

Configuration de l'accès sécurisé avec Secure FTD et ASA pour l'accès privé avec NAT

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[Secure Access et Secure Firewall Threat Defense - VPN basé sur la route dynamique \(BGP\) avec PBR](#)

[Routage basé sur la politique FTD](#)

[Configurer BGP sur FTD](#)

[Vérifier l'état du tunnel](#)

[Configurer un VPN IPsec basé sur une route statique sur un dispositif de sécurité adaptatif \(ASA\) avec PBR](#)

[Configuration VPN sur accès sécurisé](#)

[Configuration VPN sur ASA](#)

[Routage basé sur des politiques](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer le groupe de tunnels réseau d'accès sécurisé avec la traduction d'adresses réseau.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firewall Management Center
- Cisco Secure Firewall Threat Defense
- Accès sécurisé Cisco

- Appareils de sécurité adaptatifs de Cisco
- Traduction d'adresses réseau
- Routage basé sur des politiques
- Captures de paquets sur le pare-feu

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Accès sécurisé Cisco
- Appareil de sécurité adaptatif Cisco 9.22
- Routeurs Cisco

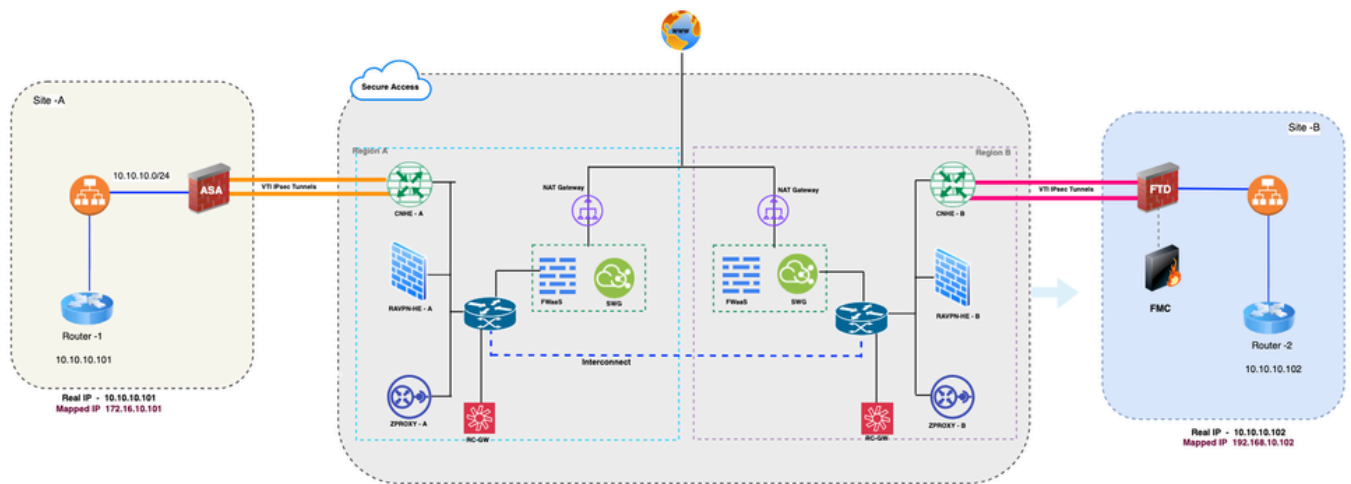
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Secure Access offre des fonctionnalités Secure Service Edge natives du cloud, notamment Secure Internet Access (SIA) et Secure Private Access (SPA). Pour les entreprises qui étendent l'accès aux applications privées aux utilisateurs distants sans réacheminer tout le trafic via un data center, Secure Access utilise les groupes de tunnels réseau (NTG) IPsec pour créer des tunnels cryptés entre les périphériques réseau sur site, tels que Cisco Firewall Threat Defense (FTD) , Adaptive Security Appliance (ASA) et Cisco Secure Access Cloud Points-of-Presence (PoP).

Ce document explique comment établir un tunnel IPsec basé sur la route à l'aide d'IKEv2 entre Cisco FTD , ASA et Cisco Secure Access, en activant la traduction d'adresses de réseau (NAT) sur l'accès sécurisé et le routage basé sur la stratégie (PBR) sur le FTD et ASA pour diriger uniquement le trafic lié à l'accès privé dans le tunnel.

Diagramme du réseau



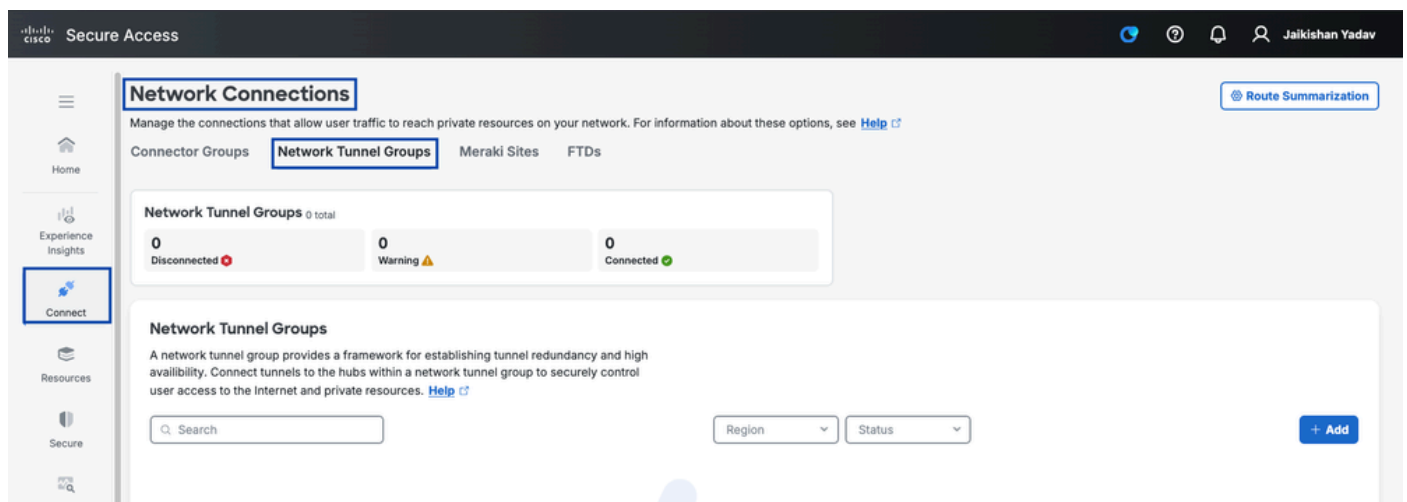
Topologie du réseau

Configurer

Secure Access et Secure Firewall Thread Defense - VPN basé sur la route dynamique (BGP) avec PBR

Configurer le groupe de tunnels réseau sur l'accès sécurisé

1. Connexion au tableau de bord Accès sécurisé [Accès sécurisé](#)
2. Accédez à Connect > Network Connections > Network Tunnel Groups et cliquez sur +Add pour configurer le groupe de tunnels réseau



3. Configuration du groupe de tunnels réseau - Paramètres généraux

- Configurer le nom du groupe de tunnels, la région et le type de périphérique
- Cliquez sur Next (suivant).

