

Configuration d'un accès sécurisé avec pare-feu sécurisé et défense contre les menaces pour un accès privé avec routage dynamique

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configuration d'accès sécurisé](#)

[Configuration du groupe de tunnels réseau](#)

[Routage d'accès sécurisé](#)

[Routage dynamique \(BGP\)](#)

[Enregistrer la configuration du groupe de tunnels réseau](#)

[Créer une ressource privée](#)

[Créer une règle de stratégie d'accès](#)

[Configuration de la défense pare-feu sécurisée contre les menaces \(FTD\)](#)

[Configuration des interfaces de tunnel virtuel](#)

[Configuration du tunnel IPsec](#)

[Configuration du routage FTD](#)

[Routage dynamique \(BGP\)](#)

[Configuration de la politique d'accès](#)

[Vérifier](#)

[Vérifier dans FTD](#)

[État du tunnel dans FTD](#)

[État du tunnel dans Secure Access](#)

[Événements dans l'accès sécurisé](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un accès sécurisé avec FTD via IPsec pour un accès privé sécurisé avec routage dynamique.

Conditions préalables

Exigences

- Connaissances de Cisco Secure Access
- Tableau de bord/locataire Cisco Secure Access
- Connaissances du Centre de gestion des pare-feu et de défense pare-feu
- Connaissances IPsec
- Connaissance du routage dynamique

Composants utilisés

- Pare-feu sécurisé exécutant 7.7.10 code
- Centre de gestion des pare-feu fourni dans le cloud. La configuration s'applique également au FMC virtuel type
- Tableau de bord Cisco Secure Access

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

Les tunnels réseau dans Secure Access peuvent être utilisés à deux fins principales : Accès Internet sécurisé et accès privé sécurisé.

Pour un accès privé sécurisé, les entreprises peuvent tirer parti de ZTA (Zero Trust Access) et/ou VPN as a Service (VPNaaS) pour connecter les utilisateurs à des ressources privées telles que des applications internes ou des data centers. Les tunnels IPsec jouent un rôle clé dans cette architecture en chiffrant de manière sécurisée le trafic réseau entre les utilisateurs et les ressources privées, garantissant que les données sensibles restent protégées lorsqu'elles traversent des réseaux non fiables. En intégrant des tunnels IPsec avec ZTA ou VPNaaS, les entreprises peuvent fournir un accès transparent et sécurisé aux ressources internes tout en conservant des contrôles de sécurité et une visibilité robustes.

Ce document décrit comment configurer un accès sécurisé avec Secure Firewall Threat Defense (FTD) via IPsec pour un accès privé sécurisé.

En outre, ce guide fournit des étapes pour configurer le routage dynamique avec BGP.

Bien que ce document couvre la configuration des tunnels IPsec pour l'accès privé sécurisé, la configuration de Zero Trust Access (ZTA) ou VPN as a Service (VPNaaS) pour l'accès aux applications privées n'est pas couverte par ce guide.

Configurer

Configuration d'accès sécurisé

Configuration du groupe de tunnels réseau

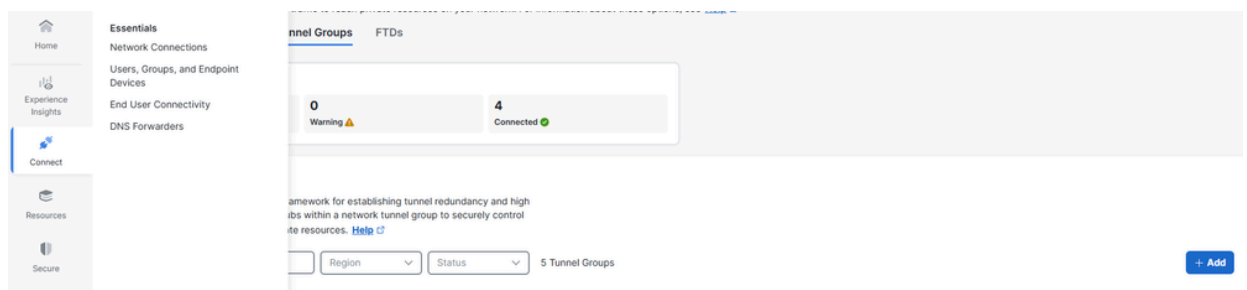
1. Accédez au panneau d'administration de [Secure Access](#).



Tableau de bord CSA

2. Ajoutez un groupe de tunnels réseau.

- Cliquez sur **Connect** > Network Connections
 - Sous Network Tunnel Groups cliquez sur > Add



Vérifier NTG

3. General Settings Configuration.

- Configurez les Tunnel Group Name, **Region** et Device Type
 - Cliquer Next

- ✓ General Settings
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Paramètres généraux

General Settings

Give your network tunnel group a good meaningful name, choose type this tunnel group will use.

