Configuration des interfaces VXLAN sur Secure FTD avec Secure FMC

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Diagramme du réseau

Configurer

- Configurer le groupe d'homologues VTEP
- Configurer l'interface source VTEP
- Configuration de l'interface VNI VTEP

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit comment configurer les interfaces VXLAN sur Secure Firewall Threat Defense (FTD) avec Secure Firewall Management Center (FMC)

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Concepts VLAN/VXLAN de base.
- Connaissances de base du réseau.
- Expérience de base de Cisco Secure Management Center.
- Expérience de base de Cisco Secure Firewall Threat Defense.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware version 7.2.4.
- Appliance virtuel Cisco Secure Firewall Threat Defense (FTDv) VMware exécutant la version

7.2.4.

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

Le VLAN extensible virtuel (VXLAN) fournit des services réseau Ethernet de couche 2 comme le VLAN traditionnel. En raison de la forte demande de segments VLAN dans les environnements virtuels, le VXLAN offre une plus grande extensibilité, une plus grande flexibilité et définit également un schéma d'encapsulation MAC-in-UDP dans lequel la trame de couche 2 d'origine a un en-tête VXLAN ajouté et est ensuite placée dans un paquet UDP-IP. Avec cette encapsulation MAC-in-UDP, VXLAN effectue un tunnel du réseau de couche 2 sur le réseau de couche 3. VXLAN offre les avantages suivants :

- Flexibilité VLAN dans les segments multilocataires :
- Évolutivité supérieure pour traiter davantage de segments de couche 2 (L2).
- Meilleure utilisation du réseau

Cisco Secure Firewall Threat Defense (FTD) prend en charge deux types d'encapsulation VXLAN.

- VXLAN (utilisé pour tous les modèles de défense contre les menaces de pare-feu sécurisé)
- Geneve (utilisé pour l'appliance virtuelle Secure Firewall Threat Defense)

L'encapsulation Geneve est nécessaire pour le routage transparent des paquets entre l'équilibreur de charge de passerelle Amazon Web Services (AWS) et les appareils, et pour l'envoi d'informations supplémentaires.

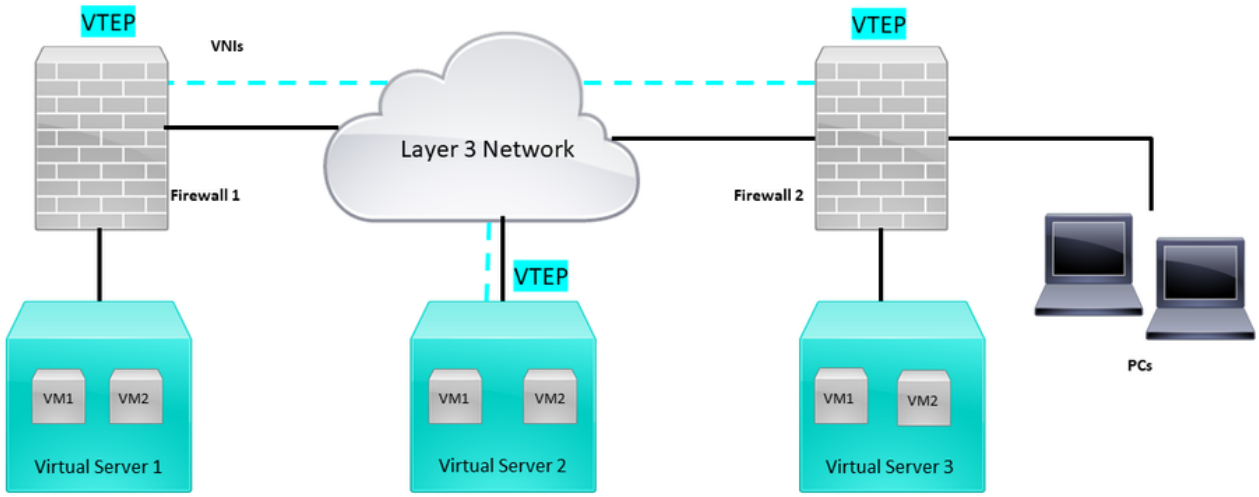
VXLAN utilise le terminal de tunnel VXLAN (VTEP) pour mapper les périphériques finaux des locataires aux segments VXLAN et pour effectuer l'encapsulation et la décapsulation VXLAN. Chaque VTEP possède deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier) où la politique de sécurité peut être appliquée, et une interface régulière appelée interface source VTEP où les interfaces VNI sont tunnellisées entre les VTEP. L'interface source VTEP est connectée au réseau IP de transport pour la communication VTEP à VTEP, les interfaces VNI sont similaires aux interfaces VLAN : il s’agit d’interfaces virtuelles qui séparent le trafic réseau sur une interface physique donnée à l’aide de l’étiquetage. La stratégie de sécurité est appliquée à chaque interface VNI. Une interface VTEP peut être ajoutée et toutes les interfaces VNI sont associées à la même interface VTEP. Il existe une exception pour le clustering virtuel de défense contre les menaces sur AWS.

La défense contre les menaces encapsule et décapsule de trois manières :

- Une adresse IP VTEP homologue unique peut être configurée de manière statique sur la défense contre les menaces.
- Un groupe d'adresses IP VTEP homologues peut être configuré de manière statique sur la défense contre les menaces.
- Un groupe de multidiffusion peut être configuré sur chaque interface VNI.

Ce document est axé sur les interfaces VXLAN pour l'encapsulation VXLAN avec un groupe de 2 adresses IP VTEP homologues configurées de manière statique. Si vous devez configurer des interfaces Geneve, consultez la documentation officielle des interfaces Geneve dans AWS ou configurez VTEP avec un seul homologue ou un groupe de multidiffusion, vérifiez l'interface VTEP avec un guide de configuration d'homologue unique ou de groupe de multidiffusion.

Diagramme du réseau



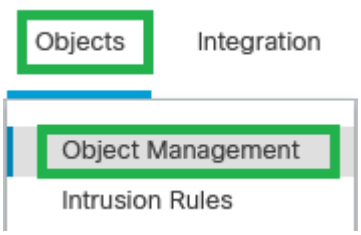
Topologie du réseau

La section configure suppose que le réseau sous-jacent est déjà configuré pour la défense contre les menaces via le Centre de gestion du pare-feu sécurisé. Ce document est axé sur la configuration du réseau de superposition.

Configurer

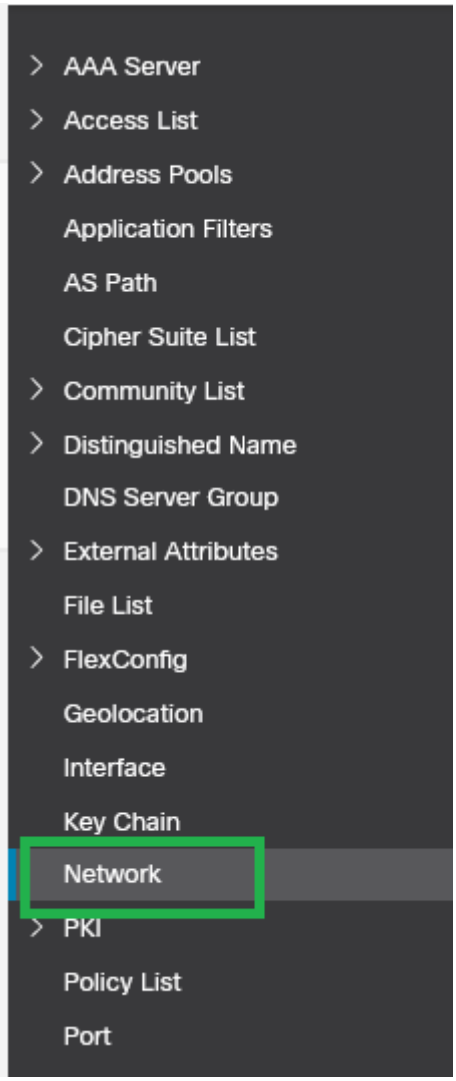
Configurer le groupe d'homologues VTEP

Étape 1: Accédez à Objets > Gestion des objets.



