Configurer l'objet de stratégie de groupe sur le fabric multisite Nexus avec NDFC 4.2

Table des matières

Introduction

Ce document décrit la configuration et la validation GPO dans les fabrics multisites VXLAN sur les

commutateurs Nexus Cloud Scale exécutant NX-OS et NDFC 4.2.

Conditions préalables

Exigences

Cisco vous recommande de connaître les domaines suivants :

- Technologies VXLAN (Virtual Extensible Local Area Network), EVPN (Ethernet Virtual Private Network) et fabric multisite
- Commutateurs Cisco Nexus Cloud Scale et fonctionnement de NX-OS (NetXus Operating System)
- Workflows de gestion et de déploiement Nexus Fabric Network Controller (NDFC) 4.2
- Segmentation du réseau et concepts de politique de sécurité

Composants utilisés

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

- N9K-C93216TC-FX2
- N9K-C93108TC-EX
- NDFC 4.2

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.

Comprendre la fonctionnalité GPO dans les fabrics EVPN VXLAN

L'option de stratégie de groupe (GPO) est un mécanisme de segmentation basé sur des stratégies conçu pour contrôler la communication entre les points d'extrémité en fonction de l'identité logique au lieu de se fier uniquement aux adresses IP, aux VLAN ou aux sous-réseaux. L'objectif principal de GPO est de simplifier l'application des politiques de sécurité et de fournir une microsegmentation évolutive entre les applications, les serveurs ou les charges de travail.

Une analogie simple consiste à penser à un hôtel où chaque client appartient à une catégorie ou à un niveau d'accès spécifique, où certaines zones sont accessibles uniquement à des clients

spécifiques et où les autorisations d'accès dépendent du rôle du client et non du numéro de la chambre. GPO fonctionne d'une manière très similaire. Au lieu de traiter les terminaux uniquement comme des adresses IP, l'objet de stratégie de groupe les classe dans des groupes de sécurité (SG). Des stratégies sont ensuite appliquées entre ces groupes pour déterminer quelles communications sont autorisées ou refusées.

Exemple :

- Les serveurs Web peuvent appartenir à un groupe de sécurité.
- Les serveurs d'applications peuvent appartenir à un autre groupe de sécurité.
- Les serveurs de base de données peuvent appartenir à un groupe de sécurité restreint.

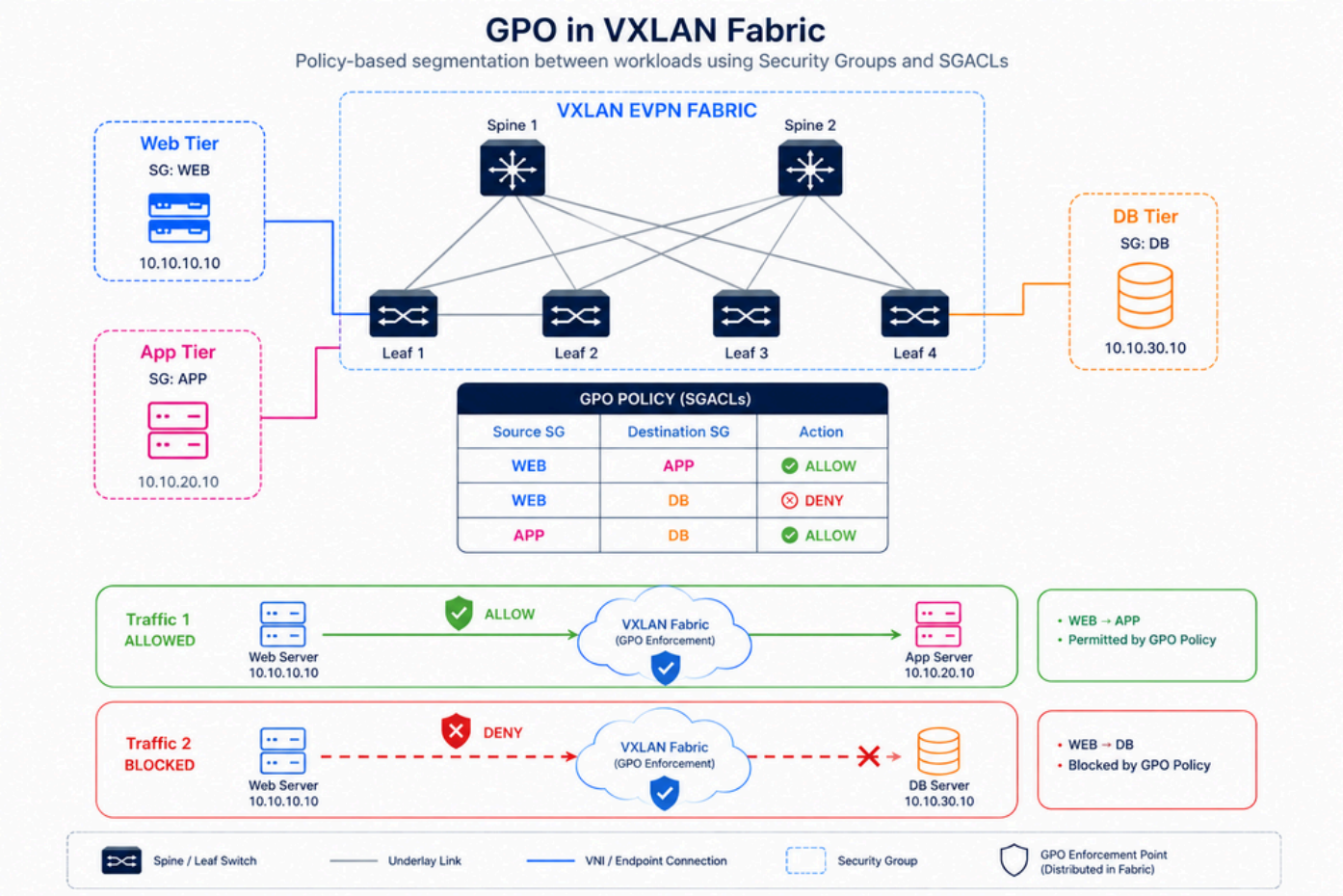
Les politiques peuvent alors définir :

- Les serveurs Web peuvent communiquer avec les serveurs d'applications.
- Les serveurs d'applications peuvent communiquer avec les serveurs de base de données.
- Les serveurs Web ne peuvent pas communiquer directement avec les serveurs de base de données.

Cette approche simplifie les opérations, car les administrateurs n'ont plus besoin de gérer un grand nombre de listes de contrôle d'accès sur plusieurs périphériques et VLAN.

Un autre avantage majeur est l'évolutivité. Dans les environnements de grande taille, les charges de travail se déplacent, évoluent de manière dynamique ou changent fréquemment d'adresses IP. L'objet de stratégie de groupe permet aux stratégies de sécurité de rester cohérentes même lorsque l'emplacement du terminal change. Au sein des fabrics EVPN VXLAN, l'objet de stratégie de groupe étend ce concept en distribuant les informations du groupe de sécurité à travers le fabric et en appliquant des listes de contrôle d'accès du groupe de sécurité (SGACL) entre les terminaux. Cela devient particulièrement important dans les data centers modernes, car le trafic est-ouest entre les charges de travail représente souvent la plus grande surface d'attaque. GPO améliore la sécurité en limitant les chemins de communication inutiles à l'intérieur du fabric du data center.

Pour une compréhension technique plus approfondie de l'architecture GPO, des concepts de microsegmentation et de l'application des politiques VXLAN, reportez-vous au livre blanc Cisco disponible à l'adresse : Sécurisation des data centers avec microsegmentation à l'aide de VXLAN GPO



GPO dans le fabric VxLAN

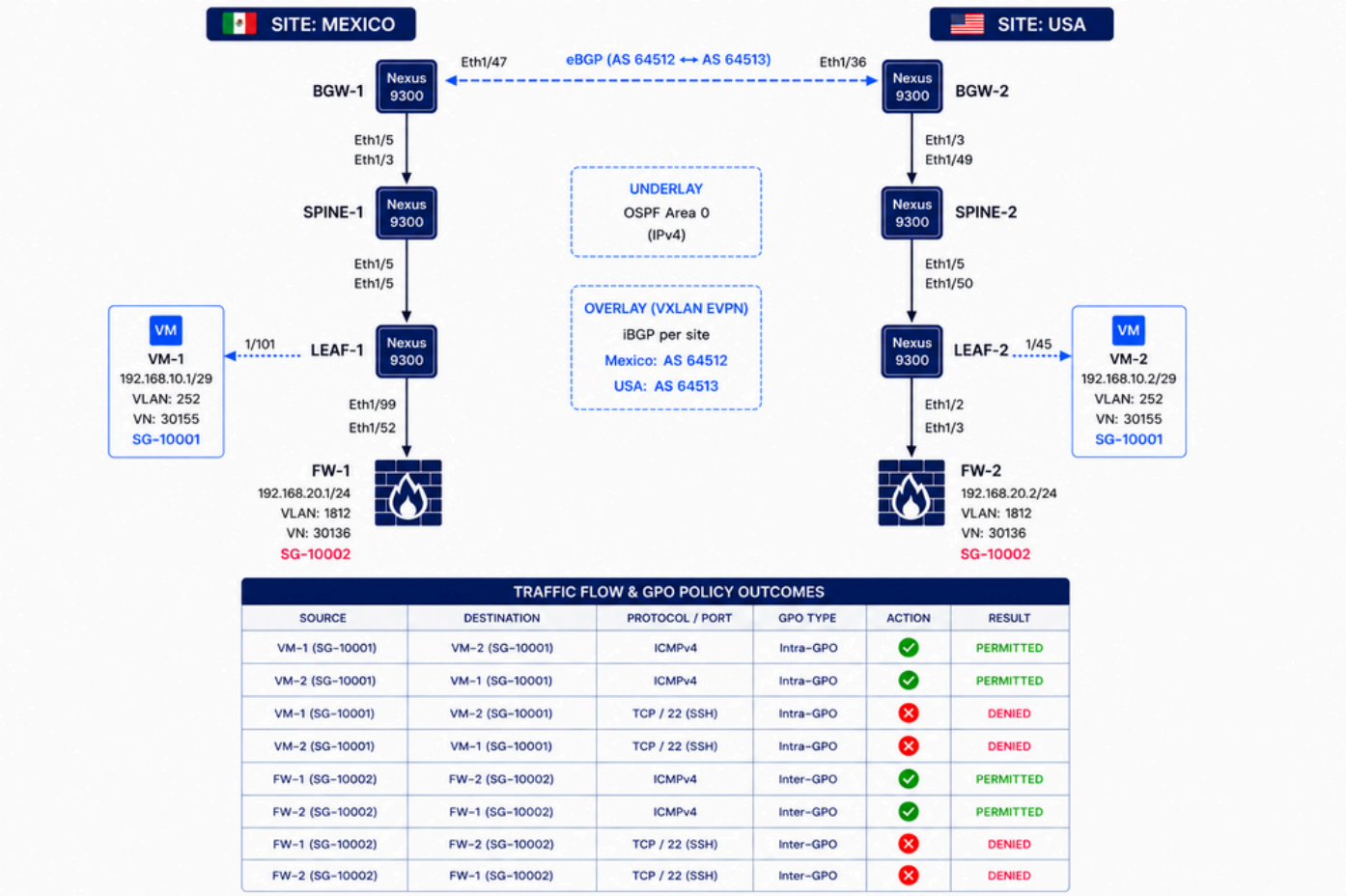
Scénario de déploiement d'un objet de stratégie de groupe multisite VXLAN utilisant NDFC 4.2 et NX-OS 10.6(3)F

Cette topologie représente un fabric multisite VXLAN déployé sur deux sites géographiquement dispersés : Mexique et États-Unis. Chaque site contient des BGW dédiés, des commutateurs Spine, des commutateurs Leaf, des machines virtuelles et des segments de pare-feu exécutés sur les commutateurs Cisco Nexus 9300 avec NX-OS 10.6(3)F. Le réseau sous-jacent utilise le protocole OSPF (Open Shortest Path First), tandis que le plan de contrôle de superposition utilise iBGP au sein de chaque site et eBGP entre BGW-1 et BGW-2 pour la communication EVPN VXLAN inter-site. Étant donné que cet environnement est un déploiement en laboratoire, les sites du Mexique et des États-Unis sont interconnectés via une liaison connectée directement entre les deux BGW afin de simplifier le modèle de connectivité multisite.

L'objet de stratégie de groupe est utilisé pour appliquer une microsegmentation basée sur des stratégies entre les groupes de sécurité (SG) indépendamment de l'adressage IP ou des limites

VLAN. Selon la table des politiques de connectivité, le trafic ICMP de VM-1 vers VM-2, FW-1 et FW-2 est autorisé, tandis que le trafic du port TCP 22 (SSH) de VM-1 vers FW-1 et FW-2 est refusé. La communication du port TCP 22 entre VM-1 et VM-2 reste autorisée car les deux terminaux appartiennent au même groupe de sécurité (SG-10001). Ce comportement montre comment GPO applique de manière dynamique différentes stratégies de trafic entre les communications intra-GPO et inter-GPO à travers le fabric multisite VXLAN.

Remarque : La version 10.6(3)F de Cisco NX-OS introduit la possibilité de restreindre la communication entre les terminaux d'un même ESG (également appelé SG) à l'aide de la fonction d'isolation intra-ESG. Cette fonctionnalité réduit le risque d'accès non autorisé au sein d'ESG et améliore la position de sécurité.