The screenshot shows the 'Add a Network Tunnel Group' configuration page. The left sidebar has four steps: 1. General Settings (selected), 2. Tunnel ID and Passphrase, 3. Routing, and 4. Data for Tunnel Setup. The main content area is titled 'General Settings' and includes instructions: 'Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.' There are three input fields: 'Tunnel Group Name' with the value 'FTD-BGP', 'Region' with a dropdown menu showing 'US (Pacific Northwest)', and 'Device Type' with a dropdown menu showing 'FTD'. At the bottom, there is a 'Cancel' button and a 'Next' button.

Accès sécurisé - Paramètres généraux des groupes de tunnels réseau

4. Configurez l'ID de tunnel et la phrase de passe.

- Configurez l'ID de tunnel et la phrase de passe.
- Cliquez sur Suivant

The screenshot shows the 'Add a Network Tunnel Group' configuration page, specifically the 'Tunnel ID and Passphrase' tab. The left sidebar has four steps: 1. General Settings, 2. Tunnel ID and Passphrase (selected), 3. Routing, and 4. Data for Tunnel Setup. The main content area is titled 'Tunnel ID and Passphrase' and includes instructions: 'Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.' There are two radio buttons for 'Tunnel ID Format': 'Email' (selected) and 'IP Address'. Below this is a 'Tunnel ID' input field with the value 'ftdbgpvpn' and a placeholder '@<org><hub>.sse.cisco.com'. There is a 'Passphrase' input field with a 'Show' button. Below the passphrase field, there is a note: 'The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.' There is a 'Confirm Passphrase' input field with a 'Show' button. At the bottom, there is a 'Cancel' button, a 'Back' button, and a 'Next' button.

5. Configuration du routage

- Configurer le numéro de périphérique AS
- Cliquez sur Save (enregistrer)

The screenshot displays the 'Routing' configuration page. On the left, a sidebar shows three steps: 'Tunnel ID and Passphrase' (checked), 'Routing' (checked), and 'Data for Tunnel Setup' (4). The main content area is titled 'Internet Protocol Version Setting for Routing'. It includes a checkbox for 'Enable IPv6 Routing in addition to IPv4' (unchecked) with a note 'IPv4 is enabled by default.' Below this is the 'Routing option' section with two radio buttons: 'Static routing' (unchecked) and 'Dynamic routing' (checked). A description for 'Dynamic routing' states: 'Use this option when you have a BGP peer for your on-premise router.' Underneath is the 'Device AS Number' field, which contains the value '65010'. At the bottom of the main content area is an 'Advanced Settings' section with three checkboxes: 'Multihop BGP' (unchecked), 'Override BGP route summarization' (unchecked), and 'Block default route advertisement' (unchecked). Each checkbox has a descriptive text. At the bottom of the page, there are three buttons: a back arrow, a 'Cancel' button, and a 'Save' button.

6. Enregistrer la configuration du groupe de tunnels réseau

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

✓ Routing

✓ Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	ftdbgpvpn@		
Primary Data Center IP Address:	44.228.138.150		2603:5004:13:20e::110:1
Secondary Tunnel ID:	ftdbgpvpn@		
Secondary Data Center IP Address:	52.35.201.56		2603:5004:13:20c::110:1
Passphrase:			

Download CSV

Done

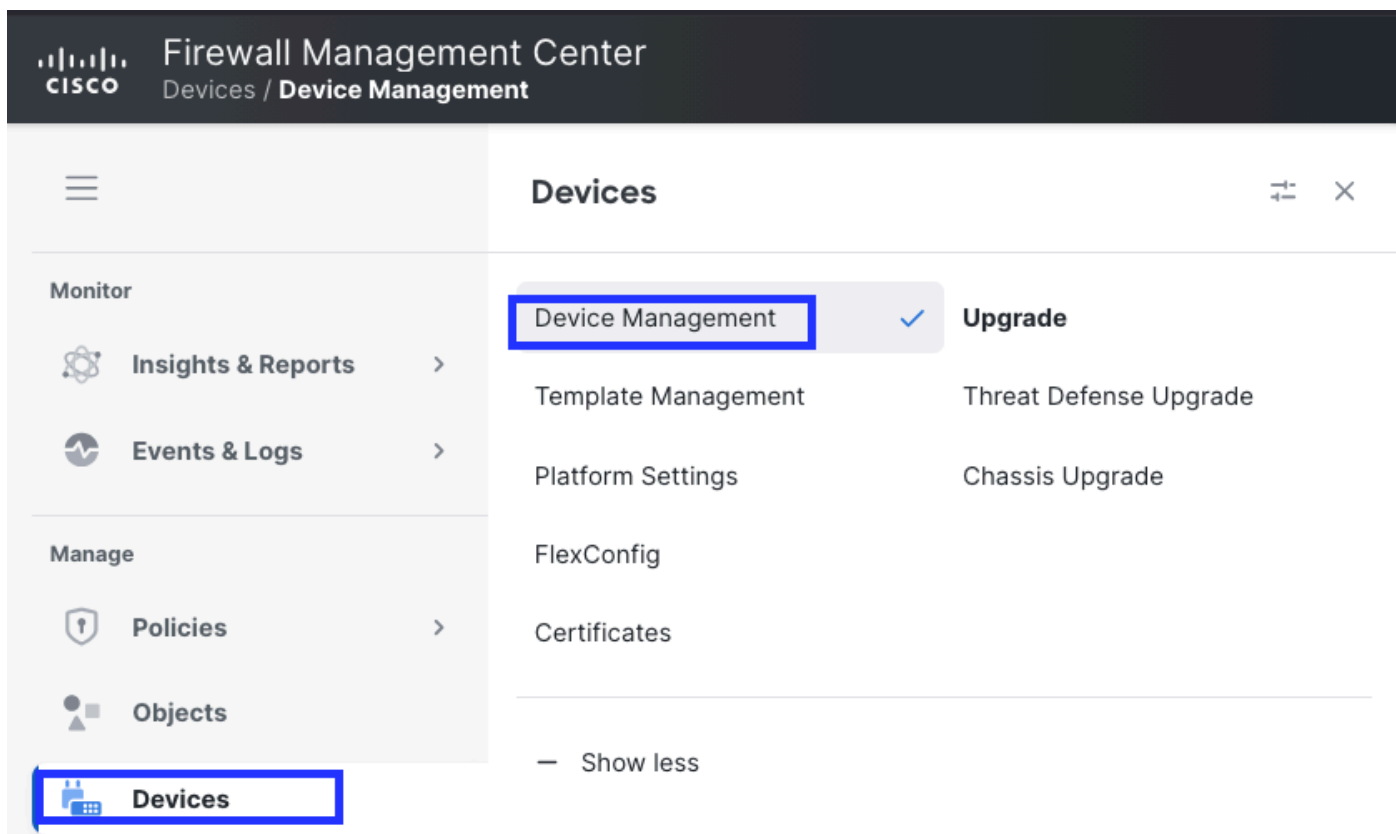
Accès sécurisé - Groupes de tunnels réseau

Configuration d'un VPN IPsec basé sur la route dynamique sur la défense FTD (Secure Firewall Threat Defense) avec PBR