Tunnel Group Name

FTD

Region

Canada (Central)

Device Type

FTD

4. Configurez l' Tunnel ID et Passphrase. Cet ID est important, car il est requis pour la configuration FTD

- Cliquez sur Next

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

ID et PSK

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

ftd1-ipsec

Passphrase

.....

The passphrase must be between special characters.

Confirm Passphrase

.....

5. Configurer le routage dynamique.

Routage d'accès sécurisé

Routage dynamique (BGP)

- Spécifiez le numéro de système autonome BGP (AS) du FTD lors de la configuration de l'homologue BGP dans Secure Access.
- Cliquez sur **Routing** > **Dynamic routing**
 - Cliquez sur **Device AS Number** et ajoutez les FTD BGP ASN
 - Cochez la **Block default route advertisement** case
 - Cliquez sur **Save**

☒ **Dynamic routing**

Use this option when you have a BGP peer for your on-premise router.

Device AS Number

64513

Advanced Settings

☐ **Multihop BGP**

Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

☐ **Multi-region backhaul**

Use Secure Access as the network backbone and prioritize regions based on origin.

☒ **Block default route advertisement**

Select to block the advertisement of the default route.

Configuration BGP CSA



Remarque : Les routes annoncées par l'accès sécurisé précèdent le chemin AS d'origine pour inclure : 1 pour les tunnels primaires et 2 pour les tunnels secondaires. Les scénarios de liaison multirégion sont pris en charge. Pour plus d'informations, cliquez sur .

Enregistrer la configuration du groupe de tunnels réseau

Téléchargez et enregistrez les données de configuration du tunnel, car elles sont nécessaires à la configuration FTD.

- Cliquez sur **Download CSV**
- Cliquez sur **Done**

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:

ftd1-ipsec@

Primary Data Center IP Address:

Secondary Tunnel ID:

ftd1-ipsec@

Secondary Data Center IP Address:

Passphrase:

Download CSV

Done

Données NTG

Summary

✖ Disconnected			
Region	Canada (Central)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	64513
Last Status Update	Feb 18, 2026 3:58 PM	Peer (Secure Access) BGP AS	64512
		BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120
		Multihop BGP Addresses	—
		Multihop TTL	—

Paramètres BGP



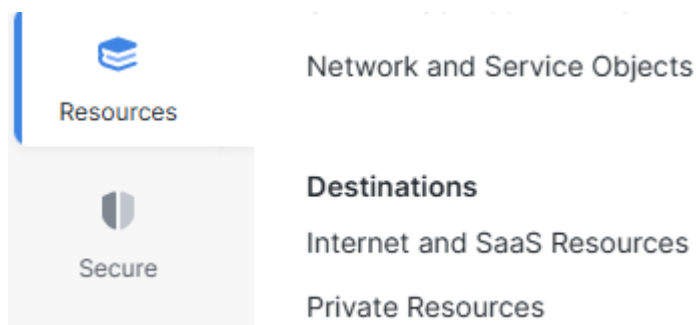
Remarque : Cliquez sur Network Tunnel Group pour afficher le numéro de système autonome BGP et les adresses IP des homologues BGP, qui sont configurées ultérieurement du côté FTD.

Créer une ressource privée

Les ressources privées sont des applications internes, des réseaux ou des sous-réseaux hébergés dans votre data center ou votre environnement de cloud privé. Ces ressources ne sont pas accessibles au public et sont protégées derrière l'infrastructure de votre entreprise.

En les définissant en tant que ressources privées dans Secure Access, vous pouvez activer l'accès contrôlé via des solutions telles que Zero Trust Access (ZTA) ou VPN as a Service (VPNaaS). Les utilisateurs peuvent ainsi se connecter en toute sécurité aux systèmes internes en fonction de l'identité, de la position des périphériques et des politiques d'accès, sans exposer les ressources directement à Internet.

Accédez à **Resources > Private Resources** > cliquez sur **Add**.



RP

- Spécifiez le **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Spécifiez les ports et les protocoles, et ajoutez des ressources privées supplémentaires si nécessaire
- Sélectionnez les connexions souhaitées Connection Method en fonction de vos besoins, par exemple les connexions de confiance zéro et/ou les connexions VPN, en fonction de vos besoins
- Cliquez sur Save

Private Resource Name

Description (optional)

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges
172.16.15.55	TCP - (HTTP/H...	8080

