Cisco Catalyst SD-WAN and Microsoft's Secure Service Edge (SSE) Solution Integration User Guide

September 2024

Contents

Introduction

Cisco and Microsoft's Secure Service Edge (SSE) solution have collaborated to enhance the security of customer branch internet traffic through efficient redirection. The integration of Cisco Catalyst® SD-WAN with Microsoft's SSE solution facilitates inspection of north-south traffic originating from SD-WAN branches destined for the internet or Software-as-a-Service (SaaS) applications routed through Microsoft's SSE solution.

This guide details the process of securing Cisco Catalyst SD-WAN sites using Microsoft's SSE solution specifically for internet and SaaS applications. The integration has undergone extensive testing and validation for deployment on Cisco IOS® XE SD-WAN routers running software versions 17.12 or 20.12, in conjunction with the Microsoft's SSE solution cloud dashboard. A key customer benefit is the seamless deployment of a comprehensive end-to-end SD-WAN and security solution.

Microsoft Entra Internet Access and Microsoft Entra Private Access are integral components of Microsoft's SSE solution. Microsoft Entra Internet Access ensures secure access to internet and SaaS apps, providing robust protection for users, devices, and data against internet-borne threats. This document focuses on the Internet Access use case.

Overview of configuration steps

Step 1. Create remote networks using the Microsoft Entra Admin Center.

Step 2. Establish connectivity—Configure an IPsec tunnel in Cisco Catalyst SD-WAN Manager using a SIG parcel.

Step 3. Redirect traffic—Configure data policy for application-based traffic redirected from branch edge devices.

Step 4. Validate the configuration.

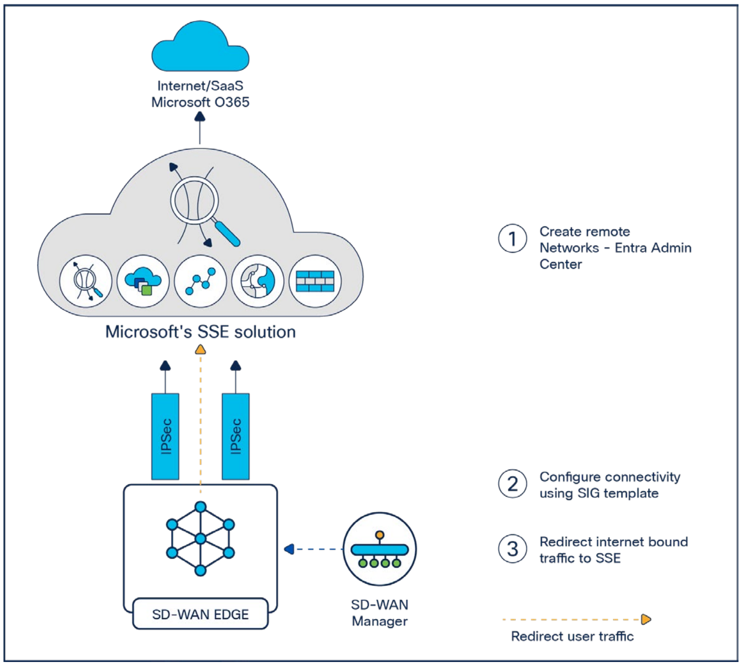

Internet/SaaS
Microsoft O365
Microsoft's SSE solution
IPSec
IPSec
SD-WAN EDGE
SD-WAN
Manager
1 Create remote Networks - Entra Admin Center
2 Configure connectivity using SIG template
3 Redirect internet bound traffic to SSE
Redirect user traffic

Figure 1.
Integration between Catalyst SD-WAN and Microsoft's SSE solution

Detailed steps

Step 1. Create remote networks using the Microsoft Entra Admin Center

Remote networks enable administrators to define and configure remote network locations, including names, regions, and bandwidth capacity, and add one or more Customer Premises Equipment (CPE) links to a given remote network.

Overview

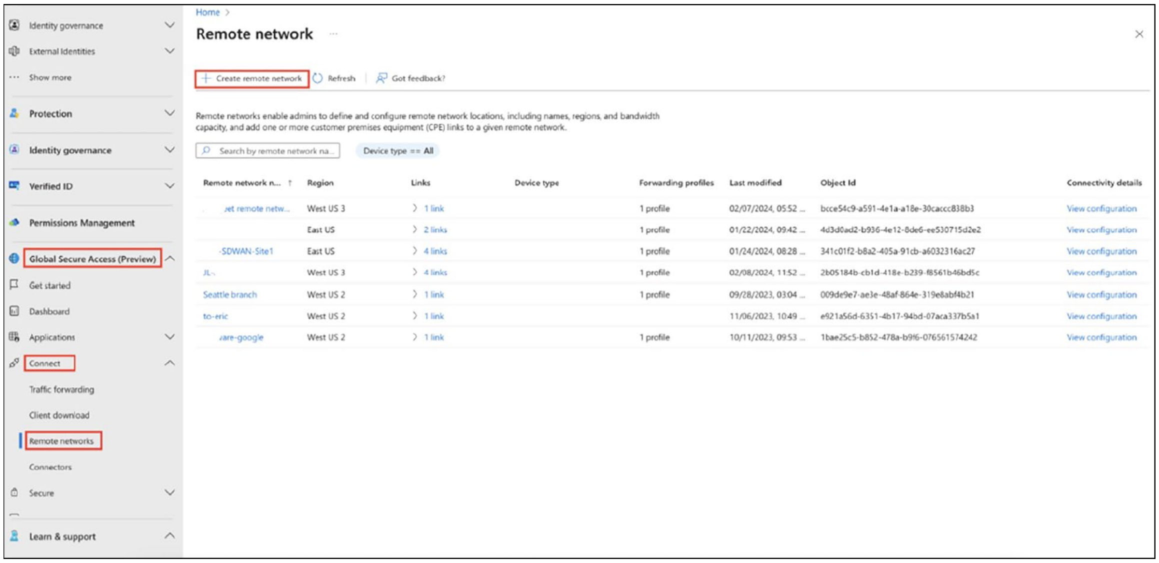
- Create two different remote networks in two different regions. For each remote network, create two links. Each of these links will be used for active/backup tunnel configuration when designing High Availability (HA) pairs on CPE.

  Reference: How to create a remote network with Global Secure Access (preview) –Global Secure Access | Microsoft Learn

- For each link definition, fill in the basic link details, IPsec-related security attributes, and IKEv2 values.

Workflow

1. On the Microsoft Entra Admin Center homepage, select Global Secure Access (preview) > Connect > Remote Networks, and click the Create Remote Network button.

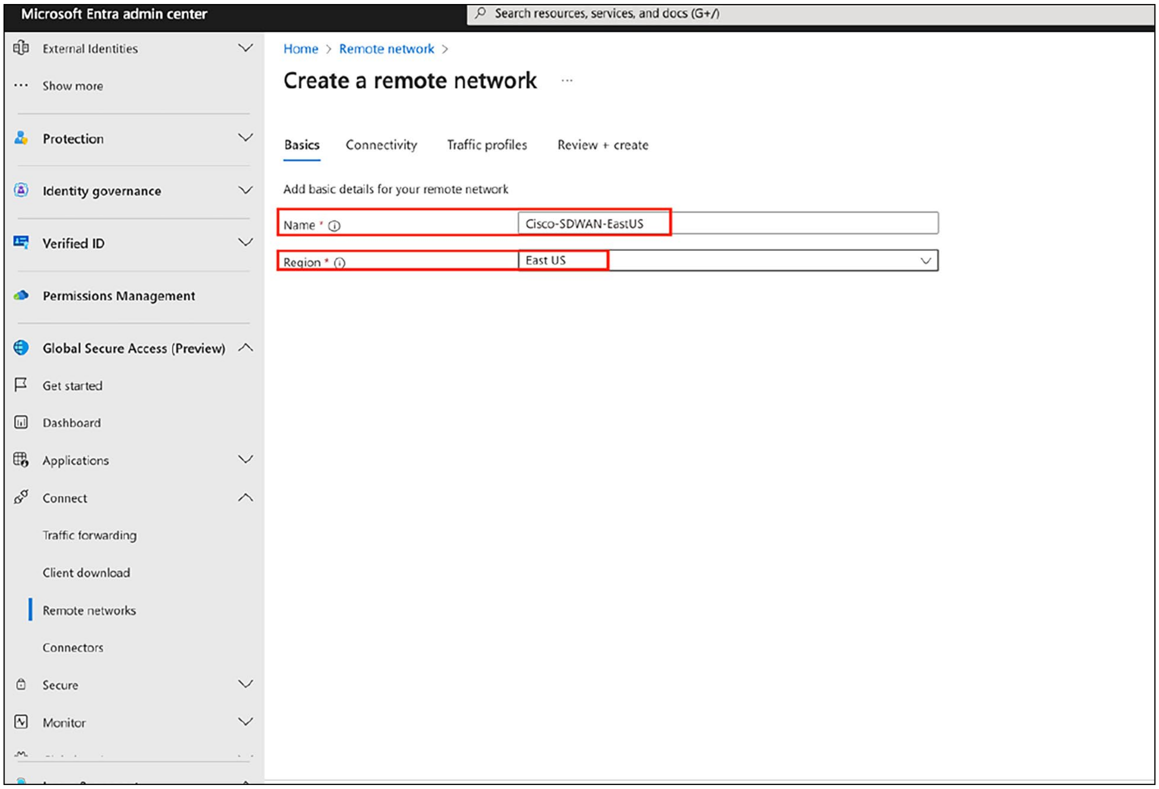


Remote networks enable admins to define and configure remote network locations, including names, regions, and bandwidth capacity, and add one or more customer premises equipment (CPE) links to a given remote network.