Configuration pas à pas de l'objet de stratégie de groupe avec NDFC 4.2 dans les fabrics EVPN VXLAN

Ces étapes s'appliquent lorsque le fabric multisite VXLAN est déjà opérationnel et configuré avec NDFC 4.2, et que l'objet de stratégie de groupe doit être implémenté ultérieurement. La section

Automation Using Nexus Dashboard in Securing Data Centers with Microsegmentation Using VXLAN GPO montre la configuration à partir de la création d'un fabric VXLAN à site unique.

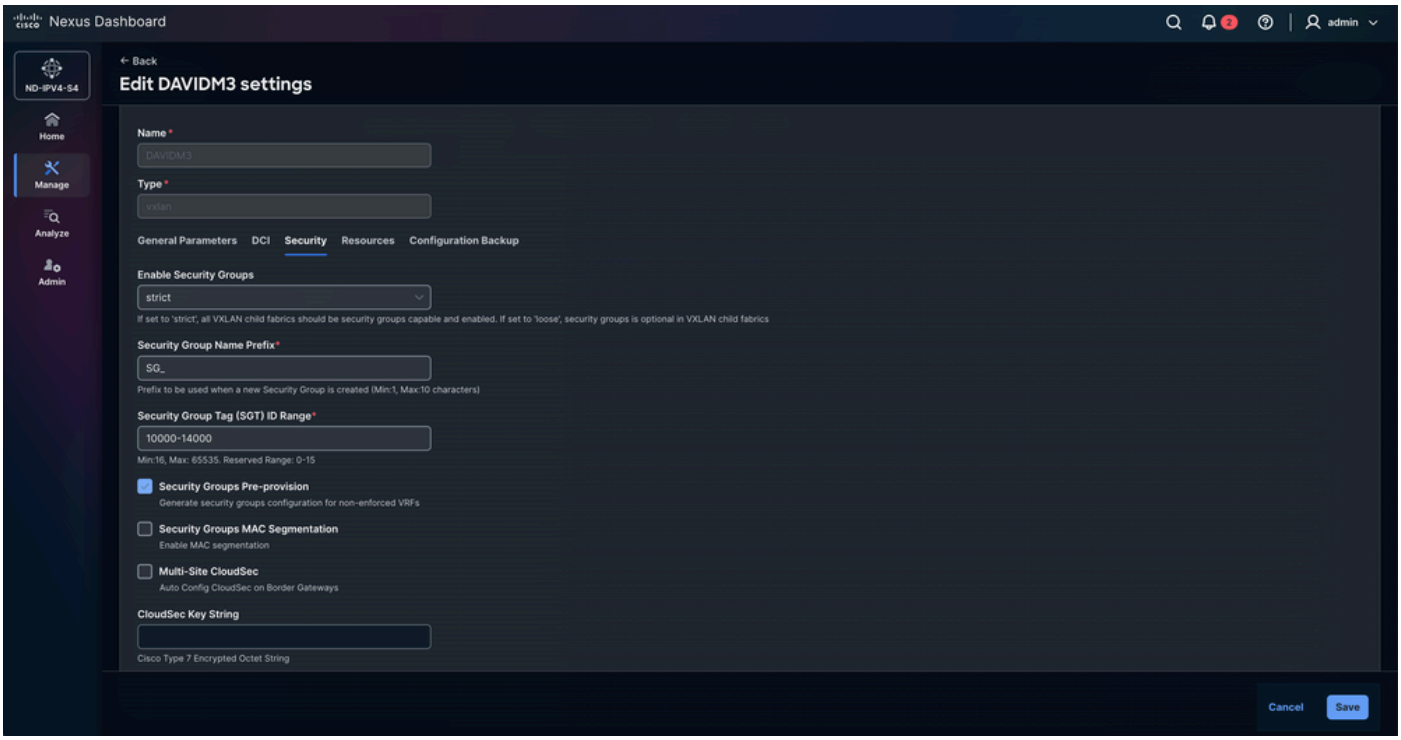
⚠ Mise en garde : Lorsque l'objet de stratégie de groupe fonctionne dans un fabric EVPN VXLAN, la communication n'a lieu que si l'accessibilité de la destination existe et que la stratégie de sécurité autorise le trafic. L'application des politiques repose sur les informations IP, qui nécessitent des entrées ARP et des interfaces SVI pour les réseaux internes. Cela signifie que le VLAN qui appartient au VRF du locataire doit avoir une SVI configurée. Par conséquent, l'application ne s'applique pas au trafic qui contient uniquement des en-têtes de couche 2 et ne peut donc pas être utilisé avec l'extension de couche 2 VXLAN. NX-OS version 10.6(2)F introduit la prise en charge de la microsegmentation basée sur MAC.

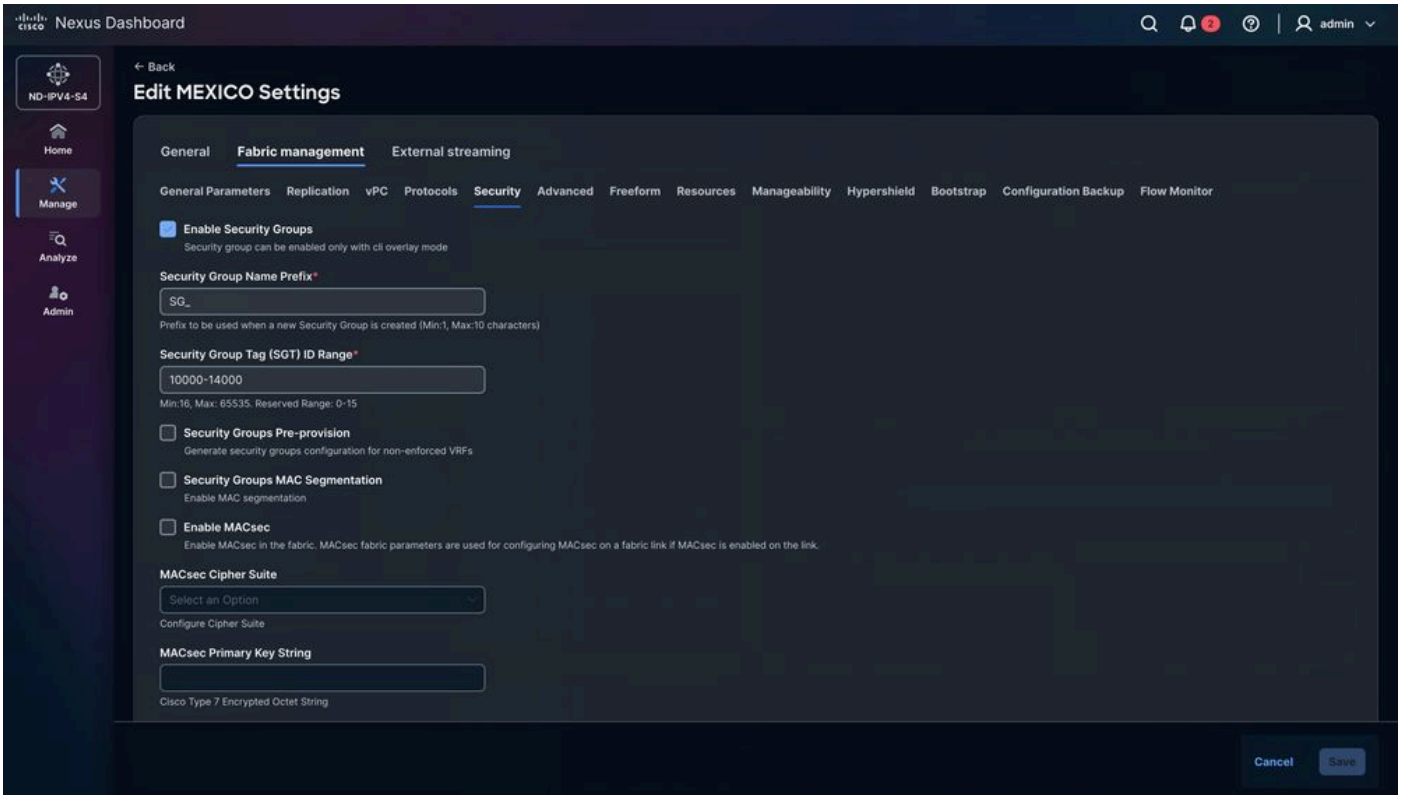
Étape 1 : activation des groupes de sécurité dans le fabric parent

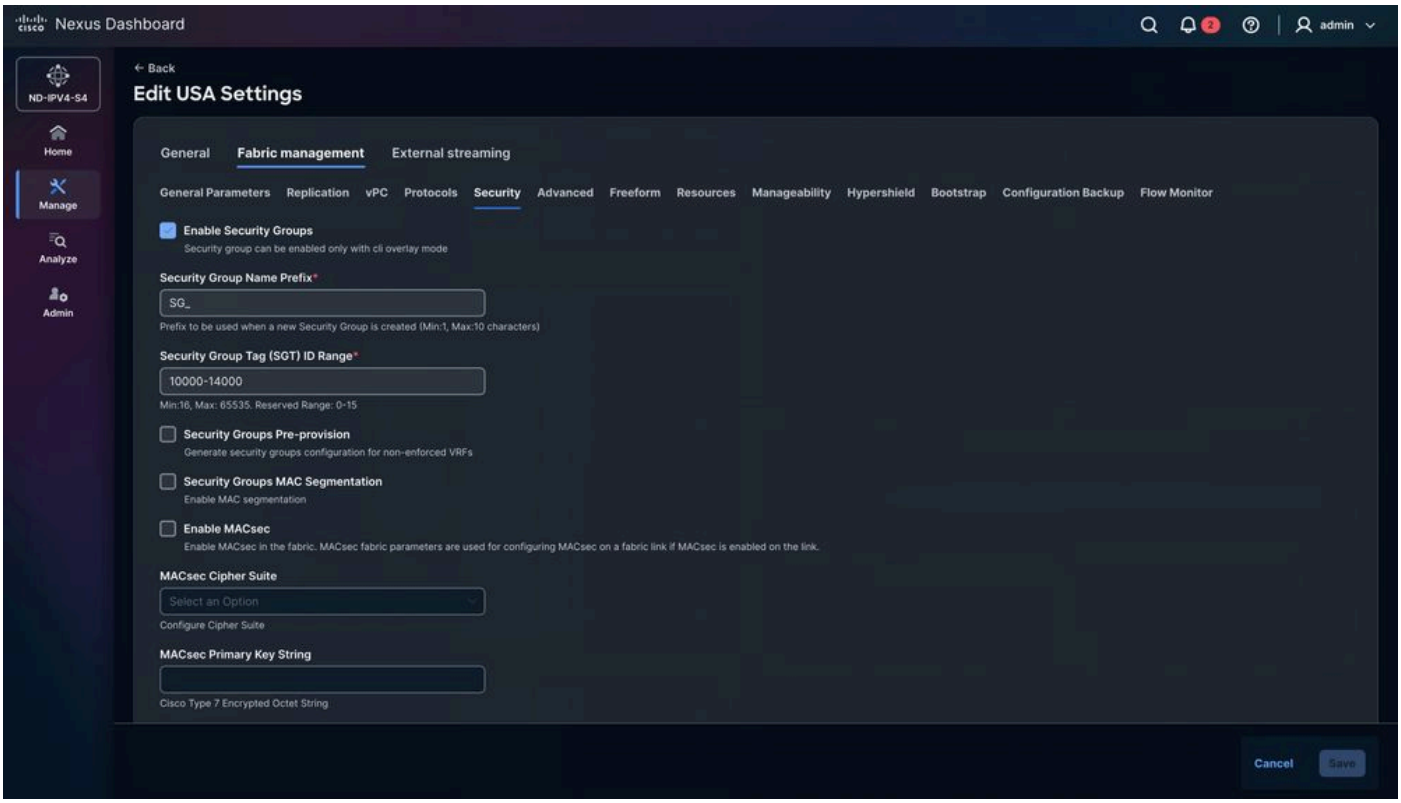
- Accédez à Manage > Fabric Groups, sélectionnez le groupe de fabrics DAVIDM3, puis choisissez Actions > Edit Fabric Group Settings. Dans la section Security, activez Security Groups, définissez le mode sur Strict et définissez Security Groups Pre-provision.
  - Sélectionnez le groupe de fabrics qui vous intéresse. Dans cet exemple, le groupe de fabrics sélectionné est appelé DAVIDM3, qui est également le nom du fabric multisite.
- Répétez ces étapes pour chaque fabric enfant.
  - Accédez à Manage > Fabric, sélectionnez USA, puis accédez à Actions > Edit Fabric Group Settings. Dans la section Sécurité, activez Groupes de sécurité et définissez le mode sur Strict.
  - Naviguez jusqu'à Manage > Fabric, sélectionnez MEXICO, puis accédez à Actions > Edit Fabric Group Settings. Dans la section Sécurité, activez Groupes de sécurité et définissez le mode sur Strict.

✎ Remarque : Si cette option est définie sur strict, tous les fabrics enfants VXLAN doivent être compatibles et activés avec les groupes de sécurité. S'ils sont définis sur lâche, les groupes de sécurité sont facultatifs dans les fabrics enfants VXLAN.

🔍 Conseil : Pour conserver une visibilité claire, utilisez les mêmes plages d'ID de balise de groupe de sécurité (SGT) dans le fabric parent et dans tous les fabrics enfants. La plage de fabrics parent doit couvrir les plages utilisées par tous les fabrics enfants.


