Configuration d'un accès sécurisé avec pare-feu sécurisé et défense contre les menaces pour un accès privé avec routage basé sur des stratégies

Table des matières

Introduction

Ce document décrit comment configurer l'accès sécurisé avec FTD via IPsec pour l'accès privé sécurisé avec le routage basé sur la stratégie.

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 basé sur des politiques

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 présente les étapes de configuration du routage basé sur des politiques.

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

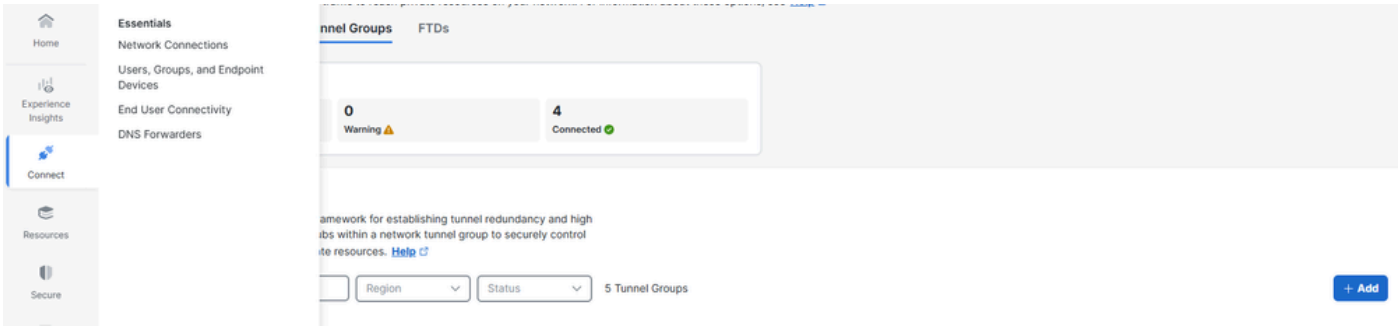
Configuration d'accès sécurisé

Configuration du groupe de tunnels réseau

1. Accédez au panneau d'administration de Secure Access.

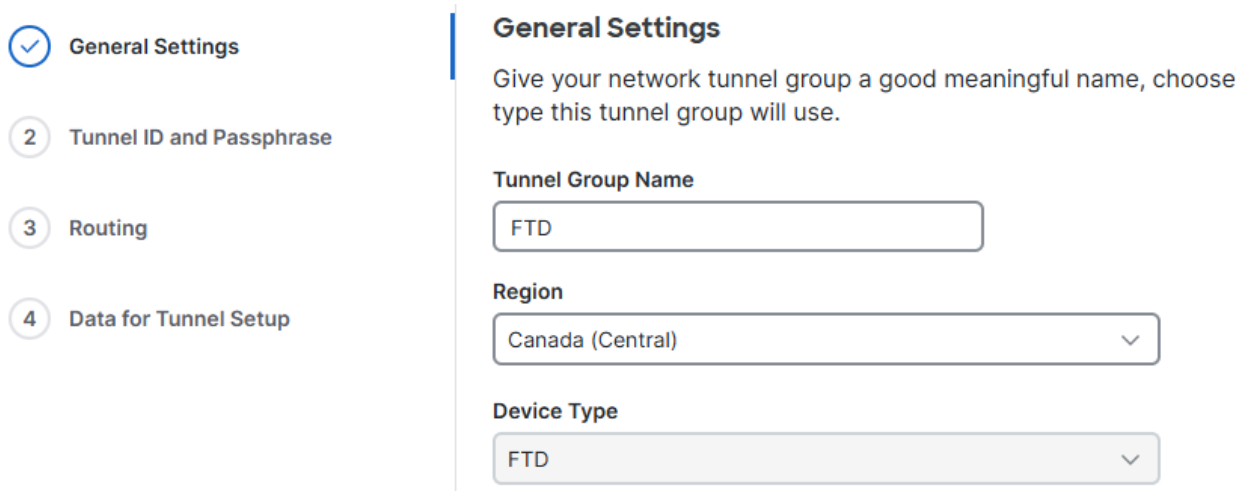
2. Ajoutez un groupe de tunnels réseau.

- Cliquez surConnect> Network Connections
  - Sous Network Tunnel Groups cliquez sur > Add



3. General Settings Configuration.

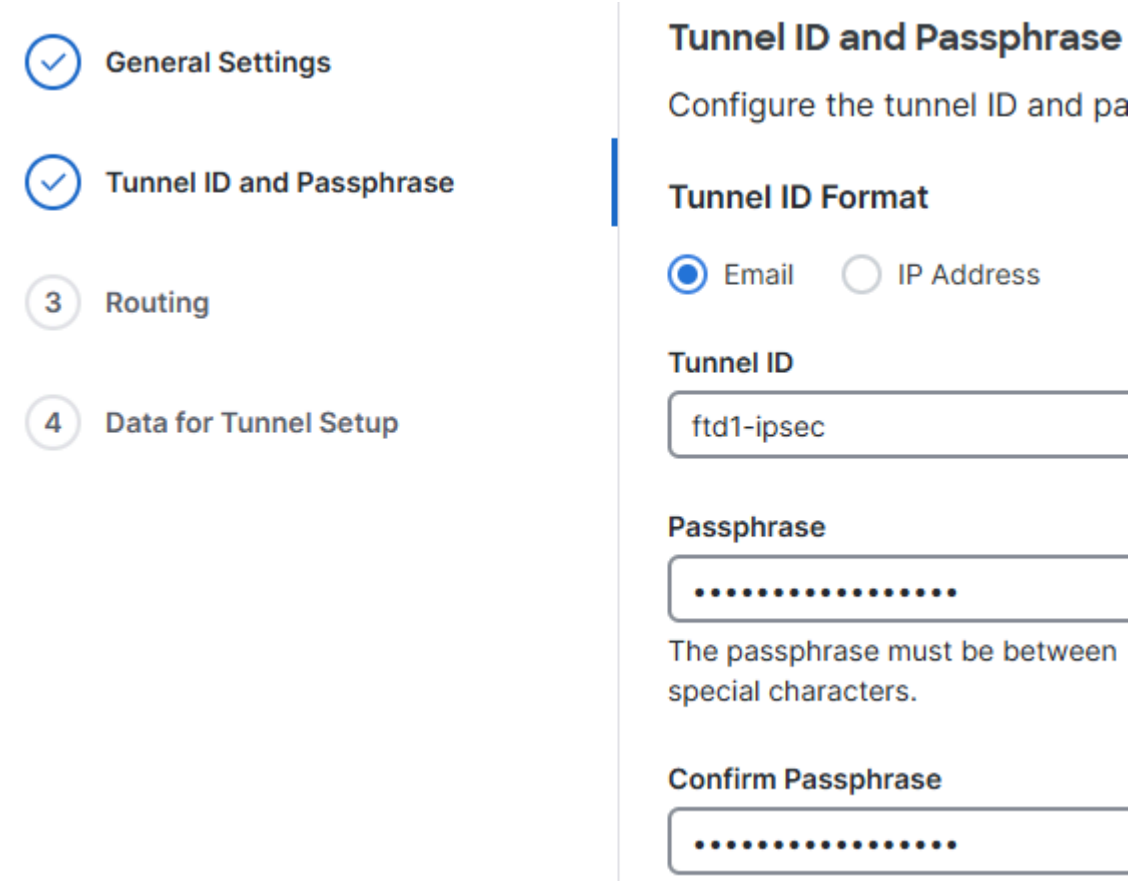
- Configurez les Tunnel Group Name, **Region** et Device Type
  - Cliquer Next



Paramètres généraux

4. Configurez Tunnel ID et Passphrase.

- Configurez l' **Tunnel ID**etPassphrase. Cet ID est important, car il est requis pour la configuration FTD
- Cliquez sur Next



ID et PSK

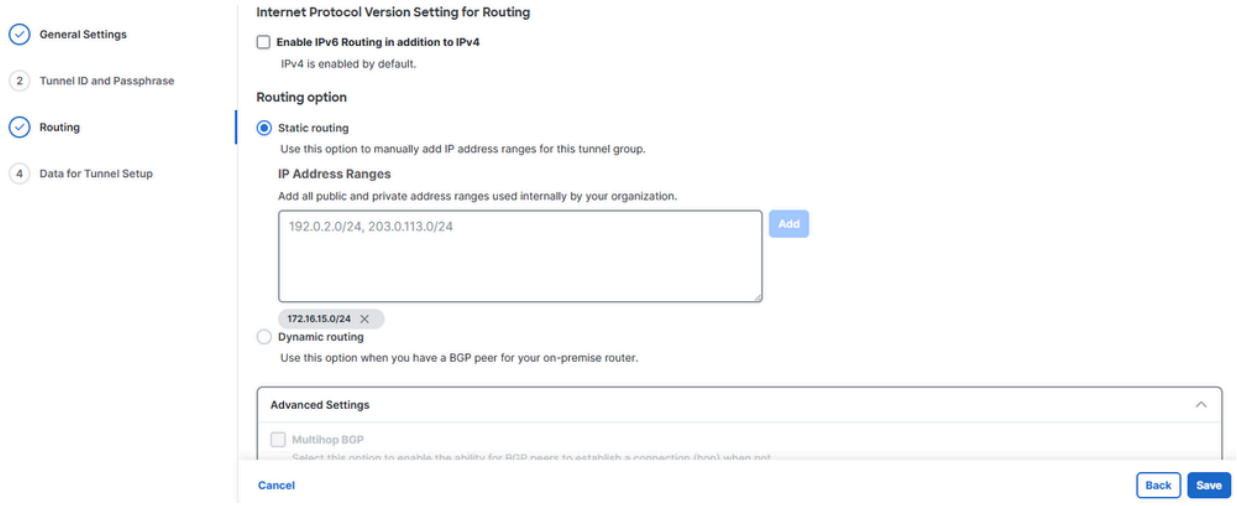
5. Configurer le routage statique.

Routage d'accès sécurisé

Routage basé sur des politiques

Ajoutez le ou les réseaux protégés par le FTD auxquels vous souhaitez que les utilisateurs distants puissent accéder via ZTA et/ou VPNaaS, puis cliquez sur Save (Enregistrer).

