

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are large, soft-edged, overlapping shapes in similar colors, giving the overall image a sense of depth and movement.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Strengthening the first line of defense using Cisco Secure Firewall and Cisco Umbrella

Dinesh Moudgil

Technical Leader, Cloud and Network Security TME

Security Business Group

BRKSEC-1026



#CiscoLive

Cisco Secure Firewall and Cisco Umbrella integration provides multi-layered uniform security policy for DNS and Web traffic for on-prem and remote users leading to faster protection and improved internet performance.

Abstract

In a typical deployment, a perimeter firewall provides the security to ensure users are protected from attacks and threats. Nowadays, most of the applications are hosted on the cloud rather than on-prem and it is pertinent to ensure that any traffic to/from the internet is being controlled and inspected. Thus, Cisco Umbrella, our first line of defense, provides secure access to the internet for roaming and branch users.

This session covers an overview of the integration between Cisco Umbrella and Cisco Secure Firewall and details about features like Secure Internet Gateway (SIG), Umbrella DNS Connector, and simplified IPSec tunnel configuration to secure remote and branch users while accessing internet resources.

Cisco Webex App

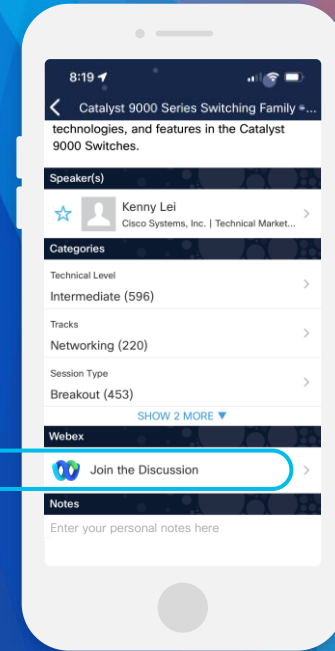
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1026>

Your Speaker

Dinesh Moudgil



- dmoudgil@cisco.com
- From Chandigarh, India
- CCIE Security #58881
- 7 Years with Cisco
- TAC - HTTS - TME Leader
- Lead VPN & Simplified Branch Initiatives
- Like outdoors and guitar



cisco *Live!*

What do you imagine might be some of the challenges most of the customers face while managing security policies for on-prem and remote resources?

Attackers are Everywhere

90%

Of malware use
DNS in attacks

68%

Of organizations
don't monitor their DNS

1 in 3

Reported breaches could
have
been controlled by DNS

\$100–
200B

Global losses could have
been prevented by DNS

Source: Cisco Security Research Report, CGA Report: The Economic Value of DNS Security

Why focus on DNS?

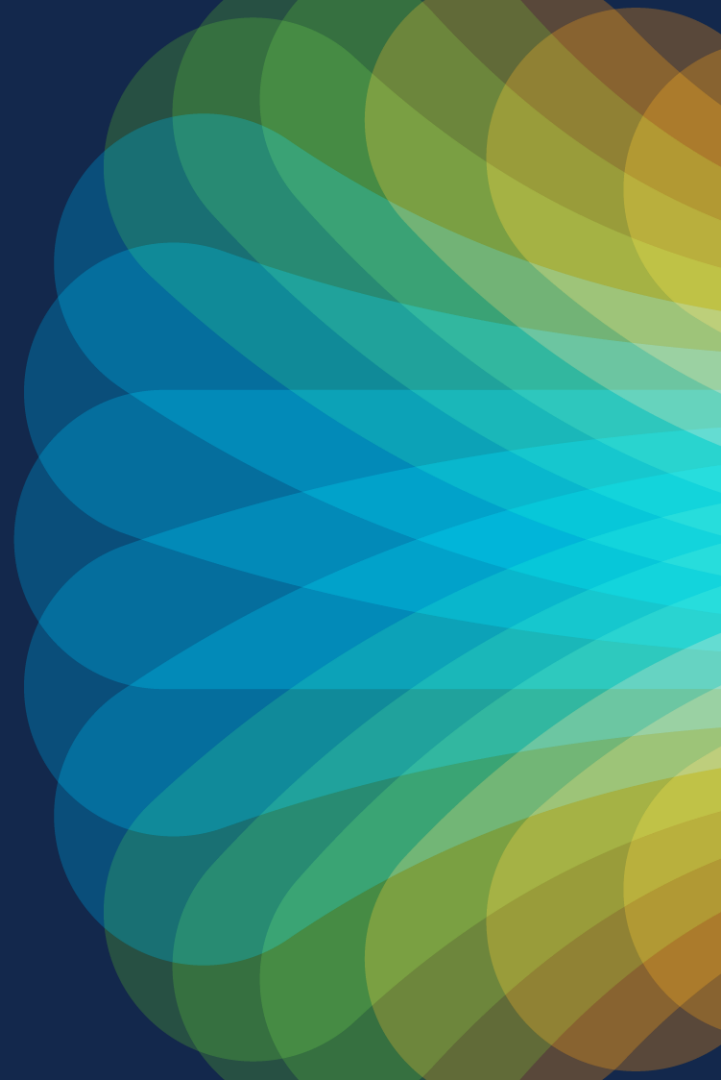
- The first step in most Internet connections
- Most easily overlooked
 - was created to connect, not to protect
- One of the easiest to secure
 - 1 in 3 breaches could have been prevented*
- Most efficient to secure
 - Commonly used mechanism by attackers

*Cisco Secure 2022 DNS Discoveries Report

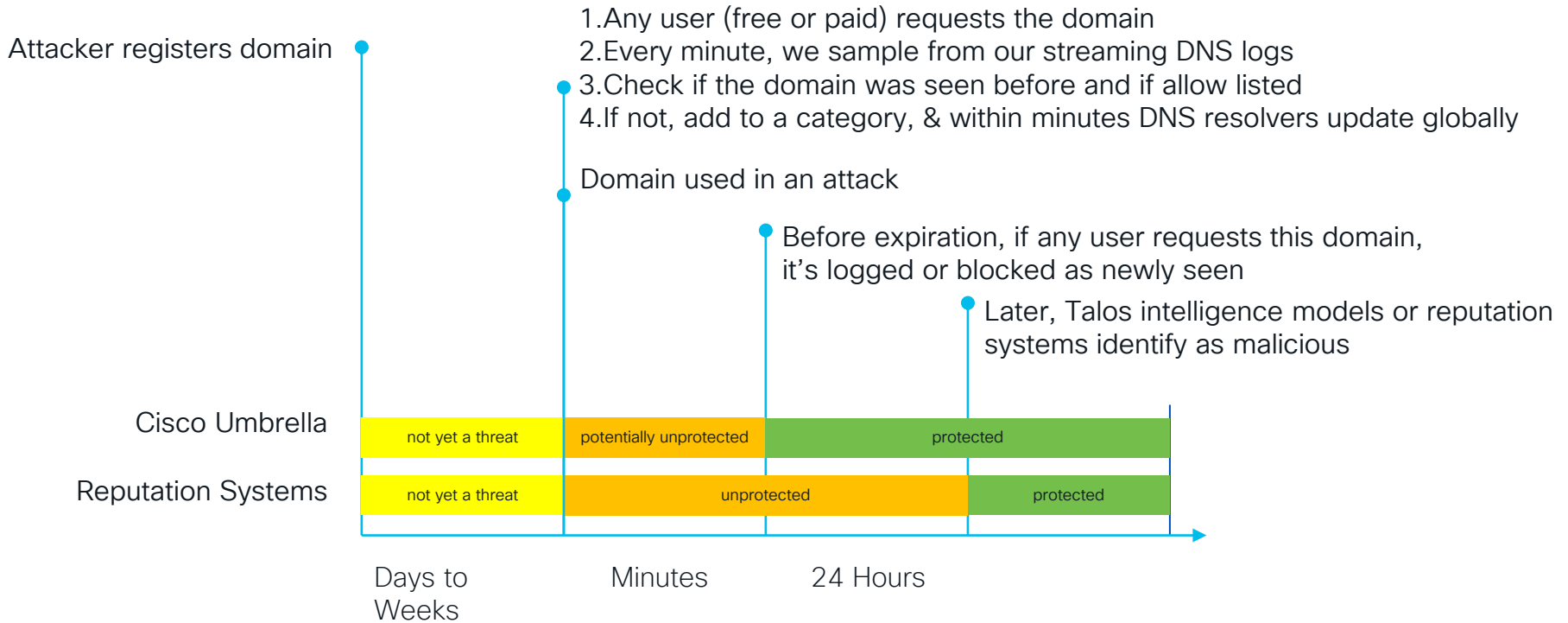
Agenda

- Umbrella DNS Connector
- Demonstration
- Umbrella SASE Auto Tunnel
- Demonstration
- Best Practices
- Conclusion

Umbrella DNS Connector



Why add Umbrella DNS Connector to FTD?



FTD SI DNS Security

- Backed by TALOS
- Block and Allow List based on domains
- Various Actions:
 - Drop
 - Domain Not Found
 - Sinkhole

Umbrella DNS Security

- Backed by TALOS
- Cloud Security Service
- Enforcement
- Unmatched Threat Intel

Benefits

- What better than Cisco Secure
 - 620 billion DNS requests daily*
 - Talos Intelligence
- Common DNS Policies for all branches
- Multi-layered DNS Security
- Eliminates the need for advanced NGFW features e.g. URL filtering & TLS Decryption
- Improved Internet Performance
- Uniform Security policy for Hybrid workers

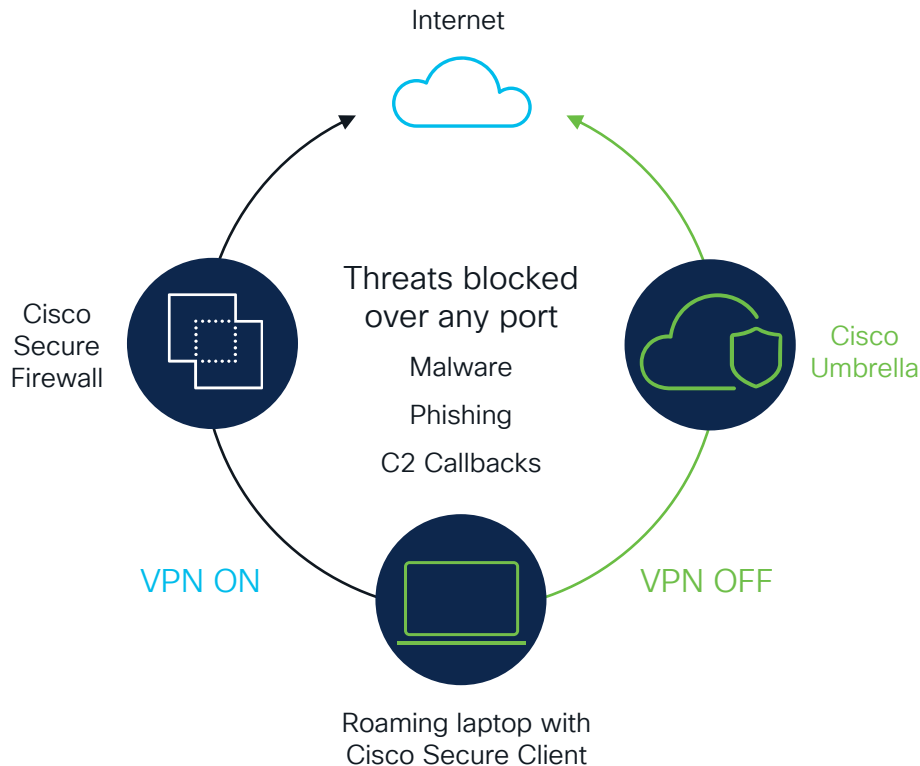
*Cisco Secure 2022 DNS Discoveries Report

Common DNS Policy Stack

Remote workers off VPN using
Umbrella Roaming Module

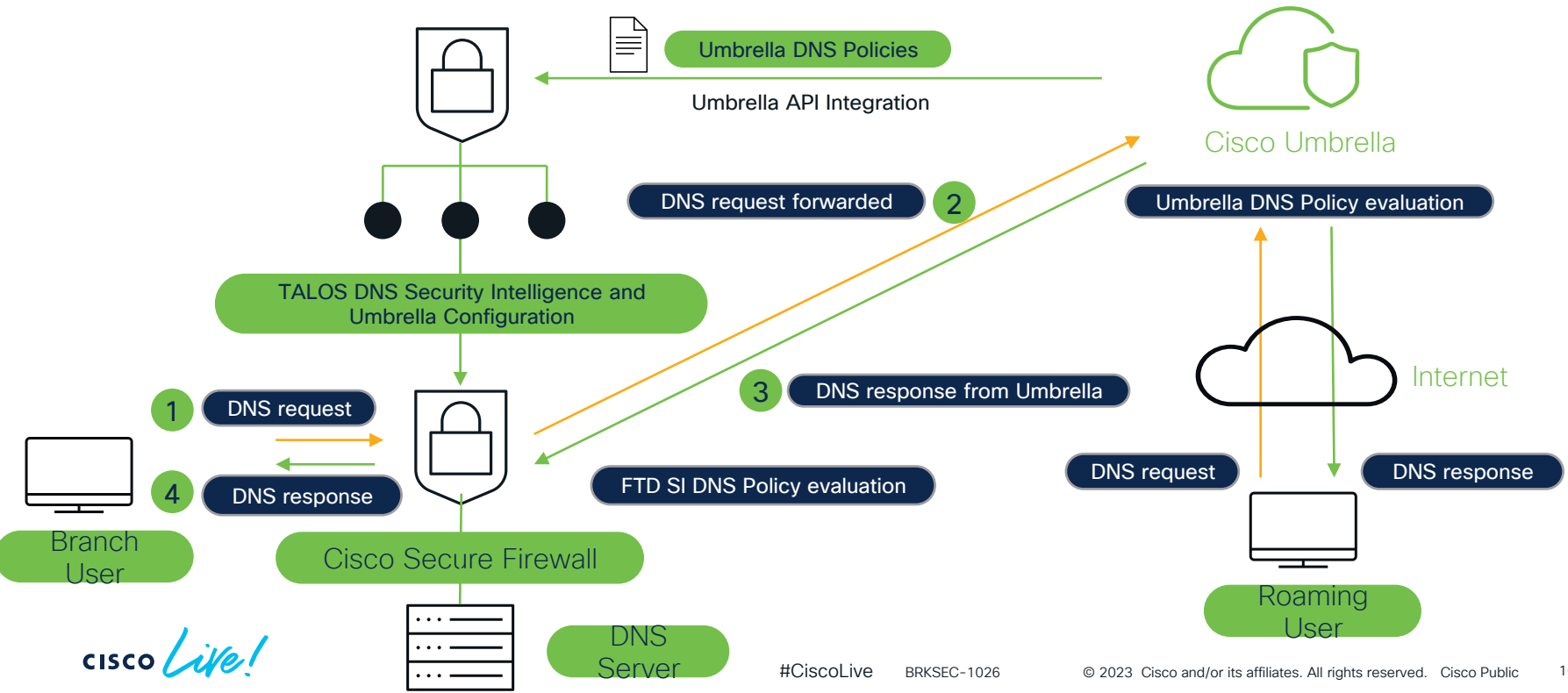
Remote workers connecting
over VPN to the HQ