Nexus Dashboard
admin
ND-IPV4-S4
Home
Manage
Analyze
Admin
← Back
Edit DAVIDM3 settings
Name *
DAVIDM3
Type *
vxlan
General Parameters
DCI
Security
Resources
Configuration Backup
Enable Security Groups
strict
If set to 'strict', all VXLAN child fabrics should be security groups capable and enabled. If set to 'loose', security groups is optional in VXLAN child fabrics
Security Group Name Prefix*
SG_
Prefix to be used when a new Security Group is created (Min:1, Max:10 characters)
Security Group Tag (SGT) ID Range*
10000-14000
Min:16, Max: 65535. Reserved Range: 0-15
Security Groups Pre-provision
Generate security groups configuration for non-enforced VRFs
Security Groups MAC Segmentation
Enable MAC segmentation
Multi-Site CloudSec
Auto Config CloudSec on Border Gateways
CloudSec Key String
Cisco Type 7 Encrypted Octet String
Cancel
Save


Nexus Dashboard
admin
ND-IPV4-S4
Home
Manage
Analyze
Admin
← Back
Edit MEXICO Settings
General
Fabric management
External streaming
General Parameters
Replication
vPC
Protocols
Security
Advanced
Freeform
Resources
Manageability
Hypershield
Bootstrap
Configuration Backup
Flow Monitor
Enable Security Groups
Security group can be enabled only with cli overlay mode
Security Group Name Prefix*
SG_
Prefix to be used when a new Security Group is created (Min:1, Max:10 characters)
Security Group Tag (SGT) ID Range*
10000-14000
Min:16, Max: 65535. Reserved Range: 0-15
Security Groups Pre-provision
Generate security groups configuration for non-enforced VRFs
Security Groups MAC Segmentation
Enable MAC segmentation
Enable MACsec
Enable MACsec in the fabric. MACsec fabric parameters are used for configuring MACsec on a fabric link if MACsec is enabled on the link.
MACsec Cipher Suite
Select an Option
Configure Cipher Suite
MACsec Primary Key String
Cisco Type 7 Encrypted Octet String
Cancel
Save



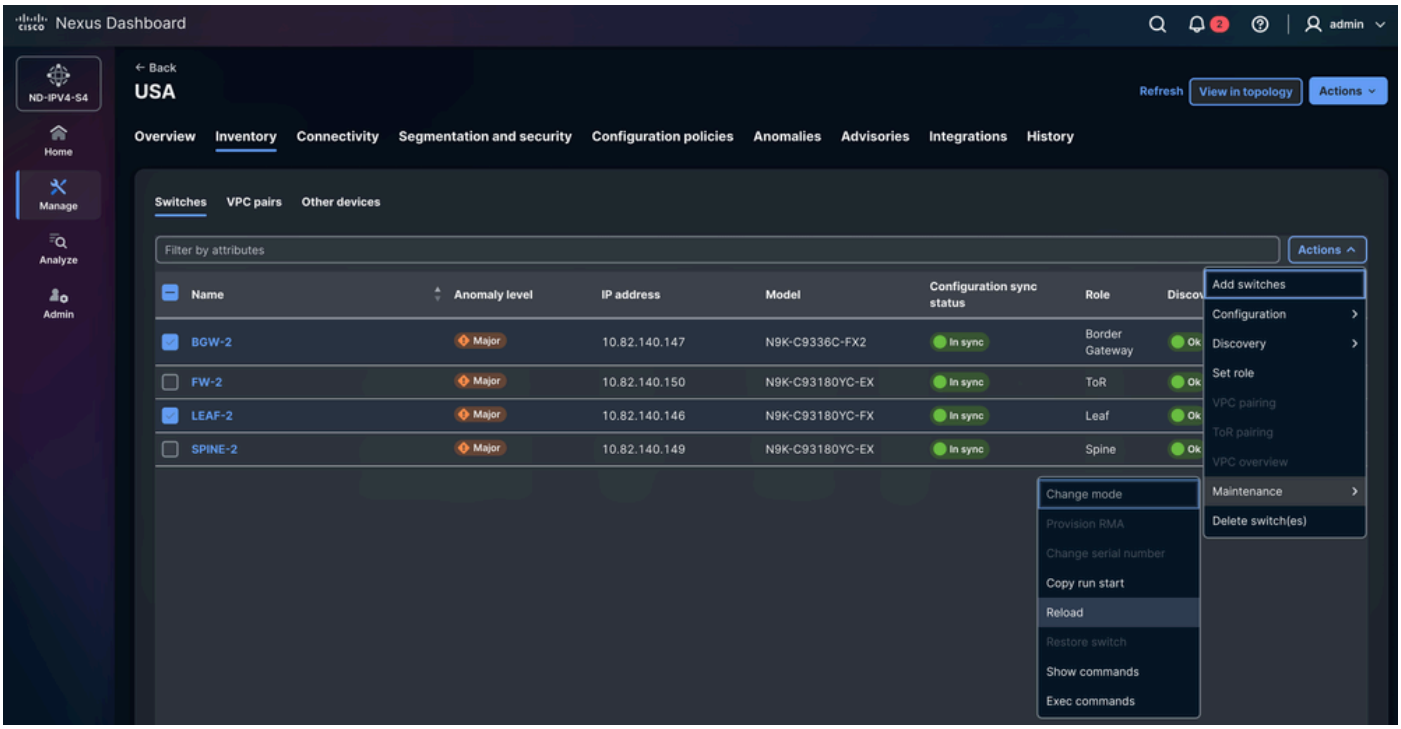
Étape 2. Recalculer la configuration du fabric et recharger les commutateurs pour le déploiement GPO

NDFC vous invite automatiquement à recharger un groupe spécifique de commutateurs Nexus en fonction de leur rôle. Dans cet exemple, LEAF-1, LEAF-2, BGW-1 et BGW-2 doivent être rechargés. Cette action doit être exécutée manuellement par l'administrateur réseau. Le rechargement est requis et ne peut pas être ignoré, car GPO requiert la découpe TCAM.

Remarque : Si le périphérique n'est pas rechargé, la modification TCAM peut apparaître dans la configuration en cours ; toutefois, comme le commutateur n'a pas été redémarré, le paramètre n'est pas appliqué à la mémoire matérielle. Par conséquent, la fonctionnalité ne peut pas fonctionner comme prévu.

Pour recharger les commutateurs Nexus :

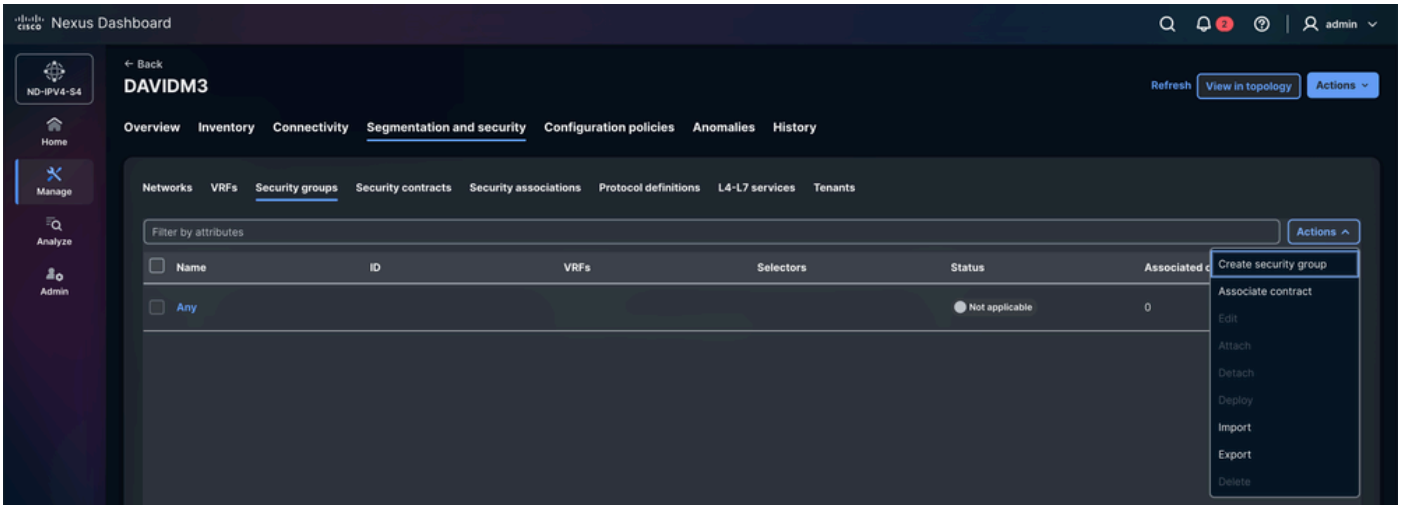
Accédez à Manage > Fabrics > MEXICO/USA > Inventory > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions > Maintenance > Reload.



Étape 3. Créer un groupe de sécurité

Définissez les groupes de sécurité pour chaque terminal. Chaque point d'extrémité des fabrics VXLAN peut avoir un seul groupe de sécurité. Cette approche n'est pas efficace. Regroupez les terminaux dans le monde entier (machines virtuelles, pare-feu, optimiseurs TCP, etc.).

Naviguez jusqu'à Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security Groups > Actions > Create security group.



Étape 3.1 Configuration du nom du groupe de sécurité

- NDFC attribue automatiquement un nom aléatoire. Le nom peut être modifié ; il est recommandé d'utiliser un nom représentatif facile à identifier pour les terminaux.
- Dans ce scénario :
    - VM -> SG_VM
    - Pare-feu -> SG_FW

Étape 3.2 Configuration de VRF

- Sélectionnez le service partagé (VRF) auquel les points d'extrémité appartiennent.
- Dans ce scénario : Les machines virtuelles et les pare-feu appartiennent au client CISCO-TAC.

Facultatif, Créer un VRF.

Par défaut, le mode d'application des stratégies d'un VRF locataire nouvellement créé est défini sur Non appliqué. Dans cet état, même si les critères de classification et les SGACL entre les groupes de sécurité sont configurés, aucune application de stratégie n'a lieu. Pour activer l'application de la liste SGACL, le VRF doit être explicitement configuré en mode forcé.

Lorsque le VRF fonctionne en mode forcé, un comportement de stratégie par défaut est défini :

- Refuser : Tout le trafic de monodiffusion est abandonné sauf si une règle d’autorisation l’autorise explicitement.
- Autoriser : Tout le trafic de monodiffusion est autorisé sauf s'il est explicitement bloqué par une règle de refus.

Les terminaux appartenant au même groupe de sécurité peuvent communiquer entre eux sans avoir besoin de règles SGACL. Les listes SGACL définissent des stratégies de sécurité uniquement entre différents groupes de sécurité.

La version 10.6(3)F de Cisco NX-OS introduit la possibilité de restreindre la communication entre les terminaux d'un même objet de stratégie de groupe, également appelée fonction d'isolation intra-objet de stratégie de groupe. Avant cette version, les règles appliquées aux points d'extrémité au sein du même groupe de sécurité étaient ignorées et le trafic était autorisé par défaut.

Étape 3.3 Configuration de l’ID de balise du groupe de sécurité

NDFC attribue automatiquement un ID de balise aléatoire à partir de la plage prédéfinie dans la configuration du fabric. Bien qu'un ID de balise puisse être sélectionné manuellement, il doit être

compris dans la plage définie pour les fabrics enfant et parent.

Dans ce scénario :

- VM-1 et VM-2 : 10001
- FW-1 et FW-2 : 10002

Étape 3.4 Fixation

Si l'option Attacher n'est pas activée, le groupe de sécurité n'est pas appliqué au client CISCO-TAC.

Étape 3.5 Configuration des sélecteurs

- Les sélecteurs déterminent quels terminaux et adresses IP externes sont associés à un groupe de sécurité spécifique.

NDFC 4.2 prend en charge trois types de sélecteurs natifs :

1) Sélecteurs IP : les sélecteurs IP associent des terminaux ou des sous-réseaux IP à un groupe de sécurité en fonction des informations IP.

a. Point de terminaison connecté : identifie les points de terminaison directement connectés au fabric, tels que les machines virtuelles, les serveurs ou les hôtes physiques connectés aux commutateurs Leaf.
b. Sous-réseau externe : associe des préfixes IP externes à un groupe de sécurité. Ce type est utilisé pour les réseaux qui existent en dehors du fabric VXLAN, tels que les data centers externes, les segments WAN ou les réseaux connectés à Internet. Le trafic provenant de ou destiné à ces préfixes est classifié avec le groupe de sécurité configuré.

2) Sélecteurs réseau : les sélecteurs réseau associent un groupe de sécurité à un segment de réseau VXLAN spécifique. La classification est appliquée en fonction de l'identificateur de réseau (L2VNI). Tous les terminaux appartenant à ce réseau héritent du groupe de sécurité attribué, ce qui simplifie le déploiement des stratégies lorsque plusieurs terminaux partagent le même segment.