- Cliquez sur Routing> **Static routing**
  - Ajoutez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez faire passer le trafic via Secure Access, puis cliquez surAdd
  - Cliquez surSave

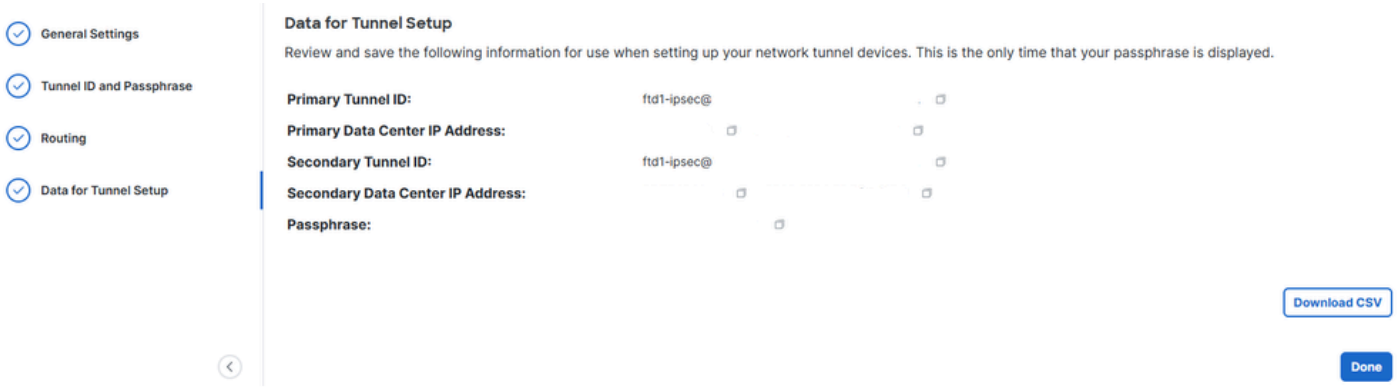


Routage statique CSA

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



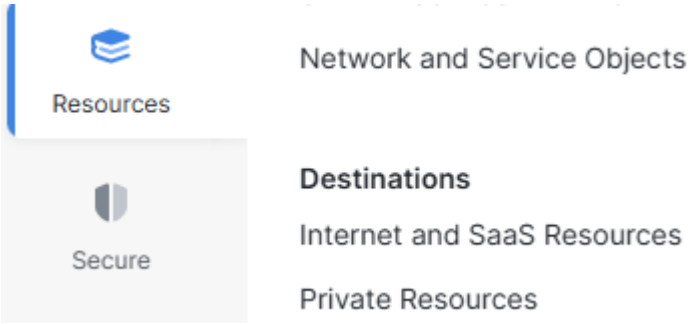
Données NTG

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.

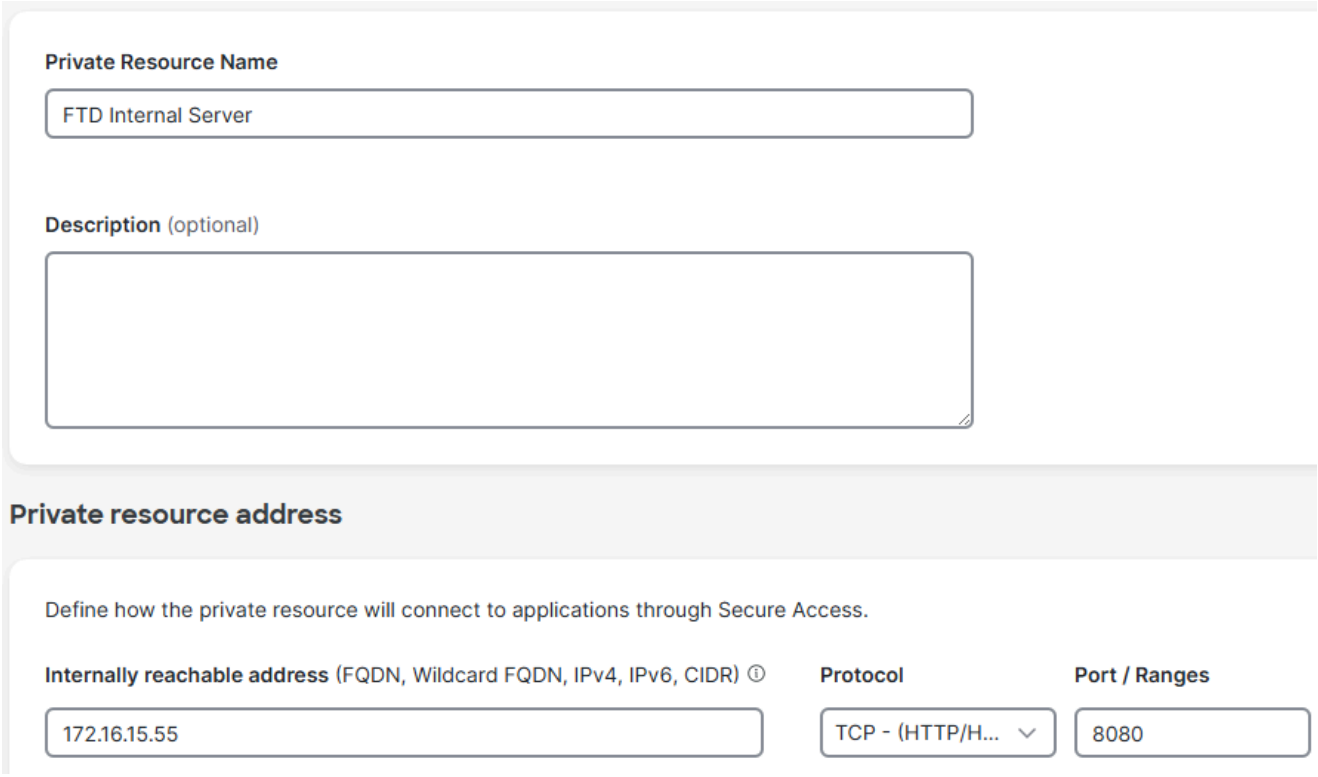
En les définissant en tant que ressources privées dans Secure Access, vous pouvez activer l'accès contrôlé via des solutions telles que Zero Trust Access (ZTA) ou VPN as a Service (VPNaaS). Les utilisateurs peuvent ainsi se connecter en toute sécurité aux systèmes internes en fonction de l'identité,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

Accédez à **Resources** > **Private Resources**> cliquez surAdd.



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



Ressource privée

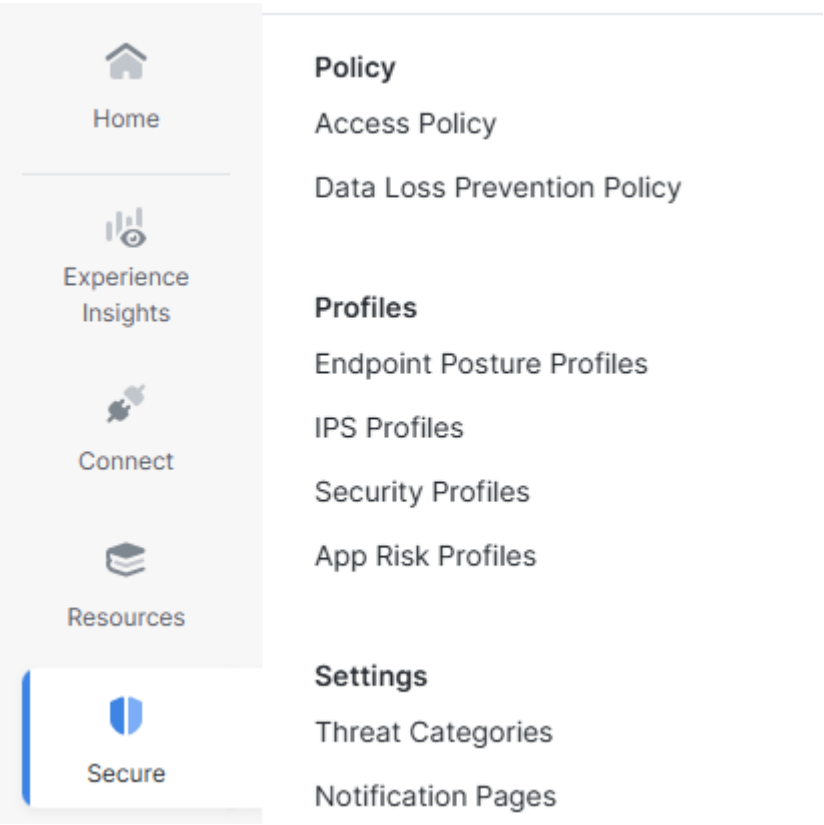
Créer une règle de stratégie d'accès

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

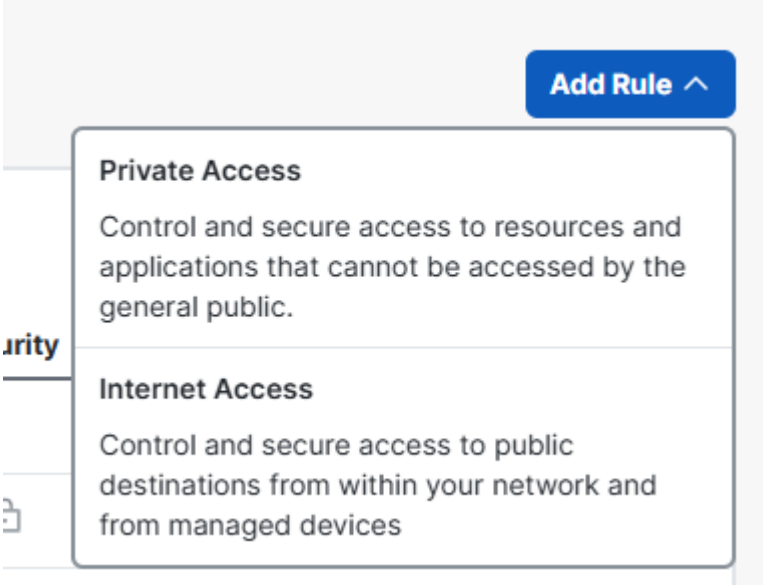
spécifiques en fonction de facteurs tels que l'identité de l'utilisateur, l'appartenance à un groupe, la position de l'appareil, l'emplacement ou d'autres conditions de stratégie. Cela garantit que les systèmes internes sensibles restent protégés de l'accès public général tout en restant disponibles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

Naviguez jusqu'à Secure>Access Policy



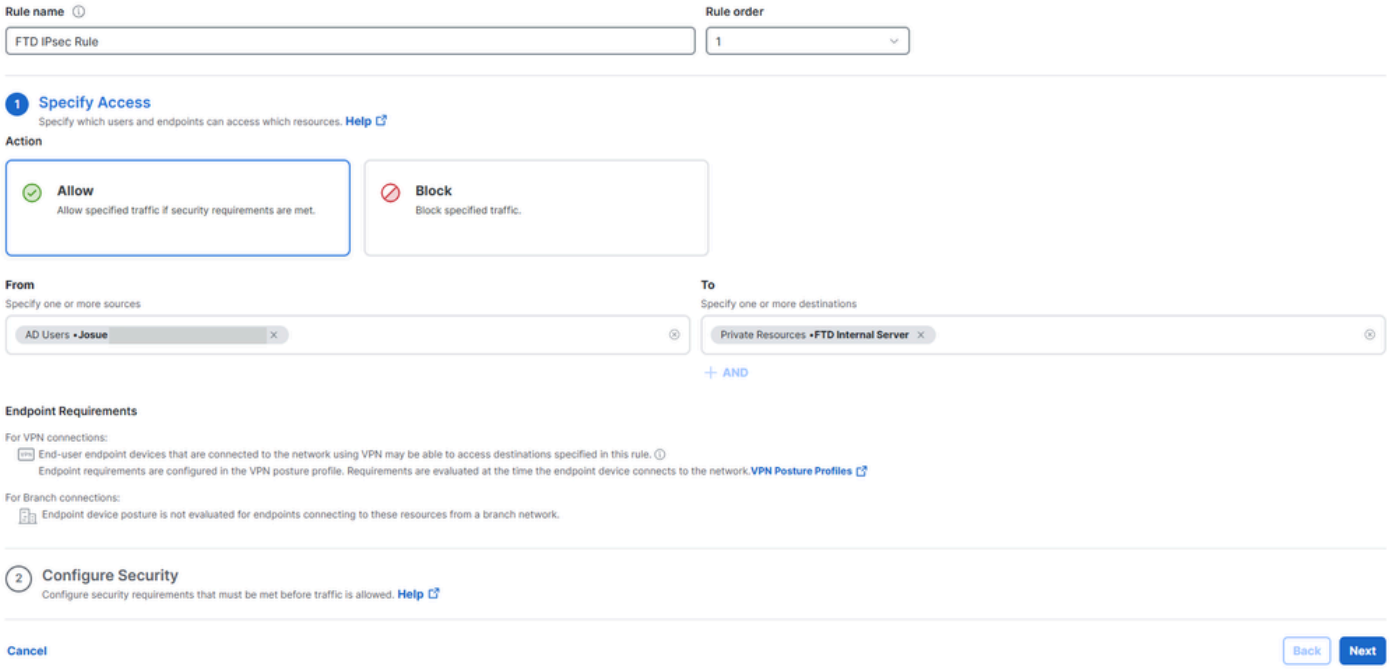
ACP

- Cliquez sur Add Rule
  - Cliquez sur Private Access



Ajouter un ACP

- Cliquez sur Rule Name et donnez-lui un nom
- Cliquez surAction, sélectionnez Allowpour autoriser ce trafic
- CliquezFromsur et spécifiez les utilisateurs auxquels l'autorisation est accordée
- Cliquez sur Toet spécifiez l'accès que ces utilisateurs ont basé sur cette règle
- Cliquez surNext, puis Savedans la page suivante