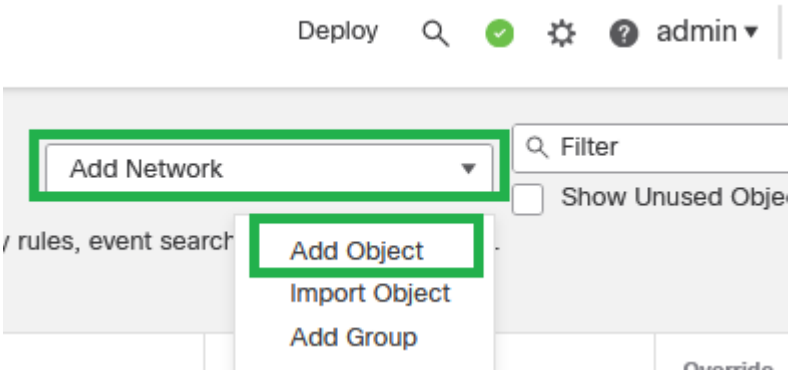
Objets - Gestion des objets

Étape 2: Cliquez sur Réseau dans le menu de gauche.



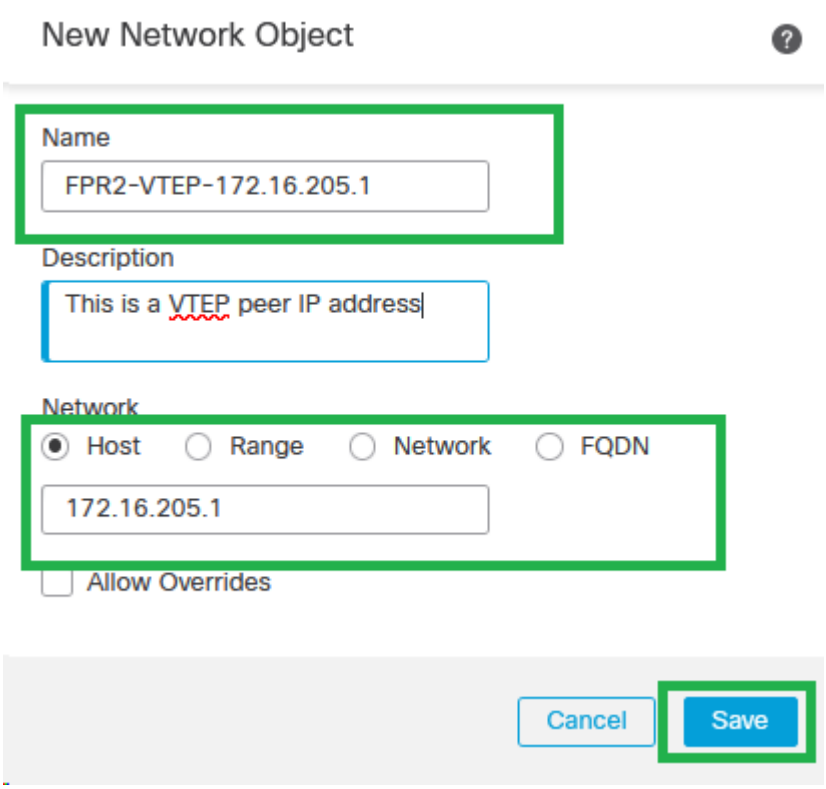
Réseau

Étape 3: Créez des objets hôtes réseau pour les adresses IP homologues VTEP. Cliquez sur Add Network > Add Object.



Ajouter un réseau - Ajouter un objet

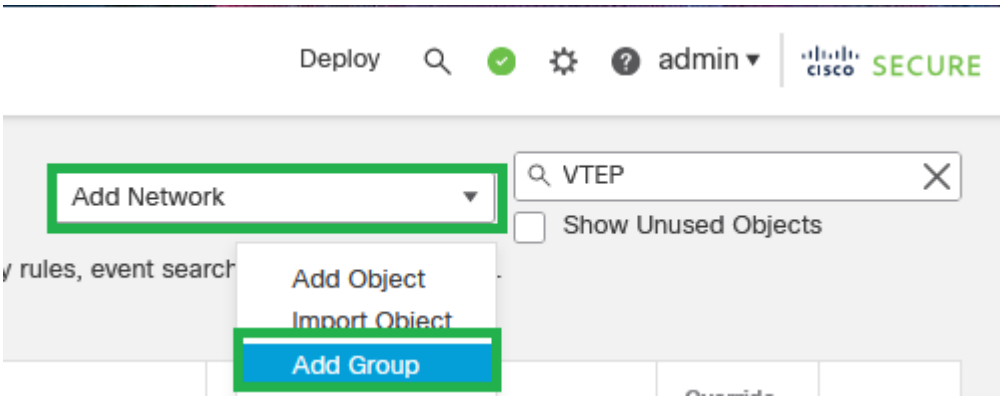
Étape 4: Créez un nouvel objet réseau hôte pour l'homologue VTEP. Configurez un nom d'objet et une adresse IP, puis cliquez sur Enregistrer.