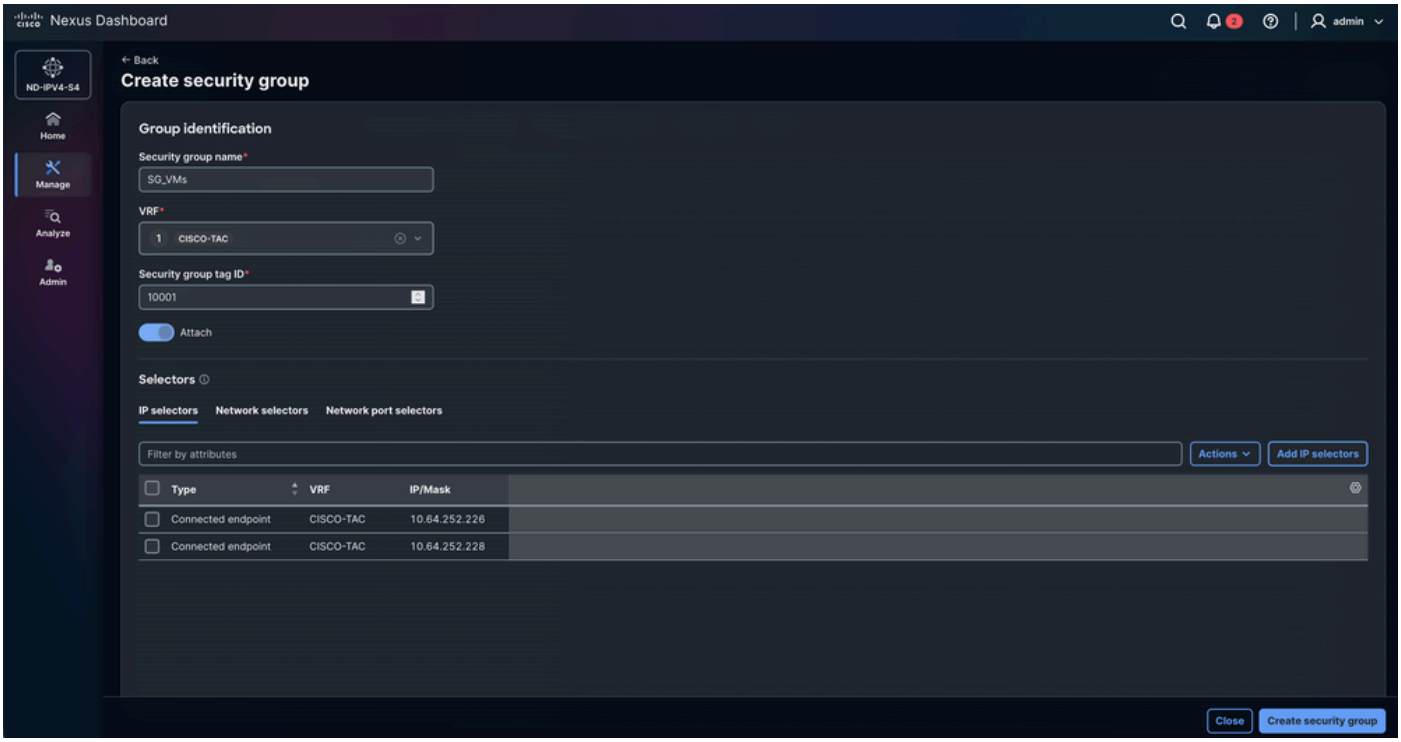
3) Sélecteurs de ports réseau : les sélecteurs de ports réseau classent le trafic en fonction de l'interface physique du commutateur par laquelle le trafic entre dans le fabric. Un groupe de sécurité peut être attribué au trafic reçu sur un port ou une interface spécifique. Cette approche est généralement utilisée pour les périphériques connectés via des réseaux externes, des

appliances de service ou des liaisons d'infrastructure où la classification IP des terminaux n'est pas possible.

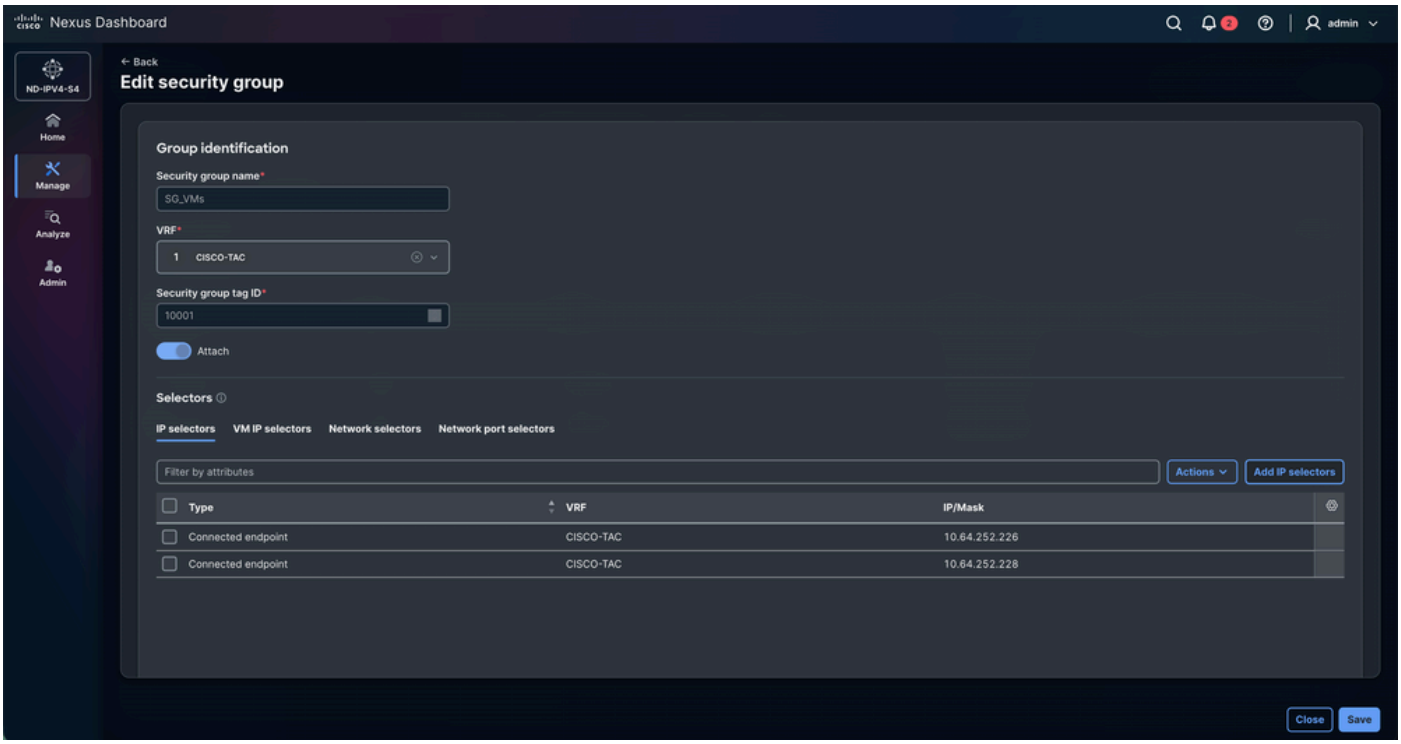
Résumé de la configuration du groupe de sécurité

Périphérique	Nom du groupe de sécurité	VRF	ID balise du groupe de sécurité	Sélecteurs
VM-1	SG_VM	CISCO-TAC	10001	Sélecteurs IP
VM-2	SG_VM	CISCO-TAC	10001	Sélecteurs IP
FW-1	SG_FW	CISCO-TAC	10002	Sélecteurs IP
FW-2	SG_FW	CISCO-TAC	10002	Sélecteurs IP

Configuration du groupe de sécurité pour les VM



Configuration du groupe de sécurité pour les pare-feu



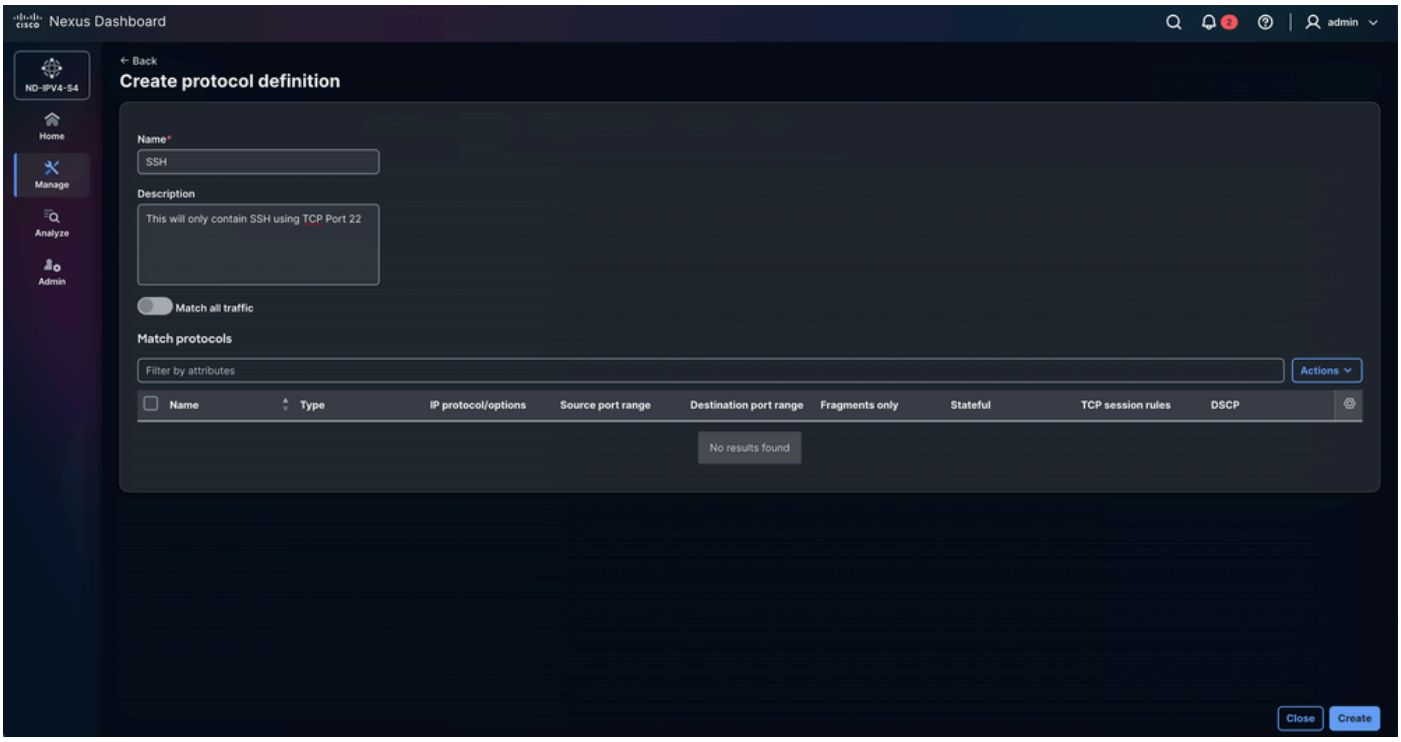
Étape 4 : configuration des définitions de protocole

L'option Créer une définition de protocole permet de définir les paramètres de protocole réseau et les caractéristiques de trafic correspondant à un objet de stratégie de groupe (GPO). Il permet aux administrateurs de spécifier des critères tels que le type de protocole, les numéros de port et d'autres attributs de paquets afin que la stratégie correspondante puisse être appliquée aux flux de trafic souhaités.

Dans ce scénario, l'objectif est d'autoriser uniquement le trafic ICMP tout en bloquant explicitement le trafic TCP sur le port 22 (SSH). Cette politique garantit que les tests d'accessibilité du réseau restent autorisés, tandis que l'accès SSH non autorisé ou indésirable est restreint manuellement.

Naviguez jusqu'à Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Protocol definitions > Actions > Create protocol definition.

Saisissez le nom et la description.



Accédez à Actions > Créer une entrée de protocole.

- Name : SSH
- Type : IPv4
    - IP et IPv6 sont également disponibles.
- Protocole/options IP : TCP
    - UDP, EIGRP et PIM, entre autres, sont pris en charge.

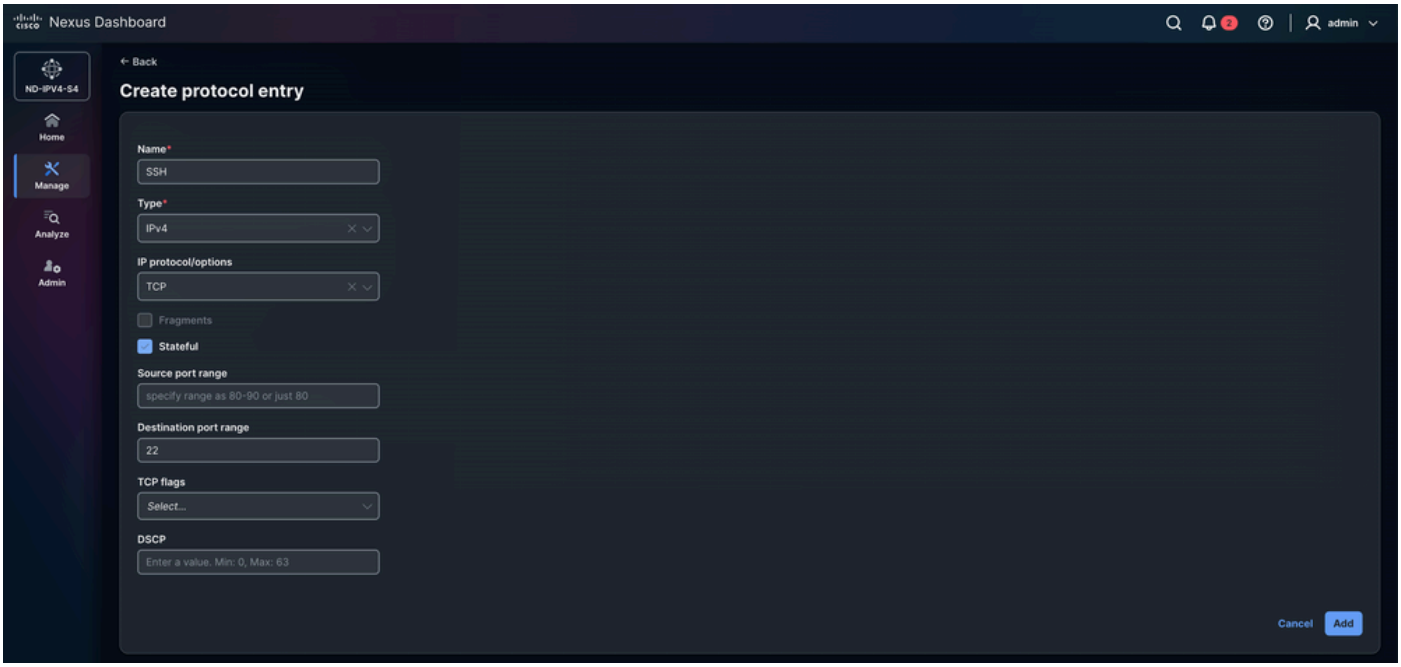
- Fragments : Permet à la règle de correspondre aux paquets IP fragmentés. Cela est utile car les paquets volumineux peuvent être fractionnés en fragments lorsqu'ils dépassent la MTU du réseau. L'activation de cette option garantit que la stratégie s'applique également à ces fragments.