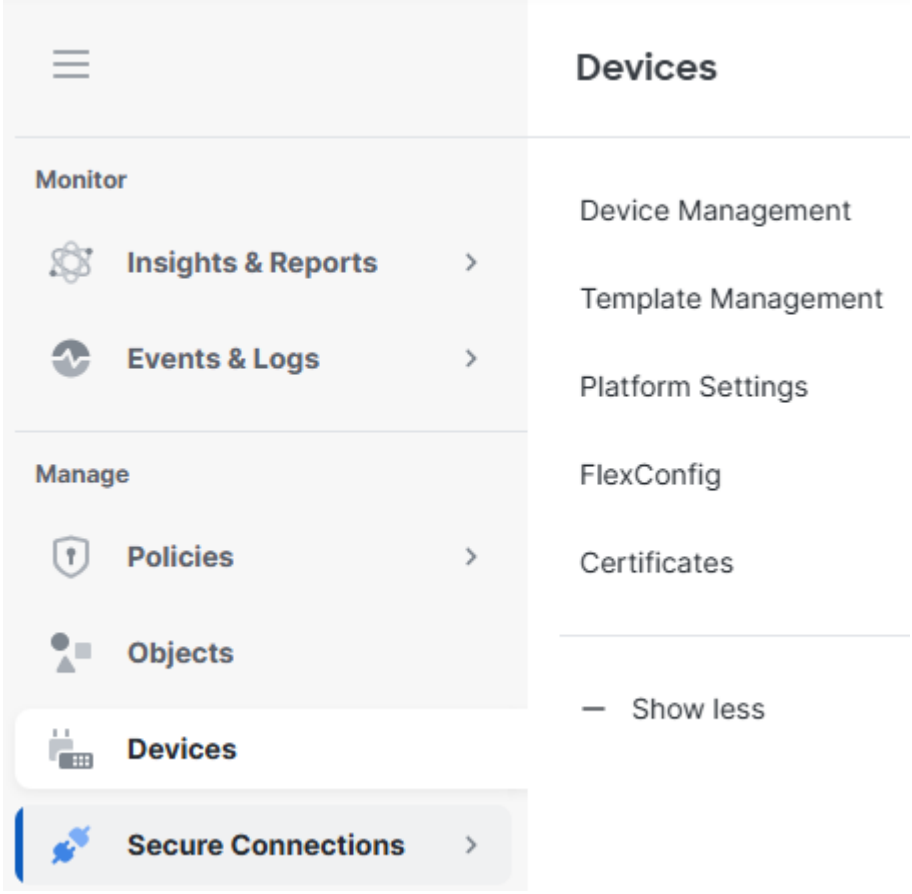
Configuration ACP

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

Configuration des interfaces de tunnel virtuel

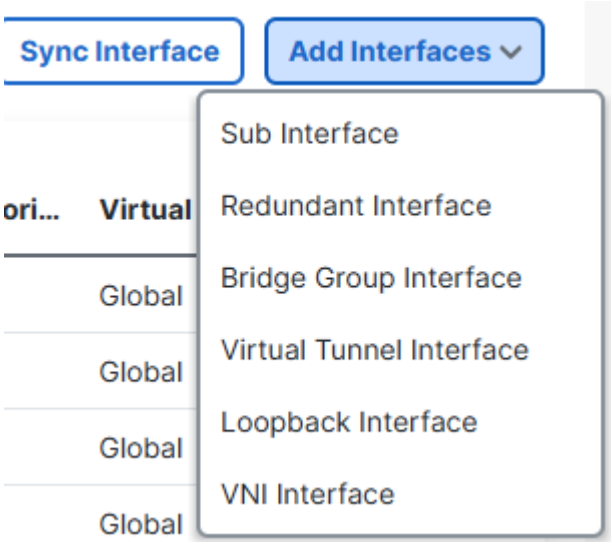
Une interface de tunnel virtuel (VTI) sur FTD est une interface logique de couche 3 utilisée pour configurer des tunnels VPN IPsec basés sur la route.

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

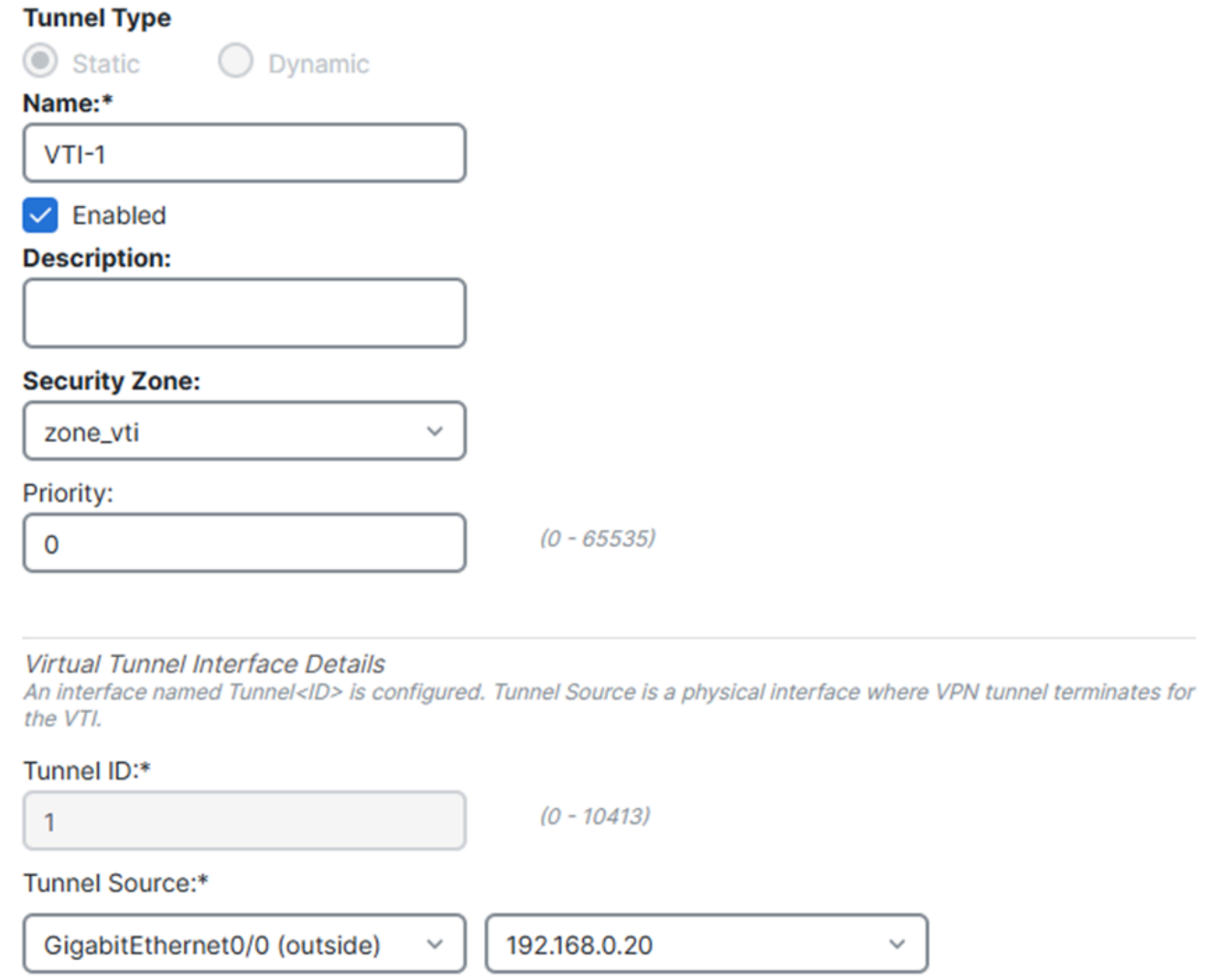


Ajouter des VTI

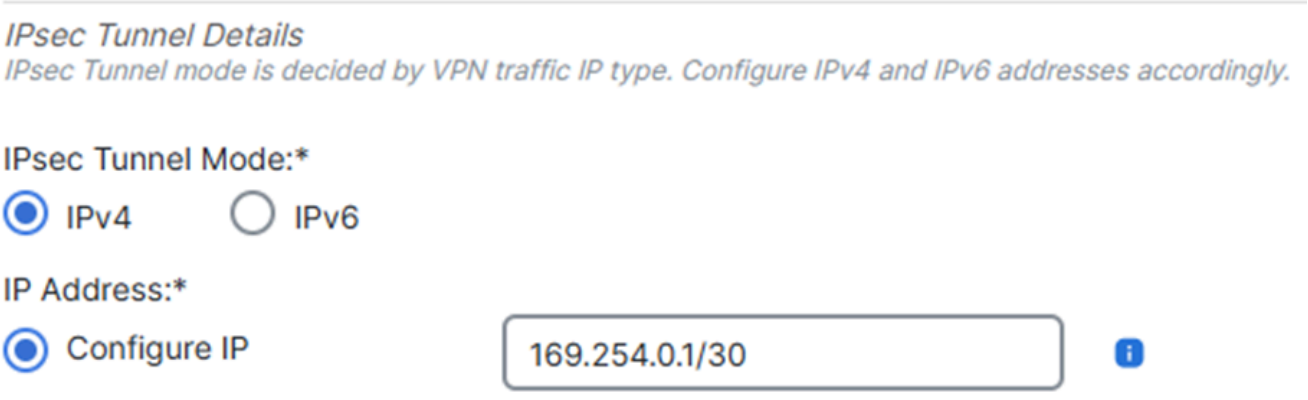
Interface de tunnel virtuel 1 :

- 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 sélectionnezIPv4
- Cliquez sur IP Address et configurez l'adresse IP pour le VTI
- Cliquez surOK



