is a sample output from the **show ip route vrf**

```
Device# show ip route vrf 1 10.2.2.0
Routing Table: 1
Routing entry for 10.2.2.0/24
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via ospf 1
  Advertised by ospf 1 subnets
  Last update from 172.16.255.11 on Sdwan-system-intf, 00:39:49 ago
  Routing Descriptor Blocks:
  * 172.16.00 (default), from 172.16.255.11, 00:39:49 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
```

```
Device# show run | i cts
cts role-based sgt-map vrf 1 10.2.2.0/24 sgt 24
Device# sho ip cef vrf 1 10.2.2.0/24 detail
10.2.2.0/24, epoch 0, flags [cover dependents, subtree context, SDWAN]
  Covered dependent prefixes: 1
    notify cover updated: 1
  SC owned,sourced: FIB_SC: RBAC - [SGT 24 S D]
  1 IPL source [no flags]
  nexthop 172.16.255.11 Sdwan-system-intf
```



CHAPTER 22

Unified Threat Defense Resource Profiles

Table 96: Feature History

Feature Name	Release Information	Description
Configure Unified Threat Defense Resource Profiles	Cisco IOS XE Catalyst SD-WAN 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 414

- Configure Unified Threat Defense Resource Profiles , on page 414
- Verify Unified Threat Defense Resource Profiles, on page 415

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

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.2, for all ISR1100 platforms, you must reboot the device to change resource profiles.

Configure Unified Threat Defense Resource Profiles

Configure the Unified Threat Defense Resource Profiles Using Cisco SD-WAN Manager

You can configure the Unified Threat Defense resource profiles using Cisco Catalyst SD-WAN Manager by doing the following:

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

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

3. Choose the device(s).
4. Click **Security App Hosting**.
5. Enter a template name and description.
6. 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.
7. To download the URL database on the device, choose **Yes**.
8. 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.
9. Click **Save**.
10. Add this template to the device template.
11. 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 23

Enable MACsec Using Cisco Catalyst SD-WAN Manager

Table 97: Feature History

Feature Name	Release Information	Feature Description
Enabling MACsec using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	With this feature, you can enable MACsec using Cisco Catalyst SD-WAN Manager for Cisco Catalyst SD-WAN devices on the service side. With MACsec enabled using Cisco Catalyst SD-WAN Manager, communication between devices in the service VPN is protected, thus enhancing security for the service VPN.

Information About Enabling MACsec Using Cisco SD-WAN Manager

MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption that provides data confidentiality and integrity for media access independent protocols. MACsec helps improve security at branches and between the branches. When MACsec is enabled using Cisco SD-WAN Manager, communication between the devices in the service VPN is protected, thus enhancing security in the service VPN.

MACsec, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. Only network access devices and endpoint devices such as a PC or IP phone is secured using MACsec. The 802.1AE encryption with MKA is supported on downlink ports for encryption between the routers or switches and host devices. MACsec encrypts all data except for the source and destination MAC addresses of an ethernet packet.

Supported Devices for MACsec in Cisco Catalyst SD-WAN

The following devices can be configured for MACsec encryption using Cisco SD-WAN Manager:

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

- Cisco Catalyst C8500-12X Router
- Cisco Catalyst C8500-12X4QC Router
- Cisco Catalyst C8500-20x6C Router
- Cisco Catalyst C8500L-8S4X Router

Minimum supported releases: Cisco IOS XE Release 17.12.2 and Cisco Catalyst SD-WAN Manager Release 20.12.2

- Cisco 4461 Integrated Services Router (ISR4461) K9 built-in 1G and 10G ports with NIM-2GE-CU-SFP
- C8300-2N2S-4T2X built-in 10G ports, and also with C-NIM-1X
- C-NIM-4X and C-NIM-1X on C8300 Series
- C-NIM-8T & C-NIM-8M & C-NIM-2T on C8300/C8200/C8200L Series

The support of Integrated Services Router platform in Cisco Catalyst SD-WAN are universal with all the MACsec supported scenarios.

Benefits of Enabling MACsec in Cisco Catalyst SD-WAN

- Support for Point-to-Multipoint (P2MP) deployment models.
- Support for multiple P2P and P2MP deployments on the same physical interface.
- Support for 128- and 256-bit Advanced Encryption Standard–Galois Counter Mode (AES-GCM) encryption for data packets.
- Support for 128- and 256-bit Advanced Encryption Standard-Cipher-based Message Authentication Code (AEC-CMAC) encryption for control packets.
- Support for VLAN tag in the clear option to enable Carrier Ethernet Service Multiplexing.
- Support for coexisting of MACsec and Non-MACsec sub interfaces.
- Support for configurable Extensible Authentication Protocol over LAN (EAPoL) destination address.
- Support for configurable option to change the EAPoL Ethernet type.

- Support for configurable replay protection window size to accommodate packet reordering in the service provider network.

Prerequisites for Enabling MACsec in Cisco Catalyst SD-WAN

- MACsec requires MACsec license. For more information, see https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8500-series-edge-platforms/datasheet-c78-744089.html?oid=dstetr023042#Licensing
- Layer 2 transparent Ethernet Services must be present.
- The service provider network must provide a MACsec Layer 2 Control Protocol transparency such as, Extensible Authentication Protocol over LAN (EAPoL).

Restrictions for Enabling MACsec in Cisco Catalyst SD-WAN

- MACsec is supported up to the line rate on each interface. However, the forwarding capability may be limited by the maximum system forwarding capability.
- To configure port-channel, ensure that you configure MACsec at each interface of the link bundle.
- You cannot configure MACsec on the native sub interface. However, you can configure MACsec on the main interface using the **macsec dot1q-in-clear 1**.
- If the MKA session becomes inactive because of key unwrap failure, reconfigure the pre-shared key-based MKA session using MACsec configuration commands on the respective interfaces to bring the MKA session up.
- MACsec-configured on physical interface with Ethernet Virtual Circuits (EVC) is not supported. The EAPoL frames get dropped in such cases.
- When **macsec dot1q-in-clear** is enabled, the native VLAN is not supported.

Configure MACsec Enablement in Cisco SD-WAN Manager Using a CLI Template

Use the CLI templates to configure MACsec feature in Cisco Catalyst SD-WAN Manager. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

1. Enable MACsec feature from the global configuration mode in Cisco Catalyst SD-WAN Manager.

```
key chain key_chain_name macsec
 key connectivity_association_key_name
  key-string connectivity_association_key
```

2. Configure MKA.

   The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.

   ```
   mka policy policyname
   ```

3. Configure MACsec and MKA on an interface.

   ```
   interface GigabitEthernet interface
   macsec
   mka policy policyname
   mka pre-shared-key key-chain [keychainname|fallback-key]
   ```

Here's the complete configuration example for configuring and enabling MACsec in Cisco Catalyst SD-WAN Manager:

```
key chain mka-keychain128 macsec
 key 10
interface TenGigabitEthernet0/0/5
 vrf forwarding 20
 ip address 60.60.60.2 255.255.255.0
 ip mtu 1468
 speed 1000
 mka pre-shared-key key-chain mka-keychain128
 macsec
```

Verify MACsec Enablement in Cisco SD-WAN Manager

Verify MACsec Keychains

The following is a sample output from the **show mka keychains** command that displays the list of MACsec keychains configured on a Cisco IOS XE Catalyst SD-WAN device. It shows information that displays a list of keychain name, key number and the associated interface.

```
Device# show mka keychains

MKA PSK Keychain(s) Summary...

Keychain          Latest CKN                                                                  Interface(s)
Name               Latest CAK                                                                     Applied

===========================================================================================
mka-keychain128   10                                                                            Te0/0/5

                   <HIDDEN>
```

Verify Default MACsec Policy

The following is a sample output from the **show mka default-policy detail** command that displays the default MACsec policy configured on a Cisco IOS XE Catalyst SD-WAN device. Use this command to retrieve detailed information about the default policy, including its name, cipher suite, key agreement protocol, and other parameters. The additional keywords (detail, sessions, sessions detail) provide more specific information about the default policy or its active sessions.

```
Device# show mka default-policy detail
MKA Policy Configuration ("*DEFAULT POLICY*")
========================
```

```
MKA Policy Name...........*DEFAULT POLICY*
Key Server Priority.......0
Confidentiality Offset....0
Delay Protect.............FALSE
SAK-Rekey On-Peer-Loss....0
SAK-Rekey Interval........0
Send Secure Announcement..DISABLED
Include ICV Indicator.....TRUE
SCI Based SSCI............FALSE
Use Updated Ethernet Hdr..NO
Cipher Suite(s)........ GCM-AES-128
                        GCM-AES-256

Applied Interfaces...
```

The following is a sample output from the **show mka default-policy sessions** command.

```
Device# show mka default-policy sessions
Summary of All Active MKA Sessions with MKA Policy "*DEFAULT POLICY*"...

==========================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

==========================================================================================
Te0/0/5         e8d3.22d3.2085/000d  *DEFAULT POLICY*  NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka default-policy sessions detail** command.

```
Device# show mka default-policy sessions detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)...... 80
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)
```

```
Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379101      a03d.6e5d.037f/0045  0         YES            0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 79
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
```

```
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------
```

Verify MACsec Policies

The following is a sample output from the **show mka policy** command that displays the MACsec policies configured on a Cisco IOS XE Catalyst SD-WAN device. You can specify a specific policy name to view its details, or use the keywords detail or sessions to provide additional information about the policies or their active sessions.

```
Device# show mka policy MKA-128
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
===============================================================================
MKA-128           0    FALSE 0  FALSE TRUE   GCM-AES-128     Te0/0/5
```

Verify Active MACsec Sessions

The following is a sample output from the **show mka sessions** command that displays the active MACsec sessions on a Cisco IOS XE Catalyst SD-WAN device. You can use this command to display information about the sessions, including their interface, Policy-Name and Macsec Peers etc. The additional keywords such as **`detail`**, interface **`TenGigabitEthernet`** offer more specific details about the sessions or sessions associated with a particular interface.

```
Device# show mka sessions
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

==========================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited         Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status            CKN
```

```
===========================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128          NO               NO

13              a03d.6e5d.037f/0045  1                Secured          10
```

The following is a sample output from the **show mka sessions detail** command.

```
Device# show mka sessions detail
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............ e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)...... 134
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379154      a03d.6e5d.037f/0045  0         YES           0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 133
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------
```

View MACsec Statistics

The following is a sample output from the **show mka statistics** command that displays MACsec statistics on a Cisco IOS XE Catalyst SD-WAN device for eg CAK, SAK and MKPDU statistics. When used with the keyword interface **`TenGigabitEthernet`**, it provides statistics specifically for that interface.

```
Device# show mka statistics interface TenGigabitEthernet 0/0/5
MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated............. 0
   SAKs Rekeyed............... 0
   SAKs Received.............. 1
   SAK Responses Received..... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx... 229
      "Distributed SAK".. 1
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 231
      "Distributed SAK".. 0
      "Distributed CAK".. 0
```

View Summary of MKA Sessions

The following is a sample output from the **show mka summary** command that displays a summary of MACsec-related information on a Cisco IOS XE Catalyst SD-WAN device. It includes details about the MACsec feature such as the global MKA configuration, default policy, and the number of active sessions.

```
Device# show mka summary
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

===========================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

===========================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10



MKA Global Statistics
=====================
MKA Session Totals
   Secured.................... 18
   Fallback Secured........... 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 17
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx...... 374465
      "Distributed SAK"..... 18
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 384191
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx.............................. 0
   MKPDU Rx ICV Verification............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation................... 0
   MKPDU Rx Bad Peer MN.................. 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............ 0
   SAK USE Latest AN not in USE.......... 0
```

View Hardware-related Information about MACsec

The following is a sample output from the **show macsec hw detail** command that displays detailed hardware-related information about MACsec on a Cisco IOS XE Catalyst SD-WAN device. It provides information about the hardware capabilities and configurations related to MACsec.