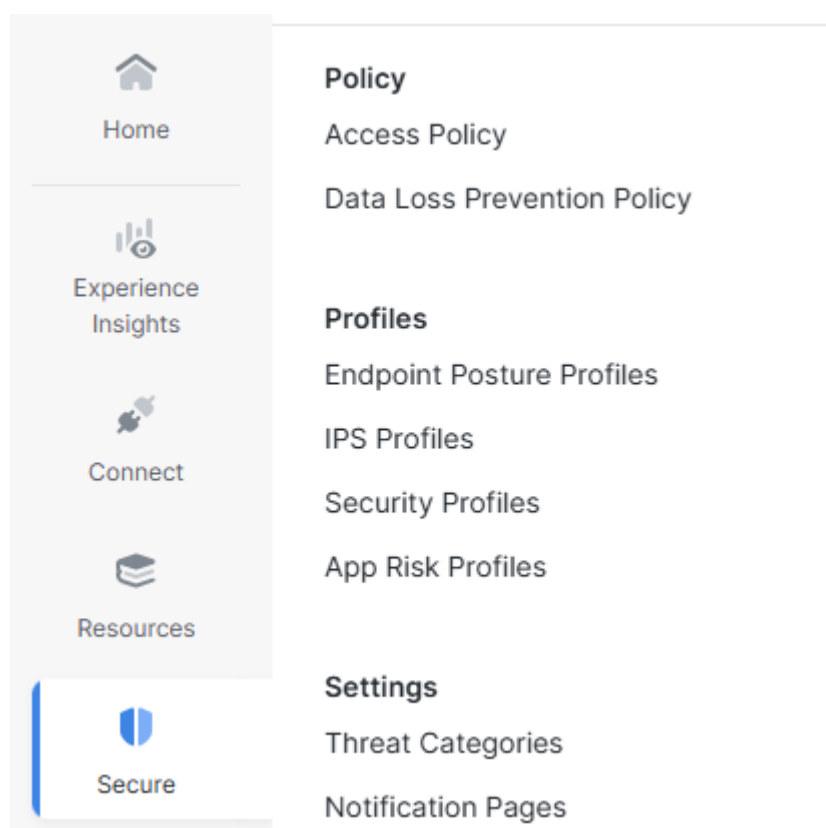
Ressource privée

Créer une règle de stratégie d'accès

Les règles d'accès privé définissent comment les utilisateurs peuvent se connecter en toute sécurité à des ressources et applications internes qui ne sont pas accessibles publiquement.

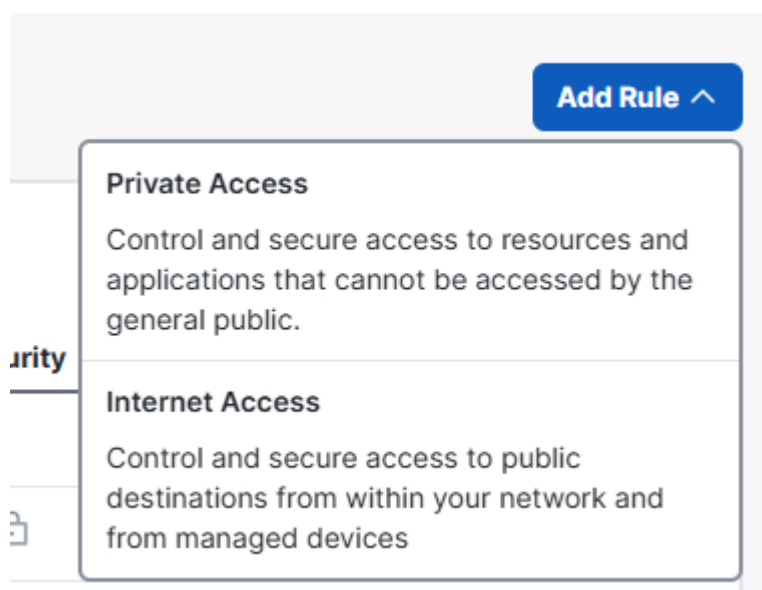
Ces règles renforcent la sécurité en contrôlant qui peut accéder à des ressources privées spécifiques en fonction de facteurs tels que l'identité de l'utilisateur, l'appartenance à un groupe, la position de l'appareil, l'emplacement ou d'autres conditions de stratégie. Cela garantit que les systèmes internes sensibles restent protégés de l'accès public général tout en restant disponibles en toute sécurité pour les utilisateurs autorisés via ZTA ou VPNaaS.

Naviguez jusqu'à Secure>Access Policy



ACP

- Cliquez sur **Add Rule**
 - Cliquez sur **Private Access**



Ajouter un ACP

- Cliquez sur **Rule Name** et donnez-lui un nom
- Cliquez sur **Action**, sélectionnez **Allow** pour autoriser ce trafic
- Cliquez sur **From** et spécifiez les utilisateurs auxquels l'autorisation est accordée

- Cliquez sur **To** et spécifiez l'accès que ces utilisateurs ont basé sur cette règle
- Cliquez sur **Next**, puis **Save** dans la page suivante

Rule name ① Rule order

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#)

Action

☒ **Allow**
Allow specified traffic if security requirements are met.

☐ **Block**
Block specified traffic.

