



ZSCALER AND CISCO CATALYST SD-WAN DEPLOYMENT GUIDE

Contents

Terms and Acronyms	9
About This Document	11
Zscaler Overview	11
Cisco Overview	11
Audience	11
Hardware Used	11
Software Revisions	12
Request for Comments	12
About the Guide	12
Zscaler and Cisco Introduction	14
ZIA Overview	14
ZPA Overview	14
Zscaler Resources	14
Cisco SD-WAN	15
Cisco Resources	15
Define	16
Cisco Catalyst SD-WAN Design Overview	16
Feature Background and History	17
Support through Cisco Catalyst SD-WAN 20.3/17.3 code versions (Traditional Active/Standby Tunnels and L7 Health Checking)	17
Cisco Catalyst SD-WAN 20.4/17.4 code versions (Active/Active ECMP Tunnels and Traffic Steering through SIG Route and Centralized Data Policy using SIG Templates)	17
Cisco Catalyst SD-WAN 20.5/17.5 code versions (Zscaler Automatic IPsec Tunnel Provisioning)	18
Cisco Catalyst SD-WAN 20.6/17.6 code versions (L7 Health Checks for IPsec Auto Tunnels for IOS XE SD-WAN routers and Cloud onRamp for SaaS over SIG Tunnel Support)	18

Cisco Catalyst SD-WAN 20.7/17.7 code versions (VRRP Interface Tracker support for SIG Tunnels)	18
Cisco Catalyst SD-WAN 20.8/17.8 code versions (Multiple SIG Enhancements)	18
Cisco Catalyst SD-WAN 20.9/17.9 code versions (Zscaler Automatic GRE Tunnel Provisioning and SIG Tunnel Monitoring)	18
Design	20
GRE and IPSec Tunnels	20
Packet Format and NAT	20
Throughput	21
Tunnel Source IP Addressing	21
Tunnel Liveliness	22
GRE Keepalives and DPD	22
Layer 7 Health Checks	22
ECMP Routing	22
4-Tuple ECMP	22
Source IP-Based ECMP	23
Primary vs. Secondary Data Center Placement	24
Zscaler Active/Standby Tunnel Combinations	25
One Active/Standby Tunnel Pair	25
Multiple Active/Active Tunnels with ECMP	26
Multiple Active/Standby Tunnel Pairs	27
Active/Active Tunnels with Weighted Load Balancing	28
User Traffic Redirection	28
WAN Edge with Zscaler Site Tunnel Design	29
Single WAN-Edge Design	29
Dual WAN Edge Design	32
Dual WAN Edge with Zscaler Site Service-Side Design	35
VRRP	35
Routing	35

SIG Service	37
New SIG Workflow	38
Automatic Zscaler Tunnels	39
IPSec	39
Advanced Settings for Zscaler Auto Tunnels	40
Layer 7 Health Check for Auto Tunnels	41
General Configuration Steps	41
Configuration Prerequisites	41
Design Considerations	42
Basic	42
ZIA Admin Portal	42
ECMP Tunnels	42
Auto Tunnels	42
L7 Health Checks	43
GRE	43
Cisco vEdge	43
Deploy	44
Deploy: ZIA for API Access	44
Procedure 1: Log In to ZIA	45
Procedure 2: Find Zscaler Organization Domain and Partner Base URI	45
Procedure 3: Add and Verify SD-WAN Partner Key	47
Procedure 4: Add a Partner Administrator Role	50
Procedure 5: Create a Partner Administrator	52
Procedure 6: Activate Pending Changes	55
Deploy: Cisco WAN Edge Prerequisites	56
Procedure 1: Log In to the Cisco Catalyst SD-WAN Manager	56
Procedure 2: Ensure Prerequisites are Met	56
Procedure 3: Create a SIG Credentials Feature Template	58
Deploy: Cisco WAN Edge Auto IPSec or GRE Tunnels (One Active/Standby Pair, Hybrid Transport)	61

Procedure 1: Create a SIG Template	62
Procedure 2: Add the Tunnel Configuration to the Device Template	67
Procedure 3: Add Service Route	69
Procedure 4: Verify Tunnel Operation	70
Procedure 5: (Optional) Customize L7 Health Tracker	71
Procedure 6: (Optional) Enable Advanced Zscaler Features	73
Procedure 7: (Optional) Customize Zscaler Tunnel Destination (Primary and Secondary Data Centers)	75
Deploy: Cisco WAN Edge Auto IPSec or GRE Tunnels (Active/Active Tunnels, Hybrid Transport)	78
Procedure 1: Create two loopback interfaces, one for each active tunnel (Cisco IOS XE SD-WAN only)	79
Procedure 2: Create a local policy-based routing policy (Cisco IOS XE SD-WAN only)	80
Procedure 3: (Optional) IOS XE SD-WAN Only: Configure Source IP-Based ECMP	82
Procedure 4: Create a New SIG Feature Template with Two Active Tunnels (Cisco IOS XE SD-WAN Only)	83
Procedure 5: Modify Device Template	84
Procedure 6: Add Centralized Data Policy for Traffic Redirection	87
Procedure 7: (Optional) Assign Tunnel Weights	92
Operate	93
Verify Cisco Catalyst SD-WAN Tunnel Operation from the Cisco SD-WAN Manager	93
Verify Cisco Catalyst SD-WAN Event Logs from the Cisco SD-WAN Manager	94
Verify Zscaler Tunnel Status in ZIA Admin	95
Verify Zscaler Tunnel Event Logs in ZIA Admin	96
Tunnel Logging	96
View API Calls in Zscaler ZIA (Audit Logs)	96
Verify Zscaler ZIA Service Configuration	98
Verify Zscaler Tunnel Operation Using Cisco IOS XE SD-WAN CLI	98
Verify Zscaler Tunnel Operation using Cisco vEdge CLI	102

Appendix A: Cisco Branch Base Feature Templates and Configuration Values Used 107

Feature Templates	107
AAA feature template (Cisco IOS XE SD-WAN)	107
AAA feature template (Cisco vEdge)	107
NTP Feature Template	108
Branch VPNO Feature Template	108
Branch Internet Interface Feature Template (Cisco IOS XE SD-WAN)	108
Branch Internet Interface Feature Template (Cisco vEdge)	109
Branch MPLS Interface Feature Template	109
Branch VPN512 Interface Feature Template	109
Branch VPN 1 Feature Template	110
Branch VPN1 Interface Feature Template	110
Device Templates	110
Single WAN Edge Router Sites (Cisco IOS XE SD-WAN)	110
Single WAN Edge Router Sites (Cisco vEdge)	111
Device Variable Values	111

Appendix B: Tunnel Configuration Summary (Feature and Device Templates) 113

Prerequisites	113
Cisco VPN Interface Ethernet Feature Template	113
Cisco VPN Feature Template	113
Cisco VPN Feature Template	113
SIG Credential Information from ZIA	114
Cisco SIG Credentials Feature Template	114
Example 1: Active/Standby Tunnels	115
Cisco SIG Feature Template (GRE)	115
Cisco SIG Feature Template (IPSec)	115
Device Template	116

Example 2: Active/Active Tunnels (Cisco IOS XE SD-WAN Only)	116
Cisco VPN Interface Ethernet Feature Template	116
Cisco VPN Interface Ethernet Feature Template	117
Cisco CLI Add-On Feature Template	117
Cisco SIG Feature Template (GRE)	117
Cisco SIG Feature Template (IPSec)	118
Device Template	119
Traffic Redirection	119
Service Route	119
Branch VPN1 Feature Template	119
Centralized Policy	119
Miscellaneous	120
Customize Health Tracker	120
Enable Advanced Zscaler Features	120
Customize Zscaler Tunnel Destinations (Primary and Secondary DCs)	120
Assign Tunnel Weights (Use with Active/Active Tunnels)	121
Appendix C: Cisco IOS XE SD-WAN CLI Configuration	122
Base Connectivity	122
Prerequisites	125
Common Tunnel Components	125
SIG Credentials	125
IKEv2 and IPSec Configuration	125
Zscaler Location Settings	127
L7 Health Check Configuration	127
Use Case Example 1: Active/Standby Tunnels	128
IPSec Tunnels Defined	128
GRE Tunnels Defined	128
Zscaler Tunnel Options	129
Service SIG Interface Pairs HA Pair Configuration	129

Use Case Example 2: Active/Active Tunnels	129
Tunnel Source Loopbacks Defined	129
Local Policy Route (for ISAKMP control traffic)	129
IPSec Tunnels Defined	130
Zscaler Tunnel Options	131
Service SIG Interface Pairs HA Pair Configuration	131
Traffic Redirection	131
Service SIG Route	131
Service SIG Data Policy (apply to Cisco SD-WAN Controller)	131
Miscellaneous	133
Customize Health Tracker	133
Enable Advanced Zscaler Features	133
Customize Zscaler Tunnel Destinations (Primary and Secondary DCs)	133
Customize Zscaler GRE Tunnel Destinations (Primary and Secondary DCs)	134
Assign Tunnel Weights (Use with Active/Active Tunnels)	134
Appendix D: Cisco vEdge CLI Configuration	135
Base Connectivity	135
Prerequisites	137
Use Case Example 1: Active/Standby Tunnels	137
IPSec Tunnels Defined	137
Service SIG Interface Pairs HA Pair Configuration	139
SIG Credentials	139
Traffic Redirection	139
Service SIG Route	139
Service SIG Data Policy (apply to Cisco SD-WAN Controller)	139
Miscellaneous	141
Customize Health Tracker	141
Enable Advanced Zscaler Features	141
Customize Zscaler IPSec Tunnel Destinations (Primary and Secondary DCs)	141

Appendix E: Requesting Zscaler Support	142
Appendix F: Document Revision Control	144

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
BGP	Border Gateway Protocol
Cisco SD-WAN Validator	Cisco Catalyst SD-WAN component which facilitates the initial bring-up authentication and authorization of the network elements. Formerly referred to as vBond.
Cisco SD-WAN Manager	Cisco Catalyst SD-WAN centralized network management system that provides a GUI interface and REST APIs to monitor, configure, and maintain all Cisco Catalyst SD-WAN devices in the overlay network. Formerly referred to as vManage.
Cisco SD-WAN Controller	Cisco Catalyst SD-WAN centralized control plane and policy engine. Formerly referred to as vSmart.
DIA	Dedicated Internet Access
DLP	Data Loss Prevention
DPD	Dead Peer Detection (RFC 3706)
DTLS	Datagram Transport Layer Security (RFC6347)
EBGP	External Border Gateway Protocol
ECMP	Equal Cost Multi-Path
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulated Security Payload
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
INET	Internet Networking
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
ISAKMP	Internet Security Association and Key Management Protocol
MPLS	Multiprotocol Label Switching
NAT-T	Network Address Translation traversal
NMS	Network Management System
NTP	Network Time Protocol
OMP	Overlay Management Protocol (Cisco SD-WAN)
OSPF	Open Shortest Path First
PAT	Port Address Translation
PBR	Policy-based Routing
PFS	Perfect Forward Secrecy
SIG	Secure Internet Gateway
SSH	Secure Shell
SSL	Secure Socket Layer (RFC6101)
TLOC	Transport Locator
TLS	Transport Layer Security (RFC5246)
URI	Uniform Resource Identifier

Acronym	Definition
VDI	Virtual Desktop Infrastructure
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN Edge	Cisco SD-WAN router solution
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

Zscaler Overview

Zscaler (NASDAQ: [ZS](#)), enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see [Zscaler's website](#) or follow Zscaler on Twitter @zscaler.

Cisco Overview

Cisco (NASDAQ: [CSCO](#)) helps seize the opportunities of tomorrow by proving that amazing things can happen when you connect the unconnected. An integral part of Cisco's DNA is creating long-lasting customer partnerships, working together to identify their customers' needs and provide solutions that fuel their success.

Cisco has preserved this keen focus on solving business challenges since its founding in 1984. Len Bosack and wife Sandy Lerner, both working for Stanford University, wanted to email each other from their respective offices, but technological shortcomings did not allow such communication. Technology was invented to deal with disparate local area protocols, and as a result of solving their challenge, the multiprotocol router was born.

Audience

This document is designed for network engineers and network architects interested in configuring and integrating ZIA access with Cisco WAN Edge routers. It assumes the reader has a basic comprehension of IP networking and is familiar with Cisco SD-WAN concepts and configurations. For more information, see:

- [Zscaler Resources](#)
- [Cisco Resources](#)
- [Appendix E: Requesting Zscaler Support](#)

Hardware Used

To create this document, Cisco WAN Edge router solutions were tested in various use cases. They include a C8300-1N1S-6T, ISR4331, ISR1100-4G (Cisco Viptela), and Cisco vEdge 100b.

Tech Tip

End-of-Life milestones have been announced for the vEdge router and other select SD-WAN platforms (vEdge 100, vEdge 1000, vEdge 2000, vEdge 5000, select ISR4K, select ASR1K products, and select ISR1K products). To learn more, refer to the [Cisco end-of-life announcements page](#).

Software Revisions

The following products and software versions are included as part of validation in this deployment guide. This validated set is not inclusive of all possibilities.

Product/Part Number	Software Version
Zscaler ZIA	6.1
Cisco SD-WAN Manager	20.6.1
Cisco ISR4331	17.6.1a
Cisco C8300-1N1S-6T	17.6.1a
Cisco ISR1100-4G (Cisco Viptela)	20.6.1
Cisco vEdge 100b	20.6.1
Cisco 5.1	December 2021 (Updated formatting and edited for style)

Request for Comments

- For prospects and customers: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- For Zscaler employees: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

About the Guide

This document provides technical and configuration guidance for integrating ZIA and Cisco SD-WAN, successfully using the capabilities provided by Cisco SD-WAN Manager version 20.6, Cisco vEdge version 20.6, and Cisco IOS XE SD-WAN Edge version 17.6. It includes examples to show how to provision a new service to integrate ZIA and Cisco SD-WAN IPsec tunnels. For Cisco SD-WAN, configurations that use feature templates through Cisco SD-WAN Manager and CLI are both shown. The following Cisco SD-WAN and ZIA use cases are discussed within this document.

Tech Tip

Cisco SD-WAN has been rebranded to Cisco Catalyst SD-WAN. As part of this rebranding, the vManage name has been changed to SD-WAN Manager, the vSmart name has been changed to SD-WAN Controller, and the vBond name has been changed to SD-WAN Validator. Together, the vManage, vSmart, and vBond are referred to as the SD-WAN control components or the SD-WAN control complex in this document.

- Single WAN Edge deployments
- Active/standby and active/active tunnels
- Automatic provisioning of IPsec tunnels
- Use of service route or centralized policy for traffic redirection

The Zscaler portion of this document was authored by Zscaler and the Cisco SD-WAN portion of this document was authored by Cisco. Both companies partnered to review and validate the information in this guide.

This document contains four major sections:

- The [Define](#) section gives background on the Zscaler and Cisco SD-WAN solution.
- The [Design](#) section discusses the solution components, design aspects, and any prerequisites.
- The [Deploy](#) section provides information about various configurations and best practices.
- The [Operate](#) section shows how to manage different aspects of the solution.

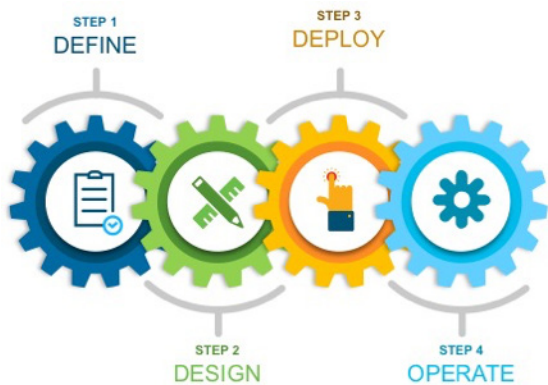


Figure 1. Define, Design, Deploy, Operate

Zscaler and Cisco Introduction

Overviews of the Zscaler and Cisco applications are described in this section.

Note

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
ZIA Test Page	Information on your Zscaler cloud.
Zscaler cloud IP data center IP Information	ZIA IP and VPN host name information by data center.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
ZIA Test Page	Information on your Zscaler cloud.
Zscaler Cloud IP Data Center IP Information	ZIA IP and VPN host name information by data center.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Cisco SD-WAN

Cisco SD-WAN powered by Cisco Viptela and Cisco IOS XE is a highly secure, cloud-scale architecture that is open, programmable, and scalable. Through the Cisco SD-WAN Manager, you can quickly establish an SD-WAN overlay fabric. Use it to connect data centers, branches, campuses, and colocation facilities to improve network speed, security, and efficiency.

This document assumes you have the Cisco SD-WAN controllers already built and operational, either through the Cisco cloud service or on-premises. Zscaler recommends that you use Cisco SD-WAN Manager to configure and manage the WAN Edge routers.

Make sure that the WAN Edge devices are already connected to the controllers in the SD-WAN overlay, and a basic device template configuration from Cisco SD-WAN Manager has been deployed on them. See the following:

- [Appendix A: Cisco Branch Base Feature Templates and Configuration Values Used](#) for base device and feature template configurations.
- [Appendix B: Tunnel Configuration Summary \(Feature and Device Templates\)](#) for a summary of feature templates required to configure the Zscaler tunnel use cases.
- [Appendix C: Cisco IOS XE SD-WAN CLI Configuration](#) and [Appendix D: Cisco vEdge CLI Configuration](#) reflect CLI-equivalent configurations for Cisco IOS XE SD-WAN and Cisco vEdge, respectively.

This document requires administrator login credentials to Cisco SD-WAN Manager and SSH administrator login credentials to the WAN Edge routers.

Cisco Resources

The following table contains links to Cisco support resources.

Name and Link	Description
Cisco SD-WAN Design Guide	An overview on the Cisco SD-WAN solution.
Cisco SD-WAN End-to-End Deployment Guide	Additional information on deploying a Cisco SD-WAN network from end-to-end.
Cisco EN&C Validated Design and Deployment Guides	Simple, modular, use-case based design and deployment guidance to provide you with validated designs and best practices.
Cisco SD-WAN Community Resources	Resource pages and discussion boards.
Cisco Catalyst SD-WAN	Additional Cisco SD-WAN resources.

Define

The following section explains Cisco SD-WAN concepts.

Cisco Catalyst SD-WAN Design Overview

Enterprises can take advantage of secure local internet breakout by using Cisco Catalyst SD-WAN combined with Zscaler. Using Cisco Catalyst SD-WAN, the network administrator can decide what traffic is forwarded to Zscaler, using either GRE or IPSec tunnels.

The following example topology shows a Cisco Catalyst SD-WAN network with two transports (MPLS and internet) and the SD-WAN control components reachable through the internet cloud. Two branch sites are shown with a data center site. SD-WAN fabric (IPSec) tunnels are built between each WAN Edge router at each site for corporate traffic. A separate pair of GRE or IPSec tunnels are built from each branch router to ZIA Public Service Edge for access to internet and SaaS applications. If the local internet transport fails, traffic can traverse the SD-WAN overlay over the MPLS transport to the data center and access the internet from there.

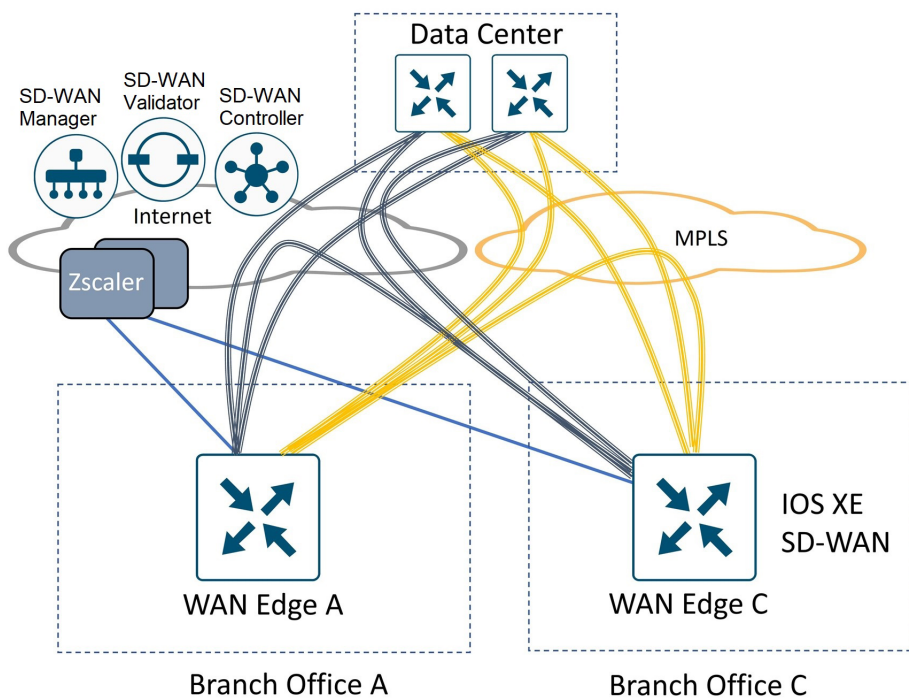


Figure 2. Example SD-WAN and ZIA network

Feature Background and History

Note

Testing was done on 20.9 SD-WAN Manager, 20.9/20.6 vEdge versions, and 17.9 IOS XE SD-WAN versions. To learn more, refer to [Cisco Recommended SD-WAN Software Versions for Controllers and WAN Edge Routers](#) for information on the latest recommended release.

The following sections discuss specifics for different versions of the Cisco SD-WAN software releases.

Support through Cisco Catalyst SD-WAN 20.3/17.3 code versions (Traditional Active/Standby Tunnels and L7 Health Checking)

Early support for Zscaler tunnels included GRE or IPSec tunnels that are configured manually through Interface VPN templates in SD-WAN Manager, either in the transport VPN (IPSec or GRE) or service VPN (IPSec). A single active/standby tunnel pair is supported per WAN Edge router, along with L7 health check probes running between the WAN Edge router and the respective ZIA Public Service Edge. The active tunnel is typically connected to a primary Public Service Edge while the standby tunnel is connected to a secondary Public Service Edge. To learn more, refer to the [Zscaler Internet Access \(ZIA\) and Cisco SD-WAN Deployment Guide](#).

Note

The recommended way to configure SIG tunnels is through the SIG feature template, supported in Cisco SD-WAN 20.4/17.4 and later code versions.

Cisco Catalyst SD-WAN 20.4/17.4 code versions (Active/Active ECMP Tunnels and Traffic Steering through SIG Route and Centralized Data Policy using SIG Templates)

The following SIG enhancements were introduced in 20.4/17.4:

- A new SD-WAN Manager SIG feature template is introduced where you can configure up to 4 active/backup tunnels pairs to get the benefit of ECMP load balancing and allow more traffic bandwidth to be redirected to Zscaler. Zscaler tunnels are configured manually using the SIG feature template and choosing the third-party SIG Provider option. Only one SIG template is attached per device, and it must be GRE or IPSec, and not a mix of both per device.
- You can assign weights to the tunnels so that more traffic can traverse one tunnel over another if necessary.
- Traffic redirection into the tunnels is accomplished through a new SIG service route, which reduces the administrative overhead of configuring static routes that require site-specific next-hop IP addresses. The SIG service route tracks the state of the SIG tunnels, and if all are marked down, the SIG service route is removed from the routing table.
- You can also configure traffic redirection to Zscaler through centralized data policy, giving additional flexibility and granularity to choose specific application traffic.

Note

Moving forward, all new features (including SIG route and SIG data policy) leverage the SIG feature template. The SIG feature template allows you to configure automatic Zscaler and Umbrella tunnels, and manual third-party tunnels. Tunnel types include IPSec and GRE.

Cisco Catalyst SD-WAN 20.5/17.5 code versions (Zscaler Automatic IPsec Tunnel Provisioning)

In 20.5/17.5, there were several updates to the SIG feature template, including accommodations for automatic discovery and tunnel provisioning to the closest Zscaler data centers based on geolocation. Layer 7 Health checking is automated and supported for vEdge WAN Edge routers as well. Only one automatic active/standby Zscaler tunnel pair is supported in this version.

Cisco Catalyst SD-WAN 20.6/17.6 code versions (L7 Health Checks for IPsec Auto Tunnels for IOS XE SD-WAN routers and Cloud onRamp for SaaS over SIG Tunnel Support)

In 20.6/17.6, up to four pairs of active/standby IPsec tunnels are supported with automatic provisioning. L7 automated health checking is introduced as an in-product BETA feature for Zscaler IPsec Auto Tunnels for IOS XE SD-WAN routers. Official support for IOS XE SD-WAN L7 Health checking for automatic IPsec Zscaler tunnels is in version 20.6.2/17.6.2. You can use loopback interfaces as source interfaces for SIG tunnels for IOS XE SD-WAN routers only. Cloud OnRamp for SaaS over SIG tunnels is also a newly supported feature in this version.

Cisco Catalyst SD-WAN 20.7/17.7 code versions (VRRP Interface Tracker support for SIG Tunnels)

In 20.7/17.7, VRRP tracking for SIG and Tunnel interfaces is supported for IOS-XE SD-WAN routers. If a tunnel that is being tracked goes down, the VRRP primary WAN Edge router decrements its priority and the backup VRRP router transitions to the primary role. For vEdge, this feature was introduced in 20.4 in CLI, but SD-WAN Manager feature template support is introduced in 20.7.

Cisco Catalyst SD-WAN 20.8/17.8 code versions (Multiple SIG Enhancements)

The following SIG enhancements were introduced in 20.8/17.8:

- Centralized data policy fallback support: In the event of a SIG tunnel failure, You can take the SD-WAN overlay routes to avoid traffic blackholing (IOS XE SD-WAN only).
- ECMP based on source IP address: This allows you to direct traffic with the same source IP address to the same SIG tunnel instead of being potentially hashed to multiple SIG tunnels (IOS XE SD-WAN only).
- IPsec tunnel creation improvements for active/active SIG tunnels: This feature ensures that IPsec control and data connections are pinned and exit out the same physical interface. You can potentially route DNS traffic for L7 health checks out the incorrect interface when using loopback interfaces as the source interface for GRE or IPsec tunnels, so a configuration workaround is required in this and previous releases (IOS XE SD-WAN only).
- Layer 7 health check for generic (manual) SIG tunnels using the SIG feature template.

Cisco Catalyst SD-WAN 20.9/17.9 code versions (Zscaler Automatic GRE Tunnel Provisioning and SIG Tunnel Monitoring)

In 20.9/17.9, the following SIG enhancements were introduced:

- Automatic provisioning of GRE-based SIG tunnels, which includes support for L7 health checks, SIG data policy fallback, multiple active/active tunnels with weighted load-balancing option, and ECMP traffic load balancing based on Source IP address (IOS XE SD-WAN only).
- SIG tunnel monitoring, which provides enhanced monitoring and visibility for automatic SIG tunnels, which includes state of the SIG tunnel, and various security event notifications (IOS XE SD-WAN and automatic SIG tunnels only).
- Global SIG credentials template enhancement: With this enhancement, there is no longer a way to create a separate SIG credentials feature template and a requirement to manually add the SIG credentials template to the device template under the Additional Templates section. Now, a credentials template is filled out only one time when a SIG feature template is first created with a specific SIG provider. The credentials template is added automatically to a device template when the SIG feature template is added.

The SIG features and hardware/software support are summarized in the following tables:

Feature	IOS XE SD-WAN Min Code Version	vEdge Min Code Version	L7 Health Check Support (IOS XE SD-WAN/vEdge)
IPSec or GRE Manual (3rd party/generic) tunnels using SIG Feature Templates (Up to 4 active/standby tunnel pairs with 4-tuple ECMP/weighted load balancing)	17.4	20.4	17.8/ 20.8*
IPSec Zscaler Auto Tunnels (One active/standby tunnel pair)	17.5	20.5	N/A/ 20.5
IPSec Zscaler Auto Tunnels (Up to 4 active/standby tunnel pairs with 4-tuple ECMP/weighted load balancing)	17.6	20.6	17.6.2/20.6
GRE Zscaler Auto Tunnels (Up to 4 active/standby tunnel pairs with 4-tuple ECMP/weighted load balancing)	17.9**	N/A	17.9/ N/A

*If you need earlier GRE support requiring L7 health checks, use traditional active/standby tunnels utilizing Interface VPN templates. Use Auto Tunnels and SIG feature templates whenever possible.

**Caveat: GRE auto tunnel loopback as a source interface tunnel is not supported until 17.9.2.

Feature	IOS XE SD-WAN Min Code Version	vEdge Min Code Version	Fallback Routing Support (IOS XE SD-WAN/vEdge)
SIG Route	17.4	20.4	17.4/ 20.4
SIG Data Policy	17.4	20.4	17.8/ N/A*

*Without Fallback Routing support for SIG data policy, SIG traffic can blackhole if the SIG tunnels are down. In earlier code versions, rely on the SIG route for SIG traffic if possible, so SIG traffic falls back to routing when the SIG tunnels are down.

Feature	IOS XE SD-WAN Min Code Version	vEdge Min Code Version
Cloud OnRamp for SaaS via SIG Tunnel	17.6	20.6
VRRP Interface Tracker Support for SIG Tunnels	17.7	20.7 (20.4 in CLI)
SIG ECMP based on Source IP address	17.8 (CLI add-on template)	N/A
SIG Tunnel Monitoring	17.9	N/A
Global SIG Credentials Template Enhancement	17.9	20.9

Design

The following sections describe the architecture behind Cisco SD-WAN deployments.

There are several points to consider when designing for Cisco Catalyst SD-WAN and Zscaler integration. It is also important to understand what features are supported in any code version, as this can affect the SIG configuration and design.

- What tunnel protocol do you use? IPSec or GRE? Are there any design restrictions related to the tunnel protocol type?
- What tunnel liveness methods are available? Do tunnels support L7 health checking?
- What is the ECMP routing behavior for multiple, active tunnels?
- Where are your primary vs secondary Zscaler data centers located?
- What are the high availability and load balancing options?
- What method do you use to redirect traffic from service-side VPN to the SIG tunnel? Is a fallback method supported?
- Are you using single Edge or dual Edges?
- Are you using automatic or manual tunnels?

The following topics address these considerations.

GRE and IPSec Tunnels

Zscaler supports both GRE and IPSec tunnels from Edge devices to transport internet traffic that first traverses the ZIA Public Service Edge.

Note

An active IPSec tunnel is defined by a unique 4-tuple of source IP address/interface, source port, destination IP address, and destination port pair. Multiple IPSec tunnels can exist that reference the same source or destination IP address, but each tunnel must have a unique 4-tuple for the tunnel to be up and operational. IPSec tunnels are dynamically added on the Zscaler side, so their source IP addresses and source ports can change.

GRE tunnels do not have source or destination ports and are statically mapped using source IP address via API or manual configuration on the Zscaler side, meaning that multiple GRE tunnels cannot be sourced from the same IP address. Also, since they are mapped manually, their source IP addresses cannot change when mapped.

Packet Format and NAT

GRE is neither TCP nor UDP but has its own protocol number (47). Because GRE is a protocol without source or destination ports, GRE packets can't be translated by Port Address Translation (PAT) devices. You can translate the source IP address of a GRE packet with Network Address Translation (NAT) with no overload, which includes static or dynamic NAT, where a single IP address is mapped only to a single publicly routable IP address. This is because no ports must be mapped.

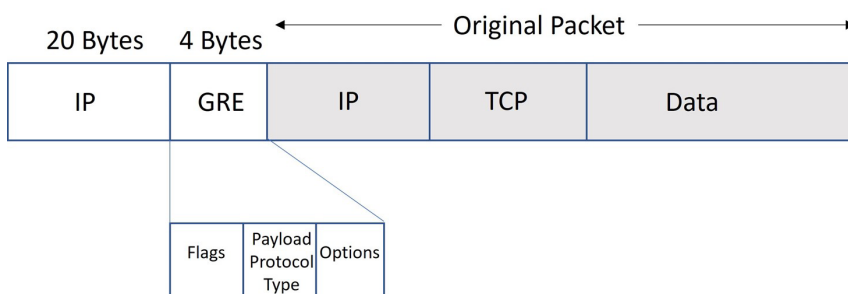


Figure 3. GRE packet encapsulation

An IPSec packet uses ESP—also a protocol without ports and unusable by PAT devices. IPSec traffic can use NAT-T to transport packets. If both ends of the IPSec connection support NAT-T, then Nat-Discovery packets are exchanged during the ISAKMP exchange. If NAT is detected, then ISAKMP packets change from UDP port 500 to UDP port 4500. ESP data packets are encapsulated inside a UDP packet with source and destination ports equal to 4500. Now you can translate the packet by a PAT device.

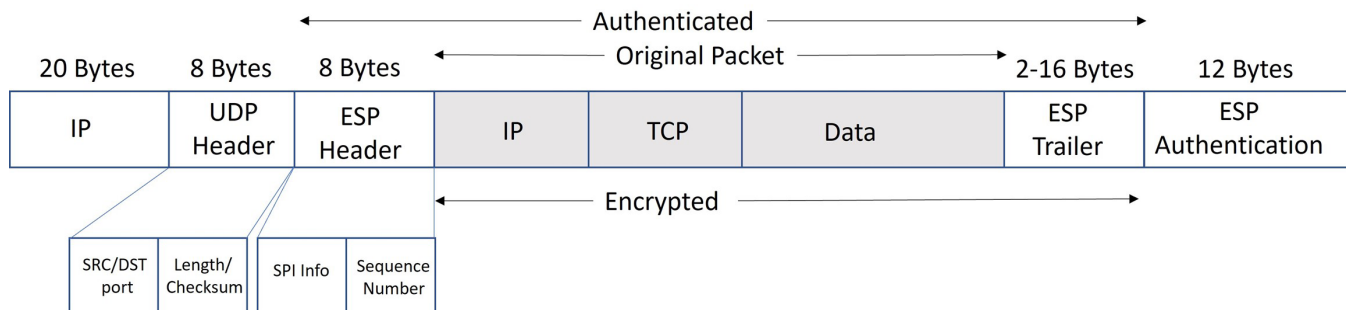


Figure 4. IPSec packet encapsulation (Tunnel Mode)

Throughput

Zscaler GRE tunnels support higher throughput than IPSec tunnels in the Zscaler cloud. IPSec tunnels can support 400 Mbps each while GRE tunnels can support 1 Gbps each. Contact your Zscaler Account team for more information on bandwidth support. Bandwidth support can vary depending on the Zscaler cloud and ZIA Public Service Edge you are connecting to.

Tunnel Source IP Addressing

Zscaler GRE tunnels require a source IP address on the WAN Edge router that is a separate, unique IP public address per destination that is constant or static. This source IP address is registered on the ZIA through APIs and is used as authentication for the GRE tunnel. Zscaler IPSec tunnels are either static or dynamic addressing and is not required to have a separate, unique IP public address (as long as the source port varies per tunnel destination). IKEv2 is used for IPSec tunnel authentication to ZIA.

Tech Tip

GRE tunnels are not influenced by NAT defined on the interface of a WAN Edge router; their source IP address remains unchanged as it transits the WAN Edge router. GRE tunnels must be either directly sourced by a public IP address or be subjected to a One-to-One NAT translation by an external device. Source IP address for IPSec tunnels, on the other hand, are subjected to NAT defined on the interface of a WAN Edge router as traffic transits.

Tunnel Liveliness

GRE Keepalives and DPD

GRE Keepalives for GRE tunnels and DPD for IPSec tunnels are traditional methods for a local router to determine whether the remote router at the end of a tunnel is reachable and able to forward traffic. Zscaler best practices advises that you send GRE Keepalives and DPD packets no more than once every ten (10) seconds.

Tech Tip

If the router sits behind any NAT device, GRE keepalives are not passed. If the router is behind a NAT device, Zscaler recommends that you disable GRE keepalives by setting the interval and retries to zero (0). GRE data packets can't be translated by PAT devices, but can be translated through a NAT device. NAT devices have only one IP address mapped to one publicly routable IP address because port mapping isn't required.

Cisco IOS XE SD-WAN routers do not support GRE keepalives through feature templates, only Cisco vEdge routers do. For Cisco IOS XE SD-WAN routers, you can configure GRE keepalives through the CLI or CLI add-on feature templates. Cisco vEdge routers currently support only periodic DPD. On-demand DPD is currently the default for Cisco IOS XE SD-WAN routers.

Layer 7 Health Checks

GRE Keepalives and DPD can validate whether the network path is up between the tunnel source and destination, but the mechanisms cannot verify whether a particular service or application is up and operational beyond the tunnel and ZIA Public Service Edge.

An L7 health check monitors latency and reachability based on HTTP request and response probes to a URL that is reachable through the Zscaler tunnels, and allows you to fail over to an alternate tunnel when reachability fails or latency degrades beyond an acceptable threshold.

To check the health of the application stack of the ZIA Public Service Edge, Zscaler recommends not performing L7 health checks to commonly visited websites. Instead, use the following non-public URL for the tracker. It is only reachable through a Zscaler tunnel: `http://gateway.<Zscaler Cloud Name>.net/vpntest`. Do not send L7 health checks more than one every 5 seconds.

ECMP Routing

The following sections explain ECMP routing.

4-Tuple ECMP

In the presence of multiple, equal-cost active paths, traffic is normally routed to an interface based on the hashing of the IP flow 4-tuple (source IP address + destination IP address + source port + destination port). Because it is based on a hash, the traffic distribution might not be exactly equal across the tunnels but with enough variability in IP addressing and ports in the network traffic, traffic distribution gets more evenly distributed across the ECMP interfaces.