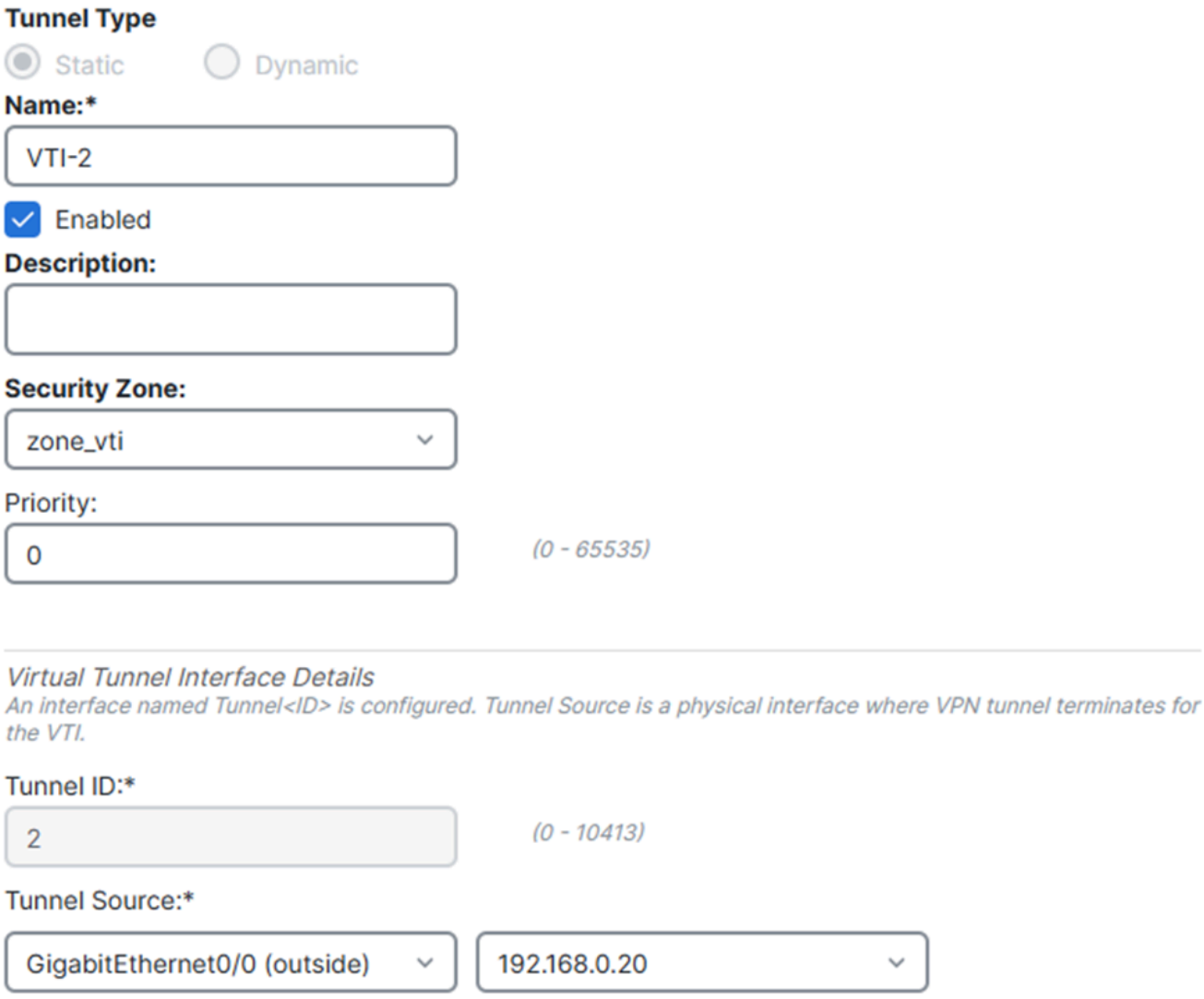
VTI1.1



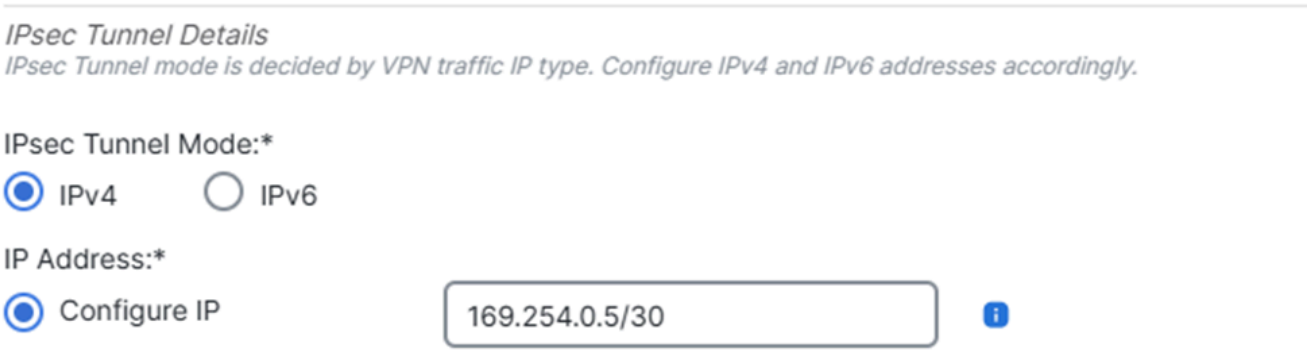
VTI1.2

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 sélectionnezIPv4
- Cliquez sur IP Address et configurez l'adresse IP pour le VTI
- Cliquez surOK

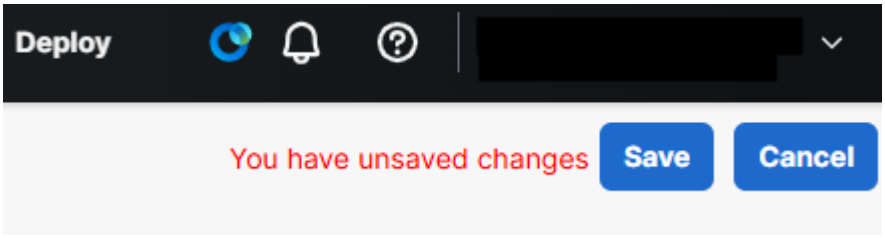


VTI2.1



VTI2.2

- Cliquez sur Enregistrer.

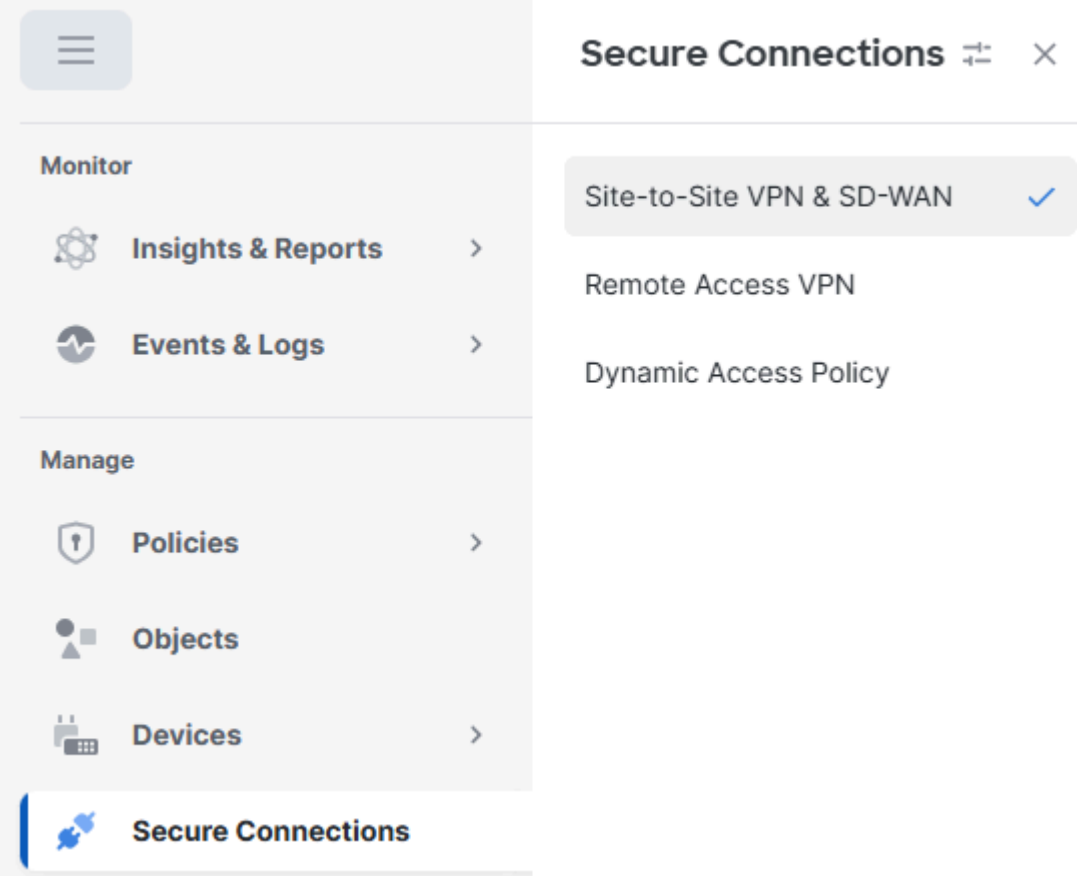


Enregistrer les modifications VTI

Configuration du tunnel IPsec

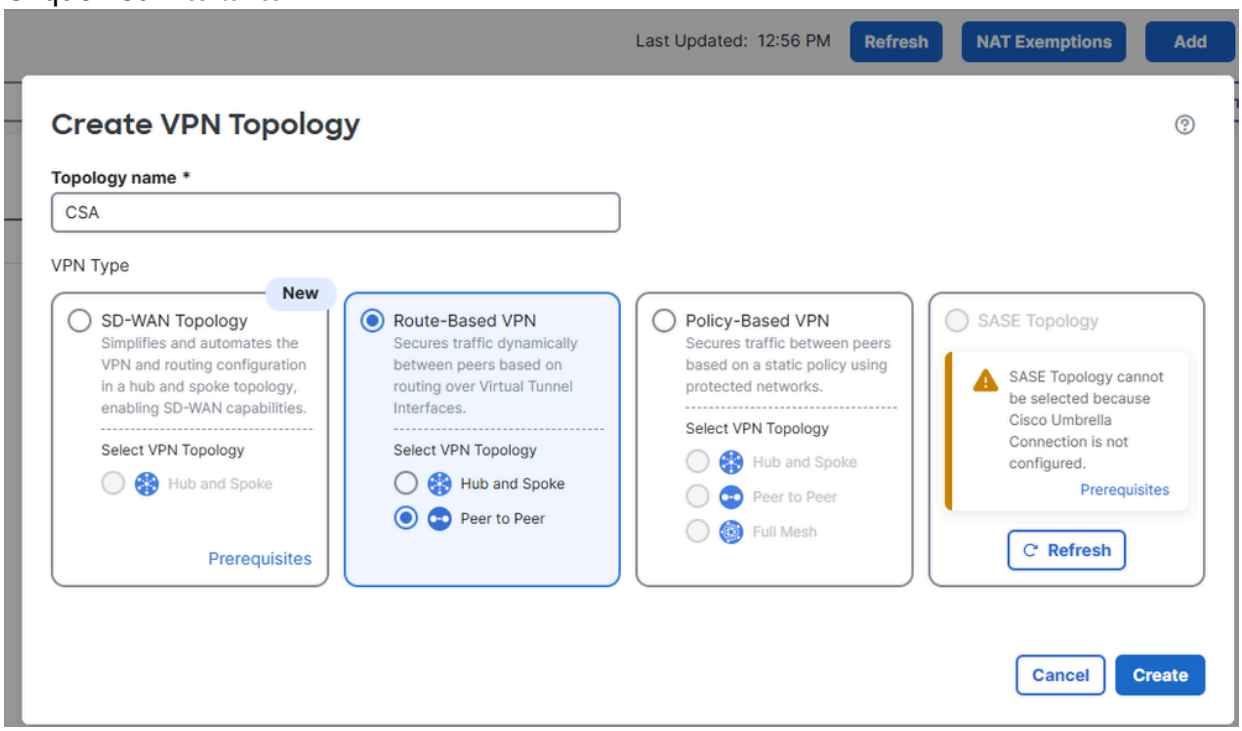
Accédez à votre tableau de bord cdFMC.