Remote network n... ↑	Region	Links	Device type	Forwarding profiles	Last modified	Object Id	Connectivity details
...et remote netw...	West US 3	1 link		1 profile	02/07/2024, 05:52 ...	bcce54c9-a591-4e1a-a18e-30caccc838b3	View configuration
	East US	2 links		1 profile	01/22/2024, 09:42 ...	4d3d0ad2-b936-4e12-8de6-ee530715d2e2	View configuration
-SDWAN-Site1	East US	4 links		1 profile	01/24/2024, 08:28 ...	341c01f2-b8a2-405a-91cb-a6032316ac27	View configuration
JL-	West US 3	4 links		1 profile	02/08/2024, 11:52 ...	2b05184b-cb1d-418e-b239-f8561b46bd5c	View configuration
Seattle branch	West US 2	1 link		1 profile	09/28/2023, 03:04 ...	009de9e7-ae3e-48af-864e-319e8abf4b21	View configuration
to-eric	West US 2	1 link			11/06/2023, 10:49 ...	e921a56d-6351-4b17-94bd-07aca337b5a1	View configuration
...are-google	West US 2	1 link		1 profile	10/11/2023, 09:53 ...	1bae25c5-b852-478a-b9f6-076561574242	View configuration

Figure 2.
Creating a remote network in the Microsoft Entra Admin Center

2. On the Basics tab, fill in the remote network name and select the region.



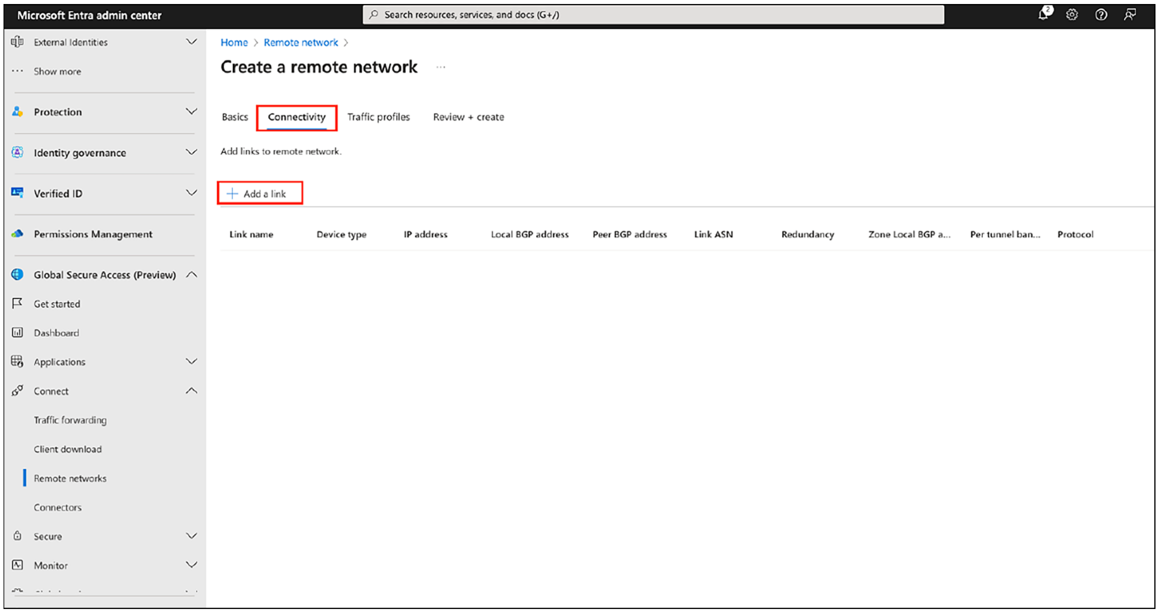
Add basic details for your remote network

Name * Cisco-SDWAN-EastUS

Region * East US

Figure 3.
Entering the network name and region

3. On the Connectivity tab, create two links for the CPE to ensure the creation of multiple tunnels, with the same remote endpoint (CPE public IP) but different local endpoints. Users can set up two or more tunnels based on their requirements.



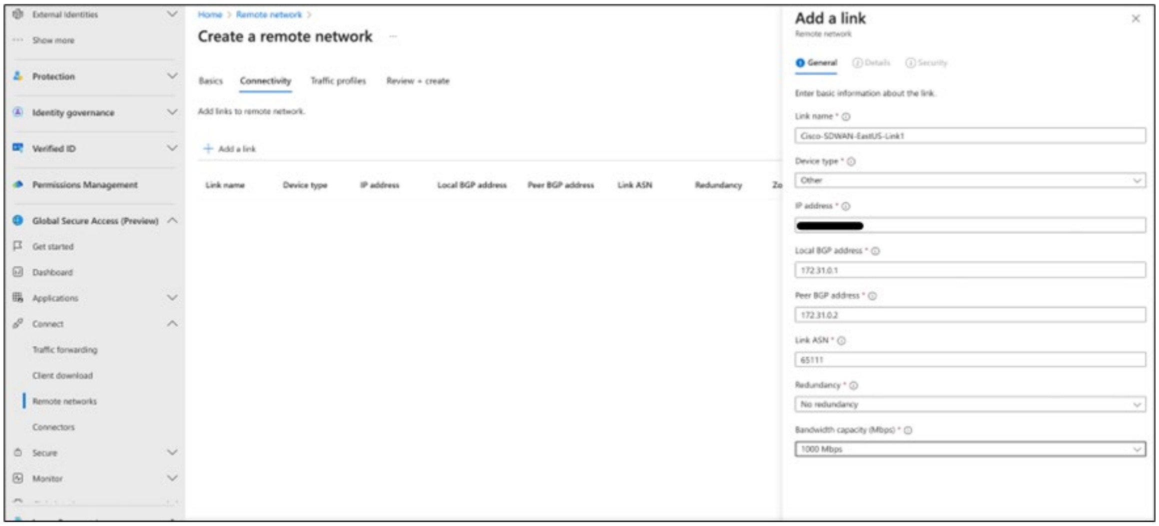
Add links to remote network.

Link name	Device type	IP address	Local BGP address	Peer BGP address	Link ASN	Redundancy	Zone Local BGP a...	Per tunnel ban...	Protocol

Figure 4.
Adding connectivity links

Note: Cisco uses policy-based packet redirection to tunnel for Microsoft apps. Therefore, Cisco routers do not require Border Gateway Protocol (BGP) for prefixes from Microsoft's SSE solution. Users should enter dummy values for BGP-related fields, as they are marked mandatory on the UI but do not affect tunnel establishment and routing.

3a. For link1 (Cisco-SDWAN-EastUS-Link1), fill in the general information including link name, device type (select "other"), IP address (CPE public IP), local BGP address, peer BGP address, link ASN, redundancy, and bandwidth capacity (Mbps).



Add links to remote network.

Add a link

Remote network

General | Details | Security

Enter basic information about the link.

Link name * : Cisco-SDWAN-EastUS-Link1

Device type * : Other

IP address * : [redacted]

Local BGP address * : 172.31.0.1

Peer BGP address * : 172.31.0.2

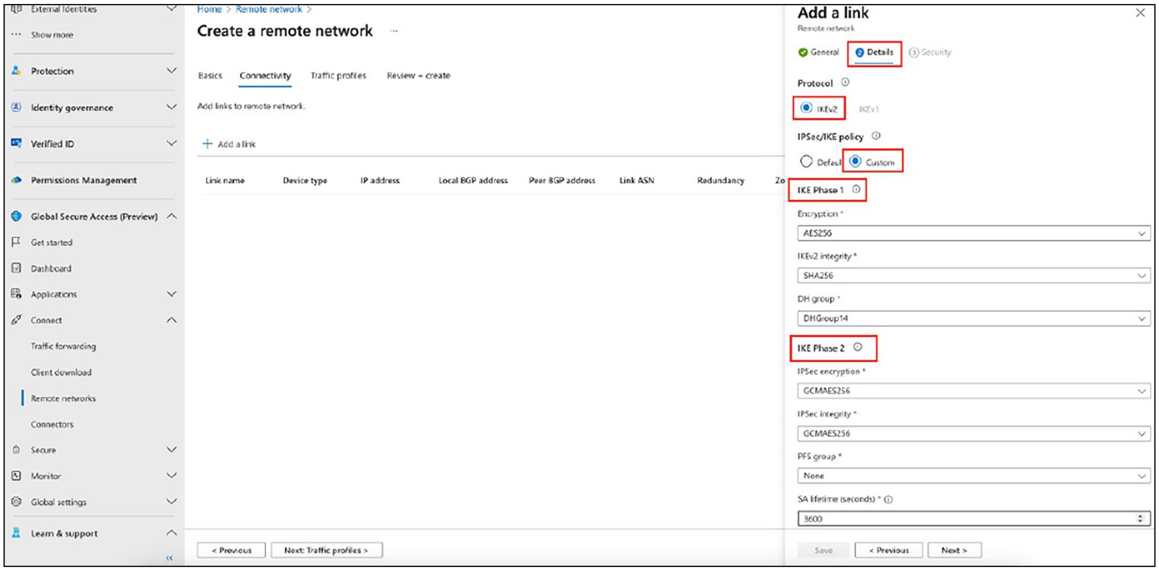
Link ASN * : 65111

Redundancy * : No redundancy

Bandwidth capacity (Mbps) * : 1000 Mbps

Figure 5.
Providing general link information

3b. On the Details tab of the Add a Link pane, fill in the IPsec and IKE v2 information.



Add links to remote network.

Add a link

Remote network

General | Details | Security

Protocol: ● IKEv2 ○ IKEv1

IPSec/IKE policy: ○ Defaul ● Custom

IKE Phase 1

Encryption * : AES256

IKEv2 integrity * : SHA256

DH group * : DHGroup14

IKE Phase 2

IPSec encryption * : GCMAES256

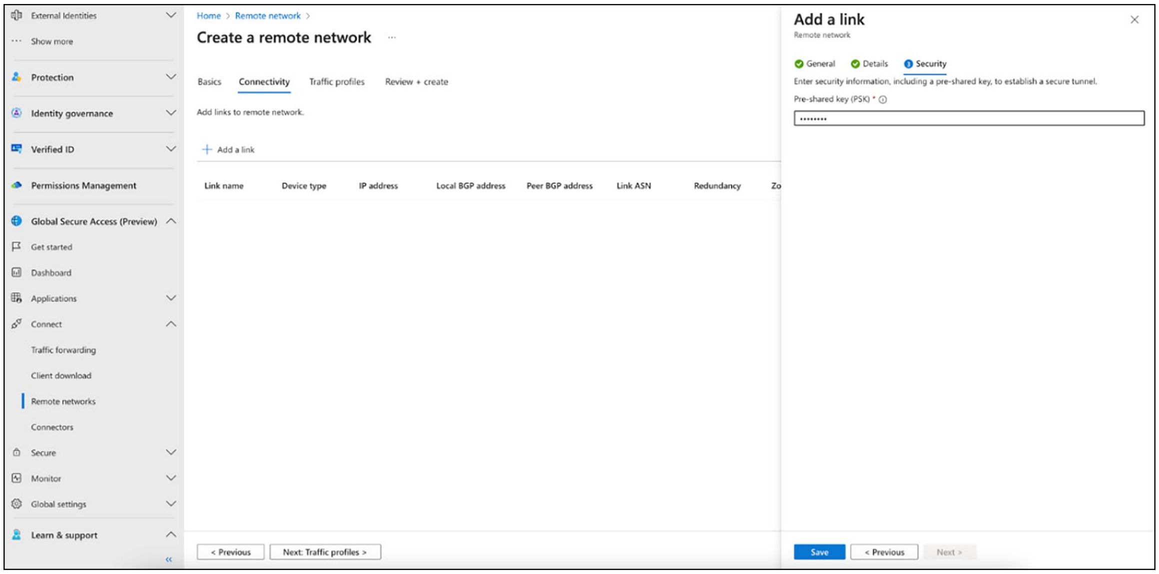
IPSec integrity * : GCMAES256

PFS group * : None

SA lifetime (seconds) * : 3600

Figure 6.
Specifying IPsec and IKEv2 information

3c. On the Security tab of the Add a Link pane, fill in the Pre-Shared Key (PSK) value.



