Security Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20

First Published: 2019-05-23

Last Modified: 2021-12-17

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

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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 SD-WAN Release 20

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 Catalyst SD-WAN

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

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

CHAPTER 3

Security Overview

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

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

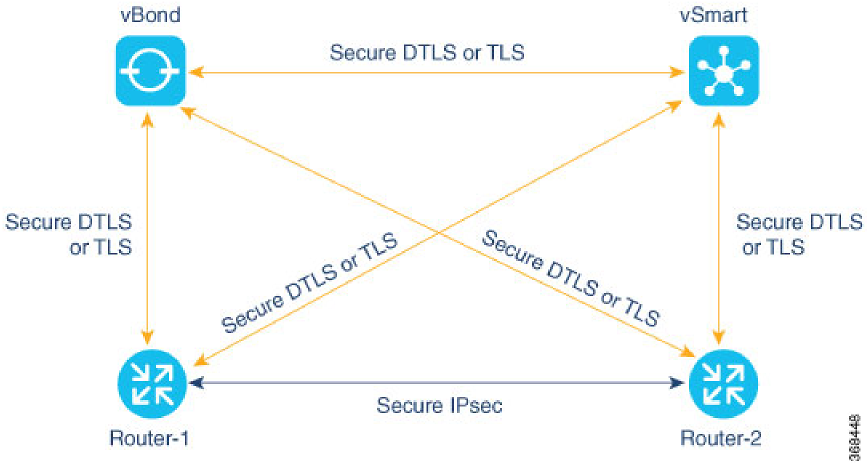
This chapter contains the following topics:

Cisco SD-WANSecurity Components

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

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

These three components—authentication, encryption, and integrity—are key to securing the Cisco SD-WAN overlay network infrastructure.



The topics on Control Plane Security Overview and Data Plane Security Overview examine how authentication, encryption, and integrity are implemented throughout the Cisco SD-WAN overlay network. The security discussion refers to the following illustration of the components of the Cisco SD-WAN network—the 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.

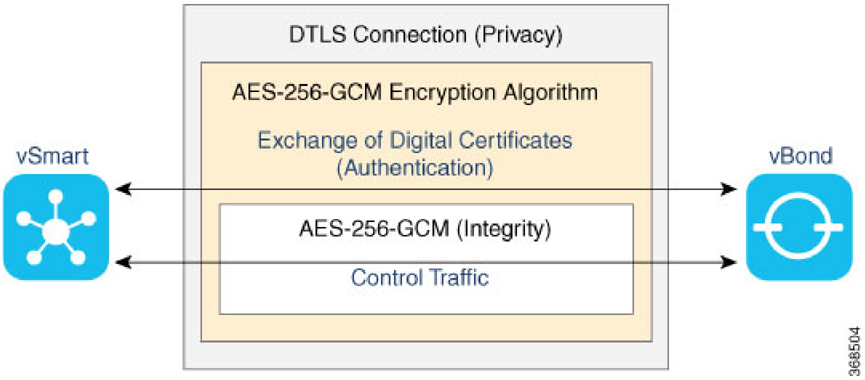
Control Plane Security Overview

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.

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)
vSmart
vBond
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.

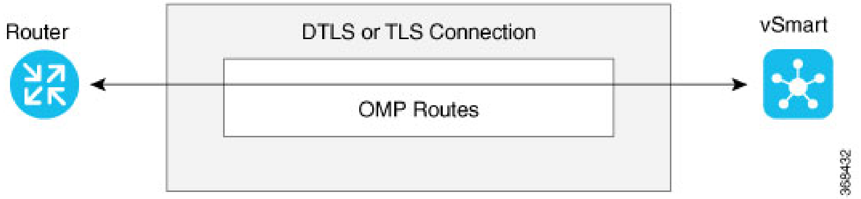
DTLS and TLS Infrastructure

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

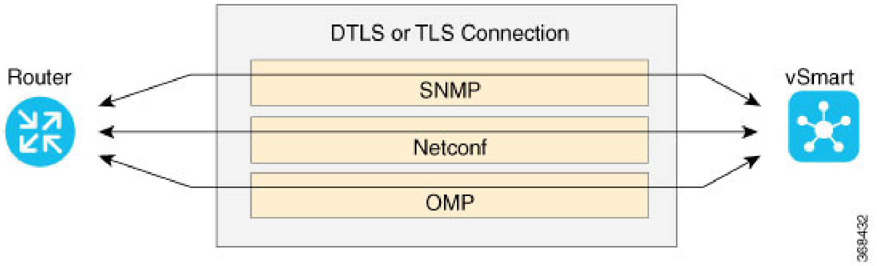
The first is the DTLS protocol, which is a transport privacy protocol for connectionless datagram protocols such as UDP, provides the foundation for the Cisco Catalyst SD-WAN control plane infrastructure. It is based on the stream-oriented Transport Layer Security (TLS) protocol, which provides security 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 SD-WAN control plane uses digital certificates with 2048-bit RSA keys to authenticate the Cisco vEdge 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 vEdge device and cannot be retrieved from the Cisco vEdge device.
- **Certificates** signed by a root certification authority (CA)— The trust chain associated with the root CA needs to be present on all Cisco vEdge 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.

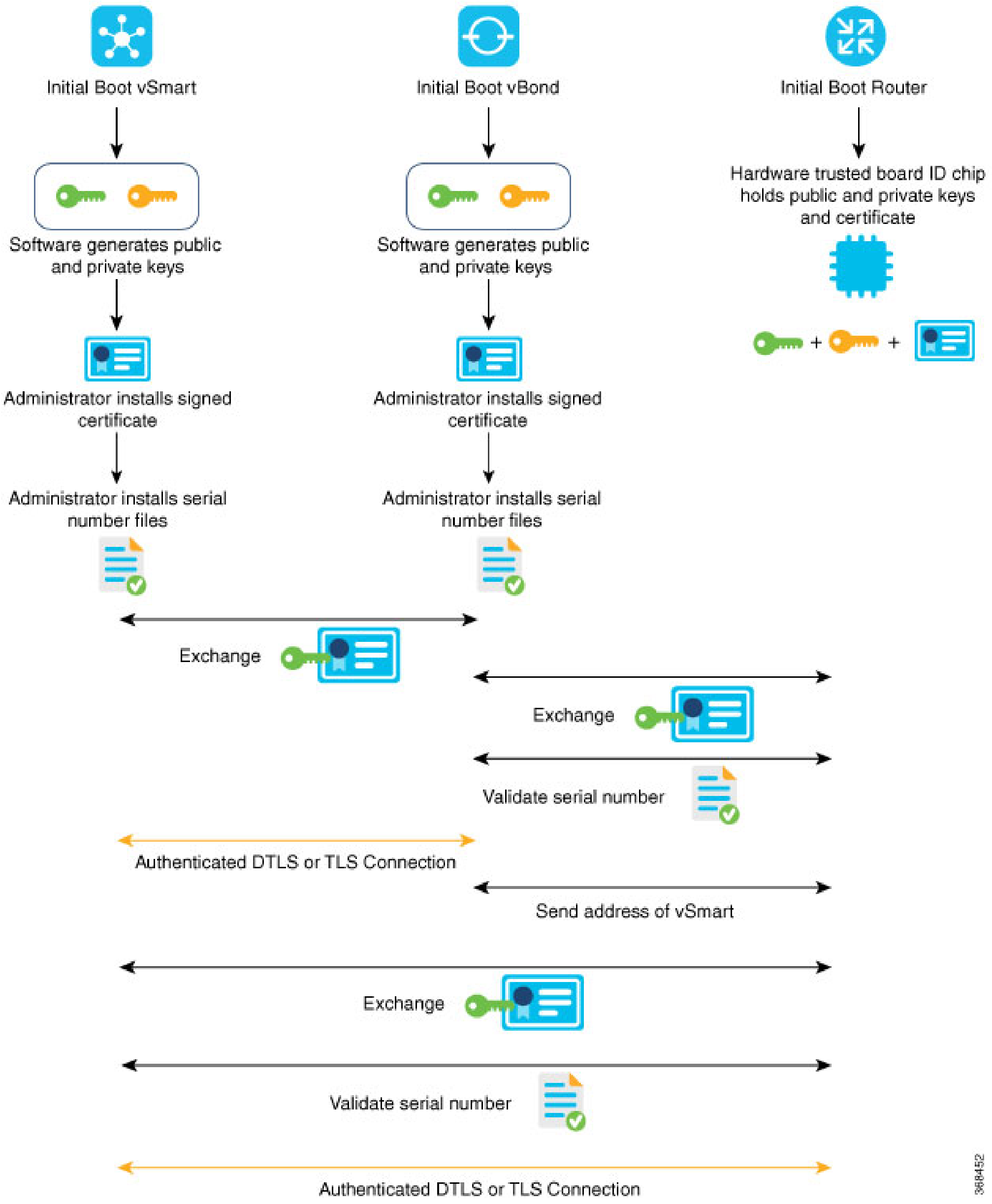
Let's first look at the PKI components that are involved in router authentication. On vEdge 100, 1000, and 2000 routers, the public and private keys and the certificates are managed automatically, by a Trusted Board ID chip that is built into the router. For vEdge 5000, instead of a Trusted Board ID chip, a Trusted Platform Module (TPM) is used. 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 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 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 or a router 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.