```
Device# show macsec hw detail
MACsec Capable Interface         RxSA Inuse
----------------------------------------------
 TenGigabitEthernet0/0/5       :        1


Other Debug Statistics
Interface TenGigabitEthernet0/0/5 HMAC:
RxOctets              0  RxUcastPkts           0  RxMcastPkts           0
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets              0  TxUcastPkts           0  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
LMAC:
RxOctets           5595  RxUcastPkts          22  RxMcastPkts           9
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets           1710  TxUcastPkts          15  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
```

View MACsec Summary

The following is a sample output from the **show macsec summary** command that displays a summary of MACsec information on the device, including MACsec capable interfaces, installed Secure Channels (SC), and MACsec enabled interfaces with their associated receive SC and VLAN.

```
Device# show macsec summary
MACsec Capable Interface                Extension              Installed Rx SC
---------------------------------------------------------------------------------
 TenGigabitEthernet0/0/0                 One tag-in-clear
 TenGigabitEthernet0/0/1                 One tag-in-clear
 TenGigabitEthernet0/0/2                 One tag-in-clear
 TenGigabitEthernet0/0/3                 One tag-in-clear
 TenGigabitEthernet0/0/4                 One tag-in-clear
 TenGigabitEthernet0/0/5                 One tag-in-clear                 1
 TenGigabitEthernet0/0/6                 One tag-in-clear
 TenGigabitEthernet0/0/7                 One tag-in-clear
 TenGigabitEthernet0/1/0                 One tag-in-clear
 TenGigabitEthernet0/1/1                 One tag-in-clear
 TenGigabitEthernet0/1/2                 One tag-in-clear
 TenGigabitEthernet0/1/3                 One tag-in-clear
 FortyGigabitEthernet0/2/0               One tag-in-clear
 FortyGigabitEthernet0/2/4               One tag-in-clear
 FortyGigabitEthernet0/2/8               One tag-in-clear
 GigabitEthernet0                        One tag-in-clear
 SDWAN System Intf IDB                   One tag-in-clear
 SDWAN vmanage_system IDB                One tag-in-clear
 LIIN0                                   One tag-in-clear
 LI-Null0                                One tag-in-clear
 Loopback65528                           One tag-in-clear
 Loopback65529                           One tag-in-clear
 SR0                                     One tag-in-clear
 Tunnel1                                 One tag-in-clear
 VoIP-Null0                              One tag-in-clear

 MACsec Enabled Interface         Receive SC   VLAN
-----------------------------------------------------
 TenGigabitEthernet0/0/5       :        1         0
```

The following is a sample output from the **show macsec mka-request-notify** command that displays information about MACsec (Media Access Control Security) enabled interfaces, including the counts of Control Plane (CR) transmit and delete Secure Channels (SC), transmit Security Associations (SA), receive SC, and delete SAs, as well as the MKA (MACsec Key Agreement) notification count on the interface "TenGigabitEthernet0/0/5.

```
Device# show macsec mka-request-notify
MACsec Enabled Interface         CR_TX_SC  DEL_TX_SC  INST_TX_SA  CR_RX_SC  DEL_RX_SC
INST_RX_SA  DEL_RX_SA  MKA_NOTIFY
------------------------------------------------------------------------------------------
 TenGigabitEthernet0/0/5       :       18        17        18        18         0
18           11         0
```

The following is a sample output from the **show macsec post** command.

```
Device# show macsec post
 MACsec Capable Interface                         POST Result
--------------------------------------------------------------
 TenGigabitEthernet0/0/0                              NONE
 TenGigabitEthernet0/0/1                              NONE
 TenGigabitEthernet0/0/2                              NONE
 TenGigabitEthernet0/0/3                              NONE
 TenGigabitEthernet0/0/4                              NONE
 TenGigabitEthernet0/0/5                              NONE
 TenGigabitEthernet0/0/6                              NONE
 TenGigabitEthernet0/0/7                              NONE
 TenGigabitEthernet0/1/0                              NONE
 TenGigabitEthernet0/1/1                              NONE
 TenGigabitEthernet0/1/2                              NONE
 TenGigabitEthernet0/1/3                              NONE
 FortyGigabitEthernet0/2/0                            NONE
 FortyGigabitEthernet0/2/4                            NONE
 FortyGigabitEthernet0/2/8                            NONE
```

Verify MACsec Configuration and Status

The following is a sample output from the **show macsec status interface** command that displays the MACsec configuration and status for interface TenGigabitEthernet 0/0/5. It shows the supported ciphers, selected cipher, replay window size, transmit and receive Secure Channel Identifiers (SCIs), and the next expected packet numbers for transmission and reception

```
Device# show macsec status interface TenGigabitEthernet 0/0/5
Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256 GCM-AES-XPN-128 GCM-AES-XPN-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure
  Include-SCI:              TRUE

 Transmit SC:
  SCI:                      E8D322D32085000D
  Transmitting:             TRUE
 Transmit SA:
  Next PN:                  10002
  Delay Protect AN/nextPN:  NA/0

 Receive SC:
  SCI:                      A03D6E5D037F0045
  Receiving:                TRUE
 Receive SA:
  Next PN:                  10077
  AN:                        1
  Delay Protect AN/LPN:      0/0
```

Configuration Example for MACsec Enablement in Cisco SD-WAN Manager

The following example displays the configuration for MACsec configured on Cisco Catalyst C8500 platforms.