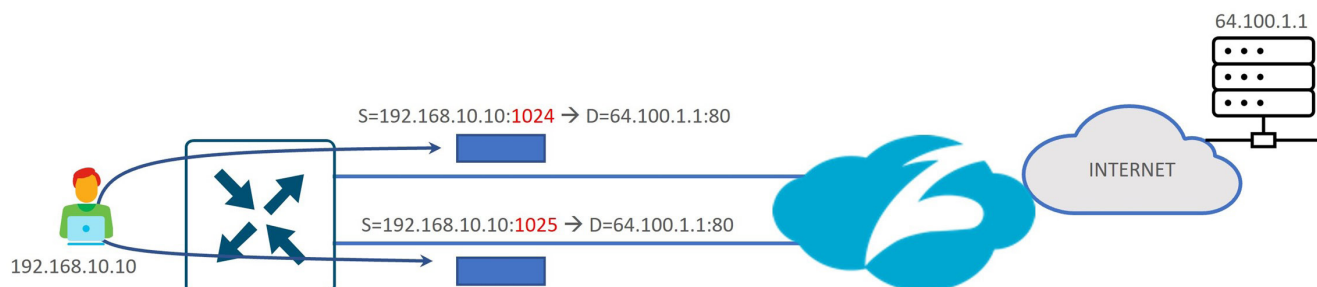


Figure 5. 4-Tuple ECMP routing

There are several applications that are known to fork off multiple sessions for a single user session (O365, Google Services, Facebook, etc.). If you have two active SIG tunnels that are pinned to two different Zscaler data centers, ECMP could pin flows from a single user to separate tunnels. The cloud application could see different client IP addresses for the same session, since NAT is applied to their source IP addresses from two different data centers, and thus, session resets from the server could occur.

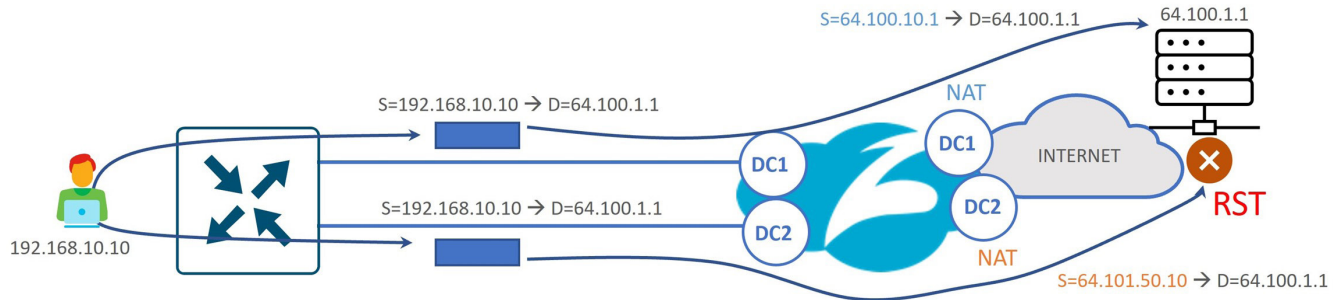


Figure 6. Single user session hashing to multiple data centers using 4-tuple ECMP

Note

Be careful when designing using multiple active/active or active/standby links with 4-tuple hashed ECMP (default setting). Especially in the case of routed dual-Edge sites, you must be careful that hashed sessions for the same user are not distributed over multiple links going to different Zscaler data centers. You must also consider how traffic is hashed during failure scenarios as well.

There might be cases where there are active/active tunnels going to the same Zscaler data center and users could be experiencing application performance issues due to a single user session taking multiple, equal-cost paths if tunnels are experiencing varying levels of latency or loss. In these cases, you could ensure that users are not being hashed to different Edge devices or different transports.

Source IP-Based ECMP

Starting in 20.8/17.8, you can configure ECMP to hash according to source IP rather than a 4-tuple. This would allow you to direct traffic with the same source IP address to the same SIG tunnel instead of being potentially hashed to multiple SIG tunnels. Note that this is supported only by IOS XE SD-WAN routers. It is enabled with the command `ip cef load-sharing algorithm src-only` through an add-on CLI template. This gives you more design flexibility in configuring your tunnel destinations and setting up active/standby pairs.

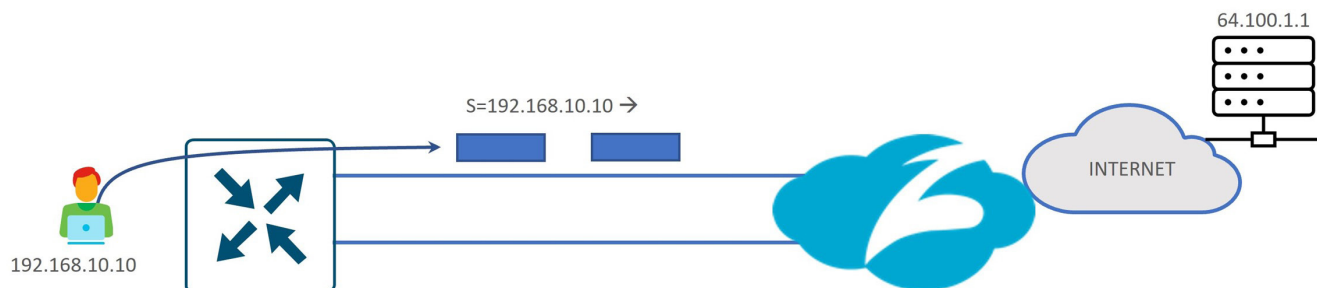


Figure 7. Source IP-based ECMP routing

Note

In Edge versions prior to 17.12, you can figure source IP-based ECMP only when the WAN Edge router is in CLI mode. If you try to use an add-on CLI template, the ECMP configuration returns to the default, which is 4-tuple. This affects hardware-based IOS XE SD-WAN routers and is fixed in 17.12.

Primary vs. Secondary Data Center Placement

The primary Zscaler data center (DC) is typically chosen to be the closest data center to your remote site and used for your active tunnels. The secondary data center is typically chosen as the next closest data center to your remote site and used for your standby tunnels.

It is not recommended to design active/active tunnels going to multiple data centers, even if you make use out of source IP-based ECMP. Latency/performance could vary from user to user depending on which tunnels are taken to Zscaler.

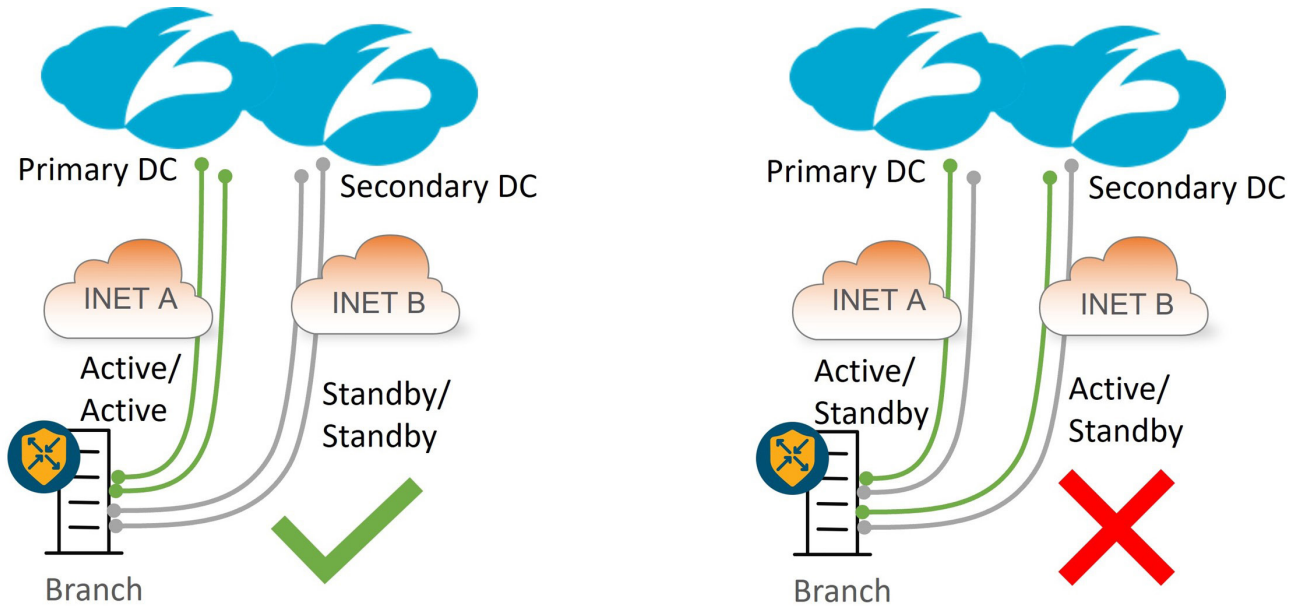


Figure 8. Active/Standby Zscaler tunnels going to Primary/Secondary DCs

Zscaler Active/Standby Tunnel Combinations

The following shows examples of different active/standby tunnel combinations to ZIA over dual internet and hybrid deployments (MPLS and internet). The deployed tunnels are either GRE or IPSec, and cannot be a combination of both. Up to four active/standby pairs are supported. Route or policy directs traffic out the active tunnels to Zscaler. Standby tunnels are fully up and operational. However, traffic isn't forwarded over these standby tunnels until their corresponding active tunnel pair partner is marked down or exceeds the latency threshold of the L7 health checks.

One Active/Standby Tunnel Pair

The following diagram shows an example of one active and one standby tunnel deployment at sites with single and dual internet circuits. In hybrid deployments, an MPLS path might offer a backhauled path to the internet via an internet gateway at a data center or regional hub site. In either deployment, if the ZIA Public Service Edge or active tunnel becomes unreachable or exceeds the latency threshold (with L7 health checks enabled), then the standby tunnel is activated. In the hybrid deployment, if the internet networking (INET) transport goes down, or if both tunnels over the INET transport exceed the latency thresholds (with L7 health checks enabled), then traffic can still take the default route over the SD-WAN overlay over the MPLS transport to the data center. Traffic can access the internet, either through an on-premises security stack or via a separate SIG tunnel originating from the data center hub router.

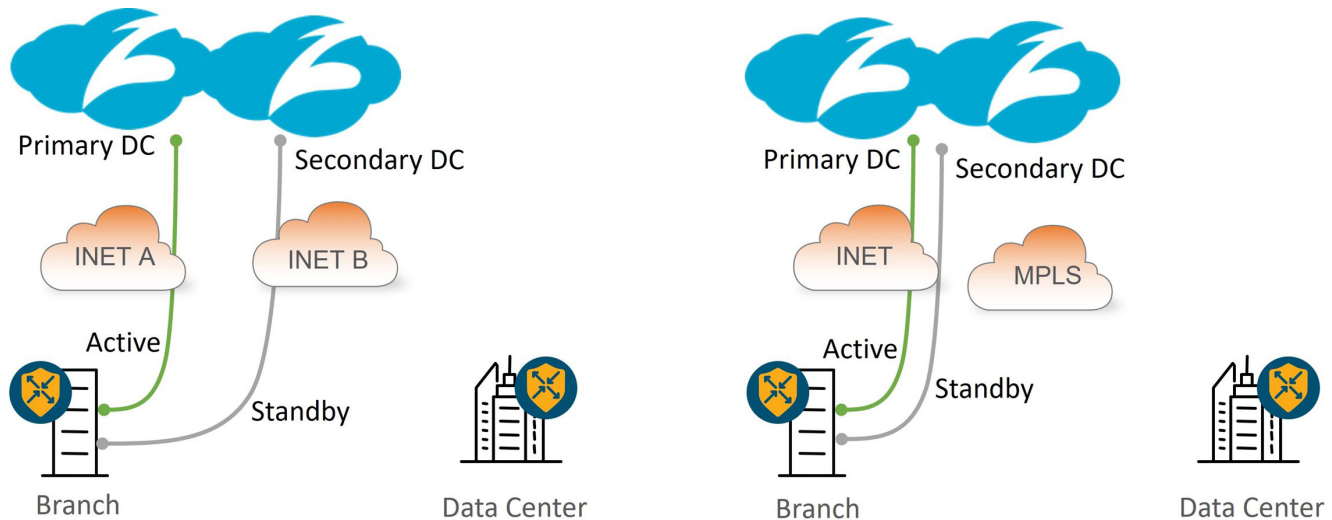


Figure 9. Active/Standby tunnel deployment on dual INET and hybrid transports

Multiple Active/Active Tunnels with ECMP

Increased cloud traffic and bandwidth limits on Zscaler tunnels require support for multiple active tunnels.

The following diagram shows an example of an active/active tunnel deployment at sites with single and dual internet circuits. In either deployment, if an active tunnel becomes unreachable or exceeds the latency threshold (with L7 health checks enabled), then traffic is reshaped to one of the remaining tunnels. In the hybrid deployment, if the INET transport goes down, or if all tunnels over the INET transport exceed the latency thresholds (with L7 health checks enabled), then traffic can still take the default route over the SD-WAN overlay over the MPLS transport to the data center. Traffic can access the internet through an on-premises security stack or via a separate SIG tunnel originating from the data center hub router. In either deployment, if the ZIA Public Service Edge becomes unreachable, traffic can fall back to the data center over the SD-WAN overlay.

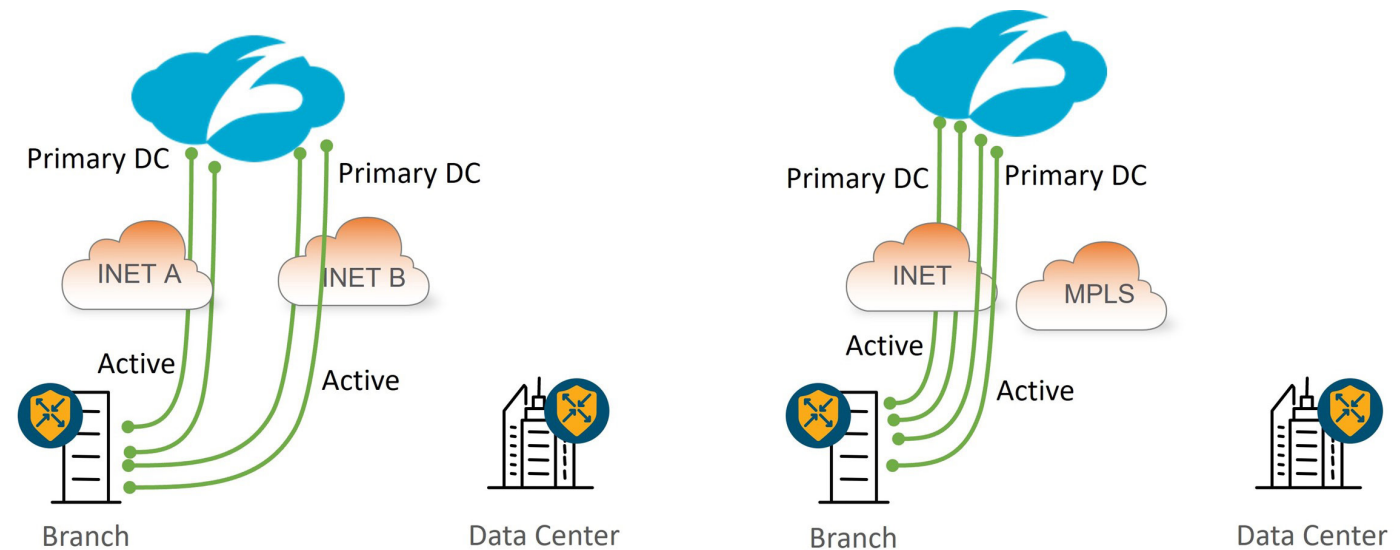


Figure 10. Multiple Active/Active tunnels on dual INET and hybrid transports

Multiple Active/Standby Tunnel Pairs

The following diagram shows an example of a multiple active/standby tunnel pair deployment at sites with dual internet and hybrid circuits. In either deployment, if an active tunnel becomes unreachable or exceeds the latency threshold (with L7 health checks enabled), then its corresponding standby tunnel is activated. In the hybrid deployment, if the INET transport goes down or if all tunnels over the INET transport exceed the latency thresholds (with L7 health checks enabled), then traffic can still take the default route over the SD-WAN overlay over the MPLS transport to the data center. Traffic can access the internet through an on-premises security stack or via a separate SIG tunnel originating from the data center hub router. In either deployment, if the ZIA Public Service Edge becomes unreachable, traffic can fall back to the data center over the SD-WAN overlay.

Note

In this scenario, 4-tuple ECMP is being used which is why the standby tunnels are going to the same DC as the active tunnels. You do not want a single user session to go to two different DCs if one of the standby links were to go active. Starting in 20.8/17.8 code, you can configure source IP-based ECMP, and use a secondary DC for the standby tunnels instead.

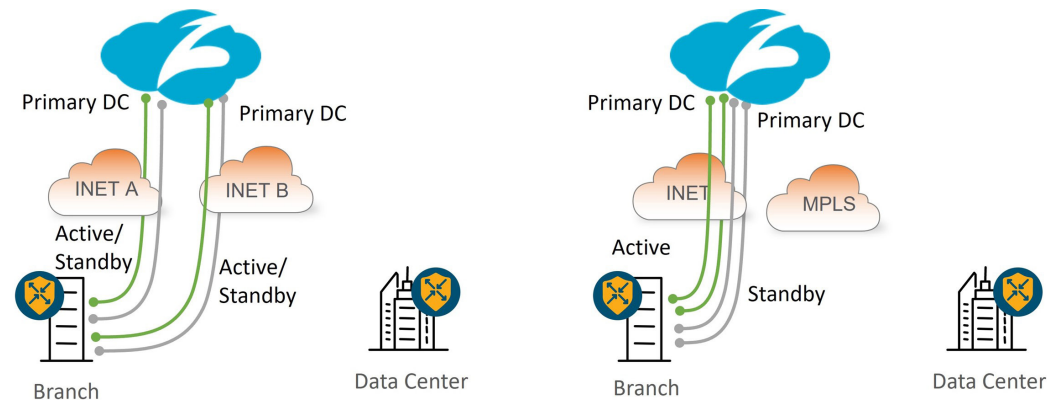


Figure 11. Multiple Active/Standby tunnel pairs

Active/Active Tunnels with Weighted Load Balancing

The following diagram shows an example of an active/active tunnel deployment spread across two internet transports. Available bandwidth might differ between the transports so you can assign weights to each tunnel and different traffic bandwidth amounts traverse each transport. In this example, weights are configured for each tunnel so that 80% of the traffic traverses INET A, while 20% of the traffic traverses the INET B. If an active tunnel becomes unreachable or exceeds the latency threshold (with L7 health checks enabled), then traffic is reshaped to one of the remaining tunnels.

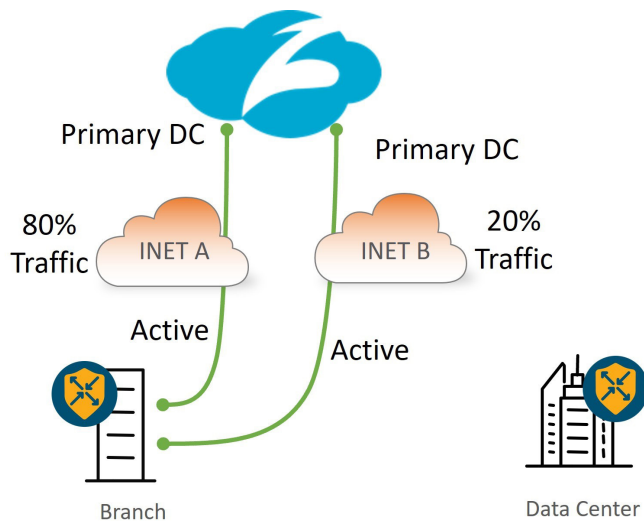


Figure 12. Active/Active weighted tunnel deployment on two internet transports

User Traffic Redirection

After the GRE or IPSec tunnels are configured and activated, there are two ways to direct user traffic to the tunnel:

- With a static route to rely on destination-based routing (typically a default route where all internet-bound traffic is sent). 20.4/17.4 code version introduces a new type of route for Zscaler or other third-party tunnels called a Service Route, which has a next hop that points to the SIG service.
- With a centralized data policy that allows you to customize the traffic sent to the Zscaler service. 20.4/17.4 supports centralized policy for both Cisco vEdge and Cisco IOS XE SD-WAN devices where you can rely on prefix-lists and applications lists to direct desired traffic to the SIG service.

Tech Tip

If both service routes and centralized policy are configured to direct user traffic, centralized policy takes precedence. You might want to configure both a SIG service route and policy in dual-edge branches with Layer 3 routing. The SIG service route is redistributed into a routing protocol at the local site. If the SIG tunnels become unreachable on an edge router, the route is withdrawn so traffic is directed to the opposite edge with active SIG tunnels. After traffic reaches the edge router with active SIG tunnels, centralized policy (or service route) is used to direct traffic to the SIG tunnel.

Fallback routing was not introduced for centralized policy until 20.8/17.8 for Cisco IOS XE SD-WAN only. Without fallback routing, traffic can blackhole when the SIG tunnel becomes unavailable. Use a SIG service route for SIG traffic instead as a workaround.

WAN Edge with Zscaler Site Tunnel Design

This section covers the various aspects of single WAN Edge and dual WAN Edge site designs with Zscaler integration. Each WAN Edge router supports up to 4 active/standby tunnel pairs. For multiple active/standby tunnel pairs, consider using IP source-based ECMP for load-balancing traffic.

Note

The source IP address of an IPSec tunnel is subjected to NAT/PAT defined on the WAN Edge interface, while the source IP address of a GRE tunnel is not. The source IP address of a GRE tunnel will pass unchanged. Note that NAT must still be defined on each physical interface where Zscaler tunnels are sourced for both GRE and IPSec tunnels so API calls can succeed.

In addition, if an external device is used to NAT the source IP address of a tunnel, IPSec tunnels can use dynamic NAT/PAT, while GRE tunnels each must use unique, One-to-One NAT addressing.

Single WAN-Edge Design

This section shows a few examples of single WAN Edge designs with Zscaler integration.

Hybrid transport with 1 active/standby tunnel:

- IPSec: The tunnel source for both the active and standby tunnels is the INET A physical interface, which can be a publicly routable or a private IP address. If it is a private address, NAT/PAT is required by an external device to translate the tunnel source IP address into a publicly routable IP address.
- GRE: The tunnel source for both the active and standby tunnels is the INET A physical interface, which can be a publicly routable or a private IP address. If it is a private address, One-to-One NAT is required by an external device to translate the tunnel source IP address into a publicly routable IP address.

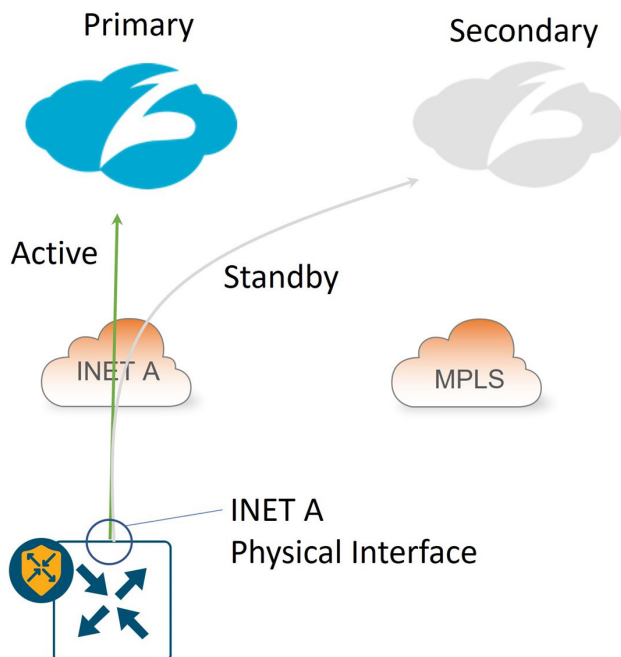


Figure 13. Single WAN Edge, Hybrid Transport, one Active/Standby Zscaler Tunnel

Hybrid transport with multiple active/standby tunnels:

- IPsec: The tunnel source is a loopback interface for each active/standby pair. You can privately address the loopback interfaces. If the INET A interface is privately addressed, NAT/PAT on an external device is needed to make the tunnel source IP addresses publicly routable.
- GRE: The tunnel source is a loopback interface for each active/standby pair. You can address the loopback interfaces either publicly or privately. If private addressing is used, you must translate each tunnel source IP address to a unique one-to-one publicly-routable address by an external device.

Note

With this design, a CLI add-on template for router local policy is required for successful L7 health checking for IOS XE SD-WAN routers. Also, there is no support for loopback interfaces as tunnel sources with the vEdge platform.

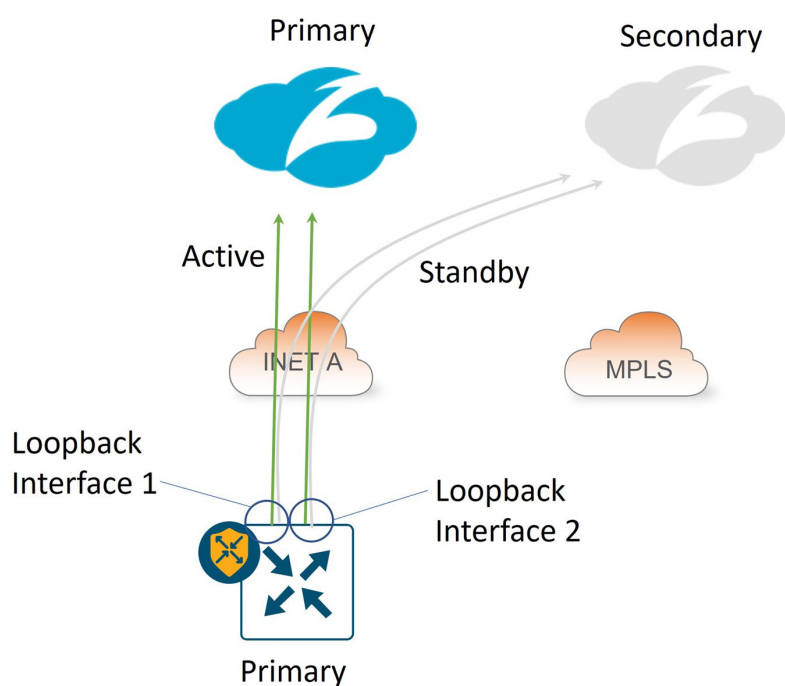


Figure 14. Single WAN Edge, Hybrid Transport, Multiple Active/Standby Zscaler tunnels

Dual-Internet transport with 1 active/standby tunnel per transport:

- IPsec: The tunnel source for the active/standby tunnel pair over INET A is the INET A physical interface, and for the active/standby tunnel pair over INET B is the INET B physical interface. You can use a publicly routable or a private IP address for the tunnel source IP address. If it is a private address, NAT/PAT is required by an external device to translate the tunnel source IP address into a publicly routable IP address.
- GRE: The tunnel source for the active/standby tunnel pair over INET A is the INET A physical interface, and for the active/standby tunnel pair over INET B is the INET B physical interface. You can use a publicly routable or a private IP address for the tunnel source IP address. If it is a private address, One-to-One NAT is required by an external device to translate the tunnel source IP address into a unique, publicly routable IP address.

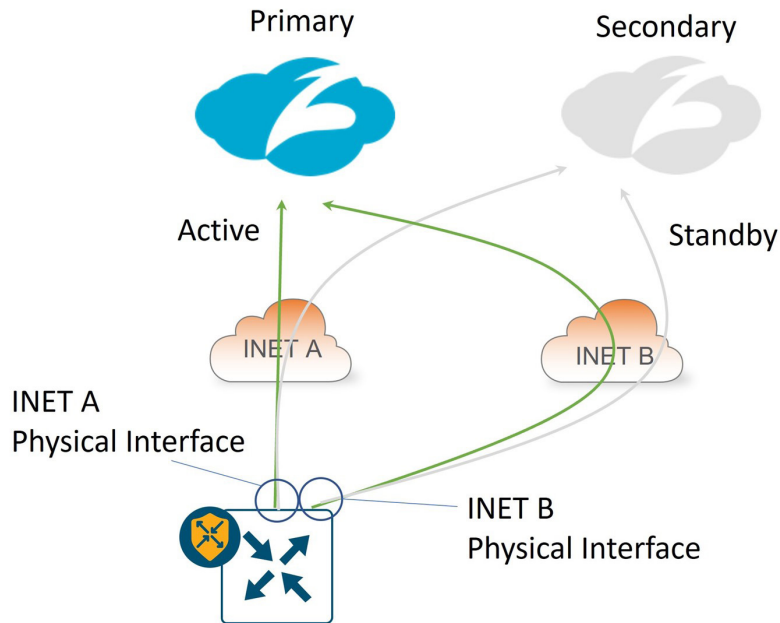


Figure 15. Single WAN Edge, Dual-Internet Transport, one Active/Standby tunnel per transport

Dual WAN Edge Design

This section shows a few examples of dual WAN Edge designs with Zscaler integration. The dual routers use VRRP or routing on the service side.

Hybrid transport with 1 active/standby tunnel per WAN Edge:

- **IPSec:** The tunnel source for the active/standby tunnel pair on both WAN Edge routers is the INET A physical interface, which for the B-side router, is on the TLOC extension link between the routers. You can use a publicly routable or a private IP address for the tunnel source IP address. The B-side router's tunnel source IP address is subjected to NAT/PAT on router A's INET A interface. If router A's INET A interface is a private address, NAT/PAT is required by an external device to translate the tunnel source IP address into a publicly routable IP address.
- **GRE:** The tunnel source for the active/standby tunnel pair on both WAN Edge routers is the INET A physical interface, which for the B-side router, is on the TLOC extension link between routers. You can use a publicly routable or a private IP address for the tunnel source IP address. The B-side router's tunnel source IP address is not subjected to NAT on router A's INET A interface and will stay unchanged. If either tunnel source is a private address, a One-to-One NAT is required by an external device to translate each tunnel source IP address into a unique, publicly routable IP address.

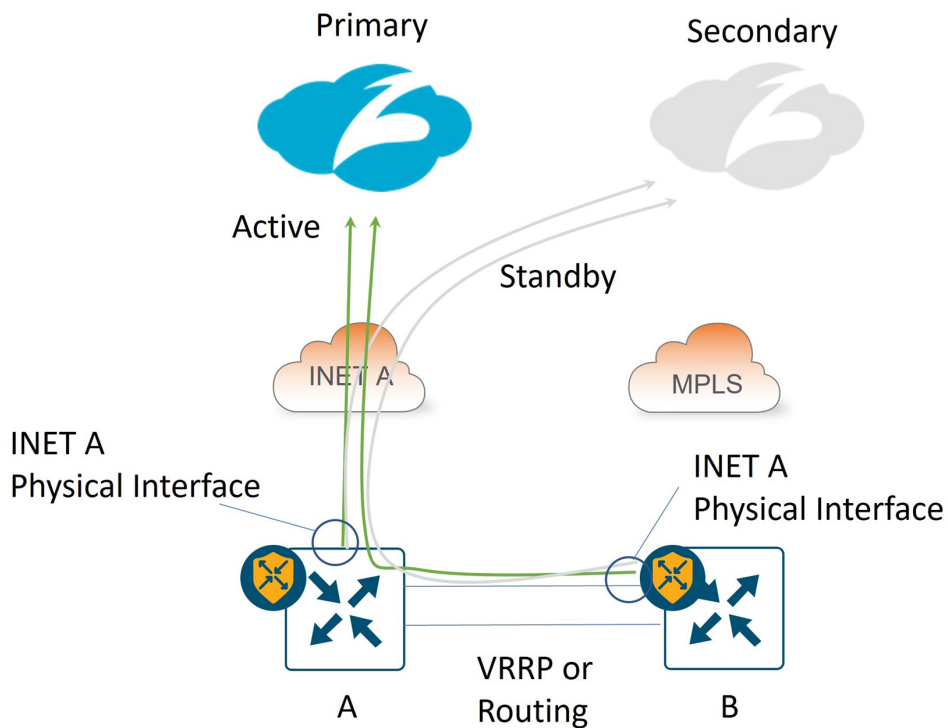


Figure 16. Dual WAN Edge, Hybrid Transport, one Active/Standby tunnel per WAN Edge

Dual-Internet transport with 1 active/standby tunnel per WAN Edge:

- **IPSec:** The tunnel source for the active/standby tunnel pair on WAN Edge A is the INET A physical interface, and for WAN Edge B, it is the INET B physical interface. You can use a publicly routable or a private IP address for the tunnel source IP address. If either INET A or INET B interface has a private address, NAT/PAT is required by an external device to translate the tunnel source IP address into a publicly routable IP address.
- **GRE:** The tunnel source for the active/standby tunnel pair on WAN Edge A is the INET A physical interface, and for WAN Edge B, it is the INET B physical interface. You can use a publicly routable or a private IP address for the tunnel source IP address. If either tunnel source is a private address, a One-to-One NAT is required by an external device to translate the tunnel source IP address into a unique, publicly routable IP address.

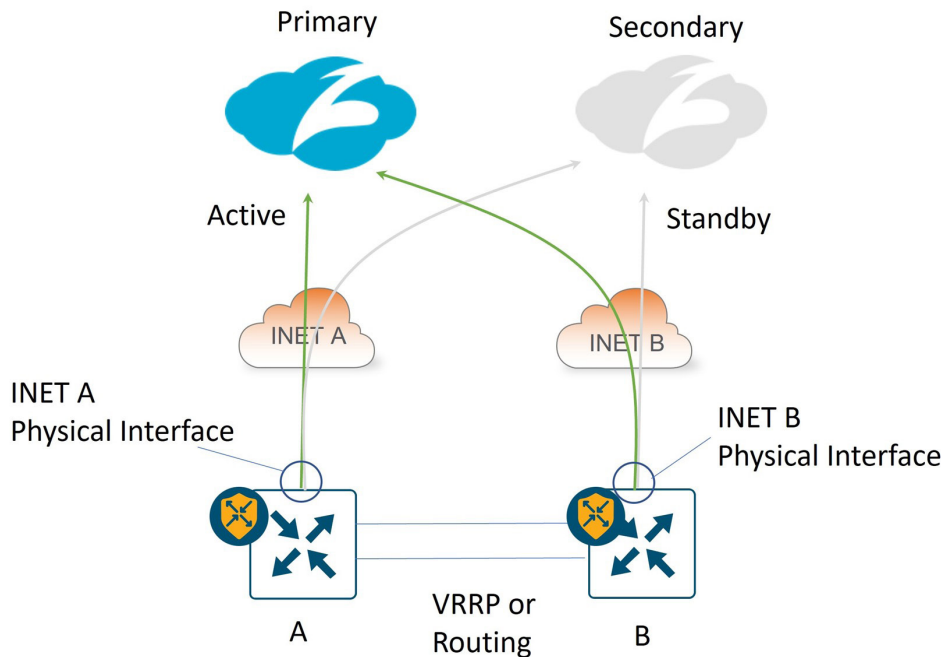


Figure 17. Dual WAN Edge, Dual Internet, one Active/Standby tunnel per WAN Edge

Dual-Internet transport with 2 active/standby tunnels per WAN Edge:

- **IPSec:** The tunnel source for the active/standby tunnel pair on both WAN Edge routers is each INET physical interface. You can use a publicly routable or a private IP address for the tunnel source IP address. The B-side router's INET A tunnel source IP address is subjected to NAT/PAT on router A's INET A interface, and the A-side router's INET B tunnel source IP address is subjected to NAT/PAT on router B's INET B interface. If the INET interfaces connecting directly to the transports are privately addressed, NAT/PAT is required by an external device to translate each tunnel source IP address into a publicly routable IP address.
- **GRE:** The tunnel source for the active/standby tunnel pair on both WAN Edge routers is each INET physical interface. You can use a publicly routable or a private IP address for the tunnel source IP address. The B-side router's INET A tunnel source IP address is not subjected to NAT on router A's INET A interface, and the A-side router's INET B tunnel source IP address is not subjected to NAT on router B's INET B interface—each GRE tunnel bypasses NAT. If any tunnel source is a private address, a One-to-One NAT is required by an external device to translate each tunnel source IP address into a unique, publicly routable IP address.

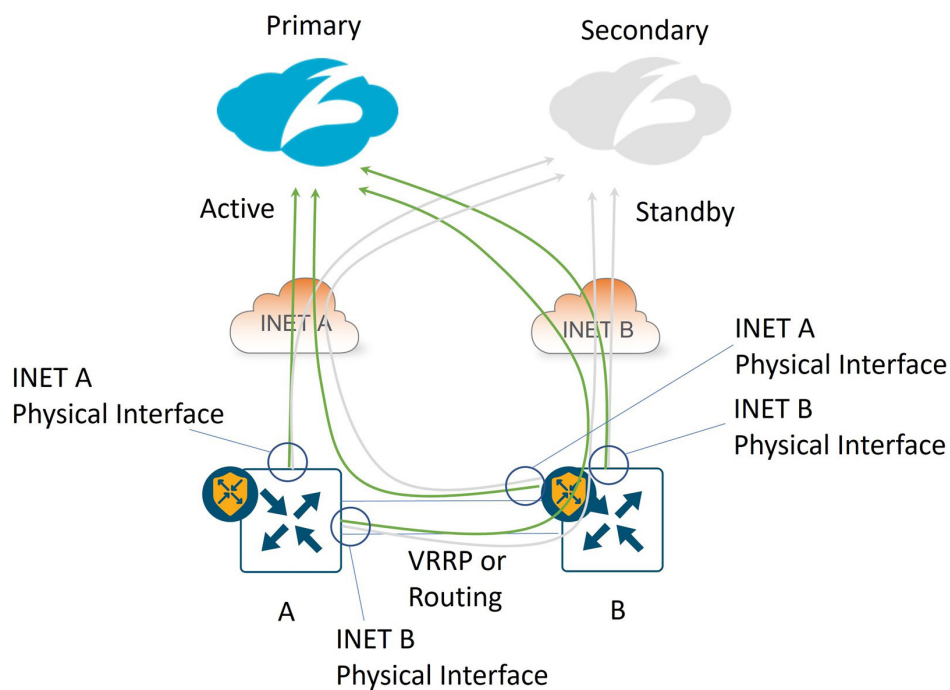


Figure 18. Dual WAN Edge, Dual Internet, two Active/Standby tunnels per WAN Edge

Dual WAN Edge with Zscaler Site Service-Side Design

For dual-router sites, you can achieve redundancy on the service-side VPNs with VRRP (layer 2) or routing (layer 3). When you are doing fallback routing with a SIG route or SIG data policy, you must be careful when you have a DIA NAT route present. If the SIG tunnel becomes inactive and traffic is subjected to fallback routing, traffic can take the DIA NAT default route (preferred over the default route from the overlay), and that might be undesirable.

VRRP

With VRRP, one WAN Edge router is declared primary and the other one standby on a per-VPN basis. The primary router forwards Zscaler traffic to Zscaler tunnels directly connected to the WAN Edge router, either through a SIG route or through centralized data policy. Use a different VRRP primary per VPN to utilize the Zscaler tunnels of both WAN Edge routers.