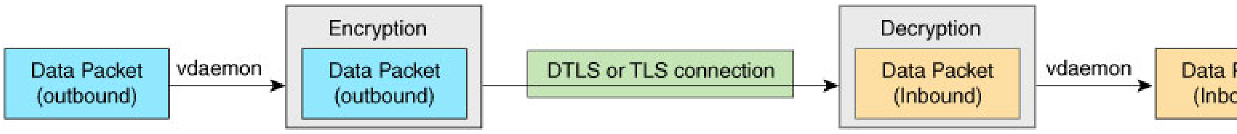
Now, let's look at how the PKI authentication components and the router serial and chassis numbers are used to authenticate router on the Cisco SD-WAN Controller overlay network. When Cisco SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and routers first boot up, they establish secure DTLS or 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 vSmart
Initial Boot vBond
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 vSmart
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

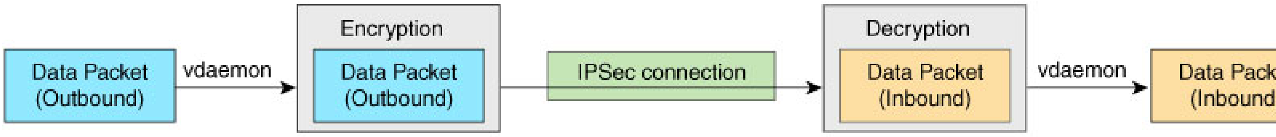
The data plane of any network is responsible for handling data packets that are transported across the network. The data plane is also sometimes called the forwarding plane. In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they 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 64.
  - 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.

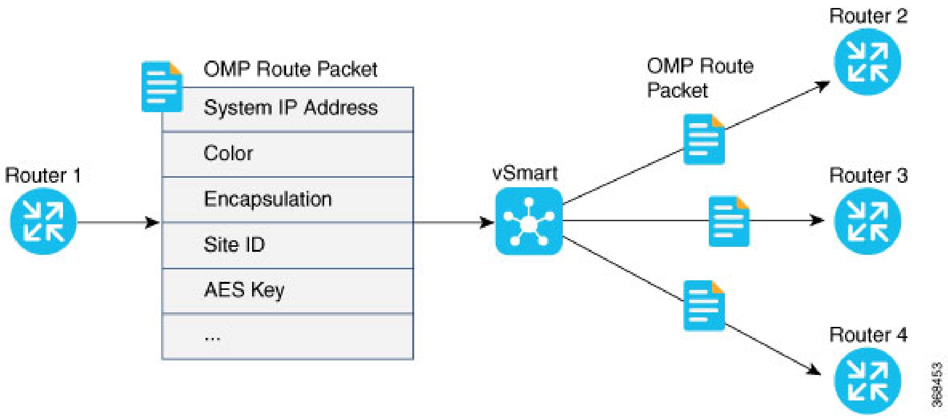
The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- 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 63



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:

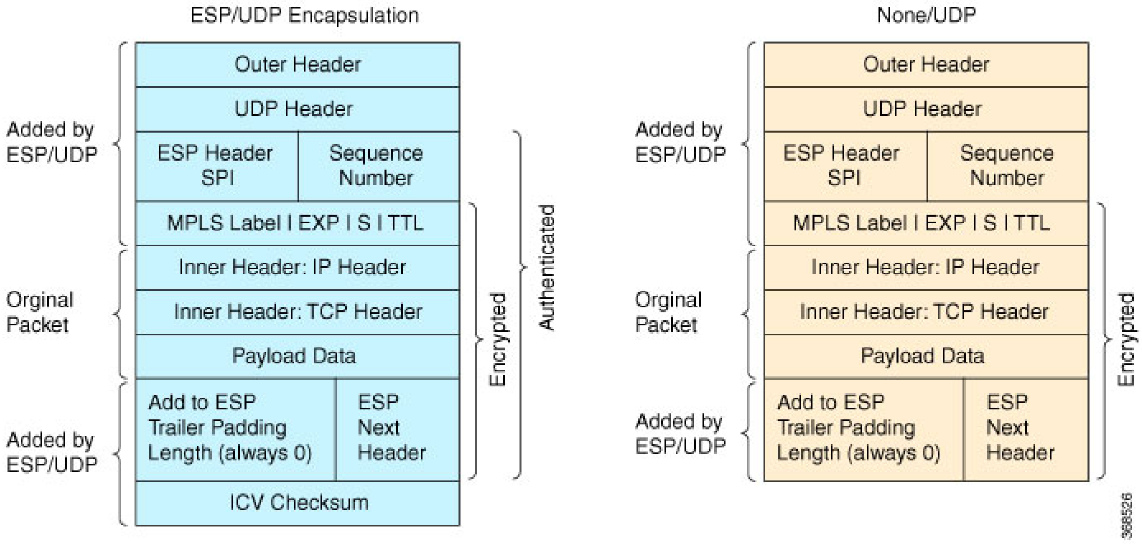
- UDP – Encapsulate ESP within UDP packets per RFC 3948, UDP Encapsulation of IPsec ESP packets.
- ESP, which is a standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets. SDWAN complies with RFC 4303, 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.

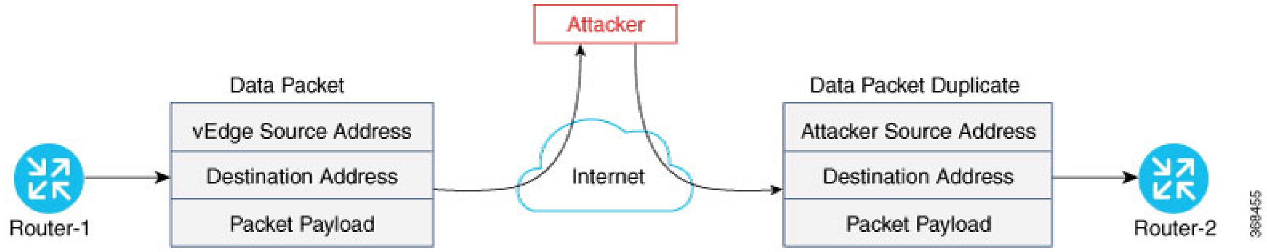
In the Cisco Catalyst SD-WAN solution, there are also enhancements to ESP to enhance its behavior to cover more of the datagram. These enhancements are similar to the way that AH works. This enhancement performs a checksum that includes calculating the checksum over all the fields in the packet—the payload,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

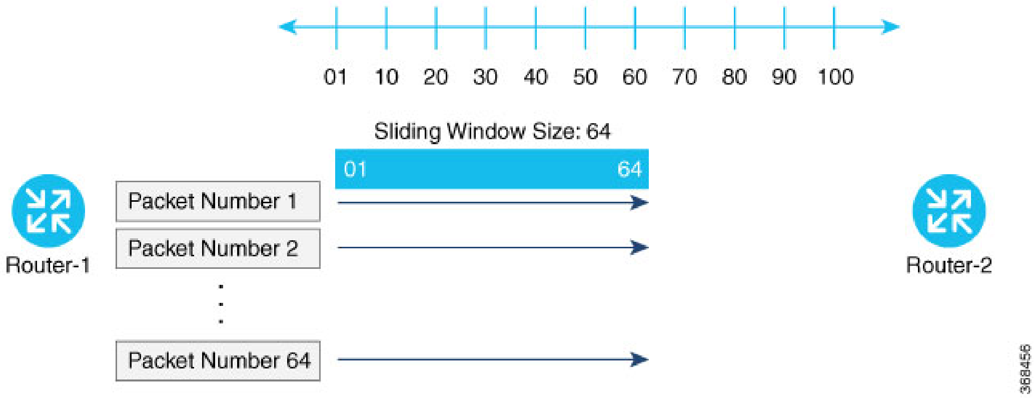


Note that Cisco Catalyst SD-WAN devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the digest. Both are distributed as part of the TLOC properties for a router.