Add a link

Remote network

✓ General ✓ Details ③ Security

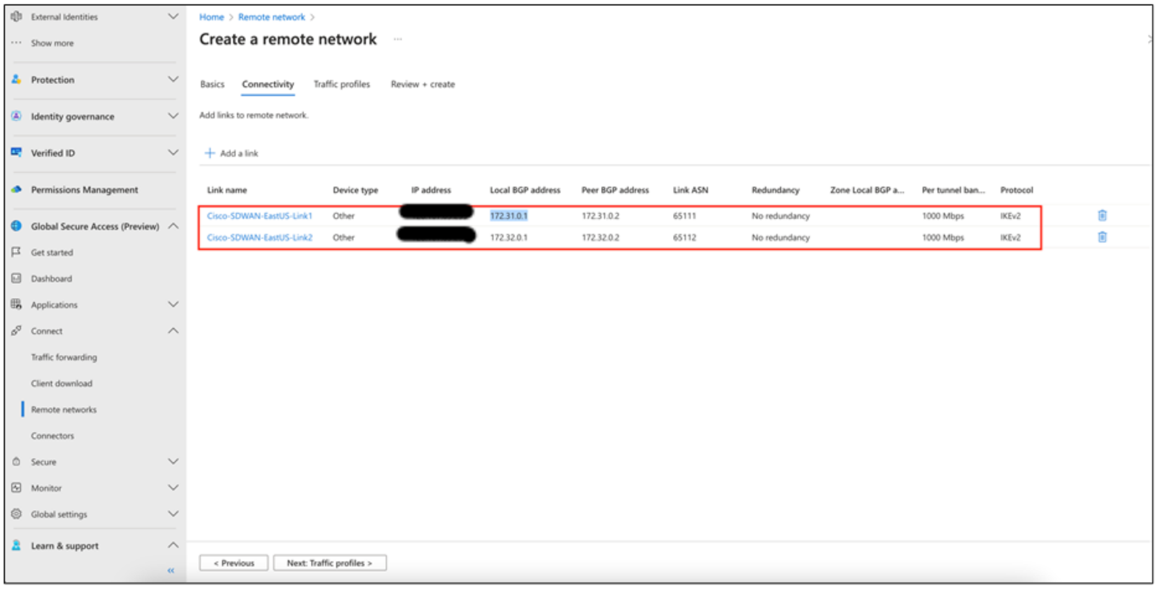
Enter security information, including a pre-shared key, to establish a secure tunnel.

Pre-shared key (PSK) * ⓘ

••••••••

Figure 7.
Providing the PSK value

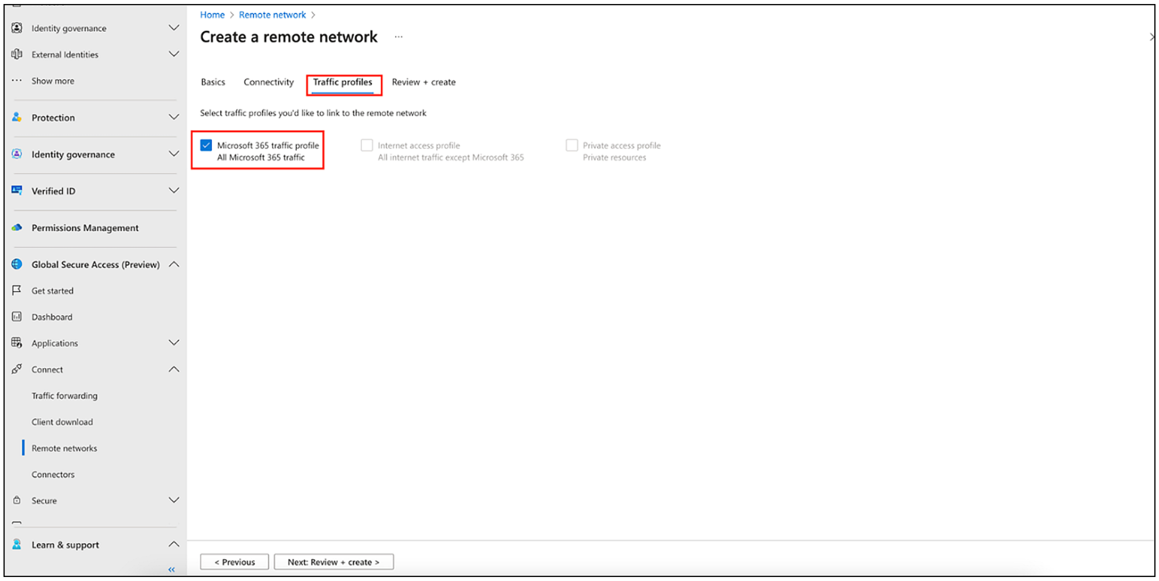
4. Create another link (Cisco-SDWAN-EastUS-Link2) for the same remote network by filling in details similar to those for link1 (Cisco-SDWAN-EastUS-Link1).



Link name	Device type	IP address	Local BGP address	Peer BGP address	Link ASN	Redundancy	Zone Local BGP a...	Per tunnel ban...	Protocol
Cisco-SDWAN-EastUS-Link1	Other	[redacted]	172.31.0.1	172.31.0.2	65111	No redundancy		1000 Mbps	IKEv2
Cisco-SDWAN-EastUS-Link2	Other	[redacted]	172.32.0.1	172.32.0.2	65112	No redundancy		1000 Mbps	IKEv2

Figure 8.
Creating a second link

5. On the Traffic Profiles tab of the remote network, select which traffic is to be allowed through these links. Currently, only the Microsoft 365 traffic forwarding profile is available for selection.



Create a remote network

Select traffic profiles you'd like to link to the remote network

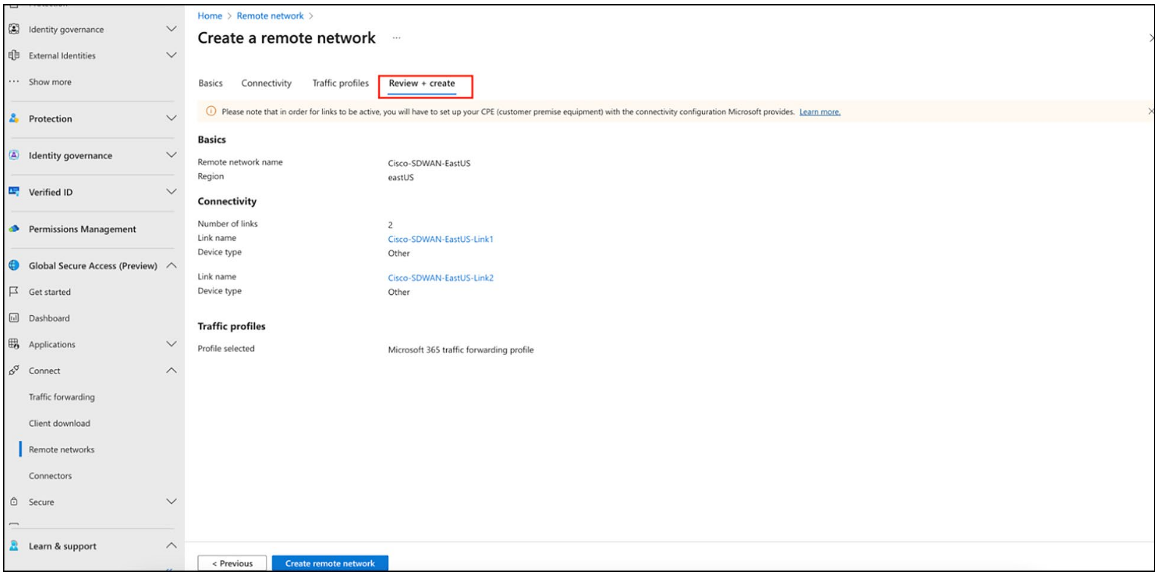
☑ Microsoft 365 traffic profile
All Microsoft 365 traffic

□ Internet access profile
All internet traffic except Microsoft 365

□ Private access profile
Private resources

Figure 9.
Completing the Traffic Profiles tab

6. Review and create the remote network as the final step.



Create a remote network

Please note that in order for links to be active, you will have to set up your CPE (customer premise equipment) with the connectivity configuration Microsoft provides. Learn more.

Basics

Remote network name	Cisco-SDWAN-EastUS
Region	eastUS

Connectivity

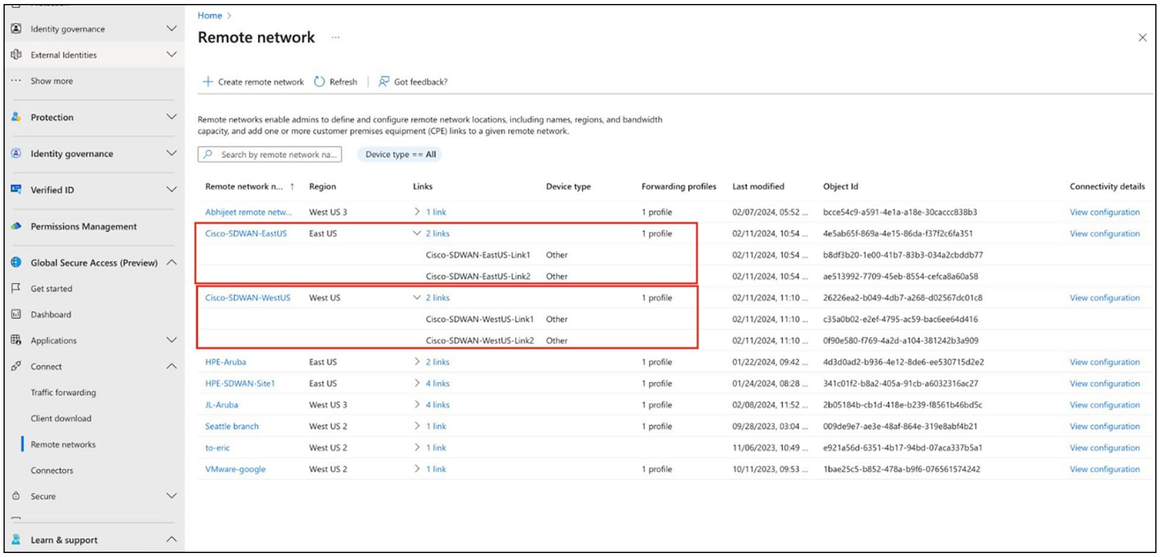
Number of links	2
Link name	Cisco-SDWAN-EastUS-Link1
Device type	Other
Link name	Cisco-SDWAN-EastUS-Link2
Device type	Other

Traffic profiles

Profile selected	Microsoft 365 traffic forwarding profile

Figure 10.
Reviewing and creating the remote network

7. Optional steps are needed when CPE uses multiple HA pairs. Create another remote network in the west region with two links, using values similar to those used for the remote network in the east region.

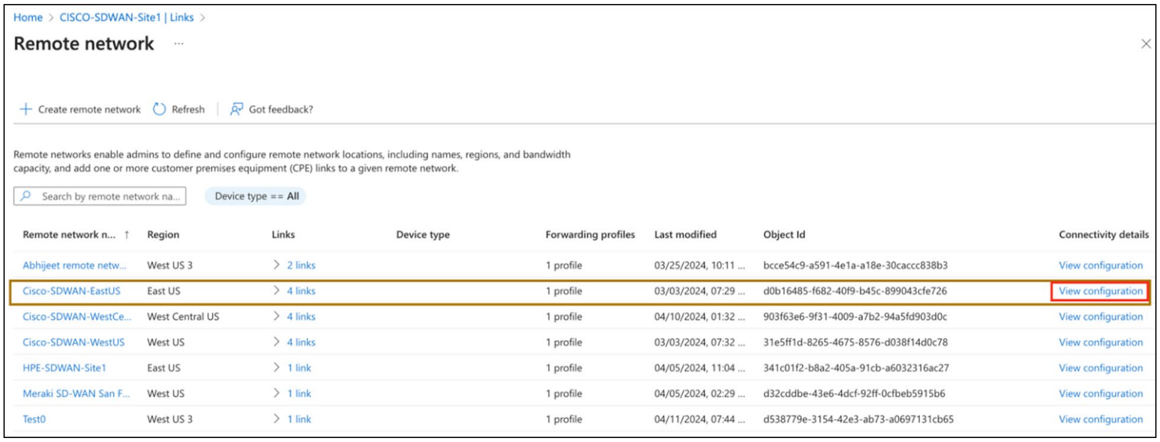


Remote networks enable admins to define and configure remote network locations, including names, regions, and bandwidth capacity, and add one or more customer premises equipment (CPE) links to a given remote network.