- VRRP interface tracker: Starting in 20.7/17.7, you can track and bind the SIG tunnel to the VRRP protocol. If the tunnel goes down, the VRRP primary decrements its priority and the backup router takes over the primary role.
- TLOC change preference: Starting in 20.7/17.7, the TLOC preference of the VRRP primary router gets increased by a configured value to avoid asymmetric traffic from other SD-WAN sites by ensuring traffic from across the overlay (WAN to LAN) is sent to the VRRP primary router. LAN to WAN traffic already uses the primary VRRP router as the default gateway.

Routing

With routing, be careful with the ECMP route hashing, as a single user session could be split between SD-WAN routers, each with their own active tunnels, which could have performance implications. You can set up routing metrics so that there is a primary/secondary router per VRF. Even if you are using data policy for SIG traffic forwarding, you can utilize the SIG route to advertise a default into the service-side routing protocol. Be careful with redistributing the SIG default route, the NAT DIA default route, and the overlay default route (default route that comes from another site through the SD-WAN overlay) into the service-side routing protocol at the same time—the default metric behavior of each varies depending on the routing protocol. The following is a summary of the behavior in this code version.

Baseline

The following shows the admin distance and metric for each default route type installed in the service VPN of the WAN Edge router. The SIG route is preferred with an admin distance of 2.

Default Route	Route Type	Admin Distance/Metric
SIG route (0.0.0.0/0)*	S (Static)	[2/65535]
NAT DIA route (0.0.0.0/0)	Nd (NAT DIA)	[6/0]
Overlay default route (0.0.0.0/0)	m (OMP)	[251/0]

OSPF

In order to inject a default route into OSPF, you need to use the default-originate option in the OSPF protocol. By default, the route appears in the next-hop router as an E2 route with an admin distance of 110 and a metric of 1, regardless of which route is installed in the routing table on the WAN Edge router.

```
O*E2 0.0.0.0/0 [110/1] via 10.219.100.6, 00:00:22, GigabitEthernet2/0/1
```


BGP

To inject the different default routes into EBGp on the service side, you must redistribute each protocol in the BGP feature template and include the default-originate configuration in BGP as well.

Use `redistribute omp` for the OMP default route, use `redistribute nat` for the DIA NAT route, and use `redistribute static` for the SIG route. By default, the following BGP routes with these default metrics are generated in this lab topology, with the NAT DIA route being preferred with a metric of 0.

Default Route	Route Type and Admin Distance/Metric
SIG route (0.0.0.0/0)	B* 0.0.0.0/0 [20/65535]
NAT DIA route (0.0.0.0/0)*	B* 0.0.0.0/0 [20/0]
Overlay default route (0.0.0.0/0)	B* 0.0.0.0/0 [20/1000]

To change the metrics to prefer the SIG route, define a router policy for each redistribution statement in the BGP feature template that needs a metric modified and add them to the localized policy attached to the WAN Edge router.

EIGRP

To inject the different default routes into EIGRP on the service side, you must redistribute each protocol in the EIGRP feature template.

Use `redistribute omp` for the OMP default route, use `redistribute nat-route` for the DIA NAT route, and use `redistribute static` for the SIG route. By default, the following External EIGRP routes with these default metrics are generated in this lab topology, with both the NAT DIA route and the OMP route being preferred with a metric of 5120.

Default Route	Route Type and Admin Distance/Metric
SIG route (0.0.0.0/0)	D*EX 0.0.0.0/0 [170/76805120]
NAT DIA route (0.0.0.0/0)*	D*EX 0.0.0.0/0 [170/5120]
Overlay default route (0.0.0.0/0)*	D*EX 0.0.0.0/0 [170/5120]

To change the metrics to prefer the SIG route, use a CLI add-on template to define the EIGRP metric associated with each redistribute statement. For example, the following assigns the best metric to the SIG default route, the second-best metric to the NAT DIA default route, and the third best metric to the OMP default route metric.

```
router eigrp eigrp-name
!
address-family ipv4 unicast vrf 1 autonomous-system 100
!
topology base
  redistribute static metric 1000000000 0 255 1 1500
  redistribute nat-route dia metric 1000000 100 255 1 1500
  redistribute omp metric 100000 1000 255 1 1500
```

SIG Service

Starting in 20.4/17.4, Zscaler tunnels can make use of the SIG service construct that was introduced in Cisco SD-WAN Manager for integration with Cisco Umbrella SIG. The SIG service keeps track of the state and next hop of the tunnels, in addition to redirecting traffic into the tunnels from the service VPN. Traffic redirection at the branch is implemented locally through service routing (defined in the service VPN feature templates) or as a centralized data policy action.

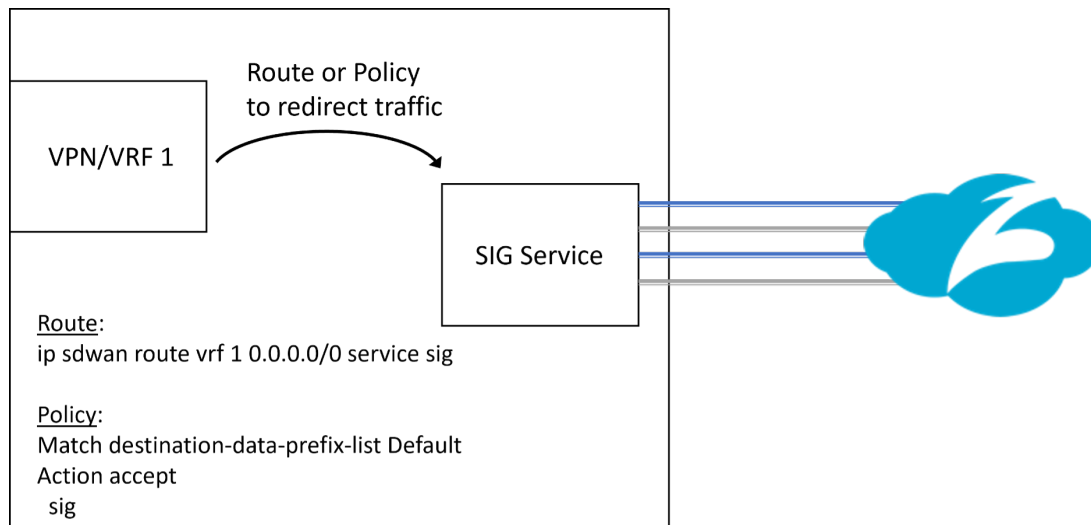


Figure 19. SIG service logical representation

New SIG Workflow

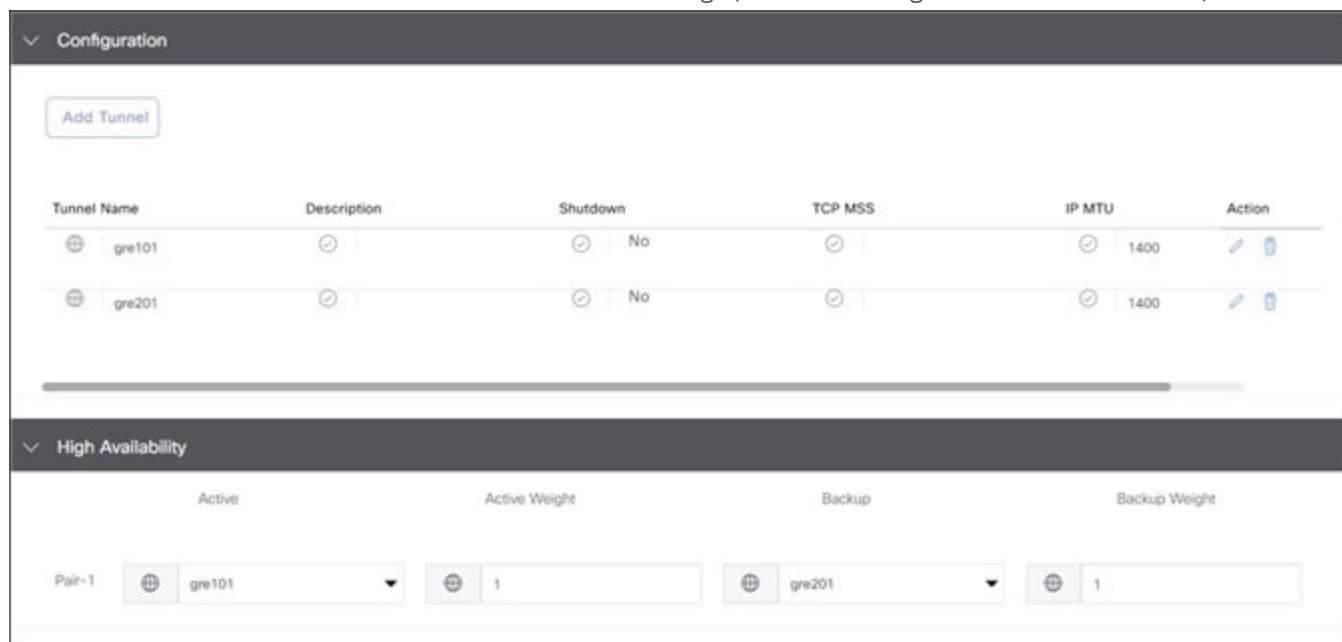
Starting in 20.4/17.4, a new unified SIG workflow is introduced with the SIG feature template, which greatly simplifies the SIG tunnel configuration process regardless of the tunnel type (Umbrella, Zscaler, other third-party IPsec or GRE tunnels). Only one SIG template is needed to configure multiple tunnels and is attached to the device template under the transport VPN. A configuration is introduced in IOS XE SD-WAN which allows multiple service VPNs to use the tunnel created with the SIG template (tunnel VRF multiplexing).





Tech Tip

Only one SIG template is allowed per device template.

In SD-WAN Manager version 20.9, the SIG template is divided into several sections:

1. Device Type, Template Name, Description, and SIG Provider (Umbrella, Zscaler, or Generic).
2. Tracker: Allows you to configure custom L7 health check tracker information.
3. Configuration: Allows you to specify different tunnel type (IPsec or GRE) and other tunnel characteristics, such as tunnel name, tracker name, tunnel source, whether the tunnel is attached to a primary or secondary data center (which is specified or discovered later) and advanced options, like IP MTU and other tunnel settings.
4. High Availability: Allows you to choose up to 4 active tunnels or 4 active/standby tunnel pairs by choosing the tunnels defined in the Configuration section under the Active or Backup column. You can also modify traffic ratios for the tunnels.
5. Advanced Settings (if applicable): Allows you to define Zscaler primary or secondary data centers and Zscaler location name if desired, and advanced Zscaler settings (XFF Forwarding, Enable IPS Control, etc).



Configuration					
Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
gre101		No		1400	 
gre201		No		1400	 





High Availability			
Active	Active Weight	Backup	Backup Weight
Pair-1  gre101	 1	 gre201	 1

Figure 20. SIG template configuration and High Availability sections

Tech Tip

In 20.4/17.4, the only two tunnel types that are offered are Umbrella and Third Party. You can configure Zscaler manual tunnels (IPsec or GRE) using the Third Party option. Starting in 20.5/17.5, the three tunnel types that are offered are Umbrella, Zscaler, and Generic. To configure automatic IPsec or GRE Zscaler tunnels, choose the Zscaler option. You can configure Zscaler manual tunnels (IPsec or GRE) using the Generic option. Zscaler recommends you use automatic tunnels if available.

Automatic Zscaler Tunnels

Automatic Zscaler Tunnels are supported for IPSec and GRE tunnels. The feature provides a level of automation in configuring tunnels, such as automatic tunnel destination discovery, location registration in ZIA, automatic configuration of authentication parameters, and automatic configuration of L7 health checks. The feature gives you secure and simplified management and allows you to deploy Zscaler tunnels across a large number of branches.

Note

vEdge does not support GRE automated tunnels, only manual ones.

IPSec

1. Automatic Zscaler IPSec tunnels are introduced in 20.5/17.5. After automatic tunnels (through the SIG feature template) and the SIG credentials feature template are added to the device template and are pushed to the WAN Edge device, the following API steps occur from the WAN Edge router to provision the IPSec tunnels.
2. An authenticated session request is made to the ZIA by sending an API key, username, password, and time stamp. The requestor receives a cookie from Zscaler, which is then used in subsequent calls as part of the authenticated session.
3. VPN credentials are added for each tunnel. Each tunnel has a unique name, FQDN, and pre-shared security key that is generated by the WAN Edge device and then shared to the Zscaler cloud. Zscaler returns a tunnel ID associated with each tunnel. For future edits and modifications, the WAN device refers to the tunnel ID.
4. Next, the VPN credential associated with the tunnel is added to a location before it is usable by Zscaler policy. If it is the first tunnel for a WAN Edge device, create a location with a unique location name and add it to ZIA via an HTTP POST. The tunnel VPN credentials are added to the location.
5. A final API activates the configuration changes made in ZIA.
6. Primary and secondary data centers are retrieved from ZIA.

Another sequence of API calls happens when a tunnel is deleted. API HTTP responses are received and the last response code is recorded for troubleshooting purposes. After the APIs are completed, you get a non-zero location ID and non-zero tunnel IDs. Whether the tunnel comes up and active depends on the Internet Key Exchange (IKE) negotiation. See the [Operate](#) section for more information on troubleshooting.

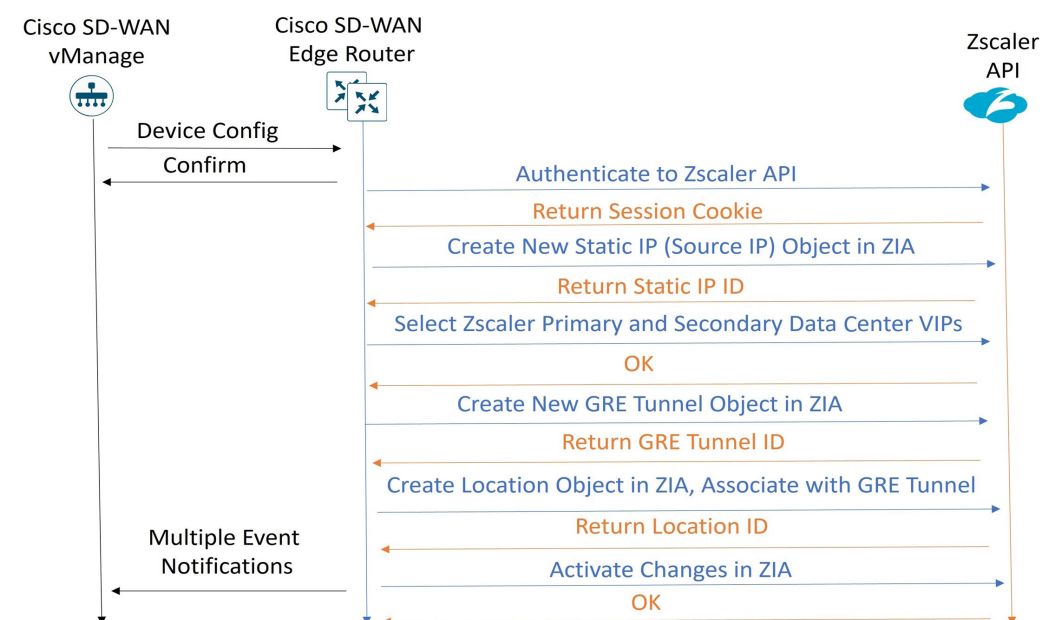


Figure 21. Advanced Settings for Zscaler Auto Tunnels

Advanced Settings for Zscaler Auto Tunnels

You can enable the following Zscaler advanced features from the SD-WAN SIG feature template:

- Primary Data-Center/Secondary Data-Center: By default, the primary and secondary data centers are automatically selected. Alternatively, you can manually choose the data centers. If a Global variable is selected, you can choose from a drop-down menu of data centers. Before 20.9 code, this list of data centers might be static and the information not completely current. If you choose device specific input, an FQDN is required for the variable for an IPSec tunnel, and a destination IP address is required for the variable for a GRE tunnel. For the latest list of data centers, go to <https://config.zscaler.com> (then choose the cloud name from the drop-down menu).
- Zscaler Location Name
- Authentication Required: If enabled, you can enable the Surrogate IP feature with its corresponding parameters
- XFF Forwarding
- Enable Firewall
- Enable IPS Control
- Enable Caution
- Enable AUP and additional AUP parameters

For additional information on these advanced location features, see [Configuring Locations](#) (government agencies, see [Configuring Locations](#)).

Advanced Settings

Primary Data-Center

✓

Auto

i

Secondary Data-Center

✓

Auto

i

Zscaler Location Name

✓

Auto

Authentication Required

✓

☐ On

☒ Off

XFF Forwarding

✓

☐ On

☒ Off

Enable Firewall

✓

☐ On

☒ Off

Enable IPS Control

✓

☐ On

☒ Off

Enable Caution

✓

☐ On

☒ Off

Enable AUP

✓

☐ On

☒ Off

Figure 22. SIG feature template Advanced Settings

Layer 7 Health Check for Auto Tunnels

L7 health checks are enabled by default on all auto-tunnels provisioned with the Secure-Internet-Gateway templates.

The L7 health check is implemented as an HTTP request. It measures route-trip latency and compares it to the threshold set. Customize the tracker if you want to change the default parameters or use a different service URL. The default settings are:

- Interval: 30 seconds
- Multiplier: 2
- Threshold: 1000 msec
- Service URL for Zscaler tunnel, enter: `http://gateway.<Zscaler Cloud Name>.net/vpntest`

For Cisco IOS XE SD-WAN, a Loopback 65530 interface in VRF 65530 is created and used to source the L7 health check probes through each active and backup tunnel. You must configure a tracker source IP address, which is a private RFC 1918 address that should not overlap with other interfaces.

For Cisco vEdge, a loopback 65530 in VPN 65530 is created by default, sourced from 192.168.0.2/32. There is no need to configure a tracker source IP address for Cisco vEdge.

For any tunnels that fail to receive a response within the interval and retransmit timers, or for any tunnels that exceed the latency threshold, the tunnel tracker status is marked down and the VPN routes pointing to this tunnel is marked standby. Crypto IKE stays up for the IPSec tunnel and tunnel status also stays up for the GRE tunnel, but the routes are withdrawn. When the tracker status goes UP (probes become reachable again or latency improves below the threshold), the tunnel can become active again and the VPN routes can be added back.

General Configuration Steps

Multiple automatic Zscaler tunnels are implemented by:

- Creating a SIG Credentials feature template for API access to Zscaler. (In 20.9 and above, this is done once after creating the first Zscaler SIG feature template; you are prompted with a link to configure the SIG credentials feature template.)
- Creating a SIG feature template to define the tracker information, tunnel types, parameters, advanced settings, and high availability information.
- Adding the SIG template and SIG Credentials feature template to the transport VPN (VPN 0) in a device template.
- Adding a SIG Service route in the service VPN or adding centralized data policy to redirect user traffic to the SIG service.

Configuration Prerequisites

For Zscaler automatic tunnels to succeed, observe the following prerequisites:

- Configure ZIA Admin Portal with a partner key, username, and password (which belongs to the partner admin role).
- Enable NAT on the internet-facing interface on the WAN Edge router. In Cisco IOS XE SD-WAN, there is a loopback 65528 in VRF 65528 by default with an IP address of 192.168.1.1 that is used as the source interface for API calls. A NAT Dedicated Internet Access (DIA) route is used to direct API traffic into the underlay.
- A DNS server configuration should exist in the transport VPN (VPN 0) and be reachable from the transport VPN (VPN 0). An Internet DNS server is often used for this purpose. The Zscaler base URI needs to be resolved from the WAN Edge router for API calls, along with the Layer 7 health check URI. The Zscaler base URI is `zsapi.<zscalercloud>.net/api/v1` where values for `<zscalercloud>` are the Zscaler Cloud domain. The automated Layer 7 health check URL is `http://gateway.<zscalercloud>.net/vpntest`
- Configure Network Time Protocol (NTP) to ensure that the WAN Edge router clock is accurate (for Zscaler API calls). This isn't required, but is highly recommended.

Design Considerations

Review the following considerations:

Basic

- NAT is required on each outgoing tunnel WAN interface for API calls to succeed.
- DNS server configuration is required in VPN 0 and reachable from VPN 0 so Zscaler API and L7 health check URLs can be resolved.
- NTP configuration is highly recommended so clocks are synced to ensure successful API calls.
- Do not change Site ID or System IP Address of a WAN Edge router when you have a SIG feature template attached. Remove the SIG feature template to remove the tunnels, make the Site ID and/or System IP address change, then re-attach the SIG feature template.

ZIA Admin Portal

When using automated tunnels, Zscaler recommends that you avoid making manual changes to the tunnels and locations in the ZIA Admin Portal as much as possible. Use SD-WAN Manager to make modifications to those parameters.

ECMP Tunnels

- When configuring multiple active/active tunnels, each tunnel is required to have a unique source IP/source port/destination IP/destination port. For multiple, active tunnels over the same transport, you can use loopback interfaces defined in VPN 0 to source multiple active tunnels from. vEdge routers do not support loopback interfaces for tunnel sources.
- There are several applications that are known to fork off multiple sessions for a single user session (O365, Google Services, Facebook, etc). If you have two active SIG tunnels that are pinned to two different Zscaler data centers, 4-tuple ECMP (the default) could pin flows from a single user to separate tunnels. The cloud application could see different client IP addresses for the same session, since NAT is applied to their source IP addresses from two different data centers, and thus, resets from the server could occur. It is required to use the same SIG data center for any active/active tunnels.
- There might be performance implications to applications using active/active tunnels and 4-tuple ECMP if the tunnels have significant performance differences. Use source IP-based ECMP to prevent a single-user session from hashing over multiple tunnels.
- Source IP-based ECMP is not supported for vEdge routers. It is supported for IOS XE SD-WAN routers and you can configure it only when the WAN Edge router is in CLI mode before version 17.12. If you try to use an add-on CLI template, the ECMP configuration goes back to the default, which is 4-tuple. This affects hardware-based IOS XE SD-WAN routers and is fixed in 17.12.

Auto Tunnels

- There is no support for vEdge auto GRE tunnels.
- When the WAN Edge routers retrieve a list of the closest GRE or IPsec Zscaler data centers through the API, the **withinCountry** flag is set to **true**. This can impact the ability of the WAN Edge to connect to the closest data center if this device is near the border of a country, and the router could connect to a data center further away (within country). This is addressed in SD-WAN Manager version 20.14.
- You can enable several advanced security features on Zscaler through APIs from the SD-WAN Manager GUI. Zscaler recommends you leave all features off as default, deploy the feature template, bring the tunnels up, then go back to edit the SIG template and enable the desired features/services. Some features might not have the proper licenses or permissions to enable, so you could get a failed HTTP response and a location might not get created if you are trying to create tunnels at the same time. It simplifies troubleshooting if you enable them separately from configuring tunnels for the first time.

- In SD-WAN Manager version 20.5, you cannot configure values greater than 255 for Idle-time-to-dissociation and Refresh-time (part of Authentication/Surrogate IP feature and Surrogate IP for Known Browser feature) in the SIG template UI. The workaround in IOS XE SD-WAN Edge routers is to use a CLI add-on template. To learn more, refer to [Cisco IOS XE Catalyst SD-WAN Qualified Command Reference](#) for additional information on Zscaler advanced features CLI commands. This is fixed in SD-WAN Manager 20.6.

L7 Health Checks

- In the 20.5 Cisco SD-WAN Manager version, L7 health checks are supported only for Cisco vEdge routers. Health checks are not supported for Cisco IOS XE SD-WAN Edge routers until the 20.6 Cisco SD-WAN Manager version.
- Starting in 20.5/17.5, you can manually configure GRE or IPSec tunnels using the generic SIG tunnel option in the SIG feature template. L7 health checking is not supported for the generic SIG tunnel option, until 20.8/17.8.
- L7 health checks are sent out on all SIG tunnels across all high availability configurations. L7 health checks can promote a standby tunnel to an active tunnel, potentially impacting existing sessions.
- Do not use custom L7 health check trackers destined to commonly visited websites, because it might cause cloud security provider IP address space to be blocked. Use `http://gateway.<Zscaler Cloud Name>.net/vpntest` as the service URL. Use only HTTP:// in the service URL to Zscaler. HTTPS:// is not valid, even though the Cisco SD-WAN Manager might accept it.
- L7 health checks should not be sent more than one every 5 seconds.

GRE

- GRE tunnel source IP addresses are not affected by NAT/PAT defined on an interface (like IPSec tunnel source IP addresses are). This means that you must address GRE tunnel source IP addresses with either a publicly routable IP address or through One-to-One NAT on an external device. Because the tunnel source IP address is used for registration with Zscaler, each GRE tunnel source IP address must be unique and should be static and not change.
- Loopback interfaces as tunnel sources for GRE are not supported until 17.9.2 and higher.
- GRE Keepalives are disabled by default in Cisco IOS XE SD-WAN devices. To configure GRE keepalives, configure a CLI add-on feature template. The command is `keepalive [[seconds] retries]` under the tunnel interface configuration.

Cisco IOS XE SD-WAN

- On an IOS XE SD-WAN router with multiple internet interfaces accessing Zscaler tunnels or multiple active tunnels sourced by loopbacks on a router with more than one transport of any type, there might be an issue where ISAKMP traffic fails to take the correct interface outbound, which can prevent IPSec tunnel formation. This was fixed 20.8/17.8, but there are still cases where DNS requests for health checks might take an incorrect interface. To work around this, use a CLI add-on policy to use a local Policy-Based Routing (PBR) policy to force DNS or any other local router control traffic to use the proper physical interface (see the [Deploy](#) section for multiple active/active tunnels).
- As referenced by [Field Notice FN72510](#), Cisco IOS XE Software: Weak Cryptographic Algorithms Are Not Allowed by Default for IPSec Configuration in Certain Cisco IOS XE Software Releases. This affects platforms starting in 17.11.1a and later, and, in a new deployment, will not allow you to configure null encryption for IPSec SIG tunnels. As a workaround, enter `crypto engine compliance shield disable` in the CLI add-on template or in CLI mode and issue a reload. Cisco does not recommend this option as weak cryptographic algorithms are insecure and do not provide adequate protection from modern threats.

Cisco vEdge

- vEdge does not support loopback interfaces for tunnel sources.
- vEdge does not support Zscaler GRE auto tunnels.
- vEdge does not support fallback for data policy for traffic redirection to a SIG tunnel.
- vEdge does not support SIG tunnel monitoring enhancements.

Deploy

The following basic steps are needed to configure auto tunnels successfully:

- [Deploy: ZIA for API Access](#). This allows Cisco SD-WAN Manager to send API calls to ZIA to provision IPsec tunnels and Zscaler locations.
- [Deploy: Cisco WAN Edge Prerequisites](#).
 - Verify NAT, DNS, and clock/NTP settings.
 - Create a SIG credentials feature template. This uses information obtained from ZIA you configured while setting up ZIA for API access.
 - If you plan on using Null Encryption, which is the default for Zscaler SIG tunnels, disable crypto compliance by entering `crypto engine compliance shield disable` in the CLI add-on template or in CLI mode and issue a reload. Refer to [Field Notice FN72510](#). Compliance is enforced starting in 17.11.1a for many platforms and won't allow you to configure weak cryptographic algorithms. While not recommended, disabling crypto compliance is a workaround in order to use the Null Encryption option.
- Deploy an IPsec Auto Tunnel use case. You can choose different use cases. Active/Standby tunnels and Active/Active tunnels using hybrid or dual-internet transports and configured with a SIG route or centralized policy are a few examples. For each use case, the following is needed:
 - Create a SIG feature template: This allows you to define multiple tunnels of certain types (Umbrella, Zscaler, or generic), and allows you to define specific characteristics about each tunnel. Then, you can define which tunnels are active and which are backup.

Tech Tip

After a tunnel type is selected in the SIG Feature Template, you can only configure additional tunnels of that same type in that specific feature template. With Zscaler tunnels using the SIG template, IPsec or GRE tunnels are both supported, but a mix of both is not supported in the same feature template. L7 health checking is not supported in this code version for generic tunnels.

- Add the SIG and SIG credentials feature template to the device template of the device you want to configure with IPsec auto tunnels.
- Add a route or modify centralized policy for traffic redirection to the Zscaler tunnels.

Tech Tip

Before moving forward, ensure that the WAN Edge router has a device template deployed from Cisco SD-WAN Manager with, at minimum, basic connectivity to the internet. For details on a base template example, see [Appendix A: Cisco Branch Base Feature Templates and Configuration Values Used](#).

Deploy: ZIA for API Access

In this section, the Zscaler side is configured for API access, which is needed when configuring the WAN Edge router for automated IPsec or GRE tunnels. When attaching SIG templates which contain Zscaler tunnels starting in 20.5 SD-WAN Manager code and later, a SIG Credentials template is required as part of the device template. This SIG Credentials feature template needs information from the Zscaler UI in order for API calls to Zscaler to succeed. It is noted in the following appropriate sections the information needed for the SIG Credentials feature template on SD-WAN Manager, which is configured in a later section.

Note that login IDs and passwords in the following images might be obscured for security reasons.

Procedure 1: Log In to ZIA

1. Log in to Zscaler using your administrator account. The login URL is `https://admin.<Zscaler Cloud Name>.net`, where `<Zscaler Cloud Name>` is the Zscaler cloud to which you have admin rights.

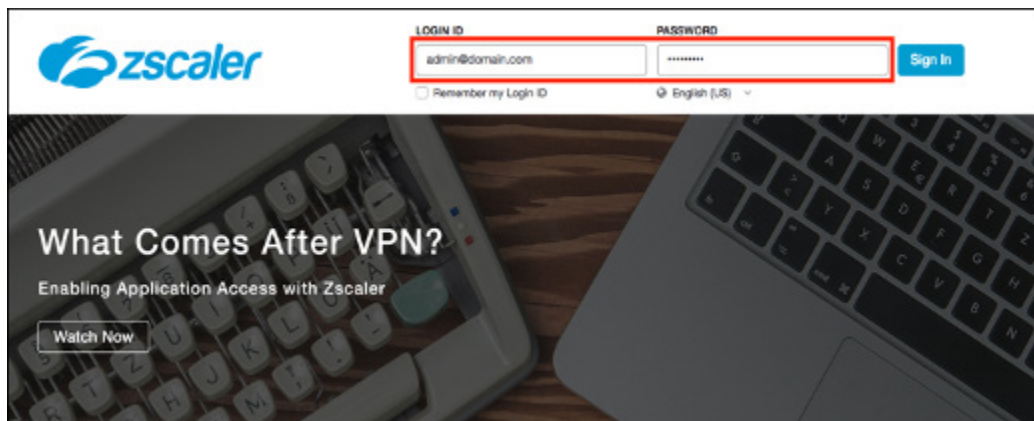


Figure 23. Login to ZIA

2. If you are unable to log in using your admin account, [contact Zscaler Support](#).

Procedure 2: Find Zscaler Organization Domain and Partner Base URI

You need the Zscaler Organization Domain and Partner Base URI for the Cisco SD-WAN Manager SIG credentials feature template.

1. Go to **Administration > Settings > Company Profile**. On the **Organization** tab, manually note the domain name listed under the **Domains** field (in this example, `ciscotest.net`). If multiple domains exist, select only one of them.

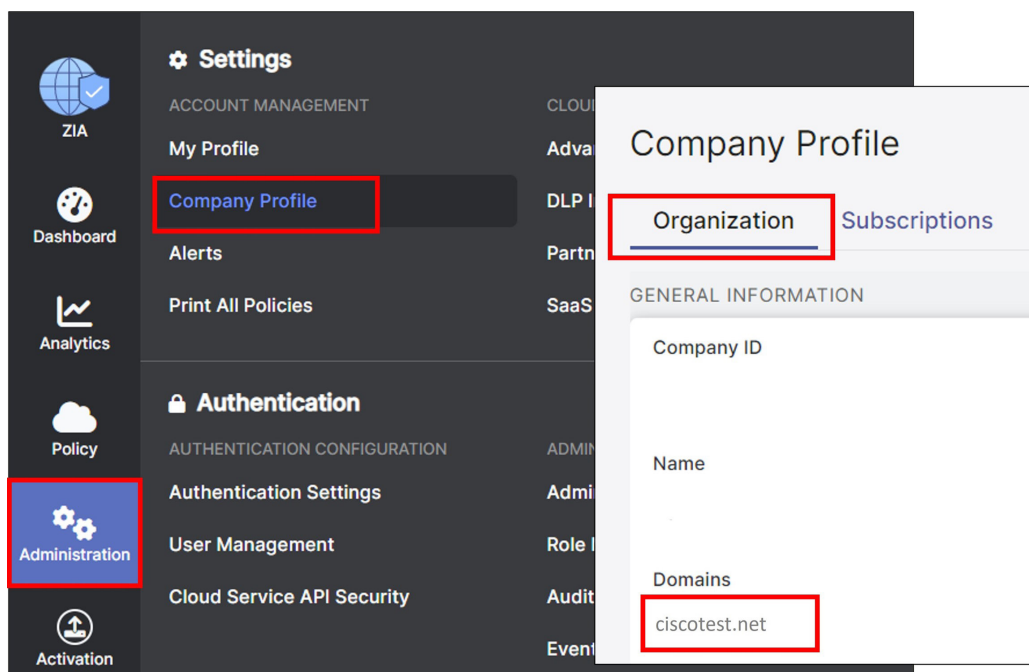


Figure 24. Company profile

Tech Tip

The Domains value in this section is used in the Organization field in the Cisco SD-WAN Manager SIG credentials feature template.

Cisco SD-WAN Manager SIG Credentials Parameter	ZIA Admin Portal Location	Zscaler Parameter	Zscaler Value
Organization	Administration > Settings > Company Profile > Organization	Domains	ciscotest.net (example)

- Go to **Administration > Authentication > Cloud Service API Security**. On the **Cloud Service API Key** tab at the top of the page, copy the base URL for your API (in this example, `zsapi.zscalerthree.net/api/v1`).

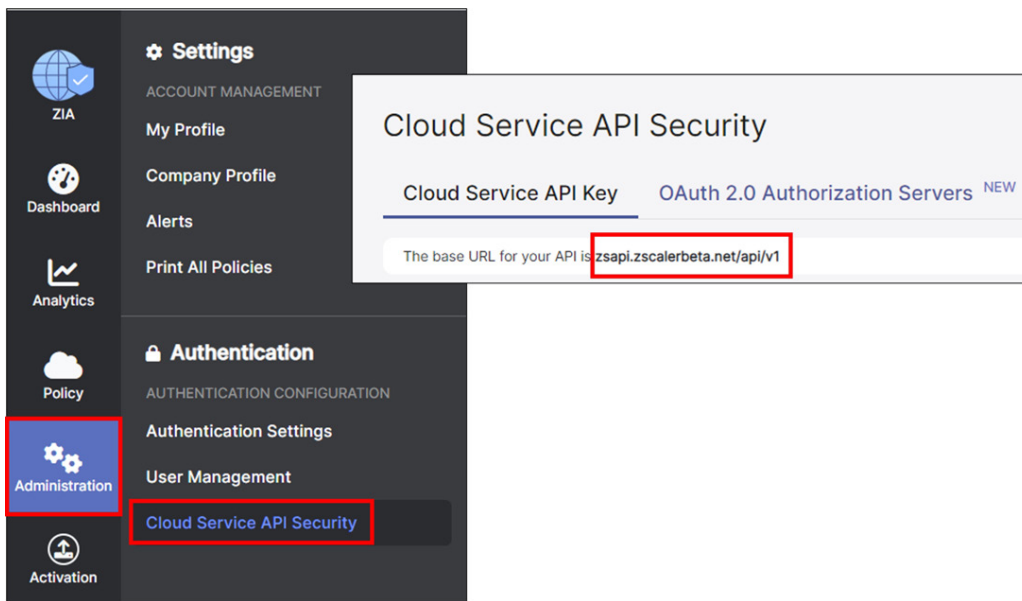


Figure 25. API key management

Tech Tip

The base URL value in this section is used in the Partner Base URI field in the Cisco SD-WAN Manager SIG credentials feature template.

Cisco SD-WAN Manager SIG Credentials Parameter			
	ZIA Admin Portal Location	Zscaler Parameter	Zscaler Value
Organization	Administration > Company Profile > Organization	Domains	ciscotest.net (example)
Partner Base URI	Administration > Authentication > Cloud Service API Security > Cloud Service API Key	Base URL for your API	zsapi.zscalerbeta.net/api/v1 (example)

Procedure 3: Add and Verify SD-WAN Partner Key

To enable ZIA for API access, the first step is to create a SD-WAN partner key. The partner key is an API key used as one form of authentication. The second form of authentication is an admin partner username and password, which is explained later in this deployment guide. Use this admin credential set for API calls. It doesn't work for logging in to the ZIA Admin Portal.