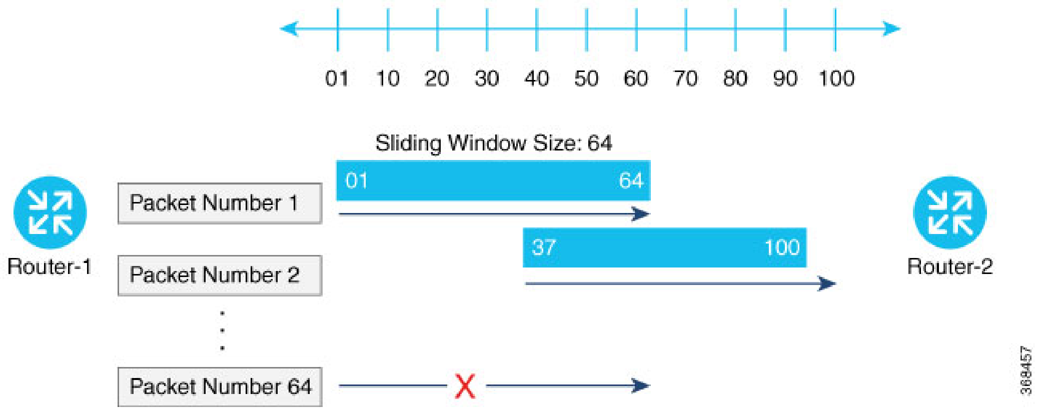
Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this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



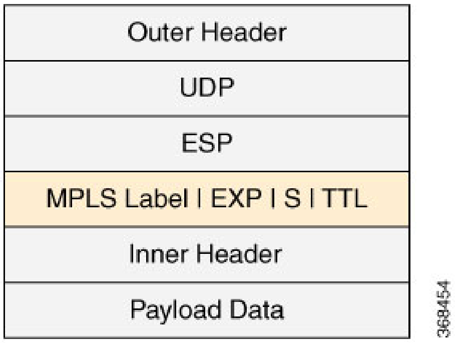
As a counter to such attacks, the Cisco Catalyst SD-WAN overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets.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

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

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

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 Security feature template for all Cisco vEdge 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 **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 1:

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.

Parameter Scope	Scope Description
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 2:

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

To configure data plane security on a Cisco SD-WAN Validator or a Cisco vEdge router, choose the **Basic Configuration** and **Authentication Type** tabs, and configure the following parameters:

Table 3:

Parameter Name	Description
Rekey Time	Specify how often a Cisco vEdge router 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
IPsec pairwise-keying	This is turned off by default. Click **On** to turn it on.

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 SD-WAN Release 20.6.1: • **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 SD-WAN Release 20.5.1 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 SD-WAN Release 20.5.1 or earlier, you may have configured authentication types using a **Security** template. When you upgrade the device to Cisco SD-WAN Release 20.6.1 or later, update the selected authentication types in the **Security** template to the authentication types supported from Cisco SD-WAN Release 20.6.1. 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 **Security** template to update and click … and click **Edit**. **4.** Click **Update**. Do not modify any configuration. Cisco SD-WAN Manager updates the **Security** template to display the supported authentication types.

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 SD-WAN Release 20.6.1 and Later

From 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 or to disable integrity check, use the following command:

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

Authentication Types Before Cisco SD-WAN Release 20.6.1

By default, IPsec tunnel connections use an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication. To modify the negotiated authentication types or to disable authentication, use the following command:

```
Device(config)# security ipsec authentication-type (ah-sha1-hmac | ah-no-id | sha1-hmac |
| none)
```

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. Except for the encryption of multicast traffic, the authentication algorithms supported by Cisco Catalyst SD-WAN do not use SHA1. However in Cisco SD-WAN Release 20.1.x and onwards, both unicast and multicast 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.
- **none** maps to no authentication. This option should only be used if it is required for temporary debugging. You can also choose this option in situations where data plane authentication and integrity are not a concern. Cisco does not recommend using this option for production networks.

For information about which data packet fields are affected by these authentication types, see Data Plane Integrity, on page 14.

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.

The encryption algorithm on IPsec tunnel connections depends on the type of traffic:

- For unicast traffic, the encryption algorithm is AES-256-GCM.
- For multicast traffic:
  - Cisco SD-WAN Release 20.1.x and later– the encryption algorithm is AES-256-GCM
  - Previous releases– the encryption algorithm is AES-256-CBC with SHA1-HMAC.

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 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 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 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 security ipsec-rekey
Device# show 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
```

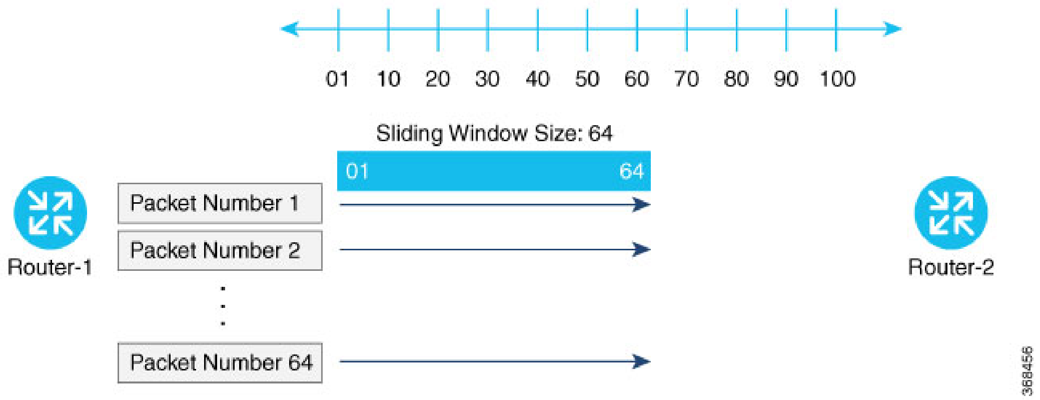
After the new key is generated, the router sends it immediately to the Cisco SD-WAN Controllers using DTLS or TLS. The Cisco SD-WAN Controllers send the key to the peer routers. The routers begin using it as soon as they receive it. Note that the key associated with the old SPI (256) will continue to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

To stop using the old key immediately, issue the **request 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.

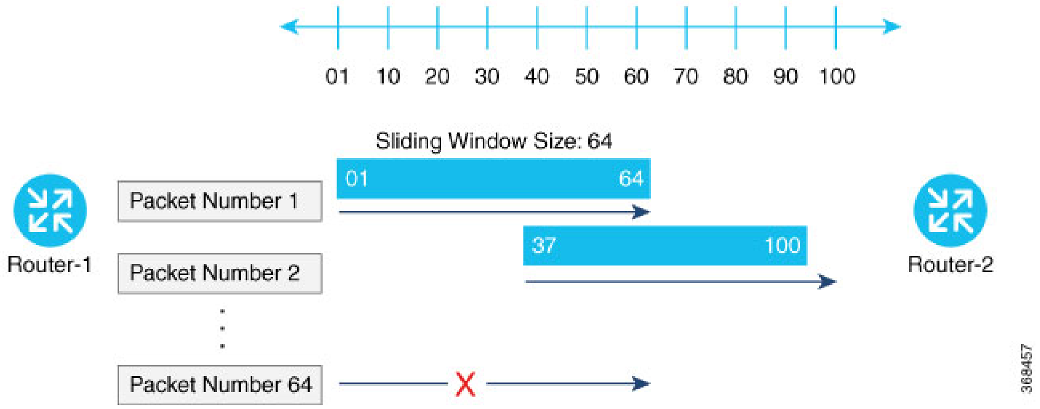
```
Device# request security ipsec-rekey
Device# request security ipsec-rekey
Device# ipsec local-sa
                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
-----------------------------------------------------------------------------
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.

Configure IKE-Enabled IPsec Tunnels

To securely transfer traffic from the overlay network to a service network, you can configure IPsec tunnels that run the Internet Key Exchange (IKE) protocol. IKE-enabled IPsec tunnels provide authentication and encryption to ensure secure packet transport.

You create an IKE-enabled IPsec tunnel by configuring an IPsec interface. IPsec interfaces are logical interfaces, and you configure them just like any other physical interface. You configure IKE protocol parameters on the IPsec interface, and you can configure other interface properties.

Note Cisco recommends using IKE Version 2.

Note From Cisco SD-WAN 19.2.x release onwards, the pre-shared key needs to be at least 16 bytes in length. The IPsec tunnel establishment fails if the key size is less than 16 characters when the router is upgraded to version 19.2.

The Cisco Catalyst SD-WAN software supports IKE Version 2 as defined in RFC 7296.

One use for IPsec tunnels is to allow vEdge Cloud router VM instances running on Amazon AWS to connect to the Amazon virtual private cloud (VPC). You must configure IKE Version 1 on these routers.

Note Cisco vEdge devices support only route-based VPNs in an IPSec configuration because these devices cannot define traffic selectors in the encryption domain.

Configure an IPsec Tunnel

To configure an IPsec tunnel interface for secure transport traffic from a service network, you create a logical IPsec interface:

```
vEdge(config)# vpn vpn-id interface ipsecnumber
vEdge(config-interface-ipsec)# ip address ipv4-prefix/length
vEdge(config-interface-ipsec)# tunnel-source ip-address | tunnel-source-interface
interface-name)
vEdge(config-interface-ipsec)# tunnel-destination ipv4-address
vEdge(config-interface-ipsec)# no shutdown
```

You can create the IPsec tunnel in the transport VPN (VPN 0) and in any service VPN (VPN 1 through 65530, except for 512).

