



Secure Internet Gateway and Secure Service Edge

- [Feature history for Secure Internet Gateway and Secure Service Edge, on page 1](#)
- [Secure Internet Gateway, on page 1](#)
- [Configure a Secure Internet Gateway, on page 2](#)
- [Configure a Secure Service Edge, on page 8](#)

Feature history for Secure Internet Gateway and Secure Service Edge

Table 1: Feature history

Feature Name	Release Information	Description
Configure Secure Service Edge	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	With this feature you can configure a Secure Service Edge (SSE) profile using Cisco Secure Access as the provider. You can associate the SSE profile to a policy group to deploy to a device.

Secure Internet Gateway

Cisco Catalyst SD-WAN edge devices support 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.

Configure a Secure Internet Gateway

Before you begin

Ensure that you enter the Umbrella and Zscaler credentials from **Administration > Settings > Cloud Provider Credentials > Cloud Credentials**.

Table 2: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see the <i>Cisco Umbrella SIG User Guide</i> .
SIG Umbrella API Key	Enter the Umbrella Management API Key. Management API keys are used in SIG is Secure Internet Gateway (SIG) - (Management) . For more information, see the Cloud Security API documentation on the Cisco DevNet portal.
SIG Umbrella API Secret	Enter the Umbrella Management API Secret. For more information, see the Cloud Security API documentation on the Cisco DevNet portal.

Table 3: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud.
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 the <i>ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started</i> .
Username	Username of the Cisco Catalyst SD-WAN partner account.
Password	Password of the Cisco Catalyst SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see Managing SD-WAN Partner Keys .

Procedure

-
- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Secure Internet Gateway**.
- Step 2** Click **Add Secure Internet Gateway**.
- Step 3** Choose **SIG Provider**.

- Umbrella
- Zscaler
- Generic

Step 4 Enter a source IP address for the probe packets.

Step 5 Create one or more trackers to monitor tunnel health.

Click **Add Tracker**. In the **Add Tracker** dialog box, configure the following:

Table 4: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. Range: 1 to 10 Default: 3

Step 6 Create tunnels.

Click **Add Tunnel**. In the **Add Tunnel** dialog box configure the following:

Table 5: Add tunnel

Field	Description
Tunnel Type	Umbrella: (Read only) ipsec Zscaler: Click ipsec or gre . Generic: Click ipsec or gre .
Interface Name (1..255)	Name of the interface.
Description	Description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.

Field	Description
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Source Public IP	(Automatic GRE tunnels to Zscaler only) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click Primary , or for a secondary data center, click Secondary . Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Tunnel Destination IP Address/FQDN	(Manual tunnels only) The IP address of the SIG provider endpoint. The configuration of FQDN for Tunnel Destination IP address is not supported.
Preshared Key	(Manual tunnels only) This field is displayed only if you choose ipsec as the Tunnel Type . Enter the password to use with the preshared key.
Advanced Options	
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 TCP 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. After one DPD message is missed by the peer, the router changes the state and sends a DPD retry message at a 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 DPD retry messages can be missed before the tunnel is marked as down. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 300 to 86400 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 The IPsec Cipher Suite defaults vary by the type of the SIG: • Umbrella: AES 256 GCM • Zscaler: None • Generic: NULL SHA 512

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus The IKE group defaults vary by the type of the SIG: • Umbrella: 14 2048-bit modulus • Zscaler: 2 1024-bit modulus • Generic: 16 4096-bit modulus
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 300 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, 4096. Default: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 Default: AES 256 GCM

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS The Perfect Forward Secrecy defaults vary by the type of the SIG: • Umbrella: None • Zscaler: None • Generic: Group 16

Note

When a security policy associated with Zscaler is removed from a device and a new configuration group is deployed, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever a security policy is removed from a device.

Step 7

Configure high availability to designate active and back-up tunnels and distribute traffic among tunnels.

Click **Add Interface Pair**. In the **Add Interface Pair** dialog box, configure the following:

Field	Description
Active Interface	Choose a tunnel that connects to the primary data center.
Active Interface Weight	Enter 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 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 Interface	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose None.

Field	Description
Backup Interface Weight	Enter 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 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.

Configure a Secure Service Edge

Before you begin

Create the Cisco SSE credentials from **Administration > Settings > Cloud Credentials**.

Gateway Options

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge**.
- Step 2** Click **Add Secure Service Edge**.
- Step 3** Choose the **SSE Provider**.
- Cisco Secure Access
 - (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler
- Step 4** Enable context sharing for VPN and SGT to allow Cisco IOS XE Catalyst SD-WAN devices to share context information with SSE.

Table 6: Context Sharing

Field	Description
VPN	Enable sharing of VPN information with SSE.
SGT	Enable sharing of SGT information with SSE.

- Step 5** Configure trackers.