Nouvel objet réseau

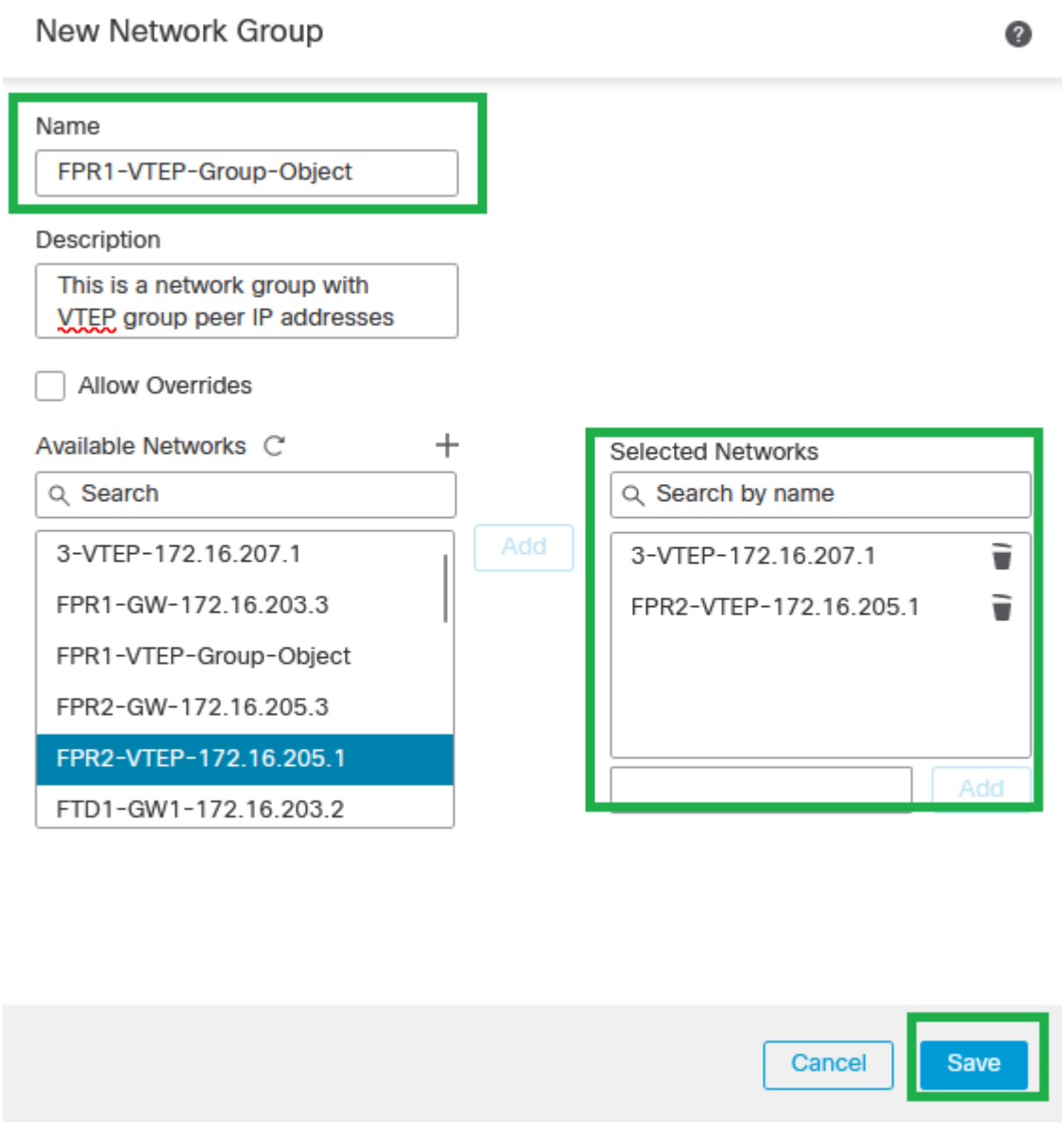
Remarque : Configurez davantage d'objets réseau hôtes pour chaque adresse IP d'homologue VTEP dont vous disposez. Ce guide de configuration contient deux objets.

Étape 5: Créez un groupe d'objets, cliquez sur Ajouter un réseau > Ajouter un groupe.



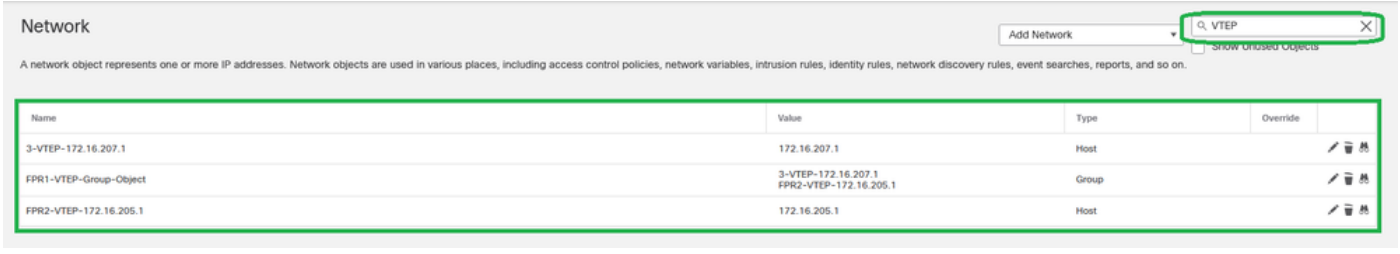
Ajouter un réseau - Ajouter un groupe

Étape 6 : Créez le groupe d'objets réseau avec toutes les adresses IP des homologues VTEP. Configurez un nom de groupe réseau et sélectionnez les groupes d'objets réseau requis, puis cliquez sur Enregistrer.



Créer un groupe d'objets réseau

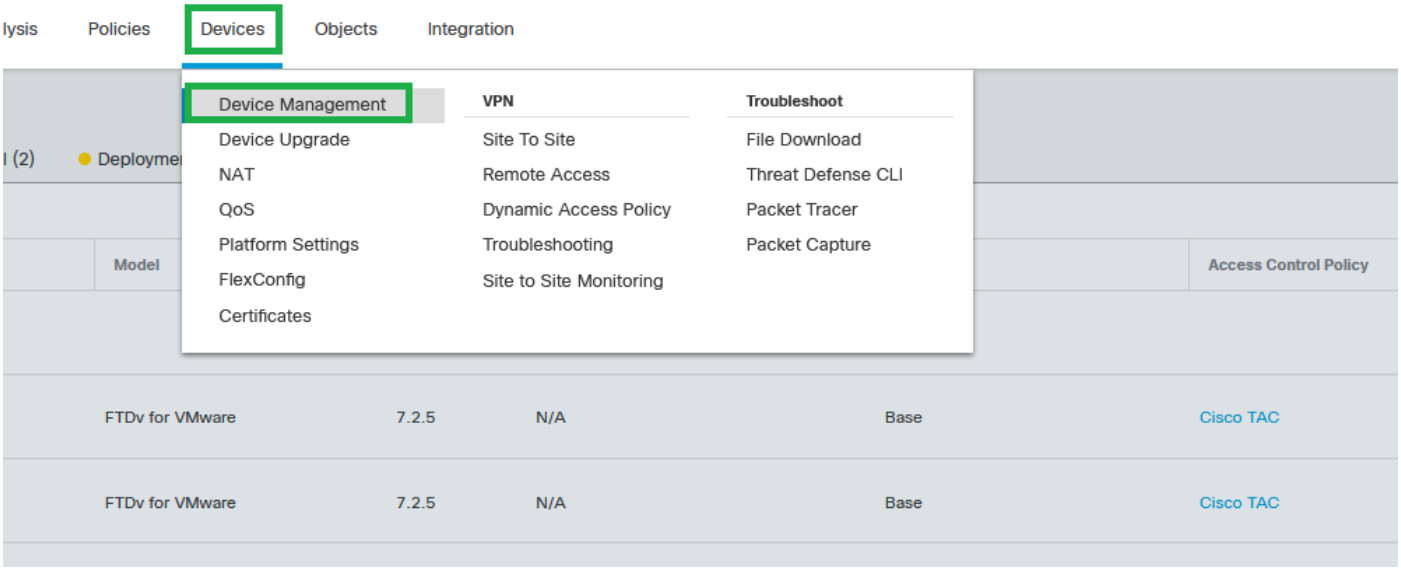
Étape 7: Validez l'objet réseau et le groupe d'objets réseau à partir du filtre Objet réseau.