```
key chain mka-keychain128 macsec
 key 10
interface TenGigabitEthernet0/0/5
 vrf forwarding 20
 ip address 60.60.60.2 255.255.255.0
 ip mtu 1468
 speed 1000
 mka pre-shared-key key-chain mka-keychain128
 macsec
```

CHAPTER 24

Cisco Catalyst SD-WAN Firewall High Availability

Table 98: Feature History

Feature	Release Information	Description
Cisco Catalyst SD-WAN Firewall High Availability	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	By implementing High Availability in Cisco Catalyst SD-WAN, you can set up two Cisco IOS XE Catalyst SD-WAN devices in either active-active or active-standby configurations. When high availability is enabled, features like the Zone Based Firewall (ZBF) and Network Address Translation (NAT) synchronize their states between the devices, whether in active-standby or active-active modes. In the event of a failure of the active device, the standby device seamlessly takes over operations without interrupting session flows, thus eliminating the need for reconnection.

Information About Cisco Catalyst SD-WAN Firewall High Availability

High availability ensures the continuous operation of essential services such as Zone Based Firewall (ZBF) and Network Address Translation (NAT). High availability provides a seamless switchover of these services in the event of a device failure.

In a high-availability environment, firewall and NAT functionalities synchronize their operational states between two Cisco IOS XE Catalyst SD-WAN devices through redundancy groups. A redundancy group is a pairing of two Cisco IOS XE Catalyst SD-WAN devices where one is designated as the active device and the other as the standby. VPNs are associated with these redundancy groups. Cisco Catalyst SD-WAN supports two redundancy groups, allowing one set of traffic to be active on one device and another set of traffic to be active on the peer device.

The synchronization of stateful features such as firewall sessions and NAT mappings from the active device to the standby device ensures that the standby device has all the necessary information to maintain service continuity if the active device fails. This seamless transition prevents service disruption and ensures high availability.

Note While high availability aims to provide seamless operation, certain features may not transition traffic as smoothly during failover scenarios. Support for Application Layer Gateway (ALG) and Application Inspection and Control (AIC) is on a best-effort basis, and the traffic switchover might not be seamless. Similarly, traffic flows involving TCP/TLS proxy (Unified Threat Defense) and Network-Based Application Recognition (NBAR)/Deep Packet Inspection (DPI) may experience disruptions during failover.

Redundancy Groups

A redundancy group is a pairing of devices in a high-availability configuration in Cisco Catalyst SD-WAN that ensures continuous service. The devices in the redundancy group can operate either in an active or standby state. VPNs are associated with the redundancy groups, and the VPN traffic is processed by the active device in the redundancy group. Cisco Catalyst SD-WAN supports a maximum of two redundancy groups.

In an active-active configuration, both devices in the two redundancy groups simultaneously process traffic, providing load balancing and redundancy. In this setup, VPNs are distributed across two Cisco IOS XE Catalyst SD-WAN devices, resulting in the creation of two redundancy groups. Redundancy group configuration should have the **preempt** option configured for active-active (two redundancy groups) mode.

In an active-standby configuration, all the VPNs are assigned to a single Cisco IOS XE Catalyst SD-WAN device, creating one redundancy group. For active-standby (only one redundancy group configured) mode, the **preempt** option is not recommended

By correctly configuring redundancy groups, you can ensure high availability and continuous service in your Cisco Catalyst SD-WAN environment. VPNs that are not associated with a redundancy group do not have their traffic protected by high availability.

VPN Associations

You can associate VPNs with redundancy groups in Cisco Catalyst SD-WAN. To do this, you must manually assign each VPN to its redundancy group. If you configure route leaking between VPNs, it is contained within the same redundancy groups, and this is enforced by Cisco SD-WAN Manager for proper traffic management and high availability.

Redundancy Group Init Roles

Init roles are used while configuring redundancy groups on Cisco IOS XE Catalyst SD-WAN devices. These roles determine the initial state of a device within a redundancy group, specifying whether it should start as the active or standby device. Proper configuration of init roles ensures that one device takes on the responsibility of handling traffic (active) while the other remains in a ready state (standby) to take over in case of a failure.

The **`init-role active`** within redundancy groups helps you to select between active and standby options when both redundancy groups have equal priority. You must configure this role appropriately for each redundancy group. Designate one device as **`init-role active`**, and configure the other as **`init-role standby`**.

When **`preempt`** is set, the redundancy group with **`init-role active`** become actives if the redundancy group priorities of the peer devices are equal. This allows for automatic switchover to their initial state after faults have been addressed.

Implicit and Explicit Tracking

Redundancy groups use object tracking to determine their state. Examples of this include Cisco Catalyst SD-WAN session tracking, NAT endpoint tracking, and interface state tracking.

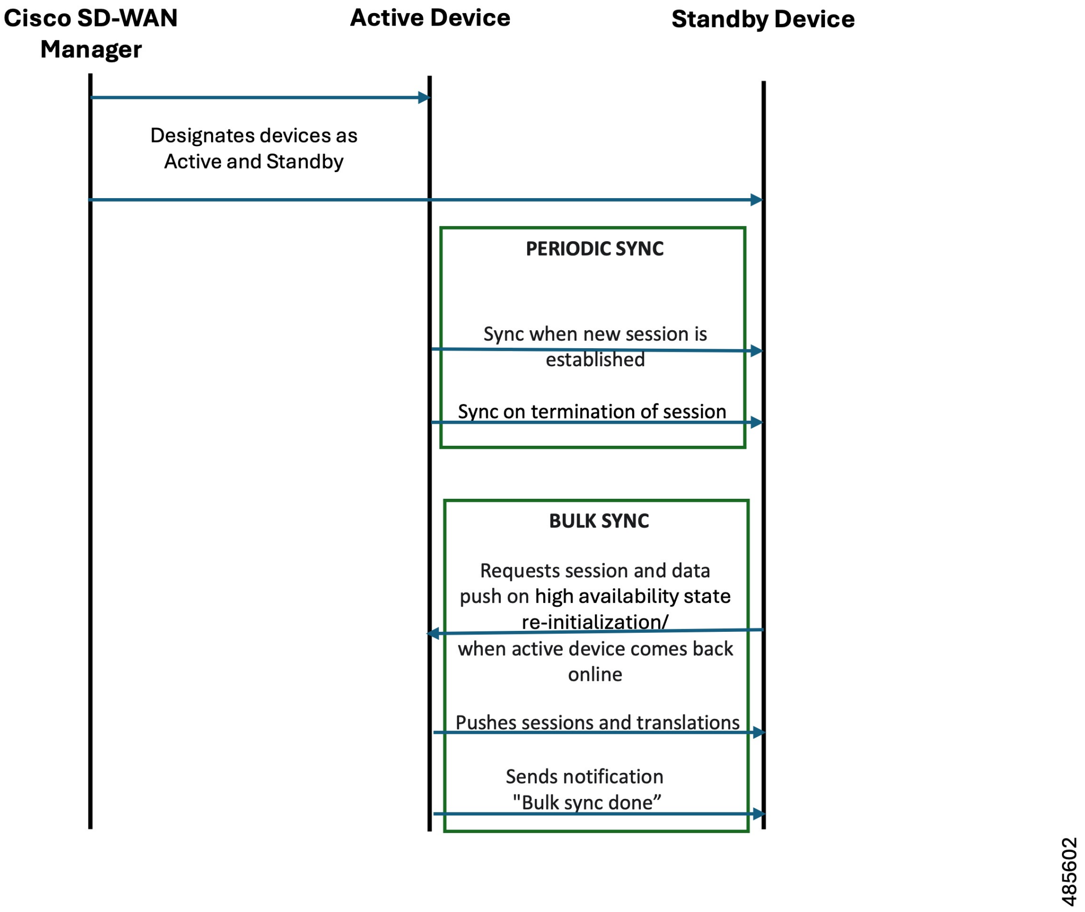
The redundancy groups can also be configured to create an object. Virtual Router Redundancy Protocol (VRRP) tracks the redundancy group object so that it can follow the redundancy group state. For example, if the redundancy group state is active, the VRRP state is primary; if the redundancy group state is standby, the VRRP state is backup.

State Synchronization

There are two types of state synchronization between the active and standby devices:

- Periodic Sync: This occurs as soon as a session is established. For example, when a NAT entry is created or a firewall session is established, the state is immediately synchronized. Similarly, when a session is deleted, the corresponding state is also removed.
- Bulk Sync: This occurs whenever the high availability state is re-initialized, or when a Cisco IOS XE Catalyst SD-WAN device is reloaded or comes back online. During this process, the standby device requests the active device to push the sessions and translations to it. After this synchronization is complete, the active device issues a **`bulk sync done`** notification to the standby device. At this point, standby device transitions to hot standby. When the bulk sync is fully completed, the standby device is considered to be in a hot standby state.

Figure 12: State Synchronization


Cisco SD-WAN Manager
Active Device
Standby Device
Designates devices as Active and Standby
PERIODIC SYNC
Sync when new session is established
Sync on termination of session
BULK SYNC
Requests session and data push on high availability state re-initialization/ when active device comes back online
Pushes sessions and translations
Sends notification "Bulk sync done"
485602

Path Optimization

Path optimization in Cisco Catalyst SD-WAN ensures that WAN traffic is always directed to the active Cisco IOS XE Catalyst SD-WAN device, thereby avoiding traffic redirection, also known as peer diversion, and ensuring efficient traffic flow. When you enable path optimization, WAN traffic consistently flows to the active Cisco IOS XE Catalyst SD-WAN device, eliminating the need for peer diversion, where traffic would otherwise be redirected from the standby device to the active device.

For LAN traffic, you can direct traffic to the active Cisco IOS XE Catalyst SD-WAN device using Interior Gateway Protocol (IGP) rewrite or Virtual Router Redundancy Protocol (VRRP) following the redundancy group.

For WAN traffic, path optimization directs the traffic to the active device, preventing it from reaching the standby device.

IGP Rewrite

IGP Rewrite is a technique used to ensure that LAN-side traffic is directed to the active Cisco IOS XE Catalyst SD-WAN device within a redundancy group. Interior Gateway Protocols (IGPs) such as Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) dynamically route traffic within a network.

By adjusting the IGP metrics or routes, you can configure the network to prefer the active Cisco IOS XE Catalyst SD-WAN device for routing LAN traffic. This ensures that the active device handles the majority of the traffic, providing efficient traffic flow and minimizing the chances of traffic being redirected to the standby device.

VRRP Following Redundancy Group State

In the context of a redundancy group, you can configure VRRP to follow the state of the redundancy group. This means that the VRRP primary role is assigned to the Cisco IOS XE Catalyst SD-WAN device with the active redundancy group, ensuring that LAN-side traffic is directed to the active redundancy group. If the active redundancy group fails, VRRP reassigns the primary role to the device with the new active redundancy group, ensuring continuous service.

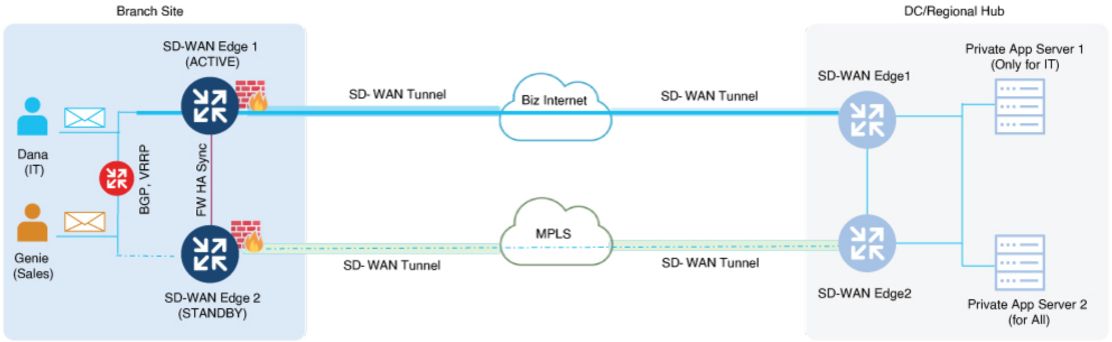
You can assign only one VPN to an interface, and the VRRP for that interface must follow the redundancy group associated with the same VPN. You can configure both VRRP and the redundancy group on the same Cisco IOS XE Catalyst SD-WAN device.

IGP Rewrite and VRRP following the redundancy group state are techniques used to attract LAN-side traffic to the device with the active redundancy group. By using these techniques, you can ensure that LAN-side traffic is consistently directed to the active redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device. Combined with path optimization for WAN traffic, this ensures that all traffic is efficiently routed to the active redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device until it fails. In such a setup, the states of firewall and NAT services are continuously synchronized between the two Cisco IOS XE Catalyst SD-WAN devices. In the event of a failover, the standby redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device takes over, and these services will continue to run seamlessly, maintaining high availability and continuous service.

In this sample topology for path optimization, VPN traffic flows through the active device, SD-WAN Edge 1, in both directions—from LAN to WAN and from WAN to LAN.

SD-WAN Edge 1, as the active device, modifies the routing parameters for LAN traffic and the OMP affinity for WAN traffic to attract traffic in both directions (LAN to WAN and WAN to LAN).

Figure 13: Path Optimization



Peer Diversion

Peer diversion is a mechanism where traffic arriving on a Cisco IOS XE Catalyst SD-WAN device with an associated redundancy group in a standby state is diverted to the peer device in the redundancy group. The peer device refers to the other device in the redundancy group.

Redundancy group configuration should include the **asymmetric-routing always-divert enable** command when setting up high availability in a redundancy group. This option ensures that when traffic reaches the standby device, it is diverted to the active device regardless of the type of traffic.

There are two methods of Peer diversion:

- LAN Divert
- WAN Divert

LAN Diversion

For the LAN traffic, based on VPN-to-redundancy group mapping, if the device is in the standby state for the traffic in a specific VPN, the traffic is diverted to the active device.

WAN Diversion

For the WAN traffic, if traffic is directed to a device in a standby state, Peer diversion uses session information from Cisco Catalyst SD-WAN to identify and redirect the traffic to the active device in the redundancy group.

Peer diversion efficiently manages traffic by diverting it to the active redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device when it arrives at a standby device. This mechanism is crucial for maintaining seamless traffic management and high availability in Cisco Catalyst SD-WAN environments. It ensures that features like Application Aware Routing and stateful services, such as firewall and NAT, are processed only on the active redundancy group.

VPN Homing

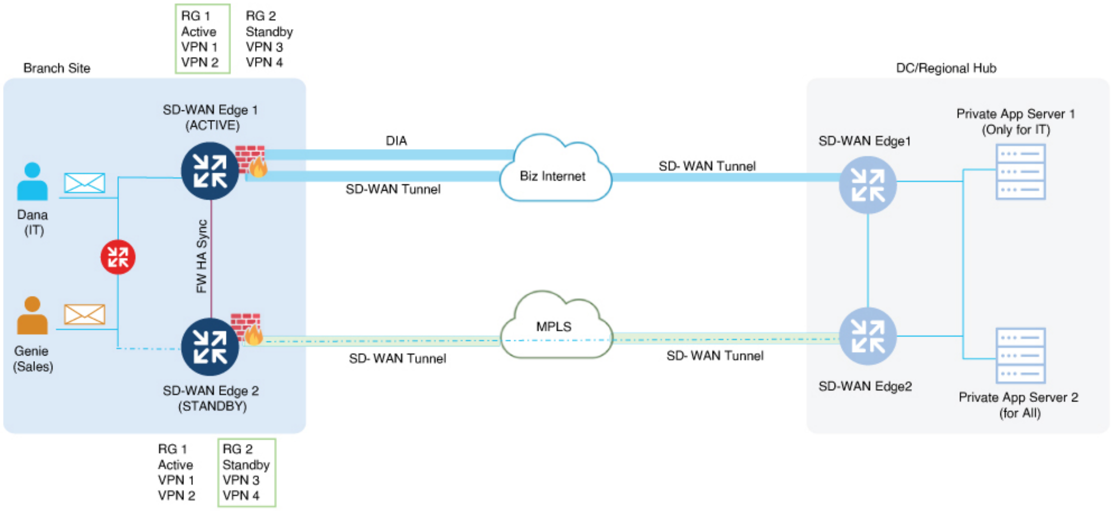
VPN homing is a technique used to manage and optimize the routing of VPN traffic through specific Cisco IOS XE Catalyst SD-WAN devices. This involves mapping VPNs to redundancy groups to determine which Cisco IOS XE Catalyst SD-WAN device will be active for the corresponding VPN traffic. Multiple VPNs can be mapped to a single redundancy group, allowing for flexible and efficient traffic management.

For seamless failover and consistent traffic routing, both the active and standby Cisco IOS XE Catalyst SD-WAN devices must have the same VPN to redundancy group mapping. This ensures that the network can maintain high availability and continuous service.

In this sample topology for VPN homing, two redundancy groups are configured for devices SD-WAN Edge 1 and SD-WAN Edge 2 in an active-active setup. As part of VPN homing, Service Side VPNs, VPN 1 and VPN 2, are associated with RG1, while VPN 3 and VPN 4 are associated with RG2.

As a result of this active-active setup, traffic is load-balanced across both devices, with SD-WAN Edge 1 handling traffic for VPN 1 and VPN 2, and SD-WAN Edge 2 handling traffic for VPN 3 and VPN 4. This configuration ensures efficient traffic management and high availability.

Figure 14: VPN homing



High Availability Interconnect