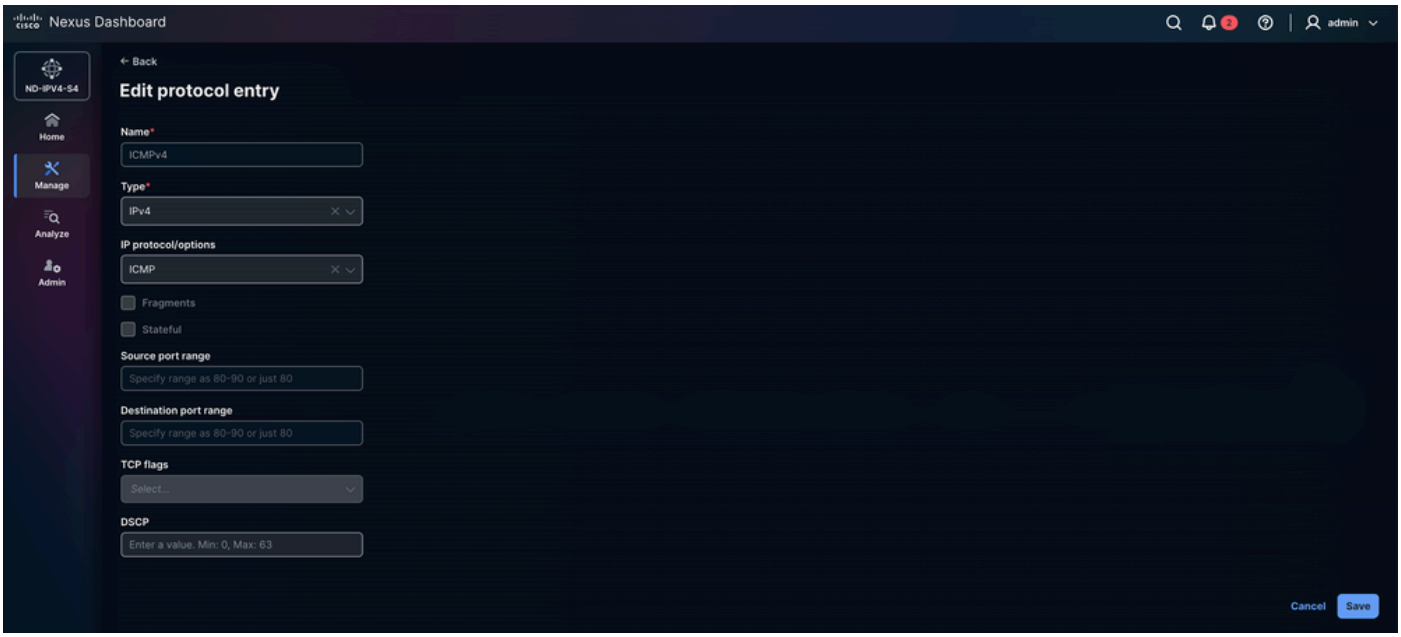
- Avec état : Un processus avec état signifie qu'il conserve une trace de toutes les modifications ou interactions qui se sont produites dans le passé, et qu'un processus en cours est exécuté avec un contexte de ces processus précédents. Dans ce cas, le protocole TCP conserve une trace des zones telles que le nombre de paquets à transférer, l'ordre des paquets et si le récepteur a reçu un paquet ou non. Lorsque l'option Stateful est sélectionnée, ces informations sont stockées en tant qu'état dans TCP.

- Plage de ports source : Cette option n'est disponible que si vous avez sélectionné TCP ou UDP dans le champ IP Protocol/Options ci-dessus.
- Plage de ports de destination : cette option n'est disponible que si vous avez sélectionné TCP ou UDP dans le champ IP Protocol/Options.
- Indicateurs TCP

    - Cette option n'est disponible que lorsque TCP est sélectionné dans le champ IP Protocol/Options.

- Il vous permet de définir les indicateurs TCP utilisés par le protocole de sécurité.
- Les indicateurs TCP font partie de l'en-tête TCP et sont utilisés pour contrôler l'établissement, la maintenance et la fermeture des connexions.
- Options disponibles :
    - ACK (accusé de réception) : Indique un accusé de réception des données reçues ou des paquets de synchronisation.
    - EST (établi) : Désigne les connexions TCP déjà établies. Lorsque cette option est activée, aucun autre indicateur TCP ne peut être sélectionné.
    - FIN (fin) : Utilisé pour fermer une connexion TCP de manière élégante.
    - RST (Reset) : Interrompt immédiatement la connexion et supprime toutes les données encore en transit.
    - SYN (Synchronisation) : Utilisé lors du lancement et de l'établissement d'une connexion TCP.





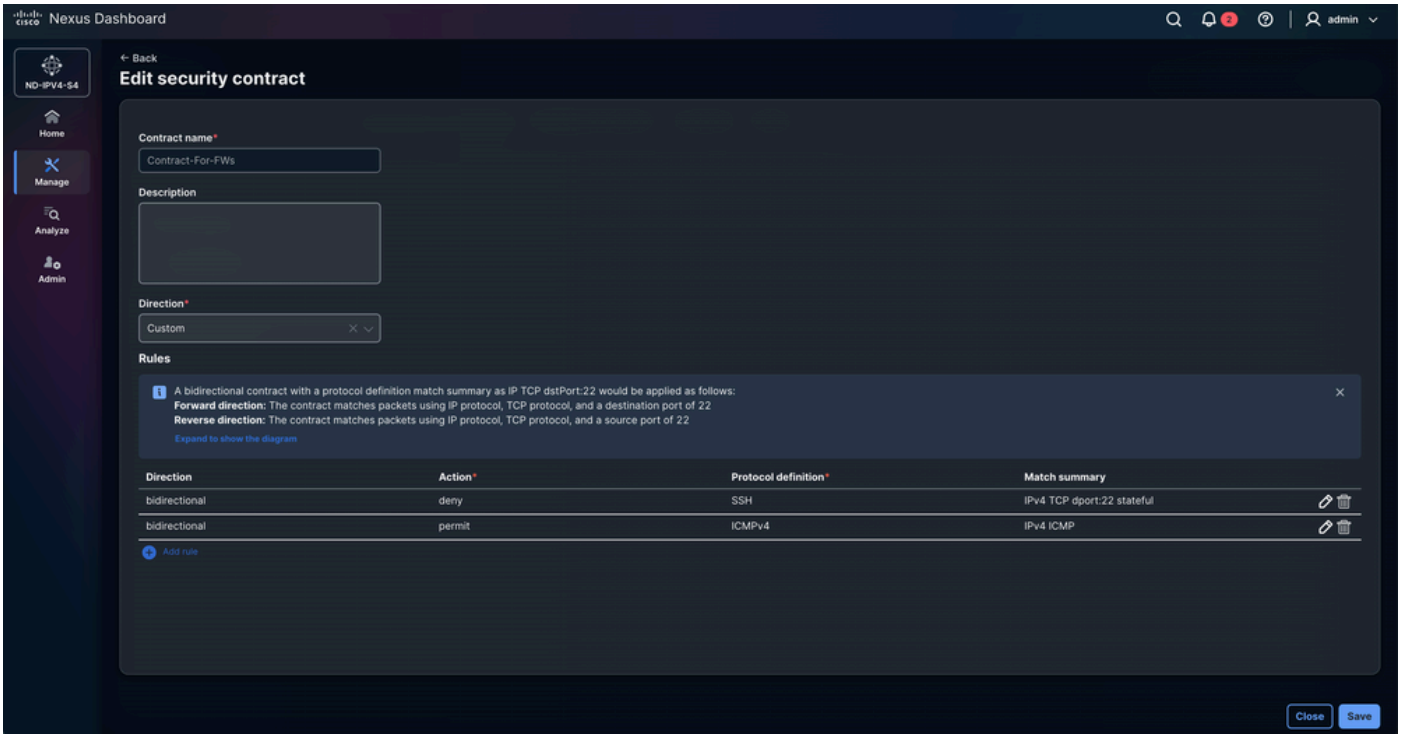
Étape 5. Configuration des contrats de sécurité

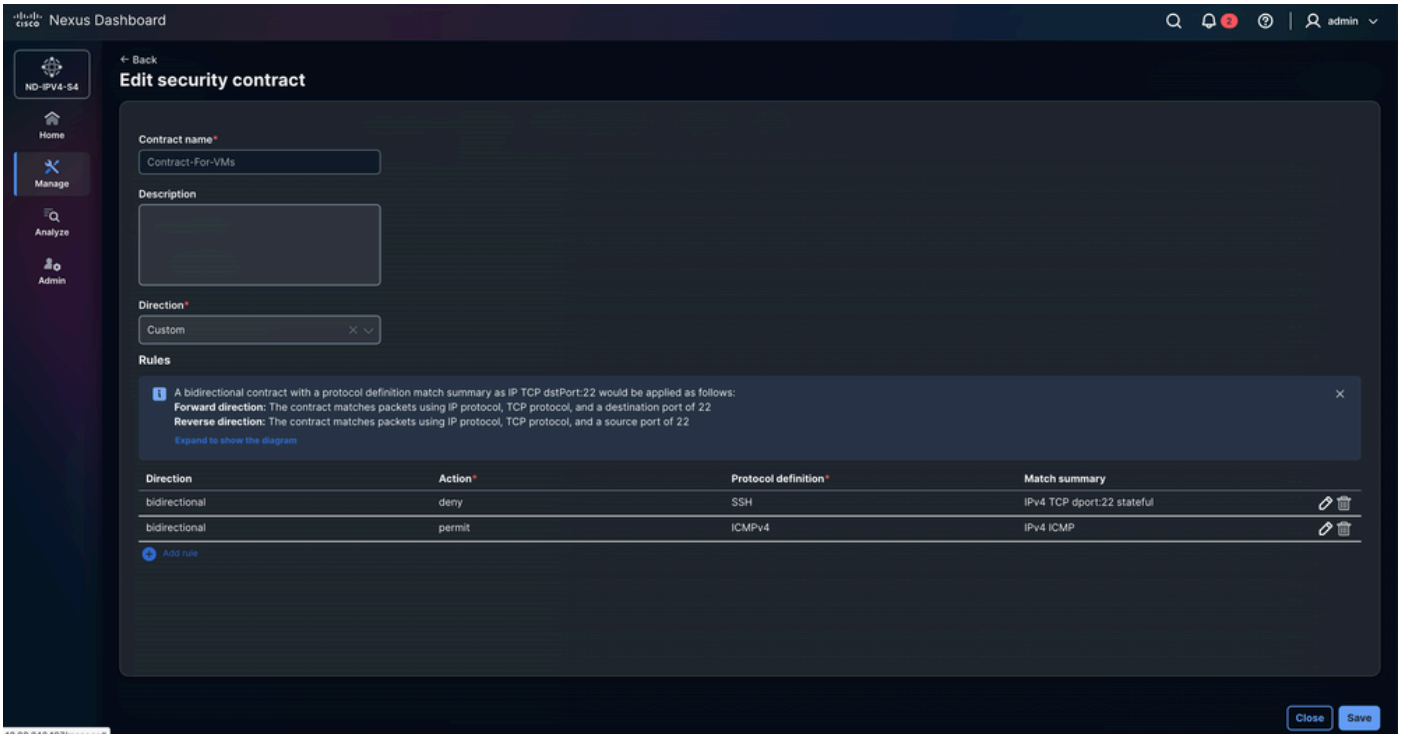
Le contrat définit les règles de communication entre les groupes de terminaux en spécifiant le trafic autorisé ou refusé en fonction des définitions de stratégie associées. Il agit en tant que mécanisme d'application qui applique les règles, les filtres et les actions de protocole configurés, garantissant que le trafic entre les groupes source et de destination est conforme aux politiques de sécurité et de segmentation prévues.

Naviguez jusqu'à Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security Contracts > Actions > Create security contract.