Valider le groupe d'objets VTEP

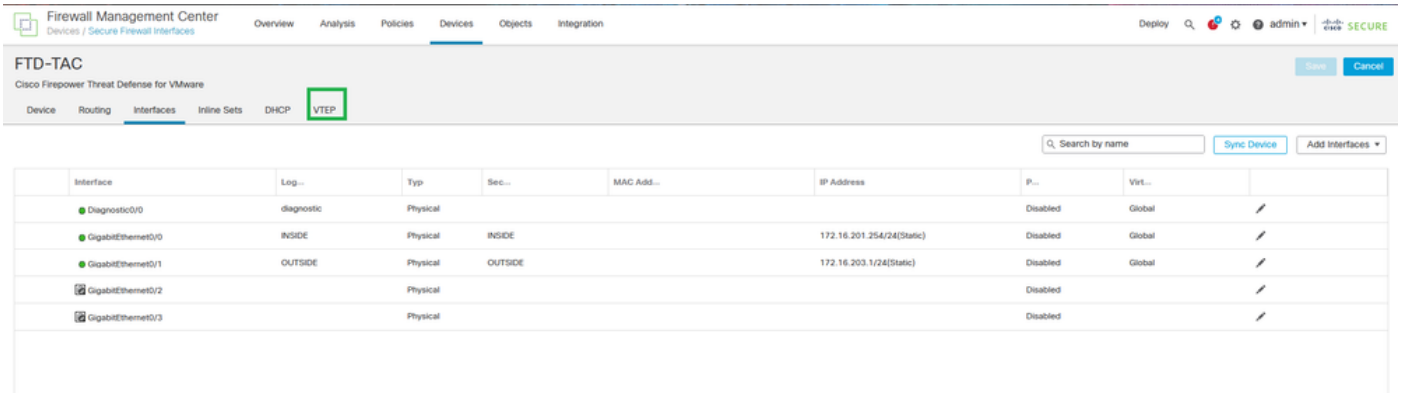
Configurer l’interface source VTEP

Étape 1: Accédez à Périphériques > Gestion des périphériques, et modifiez la défense contre les menaces.



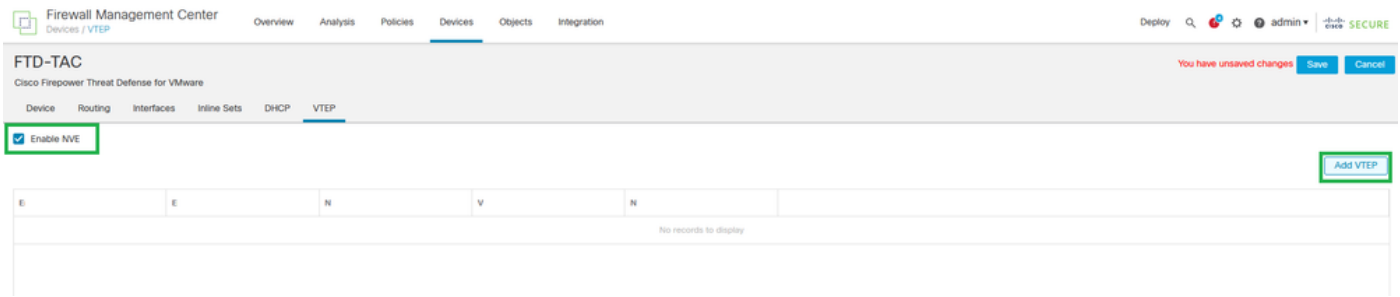
Périphériques - Gestion des périphériques

Étape 2: Accédez à la section VTEP.



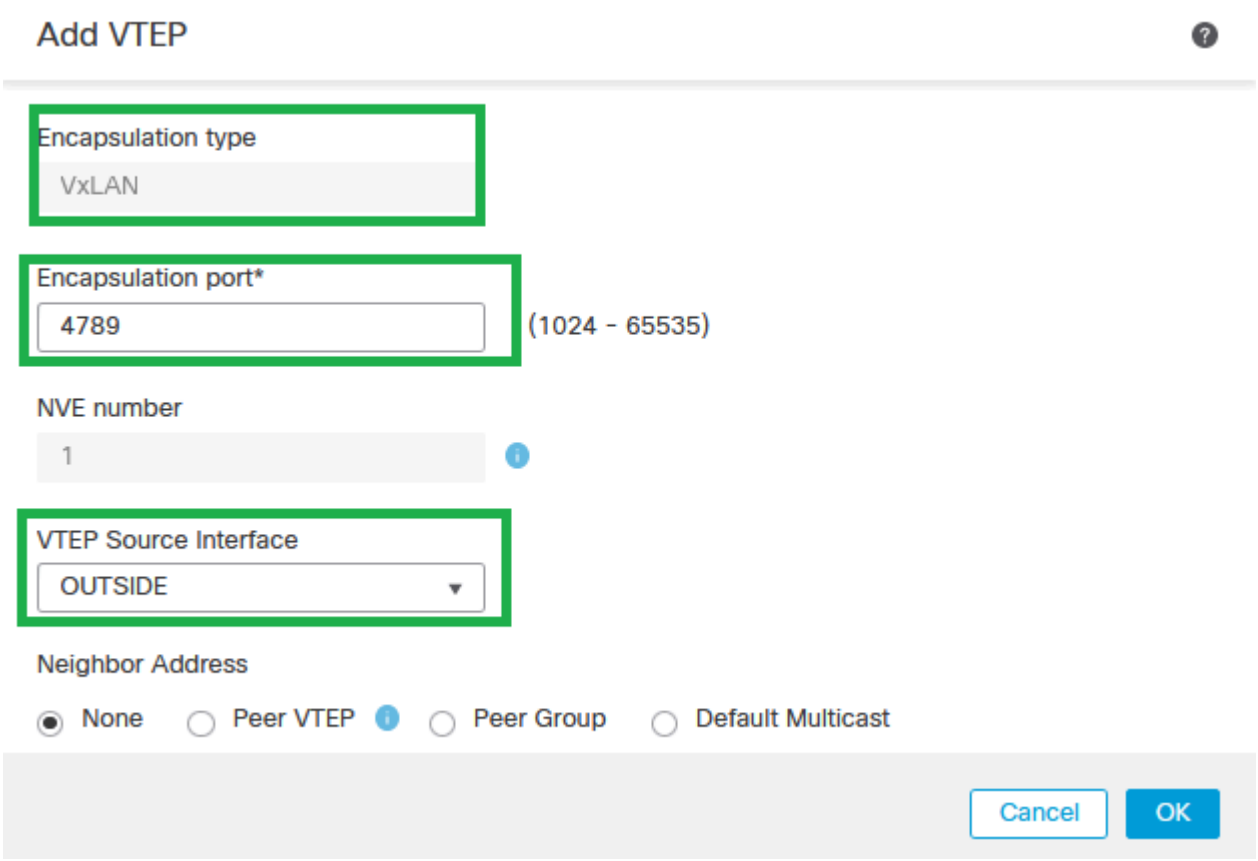
section VTEP

Étape 3: Cochez la case Enable VNE, puis cliquez sur Add VTEP.