Branch workers

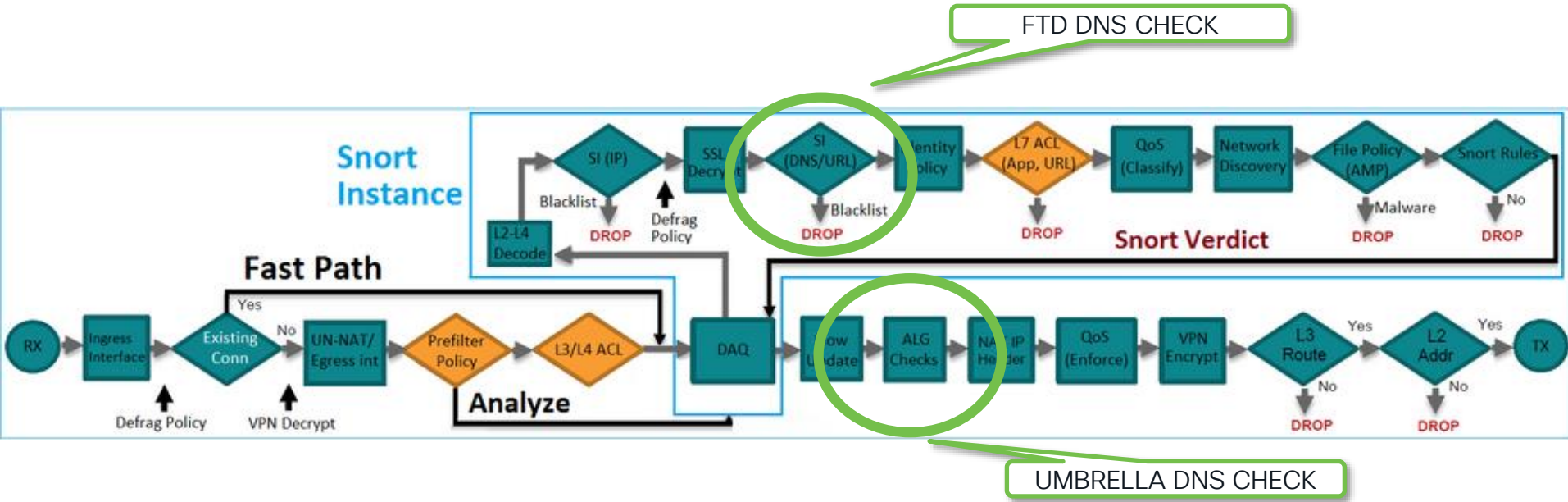


How does it work?

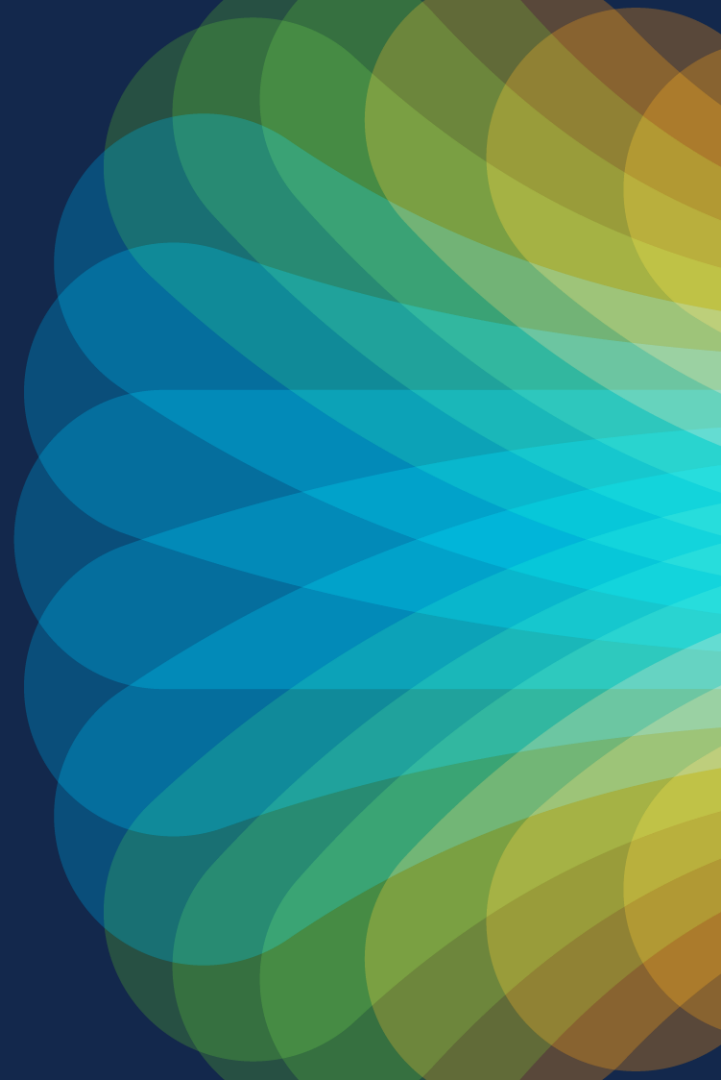
Secure Firewall Management Center



DNS Security Checks in Packet Flow



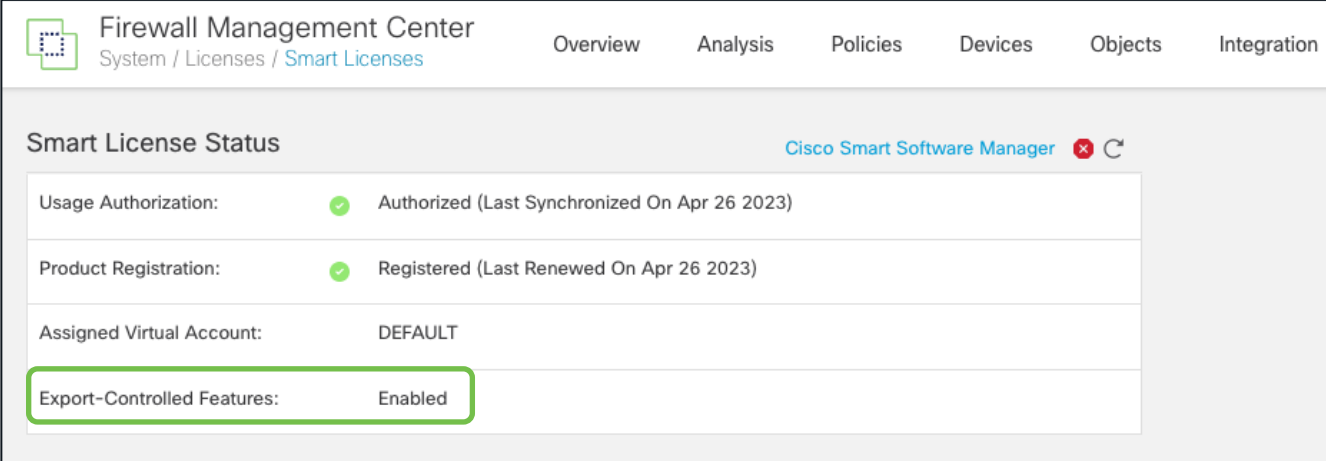
Umbrella DNS Connector Configuration



Prerequisites

Licensing requirements

- Base License enabled with “Export-Controlled Features” on FMC



The screenshot displays the 'Smart License Status' page in the Firewall Management Center. The page header includes the FMC logo, the title 'Firewall Management Center', and a breadcrumb trail 'System / Licenses / Smart Licenses'. Navigation tabs for 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration' are visible. The main content area shows the 'Smart License Status' for 'Cisco Smart Software Manager'. A table lists the following components and their status:

Component	Status
Usage Authorization:	Authorized (Last Synchronized On Apr 26 2023)
Product Registration:	Registered (Last Renewed On Apr 26 2023)
Assigned Virtual Account:	DEFAULT
Export-Controlled Features:	Enabled

- At least Cisco Umbrella DNS Security Essentials package

Additional Requirements

- Management Center has internet connectivity to access Cisco Cloud Services
- FTD is able to resolve and reach api.opendns.com
- Version Details:

Device	Version
Management Center (FMC)	7.2 & Above
Threat Defense (FTD)	6.6.0 & Above

Add Umbrella Root Certificate

Certificate Installation Path: Device > Certificates > Add

Note: Ensure Validation Usage is set as “SSL Server”

The screenshot shows the 'Add Cert Enrollment' configuration window. The 'Name*' field is set to 'Umbrella_CA_Cert'. The 'Description' field is empty. The 'CA Information' tab is selected, showing 'Enrollment Type' as 'Manual'. The 'CA Only' checkbox is checked, with a note: 'Check this option if you do not require an identity certificate to be created from this CA'. The 'CA Certificate' field contains a PEM-formatted certificate. At the bottom, the 'Validation Usage' section has three options: 'IPsec Client' (unchecked), 'SSL Client' (unchecked), and 'SSL Server' (checked and highlighted with a green box).