- Sélectionnez Add rule et configurez Direction, Action et Protocol definition.
    - Bidirectionnel :
        - Le contrat bidirectionnel s'applique comme suit avec un résumé de correspondance de définition de protocole comme IP TCP Port 22.
            - Direction avant : Le contrat établit une correspondance entre les paquets utilisant le protocole IP, le protocole TCP et un port de destination de 22
            - Direction inverse : Le contrat établit une correspondance entre les paquets utilisant le protocole IP, le protocole TCP et un port source de 22.
            - Cela s'applique quelle que soit la source ou la destination.
    - Unidirectionnel :
        - Unidirectionnelle dans un contrat de sécurité d'objet de stratégie de groupe

signifie que la stratégie est appliquée dans une seule direction du flux de trafic, autorisant ou refusant la communication du groupe de sécurité source au groupe de sécurité de destination sans appliquer automatiquement la même règle dans la direction inverse.

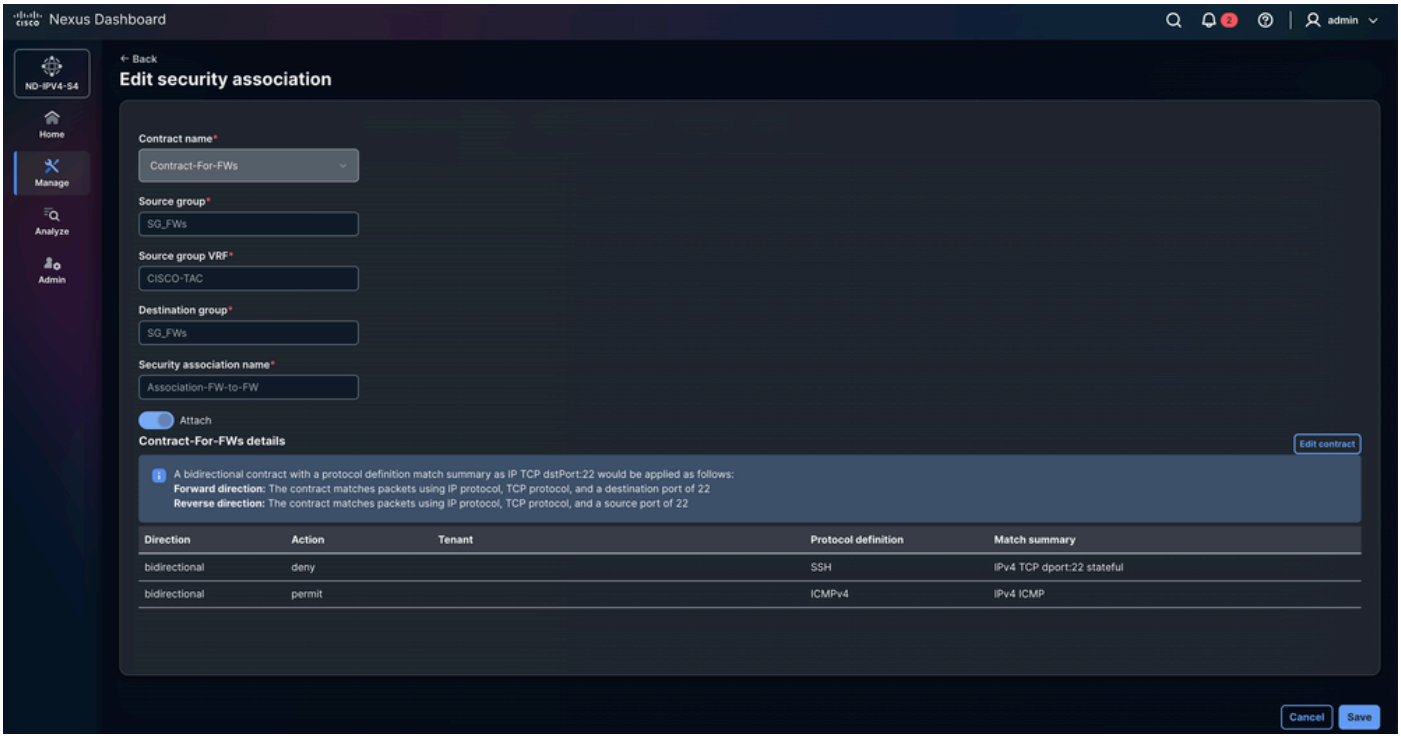


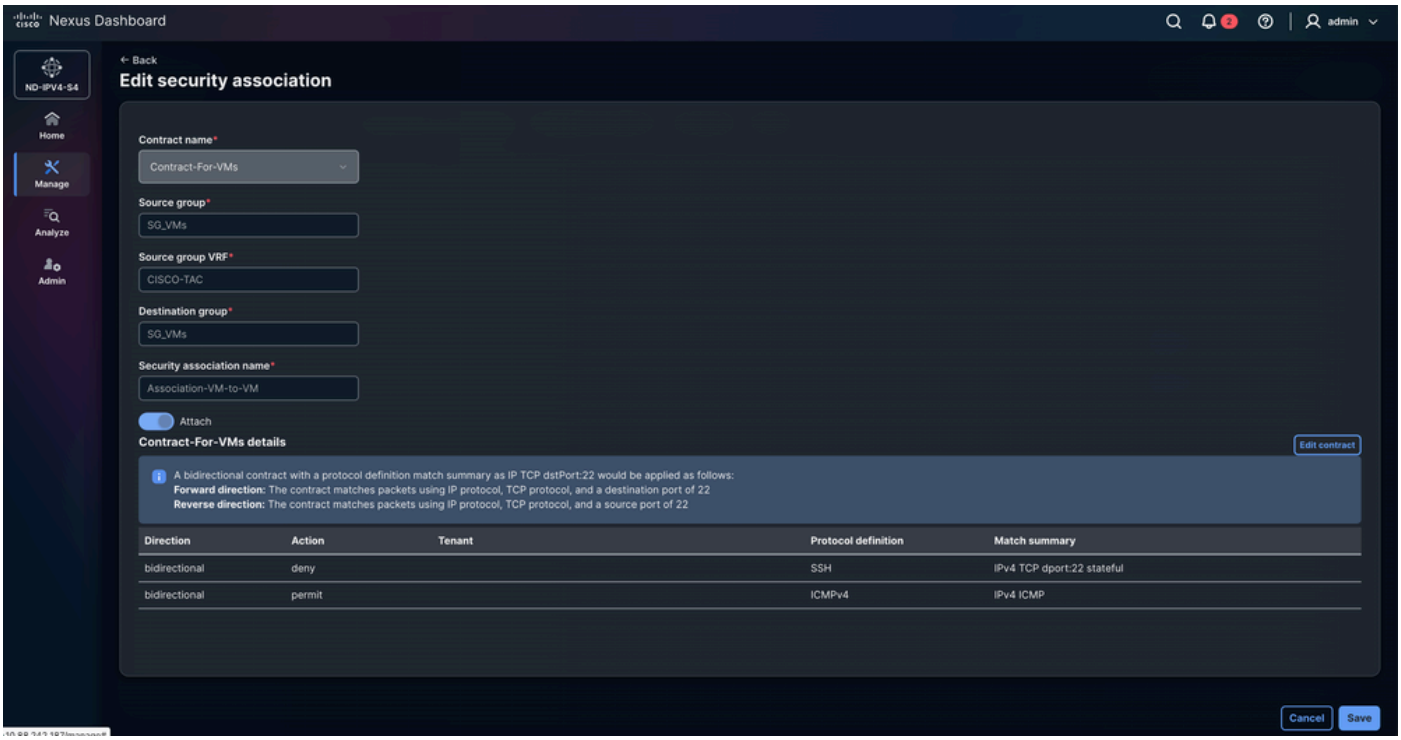


Étape 6. Configuration des associations de sécurité

Naviguez jusqu'à Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security associations > Actions > Create security association.

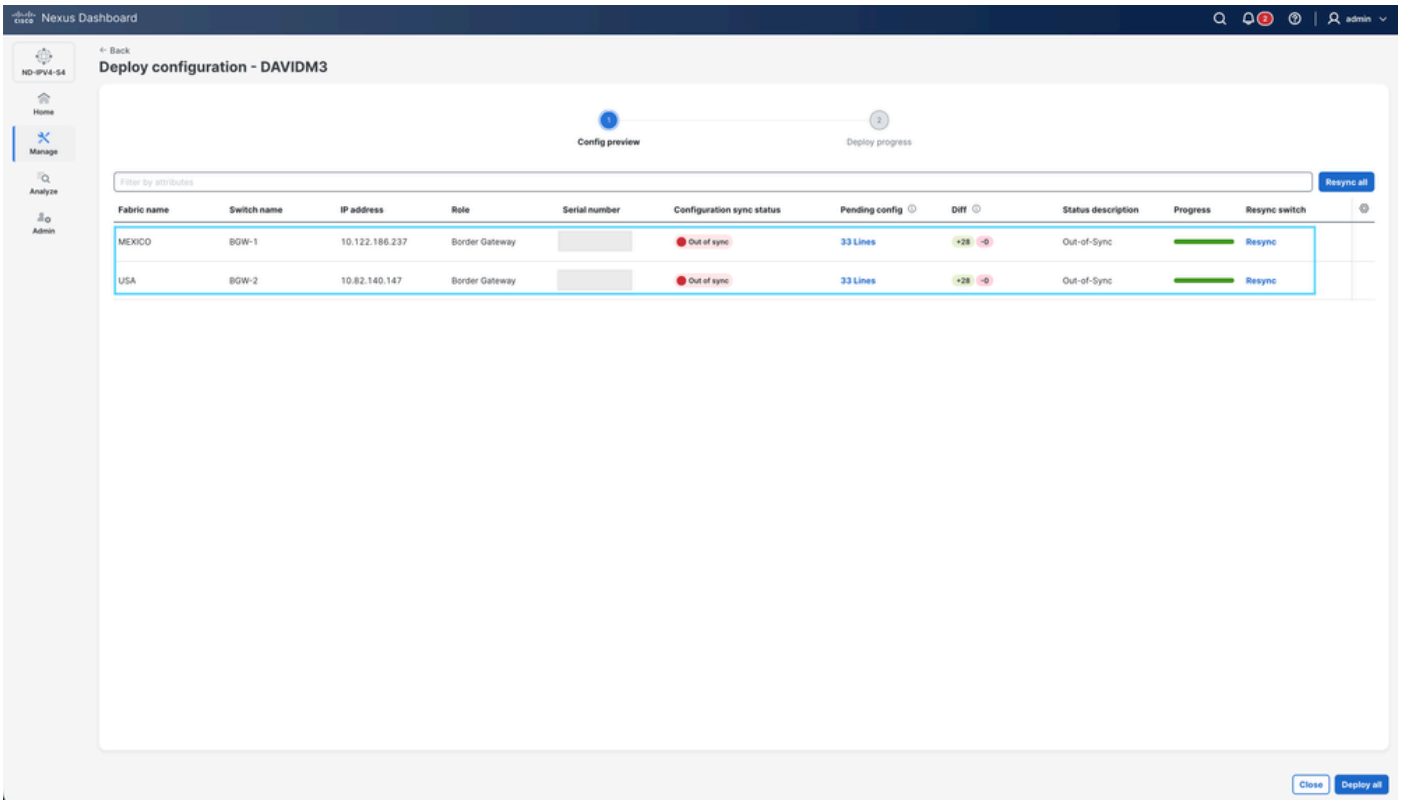
Dans Configurer les associations de sécurité, le modèle de stratégie est défini en liant les groupes de sécurité, les définitions de protocole et les contrats de sécurité. Les groupes de sécurité classent les terminaux, les définitions de protocole spécifient les types de trafic (tels que les protocoles ou les ports) et les contrats de sécurité définissent la stratégie appliquée entre les groupes de sécurité source et de destination à l'aide de ces règles de protocole. Les associations de sécurité représentent la relation qui lie ces éléments entre eux afin que le fabric puisse appliquer les stratégies de sécurité définies.