An interconnect is a dedicated connection between peer Cisco IOS XE Catalyst SD-WAN devices. It facilitates communication and synchronization between devices, allowing the high availability infrastructure to determine which redundancy group is active or standby. The interconnect also enables the transfer of session data to the standby redundancy group and provides a path for peer-diverted traffic.

In a high availability set up, the interconnect interface enables synchronization of services, such as Firewall and NAT, between two Cisco IOS XE Catalyst SD-WAN devices. This setup enables features to synchronize their state, such as sessions and translations, which is essential for seamless failover and high availability.

High Availability Configuration Options

When configuring the interconnect for high availability, you have the following options:

- Single Interface: A single physical interface or a subinterface can be used as the interconnect.
- Port Channel: A port channel can be used to provide redundancy and increased bandwidth for the interconnect.

Only a single interconnect interface may be configured. If multiple interfaces are required to meet throughput requirements, use a port channel.

On interconnect interfaces, default Quality of Service (QoS) configurations are applied to prioritize traffic. These QoS policies ensure that critical synchronization and management traffic is handled efficiently and without delay. High availability protocol traffic receives the highest precedence, followed by session management traffic, while peer divert traffic utilizes the remaining bandwidth.

Redundant Interface IDs

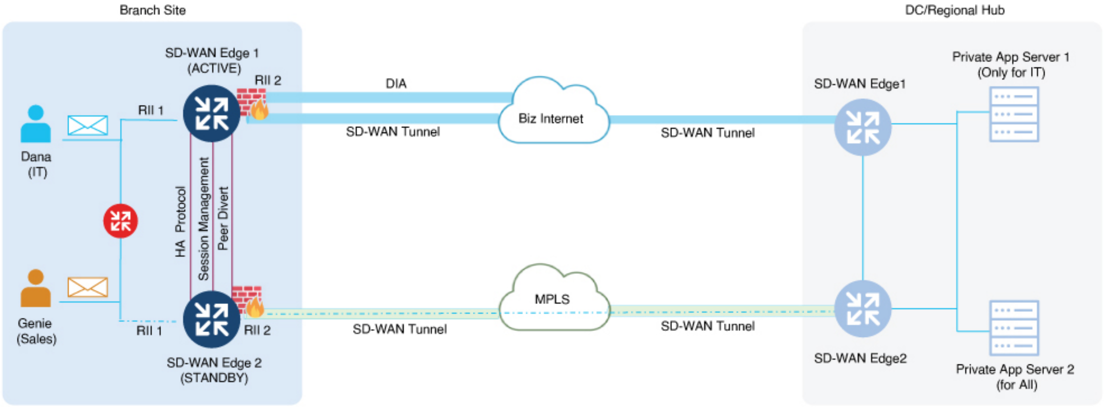
Redundant Interface IDs (RII) enable high-availability peer Cisco IOS XE Catalyst SD-WAN devices to be mapped and associated with each other. Cisco SD-WAN Manager automatically generates a unique RII for each interface on a Cisco IOS XE Catalyst SD-WAN device, and this RII must be replicated on the peer device. LAN and WAN interfaces must be configured with RII to ensure that each interface on one device corresponds to the redundant interface on another device. This includes configuring RII for the SD-WAN tunnel for service-side NAT.

By assigning matching RIIs to interfaces on both the active and standby Cisco IOS XE Catalyst SD-WAN devices, we logically pair the interfaces, forming a singular interface.

In a sample high availability interconnect topology, interconnect links (logical links) are set up between the active device (SD-WAN Edge 1) and the standby device (SD-WAN Edge 2). The high availability protocol uses keepalive messages to determine which device is active and which is standby. The state synchronization mechanism synchronizes the states of high availability features such as firewall and NAT between the active and standby devices. The peer diversion link ensures that traffic arriving on the standby device is diverted to the active device. The RII is essential to identify and manage of interfaces across active and standby devices.

Note Interfaces that do not have an RII assigned will not support high availability.

Figure 15: High Availability Interconnect and State Synchronization



NAT Pool Assignments

In Cisco Catalyst SD-WAN, NAT pools can be associated with redundancy groups to ensure high availability and efficient traffic management.

For NAT Direct Internet Access (DIA) configuration in active-active mode, two redundancy groups are configured, and NAT pools are assigned in a round-robin manner across these groups.You can use the CLI Add-on profile to assign a specific a redundancy group to a NAT pool. The mapping of NAT pools to redundancy groups should be the same as the mapping of VPNs to redundancy groups. For NAT translations to be synchronized, NAT mapping must belong to a redundancy group.

For NAT DIA configuration in active-standby mode, only one redundancy group is configured. When you associate a redundancy group with a NAT pool, the configured redundancy group is assigned to the NAT pool.

For service-side NAT configuration, NAT pools can be assigned to a VPN using service-side NAT mapping. Cisco SD-WAN Manager ensures that the redundancy group associated with the NAT pool matches the redundancy group the VPN is mapped to in the redundancy group configuration.

For more information, see NAT Deployment Models, on page 439.

NAT Deployment Models

Cisco Catalyst SD-WAN includes the following types of NAT configurations:

- NAT DIA: Allows remote sites to route traffic directly to the internet rather than routing the traffic to a central site or data center.
- Service-Side NAT: Allows you to configure internal NAT on data traffic traveling to and from the service hosts of the network overlay. Service-Side NAT translates data traffic of internal host addresses that match a configured centralized data policy.

NAT DIA

You can configure NAT DIA to allow direct internet access in high availability setups, ensuring continuous service and efficient traffic management. In a NAT DIA high availability configuration, policies must be configured, and NAT mapping must be associated with redundancy groups to ensure high availability.

Configure a pair of Cisco IOS XE Catalyst SD-WAN devices with a redundancy group. Both devices must be connected to the same set of hosts on the LAN side. When you configure one redundancy group, one device operates as the active device while the other remains in standby mode. You can connect the WAN interfaces of each device to the same or different internet service providers (ISPs) and place them on different subnets. Despite subnet differences, you can successfully divert stateful traffic because you configure the same RII on both interfaces. For more information about RII, see the section **Redundant Interface IDs** in High Availability Interconnect, on page 437.

Configure the WAN interfaces of both Cisco IOS XE Catalyst SD-WAN devices with an IGP routing protocol such as Internal Border Gateway Protocol (iBGP) or OSPF to install the NAT pool subnet into the ISP router along with other routes. During a switchover, the standby router becomes active and traffic is diverted to it as the sessions were previously synchronized.

For NAT DIA, match the reduncy group ID in the NAT mapping to the VPN traffic. Multiple VPNs belonging to the same redundancy group can share the same DIA mapping. NAT mappings configured without a redundancy group ID are used by control traffic on the device, and sessions created through this mapping are not synchronized.

You can configure NAT DIA for high availablility in Cisco SD-WAN Manager using configuration groups or by using the CLI Add-On Profile. For information see, Configure NAT DIA for Cisco Catalyst SD-WAN Firewall High Availability, on page 447, CLI Add-On Profile.

Service-Side NAT

A Service-Side NAT configuration is a used in high availability setups to ensure continuous service and efficient traffic management for overlay traffic.

In a service-side NAT for high availability configuration, configure policies and associate VPNs to redundancy group for high availability. In a Service-Side NAT high availability configuration set up, Cisco SD-WAN Manager checks whether a VPN is associated with any redundancy group and if NAT pools are configured as part of the VPN configuration. If the VPN is already associated with an redundancy group, the configured NAT pools for that VPN is considered for high availability. For information on configuring service-side NAT in Cisco SD-WAN Manager, see Configure Service-Side NAT.

Alarms and Notifications

Cisco SD-WAN Manager provides a way to monitor and log events related to redundancy group roles. When you navigate to **Monitor** > **Logs** in Cisco SD-WAN Manager, the page displays device-generated events, including those triggered by the toggling of redundancy group roles during a high availability failover.

Toggling of redundancy group roles occurs when the state of an redundancy group changes from active to standby or vice versa. This ensures continuous service during an high availability failover. The **Logs** page in Cisco SD-WAN Manager allows you to monitor and track these changes, displaying any failover events so that you can take appropriate action if necessary.

Restrictions for Cisco Catalyst SD-WAN Firewall High Availability

Device Compatibility

- Cisco IOS XE Catalyst SD-WAN devices used as active and standby devices must be of the same platform model.
- Among the Cisco Catalyst 8500 Series Edge platforms, flow-based platforms such as C8500L-8S4X platform do not support high availability.

VPN and Redundancy Group Configuration

- VPNs with route leaking must be associated with the same redundancy group.
- To maintain consistency between VRRP state and redundancy group state, each VRRP group must track the redundancy group associated with the same VPN (that is, VRRP group state follows redundancy group state).
- Both the active and standby devices must have identical NAT, firewall, and redundancy configurations. This is essential to ensure seamless failover and high availability.

Protocol and Interface Limitations

- Redundancy groups cannot be configured or managed at the individual interface level on the device

  IPv6 cannot be configured on peer interconnect interfaces.
- Because VPN0 is not part of the redundancy group, its NAT translations are not synchronized to the standby device. Control traffic of VPN 0 can be translated using NAT mapping without a redundancy group, as the traffic of VPN 0 is not required to be protected.

NAT DIA

- NAT DIA is supported only in a full mesh topology.
- NAT DIA is supported only with NAT pools; interface or loopback overload is not supported.
- Asymmetric routing in NAT DIA can be addressed by sending influenced routes to attract traffic toward the active redundancy group.
- For NAT DIA configuration in an active-active redundancy group, use the add-on CLI profile.

- For NAT DIA configuration using the add-on CLI profile, multiple NAT methods must be used to configure NAT mappings associated with the redundancy group.
- In an active-active setup with two redundancy groups, the mapping of NAT DIA pools to redundancy groups should be the same as the mapping of VPNs to redundancy groups.

High Availability Features

- Cisco Catalyst SD-WAN firewall high availability configuration and NAT DIA fallback are two ways to ensure high availability. Both features must not be used concurrently.
- The high availability link is expected to be up at all times to handle asymmetric paths.

Configure Cisco Catalyst SD-WAN Firewall High Availability

Configure Cisco Catalyst SD-WAN Firewall High Availability Using Configuration Groups Workflows

The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles. For more information see, Overview of Configuration Group Workflows.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**.
2. Enter a name for your configuration group.
3. Enter the description.
4. Click **Next**
5. Define the site settings and WAN circuits using the **Site Configurations** step.

Field	Description
Site Type	The configuration group type is **Single Router** by default. Choose **Dual Router**. Choose a role for the site: **Edge Site**: Used for branch offices or remote locations. **Border Site**: Used for data centers or central hubs.
Site Settings	Enter site specific values that may be common to other devices in Cisco SD-WAN Manager. **Local Device Access**: Enter a password for local device access. **Message of the Day:** Enter the message content to display important information to users upon login. This can include network policies, maintenance notifications, or security warnings. **Login**: Enter a login banner to display a legal notice or welcome message before the login prompt.

Field	Description
WAN Interfaces	Configure the WAN interfaces for the two Cisco IOS XE Catalyst SD-WAN devices. • **Full Mesh**: Choose this option to configure high availability with NAT DIA. • **Transport Extension**: Choose this option to extend the transport network to additional sites or devices. Choose the IP addressing method for each WAN interface: • **DHCP**: Choose this option for the WAN interface to automatically obtain an IP address from a DHCP server. • **Static IP**: Choose this option to configure the IP address, subnet mask, and gateway for the WAN interface. • **Transport Sharing to Edge Device**: Click tthis option to share the transport network with edge devices for better resource utilization. • **Transport Name**: Enter a name for the transport network. • **Interface Color**: Assign a color to each transport network to visually differentiate them in the Cisco SD-WAN Manager interface. • **Use for Secondary Login**: Choose this option if the WAN interface should be used as a secondary login path for redundancy. This applies when a secondary region is configured in the Network Hierarchy Management. • **Shared with Access Region**: Click this option if the WAN interface should be shared with an access region. • **Exclusive to Secondary Region**: Click this option if the WAN interface should be exclusive to a secondary region. • **Show Advanced**: Configure additional settings for the WAN interface.
WAN Routing	Include WAN routing details with BGP routes, OSPF routes, or multiple static IPv4 routes for your WAN transport VPN. **Note** In the case of NAT, the WAN routing selected here is used to advertise the NAT pool to the ISP
LAN and Service VPN Profile	Enable or disable VRRP settings. **Add Multiple VPNs at Once**: Use the option to add multiple VPNs. **VPN**: Enter a number for the VPN. **Number of Interfaces**: Choose the number of interfaces that will be used for each VPN segment. **Add Routing**: Configure routing protocols and static routes, or both, for each LAN segment. **Show Advanced**: Configure additional settings for the VPN segments.

6. Click **Next**.

7. On the **Additional Features** page, click **Dual Router High Availability** to create a redundancy group using the service VPNs.

   The service VPNs previously created are listed here.

8. Click the VPNs that will participate in high availability.