- Cliquez sur Secure Connection> Site-to-Site VPN & SD-WAN



S2S

- Cliquez surAdd
  - Cliquez sur Route-Based VPN
  - Cliquez sur Peer to Peer

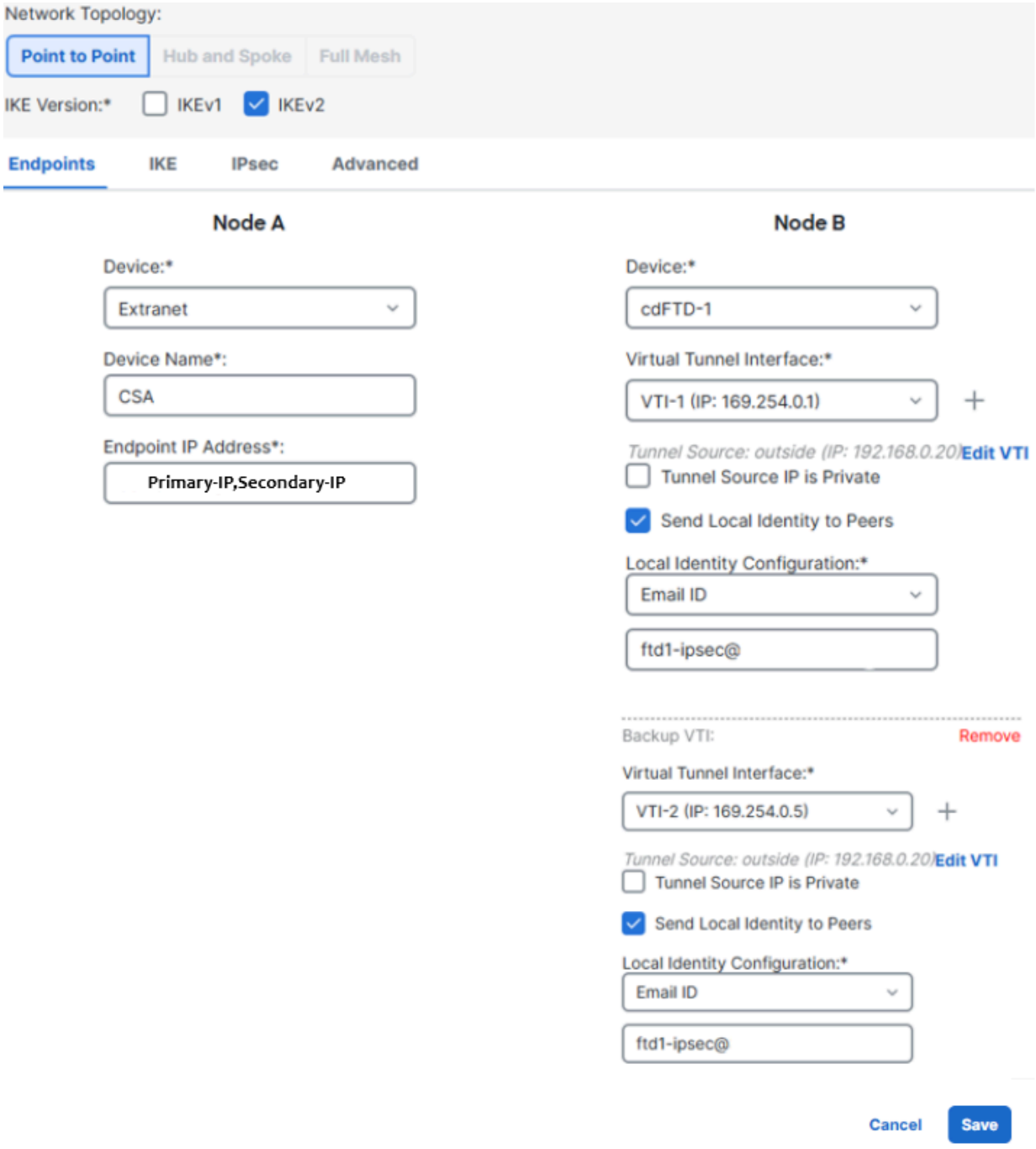


Ajouter un VPN

- À l'étape 5 de la configuration Secure Access, obtenez les ID de tunnel et les adresses IP

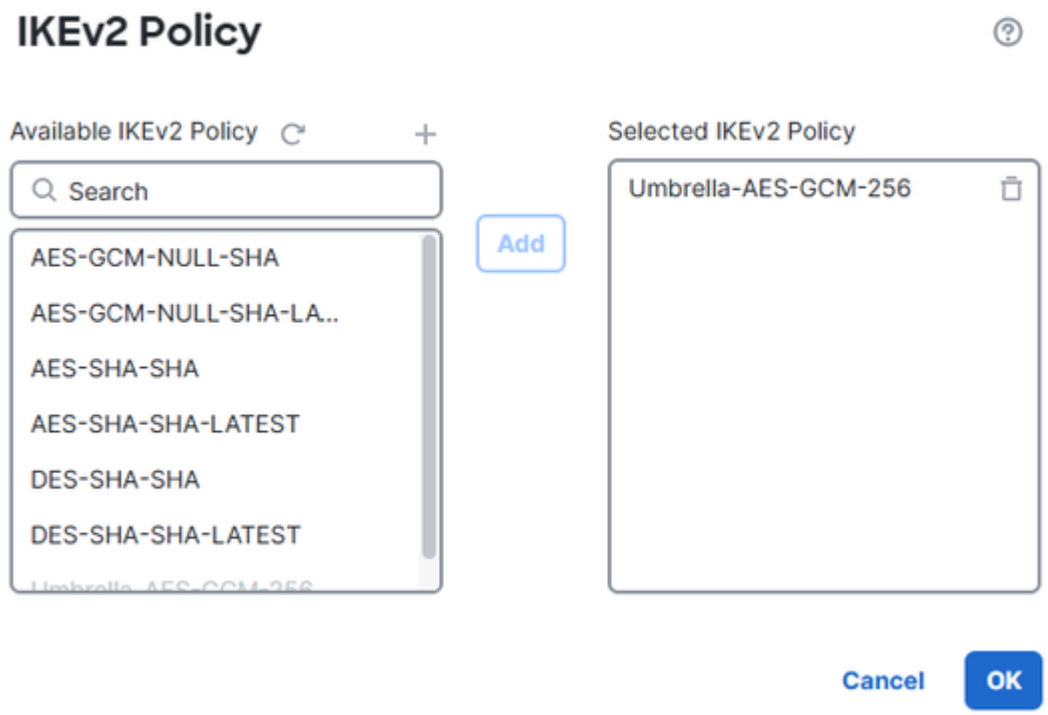
des data centers principal et secondaire

- Cliquez surEndpoints
  - SousNode A, cliquezDevicesur et sélectionnez Extranet
  - Cliquez sur Device Nameet donnez-lui un nom
  - Cliquez sur Enpoint 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 surDeviceet sélectionnez votre périphérique FTD
  - Cliquez sur Virtual Tunnel Interface et sélectionnez la première interface VTI créée à l'étape précédente
  - Cliquez sur l'Send Local Identity to Peers'option 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 surSend Local Identity to Peersonoption 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