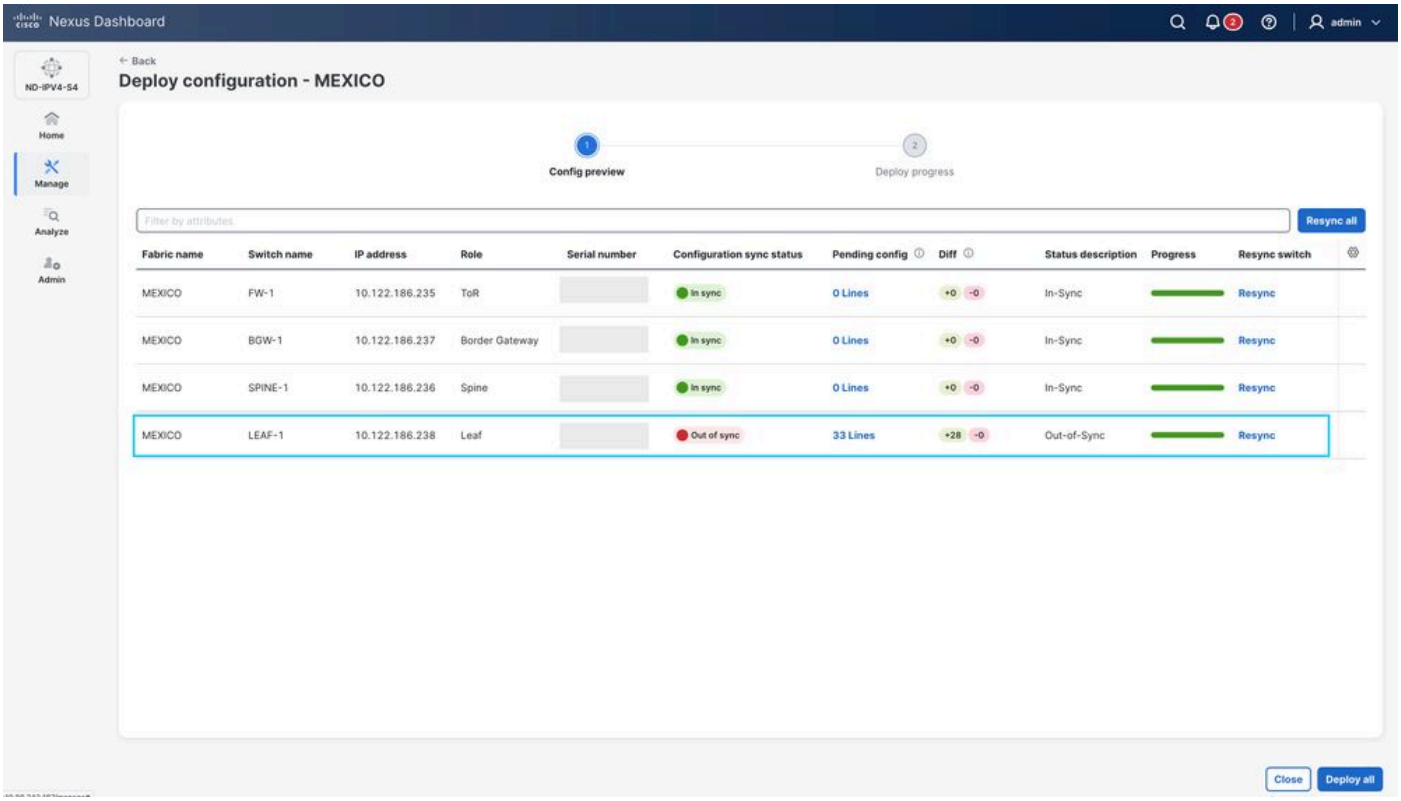


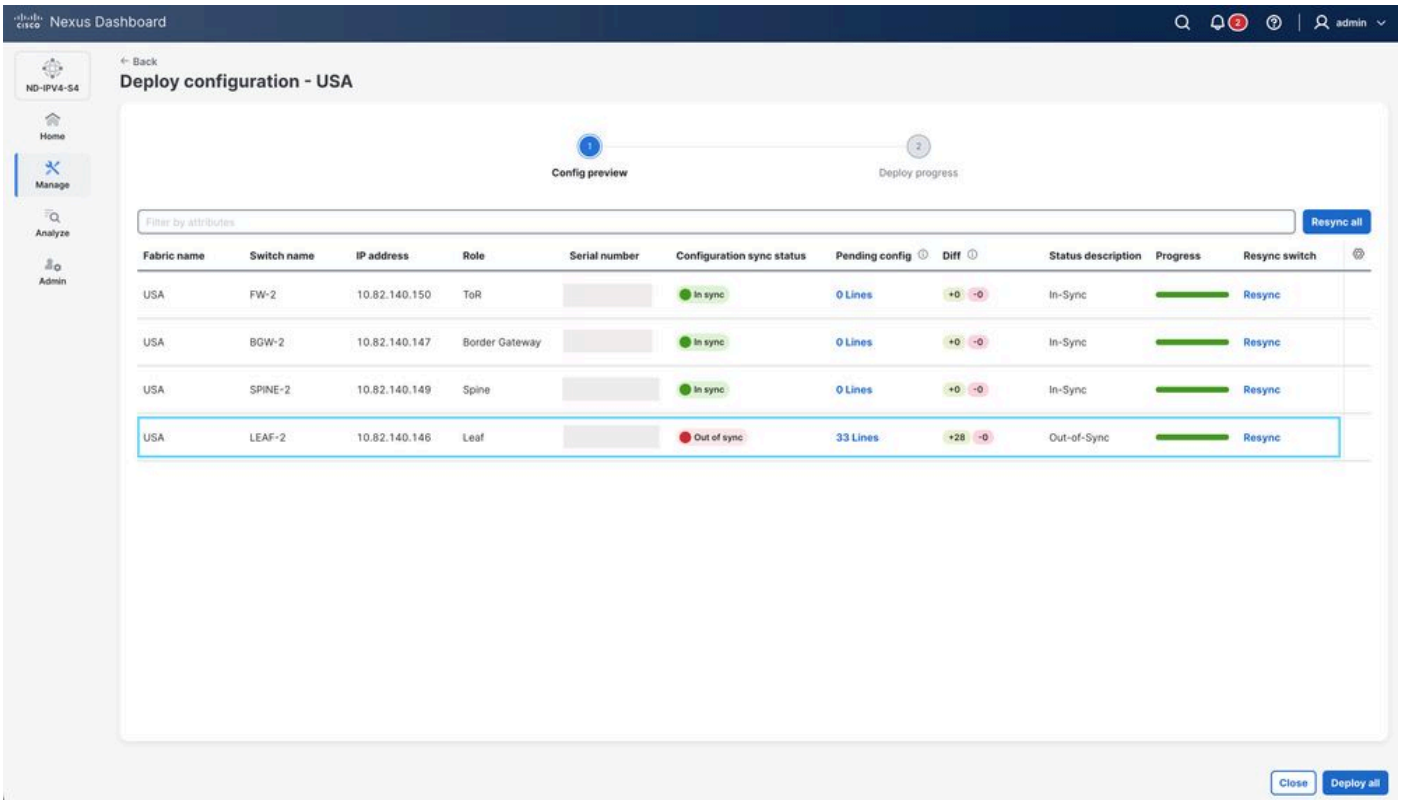


Étape 7 : validation de la configuration GPO

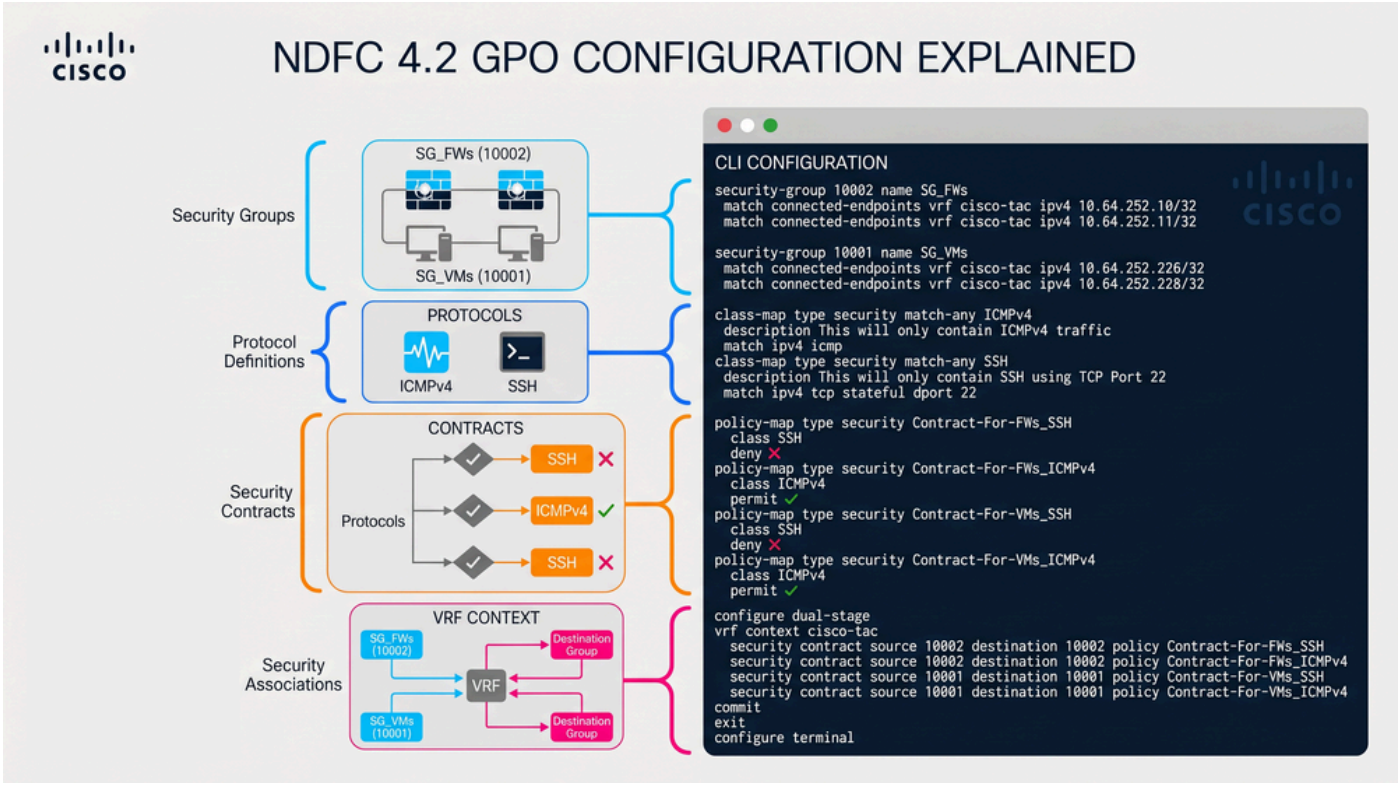
- Naviguez jusqu'à Manage > Fabrics > Fabric groups > DAVIDM3 > Actions > Recalculate and deploy.
  - La configuration de l'objet de stratégie de groupe est transmise aux passerelles de périphérie à partir du commutateur de fabric parent. Cliquez sur le nombre de lignes de configuration en attente pour vérifier et valider la configuration pouvant être déployée sur les périphériques. Ce processus doit être répété pour chaque fabric enfant.
  - Accédez à Manage > Fabrics > Fabric groups > DAVIDM3 > Inventory > Member fabrics > MEXICO > Actions > Recalculate and deploy.
  - Accédez à Manage > Fabrics > Fabric groups > DAVIDM3 > Inventory > Member fabrics > USA > Actions > Recalculate and deploy.


Nexus Dashboard
admin
ND-IPV4-S4
Home
Manage
Analyze
Admin
Back
Deploy configuration - DAVIDM3
1
Config preview
2
Deploy progress
Filter by attributes
Resync all
Fabric name
Switch name
IP address
Role
Serial number
Configuration sync status
Pending config
Diff
Status description
Progress
Resync switch
MEXICO
BGW-1
10.122.186.237
Border Gateway
Out of sync
33 Lines
+28
-0
Out-of-Sync
Resync
USA
BGW-2
10.82.140.147
Border Gateway
Out of sync
33 Lines
+28
-0
Out-of-Sync
Resync
Close
Deploy all


Nexus Dashboard
admin
ND-IPV4-S4
Home
Manage
Analyze
Admin
Back
Deploy configuration - MEXICO
1
Config preview
2
Deploy progress
Filter by attributes
Resync all
Fabric name
Switch name
IP address
Role
Serial number
Configuration sync status
Pending config
Diff
Status description
Progress
Resync switch
MEXICO
FW-1
10.122.186.235
ToR
In sync
0 Lines
+0
-0
In-Sync
Resync
MEXICO
BGW-1
10.122.186.237
Border Gateway
In sync
0 Lines
+0
-0
In-Sync
Resync
MEXICO
SPINE-1
10.122.186.236
Spine
In sync
0 Lines
+0
-0
In-Sync
Resync
MEXICO
LEAF-1
10.122.186.238
Leaf
Out of sync
33 Lines
+28
-0
Out-of-Sync
Resync
Close
Deploy all



- L'image présente la configuration de l'objet de stratégie de groupe pour BGW-1, BGW-2, LEAF-1 et LEAF-2. La configuration est identique sur tous les commutateurs. NDFC 4.2 n'applique pas la configuration dans l'ordre exact indiqué. Cette section illustre la séquence logique des commandes CLI.



Dépannage de l'opérabilité GPO VXLAN

Étape 1 : vérification de l’état des fonctions du groupe de sécurité

Vérifiez si la fonction security-group est activée sur le commutateur. L'objet de stratégie de groupe VXLAN dépend de cette fonctionnalité, car il active l'infrastructure SGT (Security Group Tag) requise pour la classification des terminaux, l'application des contrats et la programmation matérielle SGACL.

```
<#root>

BGW-1#

show feature | i i security-group


security-group 1 enabled
```

Étape 2. Vérification du mode de routage du système

Validez le mode de routage du système configuré et opérationnel sur le commutateur. L'objet de stratégie de groupe VXLAN nécessite le mode de routage Prise en charge des groupes de sécurité car l'application SGACL consomme des ressources de transfert matériel dédiées dans le pipeline ASIC.

```
<#root>

BGW-1#

show system routing mode


Configured System Routing Mode: Security-Groups Support
Applied System Routing Mode: Security-Groups Support
```

Étape 3. Vérification de l’établissement des homologues NVE VXLAN et de la capacité GPO

- Validez l'établissement d'homologue VXLAN NVE entre les périphériques de fabric locaux et les homologues multisites distants. Les informations d'objet de stratégie de groupe VXLAN

se propagent via le plan de contrôle EVPN VXLAN. Par conséquent, des contiguïtés NVE stables sont nécessaires pour l'apprentissage des balises de groupe de sécurité (SGT) et la synchronisation des contrats sur l'ensemble du fabric.
- La capacité de stratégie de groupe du champ est l'un des indicateurs les plus importants dans cette commande, car elle confirme si le VTEP distant prend en charge les extensions de stratégie de groupe VXLAN requises pour la propagation des balises de groupe et l'application du contrat SGACL dans le domaine multisite EVPN VXLAN.