From
Specify one or more sources

AD Users • Josue

To
Specify one or more destinations

Private Resources • FTD Internal Server

+ AND

Endpoint Requirements

For VPN connections:

☒ End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ①

Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

☐ Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security
Configure security requirements that must be met before traffic is allowed. [Help](#)

Cancel Back Next

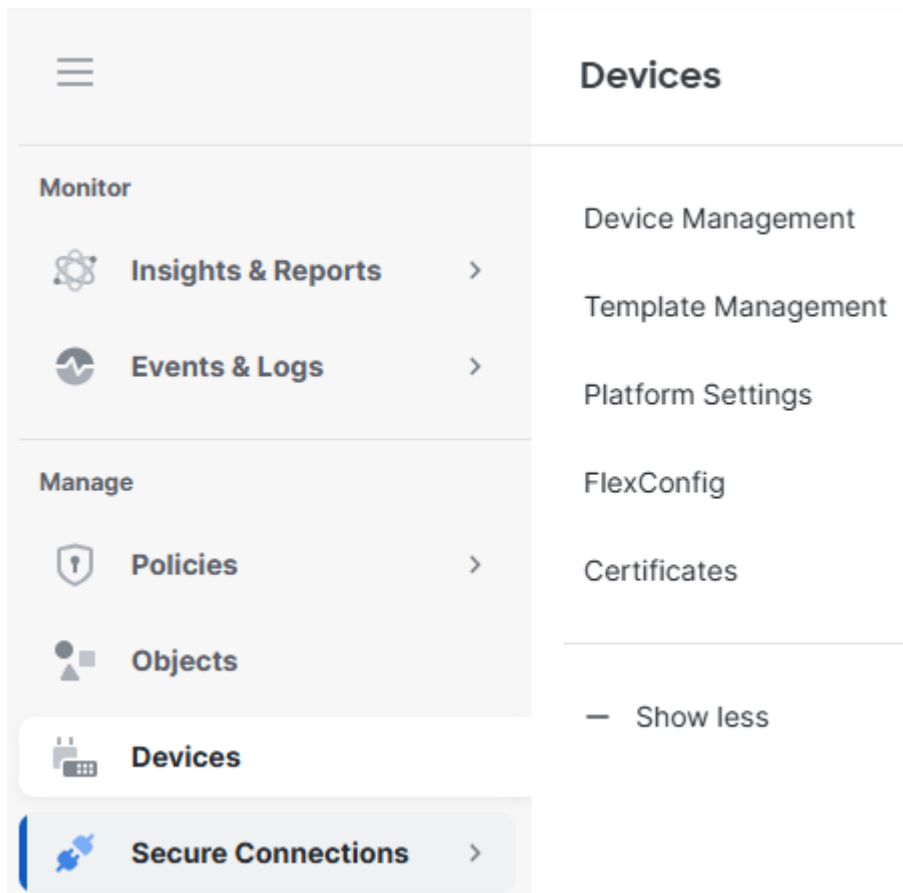
Configuration ACP

Configuration de la défense pare-feu sécurisée contre les menaces (FTD)

Configuration des interfaces de tunnel virtuel

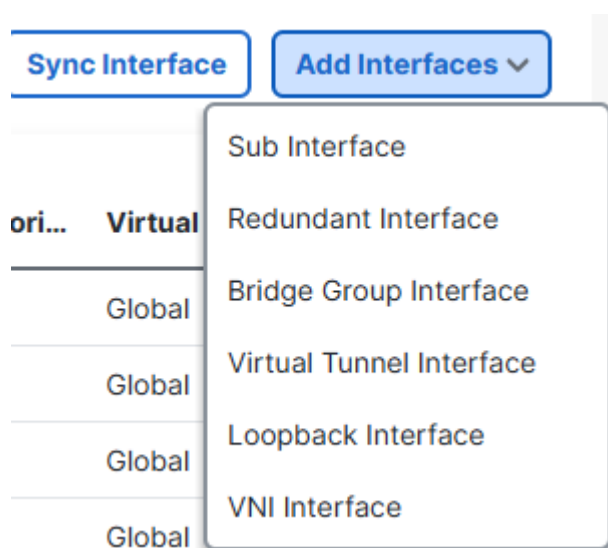
Une interface de tunnel virtuel (VTI) sur FTD est une interface logique de couche 3 utilisée pour configurer des tunnels VPN IPsec basés sur la route.

