GPO configureren op Nexus Multi-Site Fabric met NDFC 4.2

Inhoud

Inleiding

In dit document worden de GPO-configuratie en -validatie beschreven in VXLAN-verbindingen met

meerdere locaties op Nexus Cloud Scale-switches met NX-OS en NDFC 4.2.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze gebieden:

- Virtual Extensible Local Area Network (VXLAN)-, Ethernet Virtual Private Network (EVPN)- en Multi-Site Fabric-technologieën
- Cisco Nexus Cloud Scale-switches en NeXus Operating System (NX-OS)-bediening
- Beheer- en implementatieworkflows voor Nexus Fabric Network Controller (NDFC) 4.2
- Concepten voor netwerksegmentatie en beveiligingsbeleid

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

GPO-functionaliteit in VXLAN EVPN-verbindingen begrijpen

Group Policy Option (GPO) is een op beleid gebaseerd segmentatiemechanisme dat is ontworpen om de communicatie tussen eindpunten te regelen op basis van logische identiteit in plaats van alleen te vertrouwen op IP-adressen, VLAN's of subnetten. Het belangrijkste doel van GPO is om de handhaving van het beveiligingsbeleid te vereenvoudigen en een schaalbare microsegmentatie tussen toepassingen, servers of werkbelastingen te bieden.

Een eenvoudige analogie is om te denken aan een hotel waar elke gast tot een specifieke categorie of toegangsniveau behoort, bepaalde gebieden zijn alleen toegankelijk voor specifieke gasten en toegangsrechten zijn afhankelijk van de rol van de gast in plaats van het kamernummer.

GPO werkt op een vergelijkbare manier. In plaats van eindpunten puur als IP-adressen te behandelen, classificeert GPO ze in beveiligingsgroepen (SG's). Beleid wordt vervolgens toegepast tussen deze groepen om te bepalen welke communicatie is toegestaan of geweigerd.

Voorbeeld:

- Webservers kunnen tot één beveiligingsgroep behoren.
- Toepassingsservers kunnen tot een andere beveiligingsgroep behoren.
- Databaseservers kunnen tot een beperkte beveiligingsgroep behoren.

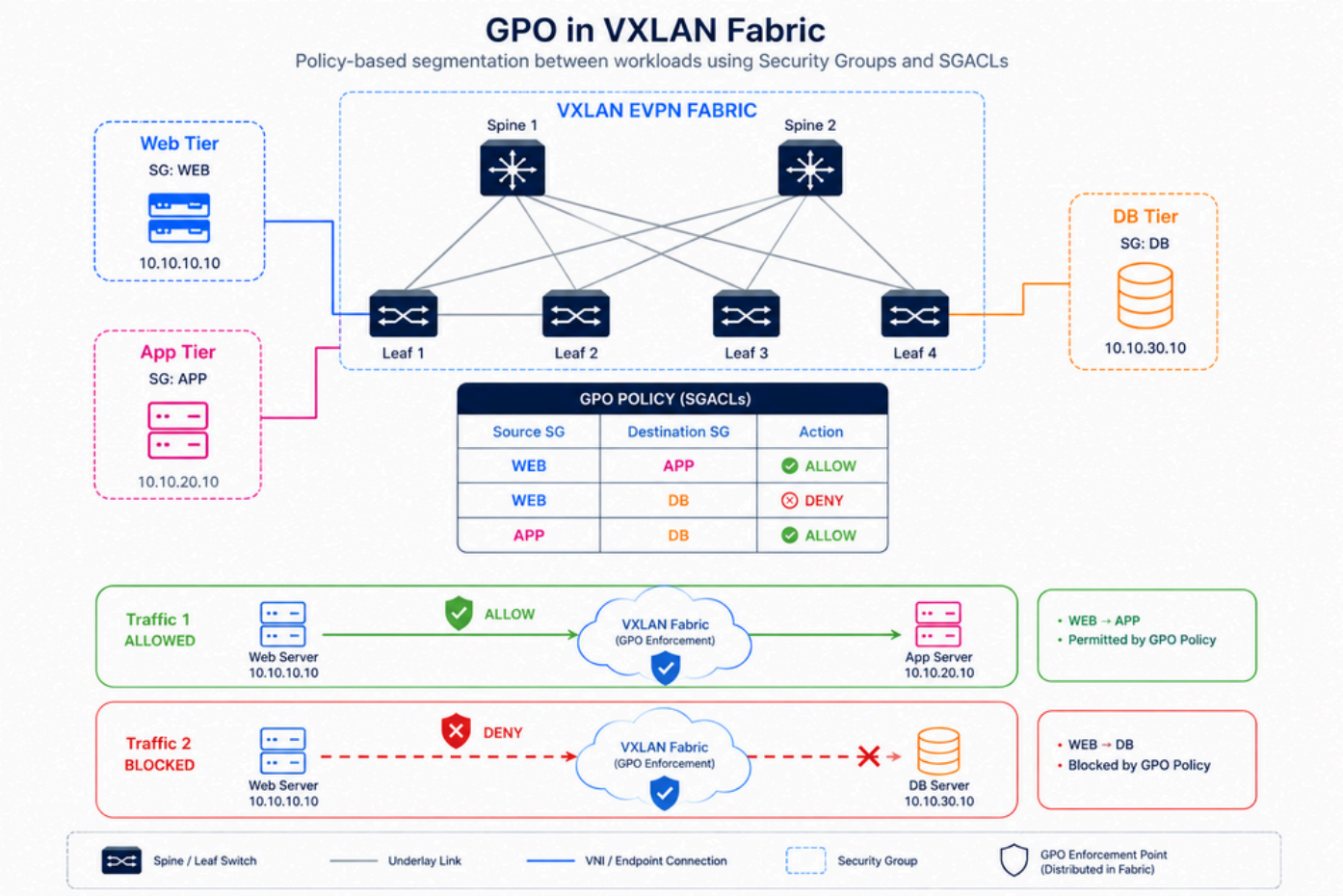
Beleid kan dan definiëren:

- Webservers kunnen communiceren met toepassingsservers.
- Toepassingsservers kunnen communiceren met databaseservers.
- Webservers kunnen niet rechtstreeks communiceren met databaseservers.