<#root>

```
BGW-1#

show nve peers detail


## Details of nve Peers:

----------------------------------------
Peer-Ip: 10.10.10.2 ---------> Corresponds to

LEAF-1 Loopback1

, used as the local VXLAN NVE source interface.
NVE Interface       : nve1
Peer State          : Up --------> Confirms that the VXLAN tunnel and EVPN adjacency are operational.
Peer Uptime         : 6d21h --------> Indicates long-term adjacency stability.
Router-Mac          : 44b6.beb3.b703 --------> Remote VTEP router MAC used for VXLAN forwarding.
Peer First VNI      : 50012
Time since Create   : 6d21h
Configured VNIs     : 30136,30155,50012 --------> VNIs expected across this VXLAN adjacency.
Provision State     : peer-add-complete --------> Confirms successful hardware and software programming
Learnt CP VNIs      : 30136,30155,50012 --------> Confirms successful EVPN control-plane synchronizatio
vni assignment mode : SYMMETRIC --------> Symmetric IRB forwarding mode is operational.
Peer Location       : FABRIC --------> Indicates a local fabric peer.

Group policy capable: yes --------> Confirms that the remote VTEP supports Group Policy extensions and c


----------------------------------------
Peer-Ip: 10.20.20.2 ---------> Corresponds to

BGW-2 Loopback1

, used as the remote BGW NVE source interface.
NVE Interface       : nve1
Peer State          : Up
Peer Uptime         : 01:36:54
Router-Mac          : 4488.1618.f093
Peer First VNI      : 30136
Time since Create   : 01:36:54
Configured VNIs     : 30136,30155,50012
Provision State     : peer-add-complete
Learnt CP VNIs      : 30136,30155,50012
vni assignment mode : SYMMETRIC
```

```
Peer Location       : DCI

Group policy capable: yes



----------------------------------------
Peer-Ip: 10.150.150.2 ---------> Corresponds to

BGW-2 Loopback100

, used as the Multi-Site Loopback interface for DCI communication.
NVE Interface       : nve1
Peer State          : Up
Peer Uptime         : 01:32:58
Router-Mac          : 0200.0a96.9602
Peer First VNI      : 30136
Time since Create   : 01:32:58
Configured VNIs     : 30136,30155,50012
Provision State     : peer-add-complete
Learnt CP VNIs      : 30136,30155,50012
vni assignment mode : SYMMETRIC
Peer Location       : DCI

Group policy capable: yes



----------------------------------------
```

Étape 4. Vérification de la formation du groupe de sécurité et de la classification des terminaux

Vérifiez que les terminaux sont correctement classés dans les groupes de sécurité (SGT). L'application de l'objet de stratégie de groupe VXLAN dépend de mappages point de terminaison-SGT précis.

<#root>

```
BGW-1#

show security-group id all



Security Group ID 10001 , Name SG_VMs ---------> Security Group assigned to the Virtual Machines endpoi

  Selector Type : Connected IPv4 Endpoints ---------> Endpoints are classified dynamically based on loc

    VRF-Name                          IPv4-Address/mask-len
    cisco-tac                         10.64.252.226/32 ---------> Endpoint mapped to Security Group 1
    cisco-tac                         10.64.252.228/32 ---------> Endpoint mapped to Security Group 1
```

```
Security Group ID 10002 , Name SG_FWs ---------> Security Group assigned to the Firewall endpoint group

  Selector Type : Connected IPv4 Endpoints ---------> Endpoint classification occurs using locally lear

    VRF-Name                          IPv4-Address/mask-len
    cisco-tac                         10.64.252.10/32 ---------> Firewall endpoint mapped to Security
    cisco-tac                         10.64.252.11/32 ---------> Firewall endpoint mapped to Security
```

Étape 5. Vérification des contrats de sécurité et de l'application des stratégies

Vérifiez que les contrats GPO VXLAN sont correctement installés et opérationnels. Les contrats définissent les règles de communication appliquées entre les groupes de sécurité et représentent le mécanisme de stratégie principal utilisé par l'objet de stratégie de groupe VXLAN pour la microsegmentation.

<#root>

```
BGW-1#

show contracts detail


VRF: cisco-tac ---------> Confirms that contract enforcement occurs inside the cisco-tac tenant VRF.

Contract source group 10001 dest group 10001 ---------> Policy enforcement between endpoints belonging

  Policy: Contract-For-VMs_ICMPv4 Direction: bidir ---------> Bidirectional contract for ICMPv4 traffic

    Stats: 0 ---------> No traffic has matched this contract yet.

    Class: ICMPv4 ---------> Traffic classification associated with ICMP traffic.

      match ipv4 icmp ---------> Matches ICMPv4 traffic including ping requests and replies.

    Action: permit ---------> ICMP traffic is explicitly allowed.

    OperSt: enabled ---------> Confirms that the contract is operational.

Contract source group 10001 dest group 10001

  Policy: Contract-For-VMs_SSH Direction: bidir

    Stats: 0

    Class: SSH

      match ipv4 tcp stateful dport 22 ---------> Matches SSH traffic using stateful TCP inspection.

    Action: deny ---------> SSH traffic is explicitly denied.

    OperSt: enabled

Contract source group 10002 dest group 10002

  Policy: Contract-For-FWs_ICMPv4 Direction: bidir
```

```
    Stats: 0
    Class: ICMPv4
      match ipv4 icmp
    Action: permit
    OperSt: enabled
Contract source group 10002 dest group 10002
  Policy: Contract-For-FWs_SSH Direction: bidir
    Stats: 0
    Class: SSH
      match ipv4 tcp stateful dport 22
    Action: deny
    OperSt: enabled
```

Étape 6. Vérification de l’état de la sécurité VRF

Validez l'état d'application de l'objet GPO VXLAN pour tous les VRF configurés sur le commutateur. Cette commande confirme si les stratégies SGACL et les contrats de groupe de sécurité sont activement appliqués dans le VRF du locataire.

Le résultat confirme que le VRF cisco-tac participe activement à l'application de l'objet de stratégie de groupe VXLAN, le mode étant défini sur imposé. La balise d'application 13648 identifie le contexte de stratégie SGACL interne programmé dans le matériel pour ce VRF. Le journal de refus d'action par défaut indique que tout trafic non explicitement autorisé via un contrat de groupe de sécurité est refusé et consigné, mettant en oeuvre une politique de microsegmentation de refus par défaut. En revanche, les VRF de gestion, de gestion et d'équilibrage de charge de sortie par défaut fonctionnent en mode non appliqué, ce qui signifie que les stratégies d'objet de stratégie de groupe VXLAN ne sont pas appliquées dans ces VRF et que le trafic est autorisé par défaut.

Le champ Stats suit le trafic correspondant à la stratégie de sécurité VRF. La valeur 0 sous le VRF cisco-tac indique qu'aucun trafic sans correspondance n'a déclenché le comportement de refus par défaut au moment de l'exécution de la commande, tandis que la valeur de compteur 4364 sous le VRF par défaut indique une activité de trafic au sein d'un VRF fonctionnant sans application de l'objet de stratégie de groupe VXLAN.

<#root>

```
BGW-1#
```

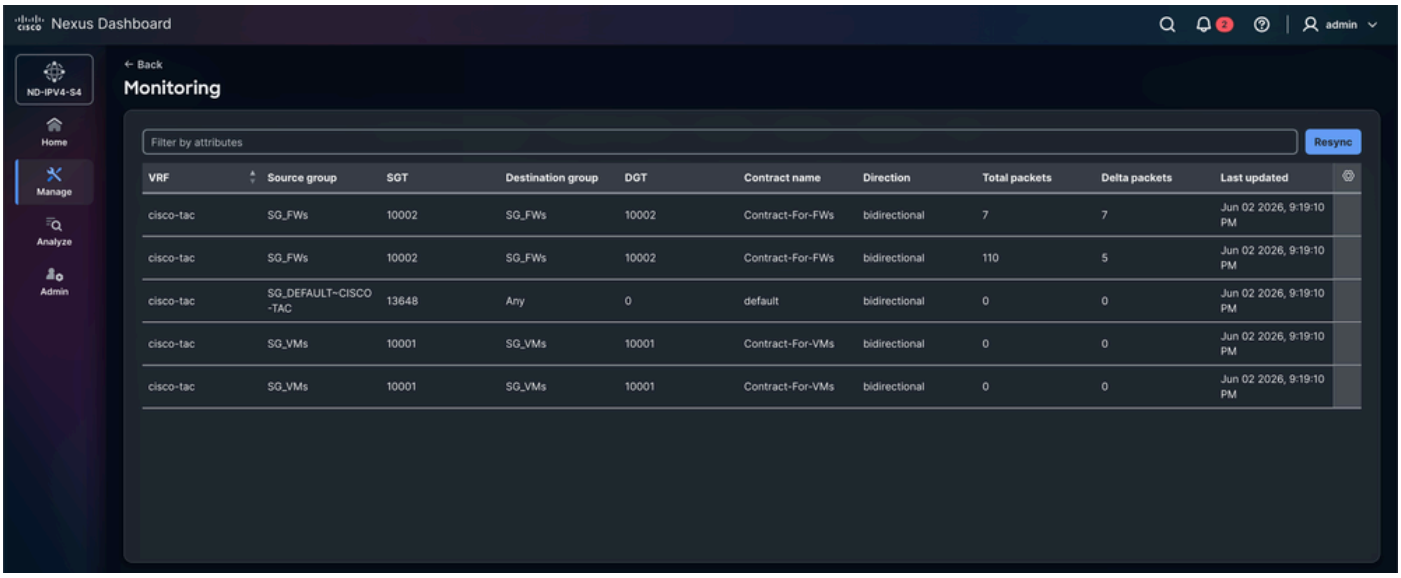
show vrf all security

```
VRF                                Mode         TAG     Action     Scope   Stats
-------------------------------------------------------------------------------
cisco-tac                          enforced     13648   deny,log   4       0
default                            unenforced   -       permit     1       4364
egress-loadbalance-resolution-     unenforced   -       permit     2       0
management                         unenforced   -       permit     3       0
```

Étape 7. Vérification de l’état de la sécurité VRF

- Validez les statistiques de correspondance de trafic pour les contrats GPO VXLAN à partir de l'interface graphique NDFC. Cette vérification confirme si le trafic correspond activement aux contrats du groupe de sécurité configurés et si l'application de la liste SGACL est opérationnelle sur le fabric multisite EVPN VXLAN.
- Dans l'interface graphique NDFC, accédez à Manage > Fabrics > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoring.
    - Cette section fournit une visibilité sur les flux de communication du groupe de sécurité, les statistiques d'accès aux contrats, les actions d'autorisation et de refus et l'activité des contrats opérationnels entre les groupes de terminaux.
    - Les statistiques de surveillance s'affichent individuellement dans chacune d'elles.
    - Les statistiques de surveillance de NDFC fournissent une couche de validation opérationnelle qui complète le dépannage basé sur l'interface de ligne de commande en confirmant l'application des politiques en temps réel et le comportement de correspondance du trafic dans le fabric.

Remarque : Lors de la première tentative de révision des statistiques de trafic dans NDFC 4.2, la section de surveillance peut apparaître initialement vide. Dans ce cas, appuyez sur le bouton Resync pour déclencher la synchronisation des statistiques de contrat à partir du fabric VXLAN. Pendant l'exécution du processus de synchronisation, l'interface utilisateur graphique affiche le message Resync status : En cours. Une fois la synchronisation terminée, appuyez sur le bouton Ok pour actualiser la vue de surveillance. Une fois la resynchronisation terminée, les statistiques de trafic associées à chaque contrat de groupe de sécurité deviennent visibles dans la section de surveillance. Afin de valider le comportement de correspondance de trafic en direct, générez du trafic entre les points d'extrémité, puis appuyez de nouveau sur le bouton Resync pour mettre à jour les statistiques de contrat affichées dans NDFC.



- Dans le scénario précédent, le trafic ICMPv4 est autorisé entre les points d'extrémité. Cependant, si une session SSH est établie, la connexion expire parce que le contrat VXLAN GPO refuse explicitement le trafic TCP destiné au port 22.

<#root>

```
FW-1#

ping 10.64.252.11


PING 10.64.252.11 (10.64.252.11): 56 data bytes
64 bytes from 10.64.252.11: icmp_seq=0 ttl=254 time=1.131 ms
64 bytes from 10.64.252.11: icmp_seq=1 ttl=254 time=0.694 ms
64 bytes from 10.64.252.11: icmp_seq=2 ttl=254 time=0.675 ms
64 bytes from 10.64.252.11: icmp_seq=3 ttl=254 time=0.657 ms
64 bytes from 10.64.252.11: icmp_seq=4 ttl=254 time=0.648 ms

--- 10.64.252.11 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.648/0.761/1.131 ms
FW-1#

ssh admin@10.64.252.11


ssh: connect to host 10.64.252.11 port 22: Connection timed out
```

Informations connexes

[Guide de configuration VXLAN de la gamme Cisco Nexus 9000 NX-OS, version 10.6(x)]

Sécurisation des data centers avec microsegmentation via VXLAN GPO

Déploiement de la microsegmentation dans les fabrics EVPN VXLAN Cisco NX-OS avec l'option de stratégie de groupe (GPO) VXLAN

Automatisation de la micro-segmentation et déploiement de services de couche 4 à 7 dans les fabrics EVPN VXLAN à l'aide de l'option de stratégie de groupe (GPO) et du tableau de bord Nexus

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.