1. Accédez à **Devices** > **Device Management**.



Périphériques FTD

- Cliquez sur le périphérique FTD, Interfaces
 - Cliquez sur Add Interfaces
 - Cliquez sur Virtual Tunnel Interface
 - Créez deux interfaces de tunnel virtuel, une pour le concentrateur d'accès sécurisé principal et une autre pour le concentrateur d'accès sécurisé secondaire



Ajouter des VTI

Interface de tunnel virtuel 1 :

- Donnez-lui un nom, cliquez sur [Enable](#)
- Sélectionnez ou créez un [Security Zone](#)
- Cliquez sur [Tunnel ID](#) et donnez une valeur.
- Cliquez sur [Tunnel Source](#) et spécifiez l'interface WAN à partir de laquelle le tunnel sera établi
- Cliquez sur [IPsec Tunnel Mode](#), puis sélectionnez [IPv4](#)
- Cliquez sur [IP Address](#) et configurez l'adresse IP pour le VTI

Cliquez sur [OK](#)

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Security Zone:

zone_vti

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:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI1.1

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

169.254.0.1/30



VTI1.2

Interface de tunnel virtuel 2 :

- Donnez-lui un nom, cliquez sur **Enable**
- Sélectionnez ou créez un **Security Zone**
- Cliquez sur **Tunnel ID** et donnez-lui une valeur
- Cliquez sur **Tunnel Source** et spécifiez l'interface WAN à partir de laquelle le tunnel sera établi
- Cliquez sur **IPsec Tunnel Mode**, puis sélectionnez **IPv4**
- Cliquez sur **IP Address** et configurez l'adresse IP pour le VTI
- Cliquez sur **OK**

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-2

☒ Enabled

Description:

Security Zone:

zone_vti

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:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI2.1

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:*

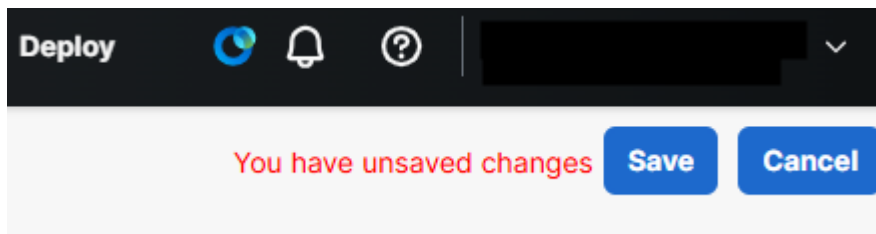
☒ Configure IP

169.254.0.5/30



VTI2.2

Cliquez sur Enregistrer.

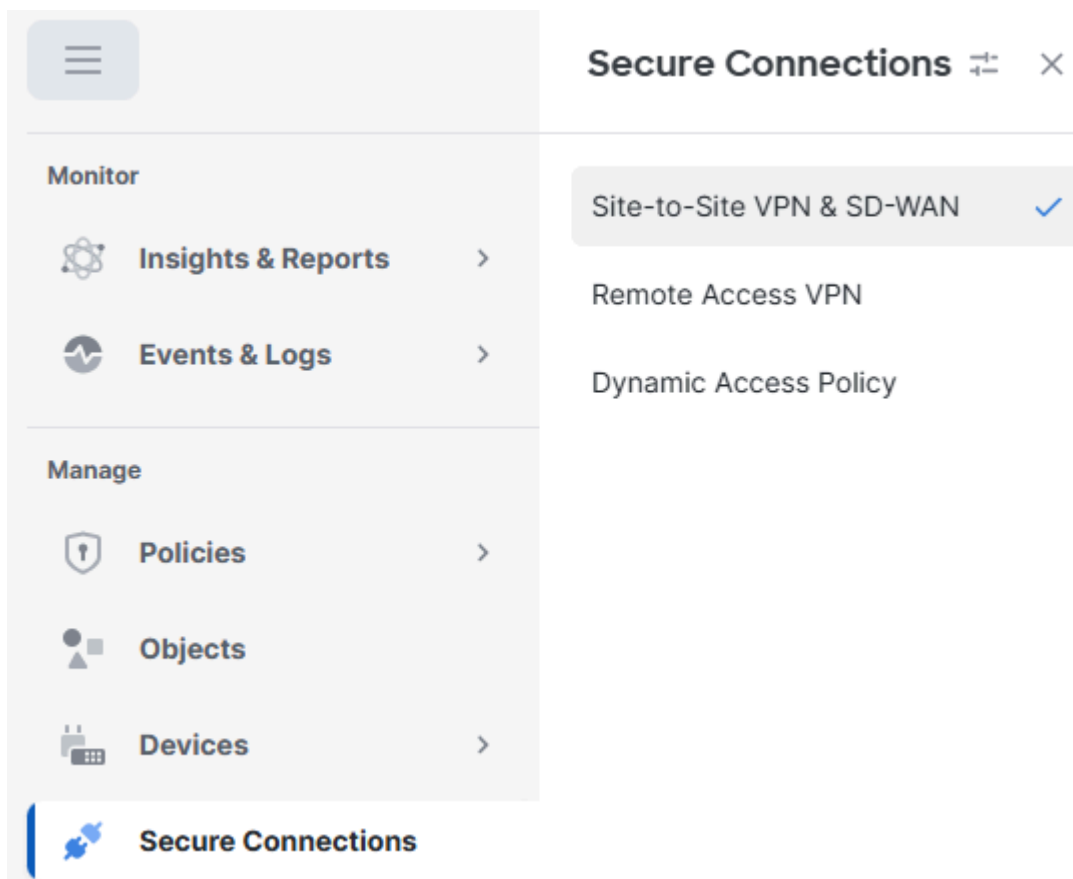


Enregistrer les modifications VTI

Configuration du tunnel IPsec

Accédez à votre tableau de bord cdFMC.