Add Cert Enrollment

Name*

Umbrella_CA_Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

☒ CA Only
Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIE6jCCA9KgAwIBAgIQCjUI1  
VwpKwF9+K1lwA/35DANBgkq  
hkiG9w0BAQsFADBhMQswCQ  
YDVQQG  
EwJVUzEVMBMGA1UEChMM  
RGlnaUNlcnQgSW5jMRkwFwY  
DVQQLExB3d3cuZGlnaWNlcn  
QuY29tMSAw  
-----END CERTIFICATE-----
```

Validation Usage: ☐ IPsec Client ☐ SSL Client ☒ SSL Server

FMC Configuration

FMC Workflow

1. Configuring Cisco Umbrella Connection



2. Configuring Umbrella DNS Policy



3. Configuring Umbrella DNS Rule



4. Map the policy in Security Intelligence in ACP

1. Configuring Cisco Umbrella Connection

- Navigate to Integrations > Other Integrations > Cloud Services > Cisco Umbrella Connection

- **General Tab**

7 Digit Umbrella organization identifier

Key used by FMC to perform API requests against an Umbrella Org

Secret used by FMC to perform API requests against an Umbrella Org

Token used by the FTD to register and forward the DNS requests.

Connectivity test to Umbrella

Cisco Umbrella Connection

General Advanced

Organization ID*

Network Device Key*

Network Device Secret*

Legacy Network Device Token*

Test Connection

Save

Where are my Umbrella details ?

<https://login.umbrella.com/> ➡ <https://dashboard.umbrella.com/o/<org-id>/>

The screenshot shows the Cisco Umbrella dashboard for API Keys. The left sidebar contains navigation links: Overview, Deployments, Policies, Reporting, Investigate, Admin (highlighted with a green box and labeled 1), Accounts, User Roles, Log Management, Authentication, Bypass Users, Bypass Codes, API Keys (highlighted with a green box and labeled 2), and Licensing. The main content area is titled 'API Keys' and includes a warning about Legacy API keys. Below the warning are four summary cards: API Keys (0), KeyAdmin Keys (0), Static Keys (3), and Legacy Keys (4, highlighted with a green box and labeled 3). At the bottom is a table of API key categories (labeled 4), including Umbrella Network Devices, Legacy Network Devices, Umbrella Reporting, and Umbrella Management, each with a 'Keys' count and a dropdown arrow.

Category	Keys
Umbrella Network Devices	0
Legacy Network Devices	1
Umbrella Reporting	1
Umbrella Management	0

Where are my Umbrella details ?

Reference

Umbrella Network Devices Keys 1

⚠ For security reasons, your secret will only be displayed once. For future reference, copy this secret and keep it in a safe place.

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

Check out the [docs](#)

Key	Secret	Created
a8bcfaca12fc41be8172951cc3ac1b01	1ff76806d2da41b7a9d9acabfcb84352	27 April 2023

Network Device Key

Network Device Secret

REFRESH DELETE

Legacy Network Devices Keys 1

Network Devices may authenticate directly with your Cisco Umbrella account credentials, or they may authenticate using an API token. You can obtain your API token below (all devices under your account use the same token). If you wish to revoke access for your current token, use the "Refresh Token" link to obtain a new one.

Check out the [documentation](#) for

Token	Created
1DB0829B2B7742E7CE975E278D299A1B003F	

Legacy Network Device Token

Umbrella Management Keys 1

⚠ For security reasons, your secret will only be displayed once. For future reference, copy this secret and keep it in a safe place.

The API Key and secret pair enable you to manage the deployment for your different organizations. This includes the management of networks, roaming clients and other core-identity types.

Check out the [documentation](#) for step by step instructions.

Key	Secret	Created
b8e01fe5913c42a0b3648c358ccd6535	210980c238e44290b677753d2ac3ecbe	27 April 2023

Management Key

Management Secret

REFRESH DELETE

2. Configuring Umbrella DNS Policy

- Navigate to Policies > DNS > Add DNS Policy > Umbrella DNS Policy

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Policies' tab is active. On the left, a sidebar lists DNS policies: 'Default DNS Policy' and 'Default Umbrella DNS Policy'. A green circle with the number '2' highlights the 'Default Umbrella DNS Policy'. A modal window titled 'New Umbrella DNS Policy' is open in the center, featuring a 'Name*' field and a 'Description' field. At the bottom of the modal are 'Cancel' and 'Save' buttons. In the background, a table lists existing policies. A green circle with the number '1' highlights the 'Add DNS Policy' button and the 'Umbrella DNS Policy' option in the dropdown menu.

Policy Type	Last Modified
DNS POLICY	2023-04-24 13:07:11 Modified by "admin"
UMBRELLA DNS POLICY	2023-04-27 01:01:43 Modified by "admin"

3. Configuring Umbrella DNS Rule

- New Umbrella DNS Policy created with a predefined Global rule with default values

The screenshot shows the Cisco Umbrella DNS Policy configuration page. The policy name is "FMC Umbrella DNS Policy" and the description is "FMC Umbrella DNS Policy for Branch FTDs". The "Rules" tab is selected, showing a table with one rule. The "Umbrella Protection Policy" is set to "Default Policy" and the "Bypass Domain" is "None". A "Refresh the Umbrella Policy" button is visible in the top right. A "Save" button is also present. A callout points to the edit icon in the bottom right corner of the table, labeled "Editing the Umbrella Policy".

Umbrella DNS Policy Name

Umbrella DNS Policy Description

Refresh the Umbrella Policy

FMC Umbrella DNS Policy

FMC Umbrella DNS Policy for Branch FTDs

Rules

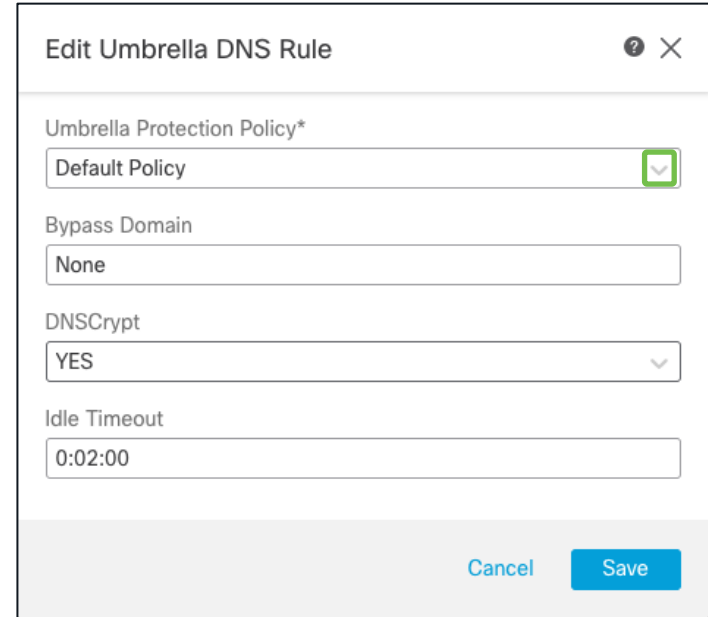
#	Interface Objects	Umbrella Protection Policy	Bypass Domain
1	any	Default Policy	None

Umbrella Protection Policy Last Updated: in 0 seconds [2023-04-26 15:55:18]

Editing the Umbrella Policy

Editing Umbrella global rule

- Umbrella Protection Policy (Mandatory)
 - Name of Cisco Umbrella Policy
- Bypass Domain (Optional)
 - Local domains for which DNS requests bypass Cisco Umbrella
- DNSCrypt (Optional)
 - Encrypt DNS requests sent from the FTD to Cisco Umbrella
- Idle Timeout (Optional)
 - Time taken by FTD to remove a connection from client to Umbrella server if no response from server



The screenshot shows a dialog box titled "Edit Umbrella DNS Rule" with a question mark icon and a close button (X) in the top right corner. The dialog contains four configuration fields:

- Umbrella Protection Policy***: A dropdown menu showing "Default Policy" with a green checkmark icon to its right.
- Bypass Domain**: A text input field containing the word "None".
- DNSCrypt**: A dropdown menu showing "YES" with a downward arrow icon to its right.
- Idle Timeout**: A text input field containing "0:02:00".

At the bottom right of the dialog, there are two buttons: "Cancel" (in blue text) and "Save" (in a blue box).

Editing Umbrella global rule

- DNS Policies retrieved from Umbrella organization account

The screenshot shows the 'Edit Umbrella DNS Rule' page in the FMC Dashboard. The page is titled 'Policies / Management DNS Policies'. It features a list of DNS Policies on the left and a table of policy settings on the right. A callout labeled 'FMC Dashboard' points to the left sidebar. Another callout labeled 'Umbrella Dashboard' points to the main content area.

Umbrella Protection Policy*

- Default Policy
- SampleDNSPolicy
- BranchFTDPolicy
- Default Policy

YES

Idle Timeout

0:02:00

Category Migration Complete.
All legacy content categories have been successfully migrated or your policies did not previously contain any legacy categories. For more information, see [Umbrella's Help](#).

1	Branch FTD Policy	Protection DNS Policy	Applied To 1 Identity	Contains 4 Policy Settings	Last Modified Apr 27, 2023
2	SampleDNSPolicy	Protection DNS Policy	Applied To 0 Identities	Contains 4 Policy Settings	Last Modified Apr 27, 2023
3	Default Policy	Protection DNS Policy	Applied To All Identities	Contains 3 Policy Settings	Last Modified Jul 19, 2020

4. Map the policy in Security Intelligence in ACP

- Navigate to Policies > Access Control> Device ACP > Security Intelligence

The screenshot shows the Cisco ACP interface for configuring Security Intelligence. A green box labeled '1' highlights the 'Security Intelligence' tab in the breadcrumb navigation. An orange callout labeled 'Umbrella DNS Policy' points to the 'Umbrella DNS Policy' dropdown menu. Another orange callout labeled 'Security Intelligence (SI) DNS Policy' points to the 'Default DNS Policy' dropdown menu. A green callout labeled '2' points to the dropdown menu for the 'Umbrella DNS Policy', which is currently set to 'None'. A zoomed-in view of this dropdown menu is shown below, with a green box highlighting the 'FMC Umbrella DNS Policy' option.

Return to Access Control Policy Management

Base ACP

Packets → Prefilter Rules → Decryption → **Security Intelligence** → Identity → Access Control → More

DNS Protection

DNS Protection blocks traffic from known threats by the domain name. Intelligence for these threats is derived from both TALOS and Cisco Umbrella.

DNS Policy

Default DNS Policy

Umbrella DNS Policy

None

Switch to Legacy UI

Analyze Discard Save

Targeted: 1 device

Umbrella DNS Policy

None

None

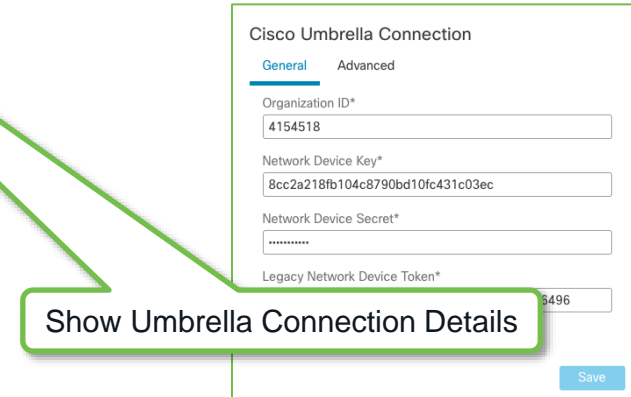
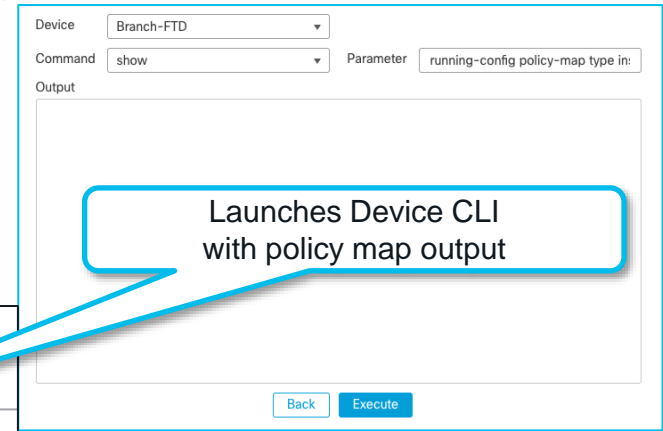
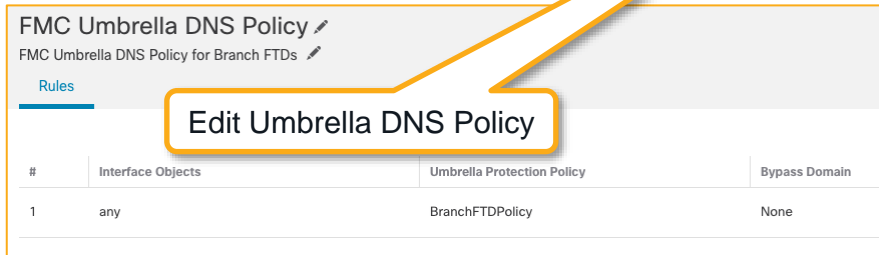
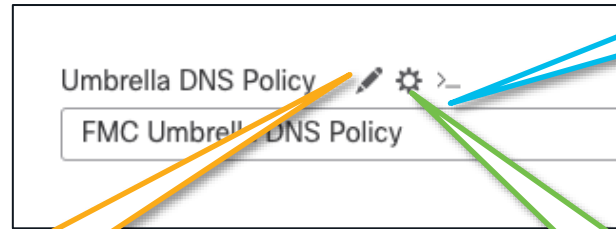
Default Umbrella DNS Policy

FMC Umbrella DNS Policy

Note: Default Umbrella Policy: None

Map the policy in Security Intelligence in ACP

- Umbrella DNS Policy Options



Verification



Verifying FMC Deployment

Navigate to Notifications > Deployments > Show Deployments History

- Verifying Transcript Details for the Umbrella Root CA Certificate Deployment on FTD

Job Name	Deployed by	Start Time
Deploy_Job_7	admin	Apr 26, 2023
Device	Transcript	Preview
Branch-FTD	Completed	
Certificate_Job_1	System	Apr 26, 2023
Device	Transcript	Preview
Branch-FTD	Completed	
Deploy_Job_6	admin	Apr 26, 2023
Device	Transcript	Preview
Branch-FTD	Completed	

Transcript Details