The IPsec interface has a name in the format **ipsec***number*, where *number* can be from 1 through 255.

Each IPsec interface must have an IPv4 address. This address must be a /30 prefix. All traffic in the VPN that is within this IPv4 prefix is directed to a physical interface in VPN 0 to be sent securely over an IPsec tunnel.

To configure the source of the IPsec tunnel on the local device, you can specify either the IP address of the physical interface (in the **tunnel-source** command) or the name of the physical interface (in the **tunnel-source-interface** command). Ensure that the physical interface is configured in VPN 0.

To configure the destination of the IPsec tunnel, specify the IP address of the remote device in the **tunnel-destination** command.

The combination of a source address (or source interface name) and a destination address defines a single IPsec tunnel. Only one IPsec tunnel can exist that uses a specific source address (or interface name) and destination address pair.

Configure an IPsec Static Route

To direct traffic from the service VPN to an IPsec tunnel in the transport VPN (VPN 0), you configure an IPsec-specific static route in a service VPN (a VPN other than VPN 0 or VPN 512) :

```
vEdge(config)# vpn vpn-id
vEdge(config-vpn)# ip ipsec-route prefix/length vpn 0 interface
ipsecnumber [ipsecnumber2]
```

The VPN ID is that of any service VPN (VPN 1 through 65530, except for 512).

prefix/length is the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.

The interface is the IPsec tunnel interface in VPN 0. You can configure one or two IPsec tunnel interfaces. If you configure two, the first is the primary IPsec tunnel, and the second is the backup. With two interfaces, all packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.

Enable IKE Version 1

When you create an IPsec tunnel on a vEdge router, IKE Version 1 is enabled by default on the tunnel interface. The following properties are also enabled by default for IKEv1:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours
- SA establishment mode—Main

By default, IKEv1 uses IKE main mode to establish IKE SAs. In this mode, six negotiation packets are exchanged to establish the SA. To exchange only three negotiation packets, enable aggressive mode:

Note IKE aggressive mode with pre-shared keys should be avoided wherever possible. Otherwise a strong pre-shared key should be chosen.

```
vEdge(config)# vpn vpn-id interface ipsec number ike
vEdge(config-ike)# mode aggressive
```

By default, IKEv1 uses Diffie-Hellman group 16 in the IKE key exchange. This group uses the 4096-bit more modular exponential (MODP) group during IKE key exchange. You can change the group number to 2 (for 1024-bit MODP), 14 (2048-bit MODP), or 15 (3072-bit MODP):

```
vEdge(config)# vpn vpn-id interface ipsec number ike
vEdge(config-ike)# group number
```

By default, IKE key exchange uses AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. You can change the authentication:

```
vEdge(config)# vpn vpn-id interface ipsec number ike
vEdge(config-ike)# cipher-suite suite
```

The authentication *suite* can be one of the following:

- **aes128-cbc-sha1**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- **aes128-cbc-sha2**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity
- **aes256-cbc-sha1**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity; this is the default.
- **aes256-cbc-sha2**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity

By default, IKE keys are refreshed every 1 hours (3600 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds). It is recommended that the rekeying interval be at least 1 hour.

```
vEdge(config)# vpn vpn-id interface ipsec number ike
vEdge(config-ike)# rekey seconds
```

To force the generation of new keys for an IKE session, issue the **request ipsec ike-rekey** command.

```
vEdge(config)# vpn vpn-id interfaceipsec number ike
```

For IKE, you can also configure preshared key (PSK) authentication:

```
vEdge(config)# vpn vpn-id interface ipsec number ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret password
```

password is the password to use with the preshared key. It can be an ASCII or a hexadecimal string from 1 through 127 characters long.

If the remote IKE peer requires a local or remote ID, you can configure this identifier:

```
vEdge(config)# vpn vpn-id interface ipsec number ike authentication-type
vEdge(config-authentication-type)# local-id id
vEdge(config-authentication-type)# remote-id id
```

The identifier can be an IP address or any text string from 1 through 63 characters long. By default, the local ID is the tunnel's source IP address and the remote ID is the tunnel's destination IP address.

Enable IKE Version 2

When you configure an IPsec tunnel to use IKE Version 2, the following properties are also enabled by default for IKEv2:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours

By default, IKEv2 uses Diffie-Hellman group 16 in the IKE key exchange. This group uses the 4096-bit more modular exponential (MODP) group during IKE key exchange. You can change the group number to 2 (for 1024-bit MODP), 14 (2048-bit MODP), or 15 (3072-bit MODP):

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# group number
```

By default, IKE key exchange uses AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. You can change the authentication:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# cipher-suite suite
```

The authentication *suite* can be one of the following:

- **aes128-cbc-sha1**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- **aes128-cbc-sha2**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity
- **aes256-cbc-sha1**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity; this is the default.
- **aes256-cbc-sha2**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity

By default, IKE keys are refreshed every 4 hours (14,400 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds):

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)#  rekey seconds
```

To force the generation of new keys for an IKE session, issue the **request ipsec ike-rekey** command.

For IKE, you can also configure preshared key (PSK) authentication:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret password
```

password is the password to use with the preshared key. It can be an ASCII or a hexadecimal string, or it can be an AES-encrypted key.

If the remote IKE peer requires a local or remote ID, you can configure this identifier:

```
vEdge(config)# vpn vpn-id interface ipsecnumber ike authentication-type
vEdge(config-authentication-type)# local-id id
vEdge(config-authentication-type)# remote-id id
```

The identifier can be an IP address or any text string from 1 through 64 characters long. By default, the local ID is the tunnel's source IP address and the remote ID is the tunnel's destination IP address.

Configure IPsec Tunnel Parameters

Table 4: Feature History

Feature Name	Release Information	Description
Additional Cryptographic Algorithmic Support for IPSec Tunnels	Cisco SD-WAN Release 20.1.1	This feature adds support for `HMAC_SHA256`, `HMAC_SHA384`, and `HMAC_SHA512` algorithms for enhanced security.

By default, the following parameters are used on the IPsec tunnel that carries IKE traffic:

- Authentication and encryption—AES-256 algorithm in GCM (Galois/counter mode)
- Rekeying interval—4 hours
- Replay window—32 packets

You can change the encryption on the IPsec tunnel to the AES-256 cipher in CBC (cipher block chaining mode, with HMAC using either SHA-1 or SHA-2 keyed-hash message authentication or to null with HMAC using either SHA-1 or SHA-2 keyed-hash message authentication, to not encrypt the IPsec tunnel used for IKE key exchange traffic:

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# cipher-suite (aes256-gcm | aes256-cbc-sha1 | aes256-cbc-sha256 |
aes256-cbc-sha384 | aes256-cbc-sha512 | aes256-null-sha1 | aes256-null-sha256 |
aes256-null-sha384 | aes256-null-sha512)
```

By default, IKE keys are refreshed every 4 hours (14,400 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds):

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)#  rekey seconds
```

To force the generation of new keys for an IPsec tunnel, issue the **request ipsec ipsec-rekey** command.

By default, perfect forward secrecy (PFS) is enabled on IPsec tunnels, to ensure that past sessions are not affected if future keys are compromised. PFS forces a new Diffie-Hellman key exchange, by default using the 4096-bit Diffie-Hellman prime module group. You can change the PFS setting:

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# perfect-forward-secrecy pfs-setting
```

pfs-setting can be one of the following:

- **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. This is the default.
- **none**—Disable PFS.

By default, the IPsec replay window on the IPsec tunnel is 512 bytes. You can set the replay window size to 64, 128, 256, 512, 1024, 2048, or 4096 packets:

```
vEdge(config-interface-ipsecnumber)# ipsec
vEdge(config-ipsec)# replay-window number
```

Modify IKE Dead-Peer Detection

IKE uses a dead-peer detection mechanism to determine whether the connection to an IKE peer is functional and reachable. To implement this mechanism, IKE sends a Hello packet to its peer, and the peer sends an acknowledgment in response. By default, IKE sends Hello packets every 10 seconds, and after three unacknowledged packets, IKE declares the neighbor to be dead and tears down the tunnel to the peer. Thereafter, IKE periodically sends a Hello packet to the peer, and re-establishes the tunnel when the peer comes back online.

You can change the liveness detection interval to a value from 0 through 65535, and you can change the number of retries to a value from 0 through 255.

Note For transport VPNs, the liveness detection interval is converted to seconds by using the following formula:

Interval for retransmission attempt number N = *interval* * 1.8^{N-1}

For example, if the interval is set to 10 and retries to 5, the detection interval increases as follows:

- Attempt 1: 10 * 1.8^{1-1}= 10 seconds
- Attempt 2: 10 * 1.8^{2-1}= 18 seconds
- Attempt 3: 10 * 1.8^{3-1}= 32.4 seconds
- Attempt 4: 10 * 1.8^{4-1}= 58.32 seconds
- Attempt 5: 10 * 1.8^{5-1}= 104.976 seconds