- Cliquez sur **Secure Connection** ➤ **Site-to-Site VPN & SD-WAN**



S2S

- Cliquez sur **Add**
 - Cliquez sur **Route-Based VPN**
 - Cliquez sur **Peer to Peer**

Last Updated: 12:56 PM [Refresh](#) [NAT Exemptions](#) [Add](#)

Create VPN Topology

Topology name *

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

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

[Prerequisites](#)

[Refresh](#)

[Cancel](#) [Create](#)

Ajouter un VPN

- À l'étape 5 de la configuration Secure Access, obtenez les ID de tunnel et les adresses IP des data centers principal et secondaire
- Cliquez sur Endpoints
 - Sous Node A, cliquez sur Devices et sélectionnez Extranet
 - Cliquez sur Device Name 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 l'onglet Secure Access Configuration)
 - Sous Node B, cliquez sur Device 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 (à partir de "Save Network Tunnel Group Configuration" sous la configuration d'accès sécurisé)
 - 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, entrez l'ID de tunnel secondaire (à partir de "Save Network Tunnel Group Configuration" sous la configuration d'accès sécurisé)
 - Cliquez sur Enregistrer

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

Extranet
▼

Device Name*:

CSA

Endpoint IP Address*:

Primary-IP,Secondary-IP

Node B

Device:*

cdFTD-1
▼

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.0.1)
▼
+

Tunnel Source: outside (IP: 192.168.0.20)[Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*

Email ID
▼

ftd1-ipsec@

Backup VTI: Remove

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.0.5)
▼
+

Tunnel Source: outside (IP: 192.168.0.20)[Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*

Email ID
▼

ftd1-ipsec@

Cancel
Save

Configuration FTD VTI

- Cliquez sur IKE
 - Cliquez sur **IKEv2 Settings** > Policies
 - Sélectionnez l'**Umbrella-AES-GCM-256** option

Cliquez sur OK

IKEv2 Policy



Available IKEv2 Policy  

Search

AES-GCM-NUL-
SHA

AES-GCM-NUL-
SHA-LA...

AES-SHA-SHA

AES-SHA-SHA-LATEST

DES-SHA-SHA

DES-SHA-SHA-LATEST

Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256 

Cancel

OK

Stratégie IKEv2

- Cliquez sur **Authentication Type** et sélectionnez **Pre Shared Manual Key**, entrez le PSK configuré dans **Secure Access** (phrase de passe)

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256 

Authentication Type:

Pre-shared Manual Key

▼

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

IKE

- Cliquez sur **IPSEC**

- Cliquez sur IKEv2 Proposals
- Sélectionner Umbrella-AES-GCM-256
- Cliquez sur OK

Endpoints
IKE
IPsec
Advanced

Crypto Map Type:
☒ Static
☐ Dynamic

IKEv2 Mode:
Tunnel

Transform Sets:
IKEv1 IPsec Proposals
IKEv2 IPsec Proposals*

tunnel_aes256_sha
Umbrella-AES-GCM-...

Cancel
OK

IPsec

Enregistrer les propositions IKEv2

Configuration du routage FTD

Routage dynamique (BGP)

Le protocole BGP (Border Gateway Protocol) est un protocole de routage dynamique qui automatise l'échange d'informations de routage entre les systèmes autonomes (AS). Il détermine le meilleur chemin disponible pour le trafic de données en fonction des attributs et des politiques, plutôt que de se fier aux routes statiques.

En apprenant et en mettant à jour dynamiquement les routes, le protocole BGP améliore l'évolutivité, optimise la sélection des chemins et fournit un basculement automatique en cas de modification de la liaison ou du réseau.

Accédez à votre tableau de bord cdFMC.