1. Connexion au Centre de gestion des pare-feu (FMC)

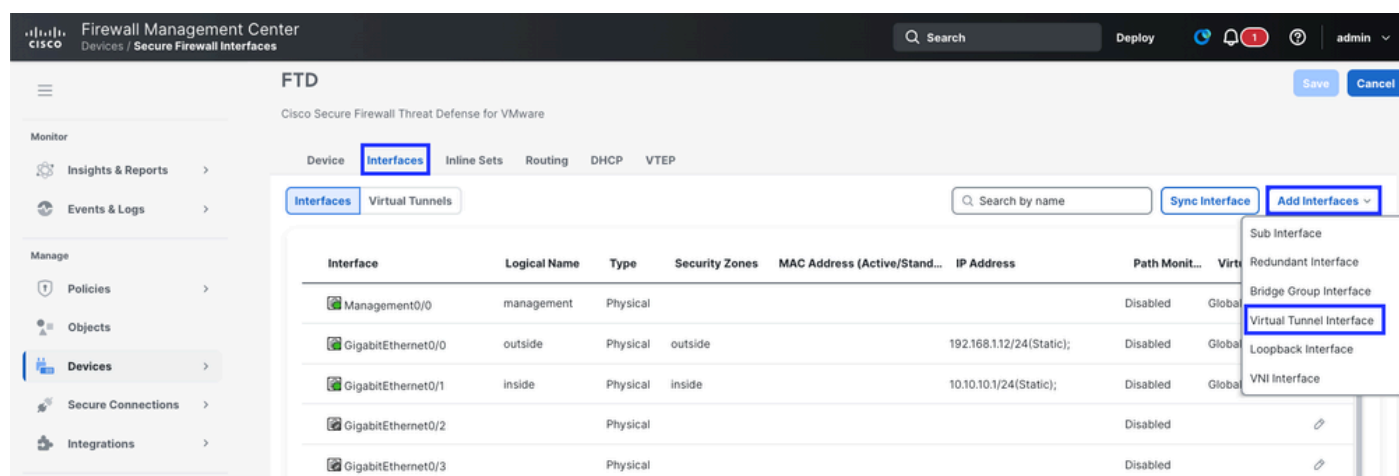
2. Configuration de l'interface de tunnel virtuel [VTI](#)

- Accédez à Périphériques > Gestion des périphériques



Gestion sécurisée du pare-feu - Tableau de bord

- Cliquez sur l'icône Crayon en regard du périphérique et accédez à la section Interface
- Cliquez sur Add interfaces et sélectionnez Virtual Tunnel Interface



Gestion sécurisée du pare-feu - Configuration FTD VTI

- Configuration de VTI

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type



Static



Dynamic

Name:*

VTI-1



Enabled

Description:

Virtual Tunnel interface for
Primary VTI VPN

Security Zone:

vti

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

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)

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:*

GigabitEthernet0/0 (outside) 192.168.1.12

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

Gestion sécurisée du pare-feu - Configuration FTD VTI

- Configurez également VTI-2 pour le VPN IPsec secondaire avec accès sécurisé

FTD Cisco Secure Firewall Threat Defense for VMware

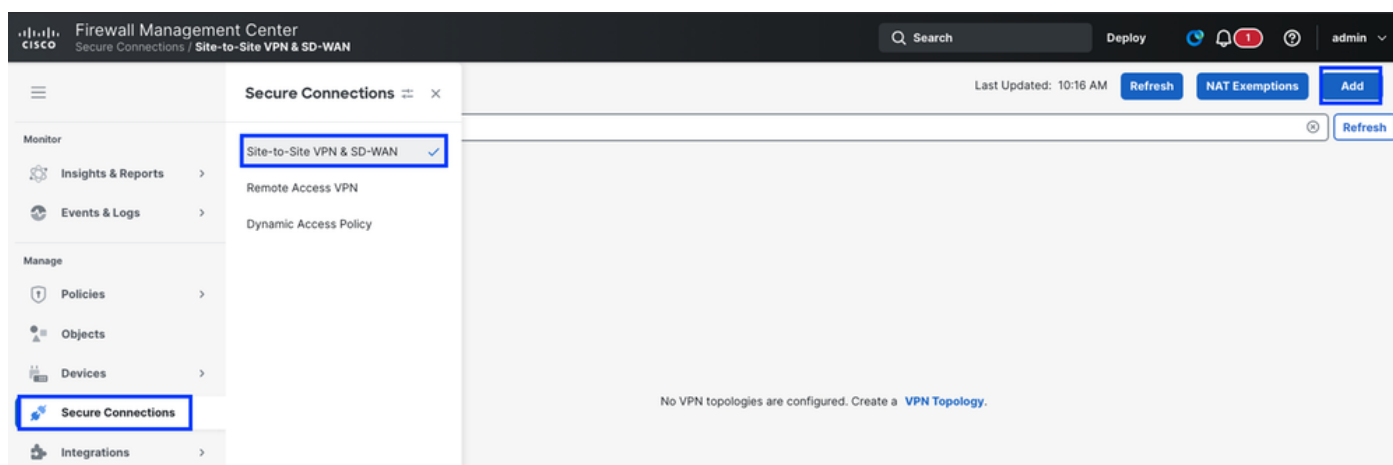
Device Interfaces Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels

Search by name Sync Interface Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stand...	IP Address	Path Monit...	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outside		192.168.1.12(Static);	Disabled	Global
Tunnel1	VTI-1	VTI	vti		169.254.2.1/30(Static);	Disabled	Global
Tunnel2	VTI-2	VTI	vti		169.254.2.5/30(Static);	Disabled	Global
GigabitEthernet0/1	inside	Physical	inside		10.10.10.1/24(Static);	Disabled	Global

3. Accédez à Secure Connections > Site-to-Site VPN & SD-WAN et cliquez sur Add pour configurer le VPN



- Créer une topologie VPN

Create VPN Topology ?

Topology Name *

SecureAccess-VPN-Primary

VPN Type

☐ SD-WAN Topology

Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ ☒ Hub and Spoke

Prerequisites

New

☒ Route-Based VPN

Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ Policy-Based VPN

Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ Full Mesh

☐ SASE Topology

! SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.

Prerequisites

Refresh

Cancel

Create

- À partir de l'étape 6 de Configurer le groupe de tunnels réseau sur l'accès sécurisé, obtenez

les ID de tunnel et les adresses IP pour les centres de données principal et secondaire.

- Cliquez sur Terminaux
- Sous Node A, cliquez sur Device (Périphérique) et sélectionnez votre périphérique FTD
- Cliquez sur Virtual Tunnel Interface et sélectionnez la première interface VTI créée à l'étape précédente
- Cliquez sur l'option Send Local Identity to Peers et sélectionnez Email ID, entrez l'ID du tunnel principal (dans « Save Network Tunnel Group Configuration » sous Configure Network Tunnel Group on Secure Access)
- Sous Node B, cliquez sur Device et sélectionnez Extranet
- Cliquez sur Nom du périphérique et donnez-lui un nom
- Cliquez sur Endpoint IP Addresses et saisissez les adresses IP principale et secondaire d'accès sécurisé séparées par une virgule (dans la section « Save Network Tunnel Group Configuration » sous « Configure Network Tunnel Group on Secure Access »)
- Cliquez sur Add Backup VTI
- Cliquez sur Virtual Tunnel Interface et sélectionnez la deuxième interface VTI créée à l'étape précédente
- Cliquez sur l'option Send Local Identity to Peers et sélectionnez Email ID, puis entrez l'ID de tunnel secondaire (à partir de « Save Network Tunnel Group Configuration » sous Configure Network Tunnel Group on Secure Access)
- Cliquez sur Enregistrer

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐

IKEv1

☒

IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.2.1)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐

Tunnel Source IP is Private

☒

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftdbgpvpn

Node B

Device:*

Extranet

Device Name:*

Secure Access

Endpoint IP Address:*

44.228.138.150,52.35.201.56

Cancel

Save

FTD sécurisé - Configuration du point d'extrémité VPN

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.2.5)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)



Tunnel Source IP is Private



Send Local Identity to Peers

Local Identity Configuration:*

Email ID

tdbgpvpn@

22-

Additional
Configuration



Route traffic to the VTI

: [Routing Policy](#)

Permit VPN traffic

: [AC Policy](#)

Cancel

Save

FTD sécurisé - Configuration du point d'extrémité VPN

- Configurer les paramètres IKEv2 conformément aux [paramètres IPsec pris en charge](#)
 - Sélectionnez Politiques comme Umbrella-AES-GCM-256
 - Sélectionner le type d'authentification comme clé manuelle prépartagée

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

Secure FTD - Paramètres VPN IKE

- Configurer les paramètres IPsec
 - Sélectionner les propositions IPsec IKEv2 comme Umbrella-AES-GCM-256
 - Activez PFS en sélectionnant Modulus Group comme 20

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Perfect Forward Secrecy

Modulus Group:

20

Cancel

Save

Secure FTD - Paramètres IPsec VPN

- Paramètres avancés
- Cliquez sur Save (enregistrer)

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

IPsec

Tunnel

IKE Keepalive:

Enable

Threshold:

10

Seconds

(Range 10 - 3600)

Retry Interval:

2

Seconds

(Range 2 - 10)

Identity Sent to Peers:

autoOrDN

Peer Identity Validation:

Do not check

Cancel

Save

Secure FTD - Paramètres VPN avancés

Routage basé sur la politique FTD

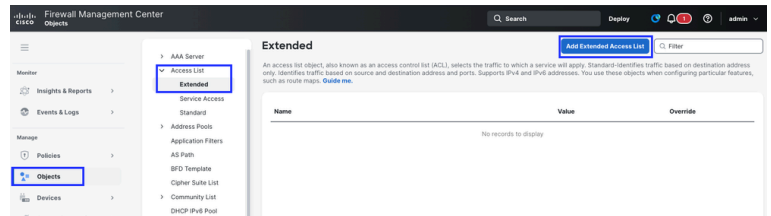
Dans le routage traditionnel, les paquets sont routés en fonction de l'adresse IP de destination. Il est difficile de modifier le routage d'un trafic spécifique dans un système de routage basé sur la destination. PBR (Policy Based Routing) étend et complète les mécanismes fournis par les protocoles de routage, vous permettant ainsi de mieux contrôler le routage.

PBR vous permet de définir la priorité IP. Il vous permet également de spécifier un chemin pour un certain trafic, tel que le trafic prioritaire sur une liaison à coût élevé. Avec PBR, vous pouvez définir un routage qui est basé sur des critères autres que le réseau de destination tels que le port source, l'adresse de destination, le port de destination, le protocole, les applications ou une combinaison de ces objets. Pour plus d'informations, référez-vous [Routage basé sur des politiques](#)

1. Configurer la liste de contrôle d'accès

- Accédez à Objets > Liste d'accès > Étendue

- Cliquez sur Add Extended Access List



Secure FTD - Liste d'accès étendue

- Attribuer un nom à la liste d'accès
- Définir l'action
 - Allow. - Le trafic défini sera envoyé au tunnel IPsec
 - Block : le trafic sera contourné à partir du tunnel IPsec
 - La règle sera mise en correspondance en fonction du numéro d'ordre (inférieur à supérieur)
- Cliquez sur Ajouter
- Cliquez sur Save (enregistrer)

Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval:
 Sec.

Network | Port | Application | Users | Security Group Tag

Available Networks

obj_10.10.10.0

Source Networks (1)
 obj_10.10.10.0

Destination Networks (0)
 any

Secure FTD - Liste d'accès étendue

New Extended Access List Object



Name
PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	obj_10.10.10.0	Any	Any	Any	Any	Any	

Displaying 1 - 1 of 1 rows < < Page 1 of 1 > > | C

☐ Allow Overrides

Cancel Save

Secure FTD - Liste d'accès étendue

2. Configurer le routage basé sur des stratégies

- Naviguez jusqu'à Devices > Device Management > FTD > Routing

Firewall Management Center
Devices / Secure Firewall Routing

Search Deploy

admin

FTD
Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP VTEP

Manage Virtual Routers
Global

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name:
Global

Description:
This is a Global Virtual Router

Select Interface:
Search

Available Interfaces

Selected Interfaces

outside
inside
management
VTI-1
VTI-2

outside
VTI-1
inside
management
VTI-2

Add

FTD sécurisé - Routage basé sur des stratégies

- Cliquez sur Ajouter
- Sélectionnez Interface d'entrée - Interface d'entrée pour le sous-réseau que nous avons défini dans la liste d'accès

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

FTD sécurisé - Routage basé sur des stratégies

- Définir les critères de correspondance et l'interface de sortie
 - Cliquez sur Ajouter
 - Sélectionnez la liste de contrôle d'accès
 - Sélectionnez Envoyer à comme adresse IP
 - Ajoutez l'adresse IP du tronçon suivant. - Les adresses IP des interfaces VTI sont 169.254.2.130 et 169.254.2.5/30. Ainsi, les adresses IP de tronçon suivant pour VTI-1 et VTI-2 seraient 169.254.2.2 et 169.2.2. 169.254.2.6 respectivement
 - Cliquez sur Enregistrer

Add Forwarding Actions



Match ACL: * +

Send To: *

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

☐ Default Interface

IPv4 settings

IPv6 settings

Recursive:

Default:

☐ Peer Address

Cancel

Save

FTD sécurisé - Routage basé sur des stratégies

FTD

You have unsaved changes Save Cancel

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

Policy Based Routing

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

Ingress Interfaces

inside

Match criteria and forward action

If traffic matches the Access List

PBR

Send through

169.254.2.2

169.254.2.6

Configure Interface Priority

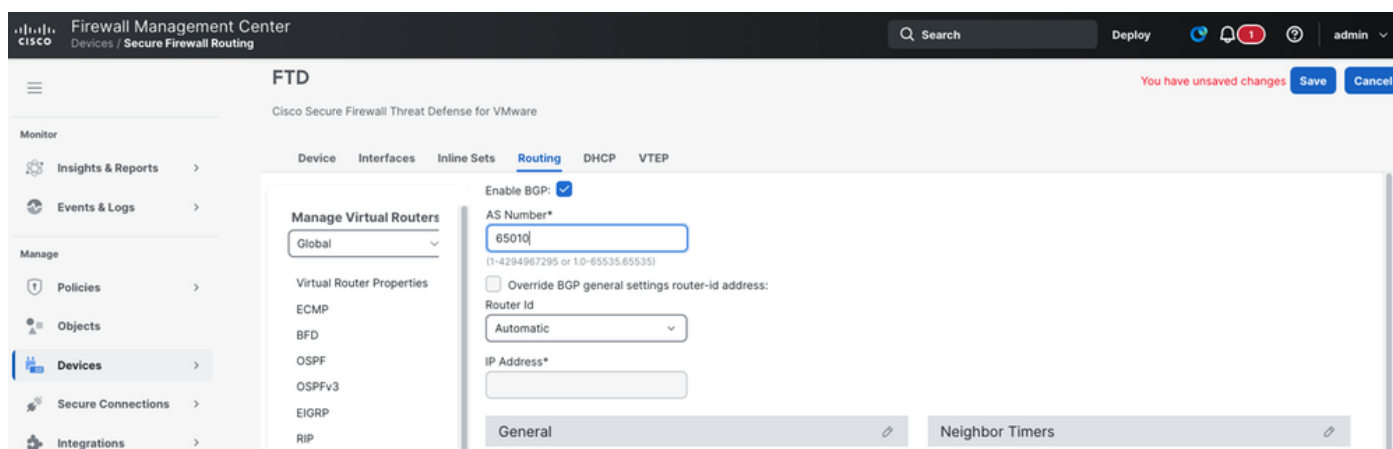
Add

FTD sécurisé - Routage basé sur des stratégies

Configurer BGP sur FTD

1. Activer BGP

- Accédez à Devices > Device Management > FTD > Routing > General Settings > BGP
- Activer BGP et ajouter le numéro de système autonome (numéro de système autonome local FTD)
- Cliquez sur Save (enregistrer)