Deze aanpak vereenvoudigt de bewerkingen omdat beheerders niet langer grote aantallen ACL's op meerdere apparaten en VLAN's hoeven te onderhouden.

Een ander groot voordeel is de schaalbaarheid. In grote omgevingen worden werklasten vaak verplaatst, dynamisch geschaald of IP-adressen gewijzigd. Met GPO kan het beveiligingsbeleid consistent blijven, zelfs wanneer de locatie van het eindpunt verandert. Binnen VXLAN EVPN-verbindingen breidt GPO dit concept uit door informatie over de beveiligingsgroep over de structuur te verspreiden en ACL's (Security Group ACL's) tussen eindpunten af te dwingen. Dit wordt vooral belangrijk in moderne datacenters omdat oost-west verkeer tussen werkbelastingen vaak het grootste aanvalsoppervlak vertegenwoordigt. GPO verbetert de beveiligingspositie door onnodige communicatiepaden in de datacenterstructuur te beperken.

Voor een dieper technisch inzicht in GPO-architectuur, micro-segmentatieconcepten en handhaving van het VXLAN-beleid, raadpleegt u de Cisco-whitepaper die beschikbaar is op: Data Centers beveiligen met microsegmentatie met behulp van VXLAN GPO



GPO in VxLAN-verbinding

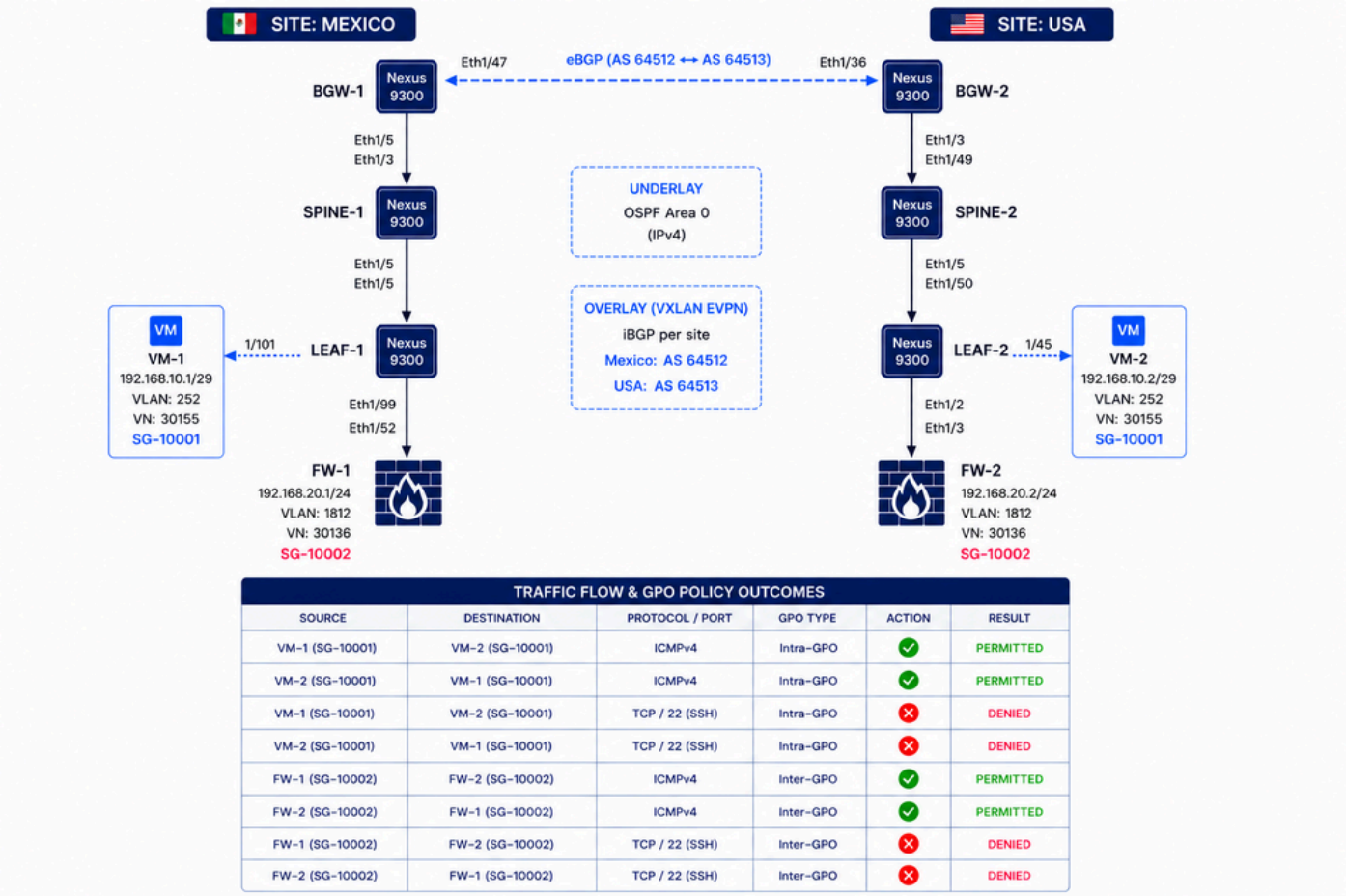
GPO-implementatiescenario voor VXLAN-multisite met behulp van NDFC 4.2 en NX-OS 10.6(3)F

Deze topologie vertegenwoordigt een VXLAN Multi-Site fabric die wordt geïmplementeerd op twee geografisch gedistribueerde locaties: Mexico en de VS. Elke site bevat speciale BGW's, Spine-switches, Leaf-switches, virtuele machines en firewallsegmenten die worden uitgevoerd op Cisco Nexus 9300-switches met NX-OS 10.6(3)F. Het onderliggend netwerk maakt gebruik van Open Shortest Path First (OSPF), terwijl het overlay control plane iBGP gebruikt binnen elke site en eBGP tussen BGW-1 en BGW-2 voor inter-site VXLAN EVPN-communicatie. Aangezien deze omgeving een laboratoriuminstallatie is, zijn de locaties in Mexico en de VS onderling verbonden via een rechtstreeks verbonden verbinding tussen beide BGW's om het connectiviteitsmodel voor meerdere locaties te vereenvoudigen.