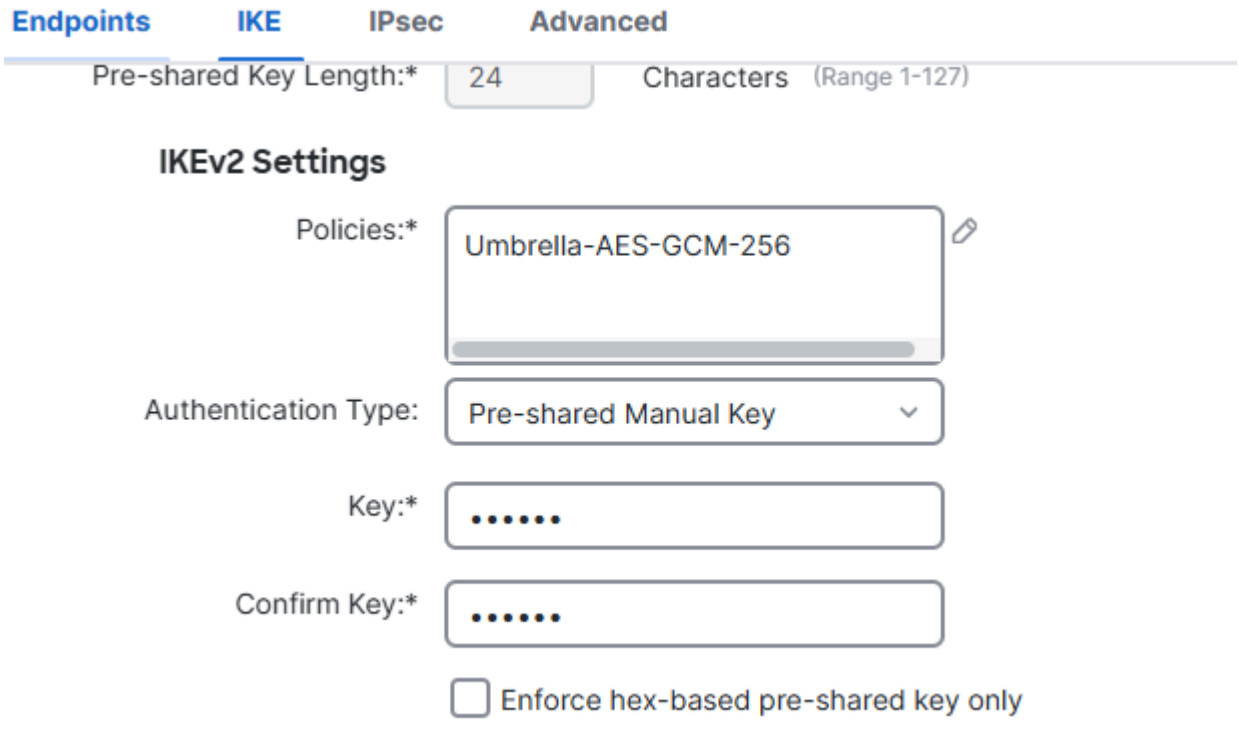
Configuration FTD VTI

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



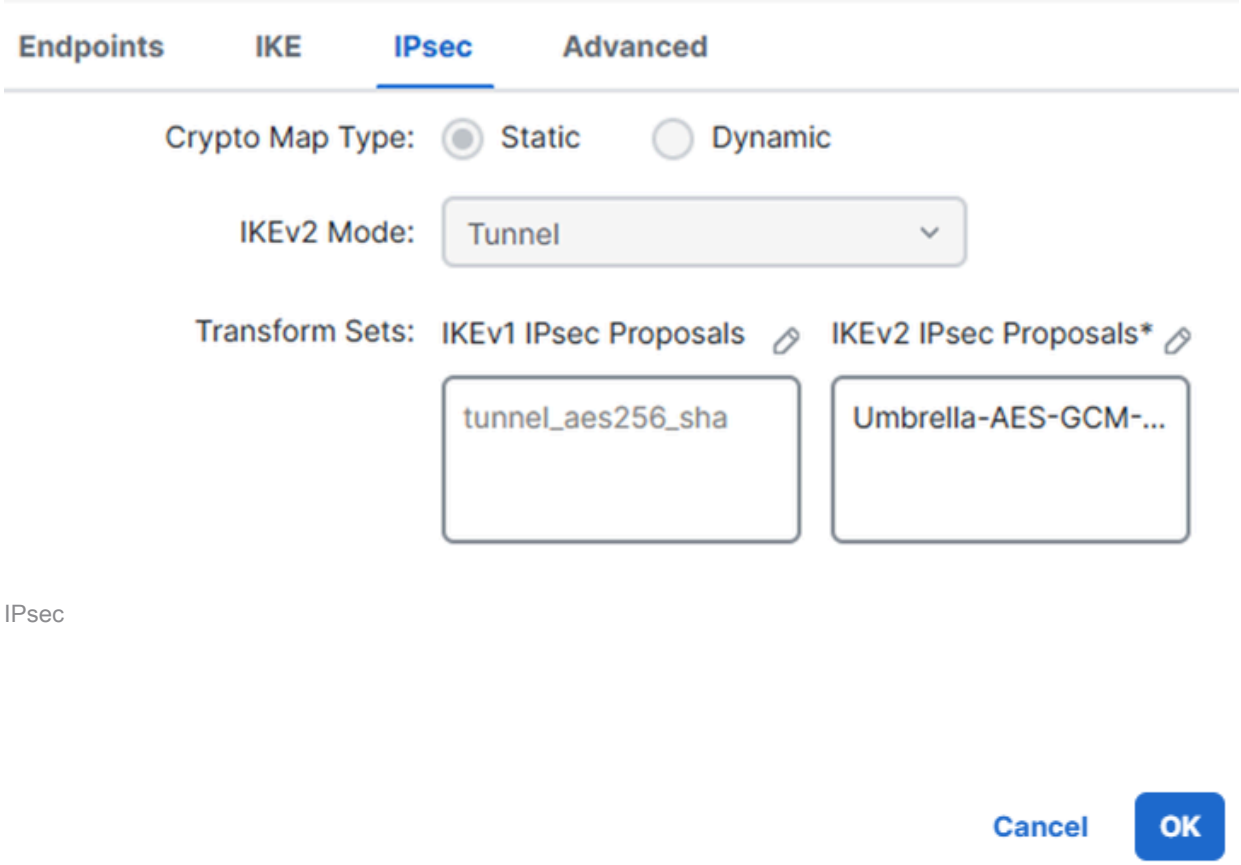
Stratégie IKEv2

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



IKE

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



IPsec

Enregistrer les propositions IKEv2

Configuration du routage FTD

Le routage PBR (Policy-Based Routing) vous permet de contrôler le transfert du trafic en fonction de critères autres que l'adresse IP de destination. Au lieu de s'appuyer uniquement sur la table de routage, PBR peut acheminer le trafic en fonction de la source, de l'application, du protocole, des ports ou d'autres politiques définies.

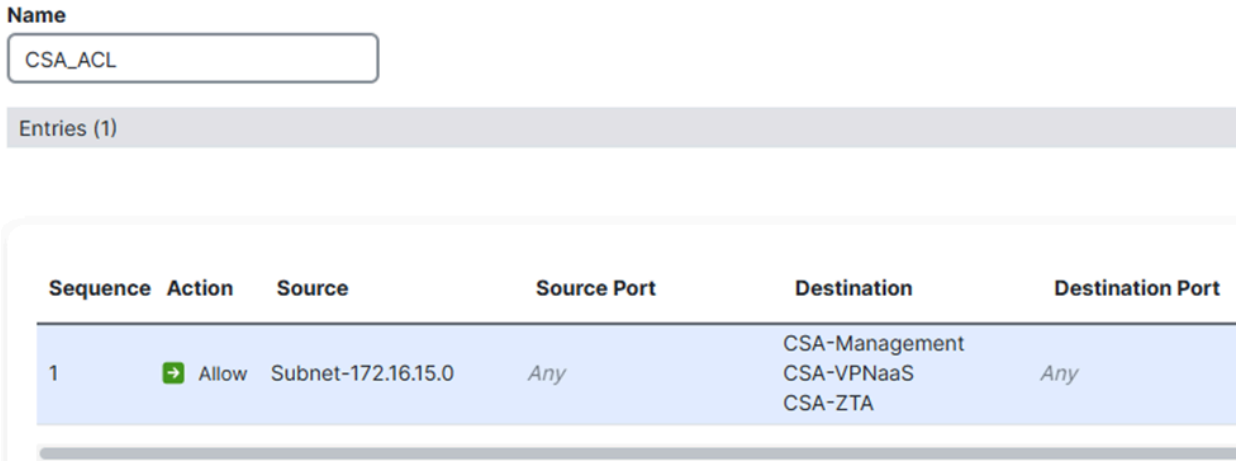
Cela permet aux entreprises d'orienter le trafic spécifique ou prioritaire sur les liaisons préférées (telles qu'une liaison Internet directe ou à bande passante élevée), d'optimiser les performances et de décomposer en toute sécurité les applications sélectionnées sans envoyer tout le trafic via un tunnel VPN.

Routage basé sur des politiques

- Naviguez jusqu'àObjects
  - Cliquez sur Access List
  - Cliquez sur Extended
  - Cliquez surAdd Extended Access List

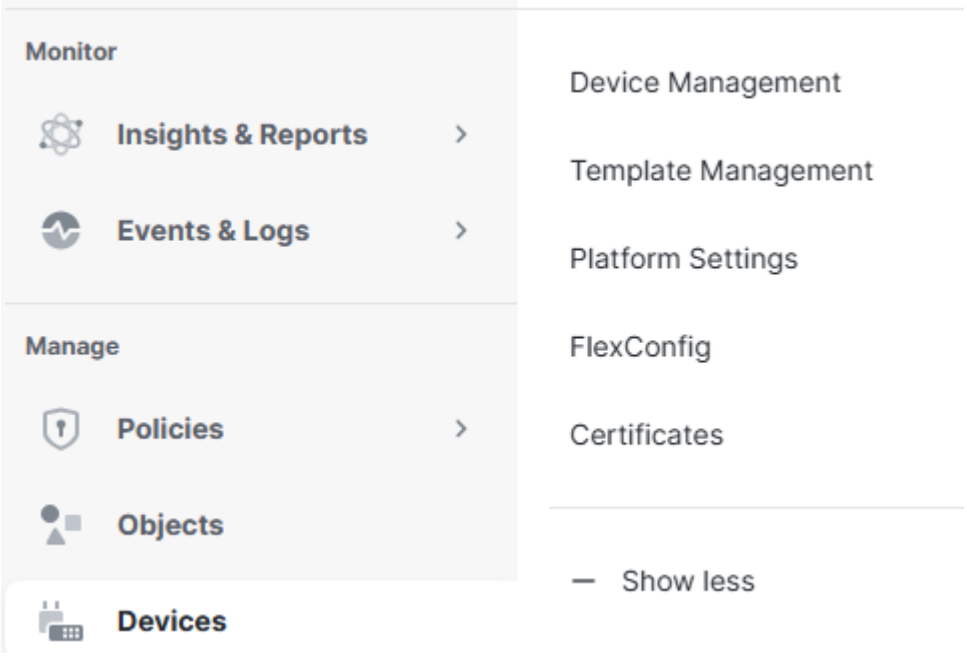
Ajouter une ACL

Créez une liste de contrôle d'accès étendue (ACL) correspondant à votre réseau source protégé par le FTD (par exemple, 172.16.15.0/24) à envoyer via le tunnel. Pour la destination, ajoutez les réseaux utilisés par ZTA (plage CGNAT) et le réseau utilisé par votre VPNaaS (cochez Virtual Private Network IP Pool).



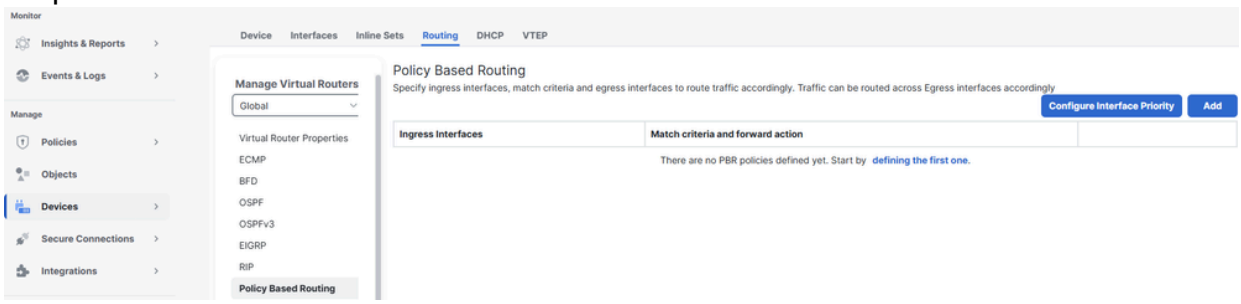
ACL

- Cliquez sur Devices> Device Management



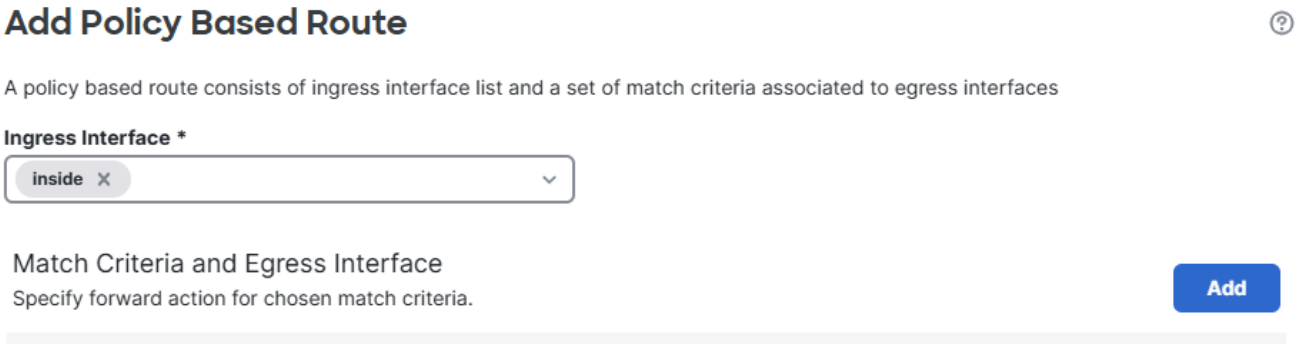
Périphérique

- Cliquez sur le FTD
  - Cliquez surRouting
  - Cliquez sur Policy Based Routing
  - Cliquez sur Add