FTD sécurisé - Routage BGP

- Accédez à BGP > IPv4

2. Ajouter un voisin BGP - Les homologues BGP d'accès sécurisé sont 169.254.0.5 et 169.254.0.9

Add Neighbor



IP Address*

169.254.0.5

Remote AS*

64512

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☐ Allow connections with neighbor that is not directly connected

☒ Limited number of TTL hops to neighbor

TTL Hops

254

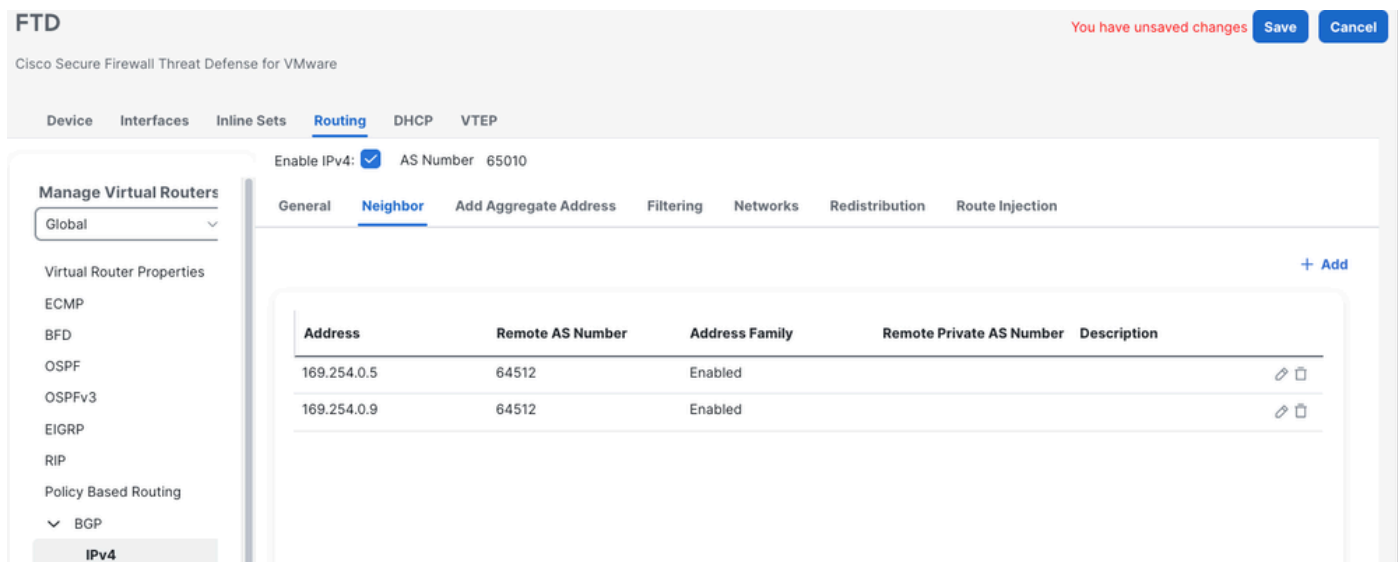
(1-254)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