While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker endpoint with default values for failover parameters. However, you can also create customized trackers with failover parameters that suit your requirements.

- a) In the **Source IP Address** field, enter a source IP address without a subnet mask.
- b) Click **Add Tracker**. In the **Add Tracker** pop-up window, configure the following:

Table 7: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the Secure Service Edge endpoint of the tunnel. Default: service.sig.umbrella.com
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is up or down. Range: 1 to 10 Default: 3

Step 6 Create tunnels.

Click **Add Tunnel**. In the **Add Tunnel** pop-up window, under **Basic Settings**, configure the following:

Table 8: Basic Settings

Field	Description
Tunnel Type	• Cisco Secure Access: (Read only) ipsec • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler: ipsec or gre
Interface Name (1..255)	Name of the interface.
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface. The tunnel source interface supports loopback.

Field	Description
Source Public IP	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
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.
Advanced Options (Optional)	
Shutdown	Click the radio button to enable this option. Default: Disabled
Enable Tracker	Click the radio button to enable this option.
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 TCP 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 Internet Key Exchange (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 Dead Peer Detection (DPD) retry messages if the DPD retry message is missed by the peer. If a peer misses a DPD message, the router changes the state and sends a DPD retry message. The message is sent at a faster retry interval, which is the number of seconds between DPD retries. The default DPD retry message is sent every 2 seconds. The tunnel is marked as down after five DPD retry messages are missed. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 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.
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 3600 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, or 4096 packets. Default: 512

Field	Description
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 Default: AEM 256 GCM
Perfect Forward Secrecy	Specify the Perfect Forward Secrecy (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

Step 7

Applicable only to Cisco Secure Access: **Region** : When you choose the region, a pair of primary and secondary region is selected. Choose the primary region that Cisco Secure Service Edge provides from the drop-down list and the secondary region is auto-selected in Cisco SD-WAN Manager . If the primary region with a unicast IP address is not reachable then the secondary region with a unicast IP address is reachable and vice versa. Cisco Secure Access ensures that both the regions are reachable at all times.

Note

You can configure any DNS server on the device which connects to HTTPS to get the public IP address. To configure a source interface for HTTPS, use the **ip http client source-interface** command on Cisco SD-WAN Manager .

Step 8

Configure high availability to designate active and back-up tunnels and distribute traffic among tunnels.

Click **Add Interface Pair**. In the **Add Interface Pair** pop-up window, configure the following:

Table 9: Add interface pair

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

Field	Description
Active Interface Weight	Enter 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 to both the tunnels, 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 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 Interface	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 Interface Weight	Enter 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 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.

Step 9 (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Configure advanced settings.

Applicable only to Zscaler:

Field	Description
Primary Datacenter	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Secondary Datacenter	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.

Table 10: Zscaler location

Field	Description
Zscaler Location	Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , enter unique location name for primary and secondary routers. For more information about locations, see <i>ZIA Help > Traffic Forwarding > Location Management > About Locations</i> .
Country	You can enable or disable this option only if either primary or secondary data center is set to Auto. When you choose Auto, the data center selected is within the country of the device.

Table 11: Gateway options

Field	Description
Authentication Required	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable Caution	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable AUP	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
XFF Forwarding	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable IPS Control	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable Firewall	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1)

Table 12: Bandwidth control

Field	Description
Enforce Bandwidth Control	Enable to enforce bandwidth control on the location. • Download (Mbps) : Specify the maximum bandwidth limits for download. • Upload (Mbps) : Specify the maximum bandwidth limits for upload. For more information about locations, see <i>ZIA Help > Traffic Forwarding > Location Management > About Locations</i> .

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1)

Table 13: Sub-locations

Field	Description
Name	Enter a name for the sub-location.
Service VPN	Select a service VPN from the drop-down menu.
IP Address	Enter an IP address or a range of IP addresses for the service VPN.
Authentication Required	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable Caution	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable AUP	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
XFF Forwarding	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enable IPS Control	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off

Field	Description
Enable Firewall	See <i>ZIA Help > Traffic Forwarding > Location Management > Configuring Locations</i> . Default: Off
Enforce Bandwidth Control	Choose one of the following: • Location Bandwidth : Uses bandwidth of the parent location on the sub-location. The download and upload maximum bandwidth limits are the same as specified for the parent location. A percentage of the parent location bandwidth is allocated to the sub-location based on the allocations of other sub-locations. For more information, see <i>Secure Internet and SaaS Access (ZIA) Help > Traffic Forwarding > Location Management > Configuring Sub-Locations</i> . • Override : Overrides the bandwidth of the parent location. Specify the maximum bandwidth limits for Download (Mbps) and Upload (Mbps) . This bandwidth is dedicated to the sub-location and not shared with other sub-locations. • Disable : Disables the sub-location traffic from any bandwidth management