```
FMC >> crypto ca trustpoint Umbrella_CA_Cert
FMC >> enrollment terminal
FMC >> no subject-name
FMC >> revocation-check none
FMC >> keypair <Default-RSA-Key>
FMC >> no serial-number
FMC >> no ignore-ipsec-keyusage
FMC >> no fqdn
FMC >> no ip-address
FMC >> no subject-name
FMC >> validation-usage ssl-server
FMC >> exit
FMC >> crypto ca authenticate Umbrella_CA_Cert nointeractive
Branch-FTD >> [info] : Enter the certificate in base64 representation...
End with the word "quit" on a line by itself.
```

Close

Verifying FMC Deployment

Navigate to Notifications > Deployments > Show Deployments History

- Verifying Transcript Details for the Umbrella Configuration Deployment on FTD

Job Name	Deployed by	Start Time
Deploy_Job_7	admin	Apr 26, 2023
Device	Transcript	Preview
Branch-FTD	Completed	
Certificate_Job_1	System	Apr 26, 2023
Device	Transcript	Preview
Branch-FTD	Completed	
Deploy_Job_6	admin	Apr 26, 2023
Device	Transcript	Preview
Branch-FTD	Completed	

Transcript Details

FMC >> no strong-encryption-disable
FMC >> umbrella-global
FMC >> token 1DB0829B2B7742E7CE975E278D299A1B003F6496
Branch-FTD >> [info] : Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

FMC >> local-domain-bypass "None"
FMC >> exit
FMC >> policy-map type inspect dns preset_dns_map
FMC >> parameters
FMC >> umbrella tag BranchFTDPolicy
FMC >> dns crypt
FMC >> no dp-tcp-proxy

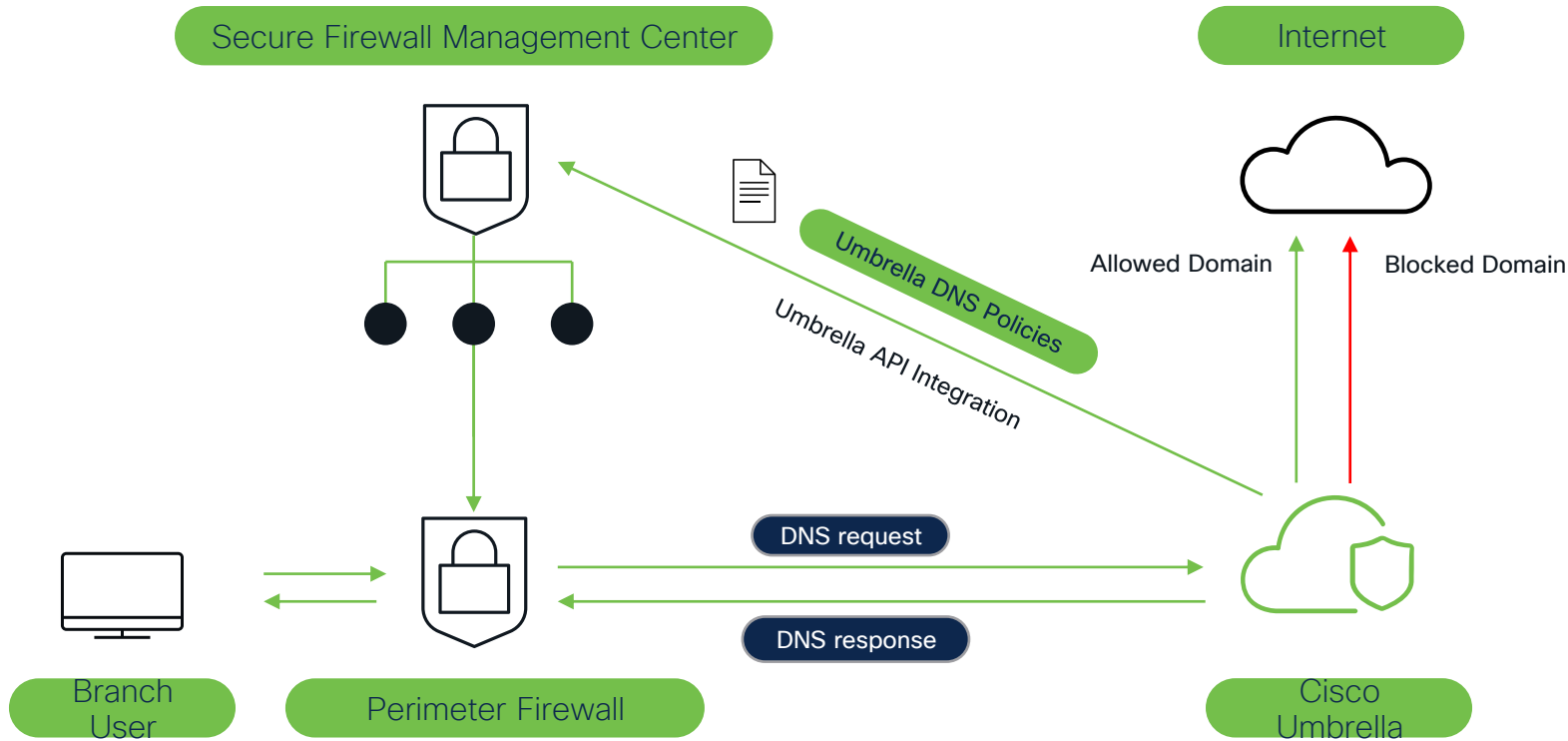
[Close](#)

Demo: Umbrella DNS Connector

In this Demo, we will

- Configure Cisco Umbrella Connection
- Configure Umbrella DNS Policy and Rule
- Map the Umbrella DNS Policy in ACP
- **Block** DNS traffic to www.twitch.tv

Demo Topology



Umbrella SASE Auto Tunnel

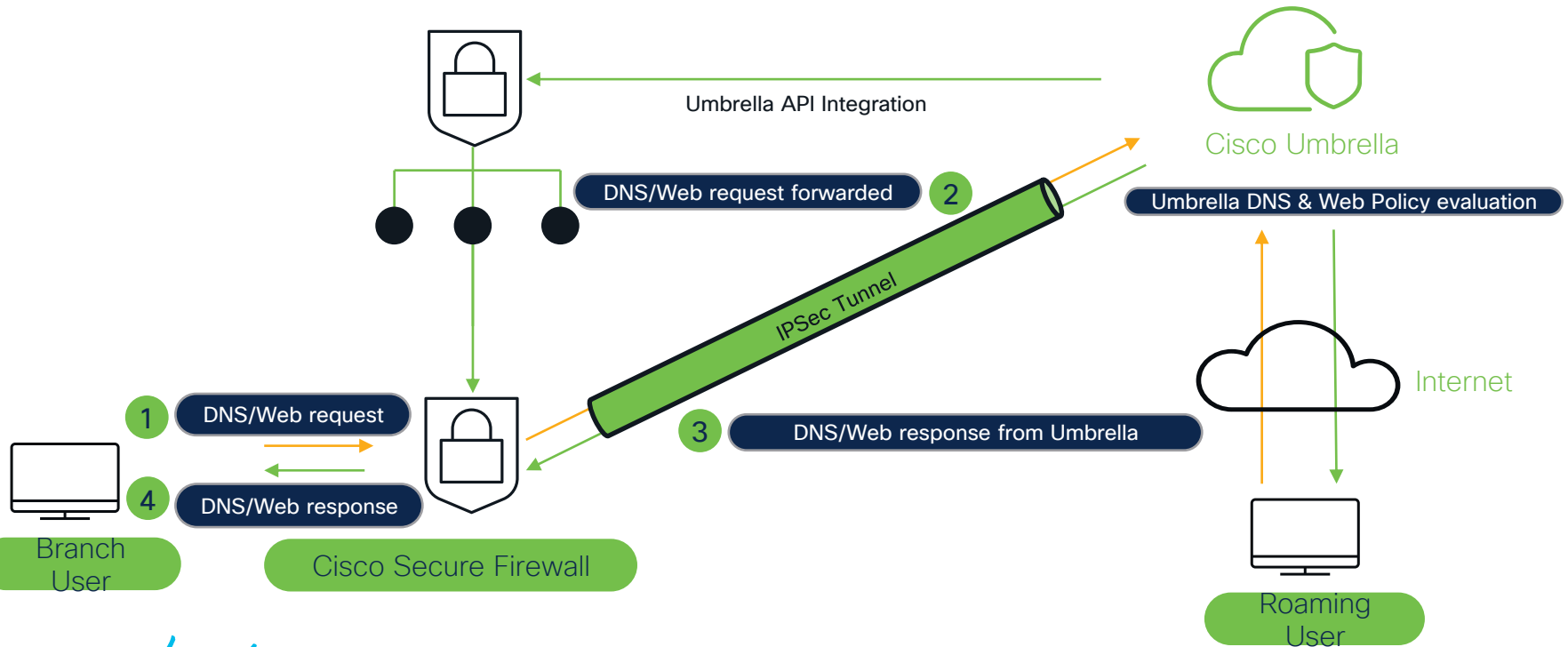


Umbrella SIG Key Features

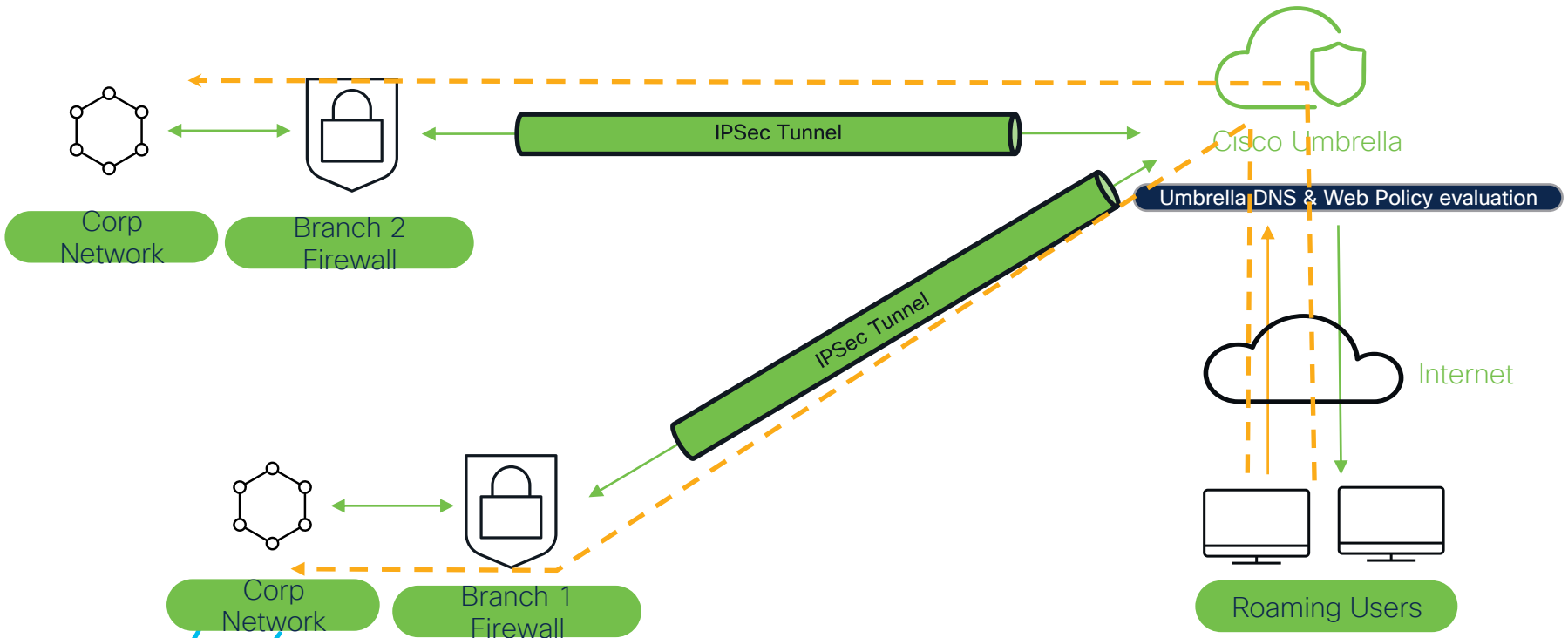
- DNS Security
- Cloud delivered firewall
- Cloud access security broker (CASB)

How does it work?

Secure Firewall Management Center



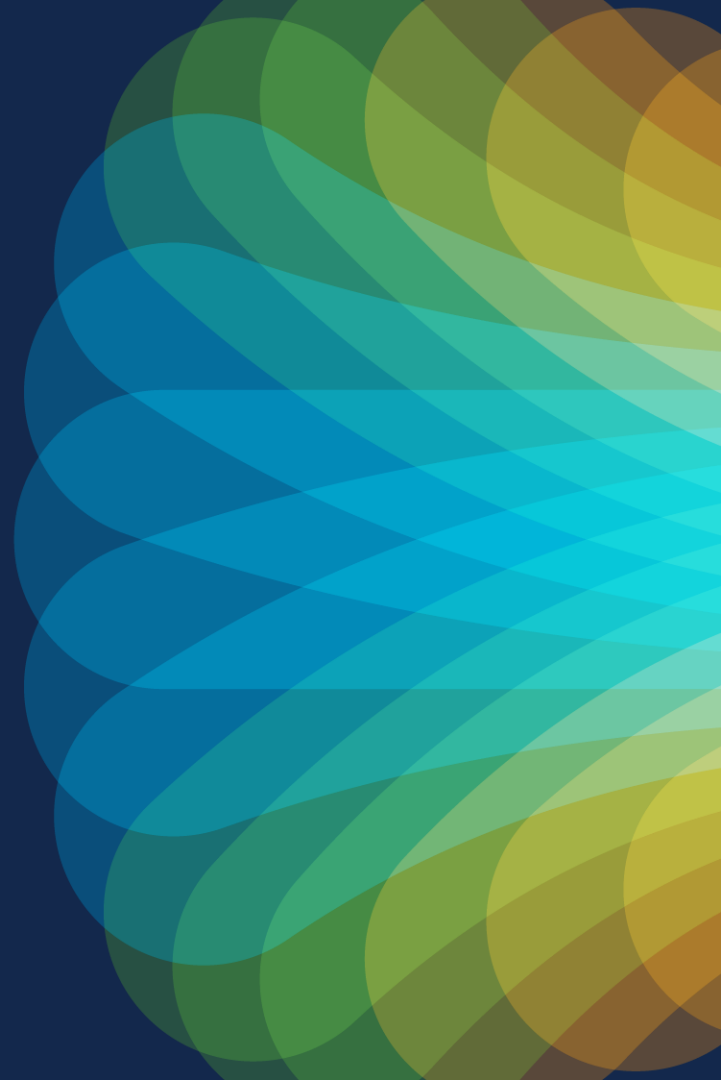
Secure Access Use Case



Benefits

- Minimal Configuration
- Automatic Network Tunnel Configuration on Umbrella
- Multi-layered DNS & Web Security
- Eliminates the need for advanced NGFW features e.g. URL filtering & TLS Decryption
- Improved Internet Performance
- Uniform Security policy for Hybrid workers

Umbrella SASE Auto Tunnel Configuration



Prerequisites

Prerequisites

- Base License enabled with “Export-Controlled Features” on FMC
- Cisco Umbrella SIG Essentials subscription or Free SIG Trial
 - One Umbrella Account per FMC (an HA pair uses one account)
- Version Details:

Device	Version
Management Center (FMC)	7.3 & Above*
Threat Defense (FTD)	7.1.0 & Above

* Manual tunnel configuration on FMC and Umbrella dashboard for version 7.3 and below

Prerequisites

- Umbrella integration on FMC under “Cisco Umbrella Connection”
 - Valid Management Key and Secret keys **mandatory**
- FMC can reach management.api.umbrella.com
- FTD supporting Route-Based VPN with Local Tunnel ID support (Version 7.1.0 and above)

Configuring Cisco Umbrella Connection

- Navigate to Integrations > Other Integrations > Cloud Services > Cisco Umbrella Connection
- **Advanced Tab**

32-byte hex public key of Umbrella servers for certificate validation

A key to fetch datacenter details from Umbrella cloud for VPN policy

A secret used to fetch datacenters from Umbrella cloud for VPN Policy

The screenshot shows the 'Cisco Umbrella Connection' configuration interface. At the top, there are two tabs: 'General' and 'Advanced'. The 'Advanced' tab is selected and highlighted with a green box. Below the tabs, there are three input fields, each with a label and a green callout box pointing to it from the left. The first field is labeled 'DNSCrypt Public Key' and is associated with the callout '32-byte hex public key of Umbrella servers for certificate validation'. The second field is labeled 'Management Key' and is associated with the callout 'A key to fetch datacenter details from Umbrella cloud for VPN policy'. The third field is labeled 'Management Secret' and is associated with the callout 'A secret used to fetch datacenters from Umbrella cloud for VPN Policy'. At the bottom of the form, there is a 'Test Connection' button and a 'Save' button.

Cisco Umbrella Connection

General **Advanced**

DNSCrypt Public Key

Management Key

Management Secret

Test Connection

Save

FMC Configuration

FMC Workflow

1. Create SASE Topology

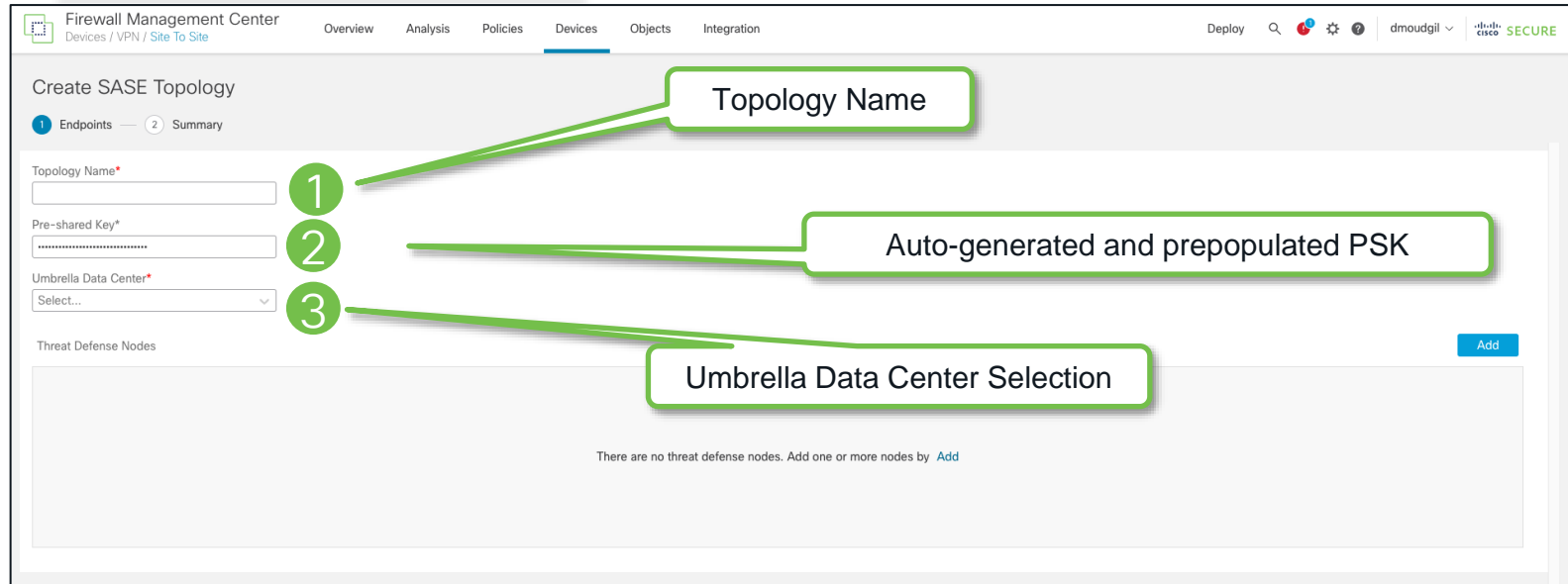
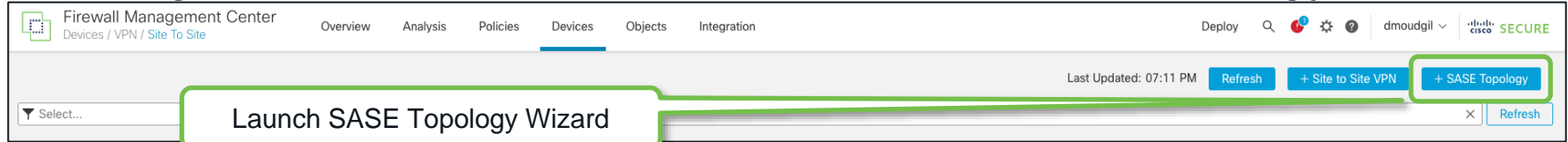
2. Select Umbrella DC

3. Add FTD nodes as Endpoint

4. Create VPN Interface

1. Create SASE Topology

- Navigate to Devices > VPN > Site to Site > SASE Topology



2. Select Umbrella DC

- Umbrella Data Centers auto populated with region and IP addresses
 - Reducing admin overhead to configure manually
- Pre-shared key auto-generated as per Umbrella PSK requirements
 - Admin override allowed
 - Common for all FTD endpoints and Umbrella for a topology

Create SASE Topology

1

Endpoints

2

Summary

Topology Name*

VPN-MumbaiUmbrella

Pre-shared Key*

.....

Umbrella Data Center*

Select...

Europe - Madrid(146.112.106.8)

Europe - Marseille(146.112.120.2)

Asia - Tokyo(146.112.112.8)

Asia - Singapore(146.112.113.8)

Asia - Hong Kong(146.112.114.8)

Asia - Mumbai(146.112.117.8)

Australia - Melbourne(146.112.119.8)

Australia - Sydney(146.112.118.8)

North America - Ashburn(146.112.82.8)

North America - Atlanta(146.112.85.8)

3. Add FTD nodes as Endpoint

- Configuring FTD as Endpoint in SASE Topology

Create SASE Topology

1 Endpoints — 2 Summary

Topology Name*

VPN-MumbaiUmbrella

Pre-shared Key*

Umbrella Data Center*

Asia - Mumbai(146.112.117.8) ▾

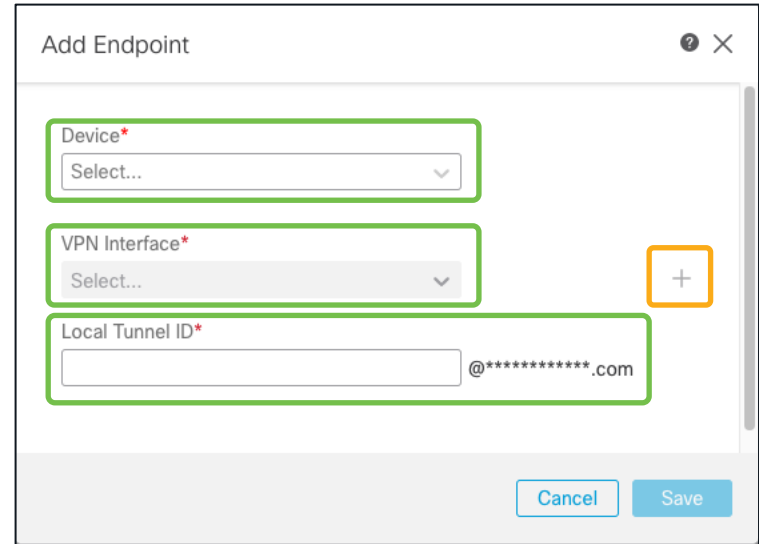
Threat Defense Nodes

Add

There are no threat defense nodes. Add one or more nodes by [Add](#)

3. Add FTD nodes as Endpoint

- Device
 - Interface with name “**outside**” or “**outside***” for egress interfaces
 - DHCP or Static IP assignment
- VPN Interface
 - VTI Interface with default params
- Local Tunnel ID
 - Customizable Tunnel ID for FTD to be deployed on Umbrella via FMC
 - Format: **<prefix>@<umbrella-generated-ID>-umbrella.com**



4. Create VPN Interface (SVTI)

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
☒ Static ☐ Dynamic

Name:*
Outside_static_vti_1

☒ Enabled

Description:

Security Zone:
Outside

Priority:
0 (0 - 65535)

Virtual Tunnel Interface Details
An interface named Tunnel-ID is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*
1 (0 - 10413)

Tunnel Source:*
TenGigabitEthernet0/0 (Outside) 172.16.2.10

IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☒ Configure IP 169.254.2.1/30
☐ Borrow IP (IP unnumbered) Select Interface +

Cancel OK

Tunnel type as **Static** by default

VTI Logical name:
< tunnel_source interface logical name > + static_vti + < Tunnel ID >

Tunnel **Enabled** by default

Security Zone configured by default

Unused unique Tunnel ID on FTD by default

Tunnel Source Interface: Auto-populated with interface named as/prefixed with "outside"

IPSec Tunnel Mode set to IPv4 by default

Picks unused IP from the IP range 169.254.X.X/30

Review Encryption Parameters

Reference