9. Click on a Cisco IOS XE Catalyst SD-WAN device to designate it as the active device for that VPN. This configures VPN homing, which determines which VPNs will participate in high availability. The following combinations are possible:

   a. **Active-Active**: Distribute the VPNs across two Cisco IOS XE Catalyst SD-WAN devices, resulting in the creation of two redundancy groups.

   b. **Active-Standby**: Assign all VPNs to a single Cisco IOS XE Catalyst SD-WAN device creating one redundancy group.

   c. **None**: Exclude VPNs from participating in high availability by setting their option to None. This means that traffic will be dropped if the active Cisco IOS XE Catalyst SD-WAN device fails.

10. Choose an high availability Interconnect option. The default selection is **Port-Channel** with a single member link, supporting up to two member links. Alternatively, you can choose a standalone interface.

11. Click **Next**.

12. In the **Summary** page, review the high availability configuration, and click **Create Configuration Group**.

Configure Cisco Catalyst SD-WAN Firewall High Availability Using Configuration Groups Feature Profiles

Create Configuration Group for High Availability

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

2. Click **Create Configuration Groups**

3. Enter a name for the configuration group.

4. Enter description for the configuration group.

5. From the **SiteType** drop-down list, choose **Dual Router**.

6. In the **Tag for Edge Device 01** field, enter a name for the first Cisco IOS XE Catalyst SD-WAN device.

   Tag names to identify the devices are displayed by default as **EdgeDevice_01** and **EdgeDevice_02**. To rename the tag names for the devices, click **Edit**.

7. In the **Tag for Edge Device 02** field, enter a name for the second Cisco IOS XE Catalyst SD-WAN device.

8. Click **Create** to create a new configuration group for two Cisco IOS XE Catalyst SD-WAN devices.

Create an Interconnect Interface for High Availability

1. From the **Transport and Management Profile** drop-down list, configure VPN 0 or the WAN VPN.

2. Click + icon next to a transport VPN, and click **Add New Feature**, and then click **Ethernet Interface**.

3. From the **Ethernet Interface** drop-down list, click **Add New** to create a Ethernet interface, which is the interconnect interface.

   The interconnect interface enables synchronization of services, such as firewall and NAT, between the two Cisco IOS XE Catalyst SD-WAN devices. It can be configured as either a physical interface or a port channel interface.

   To create a port channel interface for interconnection, click the **EtherChannel** tab.

4. From the **Ethernet Interface** page, in the **Basic Configuration** tab, enter an interface name.

5. Click the toggle **Use as Dual Router High Availability Interconnect** to enable interconnect on an interface. The interconnect only supports IPv4 addresses.

Note Only one interconnect interface can be created. To create a different interconnect interface, click **Use as Dual Router High Availability Interconnect** to disable the current interconnect. If multiple interconnect interfaces are needed, create a port-channel. For more information on creating a port-channel, see Configure a Transport Side EtherChannel Using a CLI Template.

6. Under **IPv4 Settings**, click to choose an option between **Dynamic** and **Static**.

7. Click **Save on Both Devices**.

Add a Service Profile for High Availability

The Service Profile helps you configure a VPN at LAN level. Add a Service Profile to the configuration group, and then create VPNs for the service profile. For more information about creating VPNs in the Service Profile, see Service VPN.

Configure High Availability

After you have created a service profile with VPNs, do the following:

1. From the Service Profile page, click **Add New Feature**.

2. Choose **Dual Router High Availability** to create a redundancy group using the VPNs from the Service Profile.

3. From the **Dual Router High Availability** drop-down list, click **Add New**.

4. Enter a name and description for the Dual Router High Availability profile.

   The VPNs that you created under the service profile will be listed here. Choose which VPNs will participate in high availability.

5. Click on a Cisco IOS XE Catalyst SD-WAN device to designate it as the active device for that VPN. This configures VPN homing, which determines which VPNs will participate in high availability. The following combinations are possible:

   a. **Active-Active**: Distribute the VPNs across two Cisco Catalyst IOS-XE SD-WAN devices, resulting in the creation of two redundancy groups.

b. **Active-Standby**: Assign all VPNs to a single Cisco Catalyst IOS-XE SD-WAN device, creating one redundancy group.

c. **None**: Exclude VPNs from participating in high availability by setting their option to None. This means that traffic will be dropped if the active Cisco IOS XE Catalyst SD-WAN device fails.

6. Click **WAN symmetry after switchover** to enable traffic from the WAN side to always be directed to the activeCisco IOS XE Catalyst SD-WAN device. This means that peer divert is not necessary, as the traffic will be routed to the active Cisco IOS XE Catalyst SD-WAN device, ensuring efficient and seamless traffic management.

Configure VRRP for Cisco Catalyst SD-WAN Firewall High Availability

To configure VRRP to follow the state of the redundancy group, enable **Follow Dual Router High Availability** in Cisco SD-WAN Manager. This configuration ensures that the VRRP primary role is assigned to the Cisco IOS XE Catalyst SD-WAN device with the active redundancy group, directing LAN-side traffic to the active redundancy group. If the active redundancy group fails, VRRP automatically reassigns the primary role to the device with the new active redundancy group, ensuring continuous service.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Edit the **Service Profile**.
4. Edit an Ethernet interface.
5. Click **VRRP**.
6. Click **Add VRRP IPv4** , and enter the following NAT pool parameters:

Table 99: VRRP Configuration

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100

Parameter Name	Description
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP router. Range: 100 through 40950 milliseconds Default: 100 milliseconds **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface.
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: **Track OMP**: Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. **Track Prefix List**: Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN devices determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP.
Follow Dual Router High Availability	Click to enable VRRP to follow the state of the redundancy group.
VRRP Tracking Object	Enable an object to be tracked and perform an action, either `decrement` or `shutdown` based on the object's status. The Object number represents the interface to be tracked. Range: 1 through 100

7. Click **Add**.

Configure NAT DIA for Cisco Catalyst SD-WAN Firewall High Availability

To configure NAT DIA for high availability, do the following:

1. Create a configuration group with full mesh topology. For more information, see Create Configuration Group for NAT DIA, on page 447.
2. Create NAT Pools for high availability. For more information, see Create NAT Pools for High Availability, on page 449.

Create Configuration Group for NAT DIA

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**.
2. Enter a name for your configuration group.
3. Enter the description.
4. Click **Next**
5. Define the site settings and WAN circuits using the **Site Configurations** step.

Field	Description
Site Type	The configuration group type is **Single Router** by default. Choose **Dual Router**. Choose a role for the site: **Edge Site**: Used for branch offices or remote locations. **Border Site**: Used for data centers or central hubs.
Site Settings	Enter site specific values that may be common to other devices in Cisco SD-WAN Manager. **Local Device Access**: Enter a password for local device access. **Message of the Day:** Enter the message content to display important information to users upon login. This can include network policies, maintenance notifications, or security warnings. **Login**: Enter a login banner to display a legal notice or welcome message before the login prompt.

Field	Description
WAN Interfaces	Configure the WAN interfaces for the two Cisco IOS XE Catalyst SD-WAN devices. • **Full Mesh**: Click full mesh to configure DIA NAT. • **DHCP**: Click DHCP if the WAN interface should obtain an IP address automatically from a DHCP server. • **Static IP**: Click Static IP if you want to manually configure the IP address, subnet mask, and gateway for the WAN interface. • **Transport Name**: Enter a name to the transport network. • **Interface Color**: Assign a color to each transport network to visually differentiate them in the Cisco SD-WAN Manager interface. • **Use for Secondary Login**: Choose this option if the WAN interface should be used as a secondary login path for redundancy. This applies when a secondary region is configured in the Network Hierarchy Management. • **Shared with Access Region**: Click this option if the WAN interface should be shared with an access region. • **Exclusive to Secondary Region**: Click this option if the WAN interface should be exclusive to a secondary region. • **Show Advanced**: Click to configure additional settings for the WAN interface.
WAN Routing	Click **Add Routing** to include WAN routing details with BGP routes, OSPF routes, or multiple static IPv4 routes for your WAN transport VPN. The option you select here is used to advertise the NAT pool to the ISP.
LAN and Service VPN Profile	**Redundancy Protocol**: Click to enable or disable VRRP settings. **Add Multiple VPNs at Once**: Use the option to add multiple VPNs. **VPN**: Enter a number for the VPN. **Number of Interfaces**: Choose the number of interfaces that will be used for each VPN segment. **Add Routing**: Configure routing protocols and static routes for each VPN segment. **Show Advanced**: Click to configure additional settings for the VPN segments.

6. Click **Next**.
7. In the **Additional Features** page, click **Dual Router High Availability** to create a redundancy group using the VPNs.

   The Service VPNs that you created before will be listed here.
8. Click the VPNs that will participate in high availability
9. Click on a Cisco IOS XE Catalyst SD-WAN device to designate it as the active device for that VPN. This configures VPN homing, which determines which VPNs will participate in high availability. The following combinations are possible:

   a. **Active-Active**: Distribute the VPNs across two Cisco IOS XE Catalyst SD-WAN devices, resulting in the creation of two redundancy groups.
   b. **Active-Standby**: Assign all VPNs to a single Cisco IOS XE Catalyst SD-WAN device creating one redundancy group.
   c. **None**: Exclude VPNs from participating in high availability by setting their option to None. This means that traffic will be dropped if the active Cisco IOS XE Catalyst SD-WAN device fails.

10. Choose an high availability Interconnect option. The default selection is **Port Channel** with a single member link, supporting up to two member links. Alternatively, you can choose a standalone interface.
11. Click **Next**.
12. On the **Summary** page, review the high availability configuration, and click **Create Configuration Group**.

Create NAT Pools for High Availability

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Edit the **Transport & Management Profile**.
4. Edit an Ethernet interface.
5. Click **NAT**.
6. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT.
7. Click **Add Multiple NAT** to configure NAT pools.
8. Choose **Pool** as the NAT Type, and enter the following NAT pool parameters:

Table 100: NAT Pool Parameters

Parameter Name	Description
Pool ID	Enter a NAT pool ID.
Range Start	Enter a starting IP address for the NAT pool. a. Change the scope from **Default** to **Global** to enable the field. b. Enter the starting IP address for the NAT pool.
Range End	Enter a closing IP address for the NAT pool. a. Change the scope from **Default** to **Global** to enable the field. b. Enter the last IP address for the NAT pool.
Prefix Length	Enter the NAT pool prefix length.

Parameter Name	Description
Overload	Click to enable per-port translation. The default is **On**. **Note** If **Overload** is set to **Off**, only dynamic NAT is configured on the end device. Per-port NAT is not configured.
Dual Router High Availability Mapping	Click to enable dual router high availability mapping for the NAT pool. Enabling this ensures that traffic using this pool will be translated and protected.

9. Click **Add**.

   Similarly, you can configure high availability for NAT pools for static NAT and port forwarding.

Configure Service-Side NAT for Cisco Catalyst SD-WAN Firewall High Availability

In a service-side NAT for high availability configuration, policies must be configured and VPNs should be associated to redundancy group for high availability. Cisco SD-WAN Manager checks whether a VPN is associated with any redundancy group and if NAT pools are configured as part of the VPN configuration. If the VPN is already associated with an redundancy group, the configured NAT pools for the VPN will be considered. For information on configuring service-side NAT in Cisco SD-WAN Manager, see Configure Service-Side NAT.

Configure Cisco Catalyst SD-WAN Firewall High Availability Using CLI Commands

For information about using the CLI Profile in a configuration group, see CLI Add-On Profile.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure Cisco Catalyst SD-WAN firewall high availability in an active-active redundancy group or in an active-standby redundancy group.

Configure High Availability in an Active-Active Redundancy Group