Remote network n... ↑	Region	Links	Device type	Forwarding profiles	Last modified	Object Id	Connectivity details
Abhijeet remote netw...	West US 3	1 link		1 profile	02/07/2024, 05:52 ...	bcce54c9-a591-4e1a-a18e-30caccc838b3	View configuration
Cisco-SDWAN-EastUS	East US	2 links		1 profile	02/11/2024, 10:54 ...	4e5ab65f-869a-4e15-86da-f37f2c6fa351	View configuration
		Cisco-SDWAN-EastUS-Link1	Other		02/11/2024, 10:54 ...	b8df3b20-1e00-41b7-83b3-034a2cbddb77	
		Cisco-SDWAN-EastUS-Link2	Other		02/11/2024, 10:54 ...	ae513992-7709-45eb-8554-cefca8a60a58	
Cisco-SDWAN-WestUS	West US	2 links		1 profile	02/11/2024, 11:10 ...	26226ea2-b049-4db7-a268-d02567dc01c8	View configuration
		Cisco-SDWAN-WestUS-Link1	Other		02/11/2024, 11:10 ...	c35a0b02-e2ef-4795-ac59-bac6ee64d416	
		Cisco-SDWAN-WestUS-Link2	Other		02/11/2024, 11:10 ...	0f90e580-f769-4a2d-a104-381242b3a909	
HPE-Aruba	East US	2 links		1 profile	01/22/2024, 09:42 ...	4d3d0ad2-b936-4e12-8de6-ee530715d2e2	View configuration
HPE-SDWAN-Site1	East US	4 links		1 profile	01/24/2024, 08:28 ...	341c01f2-b8a2-405a-91cb-a6032316ac27	View configuration
JL-Aruba	West US 3	4 links		1 profile	02/08/2024, 11:52 ...	2b05184b-cb1d-418e-b239-f8561b46bd5c	View configuration
Seattle branch	West US 2	1 link		1 profile	09/28/2023, 03:04 ...	009de9e7-ae3e-48af-864e-319e8abf4b21	View configuration
to-eric	West US 2	1 link			11/06/2023, 10:49 ...	e921a56d-6351-4b17-94bd-07aca337b5a1	View configuration
VMware-google	West US 2	1 link		1 profile	10/11/2023, 09:53 ...	1bae25c5-b852-478a-b9f6-076561574242	View configuration

Figure 11.
Creating another remote network in the west region

8. Users can click the View Configuration option for each remote network to see the data center IPs and IKE encryption/auth details to be used in Cisco Catalyst SD-WAN Manager.



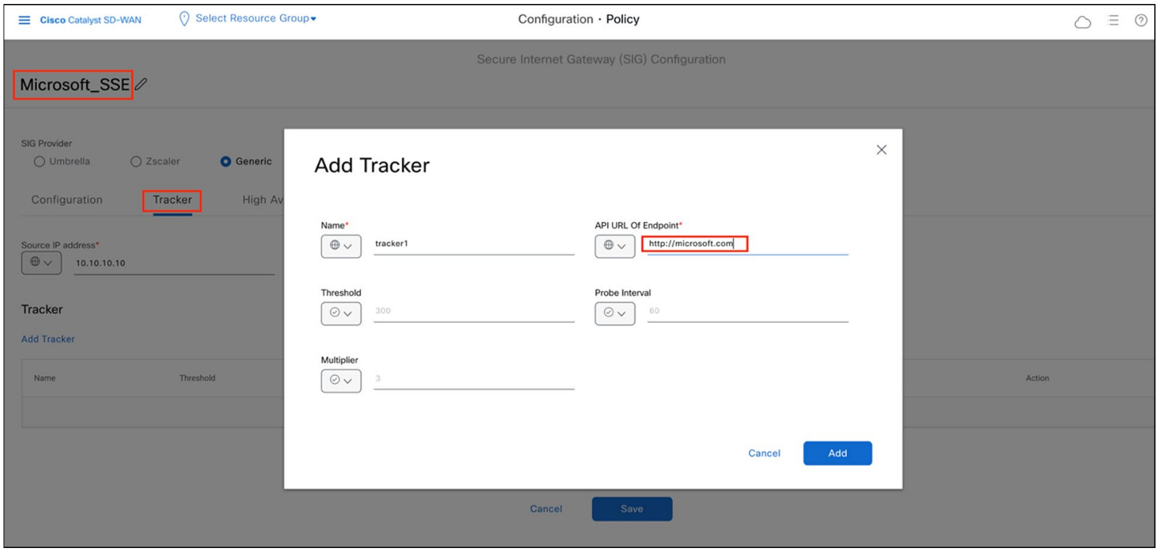
Remote networks enable admins to define and configure remote network locations, including names, regions, and bandwidth capacity, and add one or more customer premises equipment (CPE) links to a given remote network.

Remote network n... ↑	Region	Links	Device type	Forwarding profiles	Last modified	Object Id	Connectivity details
Abhijeet remote netw...	West US 3	2 links		1 profile	03/25/2024, 10:11 ...	bcce54c9-a591-4e1a-a18e-30caccc838b3	View configuration
Cisco-SDWAN-EastUS	East US	4 links		1 profile	03/03/2024, 07:29 ...	d0b16485-f682-40f9-b45c-899043cfe726	View configuration
Cisco-SDWAN-WestCe...	West Central US	4 links		1 profile	04/10/2024, 01:32 ...	903f63e6-9f31-4009-a7b2-94a5fd903d0c	View configuration
Cisco-SDWAN-WestUS	West US	4 links		1 profile	03/03/2024, 07:32 ...	31e5ff1d-8265-4675-8576-d038f14d0c78	View configuration
HPE-SDWAN-Site1	East US	1 link		1 profile	04/05/2024, 11:04 ...	341c01f2-b8a2-405a-91cb-a6032316ac27	View configuration
Meraki SD-WAN San F...	West US	1 link		1 profile	04/05/2024, 02:29 ...	d32cddbe-43e6-4dcf-92ff-0cfbeb5915b6	View configuration
Test0	West US 3	1 link		1 profile	04/11/2024, 07:44 ...	d538779e-3154-42e3-ab73-a0697131cb65	View configuration

Figure 12.
Locating the View Configuration option

Step 2. Configure an IPsec tunnel in Cisco Catalyst SD-WAN Manager using a SIG parcel

1. Configure the IPsec tunnel in Cisco Catalyst SD-WAN Manager using a Secure Internet Gateway (SIG) parcel. This configuration establishes a secure remote network connection between Microsoft's SSE solution and the Cisco Catalyst SD-WAN using an IPsec tunnel.
2. Set up tunnels using SIG templates: On the Catalyst SD-WAN Manager dashboard, select Configuration -> Policy Group -> Secure Internet Gateway (SIG).
3. Click the Add Secure Internet Gateway tab and create a SIG named Microsoft SSE.
4. Within the SIG template, select the Generic Tunnel option. Additionally, create a tracker to ensure the health of the tunnel. In this example, we have used microsoft.com.



Microsoft_SSE

SIG Provider: ○ Umbrella ○ Zscaler ● Generic

Source IP address*: 10.10.10.10

Name*: tracker1

API URL Of Endpoint*: http://microsoft.com

Threshold: 300

Probe Interval: 60

Multiplier: 3

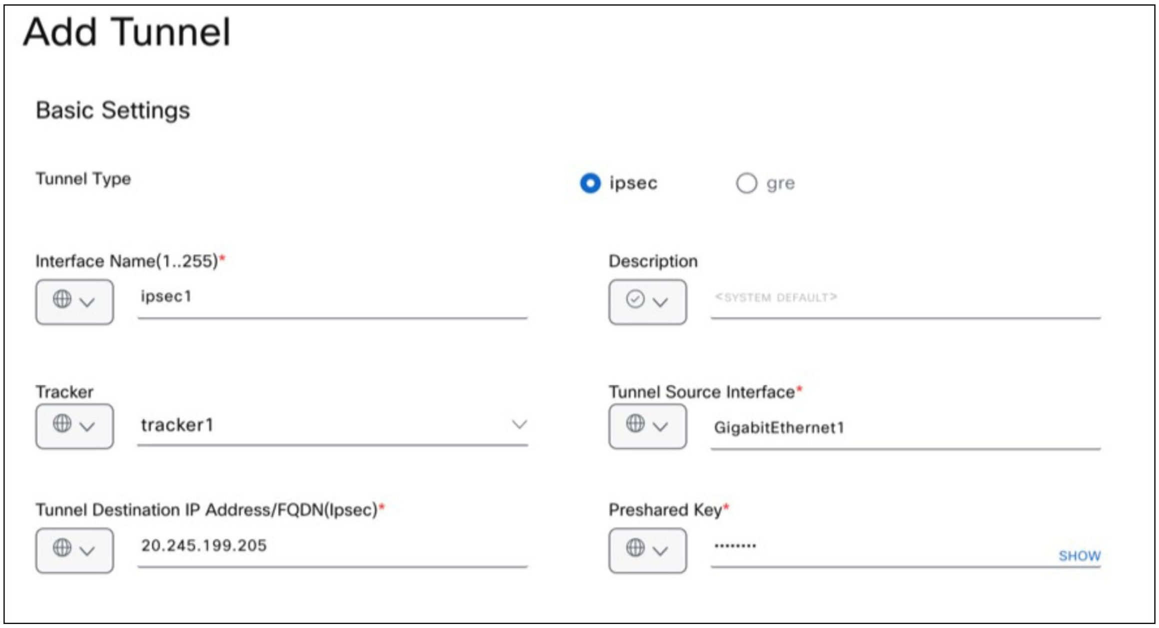
Figure 13.
Adding a tracker to the IPsec tunnel in the Catalyst SD-WAN Manager dashboard

After establishing the tracker, create four IPsec tunnels. Configure two tunnels for HA-pair1 and another two tunnels for HA-pair2. The two HA pairs are configured as shown below:

```
ipsec1 ------- > HA-pair1 (active tunnel), connected through WAN link1 of CPE to
Microsoft Cisco-SDWAN-WestUS-Link1

ipsec2 ------- > HA-pair1 (standby tunnel), connected through WAN link1 of CPE to
Microsoft Cisco-SDWAN-EastUS-Link1

ipsec3 ------- > HA-pair2 (active tunnel), connected through WAN link2 of CPE to
Microsoft Cisco-SDWAN-WestUS-Link2

ipsec4 ------- > HA-pair2 (standby tunnel), connected through WAN link2 of CPE to
Microsoft Cisco-SDWAN-EastUS-Link2
```

Note: Users can create up to four HA pairs, enabling a total of eight IPsec tunnels.