- Cliquez sur [Devices](#) > Device Management

Monitor


Insights & Reports


Events & Logs

Manage


Policies


Objects


Devices

Device Management

Template Management

Platform Settings

FlexConfig

Certificates

Show less

Périphérique

- Cliquez sur le FTD

☐ **Name**

☐ ▾ Ungrouped (1)

☐

✓ cdFTD-1

N/A - Routed

Snort 3

Périphérique FTD

- Cliquez sur Routing > BGP > IPv4 > Enable IPv4
- Cliquez sur Neighbor, et spécifiez le numéro de système autonome BGP pour l'accès sécurisé, ainsi que les adresses IP voisines
Reportez-vous à la remarque sous la Configuration d'accès sécurisé, où tous les détails de configuration pertinents sont fournis pour ce processus.
- Cliquez sur Save

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: ☒ AS Number 64513

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.0.2	64512	Enabled		
169.254.0.6	64512	Enabled		

+ Add

Voisin BGP



Remarque : à partir de novembre 2025, toutes les organisations d'accès sécurisé nouvellement créées utilisent l'ASN public 32644 par défaut pour l'appairage BGP dans les groupes de tunnels réseau. Les organisations existantes établies avant novembre 2025 continuent d'utiliser le ASN privé 64512 qui était précédemment réservé aux homologues BGP d'accès sécurisé.

- Cliquez sur **Networks**, puis ajoutez le ou les réseaux que vous souhaitez annoncer à Secure Access
- Cliquez sur **Save**

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: ☒ AS Number 64513

General Neighbor Add Aggregate Address Filtering **Networks** Redistribution Route Injection

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4

Network	RouteMap
Subnet-172.16.15.0	

+ Add

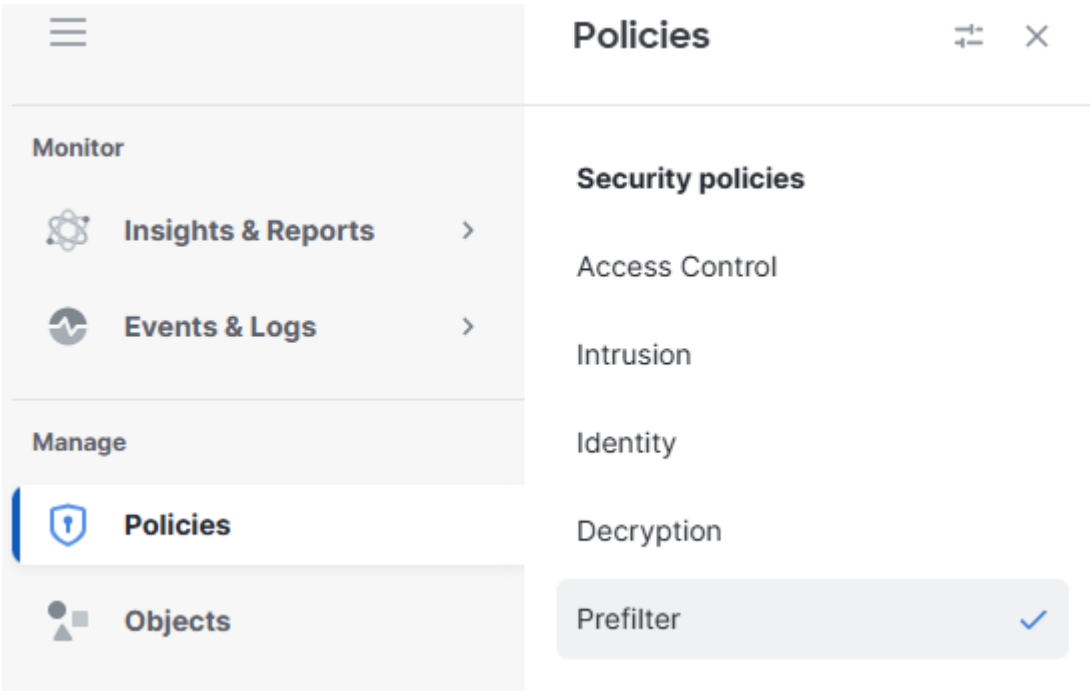
Ajouter un réseau

Configuration de la politique d'accès

Pour autoriser le trafic sur un pare-feu Cisco Firepower Threat Defense (FTD) et permettre l'accès à des ressources privées, le trafic doit d'abord passer par l'étape initiale de contrôle d'accès appelée préfiltrage.

Le préfiltrage est traité avant l'inspection approfondie et est conçu pour être simple et rapide. Il évalue le trafic à l'aide de critères d'en-tête externe de base (tels que les adresses IP et les ports source et de destination) pour autoriser, bloquer ou contourner rapidement le trafic. Lorsque le trafic est autorisé à ce stade, il peut ignorer des inspections plus gourmandes en ressources, telles que l'inspection approfondie des paquets ou les politiques d'intrusion, améliorant ainsi les performances tout en conservant le contrôle de sécurité.