```
vEdge(config-interface-ipsecnumber)# dead-peer-detection interval retries number
```

Configure Other Interface Properties

For IPsec tunnel interfaces, you can configure only the following additional interface properties:

```
vEdge(config-interface-ipsec)# mtu bytes
vEdge(config-interface-ipsec)# tcp-mss-adjust bytes
```

Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Table 5: 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.

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

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

Enterprise Firewall

Table 6: Feature History

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

Overview of Enterprise Firewall

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

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

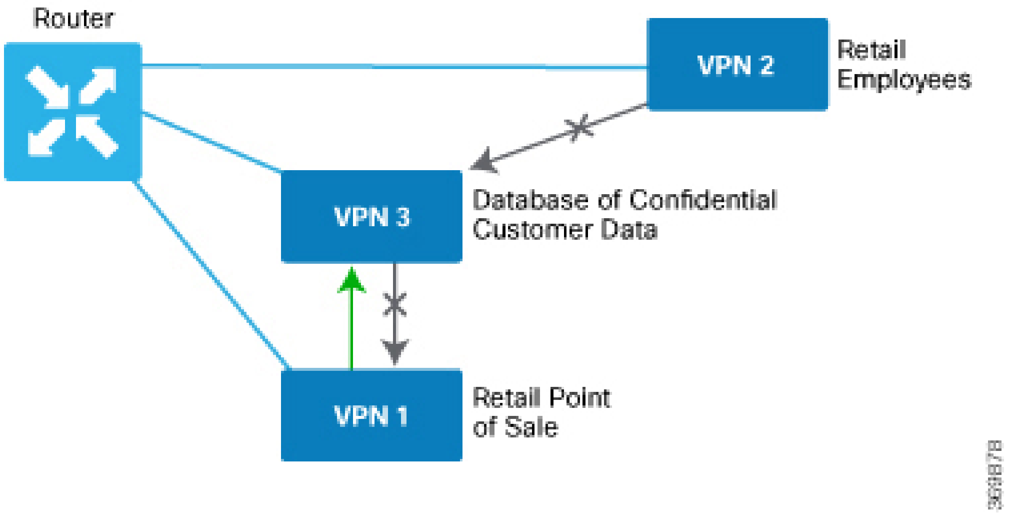
Zone configuration consists of the following components:

- Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- Firewall policy—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP. 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.
- 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.



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 behaviour 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.

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 – Create rules that you apply in the match condition of a firewall policy.

  Rules 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).

- 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.

.

Note The following policy components are not supported on Cisco vEdge devices.

- Source port list(s)
- Destination port list(s)
- Protocol list
- FDQN list
- Geolocation list
- Application list
- Rule sets

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

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. Choose an action for the rule:
   - **Inspect**
   - **Pass**
   - **Drop**
8. If you want matches for this rule to be logged, check the **Log** check box.
9. Configure one or more of the following fields.

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

Table 7: Firewall Rules

Field	Description
Source Data Prefixes	IPv4 prefixes or IPv6 prefixes or prefix lists .
Source Port(s)	Source port(s) and/or lists
Destination Data Prefix(es)	IPv4 prefixes or prefix list(s)

Field	Description
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)

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

11. (Optional) Repeat steps 4–10 to add more rules.

12. Click **Save Firewall Policy**.

Apply Policy to a Zone Pair

Table 8: Feature History

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	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.

Note On a Cisco vEdge device, packets to and from the management interface under VPN 512 do not go through the firewall module.

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.

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. 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**.

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**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose the **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time** in the left pane. A pop-up window appears with **Device Options**.
4. Click **Search**, and choose **Policy Zone Based Firewall Statistics** from the list to view the statistics for the firewall policies.

Note Firewall Charts and Policy statistics are not currently supported for Cisco vEdge devices from **Network** > **Firewall** dashboard. However, detailed statistics are available when you navigate from the Cisco SD-WAN Manager menu **Network** > **Real Time**.

Zone-Based Firewall Configuration Examples

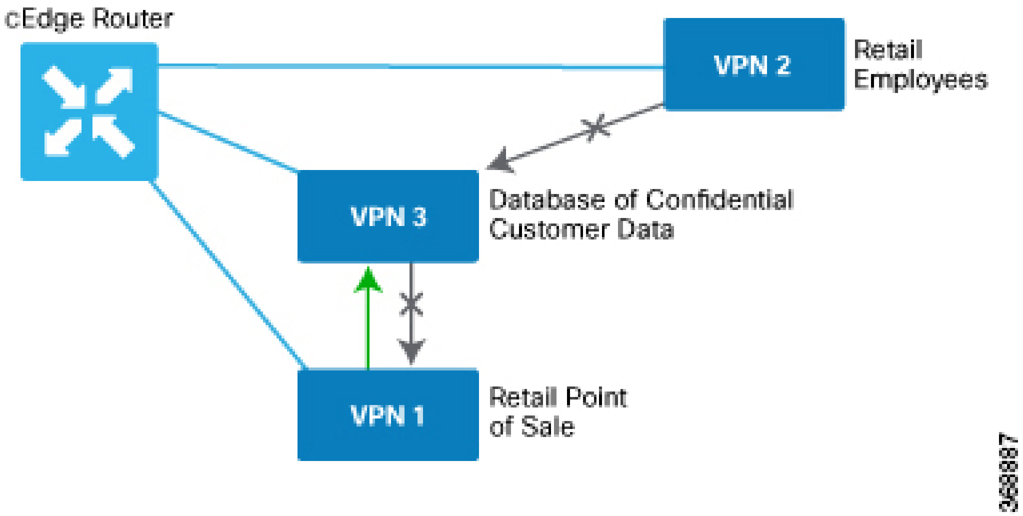
This topic provides an example of configuring a simple zone-based firewall using the CLI template or Cisco SD-WAN Manager.

Isolating Two VPNs

In this zone-based firewall configuration example, we have a scenario where a router is connected to three service-side networks:

- Guest network that provides point-of-sale (PoS) services
- Employee network
- Network that provides shared services, including shared printers and the customer database

We want users in the employee and guest networks to be able to access the shared services, but we do not want any traffic to be exchanged between the employee and guest networks. Similarly, we do not want any traffic that originates in the shared services network to enter into either the employee network or the guest network. The following figure illustrates this scenario:



In this figure:

- VPN 1 is the guest network used for PoS services.
- VPN 2 is the network used by the enterprise's employees.
- VPN 3 contains the shared services, including printers and customer databases.

The configuration consists of three sections:

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

CLI Configuration

First, we define the zones for this scenario:

```
vEdge(config)# policy
vEdge(config-policy)# zone pos-zone vpn 1
vEdge(config-policy)# zone employee-zone vpn 2
vEdge(config-policy)# zone services-zone vpn 3
```

In this simple example, each zone corresponds to a single VPN. If you were to later add a second VPN for a discrete group of employees (let's say this is VPN 20) and you wanted this VPN to be subject to the same firewall policy, you could simply add this VPN to the employee zone:

```
vEdge(config-policy)# zone employee-zone vpn 20
vEdge(config-policy)# show full-configuration
policy zone employee-zone
  vpn 2
  vpn 20
 !
!
```

Next, we configure the zone-based firewall policy. The policy matches all traffic that is destined for VPN 3, which is the services zone, and which has an IP prefix of 10.2.2.0/24. Because we want the policy to allow traffic to flow from VPN 1 and VPN 2 to VPN 3, but we do not want traffic to flow in the reverse direction, we set the action to **pass**.