GPO wordt gebruikt om op beleid gebaseerde microsegmentatie tussen beveiligingsgroepen (SG's) af te dwingen, onafhankelijk van IP-adressering of VLAN-grenzen. Op basis van de tabel

met het connectiviteitsbeleid is ICMP-verkeer van VM-1 naar VM-2, FW-1 en FW-2 toegestaan, terwijl TCP-poort 22 (SSH)-verkeer van VM-1 naar FW-1 en FW-2 wordt geweigerd. TCP-poort 22-communicatie tussen VM-1 en VM-2 blijft toegestaan omdat beide eindpunten tot dezelfde beveiligingsgroep behoren (SG-10001). Dit gedrag laat zien hoe GPO dynamisch verschillende verkeersregels afdwingt tussen intra-GPO- en inter-GPO-communicatie via de VXLAN Multi-Site fabric.

Opmerking: Cisco NX-OS Release 10.6(3)F introduceert dat u de communicatie tussen de eindpunten binnen hetzelfde ESG (ook bekend als SG) kunt beperken met behulp van de intra-ESG-isolatiefunctie. Deze functie minimaliseert het risico van ongeoorloofde toegang binnen ESG en verbetert de beveiligingspositie.



TRAFFIC FLOW & GPO POLICY OUTCOMES

SOURCE	DESTINATION	PROTOCOL / PORT	GPO TYPE	ACTION	RESULT
VM-1 (SG-10001)	VM-2 (SG-10001)	ICMPv4	Intra-GPO	✓	PERMITTED
VM-2 (SG-10001)	VM-1 (SG-10001)	ICMPv4	Intra-GPO	✓	PERMITTED
VM-1 (SG-10001)	VM-2 (SG-10001)	TCP / 22 (SSH)	Intra-GPO	✗	DENIED
VM-2 (SG-10001)	VM-1 (SG-10001)	TCP / 22 (SSH)	Intra-GPO	✗	DENIED
FW-1 (SG-10002)	FW-2 (SG-10002)	ICMPv4	Inter-GPO	✓	PERMITTED
FW-2 (SG-10002)	FW-1 (SG-10002)	ICMPv4	Inter-GPO	✓	PERMITTED
FW-1 (SG-10002)	FW-2 (SG-10002)	TCP / 22 (SSH)	Inter-GPO	✗	DENIED
FW-2 (SG-10002)	FW-1 (SG-10002)	TCP / 22 (SSH)	Inter-GPO	✗	DENIED

GPO stap voor stap configureren met NDFC 4.2 in VXLAN EVPN-verbindingen

Deze stappen zijn van toepassing wanneer de VXLAN Multi-Site Fabric al operationeel is en is geconfigureerd met NDFC 4.2 en GPO daarna moet worden geïmplementeerd. De sectie

Automation Using Nexus Dashboard in Securing Data Centers with Microsegmentation Using VXLAN GPO toont de configuratie vanaf de creatie van een VXLAN Single-Site fabric.

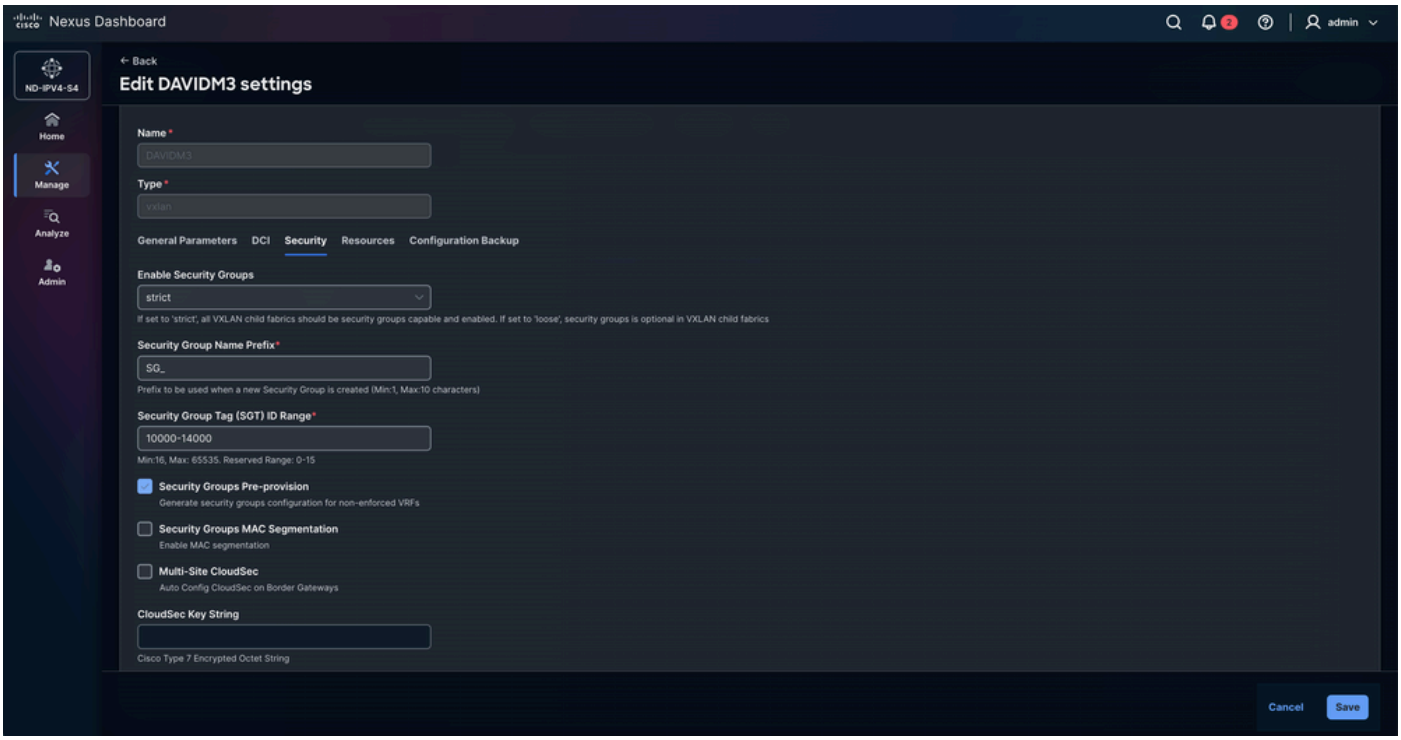
⚠ Let op: wanneer GPO in een VXLAN EVPN-fabric werkt, vindt communicatie alleen plaats als de bereikbaarheid van de bestemming bestaat en het beveiligingsbeleid het verkeer toestaat. Beleidshandhaving is gebaseerd op IP-informatie, waarvoor ARP-vermeldingen en SVI's voor interne netwerken vereist zijn. Dit betekent dat voor het VLAN van de tenant VRF een SVI moet zijn geconfigureerd. Handhaving is daarom niet van toepassing op verkeer dat alleen Layer 2-headers bevat en daarom niet kan worden gebruikt met VXLAN Layer 2-extensie. NX-OS Release 10.6(2)F introduceert ondersteuning voor MAC-gebaseerde microsegmentatie.