Activer NVE et ajouter VTEP

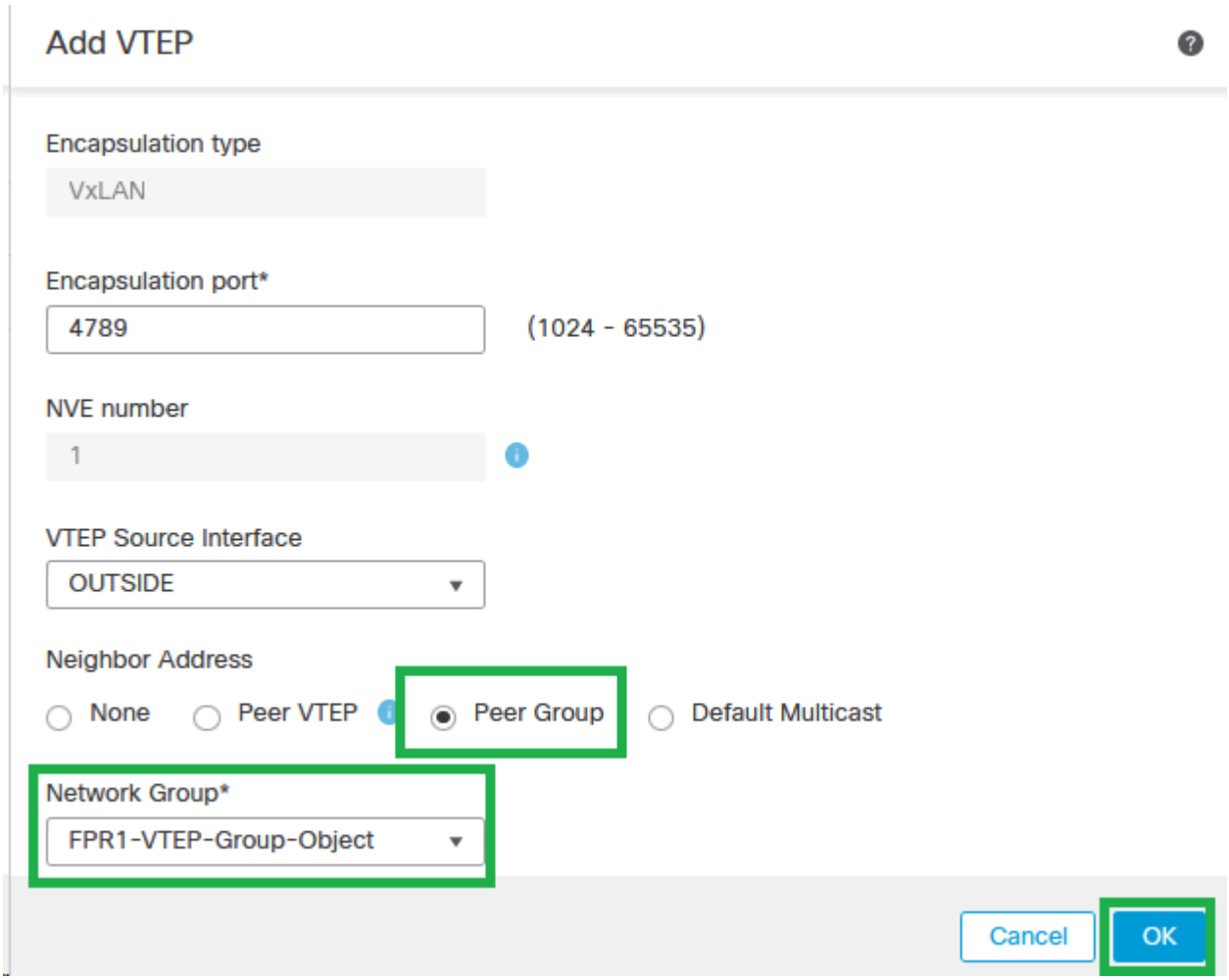
Étape 4: Choisissez VxLAN comme type d'encapsulation, entrez la valeur Encapsulation Port et choisissez l'interface utilisée pour la source VTEP sur cette défense contre les menaces (interface externe pour ce guide de configuration)



Ajouter un VTEP

Remarque : L'encapsulation VxLAN est celle par défaut. Pour AWS, vous pouvez choisir entre VxLAN et Geneve. La valeur par défaut est 4789, Any Encapsulation Port peut être choisi entre 1024 - 65535 plage selon la conception.

Étape 5: Sélectionnez Peer Group et choisissez le groupe d'objets réseau créé dans la section de configuration précédente, puis cliquez sur OK.

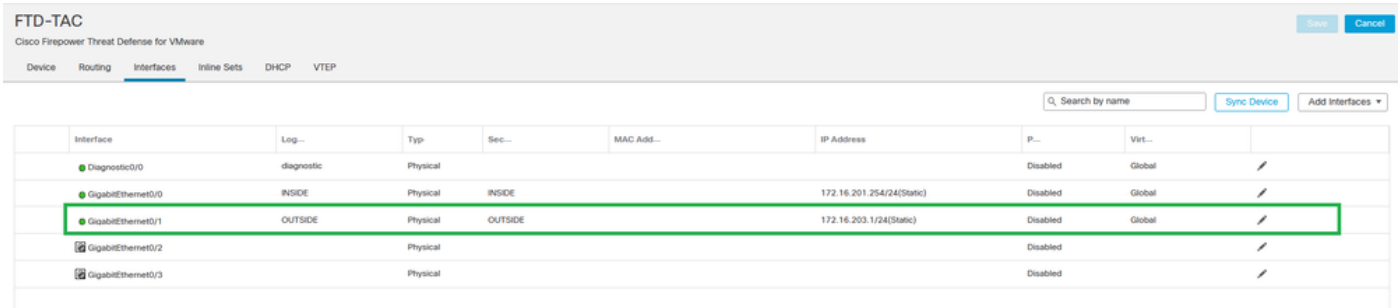


Groupe d'homologues - Groupe d'objets réseau

Étape 6: Enregistrez les modifications.

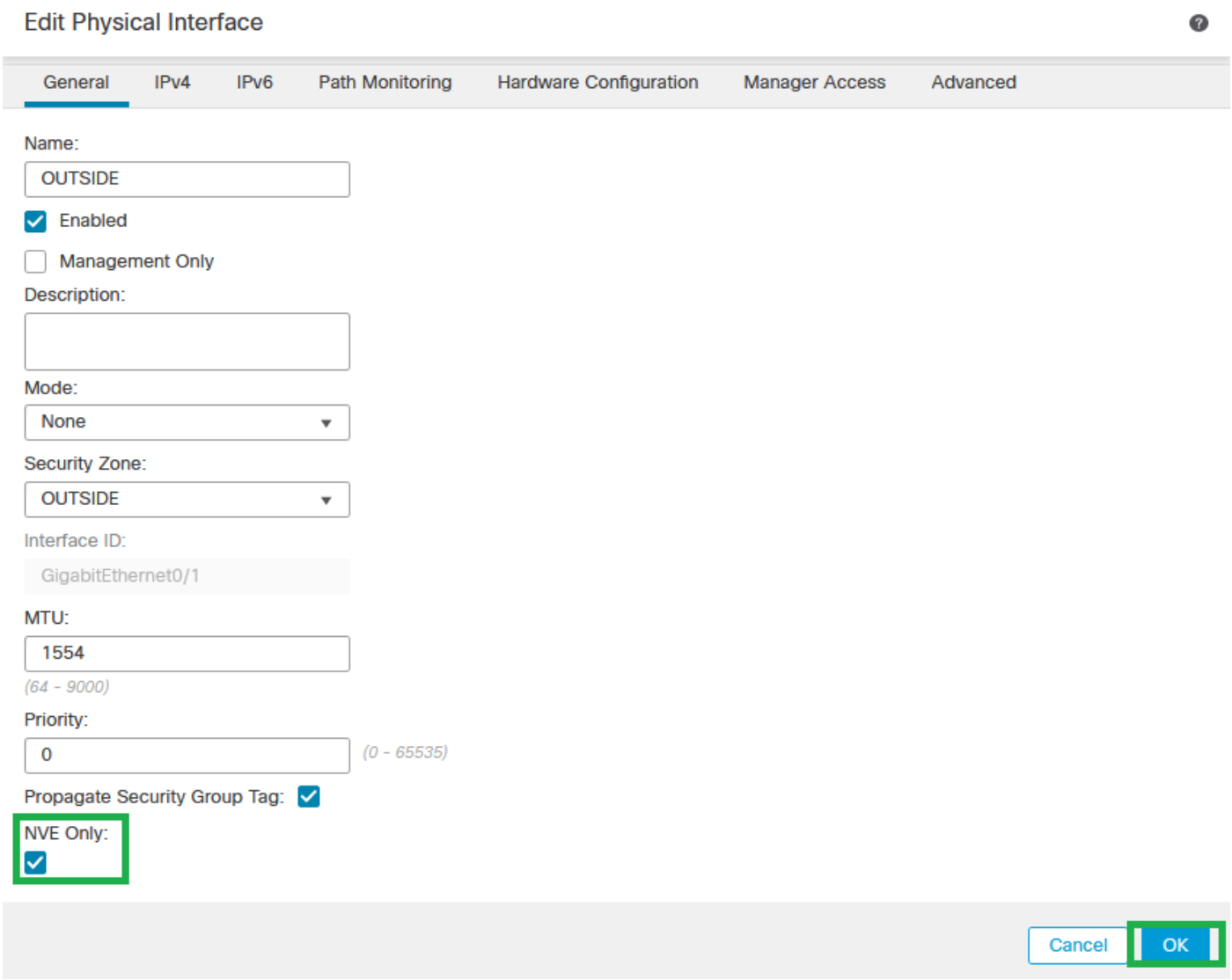
Avertissement : Une fois les modifications enregistrées, un message de modification de trame jumbo apparaît, MTU est modifié sur l'interface affectée comme VTEP à 1554, assurez-vous d'utiliser le même MTU sur le réseau sous-jacent.