```
vEdge(config-policy)# zone-based-policy vpn-isolation-policy(config-zone-based-policy)#
sequence 10(config-sequence)# match destination-ip 10.2.2.0/24
vEdge(config-sequence)# action pass
```

We want to drop any traffic that does not match the zone-based filrewall policy:

```
vEdge(config-zone-based-policy)# default-action drop
```

In the final step of the configuration process, we apply the zone-based firewall policy to the zones. Here is the zone pairing between the guest and PoS zone and the services zone:

```
vEdge(config-policy)# zone-pair pos-services-pairing
vEdge(config-zone-pair)# source-zone pos-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-policy vpn-isolation-policy
```

And here is the pairing between the employee zone and the services zone:

```
vEdge(config-policy)# zone-pair employee-services-pairing
vEdge(config-zone-pair)# source-zone employee-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-pair employee-services-pairing
```

Here is a view of the entire policy:

```
vEdge(config-policy)# show full-configuration
 policy
 zone employee-zone
  vpn 2
! zone pos-zone
  vpn 1
 ! zone services-zone
  vpn 3
!
zone-pair employee-services-pairing
  source-zone      employee-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
zone-pair services-pairing
  source-zone      pos-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
zone-based-policy vpn-isolation-policy
  sequence 10
   match
   destination-ip 10.2.2.0/24
  !
   action pass
  !
!
 default-action drop
!
!
```

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.

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.

CHAPTER 6

Cisco Umbrella Integration

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

Table 9: Feature History

Feature Name	Release Information	Description
Extended DNS (EDNS) and Local Domain Bypass Support with Cisco Umbrella Integration	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature enables cloud-based security service on Cisco vEdge devices by inspecting the DNS query. Once the DNS query is inspected, action is taken on it based on whether the query is for a local domain or an external domain.

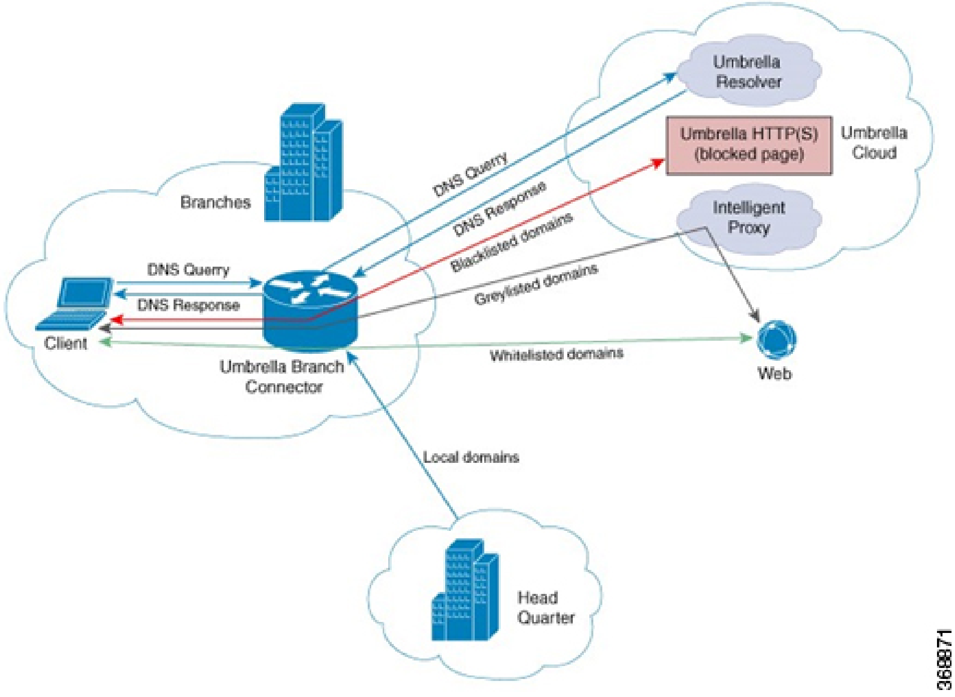
Overview of Cisco Catalyst SD-WAN Umbrella Integration

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 3: 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.

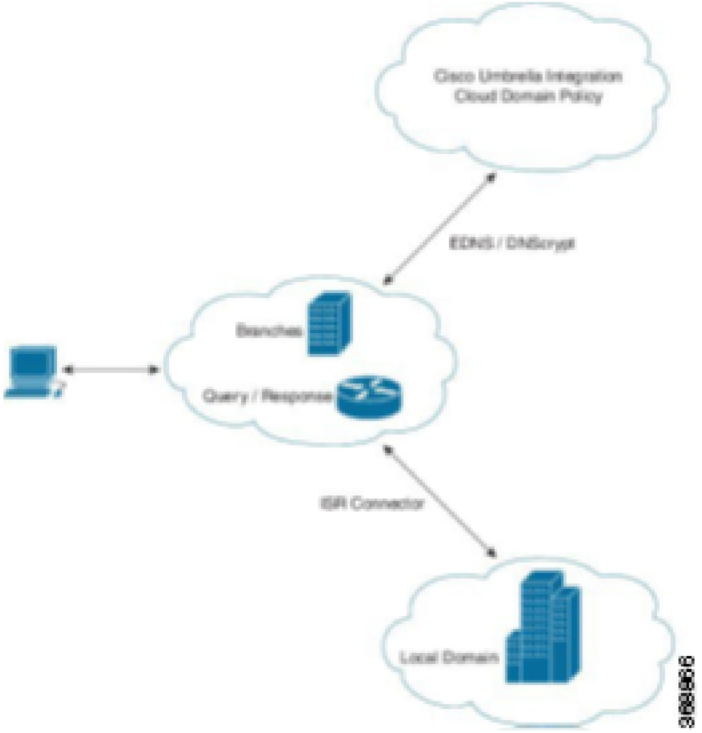
Encrypting the DNS Packet

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

Figure 4: 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.
- 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 Cisco SD-WAN Release 20.3.1 software image and 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 Cisco Umbrella Registration

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**.

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. Click **Advanced** to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
16. 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 10: 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.

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 SD-WAN Release 20.9.1, 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.

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 7

IPsec Pairwise Keys

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

Table 11: Feature History

Feature Name	Release Information	Description
Secure Communication Using Pairwise IPsec Keys	Cisco Catalyst SD-WAN Release 19.2.1	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 Cisco vEdge Routers

Use the following command to display IPSec pairwise keys information on Cisco vEdge Routers:

```
Device# show 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
```

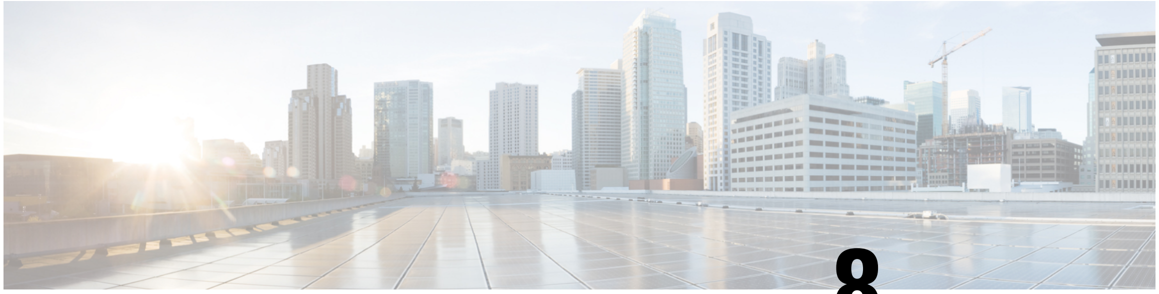
Use the following command to verify outbound connection for IPSec pairwise keys:

```
SOURCE SOURCE DEST DEST                                               REMOTE
REMOTE         AUTHENTICATION                    NEGOTIATED
       PEER          PEER
IP             PORT      IP       PORT      SPI         TUNNEL MTU TLOC ADDRESS TLOC COLOR
 USED                      KEY-HASH ENCRYPTION ALGORITHM TC SPIs KEY-HASH SPI
------------------------------------------------------------------------------------------
10.1.16.16 12366 10.1.15.15 12426 260            1441               172.16.255.15      lte
                     AH_SHA1_HMAC *****4aec      AES-GCM-256                        8
       *****d01e 1538
```

Use the following command to verify inboud connection for IPSec pairways keys:

```
Device# show ipsec inbound-connections

SOURCE  SOURCE       DEST    DEST     REMOTE           REMOTE LOCAL LOCAL  NEGOTIATED PEER
  PEER
IP      PORT          IP  PORT       TLOC ADDRESS TLOC   COLOR TLOC  ADDRESS  TLOC
COLOR ENCRYPTION  ALGORITHM  TC SPIs KEY-HASH SPI
------------------------------------------------------------------------------------------
10.1.15.15 12426 10.1.16.16 12366     172.16.255.15      lte 172.16.255.16 lte AES-GCM-256
 8 *****d01e 518
```



CHAPTER 8

Integrate Your Devices With Secure Internet Gateways

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

Table 12: Feature History

Feature	Release Information	Description
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco SD-WAN Release 20.4.1 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.

Feature	Release Information	Description
Enable Layer 7 Health Check (Automatic Tunnels)	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This features integrates the Layer 7 Health Check feature with automatic tunnels to SIGs. When you create automatic IPsec tunnels using the Cisco Secure Internet Gateway (SIG) template to Zscaler or Cisco Umbrella, a tracker is also created to monitor and load balance or failover tunnels. You can customize the parameters based on which the tracker load balances or fails over tunnels.
Support for Zscaler Automatic IPSec Tunnel Provisioning	Cisco SD-WAN Release 20.5.1 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.
Layer 7 Health Check for Manual Tunnels	Cisco SD-WAN Release 20.8.1 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.
Global SIG Credentials Template	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	With this feature, create a single global SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.

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.

- Options to Integrate Your Devices with Secure Internet Gateways, on page 69
- Configure Tunnels, on page 73
- Monitor Tunnels, on page 98

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 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:
2. Specify Cisco Umbrella or Zscaler credentials using the SIG Credentials feature template.
3. Specify the details for the tunnel to the SIGs using the 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 VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the 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.

Cisco Umbrella Integration

From Cisco SD-WAN Release 20.1.1 and Cisco vManage Release 20.2.1, use Cisco Umbrella as a SIG by choosing Umbrella as the SIG provider in the 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 73.

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 tunnels between the edge devices and the SIGs.

From Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, you can provision automatic IPSec tunnels to Zscaler Internet Access (ZIA) Public Service Edges using the 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.

For information on configuring automatic tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 73.

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 Secure Internet Gateway (SIG) feature template.

Provision manual tunnels as follows:

1. Specify the details for the tunnel to the SIG by using the 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 VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the 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.

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 SD-WAN Release 20.4.1 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 SD-WAN Release 20.4.1 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.

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.

The following table summarizes tracker support for automatic and manual tunnels:

Tunnel Type	Default Tracker	Customized Tracker
Automatic	Yes	Yes Minimum releases: Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1
Manual	No	Yes Minimum releases: Cisco SD-WAN Release 20.8.1 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.
6. If the tunnel does not meet the SLA parameters, the tracker marks the tunnel as down.
7. The device updates the routes for any service VPNs that are connected to the tunnel.

Tracker DNS Cache Timeout

Trackers attached to SIG tunnels monitor the corresponding SIG endpoints. A Cisco vEdge device resolves FQDNs of these SIG endpoints through DNS queries and caches the DNS resolved IP addresses. Trackers probe the SIG endpoint IP addresses to determine tunnel health.

The device refreshes the DNS cache containing SIG endpoint IP addresses as follows:

- Cisco SD-WAN Release 20.7.x and earlier, and Cisco vManage Release 20.7.x and earlier: Configure the DNS cache timeout using the **timer dns-cache-timeout** command on Cisco SD-WAN Manager in the system configuration mode. Cisco vEdge devices cache DNS resolved SIG endpoint IP addresses for the duration of this timeout. When the cache times out, Cisco vEdge devices refresh the cache through new DNS resolution queries. The default timeout is two minutes.

Note **timer dns-cache-timeout** also affects the caching of Cisco SD-WAN Validator IP addresses that the Cisco vEdge devices obtains by resolving FQDNs.

- Cisco SD-WAN Release 20.8.x and Cisco vManage Release 20.8.x: Cisco vEdge devices refresh cached SIG endpoint IP addresses every 2 hours. The DNS cache timeout is preconfigured and cannot be modified.
- From Cisco SD-WAN Release 20.9.1 and Cisco vManage Release 20.9.1: Configure the DNS cache timeout using the **timer tracker-dns-cache-timeout** command on Cisco SD-WAN Manager in the system configuration mode. Cisco vEdge devices cache DNS resolved SIG endpoint IP addresses for the duration of this timeout. When the cache times out, Cisco vEdge devices refresh the cache through new DNS resolution queries. The default timeout is two hours.

  When a Cisco vEdge device refreshes the cache, if a SIG endpoint FQDN is resolved to the IP address that was cached earlier, the device does not reset associated counters. In Cisco SD-WAN Release 20.8.x and earlier releases, and Cisco vManage Release 20.8.x and earlier releases, the device resets counters every time that it refreshes the cache. In some scenarios, this automatic resetting of the counters affects tracker behavior and the tracker fails to detect that the health of tunnel has degraded and it must not be used for routing traffic.

Related Topics

- Create Automatic Tunnels Using a SIG Feature Template, on page 77
- Create Manual Tunnels Using SIG Feature Template, on page 85
- Configure Tracker DNS Cache Timeout Using a CLI Template, on page 95

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 SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) for each Cisco vEdge model that you wish to connect to the SIG.

From Cisco vManage Release 20.9.1, create a single global SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) and attach the template to the required Cisco vEdges, irrespective of the device model. When you attach a 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 vEdges 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 vEdges.

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 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 SIG Credentials template for the SIG provider.

If you try to create or modify a SIG feature template, Cisco SD-WAN Manager prompts you to create a global SIG Credentials template for the SIG provider.

Related Topics

- Create Cisco Umbrella SIG Credentials Template, on page 74
- Create Zscaler SIG Credentials Template, on page 75

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 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 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 SIG Feature Template, on page 77, 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 - SIG Credentials template** to create the Cisco Umbrella SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 13: 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 Zscaler SIG Credentials Template

Minimum release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a SIG Feature Template, on page 77, 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 - SIG Credentials template** to create the Zscaler SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 14: 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 15: 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*.

Field	Description
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*.

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

Create 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 **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 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 **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 - 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 SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1 , 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. Click **New Tracker**.

   b. Configure the following:

Table 16: 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 Prior to Cisco vManage Release 20.8.1, SIG tracker monitor statistics were reset at every Domain Name System (DNS) cache timeout interval.

Beginning with Cisco vManage Release 20.8.1, SIG tracker monitor statistics are no longer reset at every DNS cache timeout interval. SIG tracker monitor statistics are reset every two hours. A SIG tracker allows you to track the health of your SIG tunnels.

c. Click **Add**.

d. 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 17: Basic Settings

Field	Description
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 SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, 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.
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.

d. (Optional) Under **Advanced Options**, configure the following:

Table 18: 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 19: 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 20: 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 21: 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 22: 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 23: Zscaler

Field	Description
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 Zscaler data center, choose the data center from the drop-down list.
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 Zscaler data center, choose the data center from the drop-down list.
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 Manual Tunnels Using SIG Feature Template

From Cisco SD-WAN Release 20.4.1 and 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 SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, or later, use the 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 SD-WAN Release 20.4.1, 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 SD-WAN Release 20.8.1, 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 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 **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 SD-WAN Release 20.8.1, Cisco vManage Relase 20.8.1.

   a. Click **New Tracker**.

   b. Configure the following:

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
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.

   c. Click **Add**.

d. 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.
Source Type	Click **INTERFACE** or **IP**.
Tracker	(Optional) Choose a tracker to monitor tunnel health. **Note** From Cisco SD-WAN Release 20.8.1 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	This field is displayed only if you chose the **Source Type** as **INTERFACE.** Enter the name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Tunnel Source IP Address	This field is displayed only if you chose the **Source Type** as **IP.** Enter the IP address of the tunnel source.
IPv4 address	This field is displayed only if you chose the **Source Type** as **IP.** (Optional) Enter the tunnel interface's IP address.
Tunnel Destination IP Address/FQDN	Enter the IP address of the SIG provider endpoint.

Field	Description
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 24: (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 25: (Tunnel Type: gre) Keep Alive

Field	Description
Interval	Time duration between successive GRE keepalive messages. **Range**: 0 to 65535 seconds **Default**: 0
Retries	Number of times the keepalive messages are sent to the remote device when no response is received from the remote device. If no response is received after these many tries, the remote device is declared down. **Range**: 0 to 255 **Default**: 3

Table 26: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.

Field	Description
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
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 27: (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

Field	Description
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
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 28: (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

Field	Description
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
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 29: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.

Field	Description
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.

11. Click **Save**.

Create Manual Tunnels Using the CLI

Minimum releases: Cisco SD-WAN Release 20.9.1 and Cisco vManage Release 20.9.1

This section provides example CLI configurations for creating manual SIG tunnels.

```
Device(config-vpn-0)# interface ipsec1
Device(config-interface-ipsec1)# description ZScaler-Primary-Account1-vpn1
Device(config-interface-ipsec1)# ip address 10.18.0.1/30
Device(config-interface-ipsec1)# tunnel-source-interface ge0/0
Device(config-interface-ipsec1)# tunnel-destination 10.225.200.20
Device(config-interface-ipsec1)# dead-peer-detection interval 5
Device(config-interface-ipsec1)# tunnel-set secure-internet-gateway-other
```

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 93

Modify Service VPN Template

To ensure that the device connects to the SIG, you must modify the 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 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 **Secure Internet Gateway**.
10. From the **Secure Internet Gateway** drop-down list, choose the 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 **SIG Credentials** drop-down list, choose the relevant SIG Credentials feature template.

    (From Cisco vManage Release 20.9.1) Cisco SD-WAN Manager automatically chooses the applicable global SIG Credentials feature template based on the 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 **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 Tracker DNS Cache Timeout Using a CLI Template

Minimum supported releases: Cisco SD-WAN Release 20.9.1 and Cisco vManage Release 20.9.1.

To configure tracker DNS cache timeout, add the CLI command sequence provided in this section to a device CLI template and attach the template to Cisco SD-WAN Manager. For more information about using a CLI template, see Create a Device CLI Template.

Note By default, CLI templates execute commands in the global configuration (config) mode.

1. Enter the system configuration mode.

   ```
   system
   ```

2. Configure tracker DNS cache timeout.

   ```
   timer tracker-dns-cache-timeout duration
   ```

The following example shows a sample configuration which defines the cache timeout as 15 minutes:

```
system
 timer tracker-dns-cache-timeout 15
```

Related Topics

Support for Layer 7 Health Check, on page 71

Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager

Table 30: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco SD-WAN Release 20.1.1	This feature lets you manually configure a GRE tunnel by using the VPN Interface GRE template or an IPSec tunnel by using the VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.

Note From Cisco SD-WAN Release 20.4.1, 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 SD-WAN Release 20.4.1, 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 VPN Interface GRE template from the group of VPN templates.

   e. In **Basic Configuration**, configure parameters as desired and then click **Save**. For more information on configuring the VPN GRE template, see VPN Interface GRE.

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 VPN Interface GRE template.

d. From the 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 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 VPN Interface IPsec template.

   d. From the VPN Interface IPsec drop-down menu, click **Create Template**.

   e. Configure the templates as desired, and then click **Save**.

Monitor Tunnels

To monitor the status of tunnels running the layer 7 health check tracker, run the **show interface** or **show support tracker interface monitors** commands.