```
redundancy
 application redundancy
  group group-id
   preempt
```

control *interface-name* **protocol** *protocol-id* **data** *interface-name*

asymmetric-routing interface *interface-name*

asymetric-routing always-divert enable

track *object-number tracker-name*

vpn *vpn-id*

track-enable *track-number*

init-role {**active**|**standby**}

path-optimization

Here’s the complete configuration example for configuring high availability in an active-active redundancy group. The Cisco IOS XE Catalyst SD-WAN device with this configuration defaults to the redundancy group being in standby when both devices come up.

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role active
   path-optimization
  group 2
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 1
   vpn 2
   track-enable 32764
   init-role standby
   path-optimization
```

Here's a sample configuration on the peer Cisco IOS XE Catalyst SD-WAN device.

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role standby
   path-optimization
  group 2
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 1
   vpn 2
   track-enable 32764
   init-role active
   path-optimization
```

Configure High Availability in an Active-Standby Redundancy Group

```
redundancy
 application redundancy
  group group-id
   preempt
   control interface-name protocol protocol-id data interface-name
   asymmetric-routing interface interface-name
   asymmetric-routing interface interface-name
   track object-number tracker-name
   vpn vpn-id
   track-enable track-number
   init-role {active|standby}
   path-optimization
```

Here's the complete configuration example for configuring high availability in an active-standby redundancy group. This Cisco IOS XE Catalyst SD-WAN device is configured to be in the standby state.

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role standby
   path-optimization
```

Here's a sample configuration for the peer Cisco IOS XE Catalyst SD-WAN device in the active state .

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role active
   path-optimization
```

Configure VRRP for High Availability Using CLI Commands

This section provides example CLI configuration to configure VRRP for high availability.

```
interface interface-name
 vrf forwarding vrf-id
 ip address ipv4-address subnet-mask
 no ip redirects
 ip mtu mtu-size
 load-interval interval
 negotiation auto
 ipv6 address ipv6-address
 no ipv6 redirects
 arp timeout timeout-value
 vrrp vrrp-group-id address-family ipv4
  vrrpv2
  track object-number decrement value
  address ipv4-address primary
 exit
 vrrp vrrp-group-id address-family ipv6
  track object-number decrement value
  address ipv6-address primary
  address ipv6-address
 exit
 redundancy rii rii-value
```

Here’s a complete configuration example for configuring VRRP for high availability.

```
interface GigabitEthernet7
 vrf forwarding 5
 ip address 12.168.51.15 255.255.255.0
 no ip redirects
 ip mtu 1496
 load-interval 30
 negotiation auto
 ipv6 address 2001:DB8:1:51::15/64
 no ipv6 redirects
 arp timeout 1200
 vrrp 45 address-family ipv4
  vrrpv2
  track 32763 decrement 10
  address 12.168.51.1 primary
 exit
 vrrp 54 address-family ipv6
  track 32763 decrement 10
  address FE80::1 primary
  address 2001:DB8:51:51::1/64
 exit
 redundancy rii 2053
```

Configure NAT for High Availability Using CLI Commands

Configure NAT DIA for High Availability

1. Configure NAT pool and redundancy.

```
ip nat pool pool-name start-ip end-ip prefix-length prefix-length
ip nat inside source list access-list pool pool-name redundancy
redundancy-group-id mapping-id mapping-id overload match-interface interface-name
ip nat inside source static inside-local-ip inside-global-ip vrf vrf-id
egress-interface interface-name redundancy redundancy-group-id mapping-id
mapping-id
ip nat inside source list access-list interface interface-name overload
```

   Here's the complete configuration example for configuring NAT pool and redundancy.

```
ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
ip nat inside source list dia-list-1 pool natpool1 redundancy 1 mapping-id 8194 overload
 match-interface GigabitEthernet3
ip nat inside source static 201.201.201.12 15.1.1.11 vrf 1 egress-interface
GigabitEthernet3 redundancy 1 mapping-id 7
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet3 overload
```

2. Configure NAT pool and port-forwarding redundancy.

```
ip nat pool pool-name start-ipaddress end-ipaddress prefix-length prefix-length
ip nat inside source list access-list pool pool-name redundancy redundancy-group
 mapping-id mapping-id overload match-interface interface
ip nat inside source static inside-local-ip inside-global-ip vrf vrf-name
egress-interface interface redundancy redundancy-group mapping-id mapping-id
ip nat inside source list access-list interface interface overload
```

   Here's the complete configuration example for configuring NAT pool and redundancy.

```
ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
ip nat inside source list dia-list-1 pool natpool1 redundancy 1 mapping-id 8194 overload
 match-interface GigabitEthernet3
ip nat inside source static 201.201.201.12 15.1.1.11 vrf 1 egress-interface
GigabitEthernet3 redundancy 1 mapping-id 7
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet3 overload
```

3. Policy configuration for NAT DIA and high availability.

```
policy
 data-policy policy-name
  vpn-list vpn-list-name
   sequence sequence-number
    match
     source-ip source-ip-address
     protocol protocol-numbers
    !
    action accept
     nat pool nat-pool-id
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn-list-name
   vpn vpn-id
  !
  site-list site-list-name
   site-id site-id
  !
 !
!apply-policy
 site-list site-list-name
  data-policy policy-name from-service
!
```

Here’s the complete configuration example for policy configuration on Cisco SD-WAN Controller for NAT and high availability.

```
policy
 data-policy b2b-vm1
  vpn-list b2b-vm1
   sequence 101
    match
     source-ip 12.201.201.0/24
     destination-ip 10.0.5.0/24
     protocol 1 6 17
    !
    action accept
     nat use-vpn 0
     nat source-dia-pool 1
    !
   !
  default-action accept
 !
!
lists
 vpn-list b2b-vm1
  vpn 1
 !
 site-list site100
  site-id 100
 !
!
apply-policy
 site-list site100
  data-policy b2b-vm1 all
!
!
```

4. NAT DIA interface configuration.

```
interface interface-name
 ip address ip-address subnet-mask
 ip nat outside
 negotiation auto
 ipv6 address ipv6-address
 ipv6 enable
 ipv6 nd ra suppress all
 redundancy rii rii-id
```

Here's a complete configuration about interface setup with NAT and redundancy.

```
interface GigabitEthernet3
 ip address 10.0.5.11 255.255.255.0
 ip nat outside
 negotiation auto
 ipv6 address 2001:A0:5::B/64
 ipv6 enable
 ipv6 nd ra suppress all
 redundancy rii 350
```

Configure Service-Side NAT for High Availability

1. Configure NAT pool and redundancy.

   ip nat pool *pool-name start-ip end-ip* **prefix-length** *prefix-length*
   ip nat inside source static *inside-local-ip inside-global-ip* **vrf** *vrf-id* **match-in-vrf redundancy** *redundancy-group-id* **mapping-id** *mapping-id* **pool** *pool-name*
   ip nat inside source list *access-list* **pool** *pool-name* **redundancy** *redundancy-group-id* **mapping-id** *mapping-id* **vrf** *vrf-id* **match-in-vrf overload**

   Here's the complete configuration example for configuring service-side NAT for high availability.

   ```
   ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
   ip nat inside source static 192.168.11.2 15.1.1.5 vrf 1 match-in-vrf redundancy 1
   mapping-id 11 pool natpool1
   ip nat inside source list global-list pool natpool1 redundancy 1 mapping-id 5 vrf 1
   match-in-vrf overload
   ```

2. Configure NAT pool and port-forwarding redundancy.

   ip nat pool *pool-name start-ipaddress end-ip* **prefix-length** *prefix-length*
   ip nat inside source static *protocol inside-local-ip local-port inside-global-ip global-port* **vrf** *vrf-id* **match-in-vrf redundancy** *redundancy-group-id* **mapping-id** *mapping-id* **pool** *pool-name*
   ip nat inside source list *access-list* **pool** *pool-name* **redundancy** *redundancy-group-id* **mapping-id** *mapping-id* **vrf** *vrf-id* **match-in-vrf overload**

   Here's the complete configuration example for configuring NAT pool and redundancy.

   ```
   ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
   ip nat inside source static udp 192.168.11.2 2558 15.1.1.11 2558 vrf 1 match-in-vrf
   redundancy 1 mapping-id 87 pool natpool1
   ip nat inside source list global-list pool natpool1 redundancy 1 mapping-id 5 vrf 1
   match-in-vrf overload
   ```

3. Policy configuration for service-side NAT and high availability.

   ```
   policy
    data-policy policy-name
     vpn-list vpn-list-name
      sequence sequence-number
       match
        source-ip source-ip-address
        protocol protocol-numbers
       !
       action accept
        nat pool nat-pool-id
       !
      !
      default-action accept
     !
   ```

```
 !
 lists
  vpn-list vpn-list-name
   vpn vpn-id
  !
  site-list site-list-name
   site-id site-id
  !
 !
!apply-policy
 site-list site-list-name
  data-policy policy-name from-service
!
```

Here’s the complete configuration example for policy configuration on Cisco SD-WAN Controller for NAT and high availability.

```
policy
 data-policy vm1
  vpn-list vm1
   sequence 20
    match
     source-ip 20.201.201.0/24
     protocol 1 6 17
    !
    action accept
     nat pool 1
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vm1
   vpn 1
  !
  site-list vm1
   site-id 100
  !
 !
!
apply-policy
 site-list vm1
  data-policy vm1 from-service
!
```

Note If you want to disable the application redundancy feature, and there are existing NAT configurations that rely on this redundancy, you must remove those NAT configurations first. Only after removing the NAT configurations can you proceed to disable the application redundancy.

Verify High Availability

Verify Redundacy Groups

The following is a sample output from the **show redundancy application group** command. This command provides detailed information about the redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, showing their redundancy group IDs, redundancy group names, and current states (active or standby). This information helps to monitor and manage high availability and failover configurations effectively.

```
Device# show redundancy application group
Group ID Group Name      State

1   Generic-Redundancy-1 STANDBY
2   Generic-Redundancy2 ACTIVE
```

The following is a sample output from the **show redundancy application group** command with group id. This command provides information about the specified redundancy application group on a Cisco IOS XE Catalyst SD-WAN device. It includes the administrative and operational states, roles of the current and peer devices, communication status, path optimization, and redundancy framework states.