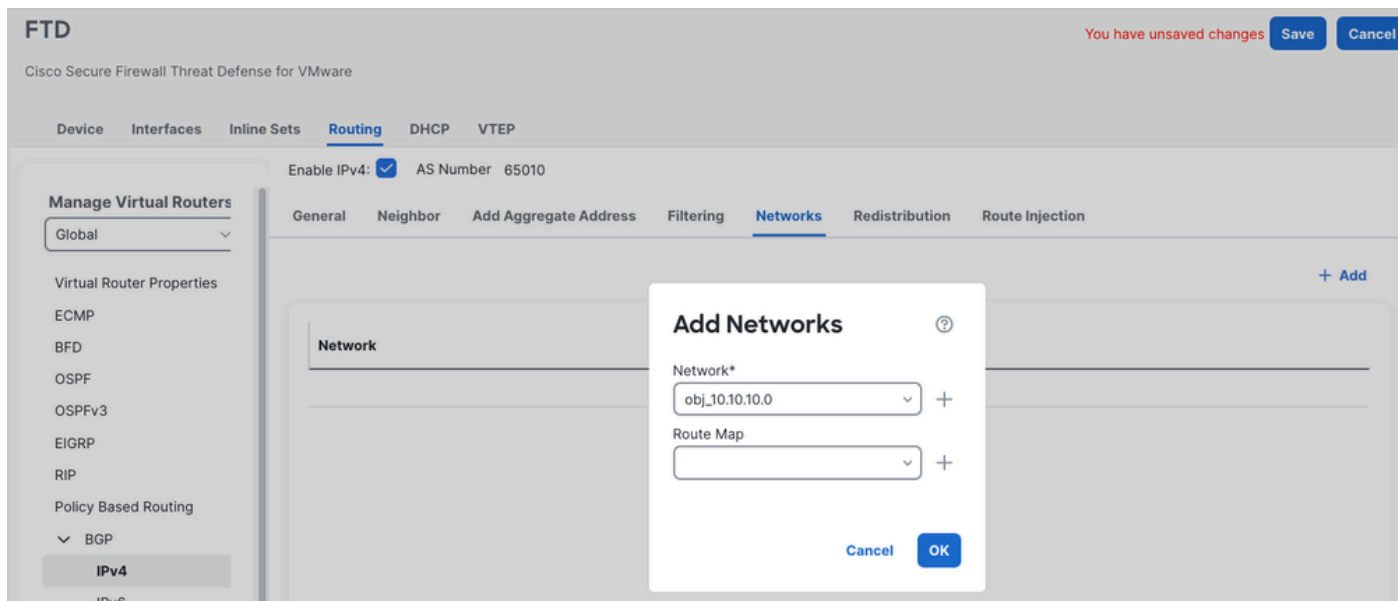
OK



FTD sécurisé - Routage BGP

3. Ajoutez les réseaux - Réseaux qui doivent être annoncés à Secure Access

- Click OK

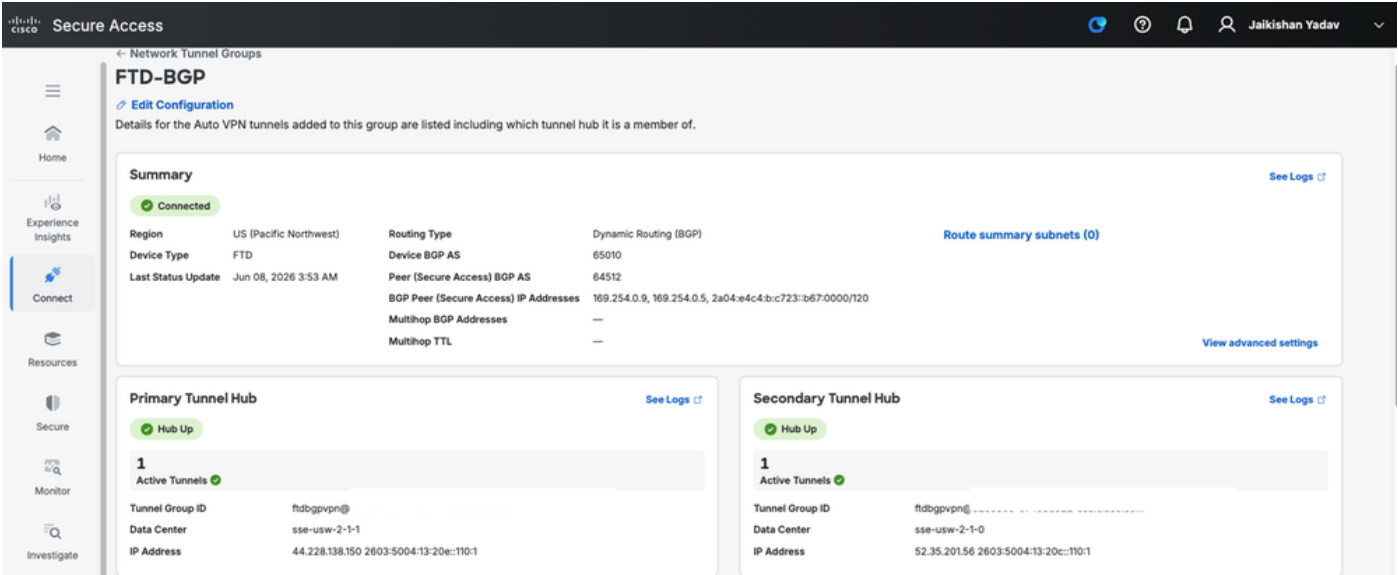


FTD sécurisé - Routage BGP

- Enregistrer et déployer les modifications

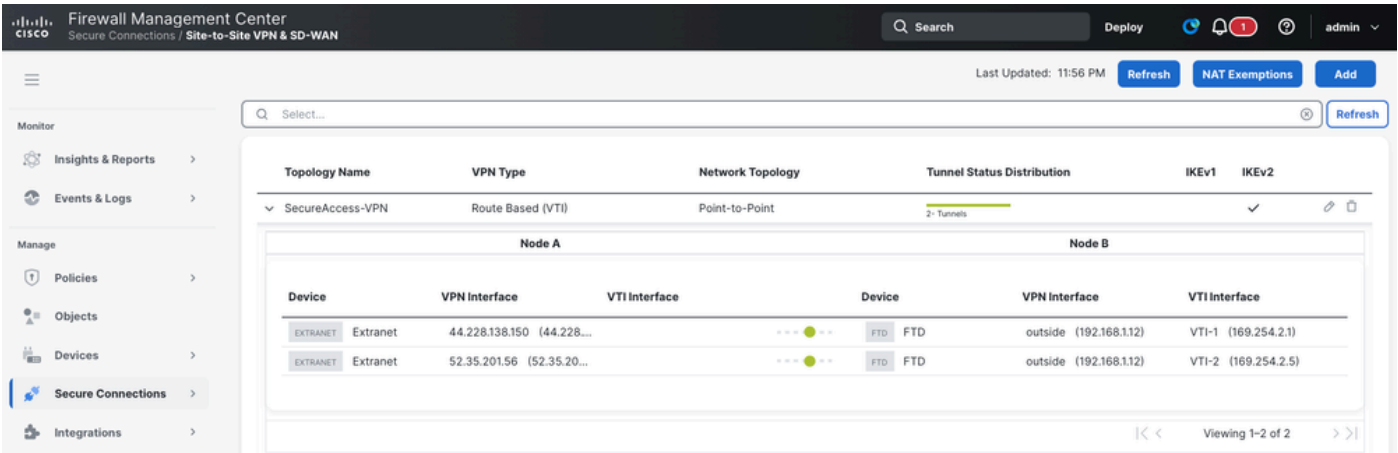
Vérifier l'état du tunnel

Sur accès sécurisé



Secure FTD - État du tunnel IPsec

Sur FMC



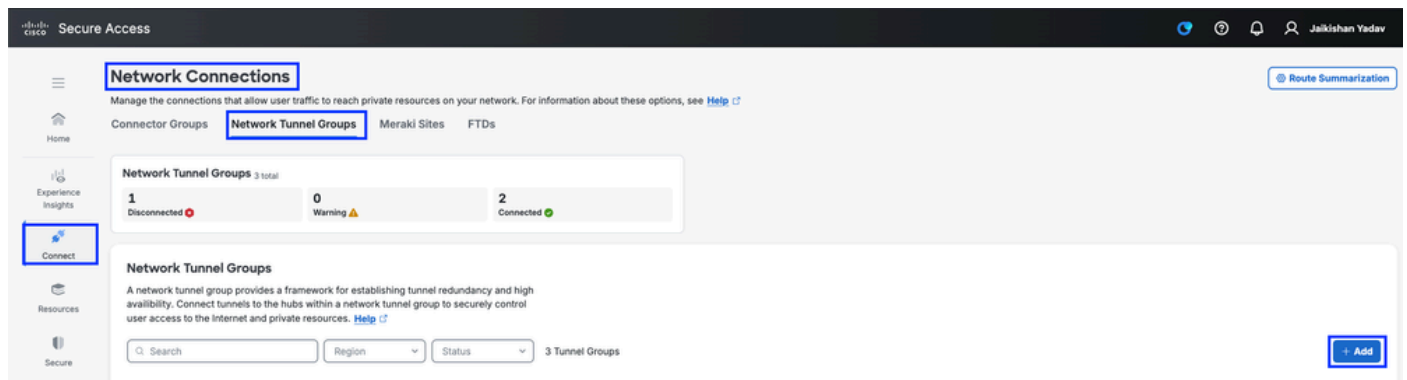
Secure FMC - État du tunnel IPsec

Configurer un VPN IPsec basé sur une route statique sur un dispositif de sécurité adaptatif (ASA) avec PBR

Configuration VPN sur accès sécurisé

1. Connexion au tableau de bord Accès sécurisé [Accès sécurisé](#)
2. Accédez à Connect > Network Connections > Network Tunnel Groups et cliquez sur +Add pour