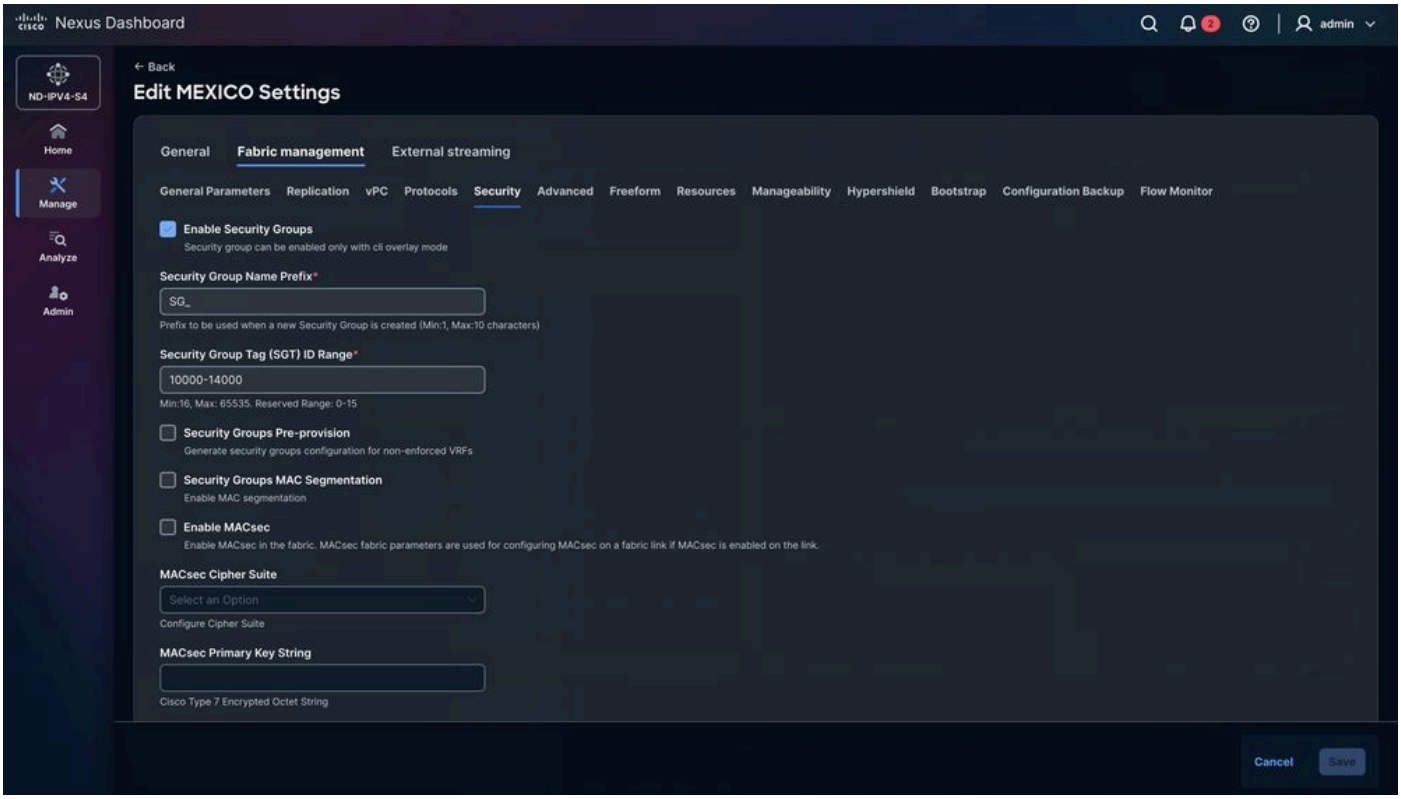
Stap 1. Beveiligingsgroepen inschakelen in de bovenliggende structuur