```
Device# show redundancy application group 1
Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE

Device# show redundancy application group 2
Group ID:2
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

The following is a sample output from the **show redundancy application group all** command. This command provides information about all redundancy application groups configured on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# show redundancy application group all
Faults states Group 1 info:
Runtime priority: [100]
RG Faults RG State: Up.
Total # of switchovers due to faults:           0
Total # of down/up state changes due to faults: 0

RG Protocol RG 1

Role: Standby
    Init Role: Standby
    Negotiation Flags 0x1
    Tunnel: UP, DIA: DOWN
    Negotiation: Enabled
    Priority: 100
    Protocol state: Standby-hot
    Ctrl Intf(s) state: Up
    Active Peer: address 10.1.55.15, priority 100, intf Po1
    Standby Peer: Local
    Log counters:
            role change to active: 1
            role change to standby: 1
            disable events: rg down state 0, rg shut 0
            ctrl intf events: up 2, down 1, admin_down 0
            reload events: local request 0, peer request 0


RG Media Context for RG 1
Ctx State: Standby
    Protocol ID: 1
    Media type: Default
    Control Interface: Port-channel1
    Current Hello timer: 3000
    Configured Hello timer: 3000, Hold timer: 10000
    Peer Hello timer: 3000, Peer Hold timer: 10000
    Stats:
            Pkts 10, Bytes 620, HA Seq 0, Seq Number 10, Pkt Loss 0
            Authentication not configured
            Authentication Failure: 0
            Reload Peer: TX 0, RX 0
            Resign: TX 1, RX 0
    Active Peer: Present. Hold Timer: 10000
            Pkts 3, Bytes 102, HA Seq 0, Seq Number 7, Pkt Loss 0


Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE

Faults states Group 2 info:
Runtime priority: [100]
```

```
RG Faults RG State: Up.
Total # of switchovers due to faults:           0
Total # of down/up state changes due to faults: 0


RG Protocol RG 2
Role: Active
    Init Role: Active
    Negotiation Flags 0x1
    Tunnel: UP, DIA: DOWN
    Negotiation: Enabled
    Priority: 100
    Protocol state: Active
    Ctrl Intf(s) state: Up
    Active Peer: Local
    Standby Peer: address 10.1.55.15, priority 100, intf Po1
    Log counters:
            role change to active: 1
            role change to standby: 0
            disable events: rg down state 0, rg shut 0
            ctrl intf events: up 2, down 1, admin_down 0
            reload events: local request 0, peer request 0



RG Media Context for RG 2
Ctx State: Active
    Protocol ID: 1
    Media type: Default
    Control Interface: Port-channel1
    Current Hello timer: 3000
    Configured Hello timer: 3000, Hold timer: 10000
    Peer Hello timer: 3000, Peer Hold timer: 10000
    Stats:
            Pkts 8, Bytes 496, HA Seq 0, Seq Number 8, Pkt Loss 0
            Authentication not configured
            Authentication Failure: 0
            Reload Peer: TX 0, RX 0
            Resign: TX 0, RX 1
    Standby Peer: Present. Hold Timer: 10000
            Pkts 4, Bytes 136, HA Seq 0, Seq Number 9, Pkt Loss 0


Group ID:2
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

Verify Protocol Details of Redundancy Groups

Examples

The following is sample output from the **show redundancy application group protocol** command.

```
Device# show redundancy application group protocol

RG Protocol RG 1
------------------
        Role: Active
        Init Role: Active
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.1.55.14, priority 100, intf Po1
        Log counters:
                role change to active: 11
                role change to standby: 7
                disable events: rg down state 3, rg shut 0
                ctrl intf events: up 5, down 2, admin_down 1
                reload events: local request 1, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 10001, Bytes 620062, HA Seq 0, Seq Number 10001, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 7385, Bytes 251090, HA Seq 0, Seq Number 10004, Pkt Loss 0



RG Protocol RG 2
------------------
        Role: Standby
        Init Role: Standby
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Standby-hot
        Ctrl Intf(s) state: Up
        Active Peer: address 10.1.55.14, priority 100, intf Po1
        Standby Peer: Local
        Log counters:
                role change to active: 3
                role change to standby: 3
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0
```

```
RG Media Context for RG 2
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 7396, Bytes 458552, HA Seq 0, Seq Number 7396, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 2
        Active Peer: Present. Hold Timer: 10000
                Pkts 7177, Bytes 244018, HA Seq 0, Seq Number 7394, Pkt Loss 0
```

This example verifies the protocol-specific details of application redundancy groups such as the current role (active or standby), status of control interfaces, negotiation flags, priorities, and peer details. The example also verifies the status of tunnels and Direct Internet Access (DIA), log counters for various events, and media context settings, including hello and hold timers. Additionally, it provides statistics on packet and byte counts, sequence numbers, packet loss, and authentication status.

Verify Redundancy Group Interfaces

The following is sample output from the **show redundancy application control-interface group** command.

```
Device# show redundancy application control-interface group 1

The control interface for rg[1] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0

The control interface for rg[2] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0
```

This example shows **`Port-channel1`** is the control interface for redundancy groups 1 **`(rg[1])`** and 2 **`(rg[2])`**. The interface is associated with protocol ID 1 and has BFD enabled.

The following is sample output from the **show redundancy application data-interface group** command.

```
Device# show redundancy application data-interface group

The data interface for rg[1] is Port-channel1
The data interface for rg[2] is Port-channel1
```

In this example, the command output indicates that the data interface for both redundancy group 1 (rg[1]) and redundancy group 2 (rg[2]) is Port-channel1. This setup ensures that Port-channel1 is used to handle the data traffic for both redundancy groups, facilitating efficient traffic management and high availability.

Verify Redundancy Interface Identifiers Configuration

The following is sample output from the **show redundancy rii** command.

```
Device# show redundancy rii
No. of RIIs in database: 10
 Interface                         RII Id     decrement
  GigabitEthernet3.104          :   2049         0
  GigabitEthernet3.103          :   2050         0
  GigabitEthernet3.102          :   2051         0
  GigabitEthernet7              :   2053         0
  GigabitEthernet3.105          :   2054         0
  Tunnel2                       :   513          0
  Tunnel1                       :   514          0
  GigabitEthernet3.101          :   2052         0
  GigabitEthernet2              :   1            0
  GigabitEthernet1              :   2            0
```

In this example, there are 10 RIIs in the database. The table lists each interface along with its associated RII ID and decrement value, which is 0 for all entries. The interfaces include various GigabitEthernet ports and Tunnel interfaces, each uniquely identified by an RII. This information helps in managing high availability by mapping and associating interfaces accurately within redundancy groups.

Verify Firewall Datapath in Redundancy Groups

The following is sample output from the **show platform hardware qfp active feature firewall datapath rg** command.

```
Device# show platform hardware qfp active feature firewall datapath rg 1

rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Stats were all zero

==== HA active stat ====
Total received messages 1
Session create requests 5
Session delete requests 5
Bulksync requests received 1
Bulksync complete 1
Session sync attempt: create 5
Session sync attempt: delete 5

==== HA standby stat ====
Stats were all zero
```

In this example, the command output shows that redundancy group 1 is active, with all transport and flow mechanisms operational. The high availability general statistics indicate no retries were necessary, suggesting stable synchronization. The active statistics reveal that session creation and deletion requests are being processed efficiently, and bulksync operations are functioning correctly. The standby statistics show no activity, which is typical in a stable high availability setup. This detailed information helps ensure seamless failover and maintain high availability in the network.

The following is sample output from the **show platform hardware qfp active feature firewall datapath rg 1 all** command.

```
Device#  show platform hardware qfp active feature firewall datapath rg 1 all
rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Total retry allocations 0
Retry allocation failures 0
Total retry entries queued 0
Flow on 0
Flow off 0
Retry timeout 0

==== HA active stat ====
Total received messages 1
Missing RII 0
Session create requests 5
Session delete requests 5
Session update requests 0
Bulksync requests received 1
Bulksync complete 1
L7 buffers allocated 0
L7 buf alloc failure 0
Failed to send L7 data 0
L7 data sent 0
Invalid opcode recvd 0
Message too short 0
Bad version number 0
Bad magic number 0
Create NAKs received 0
No HA buffer 0
No buffer false positive 0
Session sync attempt: create 5
Session sync attempt: update 0
Session sync attempt: delete 5
Session sync attempt: l7 data 0
vrf mapping failures 0
Invalid protocol 0
PAM classificaiton failure 0
Classificaiton failure 0
Could not find parent flow 0
Asymmetric routing injection 0
Data transport down 0
Bad bulk sync feature id 0
Bad bulk sync message length 0
Bulk sync error: init not complete 0
Bulk sync - active now standby 0
Bulk sync - Standby not read 0
Transport Down 0
Attempt to initiate bulk sync on active 0
Invalid no response bulk sync timer on active 0
Bulk sync request retry re-queued 0
Bulk sync request retry re-queue failed 0
Bulk sync done re-queued 0
Bulk sync done re-queue failed 0

==== HA standby stat ====
Total received messages 0
Session create requests 0
Session delete requests 0
Session update requests 0
```

```
Create NAK sent 0
Inspection policy not found 0
Could not create session 0
Could not create subordinate session 0
New sessions not allowed 0
Could not locate ingress uidb RII 0
Could not locate egress uidb RII 0
RG not configured 0
Could not locate uidb sub-block 0
Invalid zone - no inspection 0
Invalid zone - drop 0
Invalid zone pair 0
Classification failed 0
Classification results missing stats 0
Subflow RG mismatch 0
RG mismatch on create/flow exists 0
Could not find session 0
Session RG mismatch 0
Session delete miss 0
Session delete RG mismatch 0
Layer 7 data 0
Rcvd bad opcode 0
Msg too short 0
Unsupported msg version 0
Bulk sync requested 0
Bulk sync requested timeout 0
Bulk sync requested failed 0
Bulk Sync msg sent 0
Bulk sync complete 0
Peer not identified 0
Could not allocate msg buffer 0
Could not find VRF 0
Asymmetric routing redirect 0
Asymmetric routing redirect failed - no uidb_sb 0
Asymmetric routing redirect failed - no AR 0
Transport Down 0
Bulk sync failed : no response 0
Existing session removed/replaced 0
Invalid message magic number 0
```

In this example, the output displays all statistics using the `all` option in the command, providing detailed insights into the current state and performance metrics of both the active and standby components of the High Availability system. The high availability system is functioning correctly, with the active component efficiently handling requests and synchronization processes, while the standby component remains prepared without any errors or issues.

Verify Firewall Session Information in High Availability Environments

The following is sample output from the **show policy-firewall session platform detail** command.

```
Device# show policy-firewall session platform detail

[s=session  i=imprecise channel c=control channel  d=data channel u=utd inspect A/D=appfw
action allow/deny]
Session ID:0x100000B7 192.168.11.10 34157 10.0.12.131 80 proto 6 (1:1:1:1) (3:0x3000050:http)
 [sc]
 pscb : 0x156da640,  key1_flags: 0x00000000
 bucket : 34590, prev 0x0, next 0x0    fw_flags: 0x01800000 0x20c06a21,
  Flattened-AVC HA-AVC
  Root Protocol-TCP Initiator Alert Proto-State:Timewait Session-db HA-create Max-session
    icmp_error count 0 ureachable arrived: no
    scb state: active, nxt_timeout: 100, refcnt: 1 NBAR verdict count 0
    ha nak cnt: 0, rg: 1
    hostdb: 0x0, L7: 0x0, stats: 0x160ebfc0, child: 0x0
    isn:        1826966309 last ack:       987459709 next seq:         1826966394 wnd_size:
          2169783926
 wnd_scale:         29200
    isn:         987459708    last ack:        987459708    next ack:        987459708
wnd_size:          2169783926
 wnd_scale:         65535
    tcp flags:     0x00000000 :  : proto: 0018: l7 ooo drop 0x010 l7_prot 0x12 - http
    root scb: 0x0 act_blk: 0x160e3f00
    ingress/egress intf: GigabitEthernet3.101 (65530), GigabitEthernet1 (65530)
   current time 284036397554511 create tstamp: 283915721110241 last access: 284035994128283
 now 284036397556361 csec left
    nat_out_local_addr:port: 10.0.12.131:80
    nat_in_global_addr:port: 101.101.101.101:34157
    ip6: addr1 :: addr2 ::
    key ip4: addr1 10.0.12.131:80 addr2 192.168.11.10:34157
    syncookie fixup: 0x0,  halfopen linkage: 0x0 0x0
    cxsc_cft_fid: 0x00000000
    tw timer: 0x00000000 0x00000000 0x00000000 0x14f53101
    domain_ab1 0x0 l4 per filter stats 0x0 avc class id 0x3 http SGT: 0 DGT: 0
    NAT handles 0x11194110 0x00000000
    FlowDB in2out 0x00000000 alloc_epoch 0 out2in 0x00000000 alloc_epoch 0 ppe tid 0
    icmp_err_time 0 utd_context_id 0, classification epoch scb: 0x1 actblk :0x1 avc class
stats 0x0
    VPN id src 1, dst 0
    zone pair ZP_ZONE_1_untrusted_ZON_47132514 class
ZONE_1_TO_UNTRUSTED-seq-SEQUENCE-829881385-cm_
```

In this example, the command **show policy-firewall session platform detail** provides detailed information about firewall sessions on the device, particularly when high availability is involved. This command is used to gather comprehensive data about active firewall sessions, including session states, counters, and other important metrics.