The screenshot shows the 'Create SASE Topology' interface with two tabs: 'Endpoints' and 'Summary'. The 'Endpoints' tab is active, showing a list of endpoints and threat defense nodes. A green box highlights the 'Endpoints' section, which includes details for the 'Umbrella Data Center' (Continent: Asia, Data Center: Mumbai, IP Address: 146.112.117.8). Another green box highlights the 'Encryption Settings' section, which includes details for 'Encryption Policies' (Umbrella-AES-GCM-256 [AES-GCM-256]), 'Authentication Type' (Pre-shared Key), and 'IKEv2 IPsec Transform sets' (Umbrella-AES-GCM-256 [AES-GCM-256]). A yellow box highlights the 'Sequence of Steps' section, which lists: 1. Saves SASE Topology, 2. Deployment to Umbrella, 3. Deployment to FTD endpoint(s). A green box highlights the 'Triggers deployment to FTD only after Umbrella deployment is successful' section, which includes a checkbox labeled 'Deploy configuration on threat defense nodes' (checked). A yellow box highlights the 'Save' button at the bottom right.

Create SASE Topology

1 Endpoints — 2 Summary

Endpoints

Umbrella Data Center

Continent Asia

Data Center Mumbai

IP Address 146.112.117.8

Threat Defense Nodes

Device

Branch-FTD

Encryption Settings

Encryption Settings

IKEv2 Policies Umbrella-AES-GCM-256 [AES-GCM-256]

Authentication Type Pre-shared Key

IKEv2 IPsec Transform sets Umbrella-AES-GCM-256 [AES-GCM-256]

Sequence of Steps:

1. Saves SASE Topology
2. Deployment to Umbrella
3. Deployment to FTD endpoint(s)

Triggers deployment to FTD only after Umbrella deployment is successful

☒ Deploy configuration on threat defense nodes

Cancel Back Save

SASE Topology Summary

Cisco Umbrella Configuration

Topology Name: VPN-MumbaiUmbrella
Primary Data Center: Asia-Mumbai
DC IP Address: 146.112.117.8
Start Time: Apr 27, 2023 7:02 PM
Completion Time: 0%
0 Completed 0 Failure

Tunnel Configuration Status

Device
Branch-FTD

Cisco Umbrella Configuration

Topology Name: VPN-MumbaiUmbrella
Primary Data Center: Asia-Mumbai
DC IP Address: 146.112.117.8
Start Time: Apr 27, 2023 7:02 PM
Completion Time: Apr 27, 2023 7:02 PM
100%
1 Completed 0 Failure

Tunnel Configuration Status

Device	Status	Transcript
Branch-FTD	SUCCESS	

Status of Umbrella Deployment: 0 %

Status of Umbrella Deployment: 100%

Cisco Umbrella Configuration

Topology Name: VPN-MumbaiUmbrella
Primary Data Center: Asia-Mumbai
DC IP Address: 146.112.117.8
Start Time: Apr 27, 2023 7:02 PM
Completion Time: Apr 27, 2023 7:02 PM
100%
1 Completed 0 Failure

Tunnel Configuration Status

Device	Status	Transcript
Branch-FTD	SUCCESS	

Transcript Details

POST https://management.api.umbrella.com/v1/organizations/4154518/tunnels HTTP/1.1

Request JSON: {"deviceType":"other","authentication":{"type":"PSK","parameters":{"idPrefix":"FTDvChandigarh","secret":"*****"},"name":"VPN-MumbaiUmbre-Branch-FTD-4294999380"}

Response JSON: {"organizationId":"4154518","transport":{"protocol":"IPSec"},"serviceType":"SIG","client":{"deviceType":"other","authentication":{"type":"PSK","parameters":{"id":"FTDvChandigarh@4154518-605493704-umbrella.com","secret":"*****"},"createdat":"2023-04-27T19:02:44.358642189Z","modifiedat":"2023-04-27T19:02:44.358642189Z","uri":"/v1/organizations/4154518/tunnels","id":"605493704","name":"VPN-MumbaiUmbre-Branch-FTD-4294999380"}

Close

Umbrella Deployment Transcript

SASE Topology Summary

Direct cross launch to Umbrella Dashboard Network Tunnels Section

Cisco Umbrella Configuration

Topology Name: VPN-MumbaiUmbrella

Primary Data Center: Asia-Mumbai

DC IP Address: 146.112.117.8

Start Time: Apr 27, 2023 7:02 PM

Completion Time: Apr 27, 2023 7:02 PM

100%

1 Completed

0 Failure

Tunnel Configuration Status

Device

Status

Transcript

Branch-FTD

SUCCESS

Umbrella Dashboard

Close

Cisco Umbrella

Overview

Deployments

Core Identities

Network Tunnels

Policies

Reporting

Investigate

Admin

Dinesh Moudgil

Dinesh Moudgil (Cisco)

Documentation

Support Platform

Learning Center

Cisco Online Privacy Statement

Terms Of Service

© Cisco Systems

Deployments / Core Identities

Network Tunnels

To create a tunnel, you must choose a Tunnel ID and Passphrase. A unique set of credentials must be used for each tunnel. For more information, see [Network Tunnel Configuration](#).

Active Tunnels

Inactive Tunnels

Unestablished Tunnels

Unknown Tunnel Status

Data Center Locations

FILTERS

Search tunnels by name

Tunnel Name

Site

Data Center Location

Device Public IP

Tunnel Status

Last Status Update

Umbrella-SIG-Tu-vFTD-TOKYO...

Default Site

Tokyo, Japan

54.248.32.213

Active

Apr 28, 2023 - 00:44

VPN-MumbaiUmbre-Branch-F...

Default Site

Mumbai, Maharashtra - India

52.220.252.135

Active

Apr 28, 2023 - 00:44

Secure Internet Access

Results per page: 50

1-2 of 2

SASE Topology Summary

Direct quick launch to Umbrella Dashboard Network Tunnels Section

Tunnel Name	Site	Data Center Location	Device Public IP	Tunnel Status	Last Status Update	
VPN-MumbaiUmbre-Branch-F...	Default Site	Mumbai, Maharashtra - India	52.220.252.135	Active	Apr 28, 2023 - 00:44	...
Secure Internet Access						

Tunnel Name	Site	Data Center Location	Device Public IP	Tunnel Status	Last Status Update	
VPN-MumbaiUmbre-Branch-F...	Default Site	Mumbai, Maharashtra - India	52.220.252.135	Active	Apr 28, 2023 - 00:44	...
Secure Internet Access						

Tunnel ID	Device Type	Data Center IP
FTDvChandigarh@4154518-605493704-umbrella.com	other	146.112.117.8

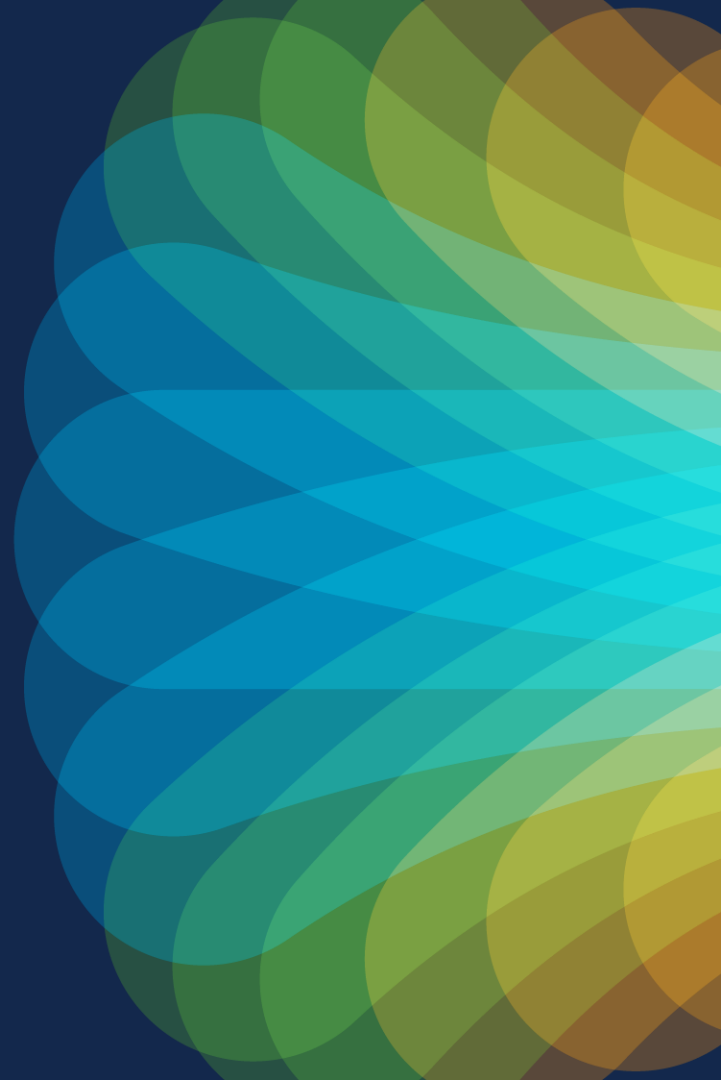
Total Network Traffic						
Traffic Data Initialized	Packets In	Bytes In	Idle Time In	Packets Out	Bytes Out	Idle Time Out
Apr 28, 2023 - 00:44	0	0 B	0 sec	0	0 B	0 sec

IPsec						
State	Age	Integrity Algorithm	Encryption Algorithm	Key Size	SPI In	SPI Out
Installed	376 sec	-	AES_GCM_16	256	c6fab471	688202e9

IKE						
Key Exchange Status	Age	PRF Algorithm	Encryption Algorithm	DH Group	Initiator SPI	Responder SPI
Established	376 sec	PRF_HMAC_SHA2_256	AES_GCM_16	ECP_384	954b31b65d38b1c9	e88a71ca0aca42f8

Results per page: 50 1-2 of 2

Verification



Deployment Task Notifications

Navigate to Notifications > Tasks

Reference

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deployments Upgrades Health **Tasks**

20+ total 0 waiting 0 running 0 retrying 20+ success 0 failures

Filter

Task	Status	Duration
Policy Deployment Policy Deployment to Branch-FTD. Applied successfully	Success	36s
Policy Pre-Deployment Pre-deploy Device Configuration for Branch-FTD success	Success	1s
Policy Pre-Deployment Pre-deploy Global Configuration Generation success	Success	3s
Umbrella Tunnel Deployment Umbrella Tunnel deployment for Site to Site VPN VPN-MumbaiUmbrella has succeeded	Success	9s

Remove completed tasks

Viewing 1-1 of 1

Umbrella Auto SASE Tunnel Status

Navigate to Devices > VPN > Site To Site

Reference

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ dmdougil ✓ cisco SECURE

Last Updated: 12:56 AM Refresh + Site to Site VPN + SASE Topology

Select...

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> VPN-MumbaiUmbrella	Route Based (VTI)	SASE	1 - Tunnels	✓	✓

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ dmdougil ✓ cisco SECURE

Edit SASE Topology

1 Endpoints 2 Summary

Topology Name*
VPN-MumbaiUmbrella

Pre-shared Key*
.....

Umbrella Data Center*
Asia - Mumbai(146.112.117.8)

Threat Defense Nodes

Device	VPN Interface	Local Tunnel ID
Branch-FTD	Outside_static_vti_1	FTDvChandigarh@4154518-605493704-umbrella.com

Local Tunnel ID Updated after deployment to Umbrella

Site to Site VPN Dashboard

Navigate to Overview > Dashboard > Site to Site VPN