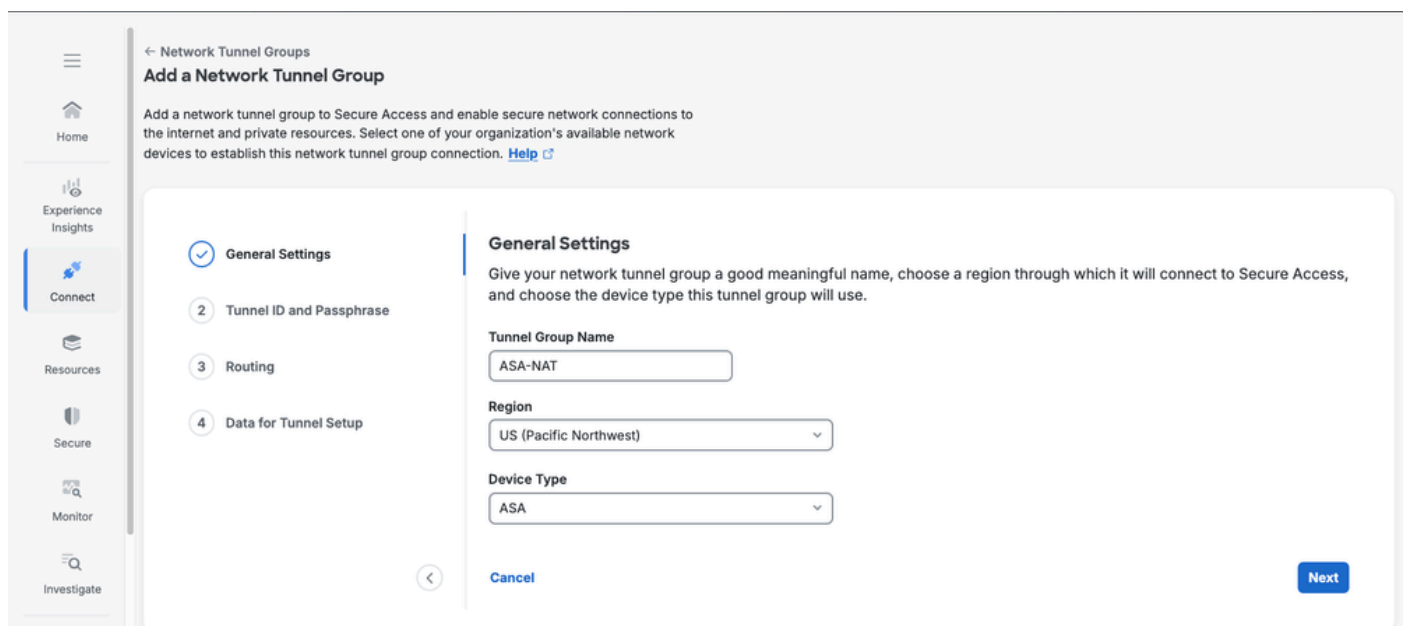
configurer le groupe de tunnels réseau



Accès sécurisé - Groupes de tunnels réseau

3. Configuration du groupe de tunnels réseau - Paramètres généraux

- Configurer le nom du groupe de tunnels, la région et le type de périphérique
- Cliquez sur Next (suivant).



Accès sécurisé - Paramètres généraux des groupes de tunnels réseau

4. Configurez l'ID de tunnel et la phrase de passe.

- Configurez l'ID de tunnel et la phrase de passe.
- Cliquez sur Suivant

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

asahomevpn @<org><hub>.sse.cisco.com

Passphrase

..... [Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

..... [Show](#)

[Cancel](#) [Back](#) [Next](#)

Accès sécurisé - Groupes de tunnels réseau

5. Activer la traduction d'adresses réseau (NAT)

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ
Source NAT
All source IP addresses translate to range:
100.96.0.0/16
☒ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ
Source NAT
Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	...
+ Add Mappings Configure full bi-directional granular control over destination IP address translation.				

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

[Cancel](#) [Back](#) [Save](#)

Accès sécurisé - Paramètres NAT des groupes de tunnels réseau

6. Ajouter le mappage NAT de destination

Flux 1 - Routeur 1 vers Routeur 2 (Site vers accès sécurisé)

Flux 2 - Du routeur 2 au routeur 1 (accès sécurisé au site)

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

- General Settings
- Tunnel ID and Passphrase
- Routing**
- Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☒ Translate to Secure Access NAT subnet

Secure Access → Site

Source NAT

Add a destination mapping to enable this rule

Accès sécurisé - Paramètres NAT des groupes de tunnels réseau



Mise en garde : Lorsque NAT est activé, BGP n'est pas possible . En outre, configurez également le VPN statique sur les périphériques en périphérie du client



Conseil : N'oubliez jamais d'envoyer une requête ping à une adresse IP traduite .
L'IP traduite est insérée dans le CIDR traduit et l'IP réel dans le CIDR original.

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ
Source NAT
All source IP addresses translate to range:

☐ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ
Source NAT
All source IP addresses translate to range:

☐ Translate to Secure Access NAT subnet

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	...
> ASA-To-FTD	Site → Secure Access	10.10.10.102/32	→ 192.168.10.102/32	ⓘ ⓘ
> FTD-To-ASA	Secure Access → Site	10.10.10.101/32	→ 172.16.10.101/32	ⓘ ⓘ

Rows per page

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

[Cancel](#) [Back](#) [Save](#)

Accès sécurisé - Paramètres NAT des groupes de tunnels réseau

Cliquez sur Enregistrer



Conseil : Pour le trafic allant de 'Site A' à 'Site B', du point de vue de CNHE-1, la direction est 'Site-> SecureAccess'

Pour le trafic allant du 'site B' au 'site A', du point de vue du CNHE-1, la direction est 'SecureAccess -> Site'

Configuration VPN sur ASA

1. Connectez-vous à l'interface de ligne de commande ASA, passez en mode enable et vérifiez la connectivité IP de base vers Internet

ASA# sh ip

Adresses IP système :

Nom d'interface Adresse IP Masque de sous-réseau Méthode

Manuel GigabitEthernet0/0 en dehors de 192.168.1.40 255.255.255.0

Manuel GigabitEthernet0/1 à l'intérieur de 10.10.10.1 255.255.255.0

Adresses IP actuelles :

Nom d'interface Adresse IP Masque de sous-réseau Méthode

Manuel GigabitEthernet0/0 en dehors de 192.168.1.40 255.255.255.0

Manuel GigabitEthernet0/1 à l'intérieur de 10.10.10.1 255.255.255.0

ASA# ping 8.8.8.8

Tapez la séquence d'échappement à abandonner.

Envoi d'écho ICMP de 5 octets, 100 octets, vers 8.8.8.8, délai d'attente de 2 secondes :

!!!!

Taux de réussite de 100 % (5/5), aller-retour min/moy/max = 20/28/30 ms

ASA#

2. Configurez la stratégie IKEv2 et activez IKEv2 sur l'interface externe

```
crypto ikev2 policy 10
cryptage aes-gcm-256
intégrité null
groupe 19
durée de vie secondes 86400
crypto ikev2 enable outside
```

3. Configuration de la proposition IPsec

```
crypto ipsec ikev2 ipsec-Proposal Ipsec-Proposal-primary
protocole esp encryption aes-gcm-256
```

4. Configurer le profil IPsec

```
crypto ipsec profile csa-profile-primary
set ikev2 ipsec-Proposal Ipsec-Proposal-primary
set ikev2 local-identity email-id <primary tunnel-id>
```

5. Configurez la stratégie de groupe et activez le protocole IKEv2 sous l'attribut.

```
group-policy csa-policy-primary internal
group-policy csa-policy-primary attributes
vpn-tunnel-protocol ikev2
```

6. Configurez le groupe de tunnels.

```
tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150 general-attributes
default-group-policy csa-policy-primary
```

```
tunnel-group 44.228.138.150 ipsec-attributes
ikev2 remote-authentication pre-shared-key <pre-shared-key>
ikev2 local-authentication pre-shared-key <pre-shared-key>
```