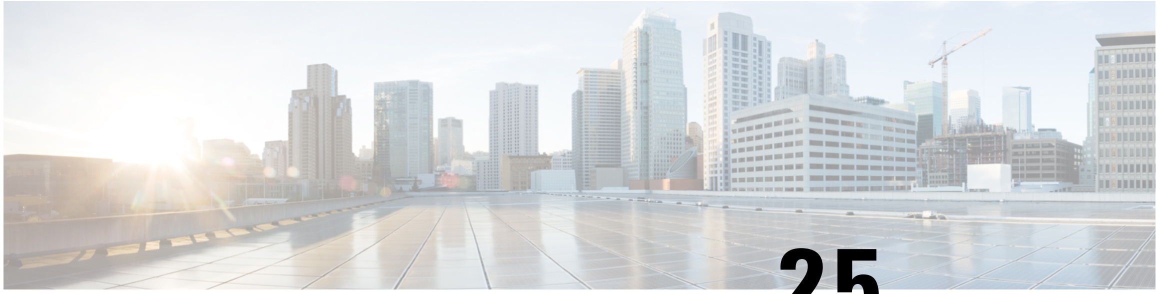
Monitor Firewall High Availability

You can monitor the traffic or applications using Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Locate the device that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the left pane, click **Real Time**.
5. From the **Device Options** drop-down list in the right pane, choose **Redundancy Group App Group**. This option allows you to view detailed information about the redundancy groups configured on the selected device.

View Network Site Topology

Cisco SD-WAN Manager provides a visual representation of the network topology for each site, featuring the Cisco IOS XE Catalyst SD-WAN devices deployed in a high-availability configuration. Cisco SD-WAN Manager displays the topology of the chosen site, illustrating the interconnected devices and their roles within the high-availability configuration. For more information, see View Network Site Topology.



CHAPTER 25

Security CLI Reference

CLI commands for configuring and monitoring security.

Security CLI Templates

The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allows you to configure intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager. Intent-based CLI template refer to the command line interface configuration that are based on the vEdge device syntax. Using CLI templates, Cisco SD-WAN Manager enables pushing vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN devices in Cisco IOS XE syntax.

Table 101: Security Policy for UTD

CLI Template Configuration	Configuration on the Device

```
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[&lt;h3&gt;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
  !
 !
!
```

CLI Template Configuration	Configuration on the Device
	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

CLI Template Configuration	Configuration on the Device
	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&gt;Access to the requested page has been denied&lt;/h3&gt;&lt;p&gt;Please contact your Network Administrator&lt;/p&gt;]]> ! web-filter url profile url_filter categories block games ! block page-profile block-url_filter log level error reputation block-threshold moderate-risk ! ! threat-inspection profile intrusion_policy threat protection policy connectivity logging level err ! utd global ! policy utd-policy-vrf-1 all-interfaces vrf 1 threat-inspection profile intrusion_policy web-filter url profile url_filter exit !

Security Monitoring Commands

- **show control connections**

CHAPTER 26

Regular Expression for URL Filtering and DNS Security

Regular Expressions

A regular expression is a pattern (a phrase, number, or more complex pattern) the CLI String Search feature matches against show or more command output. Regular expressions are case-sensitive and allow for complex matching requirements. Simple regular expressions include entries like Serial, misses, or 138. Complex regular expressions include entries like 00210... , (is), or [Oo]utput.

A regular expression can be a single-character pattern or a multiple-character pattern. That is, a regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. The pattern in the command output is referred to as a string. This section describes creating both single-character patterns and multiple-character patterns. It also discusses creating more complex regular expressions using multipliers, alternation, anchoring, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. The table below lists the keyboard characters that have special meaning.

Table 102: Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
$	Matches the end of the string.

Character	Special Meaning
_(underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis (( ), right parenthesis ( )), the beginning of the string, the end of the string, or a space.

To use these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). The following examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively.

\$ _ \+

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. Only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([]). For example,

[aeiou]matches any one of the five vowels of the lowercase alphabet, while [abcdABCD] matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the endpoints of the range separated by a dash (-). Simplify the previous range as follows:

[a-dA-D]

To add a dash as a single-character pattern in your range, include another dash and precede it with a backslash:

[a-dA-D\-]

You can also include a right square bracket (]) as a single-character pattern in your range, as shown here:[a-dA-D\-\]]

The previous example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket.

You can reverse the matching of the range by including a caret (^) at the start of the range. The following example matches any letter except the ones listed:

[^a-dqsv]

The following example matches anything except a right square bracket (]) or the letter d:

[^\]d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression. Insert a backslash before the keyboard characters that have special meaning when you want to indicate that the character should be interpreted literally.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, in that order, pattern matching fails. The multiple-character regular expression a.uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of the period character by inserting a backslash before it. For example, when the expression a\. is used in the command syntax, only the string a. will be matched.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. For example, telebit3107v32bis is a valid regular expression.

Multipliers

You can create more complex regular expressions that instruct Cisco IOS software to match multiple occurrences of a specified regular expression. To do so, you use some special characters with your single-character and multiple-character patterns. The table below lists the special characters that specify “multiples” of a regular expression.

Table 103: Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single-character or multiple-character patterns.
+	Matches 1 or more single-character or multiple-character patterns.
?	Matches 0 or 1 occurrences of a single-character or multiple-character pattern.

The following example matches any number of occurrences of the letter a, including none:

a*

The following pattern requires that at least one letter a be in the string to be matched:

a+

The following pattern matches the string bb or bab:

ba?b

The following string matches any number of asterisks (*):

**

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, the following pattern matches one or more instances of alphanumeric pairs, but not none (that is, an empty string is not a match):

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Exactly one of the alternatives can match the string. For example, the regular expression codex|telebit matches the string codex or the string telebit, but not both codex and telebit.

Anchoring

You can instruct Cisco IOS software to match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contain a specific pattern. You “anchor” these regular expressions to a portion of the string using the special characters shown in the table below.

Table 104: Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string.
$	Matches the end of the string.

For example, the regular expression ^conmatches any string that starts with con, and $sole matches any string that ends with sole.

In addition to indicating the beginning of a string, the ^ symbol can be used to indicate the logical function “not” when used in a bracketed range. For example, the expression **[^abcd]** indicates a range that matches any single letter, as long as it is not the letters a, b, c, or d.

Contrast these anchoring characters with the special character underscore (_). Underscore matches the beginning of a string (^), the end of a string ($), parentheses (( )), space ( ), braces ({}), comma (,), or underscore (_). With the underscore character, you can specify that a pattern exist anywhere in the string. For example,

_1300_ matches any string that has 1300 somewhere in the string. The string 1300 can be preceded by or end with a space, brace, comma, or underscore. So, although {1300_matches the regular expression **_1300_**, 21300 and 13000 do not.

Using the underscore character, you can replace long regular expression lists. For example, instead of specifying **^1300()()1300${1300,,1300,{1300},1300,(1300** you can specify simply **_1300_**.

Parentheses for Recall

As shown in the “Multipliers” section, you use parentheses with multiple-character regular expressions to multiply the occurrence of a pattern. You can also use parentheses around a single- or multiple-character pattern to instruct the Cisco IOS software to remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, you use parentheses to indicate memory of a specific pattern and a backslash (\) followed by a number to reuse the remembered pattern. The number specifies the occurrence of a parentheses in the regular expression pattern. If you have more than one remembered pattern in your regular expression, then \1 indicates the first remembered pattern, and \2 indicates the second remembered pattern, and so on.

The following regular expression uses parentheses for recall:

a(.)bc(.)\1\2

This regular expression matches an a followed by any character (call it character no. 1), followed by bc followed by any character (character number 2), followed by character no. 1 again, followed by character number. 2 again. So, the regular expression can match aZbcTZT. The software remembers that character number 1 is Z and character number 2 is T and then uses Z and T again later in the regular expression.

CHAPTER 27

Troubleshoot Cisco Catalyst SD-WAN Security

Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following are the support articles associated with this technology:

Document	Description
Collect an Admin-Tech in Cisco Catalyst SD-WAN Environment and Upload to TAC Case	This document describes how to initiate an `admin-tech` in a Cisco Catalyst SD-WAN environment.
Collect SAML-Trace and HAR File	This document describes how to initiate an **SAML-Trace** and **HAR File** in a Cisco Catalyst SD-WAN environment.

Document	Description
Configure and Verify SD-WAN IPsec SIG Tunnel with Zscaler	This document describes the configuration steps and verification of SD-WAN IPsec SIG tunnels with Zscaler.
Configure Cisco Catalyst SD-WAN Advanced Malware Protection (AMP) Integration and Troubleshoot	This document describes how to configure and troubleshoot the Cisco Catalyst SD-WAN Advanced Malware Protection (AMP) integration on a cEdge device with Cisco IOS® XE, as an integral part of the Cisco Catalyst SD-WAN edge security solution that aims visibility and protection for users at a branch from Malware.
Configure Cisco Catalyst SD-WAN Zone-Based Firewall (ZBFW) and Route Leaking	This document describes how to configure, verify and troubleshoot Zone-Based Firewall (ZBFW) with Route-Leaking between Virtual Private Networks (VPN).
Configure Integration with Cisco Umbrella and Troubleshooting Common Problems	This document describes Cisco SD-WAN Manager/Cisco IOS®-XE SDWAN software part of the integration with the Cisco Umbrella DNS security solution.
Configure OKTA Single Sign-On (SSO) on Cisco Catalyst SD-WAN	This document describes how to integrate OKTA Single Sign-On (SSO) on Cisco Catalyst SD-WAN.
Configure Service Side IPSec Tunnel with a C8000V on Cisco Catalyst SD-WAN	This document describes how to configure an IPSec tunnel between a SD-WAN Cisco Edge Router and a VPN Endpoint with service VRF.
Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios	This document describes how to configure Cisco Umbrella Secure Internet Gateway (SIG) tunnels with IPsec in both Active/Active and Active/Standby
Install and Uninstall UTD Engine in Cisco Catalyst SD-WAN with CLI	This document describes the procedure to install and uninstall Unified Threat Defense (UTD) via CLI in Cisco Catalyst SD-WAN routers.
Install UTD Security Virtual Image on cEdge Routers	This document describes how to install Unified Threat Defense (UTD) Security Virtual Image to enable security features on Cisco IOS XE Catalyst SD-WAN Devices.
SD-WAN Manager: How to Check and Verify Single Sign On	This document describes the basics in order to enable Single Sign On (SSO) on Cisco SD-WAN Manager and how to check/verify on Cisco SD-WAN Manager, when this feature is enabled
Troubleshoot Cisco IOS XE Catalyst SD-WAN Router IPsec Anti-Replay Failures	This document describes the IPsec Anti-Replay behavior in SD-WAN IPsec for Cisco IOS XE SD-WAN routers and how to troubleshoot Anti-Replay issues.
Troubleshoot Datapath Handling by UTD and URL-Filtering	This document describes how to troubleshoot Unified Threat Defense (UTD) also known as Snort and Uniform Resource Locator (URL) Filtering on IOS® XE WAN Edges routers.
Understand SD-WAN and Traditional Tunnels SPI Recover Differences	This document describes how to recover SD-WAN and Third Party Tunnels from %RECVD_PKT_INV_SPI error.

Feedback Request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the **Feedback** button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

Disclaimer and Caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.