Reference

The screenshot displays the Site to Site VPN Dashboard. At the top, there is a table with columns: Node A, Node B, Topology, Status, and Last Updated. The table contains one entry: Asia-Mumbai (VPN IP: 146.112.117.8) connected to NGFWBR1 (VPN IP: 172.16.2.10) via the VPN-MumbaiUmbrella topology, which is Active and last updated on 2023-05-31 09:30:13.

Below the table, a diagram shows the connection between Node A (Asia-Mumbai) and Node B (NGFWBR1). A green box highlights the Asia-Mumbai node, and a button labeled "View full information" is shown.

On the right side, a detailed view of the Asia-Mumbai VPN connection is displayed. The view includes tabs for General, CLI Details, and Packet Tracer. The General tab is selected, showing a summary of the connection. The summary includes the following information:

- Node A (146.112.117.8/0)** and **Node B (172.16.2.10/4500)**
- Transmitted:** 0 (0 B) and **Received:** 19.23 KB (19692 B)
- Received:** 0 (0 B) and **Transmitted:** 1.2 MB (1262108 B)
- Ipssec Security Associations (1)**
- Settings:** L2L Tunnel, NAT...
- Info is not available for Extranet device**
- Encaps/Encrypt:** 255 / 255 pkts
- Decaps/Decrypt:** 964 / 964 pkts
- Remaining Lifetime for SPI ID: 0x060EB27F**
- Info is not available for Extranet device**
- Inbound:** 3.99 GB (4284226000 B) and **Outbound:** 4.03 GB (4331500000 B)
- Remaining Lifetime for SPI ID: 0xC08DB8C48**
- Inbound:** No data and **Outbound:** 4.03 GB (4331500000 B)
- NGFWBR1 (VPN Interface IP: 172.16.2.10)**
- Session Type: LAN-to-LAN Detailed**
- Connection:** 146.112.117.8
- Index:** 63
- IP Addr:** 146.112
- Protocol:** IKEv2 IPsecOverNatT
- Encryption:** IKEv2: (1)AES-GCM-256 IPsecOverNatT: (1)AES
- Hashing:** IKEv2: (1)none IPsecOverNatT: (1)none
- Bytes Tx:** 19692 and **Bytes Rx:** 1262108
- Login Time:** 13:28:37 UTC Wed May 31 2023
- Duration:** 0h:13m:07s
- Tunnel Zone:** 0

Routing Configuration

Static Route to VTI Next Hop

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	Outside_static_vti_1	Global	Host_169.254.2.2	false	10	
any-ipv4	Outside	Global	172.16.2.1	false	1	

ACL for DNS & Web Traffic

Edit Extended Access List Object

Name

Entries (1)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	SGT
1	Allow	Host_172.16.3.153	Any	Any	DNS_over_TCP HTTP HTTPS DNS_over_UDP	Any	Any

Policy Based Routing

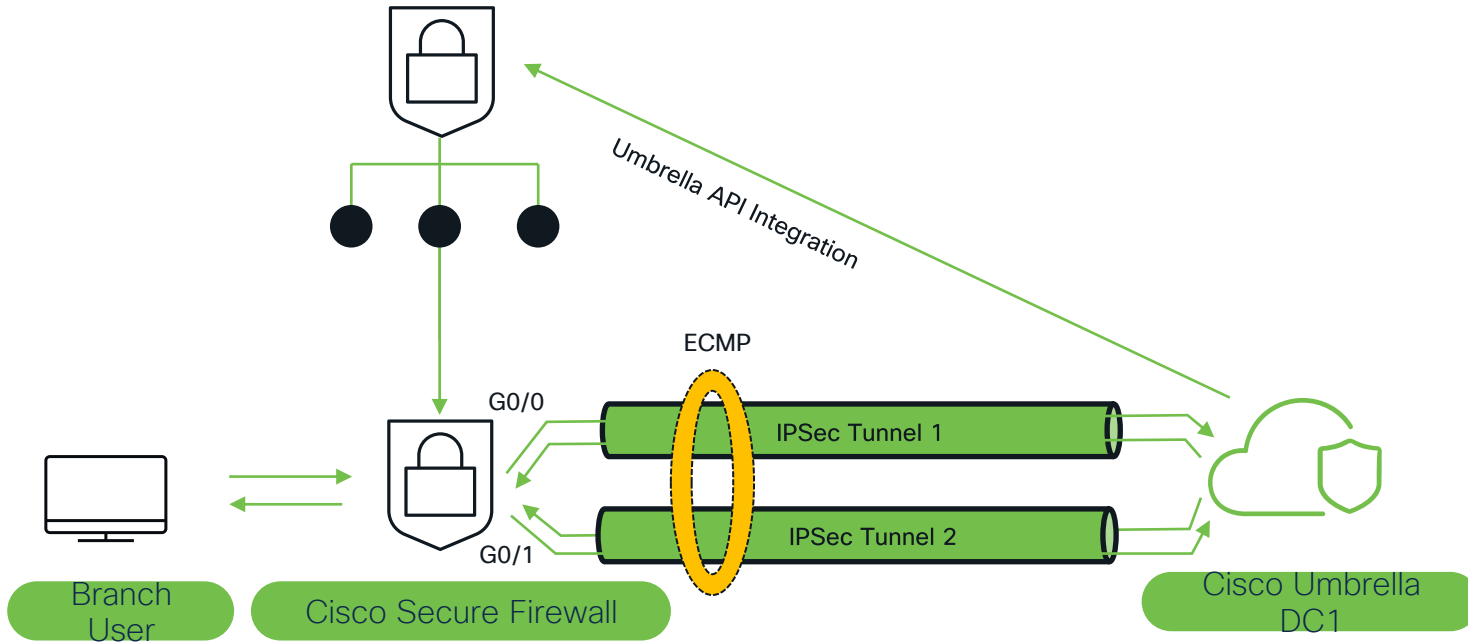
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interface

Policy Routing using SASE Tunnel

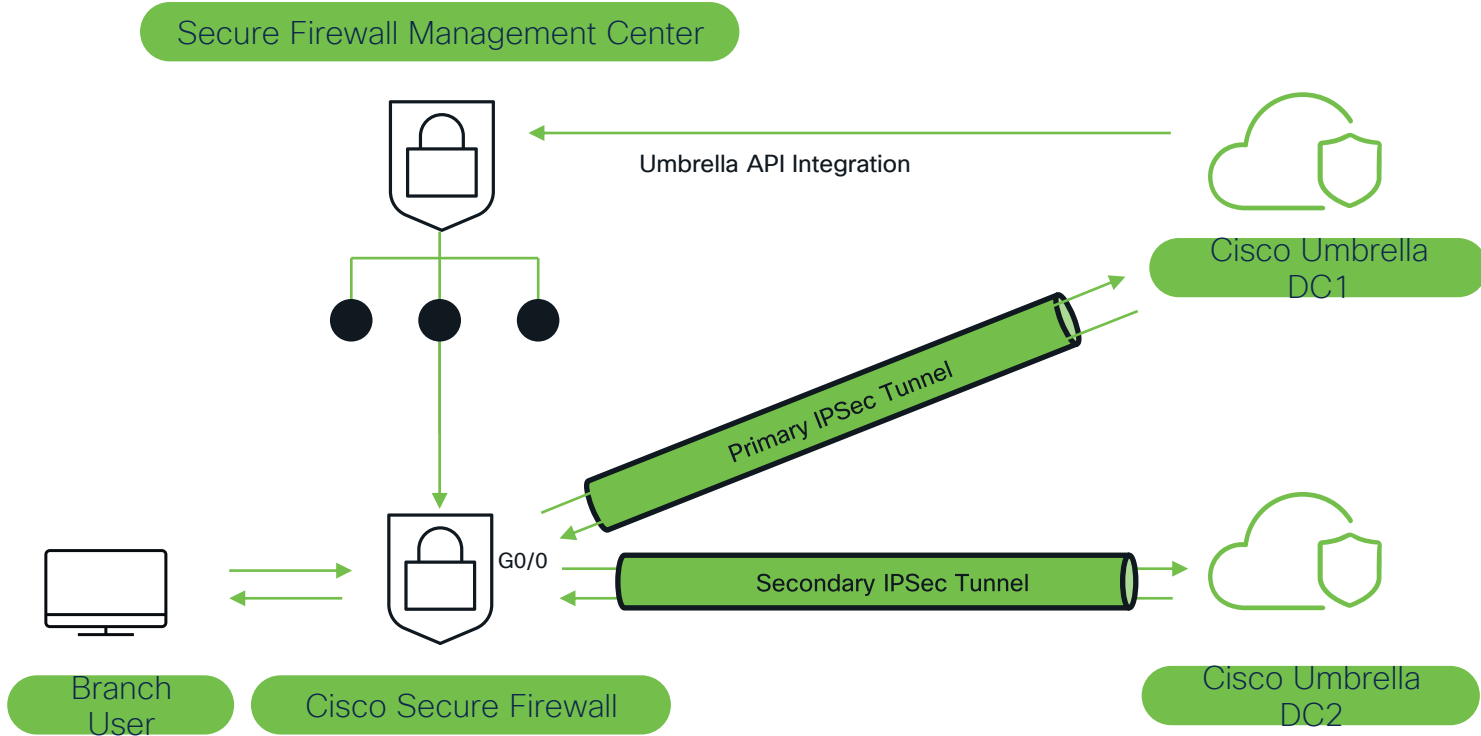
Ingress Interfaces	Match criteria and forward action
Inside	<div data-bbox="705 911 1284 966">If traffic matches the Access List Lan_To_Internet</div> <div data-bbox="1304 911 1584 966">Send through <input type="text" value="#0"/> Outside_static_vti_1</div>

FTD Level SASE Tunnel Redundancy

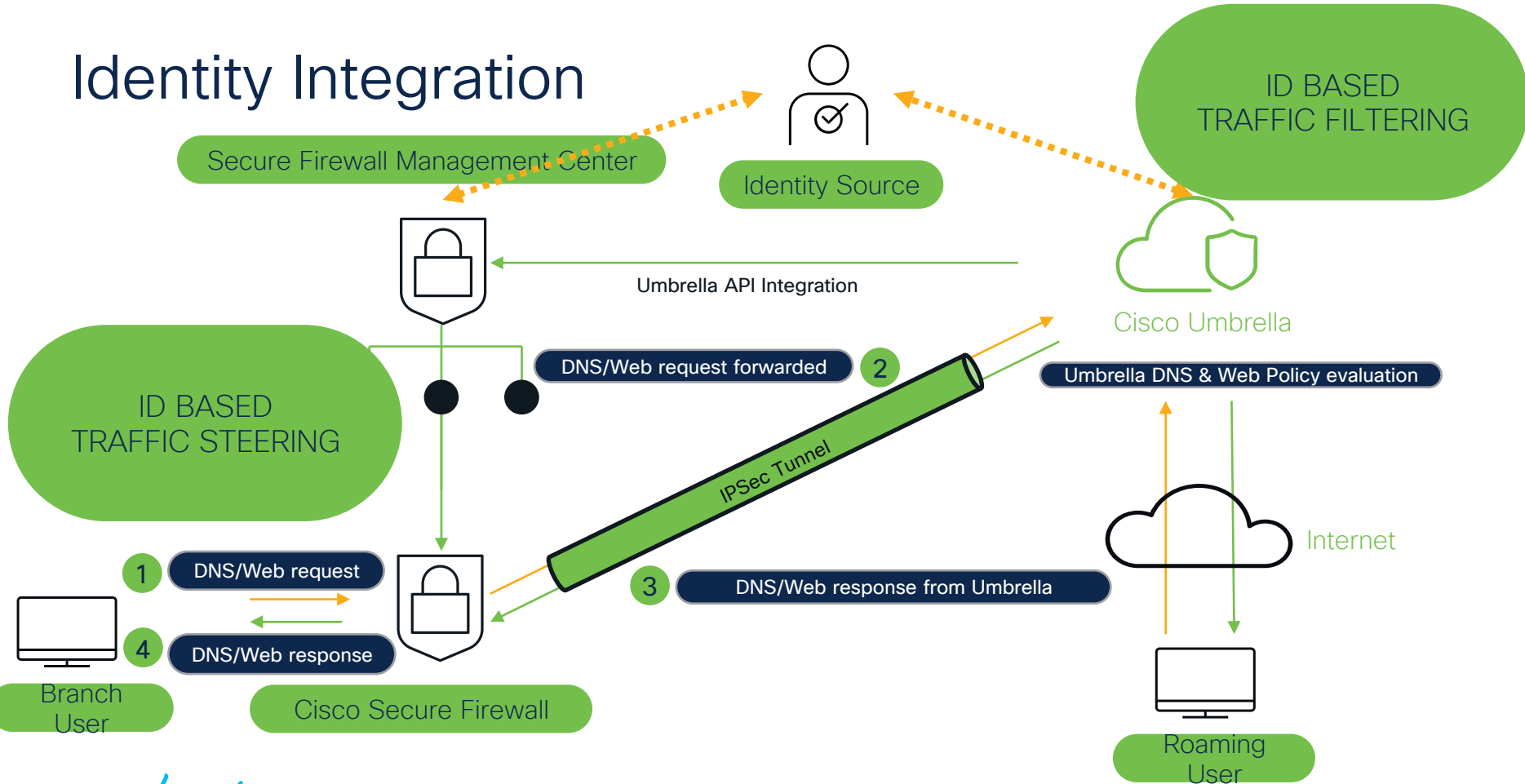
Secure Firewall Management Center



Umbrella Level SASE Tunnel Redundancy



Identity Integration

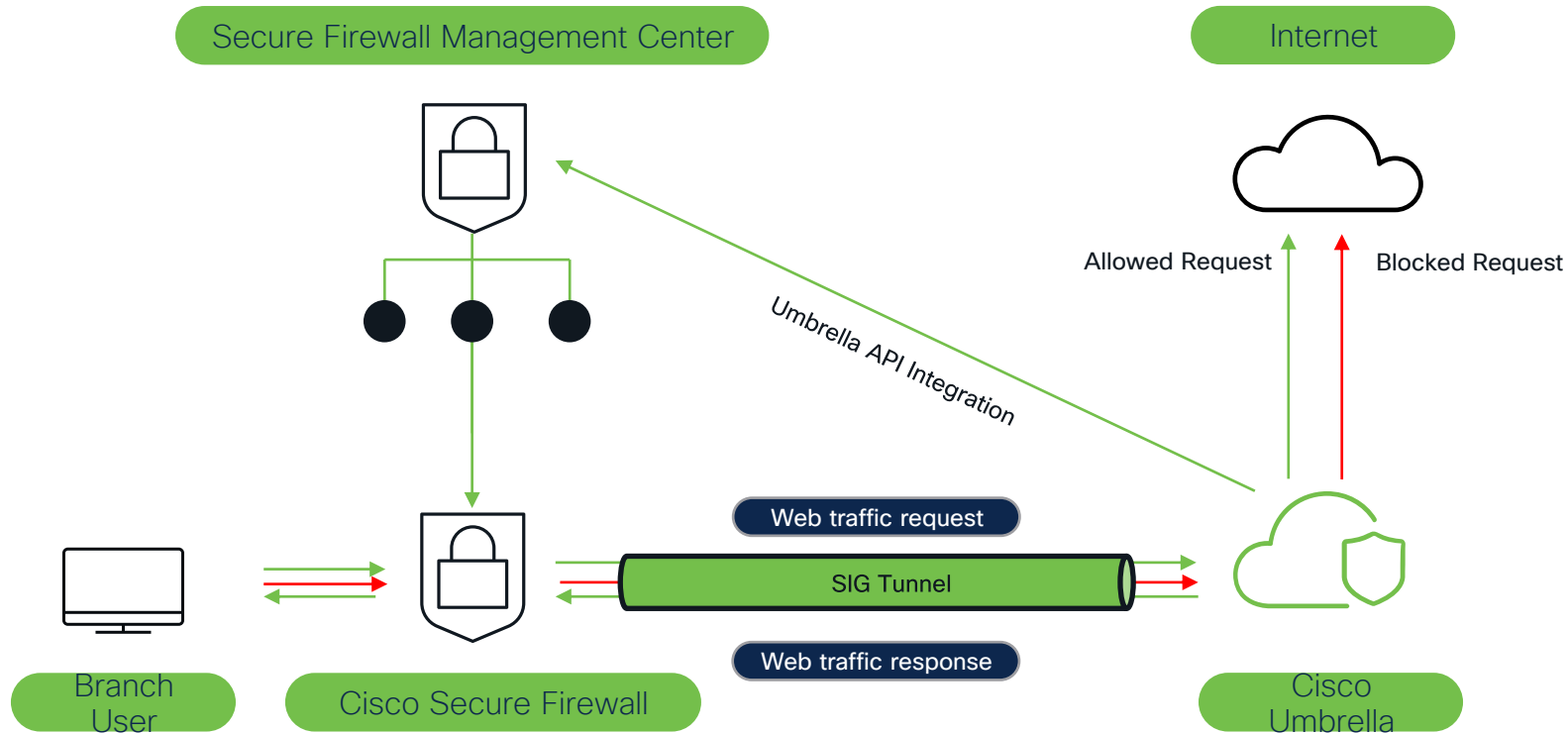


Demo: Umbrella Auto SASE Tunnel

In this Demo, we will

- Configure Umbrella Auto SASE Tunnel
- Initiate traffic from the user workstation to verify
 - Traffic to Gambling and Streaming websites is **blocked**
 - Traffic to the Cisco website is **allowed**

Demo Topology



Best Practices



Best Practices

- Base License enabled with “Export-Controlled Features” on FMC
- Umbrella Root Certificate properly installed on FTD for DNS Connector
- Umbrella Protection Policy name does not contain any spaces
- FTD internet-facing interfaces are recommended to be named/prefixed with **outside**
- Do not edit/delete SASE topology if deployment to Umbrella running for that topology

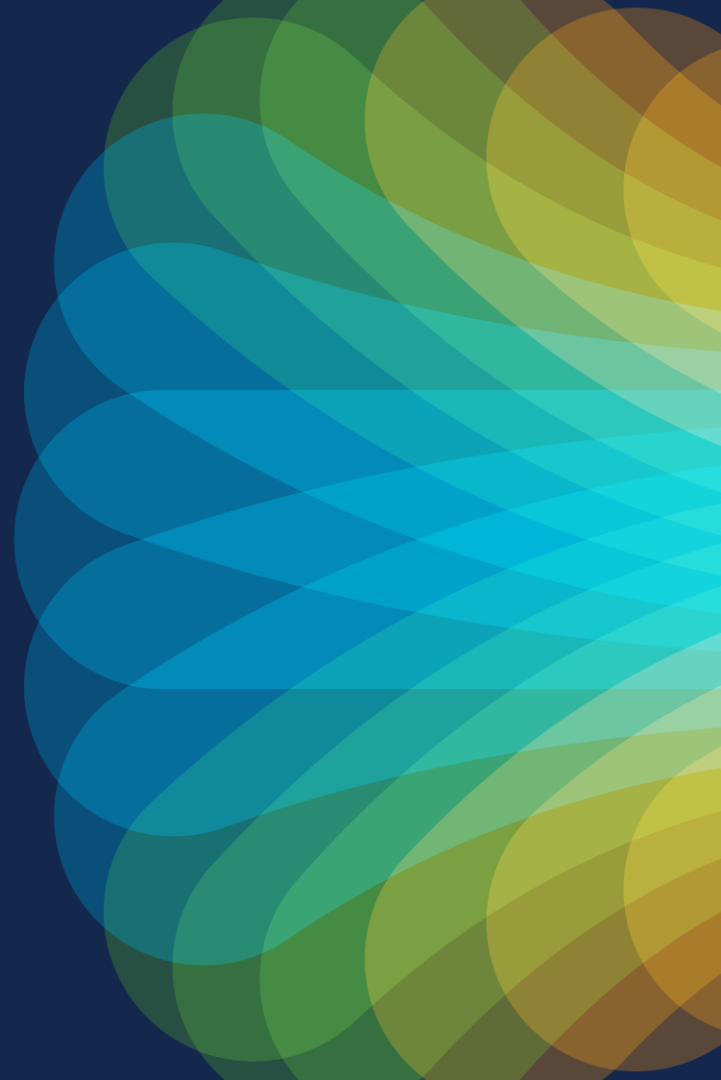
Helpful Debug Commands*

Reference

Commands	Description
<code>debug crypto condition peer <peer-IP></code>	Enabling conditional debugging for a particular peer
<code>debug vti 255</code>	Debug the Virtual Tunnel Interface information
<code>debug crypto ikev2 protocol 255</code>	Debug the ikev2 protocol related transactions
<code>debug crypto ikev2 platform 255</code>	Debug the ikev2 platform related transactions
<code>debug crypto ike-common 255</code>	Debug the common IKE related transactions
<code>debug crypto ipsec 255</code>	Debug the IPSec related transactions

* **Note:** Debugs can be resource intensive. Run them with caution, especially in production.

Conclusion



Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

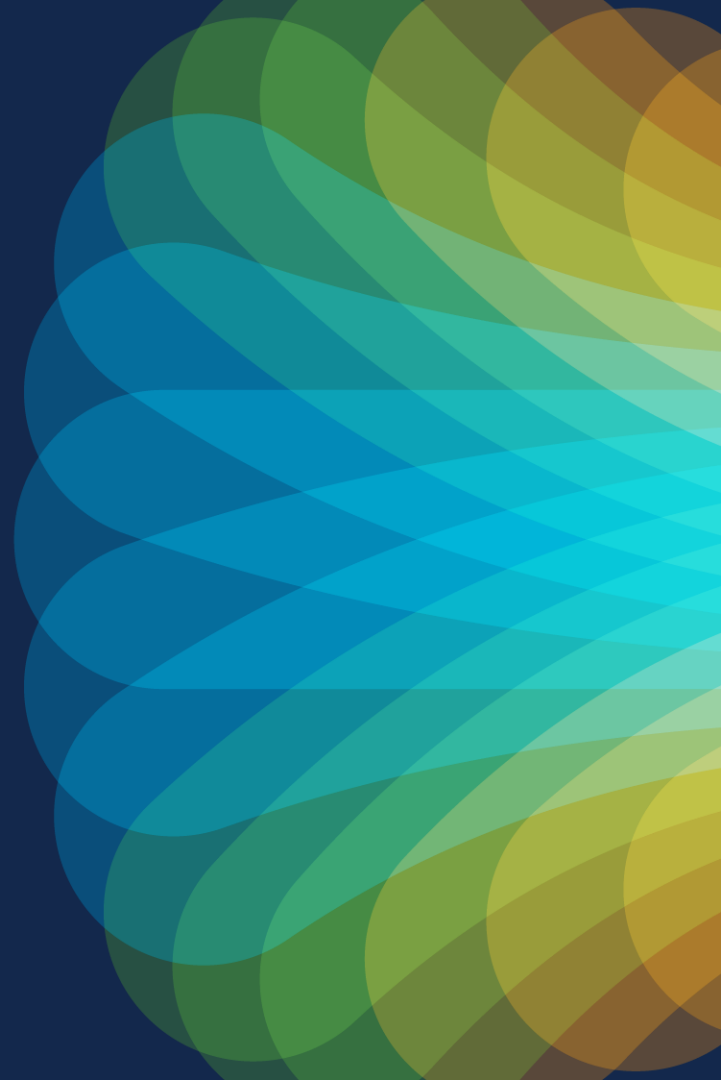


The bridge to possible

Thank you



#CiscoLive



The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy bands of color in shades of orange, red, and yellow. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

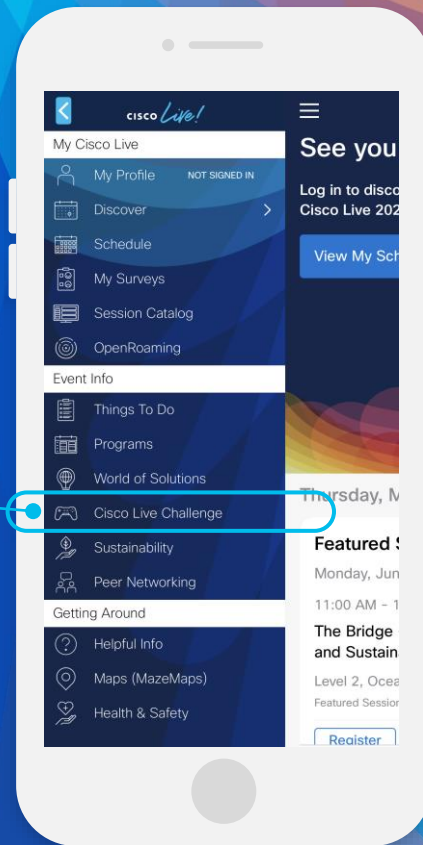
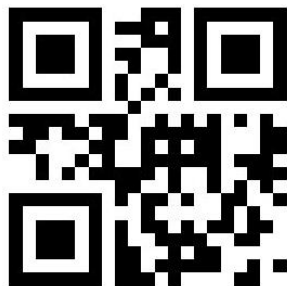
#CiscoLive

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

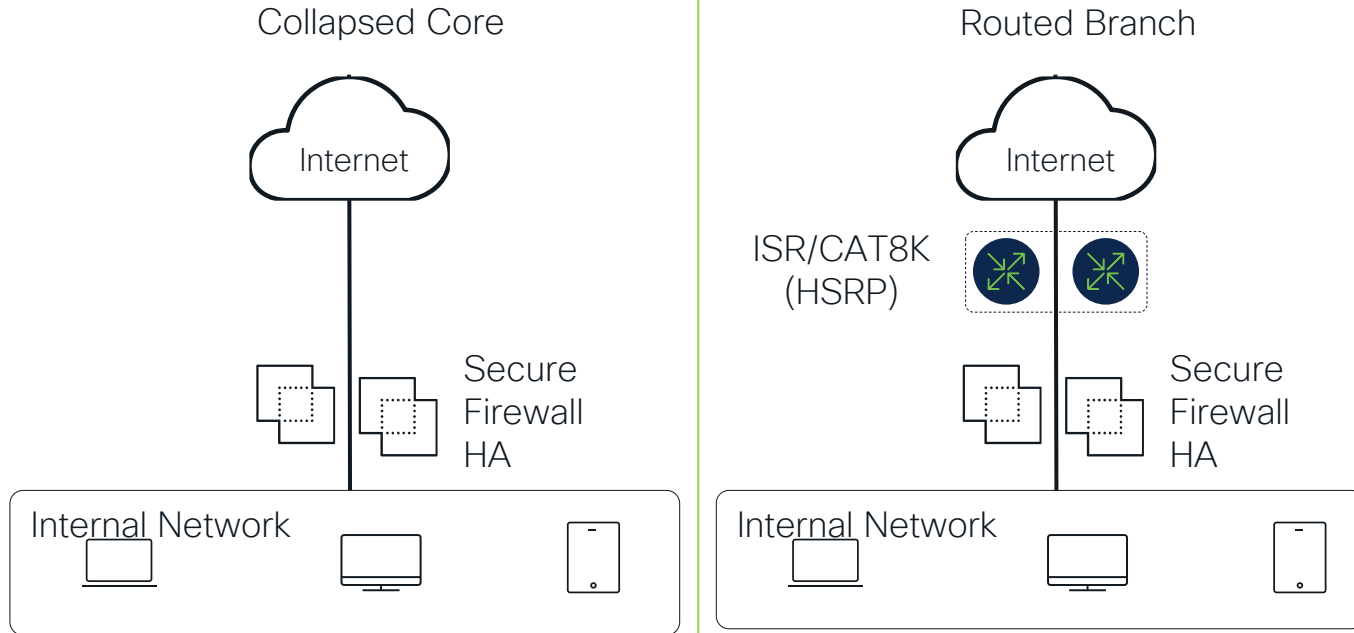
How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



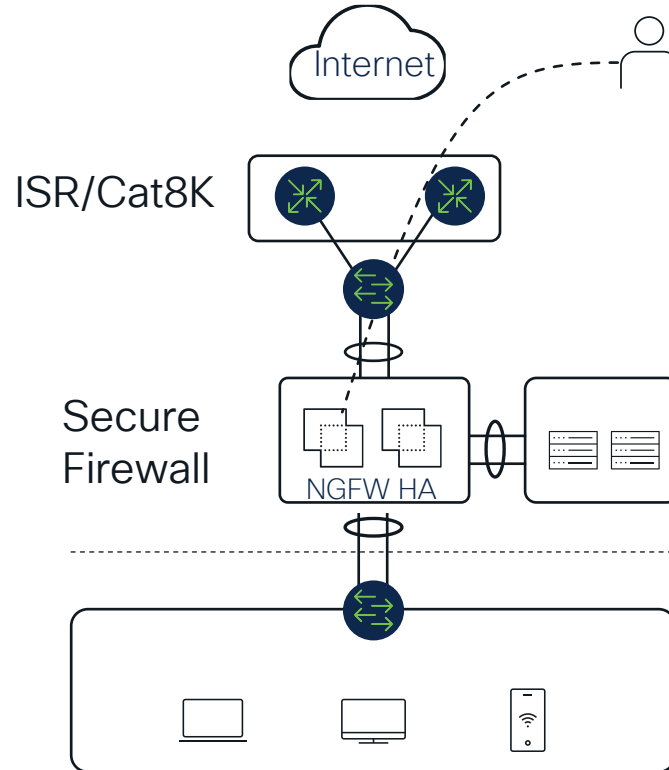
Secure Firewall Use Cases

Securing the Edge



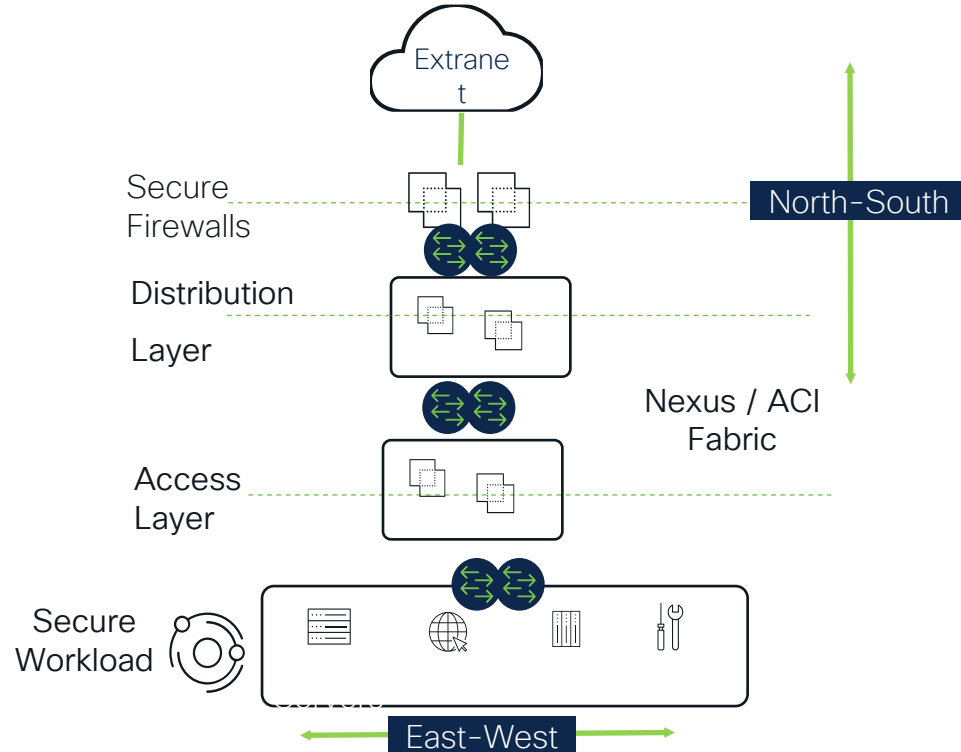
Secure Firewall Use Cases

Securing Hybrid Workers



Secure Firewall Use Cases

DC Segmentation and Threat Protection



Reference

Source: <https://docs.umbrella.com/hardware-integrations/docs/cisco-secure-firewall>

Create VPN Interface (SVTI) Contd...

Reference

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
☒ Static ☐ Dynamic

Name:*
Outside_static_vti_1

☒ Enabled

Description:

Security Zone:
Outside

Priority:
0 (0 - 65535)

Virtual Tunnel Interface Details
An interface named Tunnel-ID* is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VPN.

Tunnel ID:*
1 (0 - 10413)

Tunnel Source:*
TenGigabitEthernet0/0 (Outside) 172.16.2.10

IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☒ Configure IP 169.254.2.1/30
☐ Borrow IP (IP unnumbered) Select Interface +

Cancel OK



Add Endpoint

Device*
Branch-FTD

VPN Interface*
Outside_static_vti_1

Local Tunnel ID*
FTDvChandigarh @*****.com

Virtual Tunnel Interface Added
VTI has been created successfully.
Please go to the Device > Interfaces
page to delete/update the VTI.

OK

Cancel Save



Add Endpoint

Device*
Branch-FTD

VPN Interface*
Outside_static_vti_1

Local Tunnel ID*
FTDvChandigarh @*****.com

Cancel Save

4. Create VPN Interface (SVTI)

- All the fields auto populated
- Minimal config required
- Leverages default parameters compatible with FTD and Umbrella

Reference

The screenshot shows the 'Add Virtual Tunnel Interface' configuration window. The 'General' tab is selected. The configuration is as follows:

- Tunnel Type:** Static (selected), Dynamic
- Name:** Outside_static_vti_1
- Enabled:** ☒
- Description:** (empty field)
- Security Zone:** Outside (dropdown)
- Priority:** 0 (range 0 - 65535)
- Virtual Tunnel Interface Details:**
 - Tunnel ID:** 1 (range 0 - 10413)
 - Tunnel Source:** TenGigabitEthernet0/0 (Outside) with IP 172.16.2.10
- IPsec Tunnel Details:**
 - IPsec Tunnel Mode:** IPv4 (selected), IPv6
 - IP Address:** Configure IP (selected) with address 169.254.2.1/30. Option 'Borrow IP (IP unnumbered)' is also available with a 'Select Interface' dropdown.

Buttons for 'Cancel' and 'OK' are at the bottom right.

Verifying FMC Deployment DNS Connector

Reference

- Sample FMC Transcript for the Umbrella Configuration Deployment on FTD