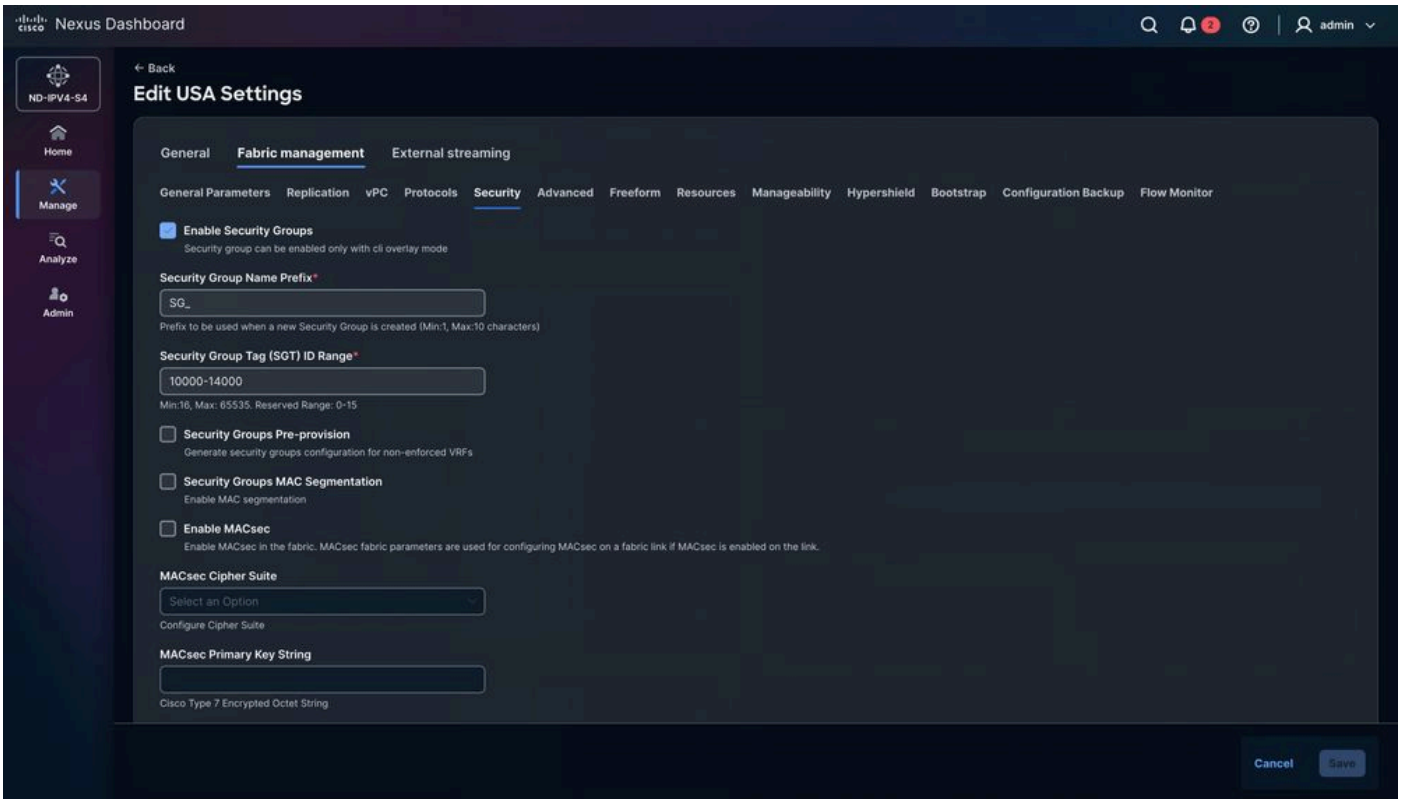
- Navigeer naar Beheer > Verbindingsgroepen, selecteer de structuurgroep DAVIDM3 en kies Acties > Verbindingsgroepinstellingen bewerken. Schakel in het gedeelte Beveiliging Beveiligingsgroepen in, stel de modus in op Strict en stel Beveiligingsgroepen in Voorvoorziening.
  - Selecteer de stof groep van belang. In dit voorbeeld wordt de geselecteerde weefselgroep DAVIDM3 genoemd, wat ook de naam is van de Multi-Site Fabric.
- Herhaal deze stappen voor elk kind stof.
  - Navigeer naar Beheer > Fabric, selecteer USA en navigeer naar Acties > Fabric Group Settings bewerken. Schakel in het gedeelte Beveiliging Beveiligingsgroepen in en stel de modus in op Strict.
  - Navigeer naar Beheren > Fabric, selecteer MEXICO en navigeer vervolgens naar Acties > Fabric Group Settings bewerken. Schakel in het gedeelte Beveiliging Beveiligingsgroepen in en stel de modus in op Strict.

✎ Opmerking: als deze optie is ingesteld op strict, moeten alle onderliggende VXLAN-verbindingen geschikt en ingeschakeld zijn voor beveiligingsgroepen. Als deze optie op los is ingesteld, zijn beveiligingsgroepen optioneel in onderliggende VXLAN-verbindingen.

🔍 Tip: gebruik dezelfde SGT-ID-bereiken (Security Group Tag) in de bovenliggende structuur en in alle onderliggende structuren om de zichtbaarheid te behouden. Het bovenliggende stoffenassortiment moet het bereik bestrijken dat door alle onderliggende weefsels wordt gebruikt.