1. Go to **Administration > Settings > Cloud Configuration > Partner Integrations**.

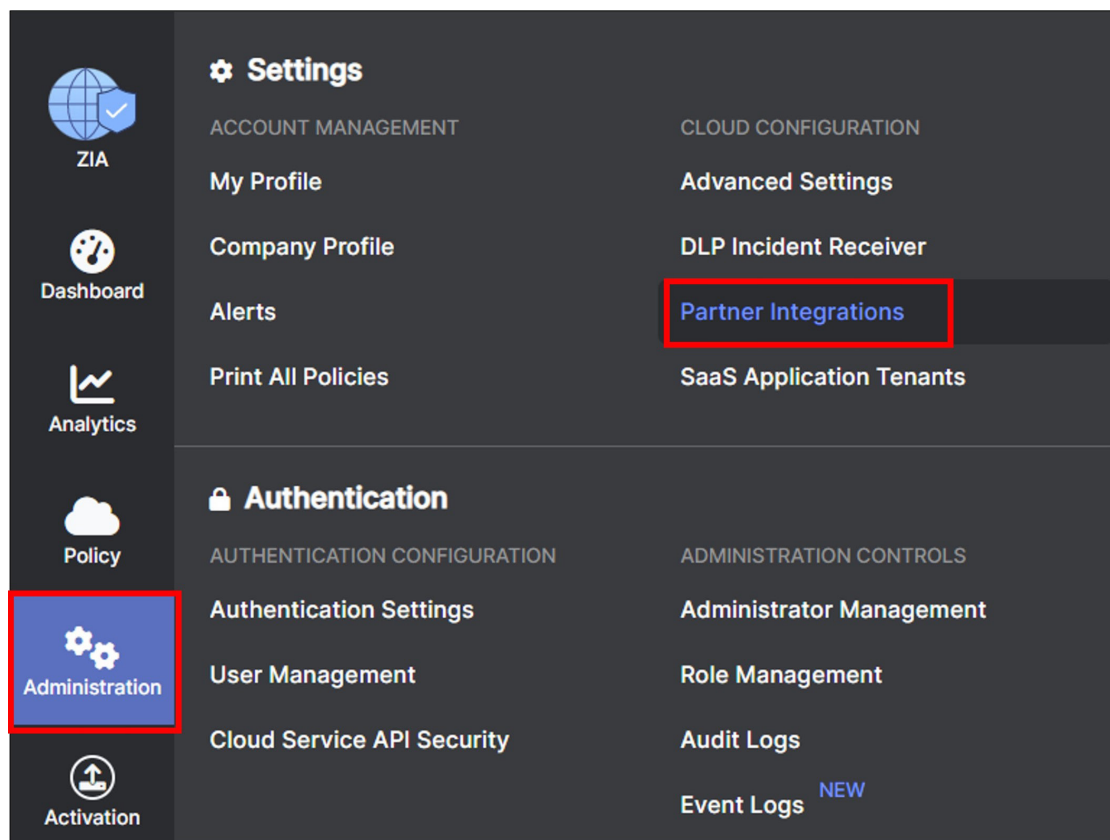


Figure 26. Partner integrations

- At the **Partner Integrations** section of the ZIA Admin Portal, select the **SD-WAN** tab. If a key already exists with a **Partner Name** Cisco Viptela, then skip to Step 6. Only one key can exist per partner name. Take care when deleting or modifying the partner key because API calls to Zscaler fail if other Cisco SD-WAN Manager instances are using the current key.
- Click **Add Partner Key**.



Figure 27. Add partner key

- Under the **Name** drop-down menu, select which SD-WAN vendor you want to create a partner key. After selecting **Cisco SD-WAN**, click **Generate**.

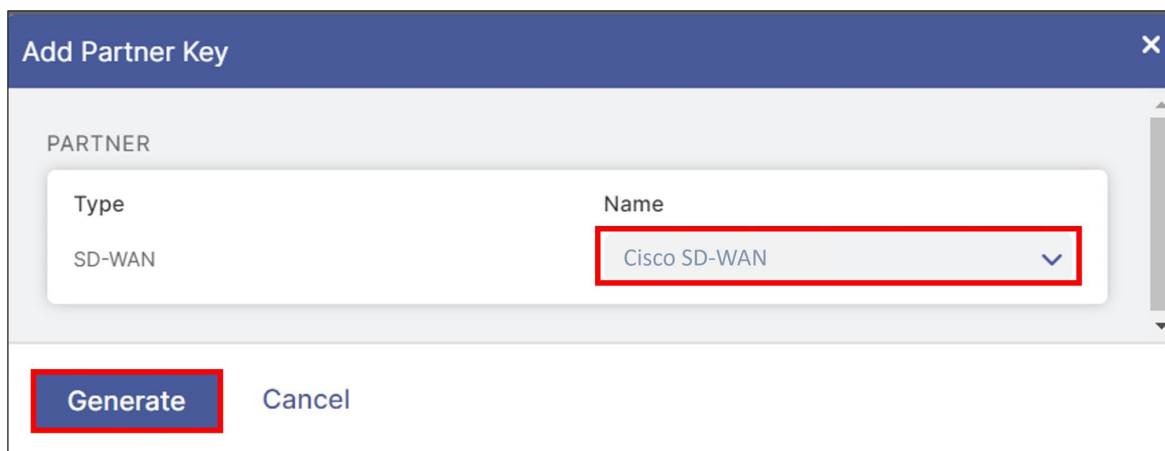


Figure 28. Generate partner key

5. See the partner key you created (**Cisco SD-WAN** in this case) in the **Partner Integrations** window. A red circle with a number above the **Activation** icon on the bottom left-side navigation is also displayed. Although you have created a partner key, the configuration change is pending. Only after activation does this configuration become active.

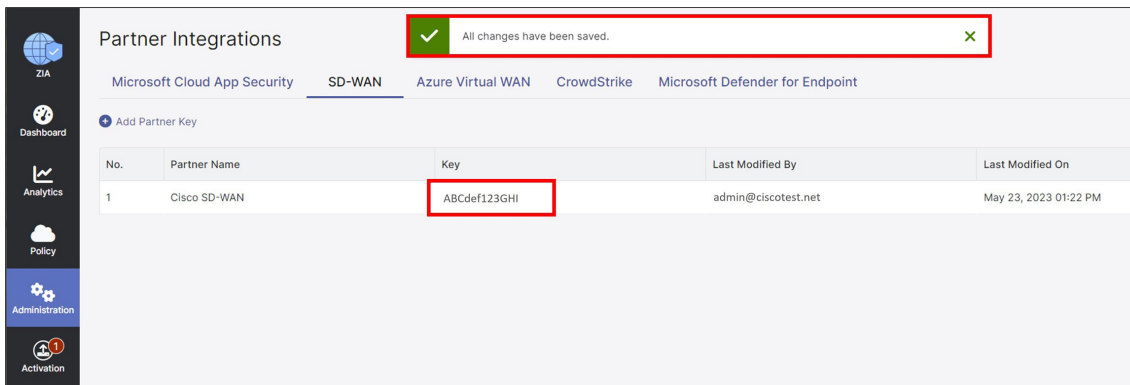


Figure 29. Partner key complete

6. Ensure to copy the **Key** value as it is required in a future step when configuring the SIG credentials feature template in the Cisco SD-WAN Manager Network Management System (NMS).

Tech Tip

The Cisco Viptela partner key value in this section is used in the Partner API Key field in the Cisco SD-WAN Manager SIG credentials feature template.

Cisco SD-WAN Manager			
SIG Credentials Parameter	ZIA Admin Portal Location	Zscaler Parameter	Zscaler Value
Organization	Administration > Company Profile > Organization	Domains	ciscotest.net (example)
Partner Base URI	Administration > Authentication > Cloud Service API Security > Cloud Service API Key	Base URL for your API	zsapi.zscalerbeta.net/api/v1 (example)
Partner API Key	Administration > Settings > Cloud Configuration > Partner Integrations > SD-WAN	Partner Name (Cisco SD-WAN or Cisco Viptela) Key	ABCdef123GHI (example)

Procedure 4: Add a Partner Administrator Role

You must create a partner administrator role and assign it to the administrator user that is used to authenticate against the Zscaler ZIA Provisioning API. By creating a partner administrator role, you can define the permissions and access to grant to a third-party partner, such as a SD-WAN partner.

1. Go to **Administration > Authentication > Administrative Controls > Role Management**.

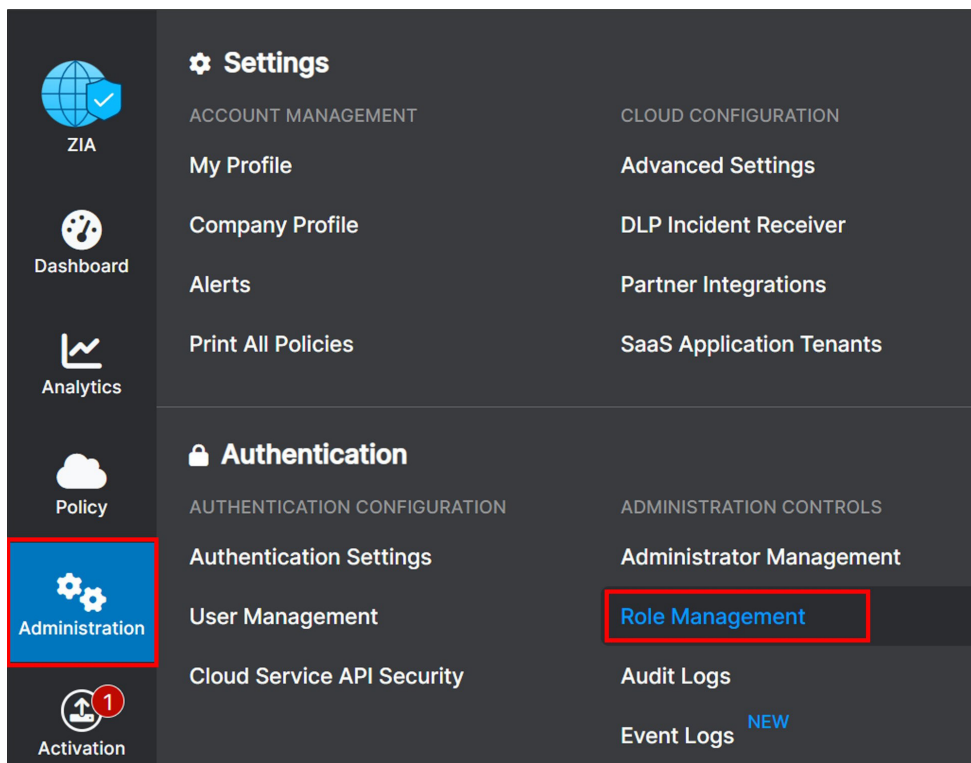


Figure 30. Role management

2. If a partner administrator role has already been created with full access, use this role, or create a separate one. A partner administrator role is listed as **Type** Partner Admin, including a Policy keyword listed under the **Full Access** column. If you use an existing role, note the **Name**, and go to [Procedure 5: Create a Partner Administrator](#) to create a partner administrator login ID and password.
3. To create a new partner administrator role, click **Add Partner Administrator Role**.

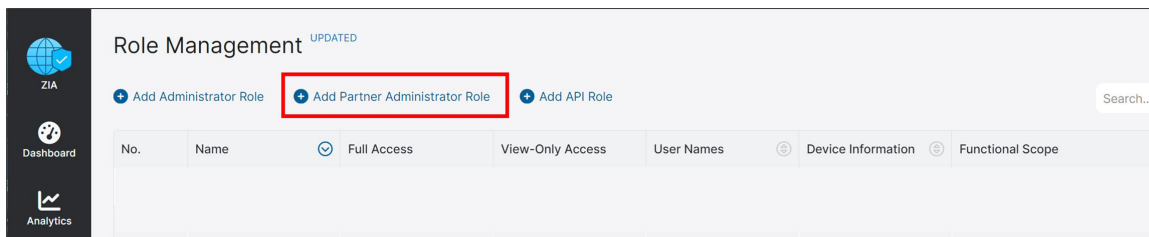


Figure 31. Add partner administrator

4. Enter the name of the partner administrator role you want to create.
5. Change the **Access Control** to Full. Full **Access Control** allows partner admins to view and edit VPN credentials and locations that the Cisco SD-WAN Manager NMS is managing via the ZIA Provisioning API. This is necessary for the Cisco SD-WAN Manager NMS to create new VPN credentials and locations in ZIA for branches.
6. Click **Save** to return to the previous screen.

The screenshot shows a modal window titled "Add Partner Administrator Role". It contains three main sections: "ADMINISTRATOR ROLE", "PERMISSIONS", and "PARTNER ACCESS".

- ADMINISTRATOR ROLE:** A text input field labeled "Name" contains the text "SD-WAN".
- PERMISSIONS:** A section labeled "Access Control" with two buttons: "Full" (selected with a checkmark and highlighted with a red box) and "View Only".
- PARTNER ACCESS:** A section titled "SD-WAN API Partner Access" with a master toggle switch that is checked. Below it are four sub-items, each with a checked checkbox:
 - Locations
 - VPN Credentials
 - Static IP
 - GRE Tunnels

At the bottom of the modal are two buttons: "Save" (highlighted with a red box) and "Cancel".

Figure 32. Partner administrator role

Procedure 5: Create a Partner Administrator

The last step required is to create a partner administrator.

1. Go to **Administration > Administration Controls > Administrator Management**.

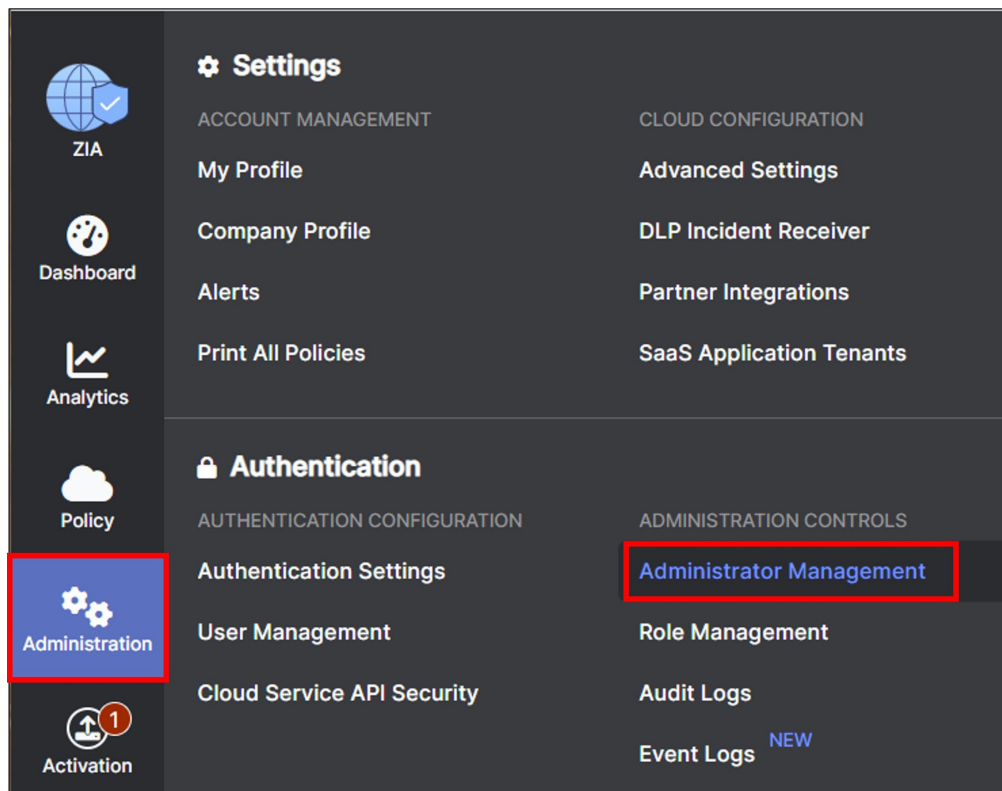


Figure 33. Administrator management

2. On the **Administrator Management** window under the **Administrators** tab, select **Add Partner Administrator**.

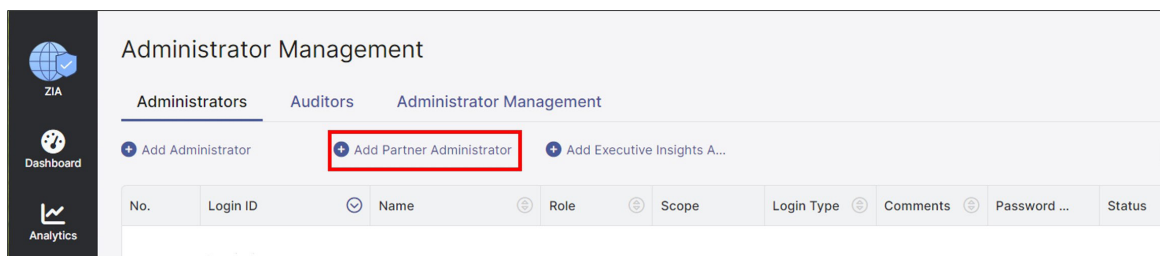


Figure 34. Add partner administrator

3. On the Add Partner Administrator window, fill in the required fields:
 - a. **Login ID:** This includes @domain which fills in automatically to the right if there is only one domain with this account. If there are multiple domains associated with this account, choose the correct one from the drop-down menu.
 - b. **Email:** Any address in email format and equal to the login ID, but cannot already exist in the current cloud (it should not be referenced anywhere).
 - c. **Name:** Name or label associated with the login ID (it should not be referenced anywhere).
 - d. **Partner Role:** Select the role created in [Procedure 4: Add a Partner Administrator Role](#).
 - e. **Status:** Enable or disable the Partner Administrator account. By default, it is enabled.

Note

Save the Login ID@Domain value and **Password** settings, as you need to enter them in the Cisco SD-WAN Manager NMS when configuring the SIG credentials template.

4. Click **Save**.

Figure 35. Save partner admin

Tech Tip

The Login ID @ domain value in this section is used in the Username field and the Password value in this section is used in the Password field in the Cisco SD-WAN Manager SIG credentials feature template.

Cisco SD-WAN Manager SIG Credentials Parameter	ZIA Admin Portal Location	Zscaler Parameter	Zscaler Value
Organization	Administration > Company Profile > Organization	Domains	ciscotest.net (example)
Partner Base URI	Administration > Authentication > Cloud Service API Security > Cloud Service API Key	Base URL for your API	zsapi.zscalerbeta.net/api/v1 (example)
Username	Administration > Administration Controls > Administrator Management > Administrators	Partner Admin Login ID	sd-wan@ciscotest.net (example)
Password	Administration > Administration Controls > Administrator Management > Administrators	Partner Admin Password	(hidden)
Partner API Key	Administration > Settings > Cloud Configuration > Partner Integrations > SD- WAN	Partner Name (Cisco SD- WAN or Cisco Viptela) Key	ABCdef123GHI (example)

Procedure 6: Activate Pending Changes

Note that the new configurations are not enabled until activation occurs.

Click **Activation** on the left-side navigation, and then click **Activate** to enable the pending configuration changes.

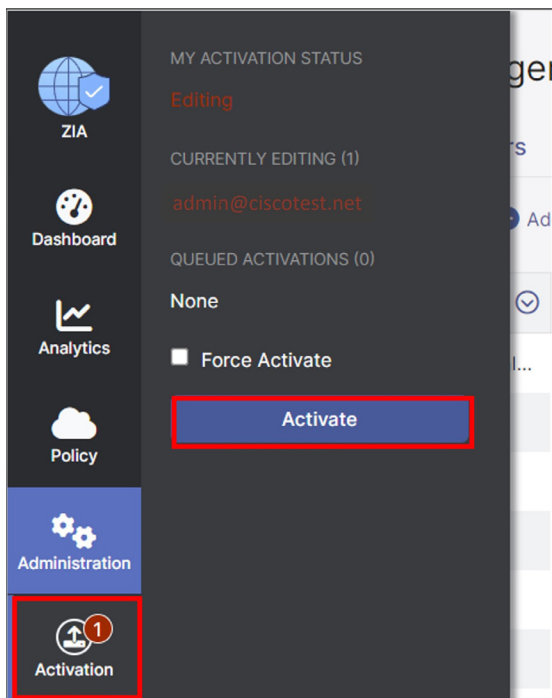


Figure 36. Activate changes

After activating pending changes, Activation Completed! appears.

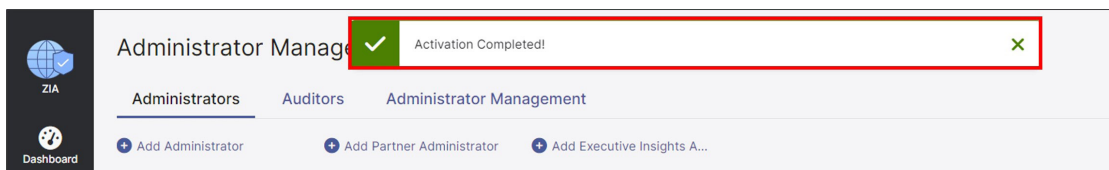


Figure 37. Activation completed

Deploy: Cisco WAN Edge Prerequisites

In this section, the prerequisites are checked and deployed.

Procedure 1: Log In to the Cisco Catalyst SD-WAN Manager

1. Open a web browser and enter the URL for your vManage instance (<https://<Cisco SD-WAN Manager IP address>:8443>). For best results, use a Google Chrome or Mozilla Firefox browser.
2. Enter the admin username and password.

Procedure 2: Ensure Prerequisites are Met

1. Verify that NAT is enabled on the internet interface that is used to access Zscaler.

This is needed for API calls requested against the ZIA Public Service Edge because a NAT DIA route is used to direct the API traffic out of the underlay. Enable a NAT in each internet interface deployed where Zscaler tunnels are built. The following is the relevant feature template information that is required:

Modifications to Feature Template: BR_VPNO_INET

Section	Parameter	Type	Variable/Value
NAT	NAT	Global	On
	NAT Type	Global	Interface

2. Verify that a primary and/or secondary DNS server is defined in the VPN 0 feature template. API calls are made to the base URI: zsapi.<Zscaler Cloud Name>.net/api/v1 or admin.<Zscaler Cloud Name>.net/api/v1 where values for [<Zscaler Cloud Name>](#) are the Zscaler Cloud domain. The automated L7 health check URL also needs DNS resolution. It is <http://gateway.<Zscaler Cloud Name>.net/vpntest>.

The following is the relevant feature template information that is required (which can be global or device-specific values):

Modifications to Feature Template: BR_VPNO

Section	Parameter	Type	Variable/Value
DNS	Primary DNS Address (IPv4)	Global	208.67.222.222
	Secondary DNS Address (IPv4)	Global	208.67.220.220