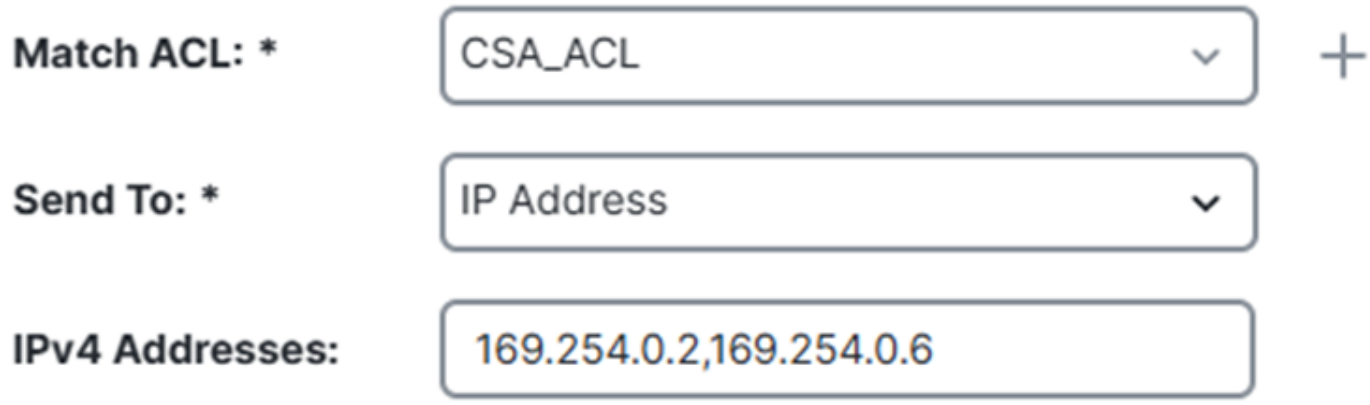
Ajouter PBR

- Cliquez sur Ingress Interface et sélectionnez l'interface d'entrée dans laquelle le trafic provenant des réseaux internes entre
- Sous Critères de correspondance et Interface de sortie, cliquez sur Add



Interface d'entrée

- Cliquez sur Match ACL et sélectionnez la liste de contrôle d'accès étendue créée précédemment
- Cliquez sur Send To and select IP Address
- Cliquez sur IPv4 Addresses et définissez comme sauts suivants les adresses IP dans les sous-réseaux d'interface VTI configurés précédemment dans le FTD (169.254.0.2 et 169.254.0.6)
- Cliquez sur Save



Configuration basée sur des stratégies

Enregistrer PBR

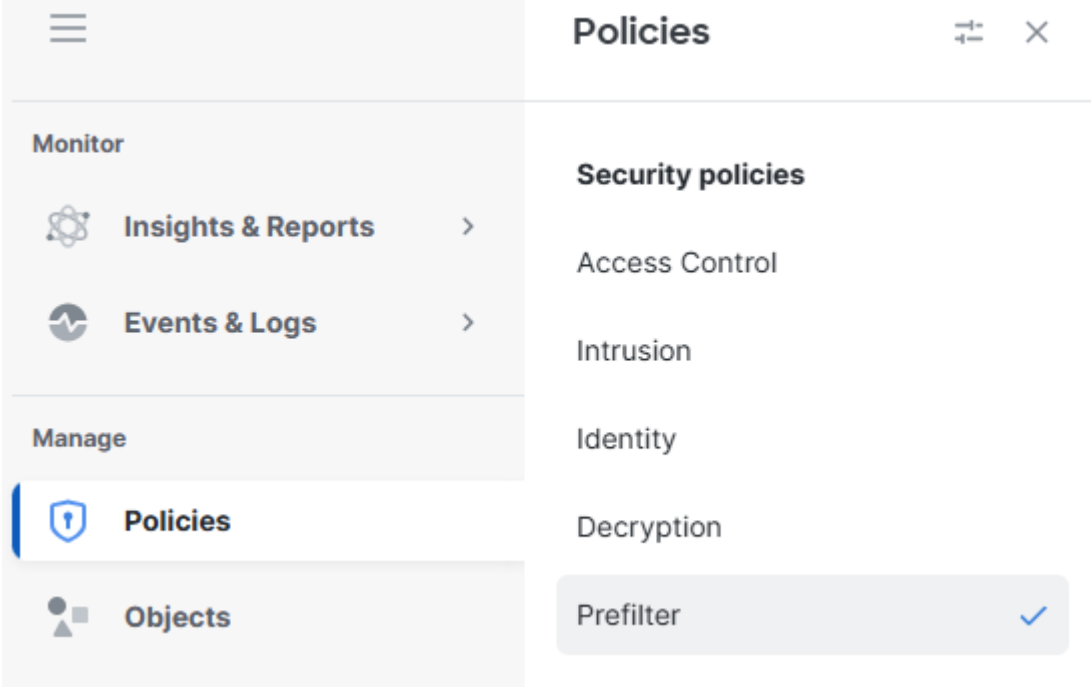
Veillez à sélectionner l'option Send To > IP Address et non l'Egress Interfaceoption.

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

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 surSave

Enregistrer la règle

À ce stade, une fois la configuration du FTD terminée et vérifiée, vous pouvez poursuivre le

déploiement. Une fois le déploiement terminé, les tunnels IPsec s'affichent correctement, confirmant ainsi l'établissement d'une connectivité sécurisée avec les ressources privées.

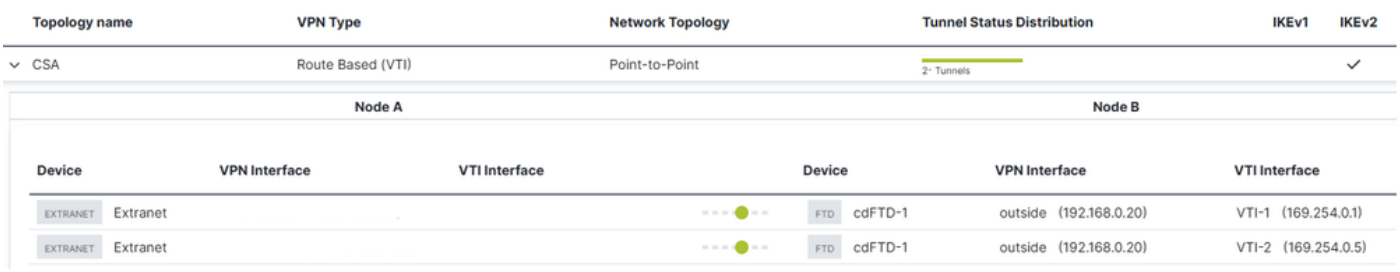
Vérifier

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 Secure Connections.
- Cliquez sur Site-to-Site VPN & SD-WAN.
- Cliquez sur le nom de la topologie.



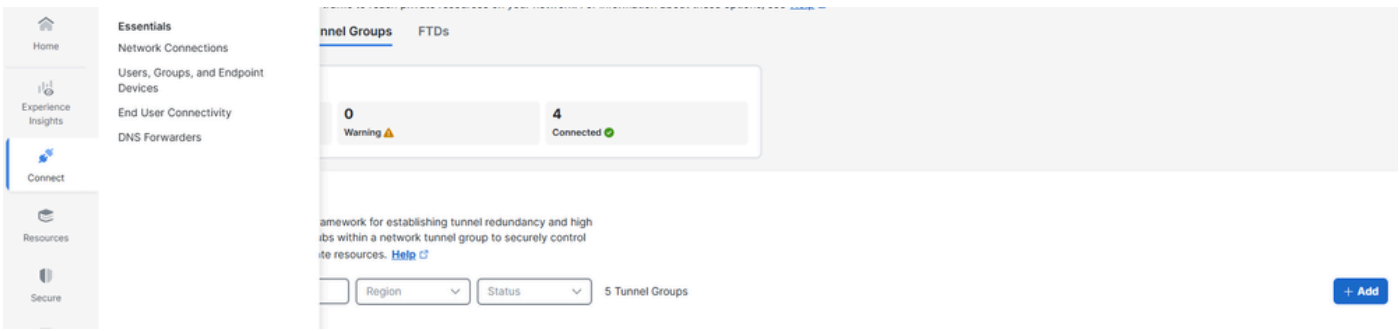
État du tunnel FTD

Vérifier dans un accès sécurisé

État du tunnel dans Secure Access

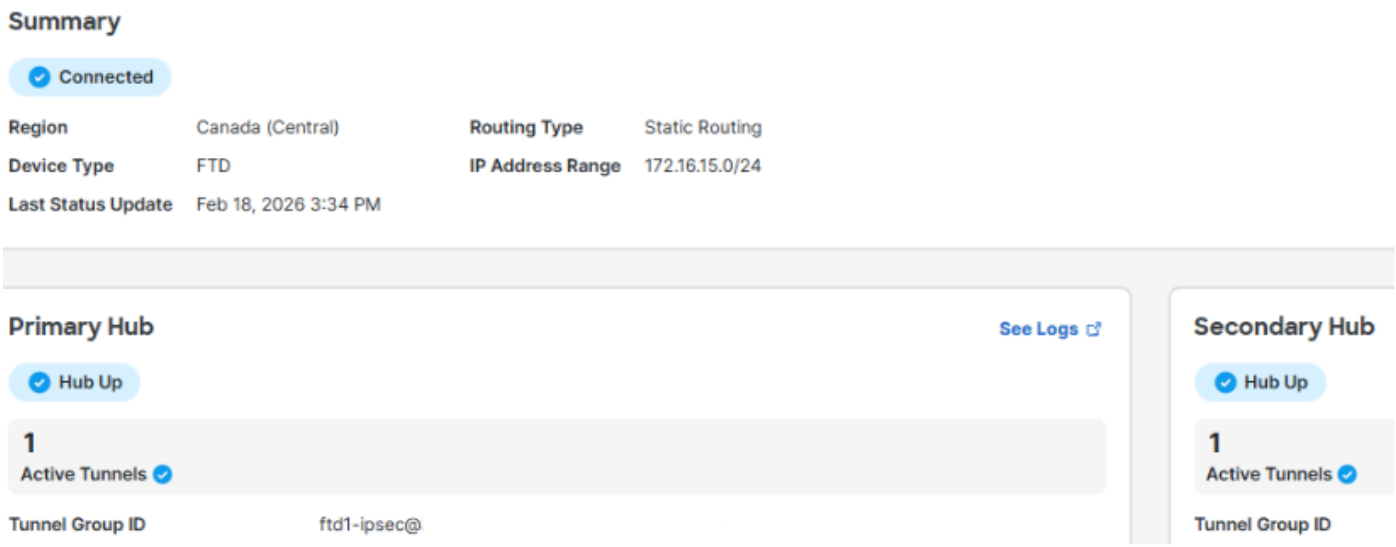
Vous pouvez afficher l'état actuel du tunnel, y compris s'il est Déconnecté, Avertissement ou Connecté. Cela permet de vérifier que le tunnel IPsec est correctement établi.