Étape 7 :Cliquez sur Interfaces et modifiez l'interface utilisée pour l'interface source VTEP. (Interface externe de ce guide de configuration)



Externe comme interface source VTEP

Étape 8 (Facultatif) :Sur la page Général, cochez la case NVE Only, puis cliquez sur OK.



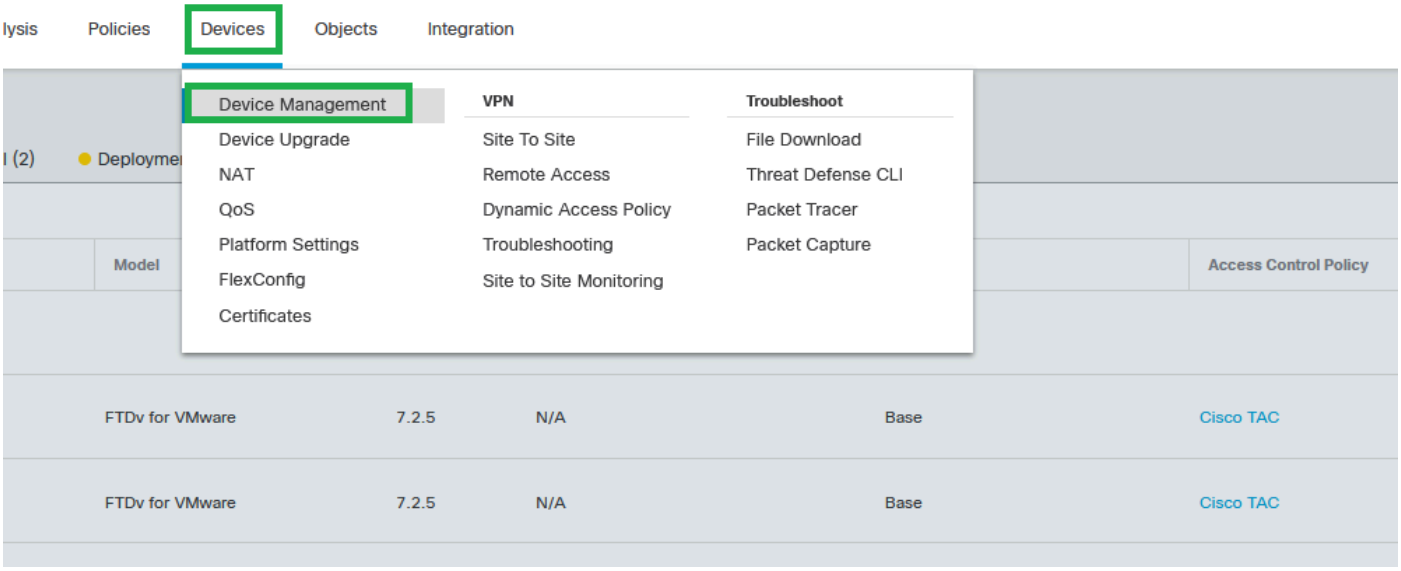
Configuration NVE uniquement

Avertissement : Ce paramètre est facultatif pour le mode routé où ce paramètre limite le trafic au VXLAN et au trafic de gestion commun uniquement sur cette interface. Ce paramètre est automatiquement activé pour le mode pare-feu transparent.

Étape 9: Enregistrez les modifications.

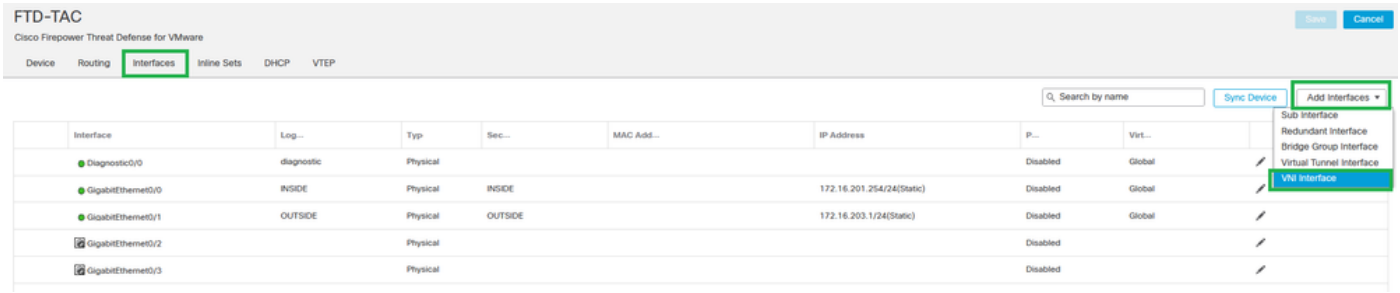
Configuration de l'interface VNI VTEP

Étape 1: Naviguez Périphériques > Gestion des périphériques, et modifiez la défense contre les menaces.