5. Add the basic tunnel information, fill in the mandatory fields, including Interface Name, Tracker, Tunnel Source Interface (WAN Link1), the Cisco-SDWAN-EastUS-Link1 remote IP address, and Pre-shared Key (as configured in the Microsoft Entra Admin Center).



Add Tunnel

Basic Settings

Tunnel Type ● ipsec ○ gre

Interface Name(1..255)*: ipsec1

Description: <SYSTEM DEFAULT>

Tracker: tracker1

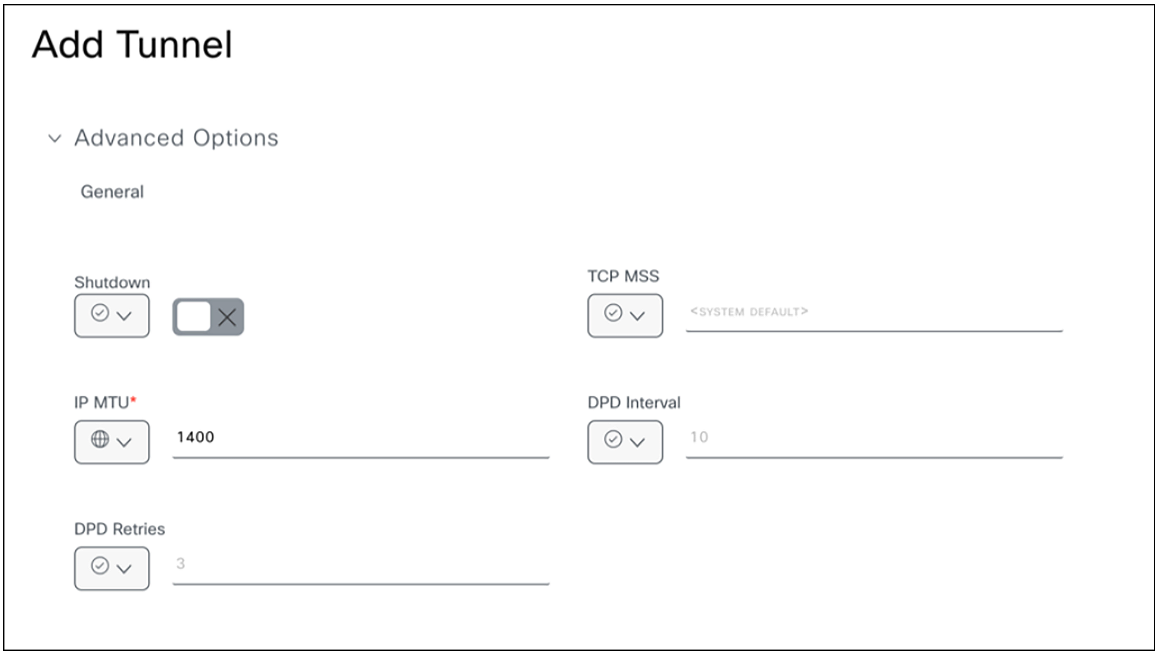
Tunnel Source Interface*: GigabitEthernet1

Tunnel Destination IP Address/FQDN(Ipsec)*: 20.245.199.205

Preshared Key*: •••••••• SHOW

Figure 14.
Providing basic tunnel information

6. Under Advanced Options, update the fields as required.



Add Tunnel

Advanced Options

General

Shutdown: ☒

TCP MSS: <SYSTEM DEFAULT>

IP MTU*: 1400

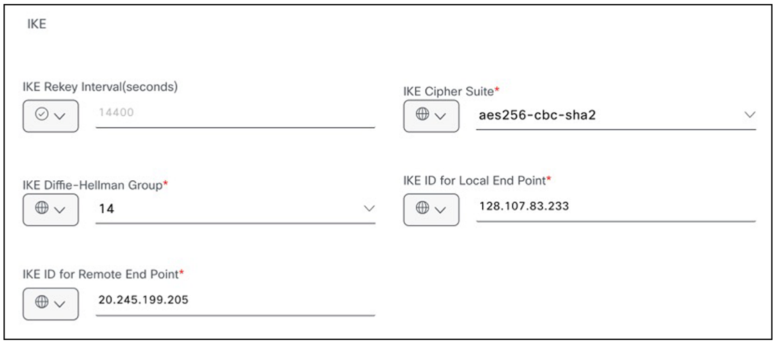
DPD Interval: 10

DPD Retries: 3

Figure 15.
Specifying advanced options

7. For the Advanced Options IKE value, fill in the encryption parameters as configured on the IKEv2 tab of Microsoft Entra Admin Center.

Cisco SD-WAN IKE config >>>



IKE

IKE Rekey Interval(seconds): 14400

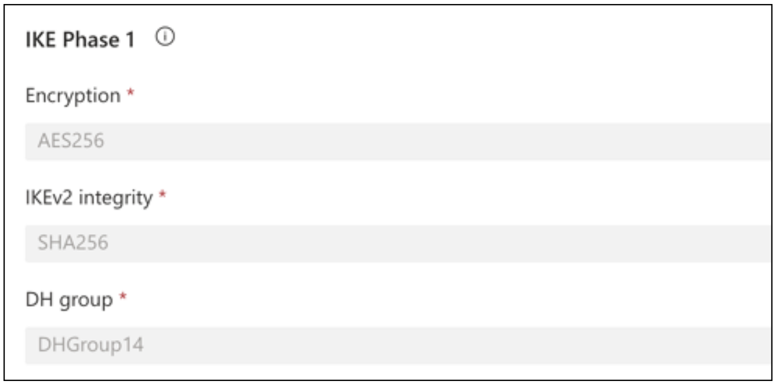
IKE Cipher Suite*: aes256-cbc-sha2

IKE Diffie-Hellman Group*: 14

IKE ID for Local End Point*: 128.107.83.233

IKE ID for Remote End Point*: 20.245.199.205

Microsoft-SSE IKE config >>>



IKE Phase 1

Encryption *: AES256

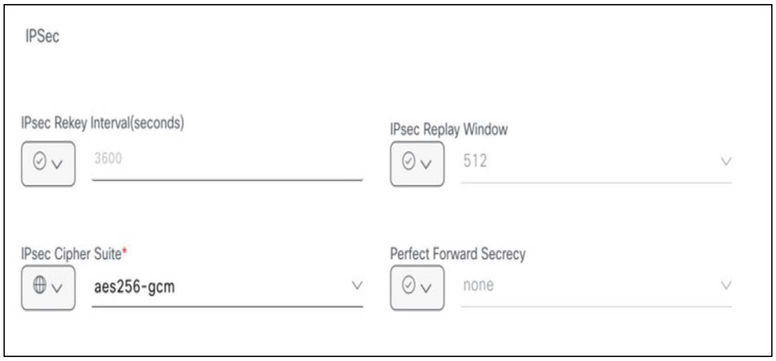
IKEv2 integrity *: SHA256

DH group *: DHGroup14

Figure 16.
Specifying the IKE value in Catalyst SD-WAN Manager

8. For the Advanced Options IPsec value, enter the encryption parameters as configured on the IKEv2 tab of the Microsoft Entra Admin Center.

Cisco SD-WAN IPsec config >>>



IPSec

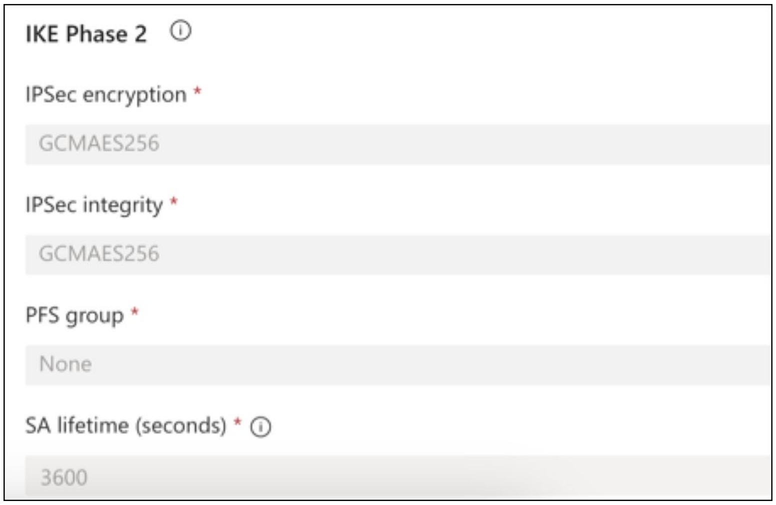
IPsec Rekey Interval(seconds): 3600

IPsec Replay Window: 512

IPsec Cipher Suite*: aes256-gcm

Perfect Forward Secrecy: none

Microsoft-SSE IPSec config >>>



IKE Phase 2 ⓘ

IPSec encryption *

GCMAES256

IPSec integrity *

GCMAES256

PFS group *

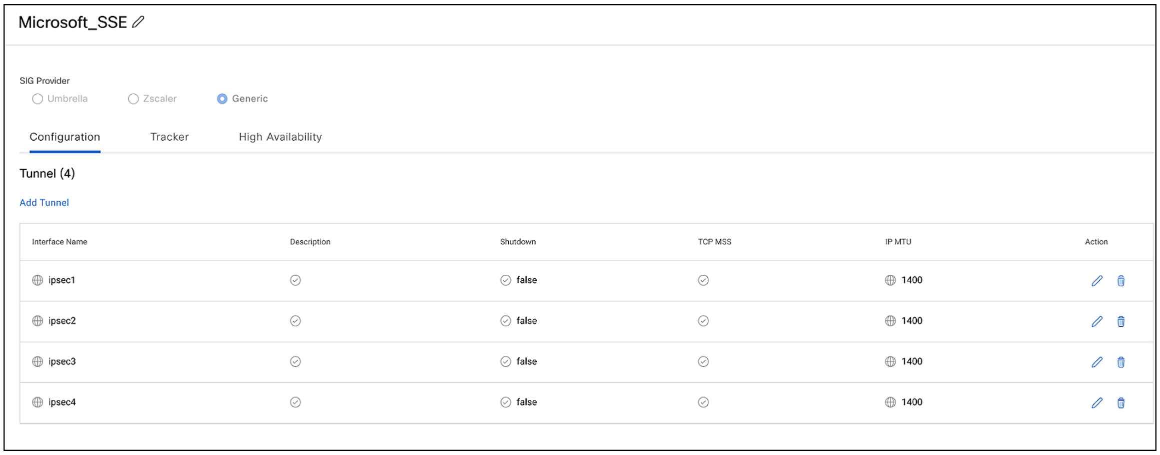
None

SA lifetime (seconds) * ⓘ

3600

Figure 17.
Specifying the IPsec value in Catalyst SD-WAN Manager

9. After establishing four IPsec tunnels, create two HA pairs using these four tunnels. The screen shot below shows tunnels configured that will participate in the HA pairs.