Accédez à Policies > Prefilter



Préfiltre

- Cliquez sur Modifier la politique de préfiltrage utilisée par votre politique d'accès

Prefilter Policy			Domain		Last Modified	
Default Prefilter Policy			Global		2025-07-24 08:27:51	
Default Prefilter Policy with default action to allow all tunnels					Modified by "admin"	
Prefilter - Josue			Global		2026-02-18 15:26:37	
					Modified by	

cliquer sur le préfiltre

- Cliquez sur Add Tunnel Rule
 - Ajouter et autoriser le trafic du réseau VPNaaS et/ou du sous-réseau ZTA vers vos ressources privées
 - Cliquez sur Save

PreFilter - Josue											
Enter Description											
Rules											
+ Add Tunnel Rule + Add Prefilter Rule Search Rules											
#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	CSA Rule	Prefilter	zone_vrt (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na

Enregistrer la règle

À ce stade, une fois la configuration du FTD terminée et vérifiée, vous pouvez poursuivre le déploiement. Après le déploiement, les tunnels IPsec et les sessions de voisinage BGP s'ouvrent avec succès, confirmant que la connectivité et le routage dynamique fonctionnent comme prévu.

Vérifier

Vérifier dans FTD

État du tunnel dans FTD

Vous pouvez afficher l'état actuel du tunnel, y compris s'il est actif ou inactif. Cela permet de vérifier que le tunnel IPsec est correctement établi.

- Cliquez sur Connexions sécurisées
- Cliquez sur VPN de site à site et SD-WAN
- Cliquez sur le nom de la topologie

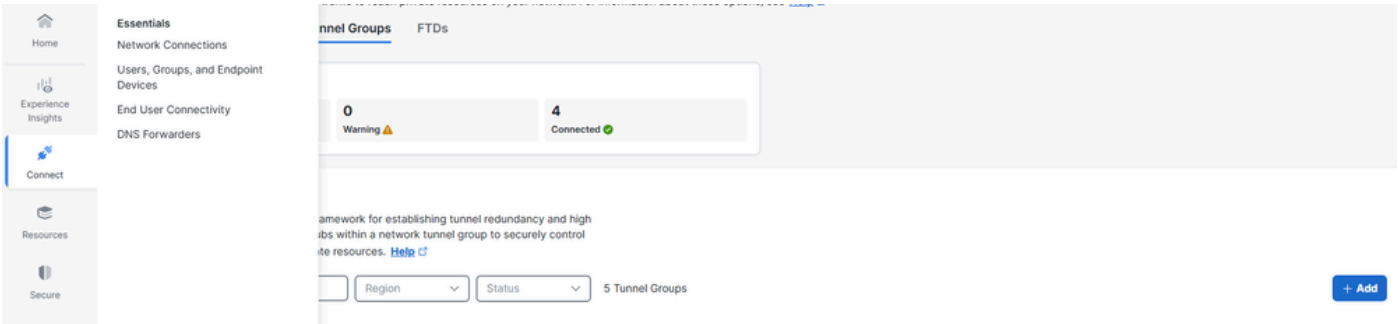
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
▼ CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

État du tunnel FTD

État du tunnel dans Secure Access

Vous pouvez afficher l'état actuel du tunnel, y compris s'il est Déconnecté, Avertissement ou Connecté. Cela permet de vérifier que le tunnel IPsec est correctement établi.

- Cliquez sur Connect > Network Connections
- Cliquez sur Network Tunnel Groups



Vérifier NTG

- Cliquez sur le groupe de tunnels réseau

Summary

Connected			
Region	Canada (Central)	Routing Type	Static Routing
Device Type	FTD	IP Address Range	172.16.15.0/24
Last Status Update	Feb 18, 2026 3:34 PM		

Primary Hub

See Logs

Hub Up

1

Active Tunnels

Tunnel Group ID ftd1-ipsec@

Secondary Hub

Hub Up

1

Active Tunnels

Tunnel Group ID

État du tunnel CSA

Événements dans l'accès sécurisé

Vous pouvez afficher les événements de tunnel et BGP et confirmer si l'état des tunnels IPsec est actif et stable, et si les sessions BGP sont établies.

Cliquez sur Monitor > Network Connectivity.

☰

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Surveiller les journaux de connexion

FTD

All severity levels

All services

All regions

Last 24 hours

Refresh

120 results

Search Text: FTD X

Reset All

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

Journaux NTG

Naviguez jusqu'à Monitor > Activity Search.

☰

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

×

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Surveiller les journaux de connexion

Sur l'un des événements associés, cliquez sur View Full Details.

13,606 Total

Page: 1 Results per page: 50 1 - 50

Source	Rule Identity	Destination	
Josue	Josue		View Full Details
Josue	Josue		Filter by Josue
Josue	Josue		Filter by
Josue	Josue		Filter by
Josue	Josue		View Rule
Josue	Josue		Edit Rule

Détails complets

Event Details



Action

Allowed

Time

Feb 18, 2026 3:30 PM

Rule Name

FTD IPsec Rule (2386307)

Enforced By

-

Source

 **Josue**

Source IP

Destination

http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)

-

Destination IP

172.16.15.55

Recherche d'activité

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.7](#)

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.