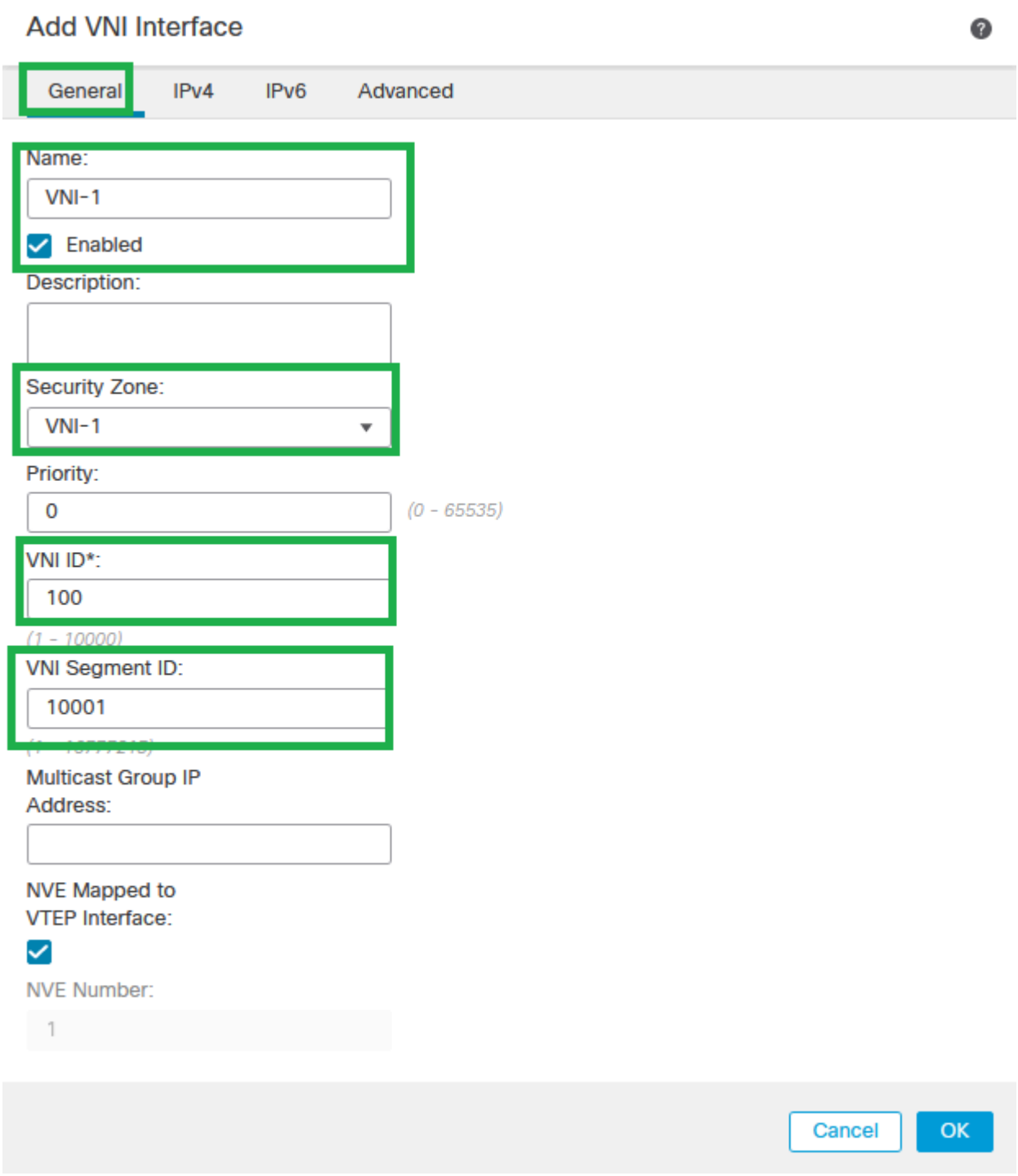
Périphériques - Gestion des périphériques

Étape 2: Dans la section Interfaces, cliquez sur Add Interfaces > VNI Interfaces.



Interfaces - Ajouter des interfaces - Interfaces VNI

Étape 3: Dans la section General, configurez l'interface VNI avec le nom, la description, la zone de sécurité, l'ID VNI et l'ID de segment VNI.



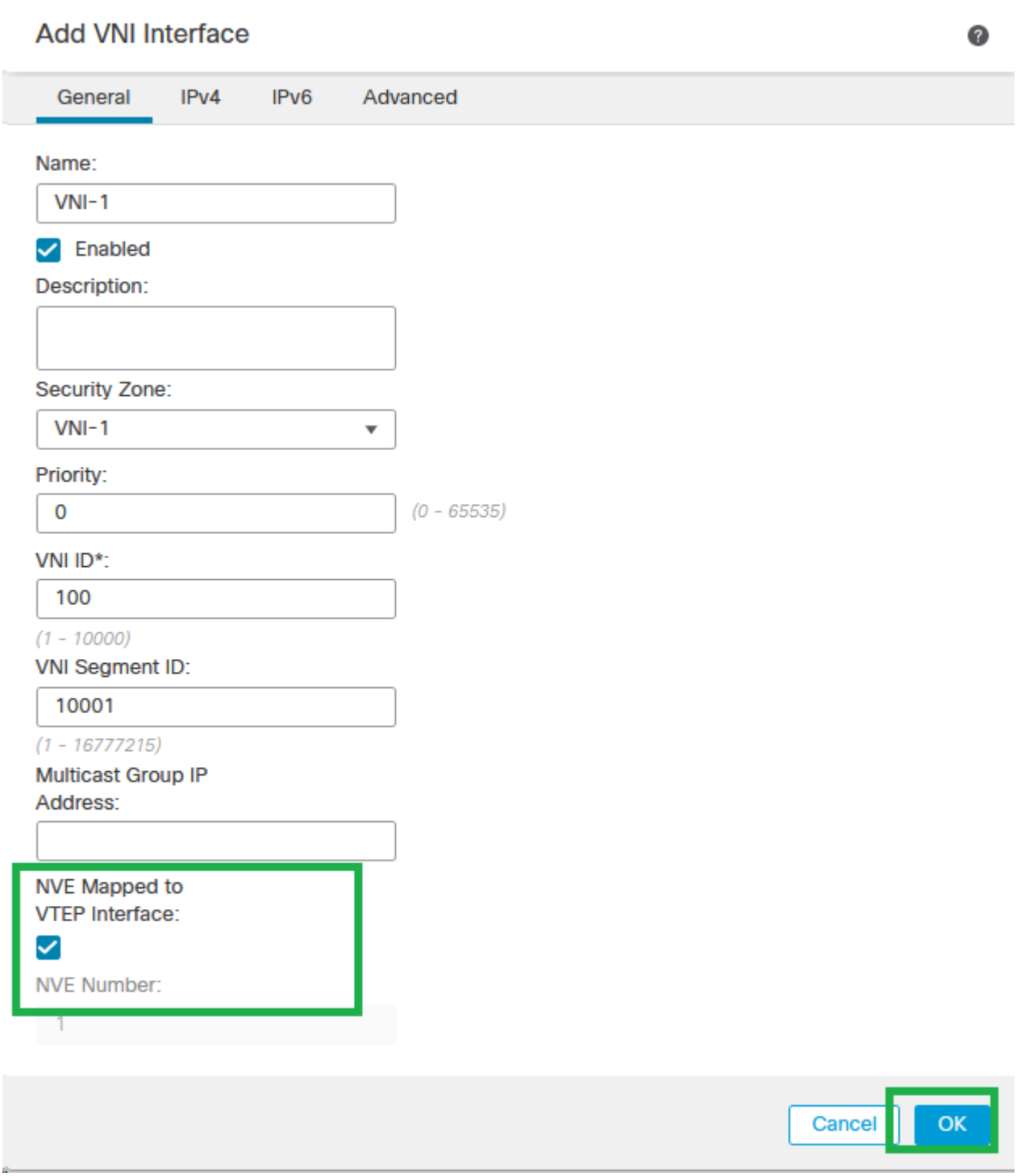
Ajouter une interface VNI

Remarque : L'ID VNI est configuré entre 1 et 10000, et l'ID de segment VNI est configuré entre 1 et 16777215 (l'ID de segment est utilisé pour l'étiquetage VXLAN).