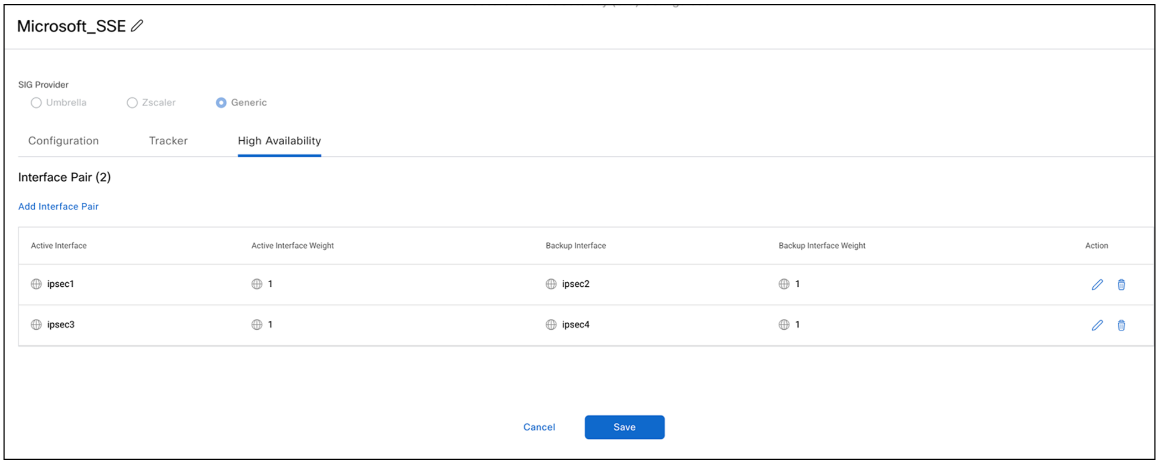
Microsoft_SSE

SIG Provider
○ Umbrella ○ Zscaler ● Generic

Tunnel (4)

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1	✓	✓ false	✓	1400	
ipsec2	✓	✓ false	✓	1400	
ipsec3	✓	✓ false	✓	1400	
ipsec4	✓	✓ false	✓	1400	

Figure 18.
Tunnels for HA pairs



Microsoft_SSE

SIG Provider

○ Umbrella ○ Zscaler ● Generic

Configuration | Tracker | High Availability

Interface Pair (2)

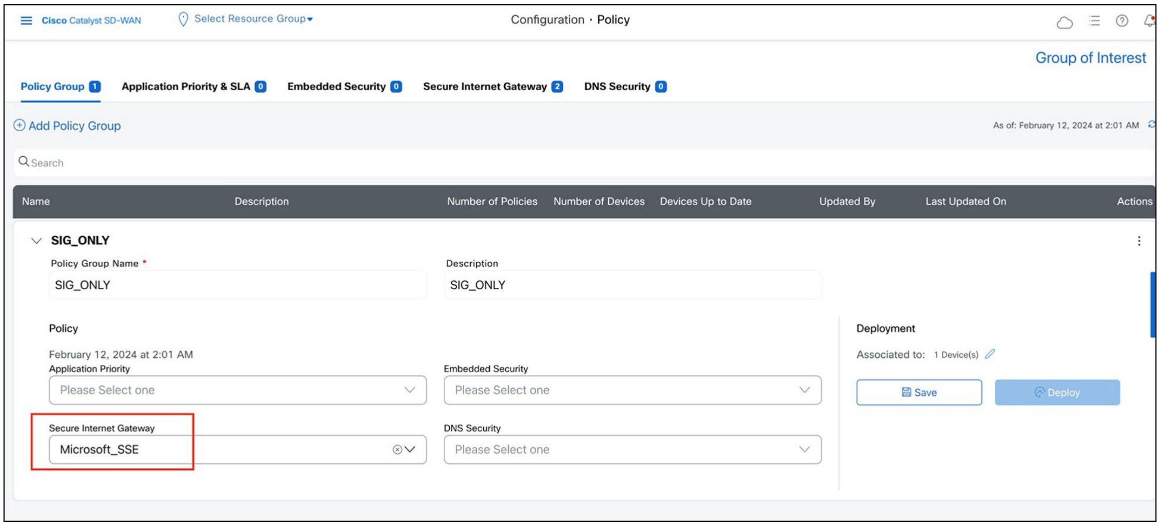
Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	1	ipsec2	1	
ipsec3	1	ipsec4	1	

Cancel | Save

Figure 19.
HA pairs configured

10. Attach the “Microsoft_SSE” template to the policy group and then deploy it to the device.



Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
SIG_ONLY							

Policy Group Name *: SIG_ONLY

Description: SIG_ONLY

Policy

February 12, 2024 at 2:01 AM

Application Priority: Please Select one

Embedded Security: Please Select one

Secure Internet Gateway: Microsoft_SSE

DNS Security: Please Select one

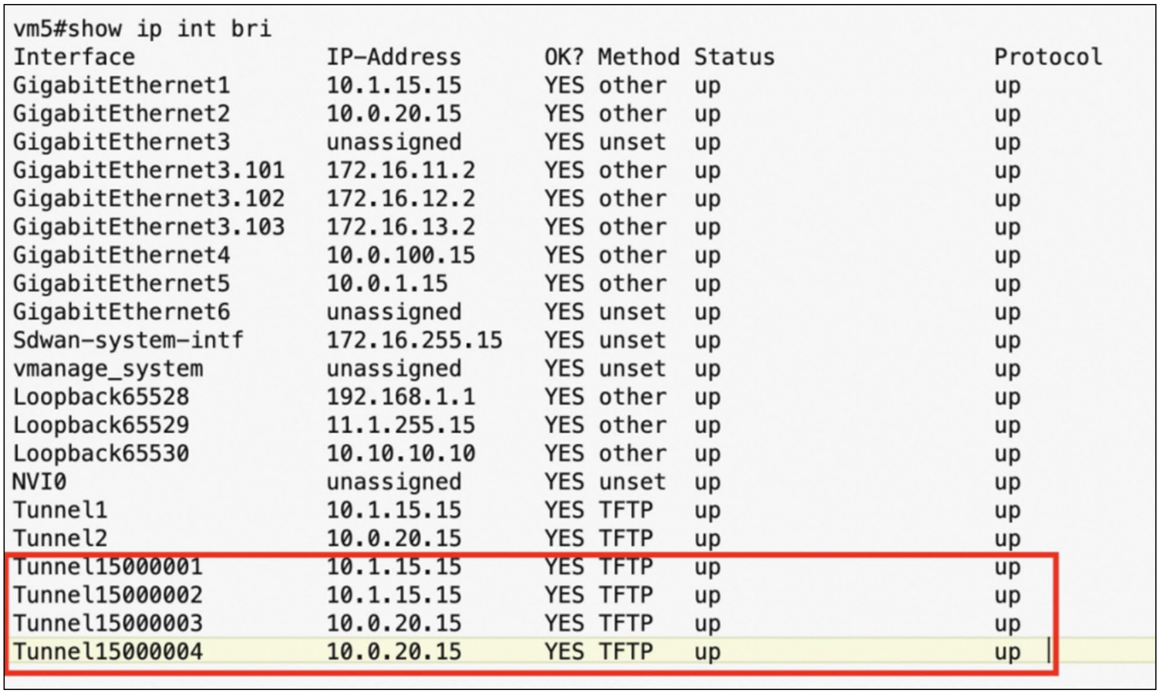
Deployment

Associated to: 1 Device(s)

Save | Deploy

Figure 20.
Attaching the “Microsoft_SSE” template

11. After successfully deploying the policy group on the CPE, all four tunnels and their respective trackers should be displayed.



```
vm5#show ip int bri
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.1.15.15      YES other  up                    up
GigabitEthernet2       10.0.20.15      YES other  up                    up
GigabitEthernet3       unassigned      YES unset  up                    up
GigabitEthernet3.101   172.16.11.2     YES other  up                    up
GigabitEthernet3.102   172.16.12.2     YES other  up                    up
GigabitEthernet3.103   172.16.13.2     YES other  up                    up
GigabitEthernet4       10.0.100.15     YES other  up                    up
GigabitEthernet5       10.0.1.15       YES other  up                    up
GigabitEthernet6       unassigned      YES unset  up                    up
Sdwan-system-intf      172.16.255.15   YES unset  up                    up
vmanage_system         unassigned      YES unset  up                    up
Loopback65528          192.168.1.1     YES other  up                    up
Loopback65529          11.1.255.15     YES other  up                    up
Loopback65530          10.10.10.10     YES other  up                    up
NVI0                   unassigned      YES unset  up                    up
Tunnel1                10.1.15.15      YES TFTP   up                    up
Tunnel2                10.0.20.15      YES TFTP   up                    up
Tunnel15000001         10.1.15.15      YES TFTP   up                    up
Tunnel15000002         10.1.15.15      YES TFTP   up                    up
Tunnel15000003         10.0.20.15      YES TFTP   up                    up
Tunnel15000004         10.0.20.15      YES TFTP   up                    up
```

Figure 21.
"Show interface" output from a branch edge device

Tracker status from branch edge device

vm5#show endpoint-tracker

```
Interface                    Record Name          Status          Address
Family    RTT in msecs     Probe ID   Next Hop
Tunnel15000001                 tracker1         Up      IPv4      226        30      None
Tunnel15000002                 tracker1         Up      IPv4      334        33      None
Tunnel15000003                 tracker1         Up      IPv4      345        31      None
Tunnel15000004                 tracker1         Up      IPv4      662        32      None
```

Step 3. Configure data policy for application-based traffic redirected from CPE

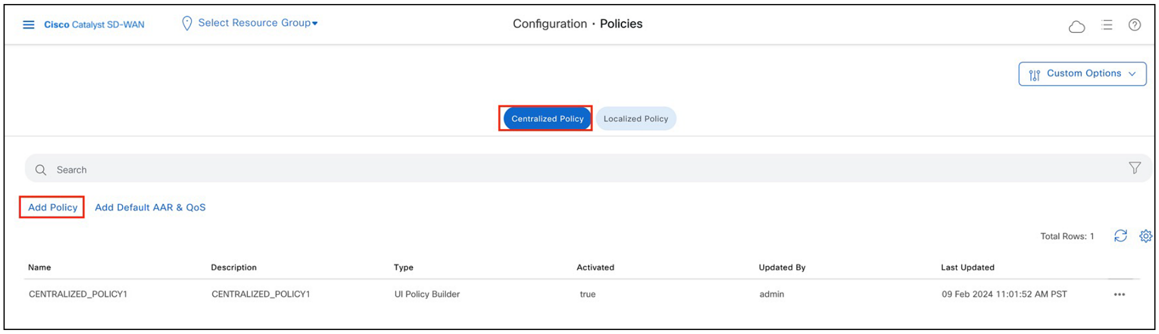
On Microsoft SSE, the user has specified that only Microsoft apps will be forwarded through the tunnel on CPE. To achieve this, a data policy on the SD-WAN is needed for application-based traffic redirected toward the SIG tunnels. The SD-WAN data policy allows using the application family or subapplications as match criteria, with an action set for SSE redirection. On the Catalyst SD-WAN CPE side, configure a data policy to route traffic from the service VPN as needed. The following is a sample policy:

- **Rule 1:** Send all DNS traffic through Direct Internet Access (DIA) for resolution.
- **Rule 2:** Send Microsoft application traffic through the SIG tunnel.
- **Rule 3:** Send all other internet traffic through DIA.