7. Configuration de l'interface de tunnel virtuel (VTI)

- Nameif peut être si votre choix
- L'adresse IP attribuée à VTI ne doit pas chevaucher une autre interface sur l'ASA
- La source du tunnel doit être l'interface externe du pare-feu
- La destination du tunnel doit être l'adresse IP du centre de données

```
interface Tunnel1
nameif VTI-1
adresse ip 169.254.2.1 255.255.255.252
interface source du tunnel à l'extérieur
tunnel destination 44.228.138.150
tunnel mode ipsec ipv4
tunnel protection ipsec profile csa-profile-primary
```

8. Configurez le routage de telle sorte que le trafic vers l'adresse IP ou le sous-réseau mappé soit routé à l'intérieur de l'interface VTI. Le saut suivant doit sélectionner IP dans la plage de VTI.

```
route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5. (pour le trafic Internet, le pool RAVPN ou CGNAT)
```

ou

```
route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5
```

Routage basé sur des politiques

1. Liste d'accès

```
access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any
```

2. Carte de routage

```
route-map RM-CSA permit 10
match ip address PBR
set ip next-hop 169.254.2.2 169.254.2.6
```

3. Appliquer la carte de routage à l'interface d'entrée

interface GigabitEthernet0/1

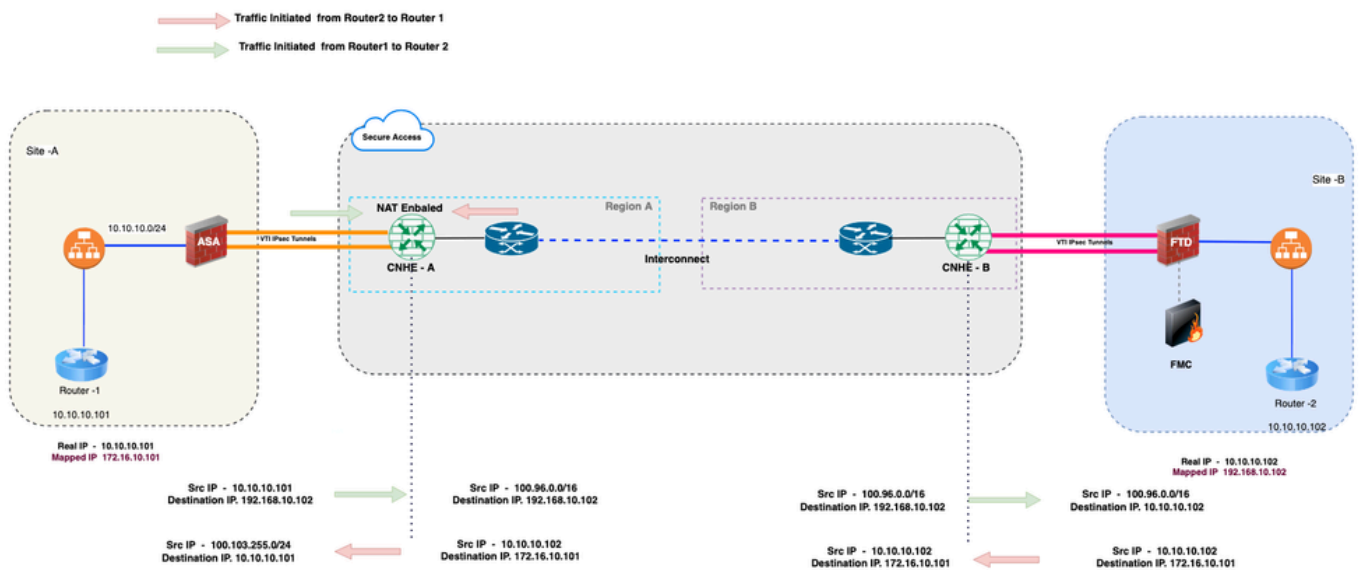
name if inside

niveau de sécurité 100

adresse ip 10.10.10.1 255.255.255.0

policy-route route route-map RM-CSA

Vérifier



Interface de routeur et état d'accessibilité GW

```
Router1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet1   192.168.1.101   YES NVRAM   down            down
GigabitEthernet2   10.10.10.101    YES NVRAM   up              up
GigabitEthernet3   unassigned      YES NVRAM   administratively down down
GigabitEthernet9   unassigned      YES unset  administratively down down
Router1#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Test 1- Router2 —> Router1. - Test Ping

```

Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#

```

Capture de paquets sur ASA (FW local)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

  1: 10:56:45.024244      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.231143      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232470      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441856      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443122      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652477      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653423      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875397      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876450      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082301      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 10:56:45.024458      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.230914      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232516      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441795      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443153      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652432      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653454      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875351      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876480      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082240      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown

```

Capture de paquets sur FTD (Remote FW)


```
ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti
```

10 packets captured

```
1: 16:06:41.122292      100.96.2.0 > 10.10.10.102 icmp: echo request
2: 16:06:41.124856      10.10.10.102 > 100.96.2.0 icmp: echo reply
3: 16:06:41.329557      100.96.2.0 > 10.10.10.102 icmp: echo request
4: 16:06:41.330442      10.10.10.102 > 100.96.2.0 icmp: echo reply
5: 16:06:41.546327      100.96.2.0 > 10.10.10.102 icmp: echo request
6: 16:06:41.547106      10.10.10.102 > 100.96.2.0 icmp: echo reply
7: 16:06:41.752036      100.96.2.0 > 10.10.10.102 icmp: echo request
8: 16:06:41.752814      10.10.10.102 > 100.96.2.0 icmp: echo reply
9: 16:06:41.967891      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968501     10.10.10.102 > 100.96.2.0 icmp: echo reply
```

10 packets shown

```
ftd# sh cap capin
```

10 packets captured

```
1: 16:06:41.123299      100.96.2.0 > 10.10.10.102 icmp: echo request
2: 16:06:41.124825      10.10.10.102 > 100.96.2.0 icmp: echo reply
3: 16:06:41.330000      100.96.2.0 > 10.10.10.102 icmp: echo request
4: 16:06:41.330396      10.10.10.102 > 100.96.2.0 icmp: echo reply
5: 16:06:41.546800      100.96.2.0 > 10.10.10.102 icmp: echo request
6: 16:06:41.547090      10.10.10.102 > 100.96.2.0 icmp: echo reply
7: 16:06:41.752448      100.96.2.0 > 10.10.10.102 icmp: echo request
8: 16:06:41.752783      10.10.10.102 > 100.96.2.0 icmp: echo reply
9: 16:06:41.968242      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968486     10.10.10.102 > 100.96.2.0 icmp: echo reply
```

10 packets shown

Essai 2. - Routeur 2 —> Test ping du routeur 1

```
Router2#sh ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   unassigned      YES NVRAM    administratively down down
GigabitEthernet2   10.10.10.102    YES NVRAM    up          up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Capture de paquets FTD (FW local)

```

ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

  1: 16:11:45.622450      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823825      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825762      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045667      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046857      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252321      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253572      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453803      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454764      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664119      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

  1: 16:11:45.622083      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823886      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825442      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045697      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046582      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252352      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253313      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453849      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454596      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664150      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown

```

Capture de paquets ASA (Remote FW)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

  1: 11:08:30.288391      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289123      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504566      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.504963      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710992      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711404      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917112      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917402      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128243      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128640      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 11:08:30.287964      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289322      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504505      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.505009      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710961      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711434      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917066      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917417      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128197      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128685      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown

```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.