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



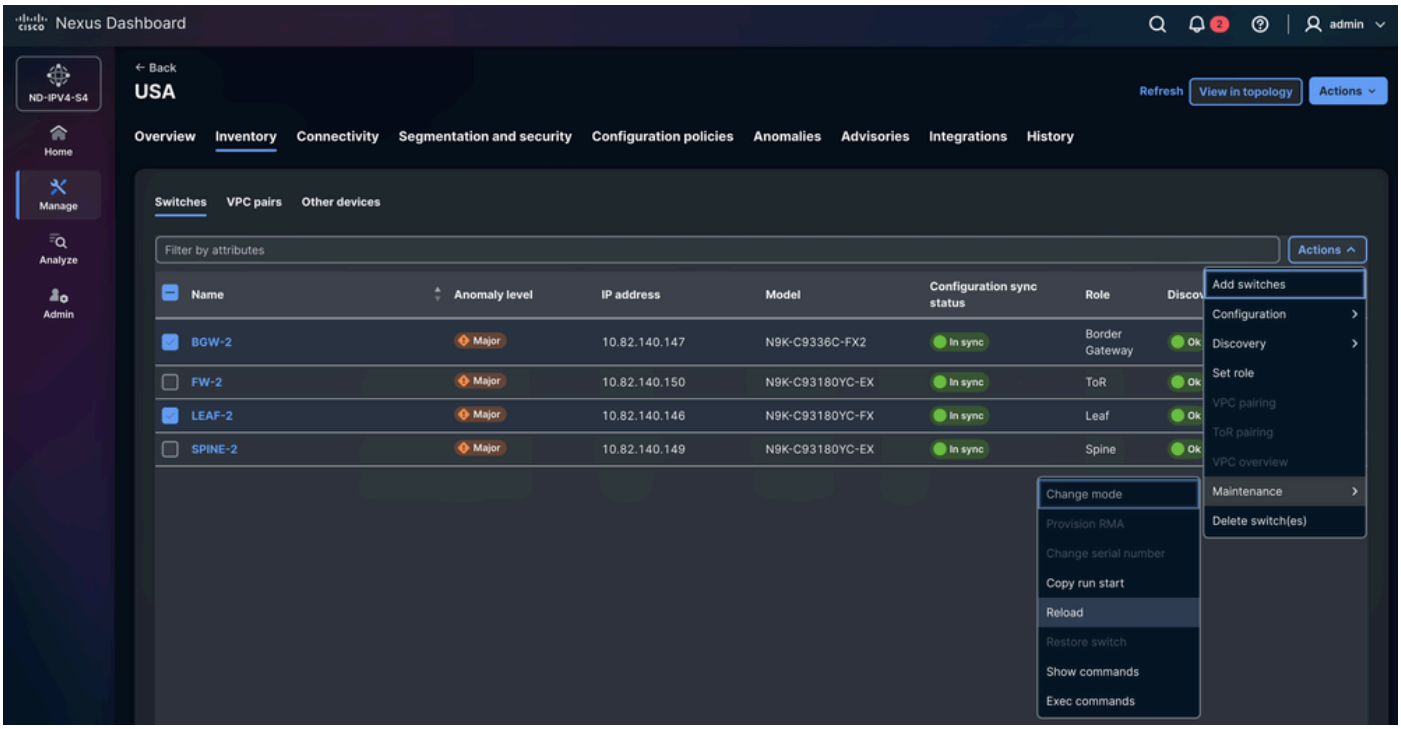
Stap 2. Fabric-configuratie opnieuw berekenen en Switches opnieuw laden voor GPO-implementatie

NDFC vraagt je automatisch om een specifieke groep Nexus-switches opnieuw te laden op basis van hun rol. In dit voorbeeld moeten LEAF-1, LEAF-2, BGW-1 en BGW-2 opnieuw worden geladen. Deze actie moet handmatig worden uitgevoerd door de netwerkbeheerder. Het opnieuw laden is vereist en kan niet worden overgeslagen omdat GPO TCAM-snijwerk vereist.

Opmerking: als het toestel niet opnieuw is geladen, kan de TCAM-wijziging worden weergegeven in de actieve configuratie. Aangezien de switch echter niet opnieuw is opgestart, wordt de instelling niet toegepast op het hardwaregeheugen. Hierdoor kan de functie niet functioneren zoals verwacht.

De Nexus-switches opnieuw laden:

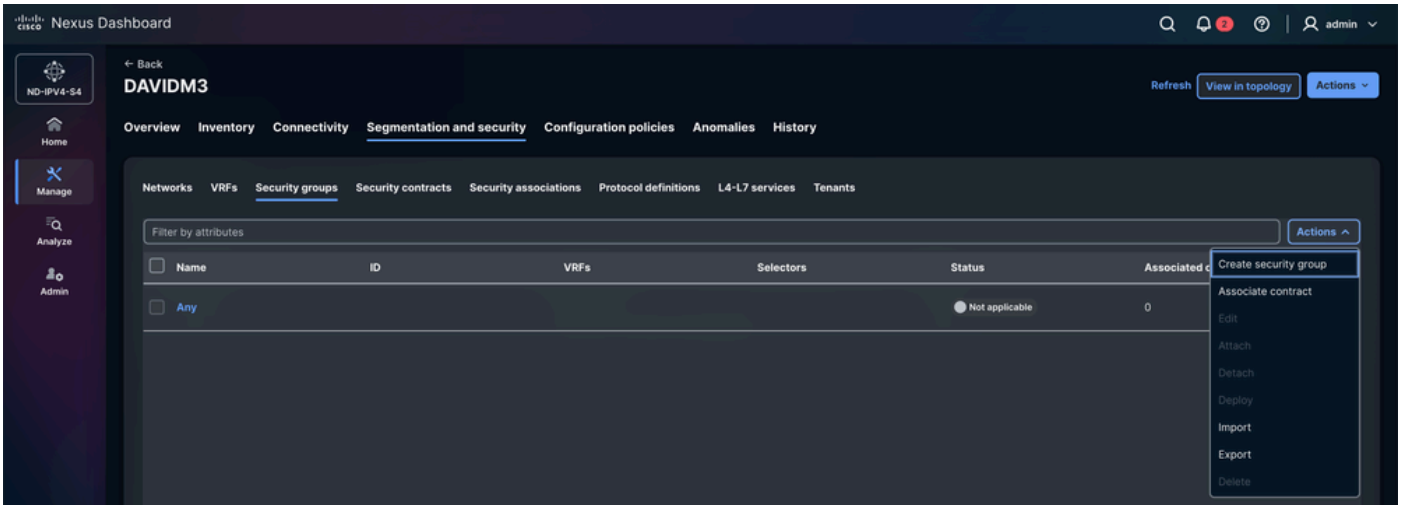
Navigeer naar Beheer > Stoffen > MEXICO/USA > Voorraad > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Acties > Onderhoud > Opnieuw laden.



Stap 3. Beveiligingsgroep maken

Definieer de beveiligingsgroepen voor elk eindpunt. Elk eindpunt in de VXLAN-verbindingen kan één beveiligingsgroep hebben. Deze aanpak is niet efficiënt schaalbaar. Wereldwijd groepseindpunten (onder andere virtuele machines, firewalls en TCP-optimizers).

Navigeer naar Beheer > Verbindingen > Verbindingsgroepen > DAVIDM3 > Segmentatie en beveiliging > Beveiligingsgroepen > Acties > Beveiligingsgroep maken.