Once the data policy is created, associate it to the controllers that will eventually be pushed to CPE.

Steps to configure a data policy

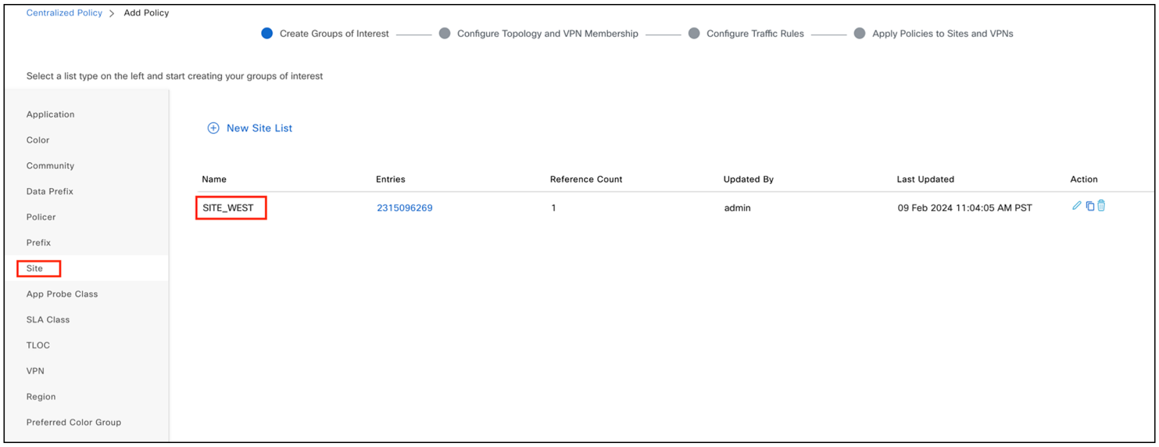
Step 1. On the Catalyst SD-WAN Manager dashboard, select Configuration > Policies > Centralized Policy, and then click Add Policy.



Name	Description	Type	Activated	Updated By	Last Updated
CENTRALIZED_POLICY1	CENTRALIZED_POLICY1	UI Policy Builder	true	admin	09 Feb 2024 11:01:52 AM PST

Figure 22.
Adding a data policy in Catalyst SD-WAN Manager

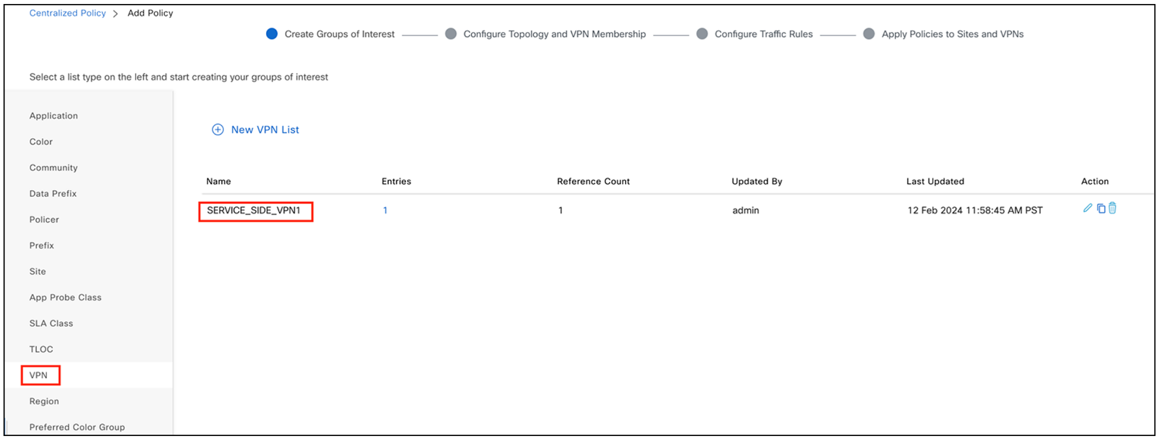
Step 2. On the Add Policy page, create groups of interest for VPN and Site.



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

Name	Entries	Reference Count	Updated By	Last Updated	Action
SITE_WEST	2315096269	1	admin	09 Feb 2024 11:04:05 AM PST	

Figure 23.
Creating a Site group of interest

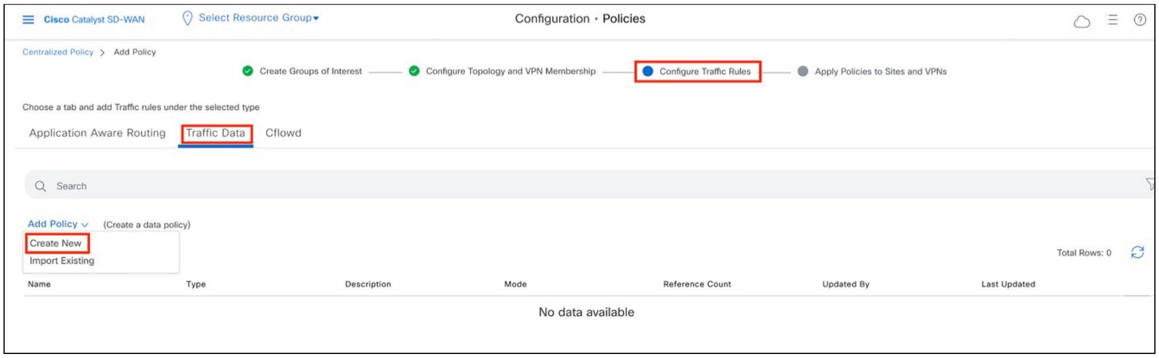


Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Updated By	Last Updated	Action
SERVICE_SIDE_VPN1	1	1	admin	12 Feb 2024 11:58:45 AM PST	

Figure 24.
Creating a VPN group of interest

Step 3. Navigate to the Configure Traffic Rules page and select Traffic Data to configure the data policy.


Cisco Catalyst SD-WAN
Select Resource Group
Configuration · Policies
Centralized Policy > Add Policy
Create Groups of Interest
Configure Topology and VPN Membership
Configure Traffic Rules
Apply Policies to Sites and VPNs

Choose a tab and add Traffic rules under the selected type

Application Aware Routing
Traffic Data
Cflowd
Search
Add Policy
Create New
Import Existing

(Create a data policy)

Total Rows: 0

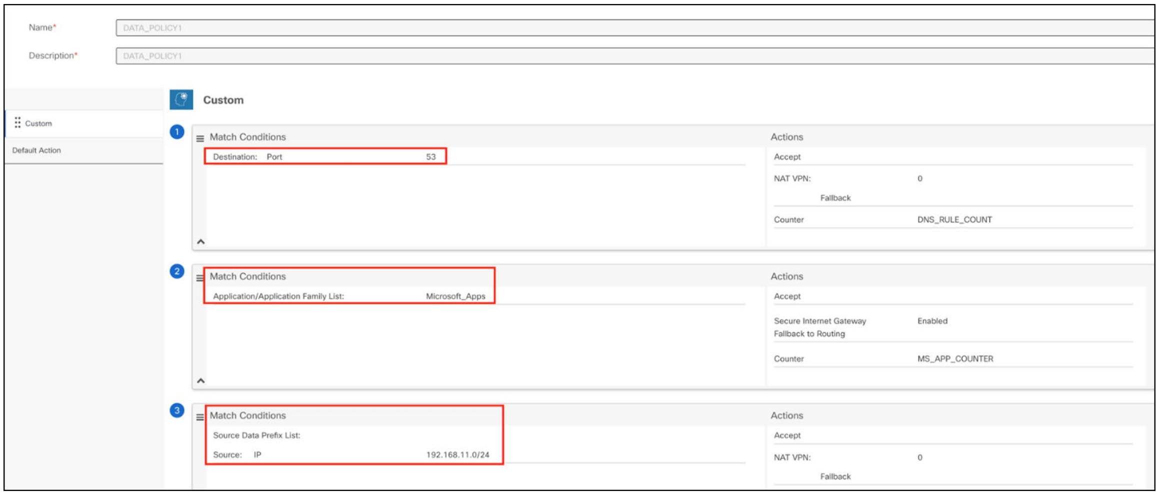
Name	Type	Description	Mode	Reference Count	Updated By	Last Updated

No data available

Figure 25.
Configuring traffic rules

Step 4. Add three sequences as the data policy defined above, with the three rules listed at the beginning of this section.

Below is a sample configuration for application-family-based policy rules (application family: Microsoft Apps, configured as a match condition for rule 2).


Name* DATA_POLICY1

Description* DATA_POLICY1

1 Match Conditions

Destination: Port 53

Actions

Accept

NAT VPN: 0

Fallback

Counter DNS_RULE_COUNT

2 Match Conditions

Application/Application Family List: Microsoft_Apps

Actions

Accept

Secure Internet Gateway Fallback to Routing Enabled

Counter MS_APP_COUNTER

3 Match Conditions

Source Data Prefix List:

Source: IP 192.168.11.0/24

Actions

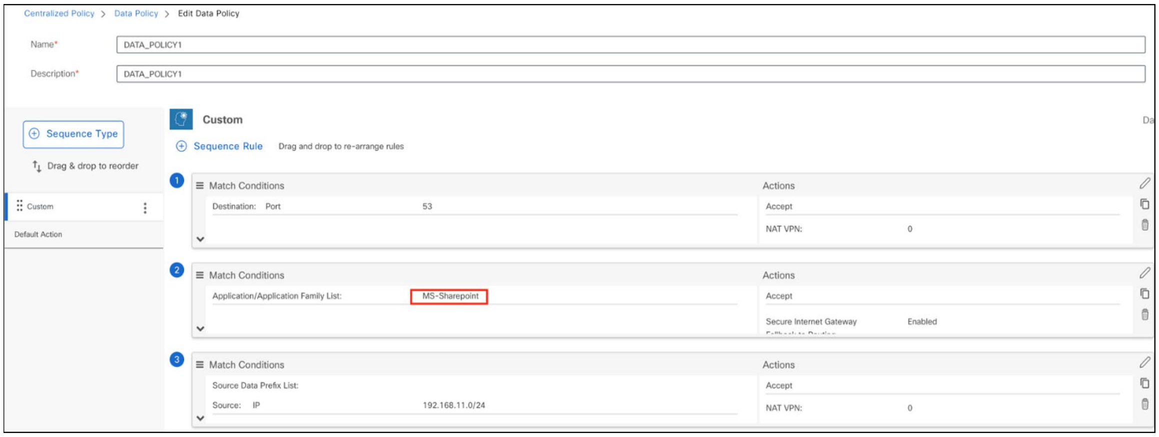
Accept

NAT VPN: 0

Fallback

Figure 26.
Configuring a policy rule based on application family

As another example of a more granular application, the user can configure a custom list of applications, each of which can have one or more subapplications, such as SharePoint.