```
FMC >> no strong-encryption-disable
FMC >> umbrella-global
FMC >> token 1DB0829B2B7742E7CE975E278D299A1B003F6496
Branch-FTD >> [info] : Please make sure all the Umbrella
Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

FMC >> local-domain-bypass "None"
FMC >> exit
FMC >> policy-map type inspect dns preset_dns_map
FMC >> parameters
FMC >> umbrella tag BranchFTDPolicy
FMC >> dnsencrypt
FMC >> no dp-tcp-proxy
FMC >> policy-map global_policy
FMC >> class class-default
FMC >> class inspection_default
FMC >> exit
FMC >> vpn-addr-assign local
```

Verifying Certificate Push DNS Connector

- Sample FMC Transcript for the Umbrella Root CA Certificate Deployment on FTD

Reference

```
FMC >> crypto ca trustpoint Umbrella_CA_Cert
FMC >> enrollment terminal
FMC >> no subject-name
FMC >> revocation-check none
FMC >> keypair <Default-RSA-Key>
FMC >> no serial-number
FMC >> no ignore-ipsec-keyusage
FMC >> no fqdn
FMC >> no ip-address
FMC >> no subject-name
FMC >> validation-usage ssl-server
FMC >> exit
FMC >> crypto ca authenticate Umbrella_CA_Cert
nointeractive
Branch-FTD >> [info] : Enter the certificate in
base64 representation....
End with the word "quit" on a line by itself.
FMC >> -----BEGIN CERTIFICATE-----
***** output truncated *****
FMC >> -----END CERTIFICATE-----
FMC >> quit
Branch-FTD >> [info] :
INFO: Certificate has the following attributes:
Fingerprint: b64852c8 1713421b 7e47e430 2f97658a
Trustpoint 'Umbrella_CA_Cert' is a subordinate CA
and holds a non self-signed certificate.
Trustpoint CA certificate accepted.
```

Verifying Umbrella Configuration on FTD DNS Connector

Reference

- To verify Cisco Umbrella configuration pushed to FTD via FMC