Stap 3.1 De naam van de beveiligingsgroep configureren

- NDFC kent automatisch een willekeurige naam toe. De naam kan worden gewijzigd; het wordt aanbevolen om een representatieve naam te gebruiken die gemakkelijk te identificeren is voor eindpunten.
- In dit scenario:
    - VM's -> SG_VM's
    - FW's -> SG_FW's

Stap 3.2 VRF configureren

- Selecteer de tenant (VRF) waartoe de eindpunten behoren.
- In dit scenario: De VM's en firewalls behoren toe aan de CISCO-TAC-huurder.

Optioneel, VRF maken.

Standaard is voor een nieuw gemaakte tenant-VRF de modus voor beleidsafdwinging ingesteld op Niet afgedwongen. In deze status vindt geen beleidshandhaving plaats, zelfs als classificatiecriteria en SGACL's tussen beveiligingsgroepen zijn geconfigureerd. Om SGACL-handhaving te activeren, moet de VRF expliciet worden geconfigureerd in de afgedwongen modus.

Wanneer de VRF in de gedwongen modus werkt, wordt een standaardbeleidsgedrag gedefinieerd:

- Deny: Al het unicast-verkeer wordt verwijderd, tenzij expliciet toegestaan door een allow-regel.
- Toestemming: Al het unicast-verkeer is toegestaan, tenzij dit expliciet wordt geblokkeerd door een weigeringsregel.

Eindpunten die tot dezelfde beveiligingsgroep behoren, kunnen met elkaar communiceren zonder dat hiervoor SGACL-regels nodig zijn. SGACL's definiëren beveiligingsbeleid alleen tussen verschillende beveiligingsgroepen.

Cisco NX-OS Release 10.6(3)F introduceert de mogelijkheid om communicatie tussen eindpunten binnen dezelfde GPO te beperken, ook bekend als intra-GPO-isolatiefunctie. Voorafgaand aan deze release worden regels die van toepassing zijn op eindpunten binnen dezelfde beveiligingsgroep genegeerd en is verkeer standaard toegestaan.

Stap 3.3 De ID van de beveiligingsgroep configureren

NDFC wijst automatisch een willekeurige tag-ID toe uit het vooraf gedefinieerde bereik in de configuratie van de fabric. Hoewel een tag-id handmatig kan worden geselecteerd, moet deze

binnen het bereik vallen dat is gedefinieerd voor zowel het onderliggende als het bovenliggende weefsel.

In dit scenario:

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

Stap 3.4 Bevestigen

Als de optie Bijvoegen niet is ingeschakeld, wordt de beveiligingsgroep niet toegepast op de CISCO-TAC-tenant.

Stap 3.5 Selectieschermen configureren

- De selectors bepalen welke eindpunten en externe IP-adressen aan een specifieke beveiligingsgroep zijn gekoppeld.

NDFC 4.2 ondersteunt standaard drie typen selectors:

1) IP-selectors: IP-selectors koppelen eindpunten of IP-subnetten aan een beveiligingsgroep op basis van IP-informatie.

a. Connected Endpoint – Identificeert eindpunten die direct aan de fabric zijn gekoppeld, zoals virtuele machines, servers of fysieke hosts die zijn aangesloten op leaf-switches.
b. Extern subnet: koppelt externe IP-voorvoegsels aan een beveiligingsgroep. Dit type wordt gebruikt voor netwerken die buiten de VXLAN-structuur bestaan, zoals externe datacenters, WAN-segmenten of internetnetwerken. Verkeer dat afkomstig is van of bestemd is voor deze voorvoegsels, wordt geclassificeerd met de geconfigureerde beveiligingsgroep.

2) Netwerkselectors: netwerkselectors koppelen een beveiligingsgroep aan een specifiek VXLAN-netwerksegment. De classificatie wordt toegepast op basis van de netwerkidentificator (L2VNI). Alle eindpunten die tot dat netwerk behoren, erven de toegewezen beveiligingsgroep, waardoor beleidsimplementatie wordt vereenvoudigd wanneer meerdere eindpunten hetzelfde segment delen.

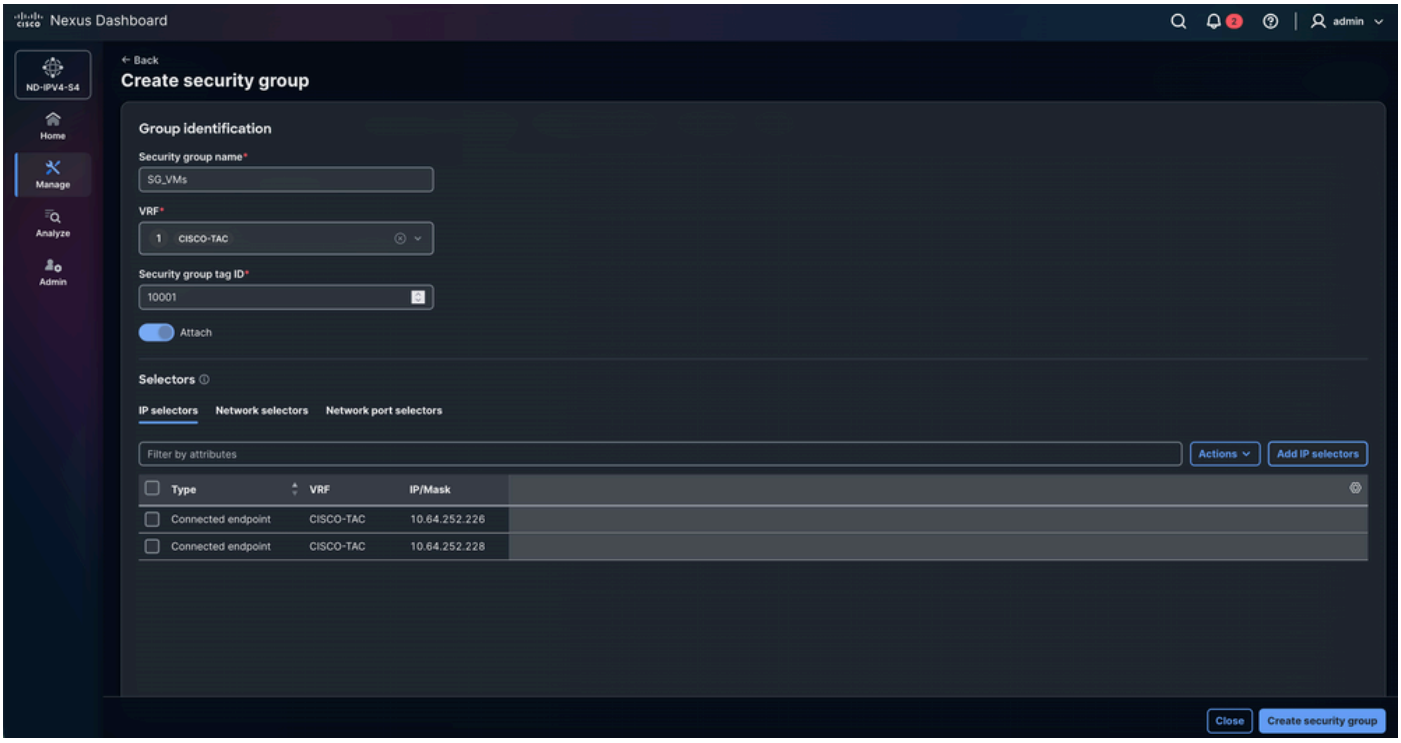
3) Netwerkpoortselectors: netwerkpoortselectors classificeren het verkeer op basis van de fysische switch-interface via welke het verkeer de verbinding binnenkomt. Een beveiligingsgroep kan worden toegewezen aan verkeer dat op een specifieke poort of interface wordt ontvangen. Deze aanpak wordt meestal gebruikt voor apparaten die zijn verbonden via externe netwerken,