Centralized Policy > Data Policy > Edit Data Policy

Name*: DATA_POLICY1

Description*: DATA_POLICY1

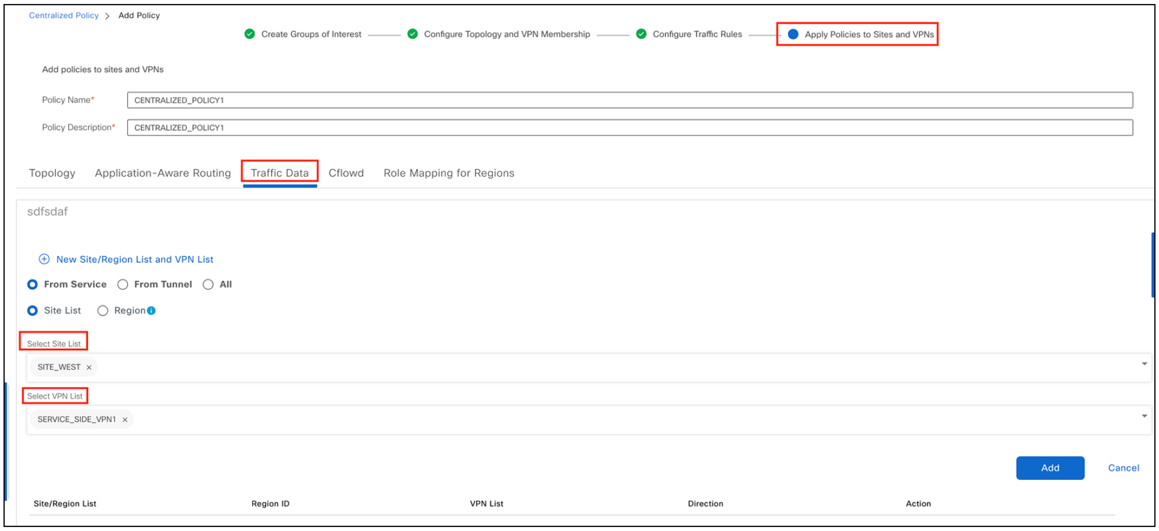
1 Match Conditions
Destination: Port 53
Actions
Accept
NAT VPN: 0

2 Match Conditions
Application/Application Family List: MS-Sharepoint
Actions
Accept
Secure Internet Gateway Enabled

3 Match Conditions
Source Data Prefix List:
Source: IP 192.168.11.0/24
Actions
Accept
NAT VPN: 0

Figure 27.
Configuring a policy rule for a subapplication

Step 5. Navigate to Apply Policies to Sites and VPNs. Click Traffic Data, and then select New Site/ Region List and VPN List. Choose the Site and VPN to apply to the data policy, and save the configuration.



Centralized Policy > Add Policy

Create Groups of Interest
Configure Topology and VPN Membership
Configure Traffic Rules
Apply Policies to Sites and VPNs

Add policies to sites and VPNs

Policy Name*: CENTRALIZED_POLICY1

Policy Description*: CENTRALIZED_POLICY1

Topology
Application-Aware Routing
Traffic Data
Cflowd
Role Mapping for Regions
sdfsdaf
⊕ New Site/Region List and VPN List

● From Service ○ From Tunnel ○ All

● Site List ○ Region

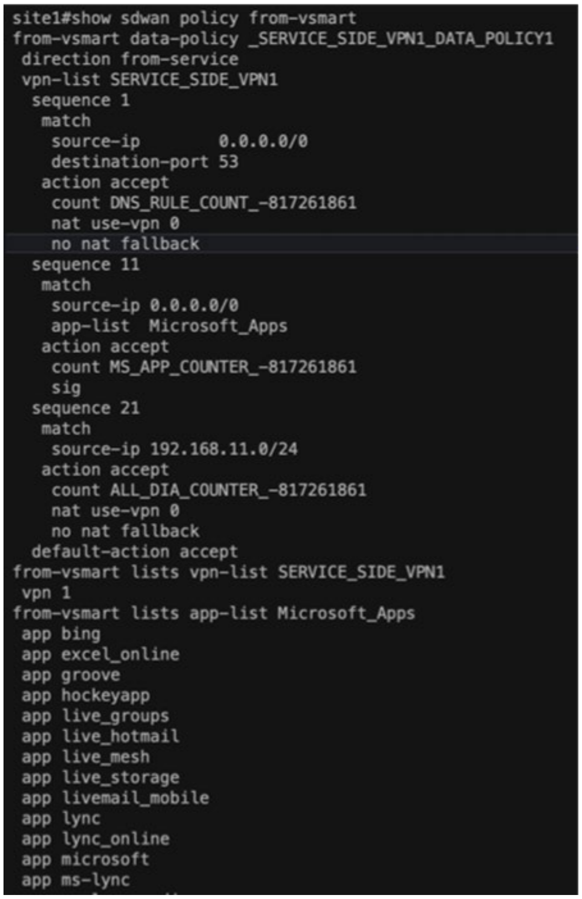
Select Site List: SITE_WEST ×

Select VPN List: SERVICE_SIDE_VPN1 ×

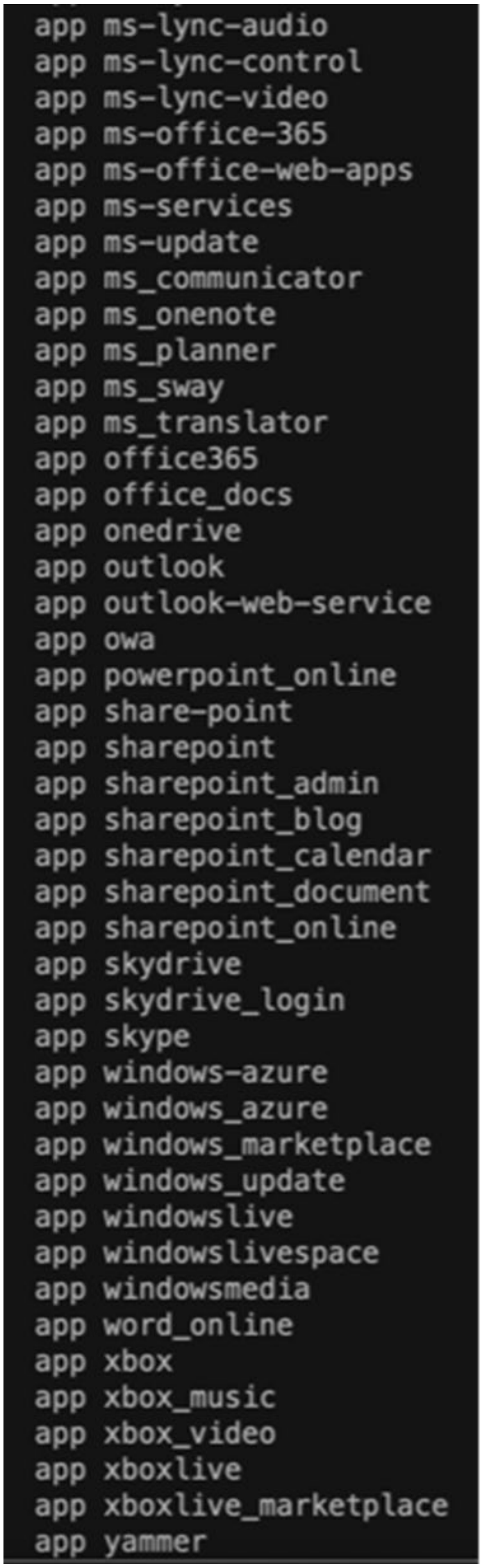
Site/Region List	Region ID	VPN List	Direction	Action

Figure 28.
Choosing the site and VPN for the data policy

Step 6. Activate the data policy and check that the policy is configured on the branch edge device.



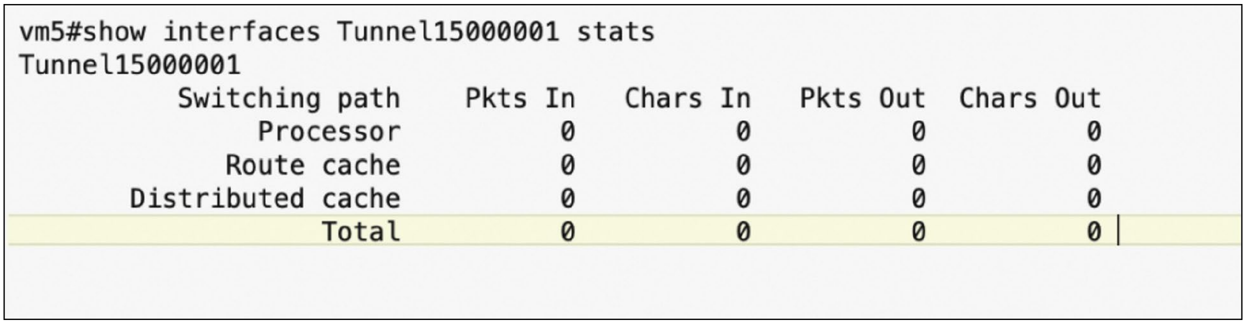
```
site1#show sdwan policy from-vsmart
from-vsmart data-policy _SERVICE_SIDE_VPN1_DATA_POLICY1
 direction from-service
 vpn-list SERVICE_SIDE_VPN1
  sequence 1
   match
    source-ip        0.0.0.0/0
    destination-port 53
   action accept
    count DNS_RULE_COUNT_-817261861
    nat use-vpn 0
    no nat fallback
  sequence 11
   match
    source-ip 0.0.0.0/0
    app-list  Microsoft_Apps
   action accept
    count MS_APP_COUNTER_-817261861
    sig
  sequence 21
   match
    source-ip 192.168.11.0/24
   action accept
    count ALL_DIA_COUNTER_-817261861
    nat use-vpn 0
    no nat fallback
  default-action accept
from-vsmart lists vpn-list SERVICE_SIDE_VPN1
 vpn 1
from-vsmart lists app-list Microsoft_Apps
 app bing
 app excel_online
 app groove
 app hockeyapp
 app live_groups
 app live_hotmail
 app live_mesh
 app live_storage
 app livemail_mobile
 app lync
 app lync_online
 app microsoft
 app ms-lync
```



```
 app ms-lync-audio
 app ms-lync-control
 app ms-lync-video
 app ms-office-365
 app ms-office-web-apps
 app ms-services
 app ms-update
 app ms_communicator
 app ms_onenote
 app ms_planner
 app ms_sway
 app ms_translator
 app office365
 app office_docs
 app onedrive
 app outlook
 app outlook-web-service
 app owa
 app powerpoint_online
 app share-point
 app sharepoint
 app sharepoint_admin
 app sharepoint_blog
 app sharepoint_calendar
 app sharepoint_document
 app sharepoint_online
 app skydrive
 app skydrive_login
 app skype
 app windows-azure
 app windows_azure
 app windows_marketplace
 app windows_update
 app windowslive
 app windowslivespace
 app windowsmedia
 app word_online
 app xbox
 app xbox_music
 app xbox_video
 app xboxlive
 app xboxlive_marketplace
 app yammer
```

Figure 29.
Verifying the data policy

Step 4. Validate the configuration–Send different application traffic and check the stats on different IPsec tunnels



```
vm5#show interfaces Tunnel15000001 stats
Tunnel15000001
         Switching path    Pkts In   Chars In   Pkts Out  Chars Out
              Processor          0          0          0          0
            Route cache          0          0          0          0
      Distributed cache          0          0          0          0
                  Total          0          0          0          0
```

Figure 30.
Validating the configuration

For more information

Please visit:

- Cisco Catalyst SD-WAN Security
- Microsoft Entra Internet Access

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-4556113-00 09/24