Mise en garde : Si le groupe de multidiffusion n'est pas configuré sur l'interface VNI, le groupe par défaut de la configuration de l'interface source VTEP est utilisé s'il est disponible. Si vous définissez manuellement une adresse IP d'homologue VTEP pour

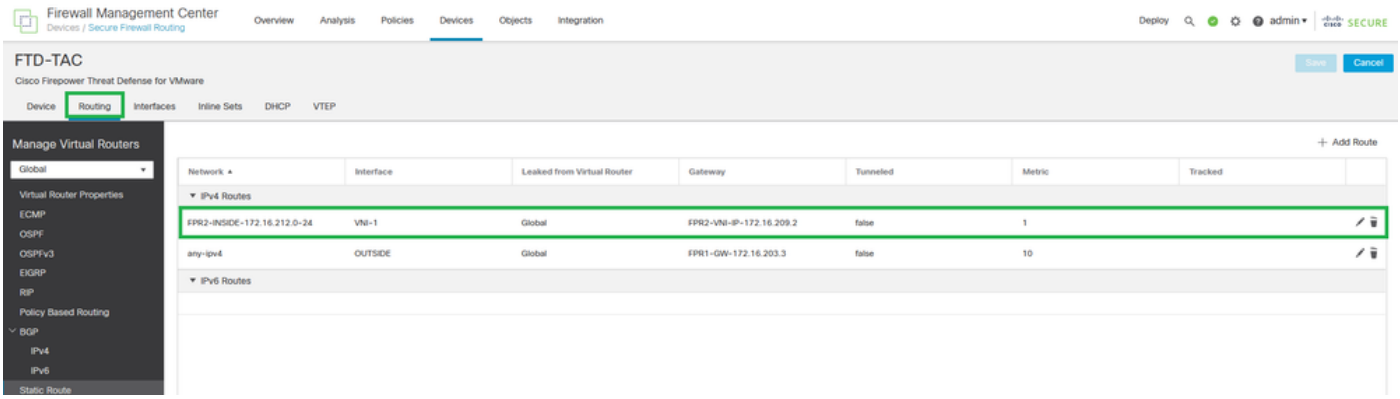
l'interface source VTEP, vous ne pouvez pas spécifier de groupe de multidiffusion pour l'interface VNI.

Étape 3: Cochez la case NVE Mapped to VTEP Interface et cliquez sur OK.



NVE mappé à l'interface VTEP

Étape 4: Configurez une route statique pour annoncer les réseaux de destination pour VXLAN à l'interface homologue VNI. Naviguez Routing > Static Route.



Configuration de route statique

Mise en garde : Les réseaux de destination pour VXLAN doivent être envoyés via l'interface VNI homologue. Toutes les interfaces VNI doivent se trouver sur le même domaine de diffusion (segment logique).

Étape 5: Enregistrez et déployez les modifications.

Avertissement : Des avertissements de validation peuvent être vus avant le déploiement, afin de garantir que les adresses IP des homologues VTEP sont accessibles depuis l'interface source VTEP physique.

Vérifier

Vérifiez la configuration NVE.

```
firepower# show running-config nve
nve 1
encapsulation vxlan
source-interface OUTSIDE
peer-group FPR1-VTEP-Group-Object
```

```
firepower# show nve 1
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
IP address 172.16.203.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
1309 packets input, 128170 bytes
2009 packets output, 230006 bytes
142 packets dropped
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Configured static peer group VTEPs:
```

```
IP address 172.16.205.1 MAC address 0050.56b3.c30a (learned)
IP address 172.16.207.1 MAC address 0050.56b3.c30a (learned)
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 172.16.205.1
IP address 172.16.207.1
Number of VNIs attached to nve 1: 1
VNIs attached:
vni 100: proxy off, segment-id 10001, mcast-group none
NVE proxy single-arm channel is off.
```

```
firepower# show nve 1 summary
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Number of discovered peer VTEPs: 2
Number of VNIs attached to nve 1: 1
NVE proxy single-arm channel is off.
```

Vérifiez la configuration de l'interface VNI.

```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

Vérifiez la configuration MTU sur l'interface VTEP.

```
firepower# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0050.56b3.26b8, MTU 1554
IP address 172.16.203.1, subnet mask 255.255.255.0
---
[Output omitted]
---
```

Vérifiez la configuration de la route statique pour les réseaux de destination.

```
firepower# show run route
```

```
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.203.3 10
route VNI-1 172.16.212.0 255.255.255.0 172.16.209.2 1
route VNI-1 172.16.215.0 255.255.255.0 172.16.209.3 1
```

Remarque : Vérifiez que les interfaces VNI sur tous les homologues sont configurées sur le même domaine de diffusion.

Dépannage

Vérifiez la connectivité avec les homologues VTEP.

Homologue 1 :

```
firepower# ping 172.16.205.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.205.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Homologue 2 :

```
firepower# ping 172.16.207.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.207.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Remarque : Un problème de connectivité d'homologue VTEP peut générer des échecs de déploiement sur Secure FMC. Assurez-vous de conserver la connectivité à toutes vos configurations d'homologues VTEP.

Vérifiez la connectivité avec les homologues VNI.

.

Homologue 1 :

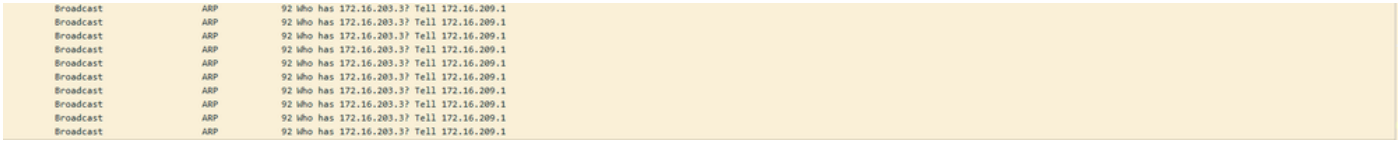
```
firepower# ping 172.16.209.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Homologue 2 :

```
firepower# ping 172.16.209.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Parfois, une route statique incorrecte configurée peut générer des résultats ARP incomplets. Configurez une capture sur l'interface VTEP pour les paquets VXLAN et téléchargez-la au format pcap, n'importe quel outil d'analyse de paquets aide à confirmer s'il y a un problème avec les routes. Assurez-vous d'utiliser l'adresse IP de l'homologue VNI comme passerelle.



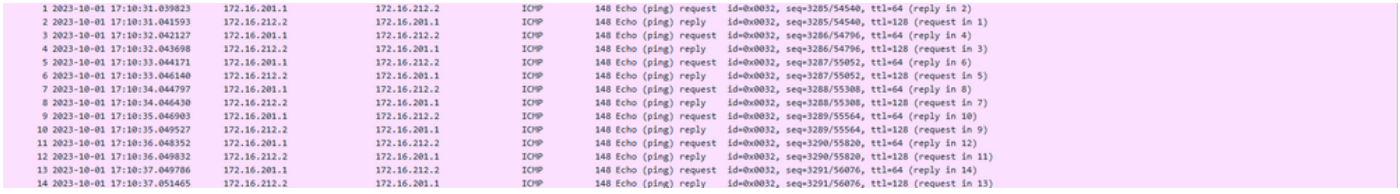
Problème de routage

Configurez les captures d'abandon ASP sur Secure FTD en cas d'abandon de pare-feu, vérifiez le compteur d'abandon ASP avec la commande show asp drop. Contactez le TAC Cisco pour une analyse.

Assurez-vous de configurer les règles de contrôle d'accès pour autoriser le trafic UDP VXLAN sur l'interface VNI/VTEP.

Parfois, les paquets VXLAN peuvent être fragmentés, assurez-vous de changer le MTU en trames jumbo sur le réseau sous-jacent pour éviter la fragmentation.

Configurez la capture sur l'interface Ingress/VTEP et téléchargez les captures au format .pcap pour l'analyse. Les paquets doivent inclure l'en-tête VXLAN sur l'interface VTEP,



Ping capturé avec en-tête VXLAN



En-tête VXLAN

Informations connexes

- Configuration des interfaces VXLAN
- Exemples d'utilisation VXLAN
- Traitement des paquets VXLAN
- Configuration de l'interface source VTEP
- Configuration de l'interface VNI
- Assistance technique de Cisco et téléchargements

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.

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.