3. Verify Network Time Protocol (NTP) is enabled, synced, and the clock is correct. An authentication session can fail with Zscaler is due to the clock time being mismatched. Configuring NTP and ensuring the NTP server time is synced is one way to prevent authentication issues.

```
WAN_EdgeE#show clock
01:49:13.091 UTC Fri Sep 3 2021
```

```
WAN_EdgeE#show ntp association
address ref clock st when poll reach delay offset disp
*~64.100.100.1 127.127.1.1 5 157 1024 377 3.000 -3.500 2.050
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

NTP is configured in a separate feature template and added to the device template in the basic information section. In the example topology, the source interface is the internet interface in VPN 0, because the NTP server is on the internet.

Feature Template Name: NTP

Section	Parameter	Type	Variable/Value
Server	Hostname/IP address	Global	time.google.com
	Source Interface	Device Specific	ntp_server_source_int

Procedure 3: Create a SIG Credentials Feature Template

Starting in 20.9 SD-WAN Manager code versions, the SIG credentials feature template is created automatically and is filled out only one time when a SIG feature template is first created with a specific SIG provider and software platform (vEdge or IOS XE SD-WAN). The credentials template is then added automatically to a device template when the SIG feature template is added. Before the 20.9 SD-WAN Manager code version, there is a SIG credentials feature template you must create and configure separately and then manually add to a separate section of the device template when the SIG template is added.

If using 20.9 SD-WAN Manager code and later, create the first Zscaler SIG feature template to create the global Zscaler SIG credentials feature template. If using 20.8 SD-WAN Manager code and earlier, create a separate SIG Credentials feature template.

1. In the top left corner of Cisco SD-WAN Manager, click the hamburger icon to open the menu.
2. Go to **Configuration > Templates > Feature or Feature Templates** at the top of the page.

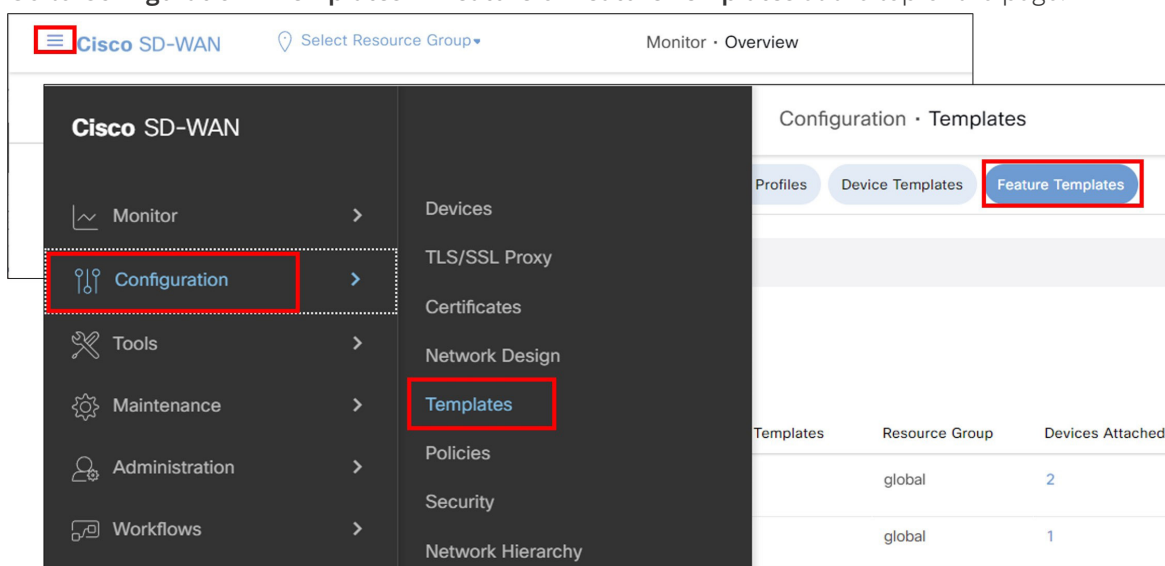


Figure 38. Configure template

3. Click **Add Template**.
4. In the **Select Devices** section, select the devices from the list that potentially can use this template. To select all IOS XE SD-WAN devices that can support SIG Templates, you can select all platforms except ISR 1100 (Viptela OS), vEdge devices, CG platforms, the IR8140 and IR8340, and the vManage and SD-WAN from the device model list (in the 20.9 release).
5. In SD-WAN Manager version 20.9 and later, in the **VPN** section, select **Cisco Secure Internet Gateway (SIG)**.

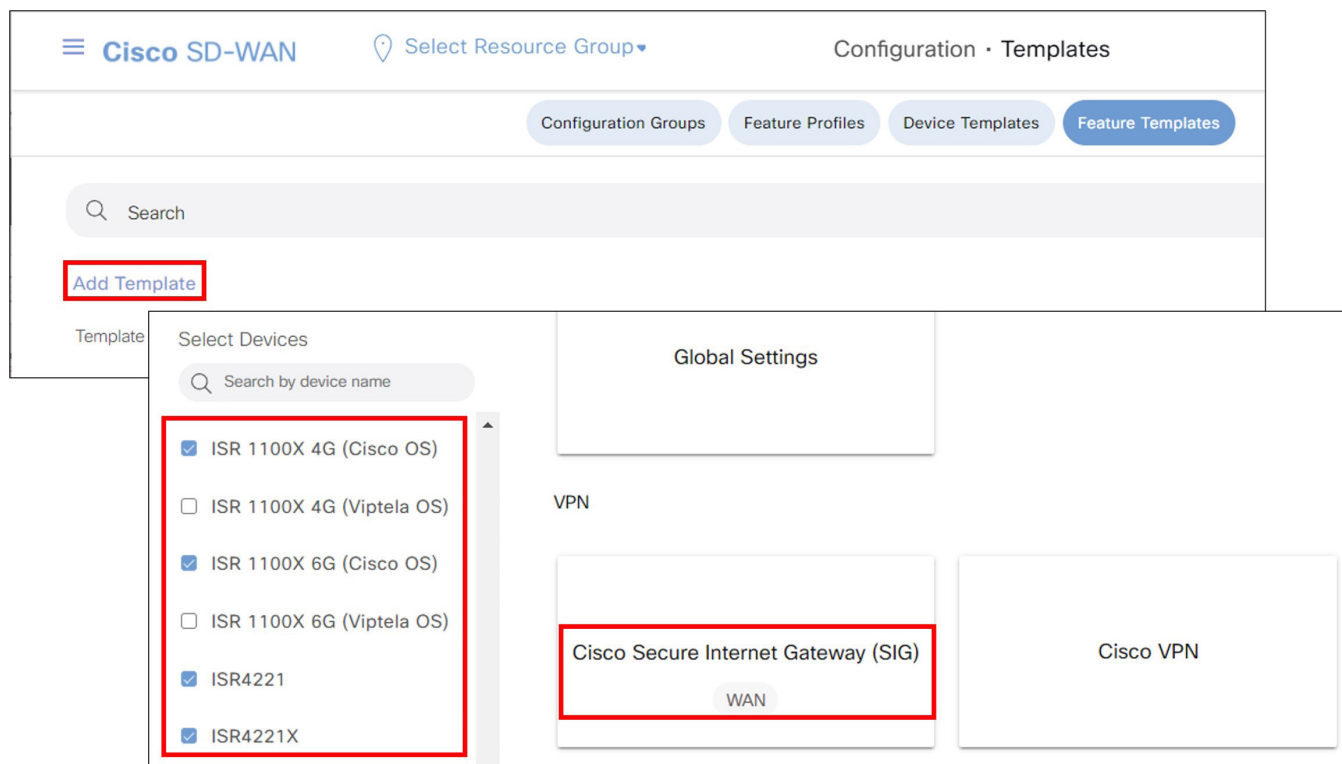


Figure 39. Add Template

6. In other SD-WAN Manager versions, in the **Other Templates** section, select **Cisco SIG Credentials**.



Figure 40. Cisco SIG credentials

7. In SD-WAN Manager version 20.9 and later, leave everything as is. The **Template Name** (Cisco-zscaler-Global-Credentials) and **Description** (Global credentials for zscaler) are already filled in, and the **SIG Provider** is already selected (**Zscaler**).

In other SD-WAN Manager versions, enter the **Template Name** (xeSig_Credentials) and **Description** (IOS XE Sig Credentials Template) and next to **SIG Provider**, select **Zscaler**.

8. Fill in the **Organization**, **Partner Base URI**, **Username**, **Password**, and **Partner API Key**. These parameters were obtained from the Zscaler configuration section:

Cisco SD-WAN Manager SIG Credentials Parameter	ZIA Admin Portal Location	Zscaler Parameter	Zscaler Value
Organization	Administration > Company Profile > Organization	Domains	ciscotest.net (example)
Partner Base URI	Administration > Authentication > Cloud Service API Security > Cloud Service API Key	Base URL for your API	zsapi.zscalerbeta.net/api/v1 (example)
Username	Administration > Administration Controls > Administrator Management > Administrators	Partner Admin Login ID	sd-wan@ciscotest.net (example)
Password	Administration > Administration Controls > Administrator Management > Administrators	Partner Admin Password	(hidden)
Partner API Key	Administration > Settings > Cloud Configuration > Partner Integrations > SD-WAN	Partner Name (Cisco SD-WAN or Cisco Viptela) Key	ABCdef123GHI (example)

Basic Details

SIG Provider ☐ Umbrella ☒ Zscaler

Organization

Partner Base URI

Username

Password

Partner API Key

Figure 41. Zscaler settings

9. Click **Save**. For SD-WAN Manager versions 20.9 and later, you are returned to a SIG feature template where you can continue to configure a SIG template, or click **Cancel** to configure a SIG template at a later time.

Deploy: Cisco WAN Edge Auto IPSec or GRE Tunnels (One Active/Standby Pair, Hybrid Transport)

In this section, you'll configure one active/standby auto tunnel pair on the internet transport: one to the primary Zscaler DC and one to the secondary Zscaler DC. Traffic is forwarded on the active tunnel to the primary DC until the active tunnel is declared to be down (through L7 health checking and/or DPD). After down, the standby tunnel to the secondary DC becomes active. When the tunnel to the primary DC recovers, it becomes active again and the tunnel to the secondary DC goes into standby.

The following deployment use case contains the following features:

- One active/standby IPSec or GRE auto tunnel pair on a single internet transport. The active tunnel connects to a primary Zscaler DC and the standby tunnel connects to a secondary Zscaler DC.
- SIG service route for redirecting traffic to Zscaler tunnels
- Customized L7 Health Tracker (optional)
- Advanced Zscaler features (optional)
- Customized Zscaler tunnel destinations (optional)

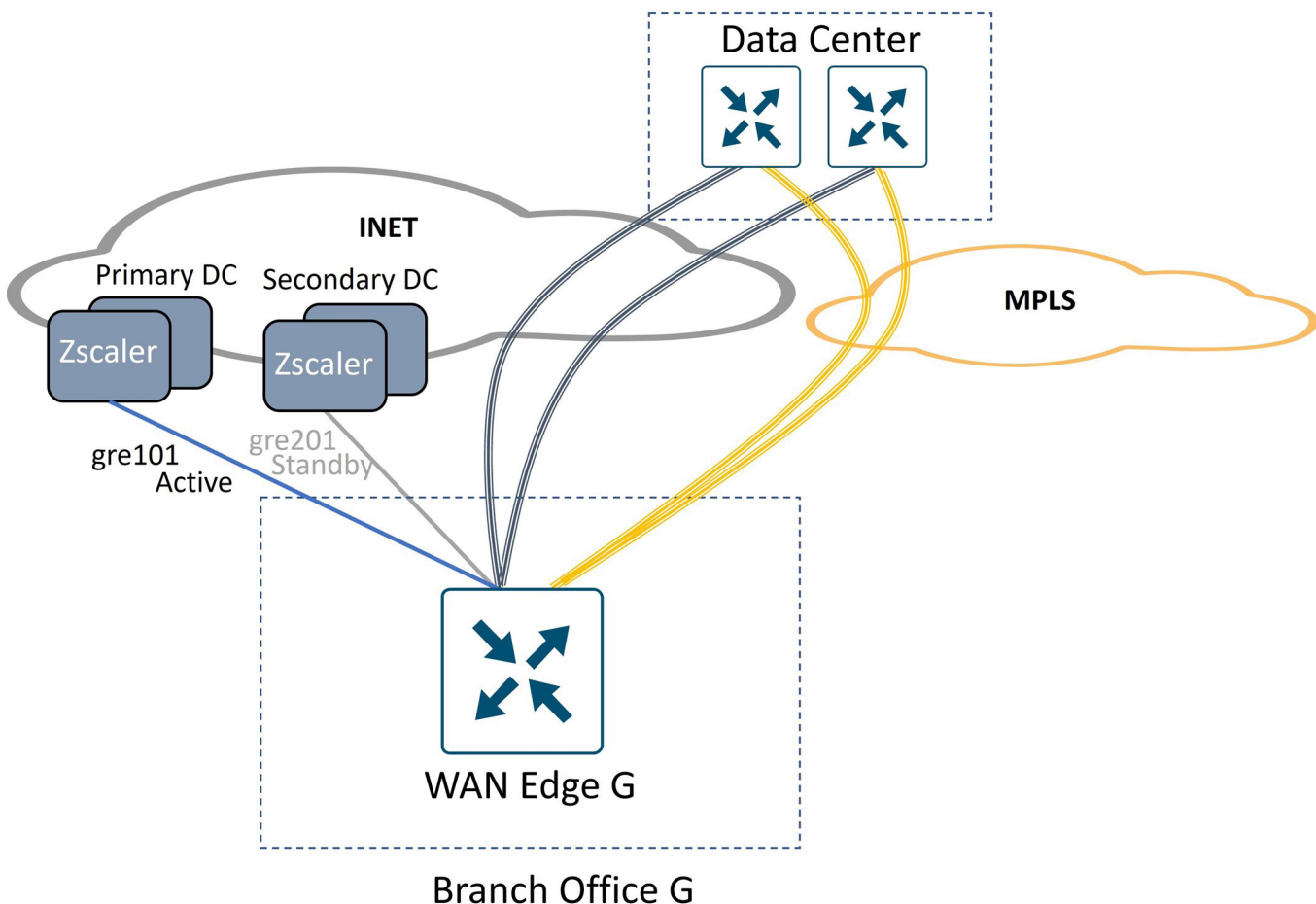


Figure 42. Cisco WAN Edge Auto IPSec or GRE tunnels

Procedure 1: Create a SIG Template

1. On the **Configuration > Templates > Feature Templates** page, click **Add Template** and select devices.
2. In the **VPN** section, select **Cisco Secure Internet Gateway (SIG)**.

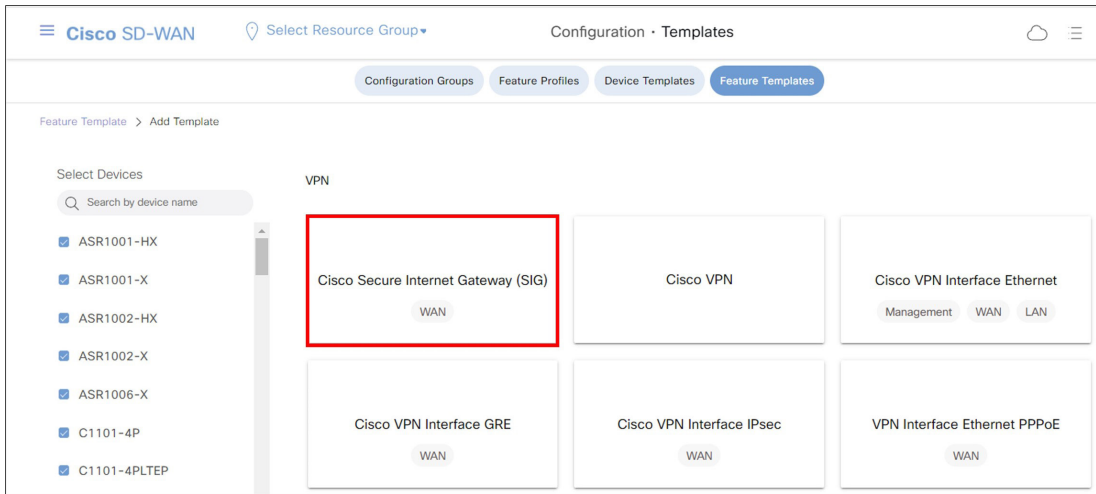


Figure 43. Cisco SIG

3. Enter the Template Name (`xeSig_zscaler`) and Description (`Cisco IOS XE Sig Zscaler Template`).
4. Next to **SIG Provider**, select **Zscaler**.
5. (Cisco IOS XE SD-WAN ONLY) A source IP address for the L7 health tracker is required. This field is a private, unique IPv4 address with a /32 prefix. In the **Tracker (Beta)** section next to **Source IP Address**, choose **Device Specific** from the drop-down menu. The variable for this parameter is labeled `zscaler_trackersrcip`. Note that this field is required for Cisco IOS XE SD-WAN routers. You can turn off health checks under the tunnel configuration advanced settings (not recommended), but you must still configure a global value or device-specific variable for the **Tracker Source IP Address**.

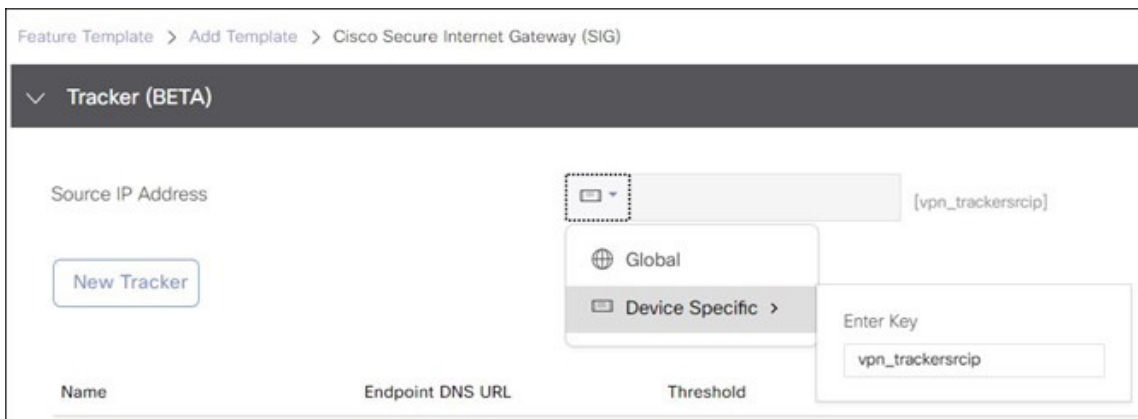


Figure 44. Add SIG template

By default, Cisco vEdge routers use source IP address 192.168.0.2 in VRF 65530 for the L7 health tracker.

You do not need to explicitly configure a tracker for SD-WAN routers because it is created automatically. By default, L7 health checks are enabled on each tunnel with the following default properties.

Section	Parameter	Type	Variable/Value
Tracker	Threshold (msec)	Default	1000
	Interval (sec)	Default	30
	Multiplier	Default	2
	API URL of endpoint	Default	http://gateway.<Zscaler Cloud Name>.net/vpntest

If you choose to change any tracker parameters, configure a custom tracker. A customized tracker configuration is shown in [Procedure 5: \(Optional\) Customize L7 Health Tracker](#).

- In the **Configuration** section, click **Add Tunnel**.
- Next to **Tunnel Type**, select **ipsec** or **gre**. The default is ipsec. After you choose a tunnel type, any additional tunnels configured in the SIG template are automatically chosen to be the same type. GRE is used in this example.

The screenshot shows the 'Configuration' section of a web interface. At the top, there is a dark header with a dropdown arrow and the text 'Configuration'. Below this, there is a large white area. In the top-left corner of this area, there is a button labeled 'Add Tunnel' which is highlighted with a red rectangular box. Below the button, the text 'Basic Settings' is visible. Under 'Basic Settings', there is a section labeled 'Tunnel Type'. This section contains two radio buttons: 'ipsec' and 'gre'. The 'gre' radio button is selected (indicated by a blue dot) and is highlighted with a red rectangular box.

Figure 45. Add tunnel

8. For **Interface Name**, use the global parameter type. Specify an **Interface Name**, which is the keyword `ipsec` or `gre`, followed by a number 1–255 (example: `ipsec1` or `gre1`). Name the interface `gre101`.
9. Next to **Description**, choose **Global** parameter and type an optional **Description** (e.g., `Primary DC Tunnel 1`).
10. Next to **Tunnel Source Interface**, select **Device Specific** and create a variable for this parameter (e.g., `pri_tunnel1_src_int`).
11. Next to **Data-Center**, select which data center at which this tunnel terminates. Each data center location (primary or secondary) is selected automatically when the configuration is deployed, or manually assigned (described later in this guide).
12. (GRE only) GRE tunnels must register their public source IP address through the API calls. Next to **Source Public IP**, select **Device Specific** and create a variable for this parameter (`pri_tunnel1_src_public_ip`).

The screenshot shows a configuration form for adding a GRE tunnel. The form has the following fields and values:

- Interface Name (1..255)**: A dropdown menu with a globe icon, set to `gre101`.
- Description**: A dropdown menu with a globe icon, set to `Primary DC Tunnel 1`.
- Tracker**: A dropdown menu with a checkmark icon, currently empty.
- Tunnel Source Interface**: A dropdown menu with a device icon, set to `[pri_tunnel1_src_int]`.
- Data-Center**: Two radio buttons, **Primary** (selected) and **Secondary** (unselected).
- Source Public IP**: A dropdown menu with a device icon, set to `[pri_tunnel1_src_public_ip]`. An information icon (i) is visible to the right of the field.

Figure 46. Add Tunnel (GRE)

13. Leave the parameters under **Advanced Options** as defaults. Under **Advanced Options**, the following default options are set for IPSec tunnels (shown in the first table) and GRE tunnels (shown in the second table).

Section	Parameter	Type	Variable/value
Advanced Options > General	Shutdown	Default	No
	Track this interface for SIG	Default	On
	IP MTU	Default	1400
	DPD Interval	Default	10
	DPD Retries	Default	3
Advanced Options > IKE	IKE Rekey Interval (seconds)	Default	14400
	IKE Cipher Suite	Default	AES 256 CBC SHA1
	IKE Diffie-Hellman Group	Default	2 1024-bit modules
Advanced Options > IPSec	IPSec Rekey Interval (seconds)	Default	3600
	IPSec Replay Window	Default	512
	IPSec Cipher Suite	Default	Null SHA1
	Perfect Forward Secrecy	Default	None

** As referenced by Field Notice FN72510, Cisco IOS XE Software: Weak Cryptographic Algorithms Are Not Allowed by Default for IPSec Configuration in Certain Cisco IOS XE Software Releases. This affects platforms starting in 17.11.1a and later, and, in a new deployment, will not allow you to configure null encryption for IPSec SIG tunnels. As a workaround, enter `crypto engine compliance shield disable` in the CLI add-on template or in CLI mode and issue a reload. Cisco does not recommend this option as weak cryptographic algorithms are insecure and do not provide adequate protection from modern threats.

Section	Parameter	Type	Variable/value
Advanced Options > General	Shutdown	Default	No
	Track this interface for SIG	Default	On
	IP MTU	Default	1400

14. Click **Add**.

15. In this use case, one additional tunnel is created (the standby tunnel to the secondary data center).

Click **Add Tunnel**.

Section	Parameter	Type	Variable/value
Configuration	Interface Name (1..255)	Global	ipsec201
	Description	Global	Secondary DC Tunnel 1
	Tunnel Source Interface	Device Specific	sec_tunnel1_src_int
	Data center	Radio Button	Secondary
	Data-Center	Radio Button	Secondary

For GRE, use the following settings:

Section	Parameter	Type	Variable/value
Configuration	Interface Name (1..255)	Global	gre201
	Description	Global	Secondary DC Tunnel 1
	Tunnel Source Interface	Device Specific	sec_tunnel1_src_int
	Data-Center	Radio Button	Secondary
	Source Public IP	Device Specific	sec_tunnel1_src_public_ip

16. Click **Add**.

17. Repeat steps 5–16 to define any additional tunnels.

18. After when you are finished adding tunnels, configure which interface you want as active and backup. Under **High Availability**, next to **Pair-1** under the **Active** column, select **ipsec101** from the drop-down menu, and under the Backup column, select **ipsec102**.

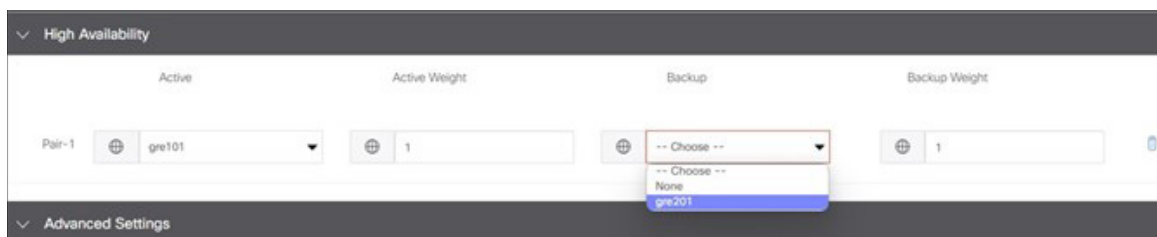


Figure 47. High availability

19. In Advanced Settings, you can choose the primary and secondary data centers (the default is automatic). You also can turn on several Zscaler features for the tunnel through the APIs. They include: Zscaler Location Name, Authentication Required, XFF Forwarding, Enable Firewall, Enable IPS Control, Enable Caution, and Enable AUP. To learn more, see [Configuring Locations](#) (government agencies, see [Configuring Locations](#)).

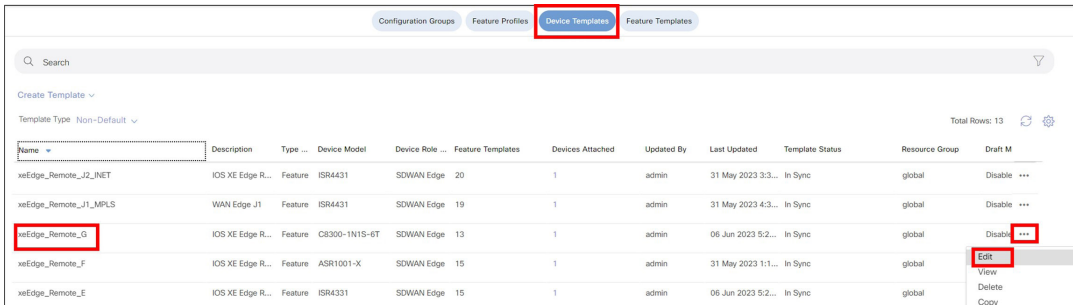
Tech Tip

Outside of **Zscaler Location Name**, do not turn on other Zscaler options under Advanced Settings when bringing up tunnels for the first time. Leave the defaults off to bring up the tunnels. When up, go back and make feature template changes to turn on desired features. Certain features might require certain subscriptions or licenses on Zscaler, and it can make troubleshooting more difficult if you turn on some of the features before bringing up the tunnels for the first time.

20. Under **Advanced Settings**, keep the defaults and click **Save** at the bottom of the screen to save the feature template.

Procedure 2: Add the Tunnel Configuration to the Device Template

1. In Cisco SD-WAN Manager, go to **Configuration > Templates > Device**, and select the **Device Templates** tab. To the right of the device template you want to modify, click ... and select **Edit** from the drop-down menu.



Name	Description	Type	Device Model	Device Role	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	Resource Group	Draft M
xeEdge_Remote_I2_INET	IOS XE Edge R...	Feature	ISR4431	SDWAN Edge	20	1	admin	31 May 2023 3:3...	In Sync	global	Disable ...
xeEdge_Remote_I1_MPLS	WAN Edge J1	Feature	ISR4431	SDWAN Edge	19	1	admin	31 May 2023 4:3...	In Sync	global	Disable ...
xeEdge_Remote_G	IOS XE Edge R...	Feature	CR300-1N1S-ET	SDWAN Edge	13	1	admin	06 Jun 2023 5:2...	In Sync	global	Disable ...
xeEdge_Remote_F	IOS XE Edge R...	Feature	ASR1001-X	SDWAN Edge	15	1	admin	31 May 2023 1:1...	In Sync	global	Edit View Delete Copy
xeEdge_Remote_E	IOS XE Edge R...	Feature	ISR4331	SDWAN Edge	15	1	admin	06 Jun 2023 5:2...	In Sync	global	

Figure 48. Cisco SD-WAN Manager template

2. Under the **Transport & Management VPN** section, select **Cisco Secure Internet Gateway** on the right-hand side. The **Cisco Secure Internet Gateway** field is inserted into the **Transport & Management VPN** section. From the drop-down menu, select the SIG feature template recently created (`xeSig_Zscaler`).



Transport & Management VPN

Cisco VPN 0 *

Cisco Secure Internet Gateway

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Additional Cisco VPN 0 Template

- ☐ Cisco BGP
- ☐ Cisco OSPF
- ☐ Cisco OSPFv3
- ☒ Cisco Secure Internet Gateway
- ☐ Cisco VPN Interface Ethernet
- ☐ Cisco VPN Interface GRE
- ☐ Cisco VPN Interface IPsec

Figure 49. Cisco SIG

- Before you can save the device template, you must attach the SIG Credentials template. In SD-WAN Manager version 20.9 and later, this is done automatically when a SIG feature template is attached to the device template. If running an earlier SD-WAN Manager version, next to **Cisco SIG Credentials ***, attach the SIG credentials feature template that was built in the prerequisites section.

CLI Add-On Template: Choose...

Policy: Choose...

Probes: Choose...

Security Policy: Choose...

Cisco SIG Credentials *: xeSig_Credentials

Figure 50. Cisco SIG credentials

- Click **Update**.
- To the right of the device configuration being updated, click ... and select **Edit Device Template** from the drop-down menu.

Device Template | xeEdge_Remote_G

Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	Interface Name(vpn512_int_name)	IPv4 Address/ prefix-length(vpn512_int_ip4_addr)
⊗	C8300-1N1S-6T-FLM250810CA	10.255.255....	WAN_EdgeG	GigabitEthernet0/0/1	192.168.255.93/23

Edit Device Template

Figure 51. Edit device template

- Fill in the missing variable values. Fill in the **Tunnel Source Interface** for the primary and secondary tunnels and which physical interface the tunnel are routed through (this is especially important if the source interface is a loopback interface). If you have configured a GRE tunnel, specify the **Source IP Address** for the tunnel that is registered on Zscaler. Fill in the source IP address for the L7 health check.
- Click **Update**.

Tunnel Source Interface(pri_tunnel1_src_int): GigabitEthernet0/0/0

Tunnel Source Interface(sec_tunnel1_src_int): GigabitEthernet0/0/0

Source IP Address(vpn_trackersrcip): 10.11.11.1/32

Hostname(host-name): WAN_EdgeE

System IP(system-ip): 10.255.255.215

Generate Password

Update Cancel

Figure 52. Cisco SIG update

- Deploy template changes: click **Next**, then **Configure Devices**. The configuration changes are pushed and Cisco SD-WAN Manager returns success.

Procedure 3: Add Service Route

The last step is to redirect traffic. In this section, a SIG service route (default route) is installed into the service VPN to direct service-side internet traffic to Zscaler. You can configure this in all service VPN templates to redirect traffic. The SIG service route is not an optional setting, but if a SIG tunnel is not up and operational on the router, the route is not installed. You can either modify the service VPN template currently in use or create a separate service VPN template for routers that use the SIG service route. In this example, the current service VPN feature template is modified.

1. On the Cisco SD-WAN Manager page, select the **Configuration > Templates > Feature** tab and find the branch service VPN feature template to modify (e.g., xeBR_VPN1).
2. To the right of the feature template, click ... and select **Edit** from the drop-down menu.

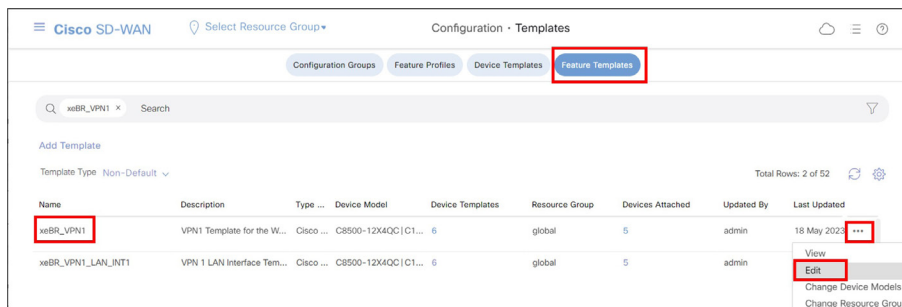


Figure 53. Cisco SD-WAN Manager feature

3. Click the **Service Route**.
4. Click the **New Service Route** button.
5. Next to **Prefix**, enter 0.0.0.0/0. The **Service** defaults to **SIG**. Click **Add** to add the service route to the configuration, then click **Update** to save the xeBR_VPN1 feature template.

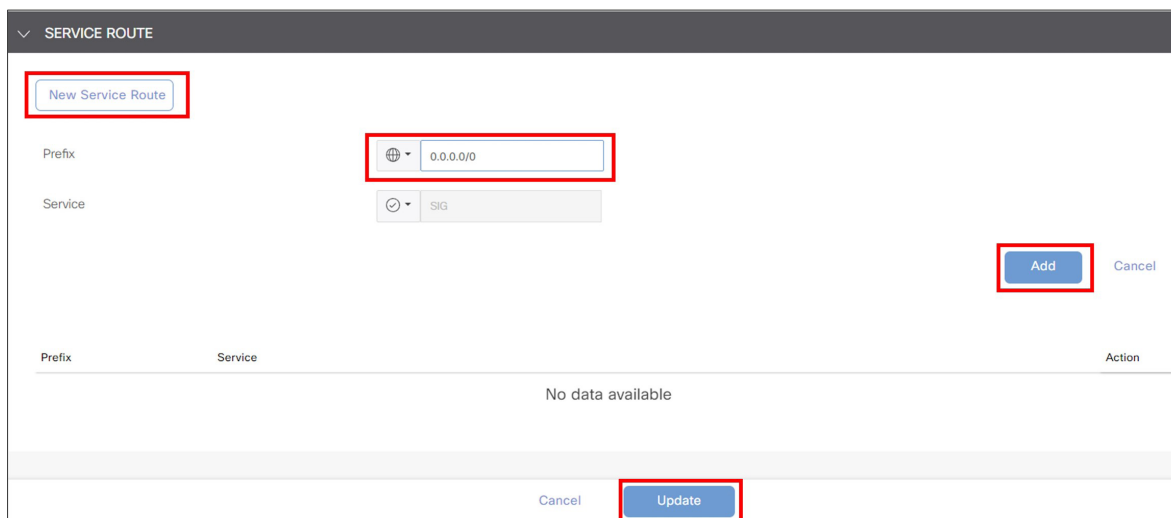


Figure 54. New service route

6. Click **Next**, then **Configure Devices**. Confirm changes on multiple devices if needed and click **OK**. The status of the configuration change returns with **Success**.

Procedure 4: Verify Tunnel Operation

1. In the SD-WAN Manager GUI under **Monitor > Tunnels**, click the **SIG Tunnels** tab to view the tunnel status and any events related to the SIG tunnel.

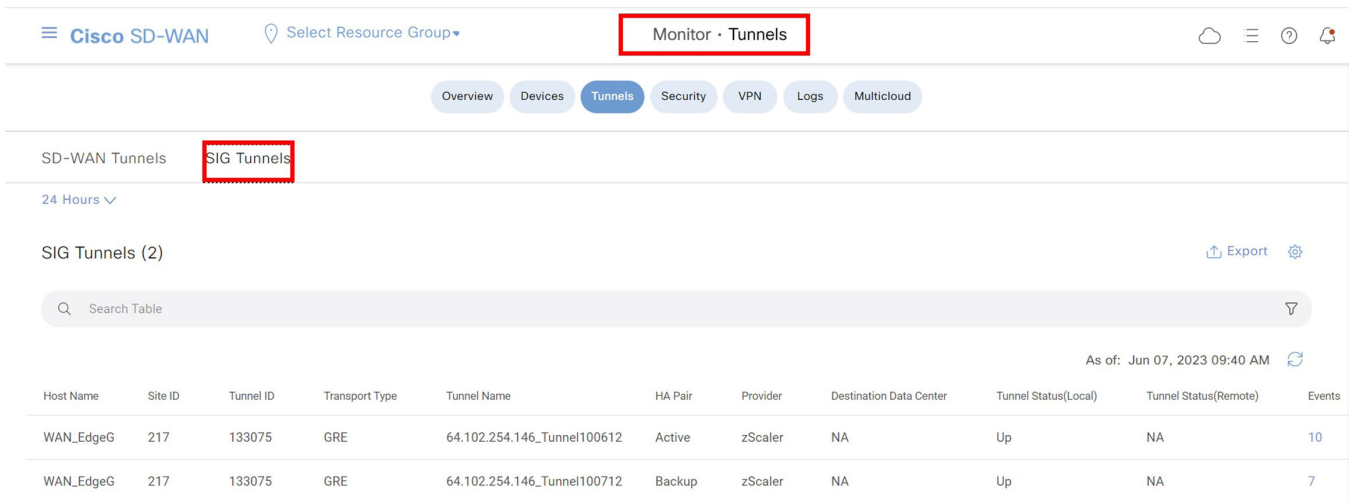


Figure 55. Monitor SIG Tunnels

2. In the SD-WAN Manager GUI under **Monitor > Devices**, click the WAN Edge router that you want to verify the tunnel operation on.
3. Under **Applications > Interface**, click **Real Time** at the top right of the chart. You can also click the interface you are interested in on the right-hand side of the chart.

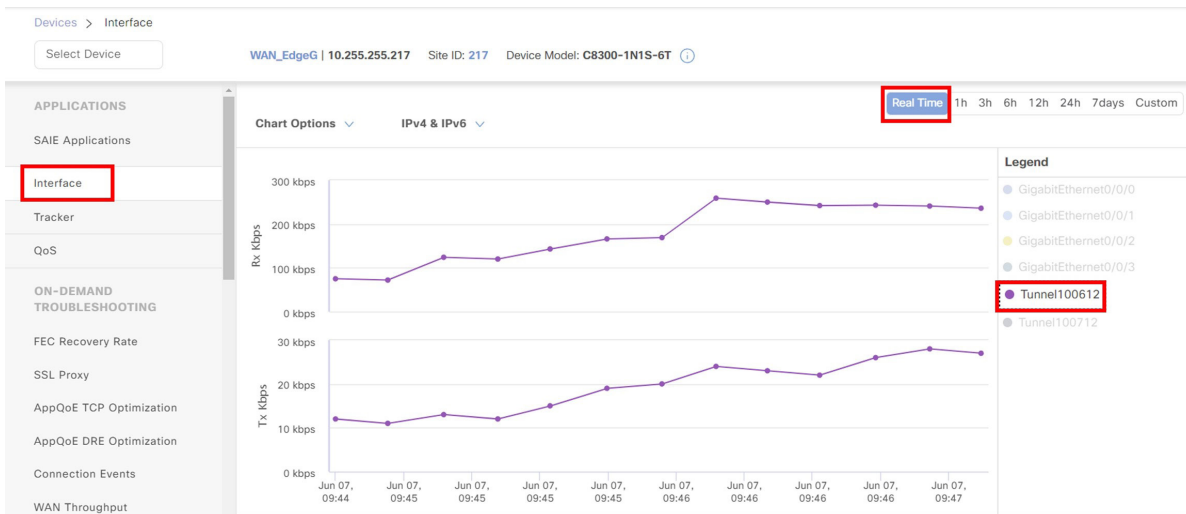


Figure 56. WAN Edge tunnel interface

- If the interface you are interested in is missing from the graph, scroll down past the chart to see the entire list of interfaces. Click the checkbox on the left for the interface you want to display on the chart. You can also view the state and statistics of the various interfaces on the device from this list.

VPN (VRF)	Interface Name	Interface description	Physical Address	IPv4 Address	IPv4 Subnet Mask	Admin Status	Oper Status
<input type="checkbox"/> 65530	Loopback65530	-	44:ae:25:3a:b1:e0	10.10.10.10	255.255.255.255	↑	↑
<input checked="" type="checkbox"/> 0	Tunnel100612	-	00:00:00:00:00:00	64.102.254.146	255.255.255.240	↑	↑
<input checked="" type="checkbox"/> 0	Tunnel100712	-	00:00:00:00:00:00	64.102.254.146	255.255.255.240	↑	↑

Figure 57. Interface state and statistics

See the [Operate](#) section of this guide for additional monitoring and troubleshooting information.

Procedure 5: (Optional) Customize L7 Health Tracker

In this section, the L7 health tracker is customized.

- In the SD-WAN Manager GUI, go to **Configuration > Templates** and click the **Feature Templates** tab. To the right of the SIG feature template that was created in the earlier section (xeSig_Zscaler), click ... and select **Edit** from the drop-down menu.
- In the **Tracker (Beta)** section, click the **New Tracker** button. Next to **Name**, select **Global** for the parameter and enter the name for the tracker (zscaler_L7_health_check), which is a label referenced by each tunnel using the tracker.
- For **Interval**, the default is 60 seconds and the minimum allowed is 20 seconds. Change the parameter to **Global**, and enter 20. For the API URL of endpoint, enter `http://gateway.<Zscaler Cloud Name>.net/vpntest` for the specific Zscaler cloud you belong to.

New Tracker

Name: zscaler_l7_health_check

Threshold: 300

Interval: 20

Multiplier: 3

API url of endpoint: http://gateway.zscalerbeta.net/vp

Figure 58. New tracker

4. Click **Add**.
5. Before finishing the update to the feature template, reference the new L7 health tracker by the tunnels already created. Under **Configuration** next to each tunnel, click the **Edit** icon.

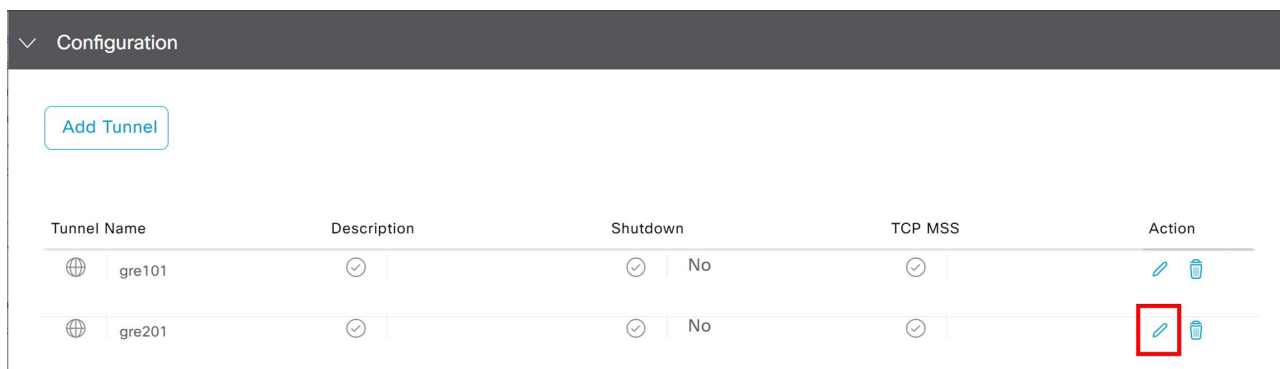


Figure 59. Add tunnel

6. Next to **Tracker**, choose the **Global** parameter, then in the drop-down menu, select the L7 health check you created, `zscaler_L7_health_check`.
7. Click **Save Changes**.

The screenshot shows the 'Update Tunnel' form. It has several fields: 'Tunnel Type' with radio buttons for 'ipsec' and 'gre' (selected); 'Interface Name (1..255)' with a text input field containing 'gre101'; 'Description' with a text input field and a checkmark icon; 'Tracker' with a dropdown menu showing 'zscaler_l7_health_check' selected (this field is highlighted with a red box); 'Tunnel Source Interface' with a dropdown menu and a text input field containing '[pri_tunnel1_src_int]'; and 'Data-Center' with radio buttons for 'Primary' (selected) and 'Secondary'.

Figure 60. Update tunnel

8. Repeat steps 5–7 with each tunnel.

- Click **Update** to save changes to the SIG feature template. Click **Next**, then **Configure Devices**. You might need to confirm configuration changes on multiple devices. Select the checkbox and click **OK**. The configuration changes are pushed out to the attached WAN Edge routers. The status returns **Success**.

```
WAN_EdgeG#show endpoint-tracker
```

Interface	Record Name	Status	RTT in msecs	Probe ID	Next Hop
Tunnel100612	zscaler_17_health_chec	Up	10	25	None
Tunnel100712	zscaler_17_health_chec	Up	77	26	None

Procedure 6: (Optional) Enable Advanced Zscaler Features

- In the ZIA Admin Portal, you can view the gateway options enabled for a location by going to **Administration > Resources > Location Management** and editing the location in which you are interested. You modify gateway options via APIs from the Cisco SD-WAN Manager.

Edit Location

Note: All partner managed location attributes must be edited from the SD-WAN partner's management portal. Any changes made here may get overridden by the SD-WAN partner.

LOCATION

Name
site217sys10x255x255x217

Country
None

City/State/Province
Enter Text

Manual Location Group
None

Exclude from Manual L
☐

Location Type
Corporate user traffic

GATEWAY OPTIONS

Use XFF from Client Request
☐

Enforce Authentication
☐

Enable Caution
☐

Enable AUP
☐

Enforce Firewall Control
☐

Figure 61. Edit location

2. To change the settings, modify the SIG template feature template in the Cisco SD-WAN Manager. Go to **Configuration > Templates > Feature Templates**. Find the name of the SIG template you want to modify (xeSig_Zscaler). Click ... to the far right of the template and select **Edit** from the drop-down menu.
3. Under **Advanced Settings**, select the **Global** parameter and click **On** next to the settings you want to enable. In this example, **Enable Caution** is enabled.
4. Click **Update**.

Note

This enables the same Zscaler advanced settings for every device this template is attached to. If you need different settings for different devices, a separate SIG feature template is required.

Feature Template > Cisco Secure Internet Gateway (SIG) > xe_Sig_Zscaler

Primary Data-Center	<input checked="" type="checkbox"/> Auto i
Secondary Data-Center	<input checked="" type="checkbox"/> Auto i
Zscaler Location Name	<input checked="" type="checkbox"/> Auto
Authentication Required	<input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off
XFF Forwarding	<input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off
Enable Firewall	<input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off
Enable IPS Control	<input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off
Enable Caution	<input checked="" type="checkbox"/> <input checked="" type="radio"/> On <input type="radio"/> Off

Figure 62. Update

5. Click **Next**, then **Configure Devices**. Confirm configuration on multiple devices if needed. Configuration changes are pushed to the devices and Success is returned.

- View the location gateway options in the ZIA Admin Portal for changes.

Figure 63. Enable caution

Procedure 7: (Optional) Customize Zscaler Tunnel Destination (Primary and Secondary Data Centers)

Zscaler recommends that you use automation to determine the primary and secondary data centers. To change the tunnel destination settings to choose your own primary and secondary Zscaler data center locations, modify the SIG template feature template.

- Go to **Configuration > Templates > Feature Templates**. Find the name of the SIG template you want to modify (xeSig_Zscaler). Click ... to the far right of the template and select **Edit** from the drop-down menu.
- Under **Advanced settings**, next to **Primary Data-Center**, select the **Device Specific** parameter and use the variable `vpn_zlsprimarydc`. Next to **Secondary Data-Center**, select **Device Specific** and use the variable `vpn_zlssecondarydc`.

Figure 64. SIG template edit

- Click **Update** to save the feature template settings.

Tech Tip

If you select a global parameter, you can select available Zscaler data centers from the drop-down menu. Select a data center that is part of your assigned Zscaler cloud. In earlier versions of the code, this list of data centers was static and thus, not fully up-to-date. Use a device specific parameter if you need to specify a data center that is not in the list or you need to specify different data centers for different devices attached to the same feature template. To get the most up-to-date list of Zscaler data centers, check: <https://config.zscaler.com/<Zscaler Cloud Name>.net/cenr>.

In this example, the list for Zscaler cloud Beta is located at <https://config.zscaler.com/zscalerbeta.net/cenr>.

Note that if you use a variable to specify a data center that is not in the recommended list for that location, then a data center is chosen automatically.

4. At the top of the page, select a device template for which you need to fill in data center values if there is more than one device attached to the SIG feature template. To the right of the device, click ... and select **Edit Device Template** from the drop-down menu.

Figure 65. Edit device template

5. Enter the values for the **Primary** and **Secondary** data centers. Use VPN Host names for IPSec tunnel destinations and IP addresses for GRE tunnel destinations. Note that auto is an acceptable value for those locations where the tunnels are automatically discovered for you. This example uses the data center locations Frankfurt IV (165.225.72.38) for **Primary** and Washington, DC (104.129.194.38) for **Secondary**.

Note

If you are filling in values for primary and secondary data center variables, use IP addresses for GRE tunnel destinations and VPN host names for IPSec tunnel destinations. If IPSec tunnels are used instead, the example would use data center locations Frankfurt IV (`fra4-vpn.zscalerbeta.net`) for primary and Washington, DC (`was1-vpn.zscalerbeta.net`) for secondary.

6. Click **Update**.

Figure 66. Update device template

7. Update variable values on other devices attached to device templates using the feature template you just modified.
8. Click **Next**, then **Configure Devices**. Confirm configuration changes on multiple devices if needed. Cisco SD-WAN Manager pushes the configuration changes and indicates **Success**.
9. Open a client browser at the site, go to <https://ip.zscaler.com>. Validate that the primary data center is accessed (in this example, Frankfurt IV).

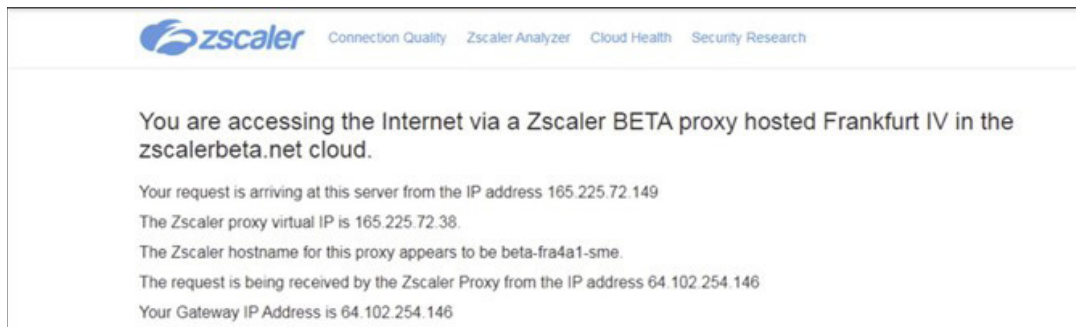


Figure 67. Zscaler IP config

Deploy: Cisco WAN Edge Auto IPSec or GRE Tunnels (Active/Active Tunnels, Hybrid Transport)

In this section, two active auto IPSec tunnels are configured, all to the same Zscaler data center. Traffic is forwarded on both tunnels to the primary data center until a tunnel is declared down (through L7 health checking and/or dead peer detection). When down, traffic is hashed to the remaining tunnel. When the downed tunnel recovers, it becomes active again and traffic is hashed to it again.

This deployment use case contains the following features:

- One active/active IPSec or GRE auto tunnel pair on a single internet transport. Both tunnels connect to the same primary Zscaler data center.
- ECMP based on the source IP address.
- Centralized data policy for redirecting traffic to Zscaler tunnels.
- Weighted tunnels.

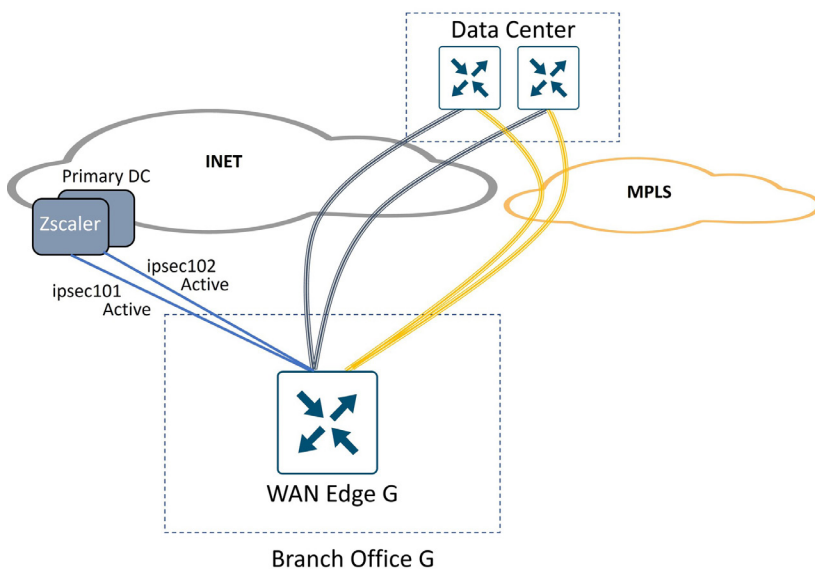


Figure 68. Cisco WAN Edge auto IPSec tunnels

Tech Tip

This use case is designed to illustrate how to configure multiple active/active tunnels over a single internet transport. You can add additional active tunnels (up to 4) or add standby tunnels for any active tunnel as well.

With 4-tuple ECMP hashing, you want to keep all active tunnels pointing to the same Zscaler DC. If you choose to implement standby tunnels, you want them pointing to the same Zscaler DC as the active tunnels in the event one or a subset of standby tunnels become active. You do not want equal cost paths where the same user application session can hash to different Zscaler DCs. Alternatively, use Source IP-based ECMP hashing, which removes this restriction.

To accommodate both tunnels to one Zscaler destination, two loopback interfaces are needed for source IP addresses since each tunnel needs a unique source IP/source port/destination IP/destination port pair.

Procedure 1: Create two loopback interfaces, one for each active tunnel (Cisco IOS XE SD-WAN only)

1. In the Cisco SD-WAN Manager, go to **Configuration > Templates > Feature Templates** tab. Click **Add Template**, select your devices, and under **VPN**, select **Cisco VPN Interface Ethernet**.
2. Enter a **Template Name** and **Description**. Under basic configuration next to **Shutdown**, choose **Global** parameter and click **No**. Next to **Interface Name**, enter `Loopback1`, and next to **IPv4 Address/prefix-length**, choose **Global** parameter and type the address (`10.10.10.1/32` in this example).

Note

You must address loopback interfaces used as the source for GRE tunnels with a unique public IP address or a unique private IP address so that One-to-One NAT can happen with an external device. You might decide to use device-specific variables rather than global parameters for this reason.

Feature Template > Add Template > Cisco VPN Interface Ethernet

Template Name*

Description*

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP TrustSec Advanced

▼ BASIC CONFIGURATION

Shutdown ☐ Yes ☒ No

Interface Name

Description

IPv4 IPv6

☐ Dynamic ☒ Static

IPv4 Address/ prefix-length

Figure 69. Loopback interface

3. Click **Save**.

4. Copy the previous template and make modifications or create new interface Ethernet feature templates by repeating steps 1 through 3 to create two total loopback addresses with the following characteristics:

Template Type: Feature Template > Cisco VPN Interface Ethernet

Feature Template Name	Section	Parameter	Type	Variable/value
Loopback1	Basic Configuration	Shutdown	Global	No
		Interface Name	Global	Loopback1
		IPv4	Radio Button	Static
		IPv4 Address/prefix-length	Global	10.10.10.1/32
Loopback2	Basic Configuration	Shutdown	Global	No
		Interface Name	Global	Loopback2
		IPv4	Radio Button	Static
		IPv4 Address/prefix-length	Global	10.10.10.2/32

Procedure 2: Create a local policy-based routing policy (Cisco IOS XE SD-WAN only)

Create a CLI add-on template that configures a local policy-based routing policy. This lets any control traffic pick the proper next-hop interface generated by the router.

1. If you've already created a CLI add-on feature template, edit the feature template and go to step 4. To create a new one, go to **Configuration > Templates**.
2. Click the **Feature Templates** tab.
3. Click **Add Template**.
4. Select the devices the feature template can apply to.
5. Under **Other Templates**, click **Cli Add-On Template**.

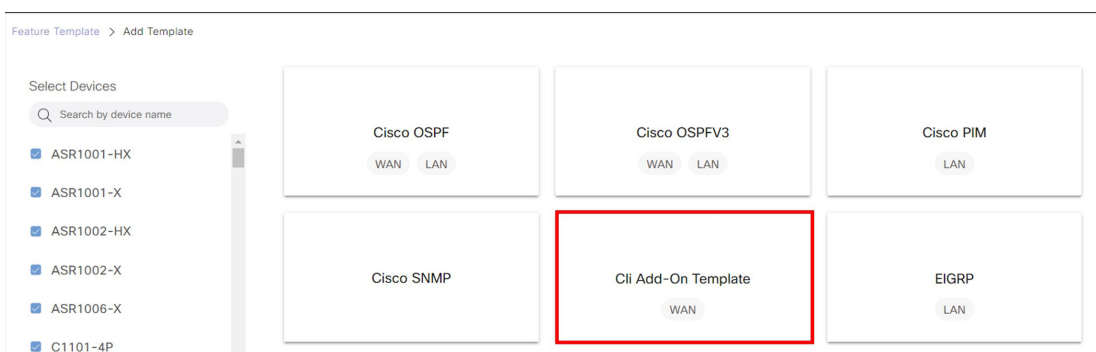


Figure 70. Other templates

6. Enter a **Template Name** (CLI-Template) and **Description** (CLI Add-on Template).
7. Add the following CLI:

```
ip access-list extended SIG
 10 permit ip host 10.10.10.1 any
 20 permit ip host 10.10.10.2 any
!
route-map Tunnel-Control permit 10
match ip address SIG
set ip next-hop 64.100.217.1
ip local policy route-map Tunnel-Control
```

8. Highlight **64.100.217.1** as the next-hop and click **(x) Create Variable**.

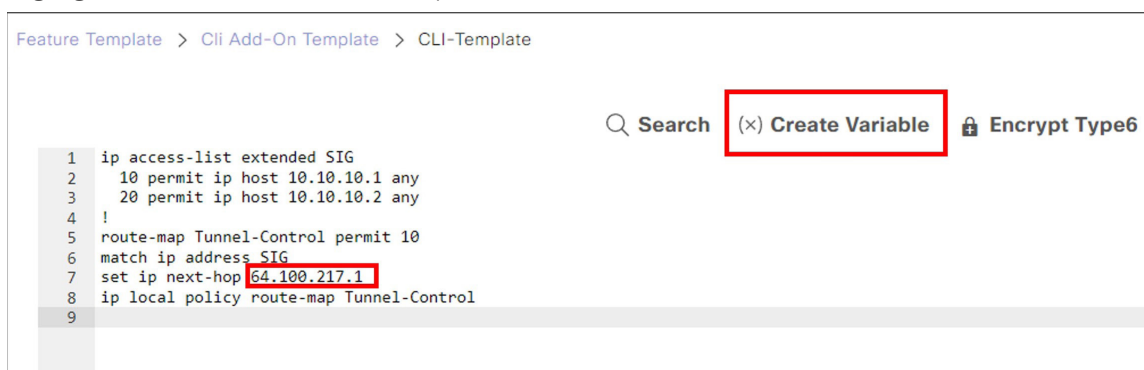


Figure 71. CLI configuration

9. In the dialog window, enter a variable name (Loopback-Tun-Src-Next-Hop-IP). This CLI template can apply to several WAN Edge routers. Click **Create Variable**.

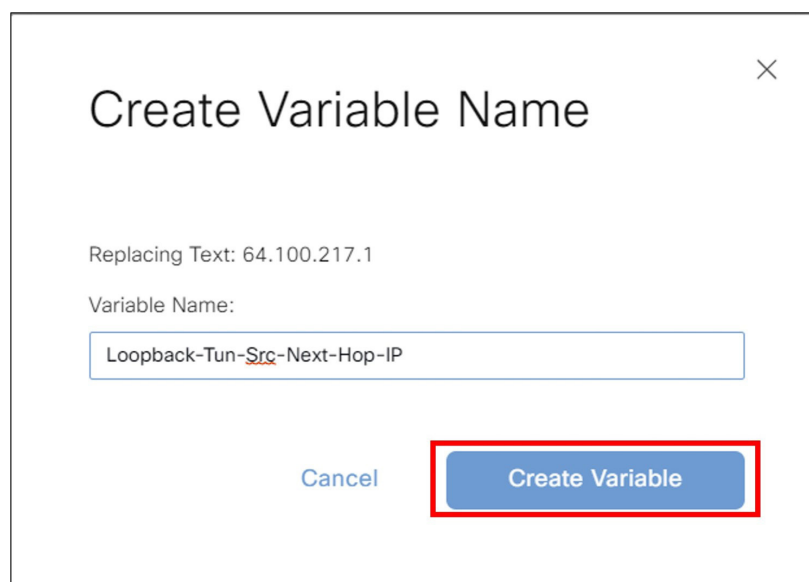


Figure 72. Create variable name

10. Click **Save/Update**.

Procedure 3: (Optional) IOS XE SD-WAN Only: Configure Source IP-Based ECMP

Note

In this version of code, you can configure source IP-based ECMP only when the WAN Edge router is in CLI mode. You first change the WAN Edge router to CLI mode and then you can configure the `ip cef load-sharing algorithm src-only` command. You must then keep the router in CLI mode. If you try to use an add-on CLI template (or any device template), the ECMP configuration returns to the default, which is 4-tuple. This seems to affect hardware-based IOS XE SD-WAN routers and is fixed in 17.12.

1. Edit the CLI add-on feature template created or modified in Procedure 2.
2. On a separate line in the configuration, enter the command `ip cef load-sharing algorithm src-only`.

```
Feature Template > CLI Add-On Template > CLI-Template

1 ip cef load-sharing algorithm src-only
2
3 ip access-list extended SIG
4 10 permit ip host 10.10.10.1 any
5 20 permit ip host 10.10.10.2 any
6 !
7 route-map Tunnel-Control permit 10
8 match ip address SIG
9 set ip next-hop {{Loopback-Tun-Src-Next-Hop-IP}}
10 ip local policy route-map Tunnel-Control
11
```

Figure 73. CLI-Template

Procedure 4: Create a New SIG Feature Template with Two Active Tunnels (Cisco IOS XE SD-WAN Only)

1. In the Cisco SD-WAN Manager, go to **Configuration > Templates** and click **Feature Templates**. Click **Add Template**, select the devices the feature template can apply to. Under **VPN**, select the **Cisco Secure Internet Gateway (SIG)** template. Enter the **Template Name** (xeSig_Zscaler_2_Loopback_Source) and **Description** (Sig Zscaler 2 Tunnels with Loopback Source).
2. Next to **SIG Provider**, click **Zscaler**.
3. Under **Tracker (BETA)**, select **Device Specific** and use the variable vpn_trackersrcip.
4. Under **Configuration**, click **Add Tunnel**.
5. Next to **Tunnel Type**, select **ipsec** or **gre**. The default is **ipsec**. After you choose a tunnel type, any additional tunnels configured in the SIG template are automatically chosen for the same type. IPsec is used in this example.
6. Next to **Interface Name**, use the global parameter type. Specify an **Interface Name**, which is the keyword **ipsec** or **gre**, followed by a number 1-255 (example: ipsec1 or gre1). Name the tunnel ipsec101.
7. Next to **Description**, choose the **Global** parameter and enter an optional **Description** (Primary DC Tunnel 1).
8. Next to **Tunnel Source Interface**, select **Device Specific** and create a variable for this parameter (pri_tunnel1_src_int).

Note

Before version 20.8/17.8, if you are using loopback interfaces as a Tunnel Source Interface, use a global parameter. When you specify a loopback interface, a Tunnel Route-via Interface field is added to the feature template so you can specify which physical interface is associated with which loopback interface. This directs data traffic out the proper interface.

9. Next to **Data-Center**, select the data center that terminates this tunnel (Primary). Each data center location (primary or secondary) is selected automatically when the configuration is deployed, or is assigned manually in a later section.

Feature Template > Cisco Secure Internet Gateway (SIG) > xeSig_Zscaler_2_Loopback_Source

Add Tunnel

Interface Name (1..255)

Description

Tracker

Tunnel Source Interface

Data-Center ☒ Primary ☐ Secondary

Figure 74. Add tunnel

10. (GRE only) GRE tunnels must register their public source IP address through the API calls. Next to **Source Public IP**, select **Device Specific** and create a variable for this parameter (pri_tunnel1_src_public_ip).
11. Leave the parameters under **Advanced Options** as defaults.
12. Click **Add**.
13. Finish configuring the tunnel interfaces by repeating steps 1–12 to configure two tunnels total with the following characteristics. All active tunnels point to the primary data center.

Section	Parameter	Type	Variable/Value
Configuration	Interface Name	Global	ipsec101
	Description	Global	Primary DC Tunnel 1
	Tunnel Source Interface	Device Specific	pri_tunnel1_src_int
	Data-Center	Radio Button	Primary
Configuration	Interface Name	Global	Ipsec102
	Description	Global	Primary DC Tunnel 2
	Tunnel Source Interface	Device Specific	pri_tunnel2_src_int
	Data-Center	Radio Button	Primary
	Data-Center	Radio Button	Primary

14. Under **High Availability**, add one additional tunnel pair and assign **ipsec101** under the **Active** column for Pair-1 and **ipsec201** under the **Active** column for Pair-2.

Figure 75. High availability

15. Click **Save** to save the new SIG feature template.

Procedure 5: Modify Device Template

Add the SIG feature template to the device template. This step assumes there is no previously defined SIG feature template configuration. If a template configuration is already defined, Zscaler recommends you delete it from the device template and push the configuration changes to the router before adding the new tunnel configuration.

1. Go to **Configuration > Templates**. Under the **Device Templates** tab, next to the device template you want to modify, click ... on the right-hand side, and select **Edit** from the drop-down menu.
2. Under **Transport & Management VPN**, click **Cisco Secure Internet Gateway** on the right-side under **Additional Cisco VPN 0 Templates**.
3. Choose the new SIG template created in the last procedure (xeSig_Zscaler_2_Loopback_Source).
4. Click **Cisco VPN Interface Ethernet** on the right-hand side two times under **Additional Cisco VPN 0 Templates** and then select **xeLoopback1** for one, and **xeLoopback2** for the other.

Transport & Management VPN

Cisco VPN 0 *

Cisco Secure Internet Gateway

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Additional Cisco VPN 0 Templates

- + Cisco BGP
- + Cisco OSPF
- + Cisco OSPFv3
- + Cisco Secure Internet Gateway
- + Cisco VPN Interface Ethernet
- + Cisco VPN Interface GRE
- + Cisco VPN Interface IPsec
- + VPN Interface Cellular
- + VPN Interface MultiLink Controller
- + VPN Interface Ethernet PPPoE
- + VPN Interface DSL IPoE

Figure 76. Transport & Management VPN

- Under **Additional Templates**, choose the **CLI Add-On Template** created earlier (CLI-Template).
- Before you save the device template, you must attach the **SIG Credentials** template. In SD-WAN Manager version 20.9 and later, this is done automatically when a SIG feature template is attached to the device template. If running an earlier SD-WAN Manager version, next to **Cisco SIG Credentials ***, attach the SIG credentials feature template that was built in the prerequisites section.
- Click **Update**.

Additional templates

Configuration Groups Feature Profiles **Device Templates** Feature Templates

ThousandEyes Agent

TrustSec

CLI Add-On Template

Policy

Probes

Tenant

Security Policy

Cisco SIG Credentials *

Figure 77. Additional templates

8. Next to the device you need to define values for, click ... and select **Edit Device Template**.
9. Fill in values for the variables created in the feature template.
10. Click **Update**.

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	C8300-1N1S-6T-FLM250810CA
System IP	10.255.255.217
Hostname	WAN_EdgeG
Loopback-Tun-Src-Next-Hop-IP	64.100.217.1
Prefix(vpn_ipv4_ip_prefix_natDIA)	Optional

Figure 78. Variable list

The following image shows the updated device template.

Tunnel Source Interface(pri_tunnel1_src_int)	Loopback1
Tunnel Source Interface(pri_tunnel2_src_int)	Loopback2
Tunnel Route-via Interface(tunnel_route_via_ipsec101)	GigabitEthernet0/0/0
Tunnel Route-via Interface(tunnel_route_via_ipsec201)	GigabitEthernet0/0/0
Source IP Address(vpn_trackersrcip)	10.10.10.10/32
Hostname	WAN_EdgeG

Figure 79. Update device template

11. Click **Next**, then **Configure Devices**. After the configuration changes are pushed to the WAN Edge, the status displays as **Success**.
12. Verify tunnel operation.

Procedure 6: Add Centralized Data Policy for Traffic Redirection

This section assumes a centralized policy already exists in the network and is activated on the Cisco SD-WAN Controllers. An example data policy is constructed which directs:

- Company destination traffic to take the SD-WAN overlay tunnels.
- DNS requests to use the DIA (if the internet transport fails, traffic is routed over the overlay).
- Box application traffic to use the DIA (if the internet transport fails, traffic is routed over the overlay).
- The remaining traffic over the SIG tunnels.

1. Go to **Configuration > Policies > Custom Options > Lists** (under **Centralized Policy**).

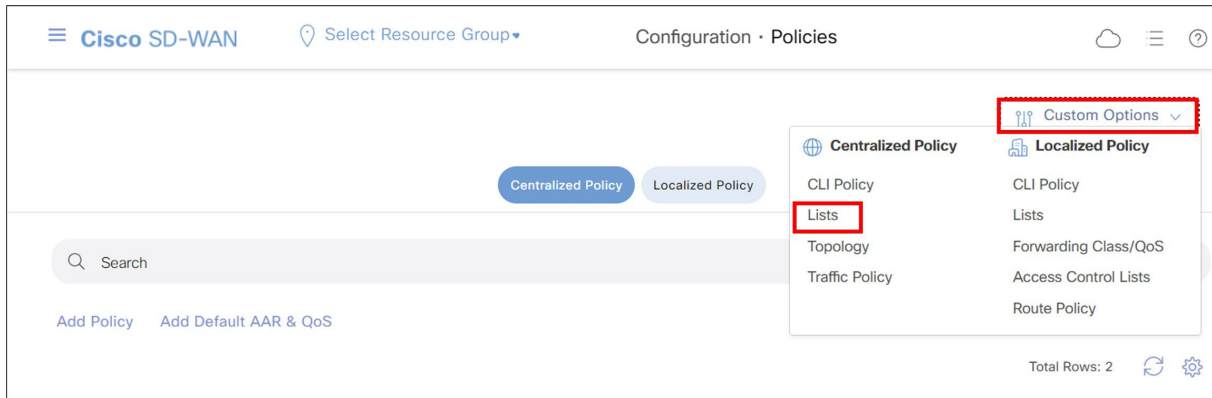


Figure 80. Cisco SD-WAN Manager custom options

2. Select **Data Prefix** from the left-side pane and create a Prefix List called `Overlay` that contains the `10.0.0.0/8` prefix and any other site prefix/summary advertised into the SD-WAN overlay.

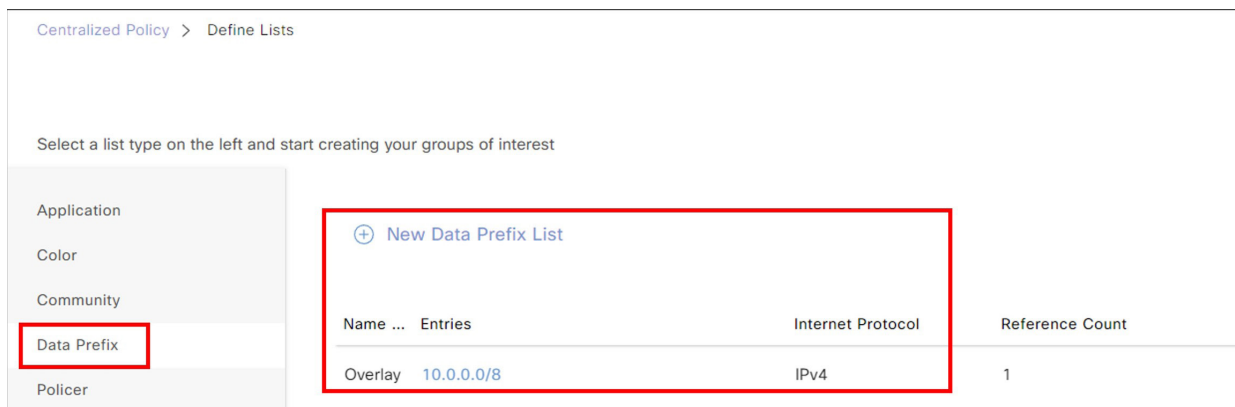


Figure 81. Define lists

3. Select **Application** from the left-side pane and create a **New Application List** called **Box**.

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class

Application List Custom Applications Cloud Discovered

[+ New Application List](#)

Application List Name*

☒ Application ☐ Application Family

Box x

Figure 82. Application list name

4. Ensure the WAN Edge router to which you are applying the policy is defined in a site list and there is a VPN list that contains the VPN to which you want to apply the policy. If not, create the site list.

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class

[+ New Site List](#)

Name	Entries	Reference Count	Updated By
J1-J2	219	0	admin
vEdge	211, 212, 213	0	admin
Zscaler-DataPolicy-Sites	214, 215, 212, 217	1	admin

Figure 83. VPN policy

5. The service VPN for Zscaler traffic is **VPN1**. Create the VPN list if needed.

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

[+ New VPN List](#)

Name	Entries	Reference Count	Updated By
VPN1	1	1	admin

Figure 84. New VPN list

6. To edit or create a new traffic policy for a WAN Edge router, go to **Custom Options** and under **Centralized Policy**, select **Traffic Policy**.

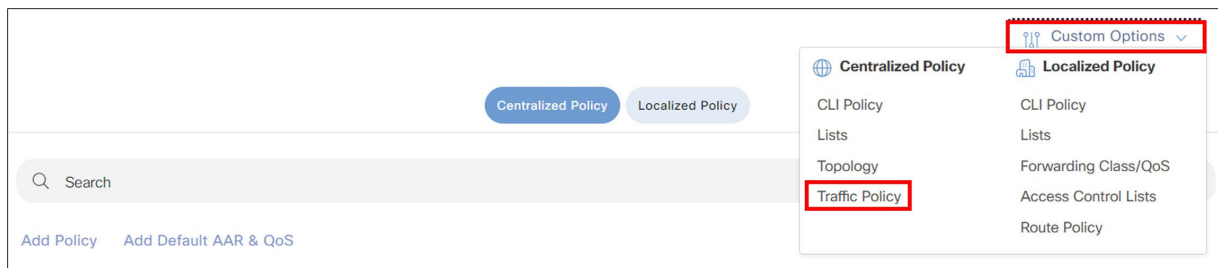


Figure 85. Configuration policies

7. Click the **Traffic Data** tab at the top of the page.

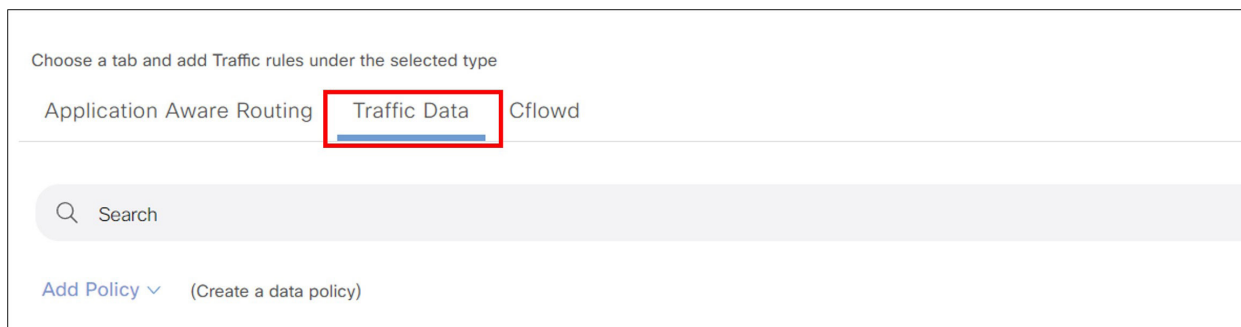


Figure 86. Traffic data

8. If there is already a data policy attached to the WAN Edge router site to which you want to add a SIG data policy, choose to edit the existing policy, or create a new data policy and import it into the master policy already attached to the Cisco SD-WAN Controllers. In this example, a new data policy is created and imported into a master policy already attached to the Cisco SD-WAN Controllers.
9. Click **Add Policy** and select **Create New** from the drop-down menu.

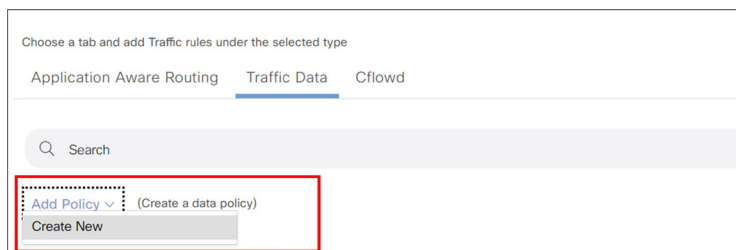


Figure 87. Add policy

10. **Name** the Data Policy (Sig_Data) and give it a **Description** (Data Policy for Sig Data).

11. Click **Sequence Type** and select **Custom**.

Figure 88. Sequence type

12. Click **Sequence Rule**. Select **Match Conditions** and **Actions**, then click **Save Match and Actions**. Repeat as needed to complete the policy.

Figure 89. Sequence rule

In this example, the following policy is configured:

Sequence Rule	Match Parameter	Match Value	Action/s
1	Destination Data Prefix	Overlay	Accept
2	DNS	Request	Accept/NAT VPN with Fallback
3	Application/Application Family List	Box	Accept/NAT VPN with Fallback
4	<empty>		Accept/Secure Internet Gateway with Fallback

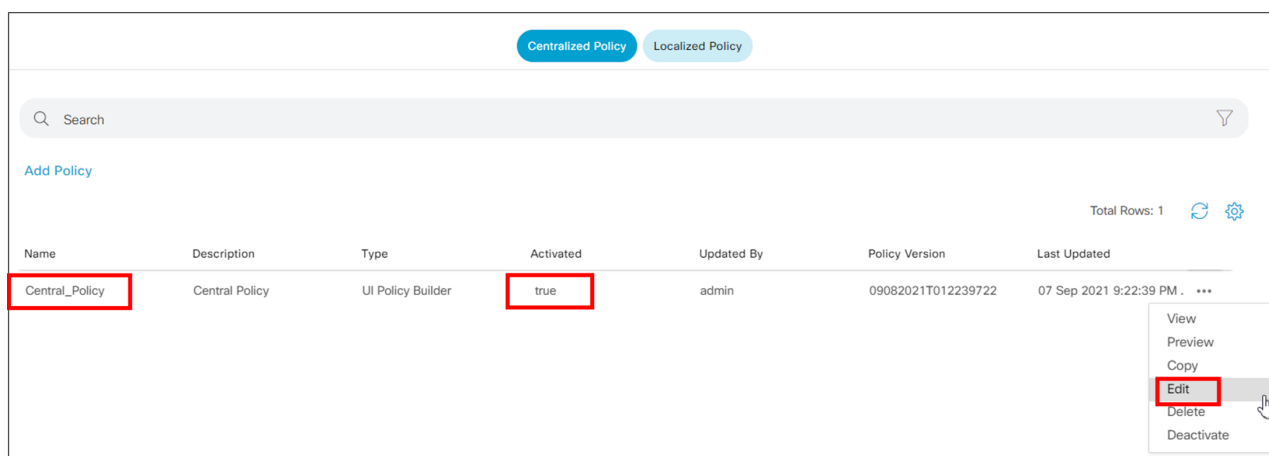
13. (Optional) Change **Default Action** from **Drop** to **Accept** for your policy if necessary.

Tech Tip

In earlier versions of IOS XE SD-WAN code and all versions of vEdge code, there is no fallback support for policy, which means if all the SIG tunnels go down on the router, the data policy still forwards traffic to the SIG service, resulting in traffic blackholing. If you are running earlier versions of code, you can redesign the policy so SIG traffic is routed normally by using an Accept action and then configuring a SIG service route in the service VPN so SIG traffic is directed to the SIG tunnel, which supports fallback routing. If the SIG tunnels fail, the SIG service route is removed so traffic can follow routes in the SD-WAN overlay. Fallback routing for centralized data policy directing traffic to SIG is supported starting in 20.8.1 SD-WAN Manager/17.8.1 IOS XE SD-WAN versions of code.

14. Click **Save Data Policy**.

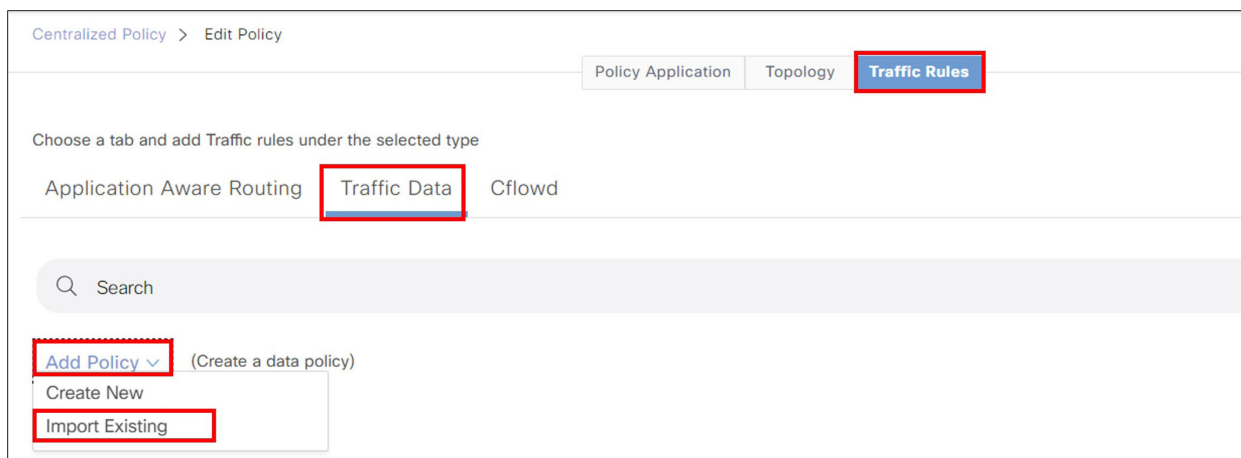
15. Import this new data policy into the master policy already attached to the Cisco SD-WAN Controllers. In the Cisco SD-WAN Manager, go to **Configuration > Policies**. Ensure **Centralized Policy** is selected. Choose to **Edit** the master policy (Central_Policy) that is currently activated.



Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Central_Policy	Central Policy	UI Policy Builder	true	admin	09082021T012239722	07 Sep 2021 9:22:39 PM

Figure 90. Edit policy

16. Click **Traffic Rules** at the top of the page so the new data policy is imported into the master policy. Click the **Traffic Data** tab. Click **Add Policy** and choose **Import Existing** from the drop-down menu.



Centralized Policy > Edit Policy

Policy Application Topology **Traffic Rules**

Choose a tab and add Traffic rules under the selected type

Application Aware Routing **Traffic Data** Cflowd

Search

Add Policy (Create a data policy)

Create New

Import Existing

Figure 91. Traffic data policy

17. In the dialog window, select the policy name created and click **Import**.
18. After the policy is imported, apply it to a site list and VPN list. Click **Policy Application** at the top of the page. Select the **Traffic Data** tab. Under **Sig_Data**, click **New Site List** and **VPN List**.
19. Ensure the radio button **From Service** is selected so data policy is applied to traffic coming from the service VPN. Select **Site list** (Zscaler-DataPolicy-Sites) and **VPN List** (VPN1). Click **Add**, then **Save Policy Changes**. A dialog window appears to push the update policy to the Cisco SD-WAN Controllers.

Figure 92. Policy application

20. Click **Activate**.

Procedure 7: (Optional) Assign Tunnel Weights

In this section, different tunnel weights are assigned to the active tunnels.

1. In the Cisco SD-WAN Manager, go to **Configuration > Templates > Feature Templates**. To the right of the SIG template that was created in the earlier section (xeSig_Zcaler_2_Loopback_Source), click ... and select **Edit** from the drop-down menu.
2. Under the **High Availability** section, configure the **Active Weight** column for each active tunnel.

Section	Parameter	Type	Variable/value
High Availability/Pair-1	Active	Global	ipsec101
	Active Weight	Global	80
High Availability/Pair-2	Active	Global	Ipsec102
	Active Weight	Global	20

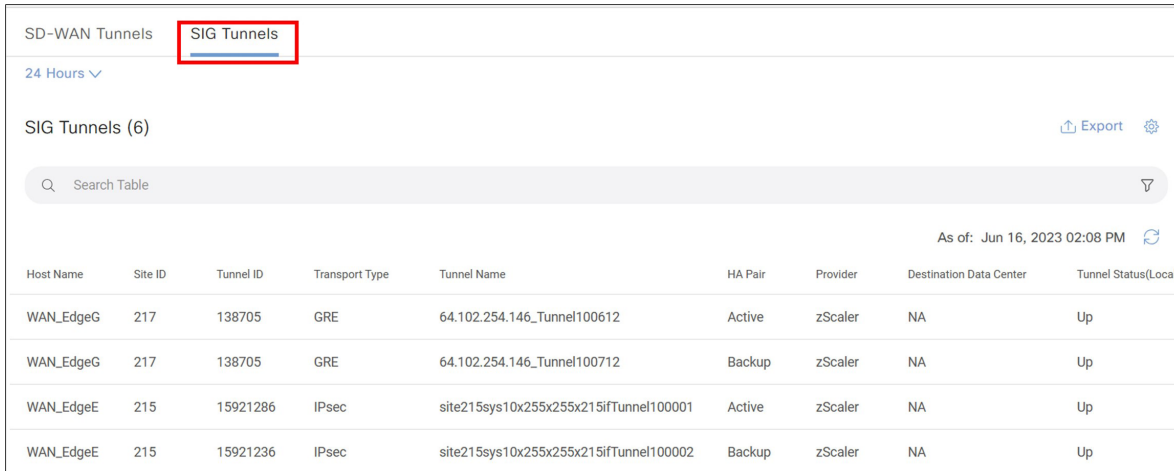
3. Click **Update** to save changes to the SIG feature template.
4. Click **Next**, then **Configure Devices**. You might need to confirm configuration changes on multiple devices. Select the checkbox and click **OK**. The configuration changes are pushed out to the attached WAN Edge routers.

Operate

The following shows different ways to monitor the Zscaler tunnels.

Verify Cisco Catalyst SD-WAN Tunnel Operation from the Cisco SD-WAN Manager

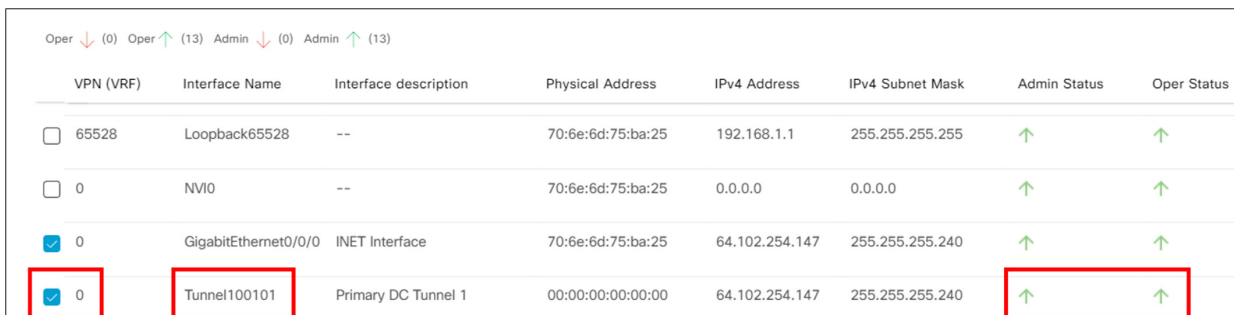
1. In the Cisco SD-WAN Manager under **Monitor** > **Network**, click the **SIG Tunnels** tab to view the tunnel status and any events related to the SIG tunnel.
2. Click the WAN Edge router that you want to verify the tunnel operation on.



Host Name	Site ID	Tunnel ID	Transport Type	Tunnel Name	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)
WAN_EdgeG	217	138705	GRE	64.102.254.146_Tunnel100612	Active	zScaler	NA	Up
WAN_EdgeG	217	138705	GRE	64.102.254.146_Tunnel100712	Backup	zScaler	NA	Up
WAN_EdgeE	215	15921286	IPsec	site215sys10x255x255x215ifTunnel100001	Active	zScaler	NA	Up
WAN_EdgeE	215	15921236	IPsec	site215sys10x255x255x215ifTunnel100002	Backup	zScaler	NA	Up

Figure 93. Interface real time

3. Select **Applications** > **Interface** > **Real Time** at the top right of the chart. You can also click the interface you are interested in on the right-hand side of the chart.
4. If the interface you are interested in is missing from the graph, scroll down past the chart to see the entire list of interfaces. Select the checkbox on the left for the interface you want to display on the chart. You can also view the state and statistics of the various interfaces on the device from this list.



VPN (VRF)	Interface Name	Interface description	Physical Address	IPv4 Address	IPv4 Subnet Mask	Admin Status	Oper Status
<input type="checkbox"/> 65528	Loopback65528	--	70:6e:6d:75:ba:25	192.168.1.1	255.255.255.255	↑	↑
<input type="checkbox"/> 0	NV10	--	70:6e:6d:75:ba:25	0.0.0.0	0.0.0.0	↑	↑
<input checked="" type="checkbox"/> 0	GigabitEthernet0/0/0	INET Interface	70:6e:6d:75:ba:25	64.102.254.147	255.255.255.240	↑	↑
<input checked="" type="checkbox"/> 0	Tunnel100101	Primary DC Tunnel 1	00:00:00:00:00:00	64.102.254.147	255.255.255.240	↑	↑

Figure 94. Interface details

Verify Cisco Catalyst SD-WAN Event Logs from the Cisco SD-WAN Manager

1. In the Cisco SD-WAN Manager, go to **Monitor > Events**.
2. In the top right-side corner, you can select the time frame over which to see the events. The default is over the last three hours.
3. In the search bar, type something to narrow your search. In this example, you see all the WAN_EdgeB device events in the last hour.

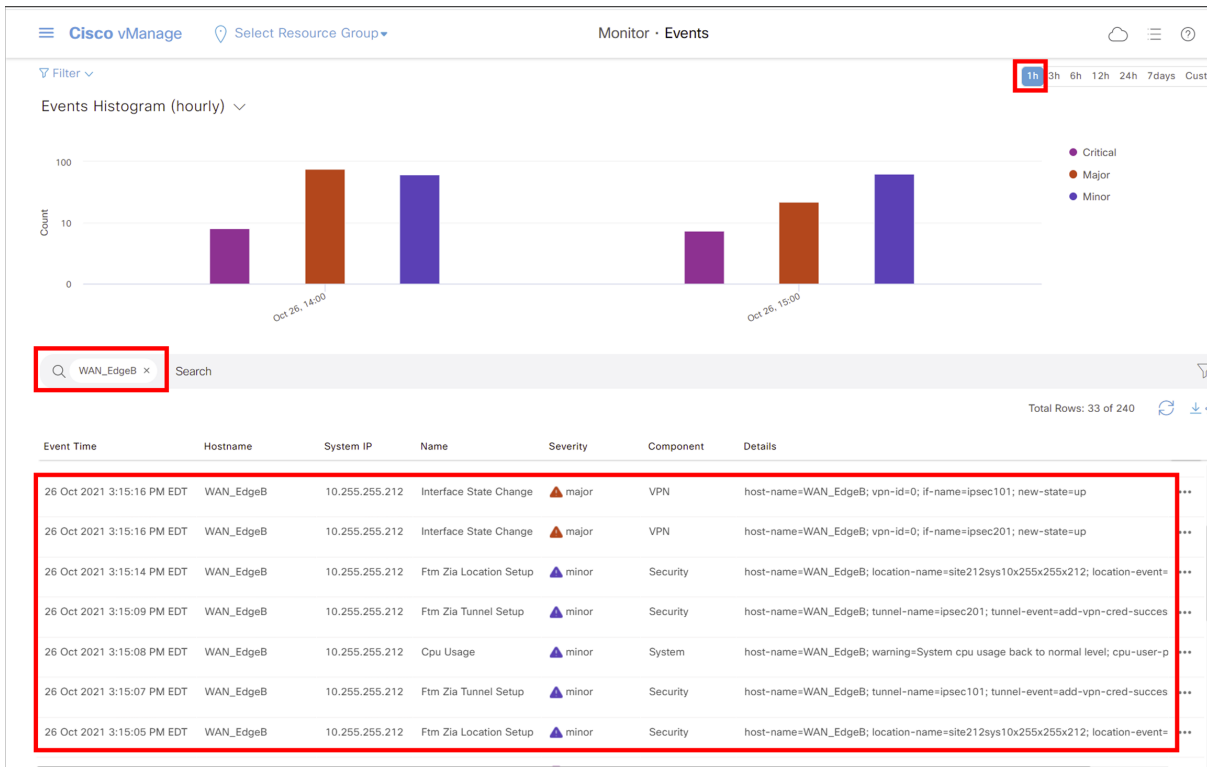


Figure 95. Select resource group

Events are generated when a location is created, when VPN credentials are associated with the tunnel, and when the tunnel state comes up.

Verify Zscaler Tunnel Status in ZIA Admin

If you want to check the status of tunnels to ZIA from your sites, ZIA shows the traffic volume sent/received from your SD-WAN appliances to see the current state of the tunnels via logging.

In the ZIA Admin Portal, go to **Analytics > Insights > Tunnel Insights**.

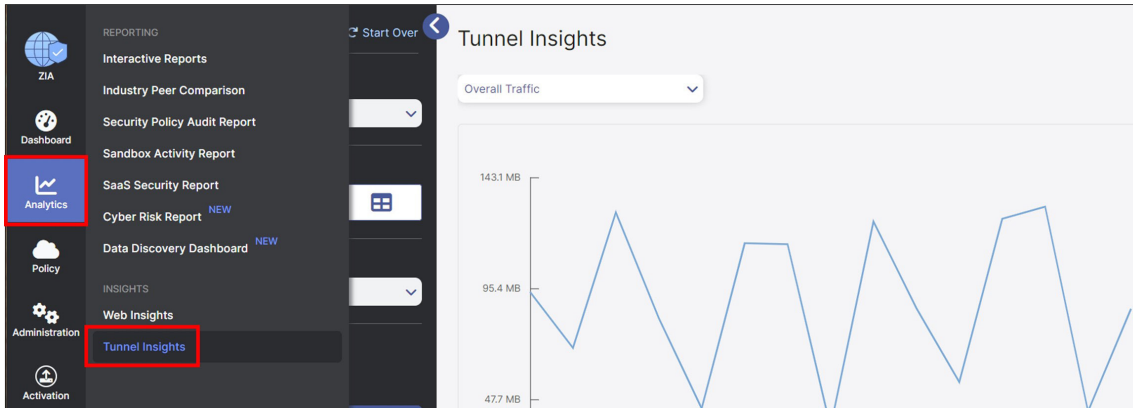


Figure 96. Tunnel insights

On the **Insights** tab, you can visualize and filter data in various ways. You can select how to categorize all tunnel traffic to graph from the drop-down menu under Tunnel Insights (by **Overall Traffic**, **Location**, **Location Group**, **Location Type**, **Tunnel Destination IP**, **Tunnel Source IP**, **Tunnel Type**, or by **VPN Credential**). You can also configure the **Timeframe**, **ChartType**, and **Metrics** you want to view. Additionally, you can filter the data shown in the chart even further by clicking the Add Filter drop-down menu and selecting various filter types and values.

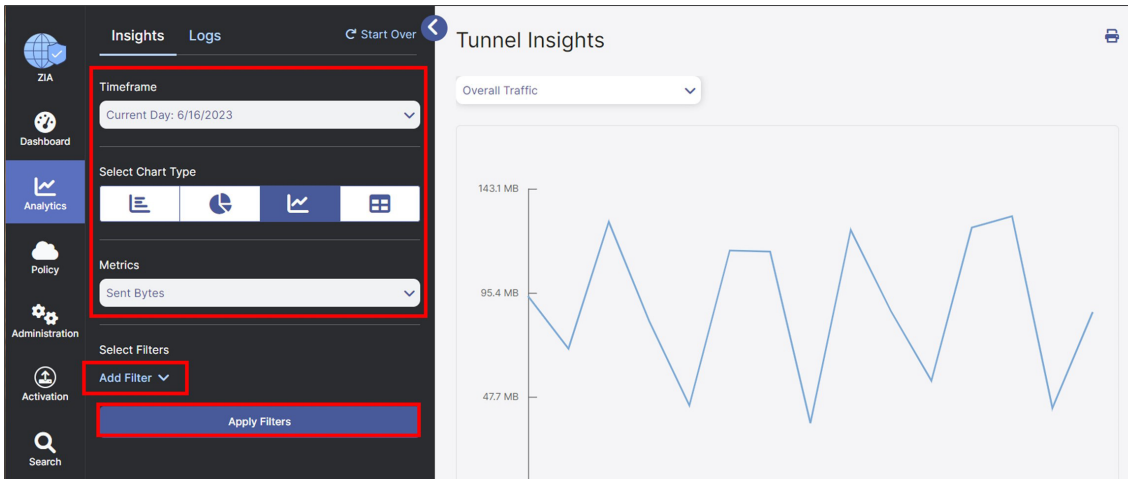


Figure 97. Tunnel insights

To learn more, see [ZIA Tunnel Data Types and Filters](#) (government agencies, see [ZIA Tunnel Data Types and Filters](#)).

Verify Zscaler Tunnel Event Logs in ZIA Admin

Tunnel Logging

To assist in troubleshooting, you can also view the state of all tunnels for your tenant from the ZIA Admin Portal. Click **Logs**. From this tab, you can then filter and change the time frame for the tunnels and sites you would like to investigate.

No...	Event Time	Tunnel Type...	Log Type
1	Friday, June 16, 2023 12:00:00 AM	GRE	Sample
2	Friday, June 16, 2023 12:00:00 AM	IPsec IKEv2	Sample
3	Friday, June 16, 2023 12:00:00 AM	IPsec IKEv2	Sample
4	Friday, June 16, 2023 12:00:00 AM	IPsec IKEv2	Sample
5	Friday, June 16, 2023 12:00:00 AM	IPsec IKEv2	Sample
6	Friday, June 16, 2023 12:00:00 AM	IPsec IKEv2	Sample
7	Friday, June 16, 2023 12:00:00 AM	IPsec IKEv2	Sample

Figure 98. Insights log

For more information, see [ZIA Tunnels Insights Logs: Columns](#) (government agencies, see [ZIA Tunnels Insights Logs: Columns](#)).

View API Calls in Zscaler ZIA (Audit Logs)

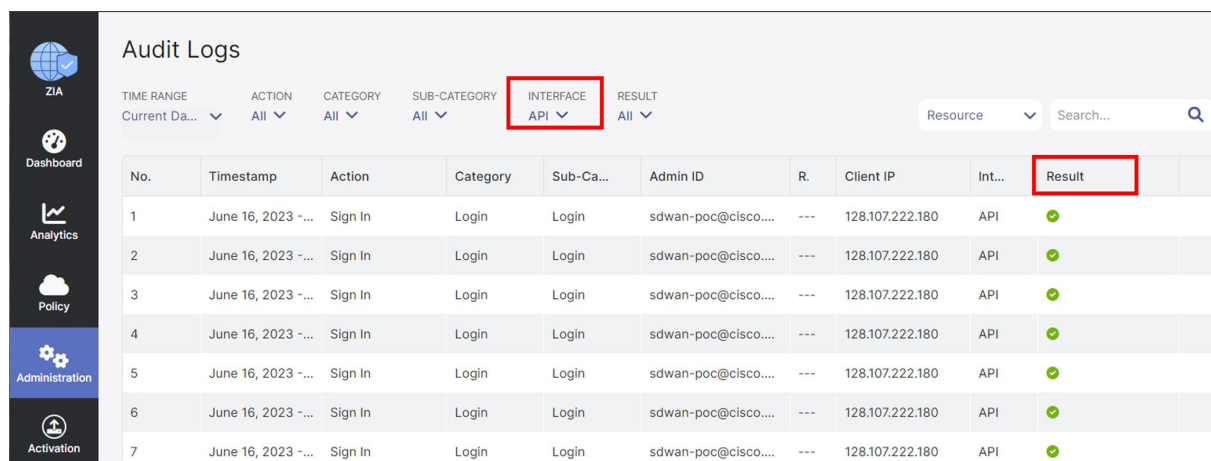
You can view the changes made to the tenant environment using the Audit Logs feature. This also allows you to view API calls into the platform.

1. Go to **Administration > Authentication > Audit Logs**.

Figure 99. Audit logs

2. In the **Audit Logs** window, you can filter out all changes to only view the API calls by selecting **API** under the **Interface** drop-down menu.

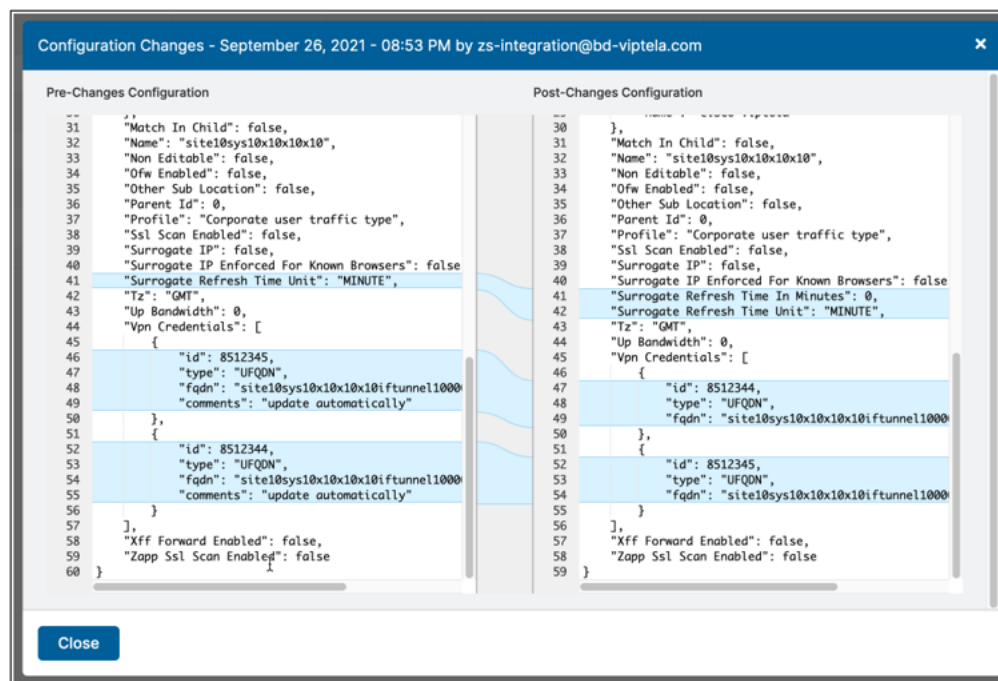
A list of all the API interactions is displayed, where the **Result** column shows whether the call was successful or failed.



No.	Timestamp	Action	Category	Sub-Ca...	Admin ID	R.	Client IP	Int...	Result
1	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓
2	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓
3	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓
4	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓
5	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓
6	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓
7	June 16, 2023 ~...	Sign In	Login	Login	sdwan-poc@cisco....	---	128.107.222.180	API	✓

Figure 100. Audit logs

Click an icon in the **Result** column to see the API data that was created or updated from the call.



Pre-Changes Configuration	Post-Changes Configuration
<pre> 31 "Match In Child": false, 32 "Name": "site10sys10x10x10x10", 33 "Non Editable": false, 34 "Ofw Enabled": false, 35 "Other Sub Location": false, 36 "Parent Id": 0, 37 "Profile": "Corporate user traffic type", 38 "Ssl Scan Enabled": false, 39 "Surrogate IP": false, 40 "Surrogate IP Enforced For Known Browsers": false 41 "Surrogate Refresh Time Unit": "MINUTE", 42 "Tz": "GMT", 43 "Up Bandwidth": 0, 44 "Vpn Credentials": [45 { 46 "id": 8512345, 47 "type": "UFQDN", 48 "fqdn": "site10sys10x10x10x10ftunnel1000", 49 "comments": "update automatically" 50 }, 51 { 52 "id": 8512344, 53 "type": "UFQDN", 54 "fqdn": "site10sys10x10x10x10ftunnel1000", 55 "comments": "update automatically" 56 } 57], 58 "Xff Forward Enabled": false, 59 "Zapp Ssl Scan Enabled": false 60 } </pre>	<pre> 30 }, 31 "Match In Child": false, 32 "Name": "site10sys10x10x10x10", 33 "Non Editable": false, 34 "Ofw Enabled": false, 35 "Other Sub Location": false, 36 "Parent Id": 0, 37 "Profile": "Corporate user traffic type", 38 "Ssl Scan Enabled": false, 39 "Surrogate IP": false, 40 "Surrogate IP Enforced For Known Browsers": false 41 "Surrogate Refresh Time In Minutes": 0, 42 "Surrogate Refresh Time Unit": "MINUTE", 43 "Tz": "GMT", 44 "Up Bandwidth": 0, 45 "Vpn Credentials": [46 { 47 "id": 8512344, 48 "type": "UFQDN", 49 "fqdn": "site10sys10x10x10x10ftunnel1000", 50 }, 51 { 52 "id": 8512345, 53 "type": "UFQDN", 54 "fqdn": "site10sys10x10x10x10ftunnel1000", 55 } 56], 57 "Xff Forward Enabled": false, 58 "Zapp Ssl Scan Enabled": false 59 } </pre>

Figure 101. Configuration changes

Verify Zscaler ZIA Service Configuration

Use the URL <https://ip.zscaler.com> from a host PC at a site to validate if you are transiting ZIA. This is what you see if you are not transiting ZIA:



Figure 102. ZIA transit traffic fail

If you are transiting ZIA, you see the following:



Figure 103. ZIA transit traffic success

Verify Zscaler Tunnel Operation Using Cisco IOS XE SD-WAN CLI

SSH to the WAN Edge router either directly or through the Cisco SD-WAN Manager (Tools > SSH Terminal) and run the following commands to verify the Zscaler tunnel operation using Cisco IOS XE SD-WAN CLI. Note that after the Zscaler API calls are successfully completed, IKEv2 and IPSec phase 2 can establish sessions. When this completes successfully, L7 health checks can start running over the tunnels.

- `show ip interface brief`: Shows interface state.
- `show sdwan secure-internet-gateway zscaler tunnels`: Shows ZIA tunnel information and last API state (only applies to automatic tunnels).
- `show crypto ikev2 session`: Shows crypto Internet Security Association and Key Management Protocol (ISAKMP) (v2) sessions.
- `show crypto ipsec sa`: Shows ipsec encryption/decryption statistics.
- `show ip route vrf <service vpn>`: Shows routing information for the service VPN.
- `show interface <tunnel>`: Shows traffic statistics.
- `show endpoint-tracker`: Shows L7 health tracker information.
- `show endpoint-tracker records`: Shows L7 health tracker information.
- `show ip sla statistics`: Shows L7 health tracker information.

The following are examples of these commands:

```
WAN_EdgeE#sh ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 64.100.215.2 YES other up up
GigabitEthernet0/0/1 10.215.10.1 YES other up up
GigabitEthernet0/0/2 192.168.215.2 YES other up up
Service-Engine0/4/0 unassigned YES unset up up
```

```
GigabitEthernet0 192.168.255.135 YES other up up
Sdwan-system-intf 10.255.255.215 YES unset up up
Loopback65528 192.168.1.1 YES other up up
Loopback65530 10.11.11.1 YES other up up
NVI0 unassigned YES unset up up
Tunnel0 64.100.215.2 YES TFTP up up
Tunnel2 192.168.215.2 YES TFTP up up
Tunnel100101 64.100.215.2 YES TFTP up up
Tunnel100201 64.100.215.2 YES TFTP up up
```

```
WAN_EdgeE#show sdwan secure-internet-gateway zscaler tunnels
```

```
-----
Tunnel100101 site215sys10x255x255x215ifTunnel100101 30556720 <removed> add-vpn-credential-info 30558350 location-init-state get-data centers 200
Tunnel100201 site215sys10x255x255x215ifTunnel100201 30556721 <removed> add-vpn-credential-info 30558350 location-init-state get-data centers 200
```

```
WAN_EdgeE#show crypto ikev2 session
```

```
IPv4 Crypto IKEv2 Session
```

```
Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote fvrf/ivrf Status
```

```
2 64.102.254.147/500 104.129.206.161/500 none/none READY
```

```
Encr:AES-CBC, keysize:256, PRF:SHA256, Hash:SHA256, DH Grp:14, Auth sign:PSK, Auth verify:PSK
```

```
Life/Active Time: 86400/949 sec
```

```
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
```

```
remote selector 0.0.0.0/0 - 255.255.255.255/65535
```

```
ESP spi in/out: 0x99AD50D4/0x3F86E386
```

```
Session-id:5, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote fvrf/ivrf Status
```

```
1 64.102.254.147/500 165.225.8.35/500 none/none READY
```

```
Encr:AES-CBC, keysize:256, PRF:SHA256, Hash:SHA256, DH Grp:14, Auth sign:PSK, Auth verify:PSK
```

```
Life/Active Time: 86400/949 sec
```

```
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
```

```
remote selector 0.0.0.0/0 - 255.255.255.255/65535
```

```
ESP spi in/out: 0x75ABF7D3/0x25E5276B
```



```

WAN_EdgeE#show crypto ipsec sa
interface: Tunnel0
  Crypto map tag: Tunnel0-vesen-head-0, local addr 64.102.254.147
  protected vrf: (none)
  local ident (addr/mask/prot/port): (64.102.254.147/255.255.255.255/0/12387)
  remote ident (addr/mask/prot/port): (64.102.254.146/255.255.255.255/0/12426)
  current_peer 64.102.254.146 port 12426
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 32144, #pkts encrypt: 32144, #pkts digest: 32144
  #pkts decaps: 32144, #pkts decrypt: 32144, #pkts verify: 32144

```

```

WAN_EdgeE#show ip route vrf 1
...
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 [2/65535], Tunnel100101
  10.0.0.0/8 is variably subnetted, 26 subnets, 3 masks
m 10.4.0.0/30 [251/0] via 10.255.255.202, 2d03h, Sdwan-system-intf
  [251/0] via 10.255.255.201, 2d03h, Sdwan-system-intf
m 10.4.0.4/30 [251/0] via 10.255.255.202, 2d03h, Sdwan-system-intf
  [251/0] via 10.255.255.201, 2d03h, Sdwan-system-intf
m 10.4.0.8/30 [251/0] via 10.255.255.202, 2d03h, Sdwan-system-intf
  [251/0] via 10.255.255.201, 2d03h, Sdwan-system-intf

```

```

WAN_EdgeE#show interface Tunnel100101
Tunnel100101 is up, line protocol is up
  Hardware is Tunnel
  Description: Primary DC Tunnel 1
  Interface is unnumbered. Using address of GigabitEthernet0/0/0 (64.100.215.2)
  MTU 9950 bytes, BW 100 Kbit/sec, DLY 50000 usec,
  reliability 255/255, txload 51/255, rxload 5/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 64.100.215.2 (GigabitEthernet0/0/0), destination 165.225.48.10

```

```

WAN_EdgeG#show interface Tunnel100612
Tunnel100612 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of GigabitEthernet0/0/0 (64.102.254.146)

```

```

MTU 9976 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel linestate evaluation up
Tunnel source 64.102.254.146 (GigabitEthernet0/0/0), destination 104.129.194.45
Tunnel Subblocks:
    src-track:
        Tunnel100612 source tracking subblock associated with GigabitEthernet0/0/0
        Set of tunnels with source GigabitEthernet0/0/0, 3 members (includes
iterators)
Tunnel protocol/transport GRE/IP

```

WAN_EdgeE#show endpoint-tracker

Interface	Record Name	Status	RTT in msecs	Probe ID
Next Hop				
Tunnel100101	#SIGL7#AUTO#TRACKER	Up	10	5
None				
Tunnel100201	#SIGL7#AUTO#TRACKER	Up	11	6
None				

WAN_EdgeE#show endpoint-tracker records

Record Name	Endpoint	EndPoint Type	Threshold(ms)	Multiplier	Interval(s)
Tracker-Type					
#SIGL7#AUTO#TRACKER	http://gateway.zscalerthree.net/vpn	API_URL	1000	2	30
interface					

WAN_EdgeE#show ip sla statistics

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

Latest RTT: 32 milliseconds

Latest operation start time: 03:02:28 UTC Wed Nov 24 2021

Latest operation return code: OK

Latest DNS RTT: 10 ms

Latest TCP Connection RTT: 11 ms

Latest HTTP Transaction RTT: 11 ms

Number of successes: 69

Number of failures: 1

Operation time to live: Forever

```

IPSLA operation id: 12
Latest RTT: 37 milliseconds
Latest operation start time: 03:02:28 UTC Wed Nov 24 2021
Latest operation return code: OK
Latest DNS RTT: 11 ms
Latest TCP Connection RTT: 15 ms
Latest HTTP Transaction RTT: 11 ms
Number of successes: 69
Number of failures: 1
Operation time to live: Forever

```

Verify Zscaler Tunnel Operation using Cisco vEdge CLI

SSH to the WAN Edge router either directly or through the Cisco SD-WAN Manager (**Tools > SSH Terminal**) and run the following commands to verify the Zscaler tunnel operation using Cisco vEdge CLI. Note that after the Zscaler API calls are successfully completed, IKEv2 and IPsec phase 2 can establish sessions. When this completes successfully, L7 health checks can start running over the tunnels.

- `show interface | tab | in ipsec`: Shows tunnel state.
- `show secure-internet-gateway zscaler tunnels`: Shows ZIA tunnel information and last API state.
- `show ipsec ike sessions`: Shows crypto ISAKMP (v2) sessions.
- `show tunnel statistics ipsec`: Shows ipsec encryption/decryption statistics.
- `show ip route vpn <service vpn>`: Shows routing information for the service VPN.
- `show ip fib vpn <service vpn>`: Shows next hop information for the service VPN.
- `show ip nat filter` or `show ip nat filter | tab`: Shows active nat translations.
- `show interface statistics`: Shows traffic statistics for each interface.
- `show support tracker interface monitors`: Shows L7 health tracker information.

The following are examples of these commands:

```

WAN_EdgeB# show interface | tab | in ipsec
0 ipsec101 ipv4 - Up Up Up vlan service 1400 00:00:00:00:00:01 1000 full 1316
0:05:32:03 4002 2524
0 ipsec201 ipv4 - Up Up Up vlan service 1400 00:00:00:00:00:01 1000 full 1316
0:05:32:03 4009 2512

```

```

WAN_EdgeB# show secure-internet-gateway zscaler tunnels
zscaler tunnels ipsec101
tunnel-name site212sys10x255x255x212ifipsec101
tunnel-id 33685023
fqdn (REMOVED)
tunnel-fsm-state add-vpn-credential-info

```

```

location-id 33685046
location-fsm-state location-init-state
last-http-req get-data centers
http-resp-code 200
zscaler tunnels ipsec201
tunnel-name site212sys10x255x255x212ifipsec201
tunnel-id 33685030
fqdn (REMOVED)
tunnel-fsm-state add-vpn-credential-info
location-id 33685046
location-fsm-state location-init-state
last-http-req get-data centers
http-resp-code 200

```

```
WAN_EdgeB# show ipsec ike sessions
```

```

ipsec ike sessions 0 ipsec101
  version 2
  source-ip 64.100.212.2
  source-port 4500
  dest-ip 104.129.206.161
  dest-port 4500
  initiator-spi 11e994148c8c114c
  responder-spi ba604f6bfa667181
  cipher-suite aes256-cbc-sha1
  dh-group "2 (MODP-1024)"
  state IKE_UP_IPSEC_UP
  uptime 0:02:17:35
  tunnel-uptime 1:01:16:19
ipsec ike sessions 0 ipsec201
  version 2
  source-ip 64.100.212.2
  source-port 4500
  dest-ip 165.225.34.44
  dest-port 4500
  initiator-spi 0a977da74a8ca235
  responder-spi dc36839e3b9138e4
  cipher-suite aes256-cbc-sha1
  dh-group "2 (MODP-1024)"

```

```
state IKE_UP_IPSEC_UP
uptime 0:02:15:45
tunnel-uptime 1:01:16:19
```

```
WAN_EdgeB# show tunnel statistics ipsec
```

```
IPSEC IPSEC RX IPSEC IPSEC TX
TUNNEL SOURCE DEST DECRYPT AUTH IPSEC RX ENCRYPT AUTH IPSEC TX
PROTOCOL SOURCE IP DEST IP PORT PORT IN FAIL FAIL OUT FAIL FAIL
```

```
-----
ipsec 64.100.212.2 64.100.1.23 12346 10424 370572 1 0 370570 0 8
ipsec 64.100.212.2 64.100.1.24 12346 65008 370594 1 0 370593 0 7
ipsec 64.100.212.2 104.129.206.161 4500 4500 15168 0 0 18970 0 0
ipsec 64.100.212.2 165.225.34.44 4500 4500 15176 0 0 18977 0 0
```

```
WAN_EdgeB# show ip route vpn 1
```

```
PROTOCOL NEXTHOP NEXTHOP NEXTHOP
VPN PREFIX PROTOCOL SUB TYPE IF NAME ADDR VPN TLOC IP COLOR ENCAP STATUS
```

```
-----
1 0.0.0.0/0 std-ipsec - ipsec101 - 0 - - - F,S
1 0.0.0.0/0 omp - - - - 10.255.255.201 mpls ipsec -
```

```
WAN_EdgeB# show ip fib vpn 1
```

```
NEXTHOP NEXTHOP NEXTHOP NEXTHOP SA
VPN PREFIX IF NAME ADDR LABEL VPN INDEX TLOC IP COLOR
```

```
-----
1 0.0.0.0/0 ipsec 165.225.48.10 - - 34 - -
1 10.4.0.0/30 ipsec 10.4.1.2 1003 - 7 10.255.255.201 mpls
1 10.4.0.0/30 ipsec 64.100.1.23 1003 - 28 10.255.255.201 biz-internet
```

```
WAN_EdgeB# show ip nat filter (or show ip nat filter | tab)
```

```
ip nat filter nat-vpn 0 nat-ifname ge0/0 vpn 0 protocol udp 64.100.212.2 64.102.254.147
public-source-address 64.100.212.2
public-dest-address 64.102.254.147
public-source-port 12346
public-dest-port 12367
filter-state established
idle-timeout 0:00:00:59
outbound-packets 3296
```

```

outbound-octets 519226
inbound-packets 3294
inbound-octets 593424
ip nat filter nat-vpn 0 nat-ifname ge0/2 vpn 0 protocol udp 10.10.10.1 104.129.206.161
public-source-address 192.168.212.2
public-dest-address 104.129.206.161
public-source-port 4500
public-dest-port 4500
filter-state established
idle-timeout 0:00:00:52
outbound-packets 15105
outbound-octets 1851428
inbound-packets 15077
inbound-octets 1846978

```

WAN_EdgeB# show interface statistics

```
AF RX RX RX RX TX TX TX TX RX RX TX TX
```

```
VPN INTERFACE TYPE PACKETS OCTETS ERRORS DROPS PACKETS OCTETS ERRORS DROPS PPS Kbps PPS
Kbps
```

```

0 ge0/0 ipv4 423562 70604112 0 213 437205 74796702 0 0 17 22 17 23
0 ipsec101 ipv4 4333 536138 0 0 2731 340154 0 0 0 0 0 0
0 ipsec201 ipv4 4336 536532 0 0 2717 337982 0 0 0 0 0 0

```

WAN_EdgeB# show support tracker interface monitors

```
Interface: ipsec101/#SIGL7#AUTO#TRA#ZIA
```

```
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec101
```

```
Monitor state : UP (flapped 0 times)
```

```
Ref count : 1
```

```
Monitor type : httping
```

```
Probe / DNS SIP : 192.168.0.2 / ::
```

```
Nameserver IP : 208.67.222.222
```

```
Src Port Base : 49172
```

```
Num of probes : 1
```

```
Max Re-transmit : 2
```

```
First Probe : 0 secs
```

```
Probe interval : 30 secs
```

```
Probe timeout : 1000 msecs
```

```
DNS TTL : 96 secs
```

DNS query/ok/fail : 611/611/0

Peer: 165.225.48.11 (UP - flapped 0 times, nretries 0)

Total requests : 0 Total responses : 0

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 : 0.00/0.00/0.00 ms

Conn min/avg/max: 0.00/0.00/0.00 ms

Interface: ipsec201/#SIGL7#AUTO#TRA#ZIA

Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec201

Monitor state : UP (flapped 0 times)

Ref count : 1

Monitor type : httping

Probe / DNS SIP : 192.168.0.2 / ::

Nameserver IP : 208.67.222.222

Src Port Base : 49173

Num of probes : 1

Max Re-transmit : 2

First Probe : 0 secs

Probe interval : 30 secs

Probe timeout : 1000 msecs

DNS TTL : 96 secs

DNS query/ok/fail : 611/611/0

Peer: 165.225.48.11 (UP - flapped 0 times, nretries 0)

Total requests : 0 Total responses : 0

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 : 0.00/0.00/0.00 ms

Conn min/avg/max: 0.00/0.00/0.00 ms

Appendix A: Cisco Branch Base Feature Templates and Configuration Values Used

This appendix shows the branch non-default base device and feature template configurations used and referenced in this guide. Zscaler tunnel configurations in the main body of this guide are built on top of these configurations. For step-by-step instructions on configuring device and feature templates, see the [Cisco SD-WAN End-to-End Deployment Guide](#).

Feature Templates

You can apply these branch base configuration feature templates to Cisco vEdge or Cisco IOS XE SD-WAN routers. However, you must define them for Cisco vEdge devices or Cisco IOS XE SD-WAN devices and not both. From Cisco SD-WAN Manager version 20.1 and later, feature templates cannot apply to both Cisco vEdge and Cisco IOS XE SD-WAN devices—they must have separate feature templates. Each of the following template names are preceded by either v or Cisco vEdge_ if the device type is a Cisco vEdge device, or an xe or xeEdge_ if the device type is a Cisco IOS XE SD-WAN device.

When creating feature templates for Cisco vEdge routers, if you want to cover the most models possible when selecting devices, select all ISR 1100 models with Cisco Viptela, and all Cisco vEdge devices (all Cisco vEdge 100 types, Cisco vEdge 1000, Cisco vEdge 2000, Cisco vEdge 5000, and Cisco vEdge Cloud).

When creating feature templates for Cisco IOS XE SD-WAN routers, if you want to cover the most models possible when selecting devices, select all models except the ISR 1100 models with Cisco Viptela, all Cisco vEdge devices, CG (Cellular Gateway) devices, Cisco SD-WAN Manager, and Cisco SD-WAN Controller devices. When creating SIG feature templates, you must also exclude the IR104s and IR8340 from the device model list.

AAA feature template (Cisco IOS XE SD-WAN)

Template: Basic Information/Cisco AAA

Template Name: xeAAA

Description: AAA Template for WAN Edge Routers

Section	Parameter	Type	Variable/Value
Local	Username	Global	netadmin
	Password	Global	(hidden)
	Privilege Level	Global	15

AAA feature template (Cisco vEdge)

Template: Basic Information/AAA

Template Name: vAAA

Description: AAA Template for WAN Edge Routers

Section	Parameter	Type	Variable/Value
Local/New User	Name	Global	netadmin
	Password	Global	(hidden)
	User Groups	Global	netadmin

NTP Feature Template

Template: Basic Information/Cisco NTP

Template Name: NTP

Description: NTP Template for WAN Edge Routers

Section	Parameter	Type	Variable/Value
Server	Hostname/IP address	Global	time.google.com
	Source Interface	Device Specific	ntp_server_source_int

Branch VPNO Feature Template

Template: VPN/VPN

Template Name: BR_VPNO

Description: VPN O Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	VPN	Global	0
	Name	Global	Transport VPN
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	208.67.222.222
	Secondary DNS Address	Global	208.67.220.220
	Hostname	Global	vbond.cisco.net
	List of IP Addresses	Global	64.100.100.113
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio Button	Next Hop
	Next Hop	Device Specific	vpn0_next_hop_ip_addr_inet
	Next Hop	Device Specific	vpn0_next_hop_ip_addr_mpls

Branch Internet Interface Feature Template (Cisco IOS XE SD-WAN)

Template: VPN/VPN Interface Ethernet

Template Name: xeBR_VPNO_INET

Description: VPN O INET Interface Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Device Specific	vpn0_inet_shutdown
	Interface Name	Device Specific	vpn0_inet_int_name
	Description	Global	INET Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn0_inet_ipv4_addr
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Tunnel>Allow Service	NTP	Global	On
NAT	NAT	Global	On
	NAT Type	Global	Interface

Branch Internet Interface Feature Template (Cisco vEdge)

Template: VPN/VPN Interface Ethernet

Template Name: vBR_VPNO_INET

Description: VPN 0 INET Interface Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Device Specific	vpn0_inet_shutdown
	Interface Name		Device Specific
	Description	Global	INET Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn0_inet_ipv4_addr
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Tunnel>Allow Service	NTP	Global	On
NAT	NAT	Global	On

Branch MPLS Interface Feature Template

Template: VPN/VPN Interface Ethernet

Template Name: BR_VPNO_MPLS

Description: VPN 0 MPLS Interface Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Device Specific	vpn0_mpls_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_name
	Description	Global	MPLS Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn0_mpls_ipv4_addr
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
Allow Service	NTP	Global	On

Branch VPN512 Interface Feature Template

Template: VPN/VPN Interface Ethernet

Template Name: VPN512_MGT_INT

Description: VPN 512 Management Interface Template for WAN Edge Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_int_name
	Description	Global	MGT Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn512_int_ipv4_addr

Branch VPN 1 Feature Template

Template: VPN/VPN

Template Name: BR_VPN1

Description: VPN 1 Template for the WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	VPN	Global	1
	Name	Global	LAN

Branch VPN1 Interface Feature Template

Template: VPN/VPN Interface Ethernet

Template Name: BR_VPN1_LAN_INT1

Description: VPN 1 LAN Interface Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Device Specific	vpn1_int1_shutdown
	Interface Name	Device Specific	vpn1_int1_name
	Description	Device Specific	vpn1_int1_description
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn1_int1_ipv4_addr

Device Templates

The following device templates are used in this guide. The table indicates what non-default feature template is used.

Single WAN Edge Router Sites (Cisco IOS XE SD-WAN)

Device Model: ISR4331 [E], C8300-1N1S-6T [G]

Template Name: xeEdge_Remote_[E,G]

Description: WAN Edge router remote site [E,G]

Template Type	Template Subtype	Template Name
Basic Information	Cisco NTP	xeNTP
	Cisco AAA	xeAAA
VPN 0	Cisco VPN	xeBR_VPN0
	Cisco VPN Interface	xeBR_VPN0_INET
	Cisco VPN Interface	xeBR_VPN0_MPLS
VPN 512	Cisco VPN Interface	xeVPN512_MGT_INT
VPN 1	Cisco VPN1	xeBR_VPN1
	Cisco VPN Interface	xeBR_VPN1_LAN_INT1

Single WAN Edge Router Sites (Cisco vEdge)

Device Model: Cisco vEdge-100b [A], ISR1100-4G [B]

Template Name: Cisco vEdge_Remote_[A,B]

Description: WAN Edge router remote site [A,B]

Template Type	Template Subtype	Template Name
Basic Information	Cisco NTP	vNTP
	Cisco AAA	vAAA
VPN 0	VPN	vBR_VPN0
	VPN Interface	vBR_VPN0_INET
	VPN Interface	vBR_VPN0_MPLS
VPN 512	VPN Interface	vVPN512_MGT_INT
VPN 1	VPN1	vBR_VPN1
	VPN Interface	vBR_VPN1_LAN_INT1

Device Variable Values

Variable	Cisco vEdge_RemoteA	Cisco vEdge_RemoteB	Cisco vEdge_RemoteE	Cisco vEdge_RemoteG
Hostname	WAN_EdgeA	WAN_EdgeB	WAN_EdgeE	WAN_EdgeG
System IP	10.255.255.211	10.255.255.212	10.255.255.215	10.255.255.217
Site ID	211	212	215	217
Interface Name (vpn1_int1_name)	ge0/0	ge0/3	GigabitEthernet0/0/0	GigabitEthernet0/0/0
Description (vpn1_int1_description)	LAN Interface	LAN Interface	LAN Interface	LAN Interface
IPv4 Address (vpn1_int1_ipv4_addr)	10.211.10.1/24	10.212.10.1/24	10.215.10.1/24	10.217.10.1/24
Shutdown (vpn1_int1_shutdown)	False	False	False	False
Interface Name(vpn512_int_name)	ge0/1	ge0/1	GigabitEthernet0	GigabitEthernet0
IPv4 Address(vpn512_int_ipv4_addr)	192.168.255.153/23	192.168.255.181/23	192.168.255.135/23	192.168.255.93/23
Address(vpn0_next_hop_ip_addr_inet)	64.102.254.151	64.100.212.1	64.102.254.151	64.100.217.1
Address(vpn0_next_hop_ip_addr_mpls)	192.168.211.1	192.168.212.1	192.168.215.1	192.168.217.1
Interface Name(vpn0_mpls_int_name)	ge0/2	ge0/2	GigabitEthernet0/0/2	GigabitEthernet0/0/2
IPv4 Address(vpn0_mpls_ipv4_addr)	192.168.211.2/30	192.168.212.2/30	192.168.215.2/30	192.168.217.2/30

Variable	Cisco vEdge_RemoteA	Cisco vEdge_RemoteB	Cisco vEdge_RemoteE	Cisco vEdge_RemoteG
Shutdown (vpn0_mpls_shutdown)	False	False	False	False
Interface Name(vpn0_inet_int_name)	ge0/4	ge0/0	GigabitEthernet0/0/0	GigabitEthernet0/0/0
IPv4 Address(vpn0_inet_ipv4_addr)	64.102.254.146/28	64.100.212.2/28	64.102.254.147/28	64.100.217.2/28
Shutdown (vpn0_inet_shutdown)	False	False	False	False
Source Interface (ntp_server_source_int)	ge0/4	ge0/0	GigabitEthernet0/0/0	GigabitEthernet0/0/0

Appendix B: Tunnel Configuration Summary (Feature and Device Templates)

For Cisco tunnel configuration, observe the following prerequisites.

Prerequisites

- Verify that NAT is enabled on the internet interface that is used to access Zscaler.
- Verify that a primary and secondary DNS server is defined in the VPN O feature template.
- Verify NTP is enabled, synced, and the clock is correct.

Cisco VPN Interface Ethernet Feature Template

Template: VPN/VPN Interface Ethernet

Template Name: xeBR_VPNO_INET

Description: VPNO INET Interface Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
NAT	NAT	Global	On
	NAT Type	Global	Interface

Cisco VPN Feature Template

Template: VPN/Cisco VPN

Template Name: xeBR_VPNO

Description: VPNO Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
DNS	Primary DNS Address (IPv4)	Global	208.67.222.222
	Secondary DNS Address (IPv4)	Global	208.67.220.220

Cisco VPN Feature Template

Template: Basic Information/Cisco NTP

Template Name: xeNTP

Description: NTP Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Server	Hostname/IP address	Global	time.google.com
	Source Interface	Device Specific	ntp_server_source_int

SIG Credential Information from ZIA

Section	Parameter	Type	Variable/Value
Organization	Administration > Company Profile > Organization	Domains	ciscotest.net (example)
Partner Base URI	Administration > Authentication > Cloud Service API Security > Cloud Service API Key	Base URL for your API	zsapi.zscalerbeta.net/api/v1 (example)
Username	Administration > Administration Controls > Administrator Management > Administrators	Partner Admin Login ID	sd-wan@ciscotest.net (example)
Password	Administration > Administration Controls > Administrator Management > Administrators	Partner Admin Password	(hidden)
Partner API Key	Administration > Settings > Cloud Configuration > Partner Integrations > SD-WAN	Partner Name (Cisco SD-WAN or Cisco Viptela) Key	ABCdef123GHI (example)

Cisco SIG Credentials Feature Template

Template: Other Templates/Cisco SIG Credentials

Template Name: xeSig_Credentials

Description: Cisco IOS XE Sig Credentials Template

Section	Parameter	Type	Variable/Value
Basic Details	SIG Provider	Radio Button	Zscaler
	Organization	Global	ciscotest.net (example)
	Partner Base URI	Global	zsapi.zscalerbeta.net/api/v1 (example)
	Username	Global	sd-wan@ciscotest.net (example)
	Password	Global	(hidden)
	Partner API Key	Global	ABCdef123GHI (example)

Example 1: Active/Standby Tunnels

- Create a Cisco SIG feature template (IPSec or GRE).
- Add Cisco SIG feature Template and SIG Credential feature template (if needed) to the Device Template.

Cisco SIG Feature Template (GRE)

Template: VPN/Cisco SIG

Template Name: xeSig_Zscaler

Description: IOS XE Sig Zscaler Template

Section	Parameter	Type	Variable/Value
Tracker (Beta)	SIG Provider	Radio Button	Zscaler
	Source IP Address	Device Specific	vpn_trackersrcip
Configuration			
Tunnel Name (gre101)	Interface Name	Global	gre101
	Description	Global	Primary DC Tunnel 1
	Tunnel Source Interface	Device Specific	pri_tunnel1_src_int
	Data-Center	Radio Button	Primary
	Source Public IP	Device Specific	pri_tunnel1_src_public_ip
Tunnel Name (gre201)	Interface Name	Global	ipsec201
	Description	Global	Secondary DC Tunnel 1
	Tunnel Source Interface	Device Specific	sec_tunnel1_src_int
	Data-Center	Radio Button	Secondary
	Source Public IP	Device Specific	sec_tunnel1_src_public_ip
High Availability/Pair-1	Active	Global	gre101
	Backup	Global	gre201

Cisco SIG Feature Template (IPSec)

Template: VPN/Cisco SIG

Template Name: xeSig_Zscaler

Description: Cisco IOS XE Sig Zscaler Template

Section	Parameter	Type	Variable/Value
Tracker (Beta)	SIG Provider	Radio Button	Zscaler
	Source IP Address	Device Specific	vpn_trackersrcip
Tunnel Name (ipsec101)	Interface Name	Global	ipsec101
	Description	Global	Primary DC Tunnel 1
	Tunnel Source Interface	Device Specific	pri_tunnel1_src_int
	Data-Center	Radio Button	Primary
Tunnel Name (ipsec201)	Interface Name	Global	ipsec201
	Description	Global	Secondary DC Tunnel 1
	Tunnel Source Interface	Device Specific	sec_tunnel1_src_int
	Data-Center	Radio Button	Secondary
High Availability/Pair-1	Active	Global	ipsec101
	Backup	Global	ipsec201

Device Template

Template Type	Template Subtype	Template Name
Basic Information	Cisco NTP	xeNTP
	Cisco AAA	xeAAA
VPN 0	Cisco VPN	xeBR_VPN0
	Cisco SIG	xeSig_Zscaler
	Cisco VPN Interface	xeBR_VPN0_INET
	Cisco VPN Interface	xeBR_VPN0_MPLS
VPN 512	Cisco VPN Interface	xeVPN512_MGT_INT
VPN 1	Cisco VPN1	xeBR_VPN1
	Cisco VPN Interface	xeBR_VPN1_LAN_INT1
Additional Templates (20.9 and later)	Cisco SIG Credentials*	Cisco-Zscaler-Global-Credentials (automatic)
Additional Templates (prior to 20.9)	Cisco SIG Credentials*	xeSig_Credentials

Example 2: Active/Active Tunnels (Cisco IOS XE SD-WAN Only)

- Create loopback interfaces to use as tunnel sources.
- Create a local policy-based routing policy via CLI add-on template.
- Create a Cisco SIG Feature Template (GRE or IPSec)
- Add loopback interface feature templates, CLI add-on template, Cisco SIG feature Template, and SIG Credential feature template (if needed) to the Device Template.

Cisco VPN Interface Ethernet Feature Template

Template: VPN/Cisco VPN Interface Ethernet

Template Name: xeLoopback1

Description: Loopback 1 Tunnel Source

Note

For GRE, loopback interfaces must be publicly addressed, or translated with One-to-One NAT on an external device (device-specific parameters can be used instead for loopback IP address and variable can be defined before applying the device template).

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	Loopback1
	IPv4	Radio Button	Static
	IPv4 Address/prefix-length	Global	10.10.10.1/32

Cisco VPN Interface Ethernet Feature Template

Template: VPN/Cisco VPN Interface Ethernet

Template Name: xeLoopback2

Description: Loopback 2 Tunnel Source

Note

For GRE, you must publicly address loopback interfaces, or translate them with One-to-One NAT on an external device (you can use and define device-specific parameters for loopback IP address and variables instead applying the device template).

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	Loopback2
	IPv4	Radio Button	Static
	IPv4 Address/prefix-length	Global	10.10.10.2/32

Cisco CLI Add-On Feature Template

Template: Other Templates/CLI Add-On Template

Template Name: CLI-Template

Description: CLI Add-On Template