```
Device# show interface

IF IF IF TCP
AF ADMIN OPER TRACKER ENCAP SPEED MSS RX TX
VPN INTERFACE TYPE IP ADDRESS STATUS STATUS STATUS TYPE PORT TYPE MTU HWADDR MBPS DUPLEX
ADJUST UPTIME PACKETS PACKETS
----------------------------------------------------------------------------------------
0 ge0/0 ipv4 10.1.16.16/24Up Up NA null transport 1500 52:54:00:93:04:c6 1000 full 1416
0:03:01:39 10405 11377
0 ge0/1 ipv4 10.0.21.16/24Up Up NA null transport 1500 52:54:00:c4:e3:6f 1000 full 1416
0:03:01:37 6214 6112
0 ge0/2 ipv4 - Up Up NA null service 1500 52:54:00:7b:e1:3f 1000 full 1416 0:03:01:37 0 0
0 ge0/3 ipv4 10.0.100.16/24Up Up NA null service 1500 52:54:00:1a:ec:8c 1000 full 1416
0:03:01:37 114 57
0 ge0/4 ipv4 10.0.14.16/24Up Up NA null service 1500 52:54:00:77:15:59 1000 full 1416
0:03:01:37 0 0
0 ipsec1 ipv4 - Up Up Up vlan service 1400 00:00:00:00:00:01 1000 full 1316 0:00:10:16 1587
 2776
0 ipsec2 ipv4 - Up Up Down vlan service 1400 00:00:00:00:00:01 1000 full 1316 0:00:10:01
41 0
```

```
0 system ipv4 172.16.255.16/32Up Up NA null loopback 1500 00:00:00:00:00:00 1000 full 1416
 0:03:01:49 0 0
1 ge0/2.101 ipv4 172.16.21.2/24Up Up NA vlan service 1496 52:54:00:7b:e1:3f 1000 full 1412
 0:03:01:37 2752 1553
2 ge0/2.102 ipv4 172.16.22.2/24Up Up NA vlan service 1496 52:54:00:7b:e1:3f 1000 full 1412
 0:03:01:39 63 56
3 ge0/2.103 ipv4 172.16.23.2/24Up Up NA vlan service 1496 52:54:00:7b:e1:3f 1000 full 1412
 0:03:01:39 59 59
512 eth0 ipv4 10.0.1.16/24Up Up NA null service 1500 00:50:56:00:01:10 1000 full 1416
0:03:01:39 2005 1196
65528 loopback65528 ipv4 192.168.0.2/24Up Up NA null service 1500 00:00:00:00:00:00 1000
full 1416 0:03:01:39 0 0
65530 loopback65530 ipv4 192.168.0.2/24Up Up NA null service 1500 00:00:00:00:00:00 1000
full 1416 0:03:01:39 0 0
0 1000 full 1416 0:03:01:39 0 0
65530 loopback65530 ipv4 192.168.0.2/24 Up Up NA null service 1500 00:00:00:00:00:00 1000
full 1416 0:03:01:39 0 0
```

In the following example, the tracker is up:

```
Device#show support tracker interface monitors
  Interface: ipsec1/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec1
   Monitor state     : UP (flapped 1 times)
   Ref count         : 1
   Monitor type      : httping
   Num of probes     : 1
   Max Re-transmit   : 2
   First Probe       : 0 secs
   Probe interval    : 30 secs
   Probe timeout     : 1000 msecs
   DNS TTL           : 33935 secs
   DNS query/ok/fail : 1/1/0

   Peer: 104.129.198.175 (UP - flapped 1 times, Re-Transmit 0)
     Total requests  : 1           Total responses : 1
     Total Tx errors : 0           Total Rx errors : 0
     Total Tx skipped: 0           Total Rx ignored: 0
     Total timeout   : 0           Connect errors  : 0
     RTT min/avg/max : 24.90/24.90/24.90 ms
     TCP min/avg/max : 11.70/11.70/11.70 ms

Interface: ipsec2/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec2
   Monitor state     : UP (flapped 0 times)
   Ref count         : 1
   Monitor type      : httping
   Num of probes     : 1
   Max Re-transmit   : 2
   First Probe       : 0 secs
   Probe interval    : 30 secs
   Probe timeout     : 1000 msecs
   DNS TTL           : 33935 secs
   DNS query/ok/fail : 1/1/0

   Peer: 104.129.198.175 (UP - flapped 0 times, Re-Transmit 0)
     Total requests  : 6           Total responses : 6
     Total Tx errors : 0           Total Rx errors : 0
     Total Tx skipped: 0           Total Rx ignored: 0
     Total timeout   : 0           Connect errors  : 0
     RTT min/avg/max : 297.32/333.95/472.63 ms
     TCP min/avg/max : 150.47/181.04/320.78 ms
```

In the following example, the tracker is down:

```
vm6# show support tracker interface monitors
Interface: ipsec1/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec1
   Monitor state : UP (flapped 0 times)
   Ref count : 1
   Monitor type : httping
   Num of probes : 1
   Max Re-transmit : 2
   First Probe : 0 secs
   Probe interval : 30 secs
   Probe timeout : 1000 msecs
   DNS TTL : 47453 secs
   DNS query/ok/fail : 1/1/0

   Peer: 192.0.2.1 (UP - flapped 0 times, Re-Transmit 0)
     Total requests : 34 Total responses : 34
     Total Tx errors : 0 Total Rx errors : 0
     Total Tx skipped: 0 Total Rx ignored: 0
     Total timeout : 0 Connect errors : 0
     RTT min/avg/max : 25.16/35.62/111.92 ms
     TCP min/avg/max : 12.45/17.71/69.28 ms

Interface: ipsec2/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec2
   Monitor state : DOWN (flapped 1 times)
   Ref count : 1
   Monitor type : httping
   Num of probes : 1
   Max Re-transmit : 2
   First Probe : 0 secs
   Probe interval : 30 secs
   Probe timeout : 1000 msecs
   DNS TTL : 47453 secs
   DNS query/ok/fail : 1/1/0

   Peer: 192.0.2.1 (DOWN - flapped 1 times, Re-Transmit 0)
     Total requests : 33 Total responses : 0
     Total Tx errors : 0 Total Rx errors : 0
     Total Tx skipped: 0 Total Rx ignored: 0
     Total timeout : 33 Connect errors : 0
     RTT min/avg/max : 0.00/0.00/0.00 ms
     TCP min/avg/max : 0.00/0.00/0.00 ms
```

CHAPTER 9

Configure Single Sign-On

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

Table 31: 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 vManage.

- 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 32: 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

Component	Value	Configuration
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.
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 vManage. 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 vManage.
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.

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.)

Field	Value to enter
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.

   Note You can also add a domain later to an existing 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.

    Note A user ID must be in an email address format, for example, **john@mystore.com**.

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 10

Security CLI Reference

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

CLI commands for configuring and monitoring security.

Security Configuration Commands

Use the following commands to configure security parameters:

```
security
 control
   protocol (dtls | tls)
   tls-port number
 ipsec
   authentication-type type
   rekey seconds
   replay-window number
 vpn vpn-id
   interface ipsecnumber
     access-list acl-name
     block-non-source-ip
     clear-dont-fragment
     dead-peer-detection  interval seconds retries number
     description text
   ike
     authentication-type type
       local-id id
       pre-shared-secret password
       remote-id id
    cipher-suite suite
    group number
    mode mode
    rekey seconds
    version number
  ip address ipv4-prefix/length
```

```
ipsec
 cipher-suite suite
 perfect-forward-secrecy pfs-setting
 rekey seconds
 replay-window number
mtu bytes
policer policer-name
rewrite-rule rule-name
[no] shutdown
tcp-mss-adjust bytes
tunnel-destination (dns-name | ipv4-address)
(tunnel-source ip-address |  tunnel-source-interface interface-name)
```

Security Monitoring Commands

- **show control connections**
- **show security-info**