```
> show running-config umbrella-global
umbrella-global
  token 1DB0829B2B7742E7CE975E278D299A1B003F6496
  public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04
:BFAB:CA43:FB79
  timeout edns 0:02:00
  local-domain-bypass "None"
```

- To verify the policy-map configuration for DNS

```
> show running-config policy-map type inspect dns
preset_dns_map
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    umbrella tag BranchFTDPolicy device-id 010a000c0da04492
  dnsencrypt
  no tcp-inspection
```

Verifying Umbrella SASE Tunnel on FTD

Reference

- To verify the details of the tunnel
- To verify the IPSec profile and the associated proposal

```
> show running-config interface tunnel 1
!
interface Tunnel1
 nameif Outside_static_vti_1
 ip address 169.254.2.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 146.112.117.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

```
> show running-config crypto ipsec
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256
 protocol esp integrity sha-256
crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set ikev2 local-identity email-id FTDvChandigarh@4154518-605493704-umbrella.com
 set reverse-route
crypto ipsec security-association pmtu-aging infinite
```

Verifying Umbrella SASE Tunnel on FTD

Reference

- To verify the IKEv2 policy set
- To verify the tunnel statistics including Tx and Rx data

```
> show running-config crypto ikev2
crypto ikev2 policy 15
  encryption aes-gcm-256
  integrity null
  group 20 19
  prf sha256
  lifetime seconds 86400
crypto ikev2 enable Outside
```

```
> show vpn-sessiondb 121

Session Type: LAN-to-LAN

Connection      : 146.112.117.8
Index           : 19                               IP Addr      :
146.112.117.8
Protocol        : IKEv2 IPsecOverNatT
Encryption      : IKEv2: (1)AES-GCM-256  IPsecOverNatT: (1)AES-
GCM-256
Hashing         : IKEv2: (1)none  IPsecOverNatT: (1)none
Bytes Tx        : 234                               Bytes Rx     : 446
Login Time      : 19:14:51 UTC Thu Apr 27 2023
Duration        : 0h:55m:16s
Tunnel Zone     : 0
```

Verifying Umbrella SASE Tunnel on FTD

Reference

- To check the tunnel status

```
> show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Internal-Control0/0	127.0.1.1	YES	unset	up	up
Internal-Control0/1	unassigned	YES	unset	up	up
Internal-Data0/0	unassigned	YES	unset	down	up
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	169.254.1.1	YES	unset	up	up
Internal-Data0/2	unassigned	YES	unset	up	up
Management0/0	203.0.113.130	YES	unset	up	up
TenGigabitEthernet0/0	172.16.2.10	YES	manual	up	up
TenGigabitEthernet0/1	172.16.3.10	YES	manual	up	up
TenGigabitEthernet0/2	unassigned	YES	unset	administratively down	up
Tunnel1	169.254.2.1	YES	manual	up	up

Verifying Umbrella SASE Tunnel on FTD

Reference

- To check the IPsec SA associated to the VTI Tunnel

```
> show crypto ipsec sa
interface: Outside_static_vti_1
Crypto map tag: __vti-crypto-map-Tunnell-0-1, seq num: 65280, local addr: 172.16.2.10

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 146.112.117.8

#pkts encaps: 35, #pkts encrypt: 35, #pkts digest: 35
#pkts decaps: 42, #pkts decrypt: 42, #pkts verify: 42
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapulated frags needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.2.10/4500, remote crypto endpt.: 146.112.117.8/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C1F8F5AD
current inbound spi : E533416F

inbound esp sas:
spi: 0xE533416F (3845341551)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings = (L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, )
slot: 0, conn_id: 19, crypto-map: __vti-crypto-map-Tunnell-0-1
sa timing: remaining key lifetime (Kb/sec): (4055040/27443)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:
spi: 0xC1F8F5AD (3254318509)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings = (L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, )
slot: 0, conn_id: 19, crypto-map: __vti-crypto-map-Tunnell-0-1
sa timing: remaining key lifetime (Kb/sec): (4193280/27443)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

>
```