```
ip cef load-sharing algorithm src-only
ip access-list extended SIG
  10 permit ip host 10.10.10.1 any
  20 permit ip host 10.10.10.2 any
!
route-map Tunnel-Control permit 10
  match ip address SIG
  set ip next-hop {{Loopback-Tun-Src-Next-Hop-IP}}
!
ip local policy route-map Tunnel-Control
```

Cisco SIG Feature Template (GRE)

Template: VPN/Cisco SIG

Template Name: xeSig_Zscaler_2_Loopback_Source

Description: Cisco IOS XE Sig Zscaler with 2 Active Active Tunnels Template

Section	Parameter	Type	Variable/Value
Configuration (gre101)	SIG Provider	Radio Button	Zscaler
	Interface Name	Global	gre101
	Description	Global	Primary DC Tunnel 1
	Tunnel Source Interface	Device Specific	pri_tunnel1_src_int
	Data-Center	Radio Button	Primary
	Source Public IP	Device Specific	pri_tunnel1_src_public_ip

Configuration (gre102)	Interface Name	Global	gre102
	Description	Global	Primary DC Tunnel 2
	Tunnel Source Interface	Device Specific	pri_tunnel2_src_int
	Data-Center	Radio Button	Primary
High Availability/Pair-1	Source Public IP	Device Specific	pri_tunnel2_src_public_ip
	Active	Global	gre101
High Availability/Pair-2	Backup	Global	None
	Active	Global	Gre102
	Backup	Global	None

Cisco SIG Feature Template (IPSec)

Template: VPN/Cisco SIG

Template Name: xeSig_Zscaler_2_Loopback_Source

Description: Cisco IOS XE Sig Zscaler with 2 Active Active Tunnels Template

Section	Parameter	Type	Variable/Value
Configuration (ipsec101)	SIG Provider	Radio Button	Zscaler
	Interface Name	Global	ipsec101
	Description	Global	Tunnel 1 to Primary DC
	Tunnel Source Interface	Global	Loopback1
Configuration (ipsec102)	Data-Center	Radio Button	Primary
	Tunnel Route-via Interface	Device Specific	pri_tunnel1_route_via
	Interface Name	Global	Ipsec102
	Description	Global	Tunnel 2 to Primary DC
High Availability/Pair-1	Tunnel Source Interface	Global	Loopback2
	Data-Center	Radio Button	Primary
	Tunnel Route-via Interface	Device Specific	pri_tunnel2_route_via
	Active	Global	ipsec101
High Availability/Pair-2	Backup	Global	None
	Active	Global	Ipsec102
	Backup	Global	None

Device Template

Template Type	Template Subtype	Template Name
Basic Information	Cisco NTP	xeNTP
	Cisco AAA	xeAAA
VPN 0	Cisco VPN	xeBR_VPN0
	Cisco SIG	xeSig_Zscaler_2_Loopback_Source
	Cisco VPN Interface	xeBR_VPN0_INET
	Cisco VPN Interface	xeBR_VPN0_MPLS
	Cisco VPN Interface	xeLoopback1
	Cisco VPN Interface	xeLoopback2
VPN 512	Cisco VPN Interface	xeVPN512_MGT_INT
VPN 1	Cisco VPN1	xeBR_VPN1
	Cisco VPN Interface	xeBR_VPN1_LAN_INT1
Additional Templates	CLI Add-On Template	CLI-Template-Sig-Local-Policy
Additional Templates (20.9 and above)	Cisco SIG Credentials*	Cisco-Zscaler-Global-Credentials (automatic)
Additional Templates (prior to 20.9)	Cisco SIG Credentials*	xeSig_Credentials

Traffic Redirection

Service Route

Branch VPN1 Feature Template

Template: VPN/VPN Interface Ethernet

Template Name: xeBR_VPN1

Description: VPN 1 Template for WAN Edge Branch Routers

Section	Parameter	Type	Variable/Value
Service Route	Prefix	Global	0.0.0.0/0
	Service	Default	SIG

Centralized Policy

Configuration > Policies > Custom Options > Centralized Policy > Lists

List Type	Name	Entries
Data Prefix	Overlay	10.0.0.0/8
Application	Box	Application/Box
Site	Zscaler-DataPolicy-Sites	212,214,215, 217
VPN	VPN1	1

Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > Traffic Data

Sequence Type (Custom)

Sequence Rule	Match Parameter	Match Value	Action/s
1	Destination Data Prefix	Overlay	Accept
2	DNS	Request	Accept/NAT VPN with Fallback
3	Application/Application Family List	Box	Accept/NAT VPN with Fallback
4	<empty>		Accept/Secure Internet Gateway with Fallback

Go to **Configuration > Policies > Centralized Policy** and **Edit** the master policy that is currently activated on the Cisco SD-WAN Controllers.

Under **Traffic Rules > Traffic Data**, import the newly-created data policy.

Under **Policy Application > Traffic Data**, choose radio button **From Service**, and add **Site List** Zscaler-DataPolicy-Sites and **VPN List** VPN1.

Miscellaneous

In the following section, the Cisco SIG feature template is modified.

Customize Health Tracker

Section	Parameter	Type	Variable/Value
Section	Parameter	Type	Variable/value
Service Route	Prefix	Global	0.0.0.0/0
	Service	Default	SIG

Enable Advanced Zscaler Features

Section	Parameter	Type	Variable/Value
Advanced Settings	Enable Caution	Global	On

Customize Zscaler Tunnel Destinations (Primary and Secondary DCs)

Section	Parameter	Type	Variable/Value
Advanced Settings	Primary Data-Center	Device Specific	vpn_zlsprimarydc
	Secondary Data-Center	Device Specific	vpn_zlssecondarydc

Assign Tunnel Weights (Use with Active/Active Tunnels)

Section	Parameter	Type	Variable/Value
High Availability/Pair-1	Active	Global	ipsec101
	Active Weight	Global	80
	Backup	Global	None
High Availability/Pair-2	Active	Global	Ipsec102
	Active Weight	Global	20
	Backup	Global	None

Appendix C: Cisco IOS XE SD-WAN CLI Configuration

This section demonstrates the CLI configuration to interoperate with Zscaler. These are equivalent to the feature and device templates shown earlier. Note that the recommended way to configure Cisco Catalyst SD-WAN devices is through feature and device templates from Cisco SD-WAN Manager.

To complete the CLI configuration, configure:

- Base connectivity
- Prerequisites
- Common tunnel components
- Use case example 1 or 2 (active/standby or active/active tunnel definitions)
- Traffic redirection (service SIG route, service DIG data policy, or both)
- Miscellaneous (optional features)

Base Connectivity

The following is a basic connectivity configuration for the Cisco IOS XE SD-WAN router. It includes one other transport (MPLS), which is not essential to the connectivity to Zscaler (except for internet access across the SD-WAN overlay to the data center in case the local internet fails). Some default configurations have been removed. These configurations correspond to feature and device templates shown in [Appendix B: Tunnel Configuration Summary \(Feature and Device Templates\)](#).

```
system
system-ip 10.255.255.215
site-id 215
organization-name "ENB-Solutions - 216151"
vbond vbond.cisco.net port 12346
!
hostname WAN_EdgeE
vrf definition 1
description LAN
rd 1:1
address-family ipv4
route-target export 1:1
route-target import 1:1
exit-address-family
!
address-family ipv6
exit-address-family
!
!
ip host vbond.cisco.net 64.100.100.113
```

```
ip name-server 208.67.220.220 208.67.222.222
ip route 0.0.0.0 0.0.0.0 64.102.254.151
ip route 0.0.0.0 0.0.0.0 192.168.215.1
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0
overload
!
interface GigabitEthernet0
  description MGT Interface
  no shutdown
  vrf forwarding Mgmt-intf
  ip address 192.168.255.135 255.255.254.0
exit
interface GigabitEthernet0/0/0
  description INET Interface
  no shutdown
  ip address 64.102.254.147 255.255.255.240
exit
interface GigabitEthernet0/0/1
  description LAN Interface
  no shutdown
  vrf forwarding 1
  ip address 10.215.10.1 255.255.255.0
exit
interface GigabitEthernet0/0/2
  description MPLS Interface
  no shutdown
  ip address 192.168.215.2 255.255.255.252
exit
interface Tunnel0
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/0/0
  no ipv6 redirects
  tunnel source GigabitEthernet0/0/0
  tunnel mode sdwan
exit
interface Tunnel2
```



```
no shutdown
ip unnumbered GigabitEthernet0/0/2
no ip redirects
ipv6 unnumbered GigabitEthernet0/0/2
no ipv6 redirects
tunnel source GigabitEthernet0/0/2
tunnel mode sdwan
exit
!
ntp server time.google.com source GigabitEthernet0/0/0 version 4
ntp source GigabitEthernet0/0/0
!
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec weight 1
color biz-internet
no allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
interface GigabitEthernet0/0/2
tunnel-interface
encapsulation ipsec weight 1
color mpls restrict
no allow-service all
no allow-service bgp
```

```

allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit

```

Prerequisites

The base configuration enables NTP to ensure an accurate clock and DNS. Enable NAT under the internet transport.

```

interface GigabitEthernet0/0/0
ip nat outside

```

Common Tunnel Components

The following are common tunnel components between the two use cases.

SIG Credentials

```

secure-internet-gateway
zscaler organization ciscotest.net
zscaler partner-base-uri zsapi.zscalerthree.net/api/v1
zscaler partner-key ABCdef123GHI
zscaler username sd-wan@ciscotest.net
zscaler password (REMOVED)

```

IPSec and IKEv2 Configuration

```

crypto ikev2 policy policy1-global
proposal p1-global
!
crypto ikev2 profile if-ipsec101-ikev2-profile
no config-exchange request
dpd 10 3 on-demand
dynamic
lifetime 86400

```

```

!
crypto ikev2 profile if-ipsec201-ikev2-profile
  no config-exchange request
  dpd 10 3 on-demand
  dynamic
  lifetime 86400
!
crypto ikev2 proposal p1-global
  encryption aes-cbc-128 aes-cbc-256
  group 14 15 16
  integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set if-ipsec101-ikev2-transform esp-null esp-sha-hmac
  mode tunnel
!
crypto ipsec transform-set if-ipsec201-ikev2-transform esp-null esp-sha-hmac
  mode tunnel
!
crypto ipsec profile if-ipsec101-ipsec-profile
  set ikev2-profile if-ipsec101-ikev2-profile
  set transform-set if-ipsec101-ikev2-transform
  set security-association lifetime kilobytes disable
  set security-association lifetime seconds 3600
  set security-association replay window-size 512
!
crypto ipsec profile if-ipsec201-ipsec-profile
  set ikev2-profile if-ipsec201-ikev2-profile
  set transform-set if-ipsec201-ikev2-transform
  set security-association lifetime kilobytes disable
  set security-association lifetime seconds 3600
  set security-association replay window-size 512

```

Zscaler Location Settings

```
sdwan
service sig vrf global
zscaler-location-settings
auth-required false
xff-forward-enabled false
surrogate ip false
surrogate idle-time 0
surrogate display-time-unit MINUTE
surrogate ip-enforced-for-known-browsers false
surrogate refresh-time 0
surrogate refresh-time-unit MINUTE
ofw-enabled false
ips-control false
aup disabled
aup block-internet-until-accepted true
aup force-ssl-inspection false
aup timeout 0
caution-enabled false
```

L7 Health Check Configuration

```
vrf definition 65530
address-family ipv4
exit-address-family
!
interface Loopback65530
no shutdown
vrf forwarding 65530
ip address 10.11.11.1 255.255.255.255
exit
ip sdwan route vrf 65528 10.0.0.1/32 service sig
```

Use Case Example 1: Active/Standby Tunnels

IPSec Tunnels Defined

```
interface Tunnel100101
  description Primary DC Tunnel 1
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip clear-dont-fragment
  ip mtu 1400
  tunnel source GigabitEthernet0/0/0
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec101-ipsec-profile
  tunnel vrf multiplexing
exit
interface Tunnel100201
  description Secondary DC Tunnel 1
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip clear-dont-fragment
  ip mtu 1400
  tunnel source GigabitEthernet0/0/0
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec201-ipsec-profile
  tunnel vrf multiplexing
exit
```

GRE Tunnels Defined

```
interface Tunnel100612
  ip unnumbered GigabitEthernet0/0/0
  ip mtu 1400
  tunnel source GigabitEthernet0/0/0
  tunnel destination dynamic
  tunnel route-via GigabitEthernet0/0/0 mandatory
  tunnel vrf multiplexing
!
interface Tunnel100712
  ip unnumbered GigabitEthernet0/0/0
```

```

ip mtu 1400
tunnel source GigabitEthernet0/0/0
tunnel destination dynamic
tunnel route-via GigabitEthernet0/0/0 mandatory
tunnel vrf multiplexing

```

Zscaler Tunnel Options

```

sdwan
interface Tunnel100101
tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference
primary-dc source-interface GigabitEthernet0/0/0
exit
interface Tunnel100201
tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference
secondary-dc source-interface GigabitEthernet0/0/0

```

Service SIG Interface Pairs HA Pair Configuration

```

sdwan
service sig vrf global
ha-pairs
interface-pair Tunnel100101 active-interface-weight 1 Tunnel100201
backup-interface-weight 1

```

Use Case Example 2: Active/Active Tunnels

Tunnel Source Loopbacks Defined

```

interface Loopback1
ip address 10.10.10.1 255.255.255.255
!
interface Loopback2
ip address 10.10.10.2 255.255.255.255

```

Local Policy Route (for ISAKMP control traffic)

```

ip cef load-sharing algorithm src-only
ip access-list extended SIG
10 permit ip host 10.10.10.1 any
20 permit ip host 10.10.10.2 any
route-map Tunnel-Control permit 10
set ip next-hop 64.102.254.151
match ip address SIG
ip local policy route-map Tunnel-Control

```

IPSec Tunnels Defined

```
interface Tunnel100101
  description Tunnel 1 to Primary DC
  no shutdown
  ip unnumbered Loopback1
  no ip clear-dont-fragment
  ip mtu 1400
  tunnel source Loopback1
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec101-ipsec-profile
  tunnel vrf multiplexing
  tunnel route-via GigabitEthernet0/0/0 mandatory
exit
interface Tunnel100201
  description Tunnel 2 to Primary DC
  no shutdown
  ip unnumbered Loopback2
  no ip clear-dont-fragment
  ip mtu 1400
  tunnel source Loopback2
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec201-ipsec-profile
  tunnel vrf multiplexing
  tunnel route-via GigabitEthernet0/0/0 mandatory
```

Zscaler Tunnel Options

```
sdwan
interface Tunnel100101
  tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference
  primary-dc source-interface Loopback1
  exit
interface Tunnel100201
  tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference
  primary-dc source-interface Loopback2
  exit
```

Service SIG Interface Pairs HA Pair Configuration

```
sdwan
  service sig vrf global
ha-pairs
  interface-pair Tunnel100101 active-interface-weight 1 None backup-interface-weight 1
  interface-pair Tunnel100201 active-interface-weight 1 None backup-interface-weight 1
```

Traffic Redirection

Service SIG Route

```
ip sdwan route vrf 1 0.0.0.0/0 service sig
```

Service SIG Data Policy (apply to Cisco SD-WAN Controller)

```
viptela-policy:policy
  data-policy _VPN1_Sig_Data
  vpn-list VPN1
  sequence 1
  match
    destination-data-prefix-list Overlay
  !
  action accept
  !
  !
sequence 11
  match
  dns request
  source-ip 0.0.0.0/0
  !
  action accept
  nat use-vpn 0
```



```
nat fallback
!
!
sequence 21
match
app-list Box
source-ip 0.0.0.0/0
!
action accept
nat use-vpn 0
nat fallback
!
!
sequence 31
match
destination-data-prefix-list Default
!
action accept
sig
sig-action fallback-to-routing
default-action drop
!
!
default-action drop
!
lists
app-list Box
app box
app box_net
!
data-prefix-list Default
ip-prefix 0.0.0.0/0
!
data-prefix-list Overlay
ip-prefix 10.0.0.0/8
!
site-list Zscaler-DataPolicy-Sites
site-id 214
```

```

site-id 215
!
vpn-list VPN1
vpn 1
!
!
!
apply-policy
  site-list Zscaler-DataPolicy-Sites
  data-policy _VPN1_Sig_Data from-service
!
!

```

Miscellaneous

Customize Health Tracker

```

endpoint-tracker zscaler_l7_health_check
  endpoint-api-url http://gateway.zscalerthree.net/vpntest
  tracker-type interface
  interval 20

interface Tunnel100101
  endpoint-tracker zscaler_l7_health_check
exit
interface Tunnel100201
  endpoint-tracker zscaler_l7_health_check
exit

```

Enable Advanced Zscaler Features

```

sdwan
  service sig vrf global
  zscaler-location-settings
  caution-enabled true

```

Customize Zscaler Tunnel Destinations (Primary and Secondary DCs)

```

sdwan
  service sig vrf global
  zscaler-location-settings
  data centers primary-data-center atl2-vpn.zscalerthree.net
  data centers secondary-data-center dfw1-vpn.zscalerthree.net

```

Customize Zscaler GRE Tunnel Destinations (Primary and Secondary DCs)

```
sdwan
service sig vrf global
zscaler-location-settings
datacenters primary-data-center 165.225.72.38
datacenters secondary-data-center 104.129.194.38
```

Assign Tunnel Weights (Use with Active/Active Tunnels)

```
sdwan
service sig vrf global
ha-pairs
interface-pair Tunnel100101 active-interface-weight 80 None backup-interface-weight 1
interface-pair Tunnel100201 active-interface-weight 20 None backup-interface-weight 1
```

Appendix D: Cisco vEdge CLI Configuration

This section demonstrates the CLI configuration to interoperate with Zscaler. These are equivalent to the feature and device templates shown earlier. Note that the recommended way to configure Cisco Catalyst SD-WAN devices is through feature and device templates from Cisco SD-WAN Manager.

To complete the CLI configuration, configure:

- Base connectivity
- Prerequisites
- Use case example 1 (active/standby tunnel definitions)
- Traffic redirection (service SIG route, service SIG data policy, or both)
- Miscellaneous (optional features)

Base Connectivity

The following is a basic connectivity configuration for the Cisco vEdge router. It includes one other transport (MPLS), which is not essential to the connectivity to Zscaler (except for internet access across the SD-WAN overlay to the data center in case the local internet fails). Some default configurations have been removed. These configurations correspond to feature and device templates shown in [Appendix B: Tunnel Configuration Summary \(Feature and Device Templates\)](#).

```
system
host-name WAN_EdgeB
system-ip 10.255.255.212
site-id 212
organization-name "ENB-Solutions - 216151"
vbond vbond.cisco.net
!
ntp
server time.google.com
source-interface ge0/0
exit
!
!
vpn 0
name "Transport VPN"
dns 208.67.220.220 secondary
dns 208.67.222.222 primary
ecmp-hash-key layer4
host vbond.cisco.net ip 64.100.100.113
interface ge0/0
ip address 64.100.212.2/28
nat
```

```
!  
tunnel-interface  
encapsulation ipsec  
color biz-internet  
no allow-service bgp  
allow-service dhcp  
allow-service dns  
allow-service icmp  
no allow-service sshd  
no allow-service netconf  
allow-service ntp  
no allow-service ospf  
no allow-service stun  
allow-service https  
!  
no shutdown  
!  
interface ge0/2  
ip address 192.168.212.2/30  
tunnel-interface  
encapsulation ipsec  
color mpls restrict  
no allow-service bgp  
allow-service dhcp  
allow-service dns  
allow-service icmp  
no allow-service sshd  
no allow-service netconf  
allow-service ntp  
no allow-service ospf  
no allow-service stun  
allow-service https  
!  
no shutdown  
!  
ip route 0.0.0.0/0 64.100.212.1  
ip route 0.0.0.0/0 192.168.212.1  
!
```

```

vpn 1
  name LAN
  interface ge0/3
  ip address 10.212.10.1/24
  no shutdown
  !
!
vpn 512
  name "Transport VPN"
  interface ge0/1
  ip address 192.168.255.181/23
  no shutdown
  !
!

```

Prerequisites

The base configuration enables NTP to ensure an accurate clock and DNS. Enable NAT under the internet transport.

```

vpn 0
  interface ge0/0
  nat

```

Use Case Example 1: Active/Standby Tunnels

IPSec Tunnels Defined

```

vpn 0
  interface ipsec101
  description "Primary DC Tunnel 1"
  ip unnumbered
  tunnel-source-interface ge0/0
  tunnel-destination dynamic
  tunnel-set secure-internet-gateway-zscaler
  tunnel-dc-preference primary-dc
  ike
  version 2
  rekey 14400
  cipher-suite aes256-cbc-sha1
  group 2
  authentication-type
  pre-shared-key-dynamic

```

```
!  
!  
ipsec  
rekey 3600  
replay-window 512  
cipher-suite null-sha1  
perfect-forward-secrecy none  
!  
mtu 1400  
no shutdown  
!  
interface ipsec201  
description "Secondary DC Tunnel 1"  
ip unnumbered  
tunnel-source-interface ge0/0  
tunnel-destination dynamic  
tunnel-set secure-internet-gateway-zscaler  
tunnel-dc-preference secondary-dc  
ike  
version 2  
rekey 14400  
cipher-suite aes256-cbc-sha1  
group 2  
authentication-type  
pre-shared-key-dynamic  
!  
!  
ipsec  
rekey 3600  
replay-window 512  
cipher-suite null-sha1  
perfect-forward-secrecy none  
!  
mtu 1400  
no shutdown  
!
```

Service SIG Interface Pairs HA Pair Configuration

```
vpn 0
  name "Transport VPN"
  dns 208.67.220.220 secondary
  dns 208.67.222.222 primary
  ecmp-hash-key layer4
  host vbond.cisco.net ip 64.100.100.113
  service sig
  ha-pairs interface-pair ipsec101 active-interface-weight 1 ipsec201
  backup-interface-weight 1
  exit
exit
```

SIG Credentials

```
secure-internet-gateway
  zscaler organization ciscotest.net
  zscaler partner-base-uri zsapi.zscalerthree.net/api/v1
  zscaler partner-key ABCdef123GHI
  zscaler username sd-wan@ciscotest.net
  zscaler password <hidden>
```

Traffic Redirection

Service SIG Route

```
vpn 1
  ip service-route 0.0.0.0/0 vpn 0 service sig
```

Service SIG Data Policy (apply to Cisco SD-WAN Controller)

```
viptela-policy:policy
  data-policy _VPN1_Sig_Data
  vpn-list VPN1
  sequence 1
  match
  destination-data-prefix-list Overlay
  !
  action accept
  !
  !
  sequence 11
  match
```



```
dns request
source-ip 0.0.0.0/0
!
action accept
nat use-vpn 0
nat fallback
!
!
sequence 31
    match
        source-ip 0.0.0.0/0
        action accept
!
action accept
nat use-vpn 0
nat fallback
!
!
sequence 31
match
source-ip 0.0.0.0/0
!
action accept
sig
!
!
default-action drop
!
lists
app-list Box
app box
app box_net
!
data-prefix-list Overlay
ip-prefix 10.0.0.0/8
!
site-list Zscaler-DataPolicy-Sites
site-id 212
```

```

site-id 214
site-id 215
!
vpn-list VPN1
vpn 1
!
!
!
apply-policy
  site-list Zscaler-DataPolicy-Sites
  data-policy _VPN1_Sig_Data from-service
!
!

```

Miscellaneous

Customize Health Tracker

```

vpn0
  tracker SIG zscaler_17_health_check
  endpoint-api-url http://gateway.zscalerthree.net/vpntest
  interval 20
interface ipsec101
  tracker zscaler_17_health_check
interface ipsec201
  tracker Zscaler_17_health_check

```

Enable Advanced Zscaler Features

```

vpn 0
  service sig
  zscaler-location-settings caution-enabled true

```

Customize Zscaler IPSec Tunnel Destinations (Primary and Secondary DCs)

```

vpn 0
  service sig
  zscaler-location-settings data centers primary-data-center atl2-vpn.zscalerthree.net
  zscaler-location-settings data centers secondary-data-center dfw1-vpn.zscalerthree.net

```

Appendix E: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration > Settings > Company Profile**.

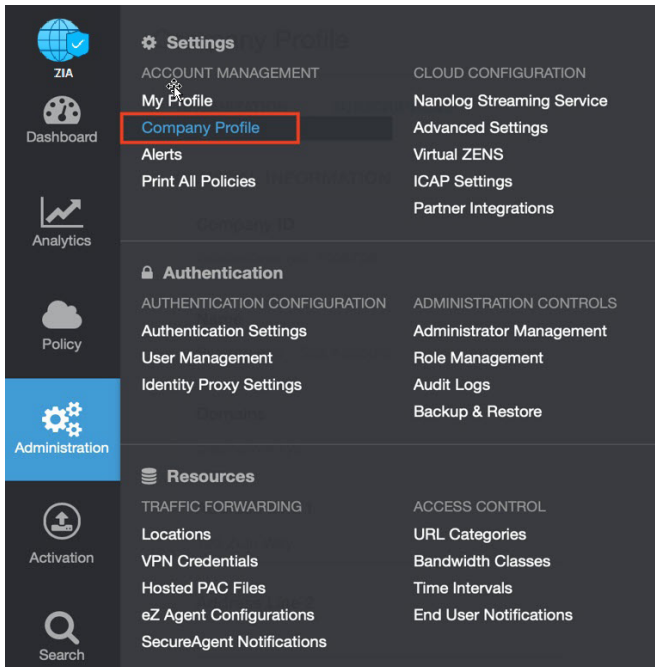


Figure 104. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID.

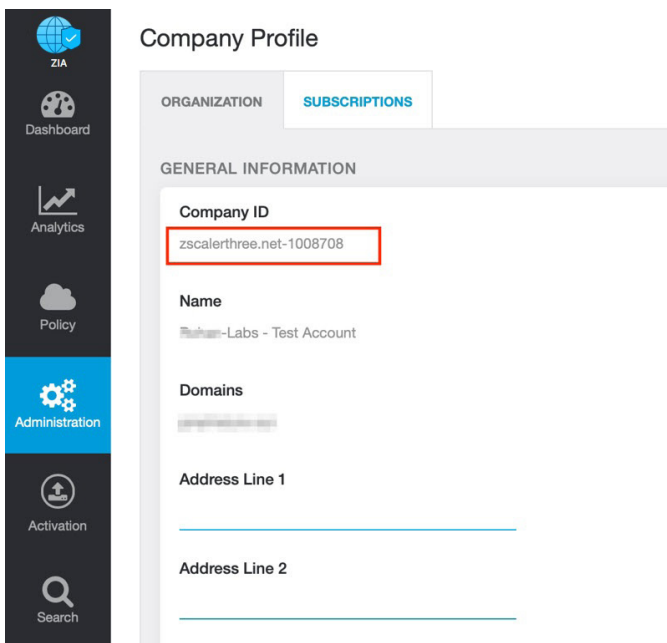


Figure 105. Company ID

3. Now that you have your company ID, you can open a support ticket. Go to **Dashboard > Support > Submit a Ticket**.

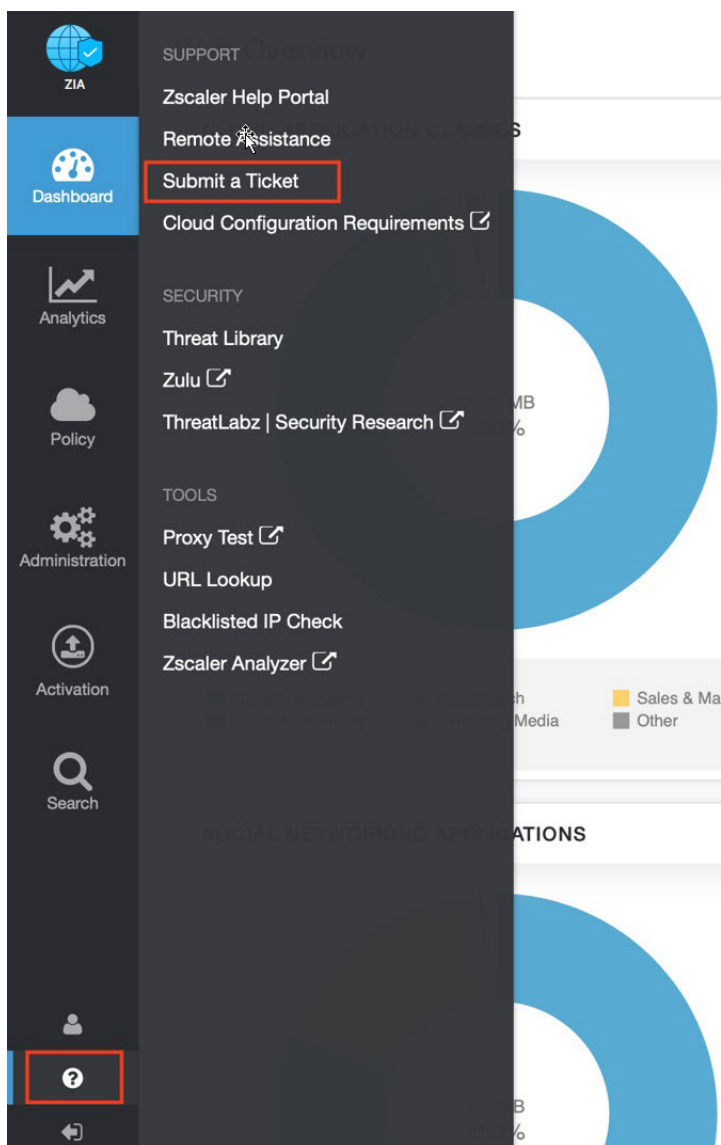


Figure 106. Submit a ticket

Appendix F: Document Revision Control

Revision	Date	Change Log
1.0	August 2017	Initial document by Zscaler and Cisco Viptela.
1.1	August 2017	Updated Viptela references to Cisco SD-WAN.
1.2	September 2017	Minor edits.
1.3	September 2018	Updated ZIA screen captures to ZIA 5.6 and added IPsec section and other supporting edits.
2.0	March 2019	Added GRE and IPsec template creation.
3.0	January 2020	Cisco SD-WAN: Updated for 19.2.099 and 19.3.0 Cisco SD-WAN Manager code, added Cisco IOS XE SD-WAN router information, added design information, added L7 health checking, and tested the ISR1100-4G running Cisco vEdge code.
3.1	February 2020	Incorporated review feedback.
4.0	September 2020	Cisco SD-WAN: Updated for 20.3.4 Cisco SD-WAN Manager and Cisco vEdge code and 17.3.4a Cisco IOS XE SD-WAN Edge code (manual GRE and IPsec tunnels). Updated ZIA screen captures for ZIA 6.1 and added instructions for GRE tunnel provisioning through ZIA.
5.0	November 2021	Cisco SD-WAN: Updated for 20.6 vManage and vEdge code and 17.6 IOS XE SD-WAN Edge code, added new information on vManage SIG templates, IPsec auto tunnels (active/standby and active/active tunnels), SIG service routes, and data policy.
5.1	December 2021	Updated formatting and edited for style.
5.2	May 2023	Cisco SD-WAN: Updated for 20.9 vManage and vEdge code and 17.9 IOS XE SD-WAN Edge code, added new information on GRE auto tunnels, Cisco SD-WAN and Zscaler design, and other features supported since 20.6 vManage/17.6 IOS XE SD-WAN code versions. Due to product rebranding, updated Cisco SD-WAN references to Cisco Catalyst SD-WAN, and updated vManage, vSmart, and vBond references to SD-WAN Manager, Controller, and Validator.