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



Vérifier NTG

- Cliquez sur le groupe de tunnels réseau

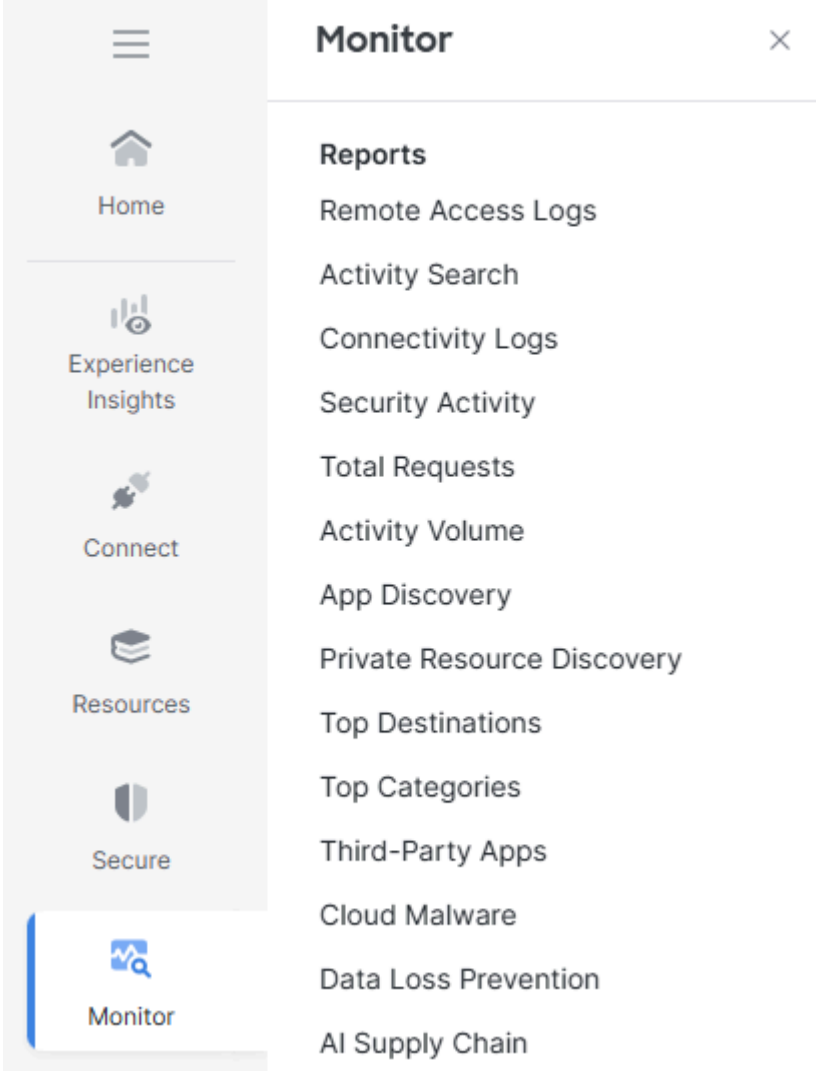


État du tunnel CSA

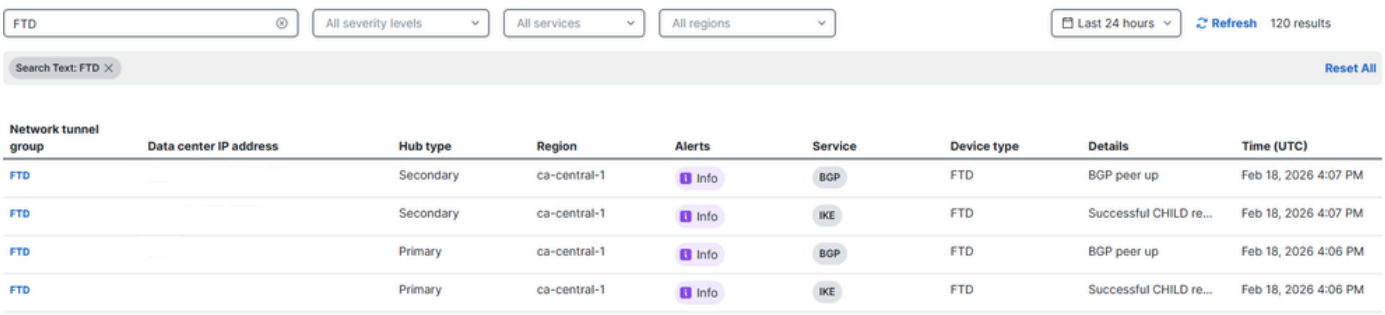
Événements dans l'accès sécurisé

Vous pouvez afficher les événements de tunnel et confirmer si l'état des tunnels IPsec est up et stable.

Cliquez sur Monitor > Network Connectivity.

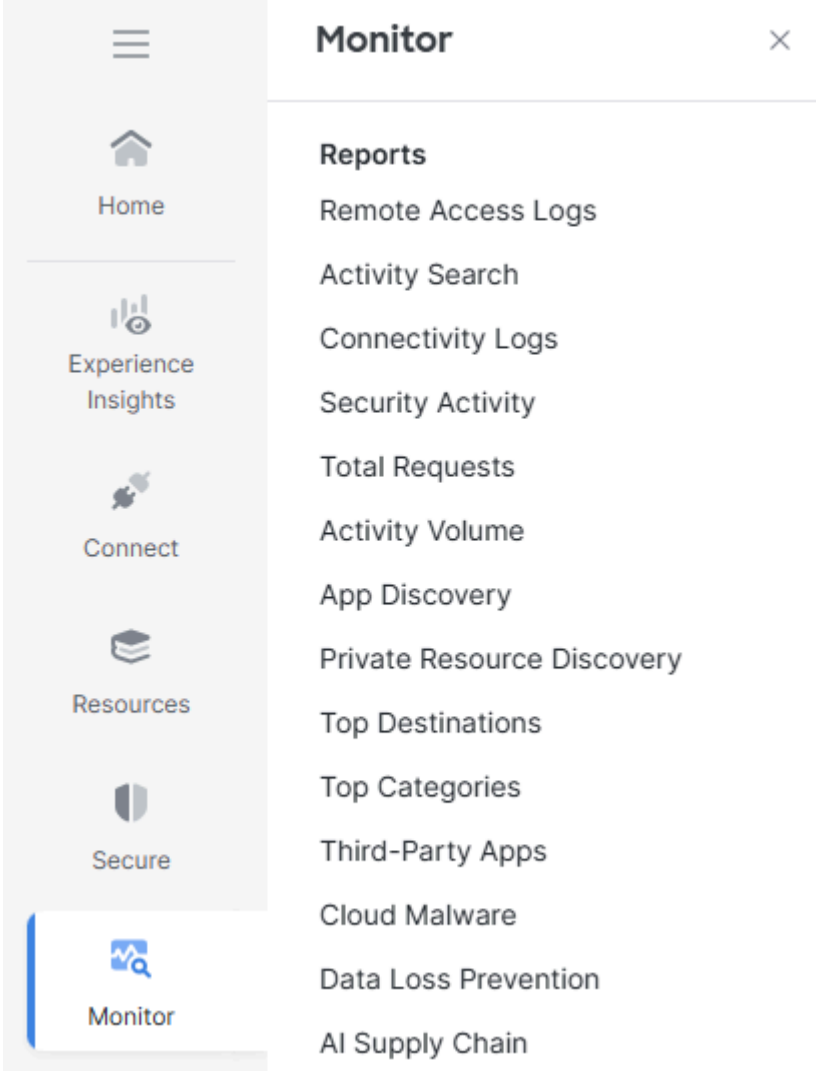


Surveiller les journaux de connexion



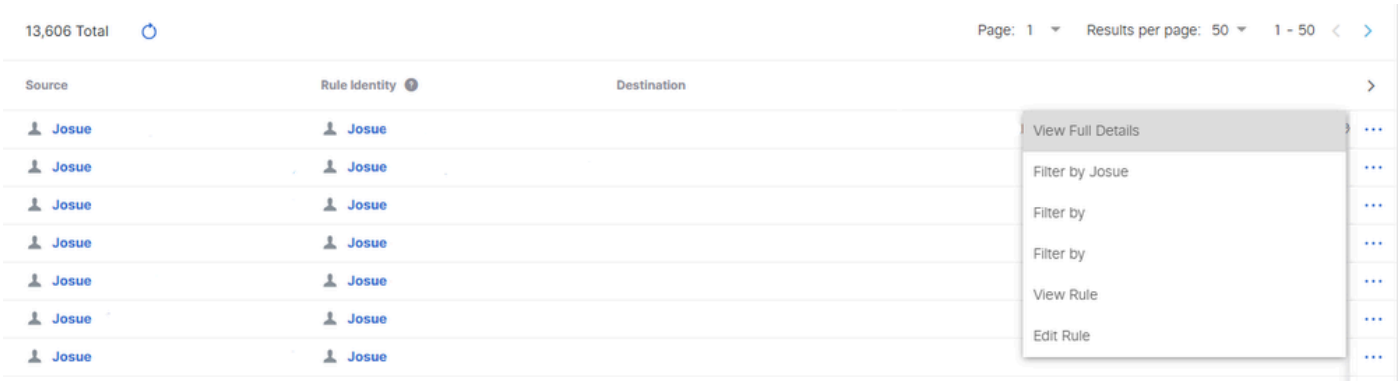
Journaux de connexion

Naviguez jusqu'à Monitor > Activity Search.

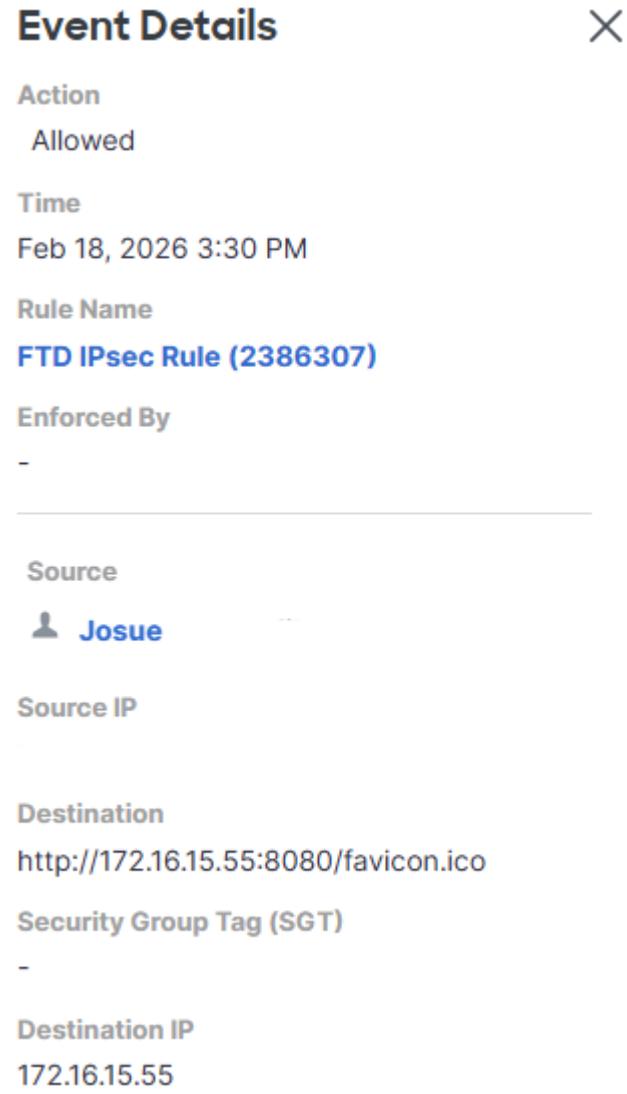


Surveiller les journaux de connexion

Pour l'un des événements associés, cliquez sur Afficher les détails complets.



Détails complets



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.