serviceapparaten of infrastructuurkoppelingen waarbij de IP-classificatie van het eindpunt niet haalbaar is.

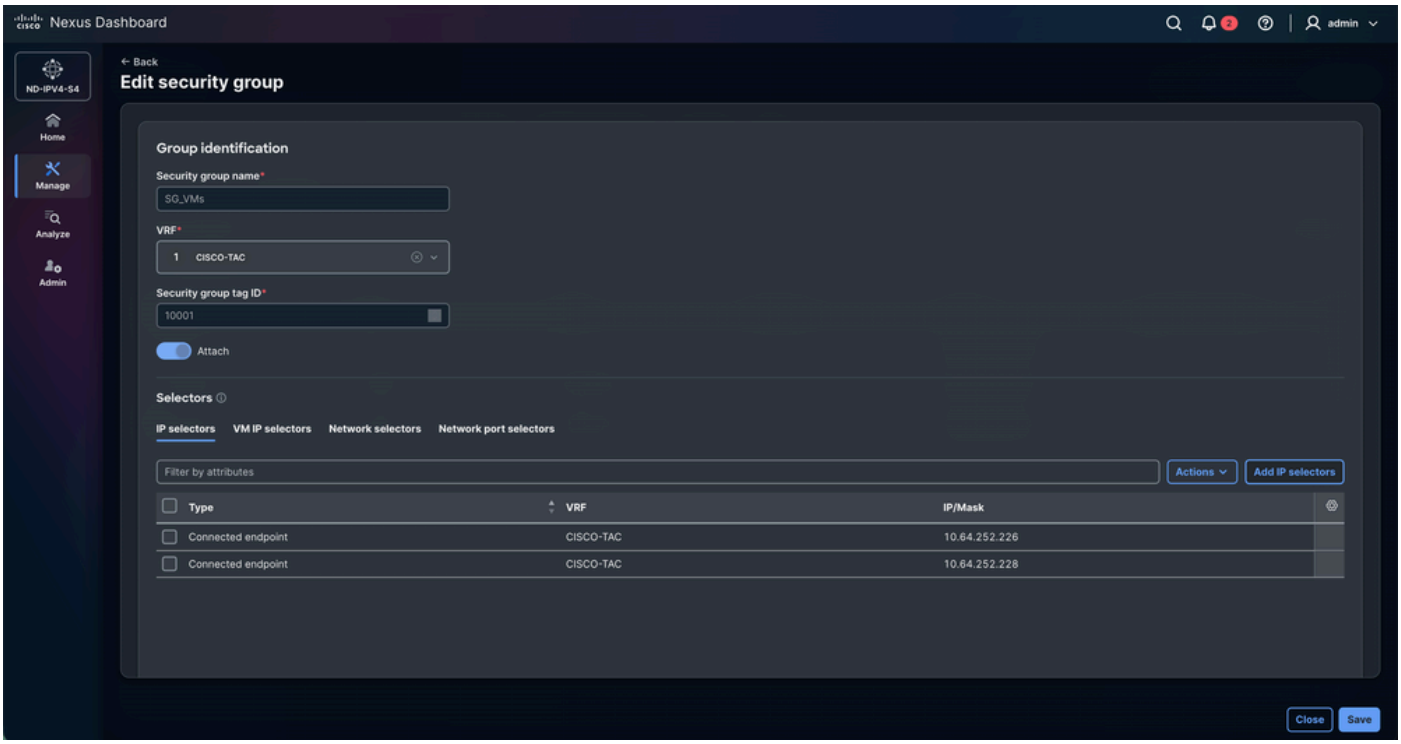
Overzicht configuratie beveiligingsgroep

Apparaat	Naam beveiligingsgroep	VRF	ID beveiligingsgroeptag	Selectors
VM-1	SG_VM's	CISCO-TAC	10001	IP-selectors
VM-2	SG_VM's	CISCO-TAC	10001	IP-selectors
FW-1	SG_FWs	CISCO-TAC	10002	IP-selectors
FW-2	SG_FWs	CISCO-TAC	10002	IP-selectors

Configuratie beveiligingsgroep voor VM's



Configuratie beveiligingsgroep voor FW's



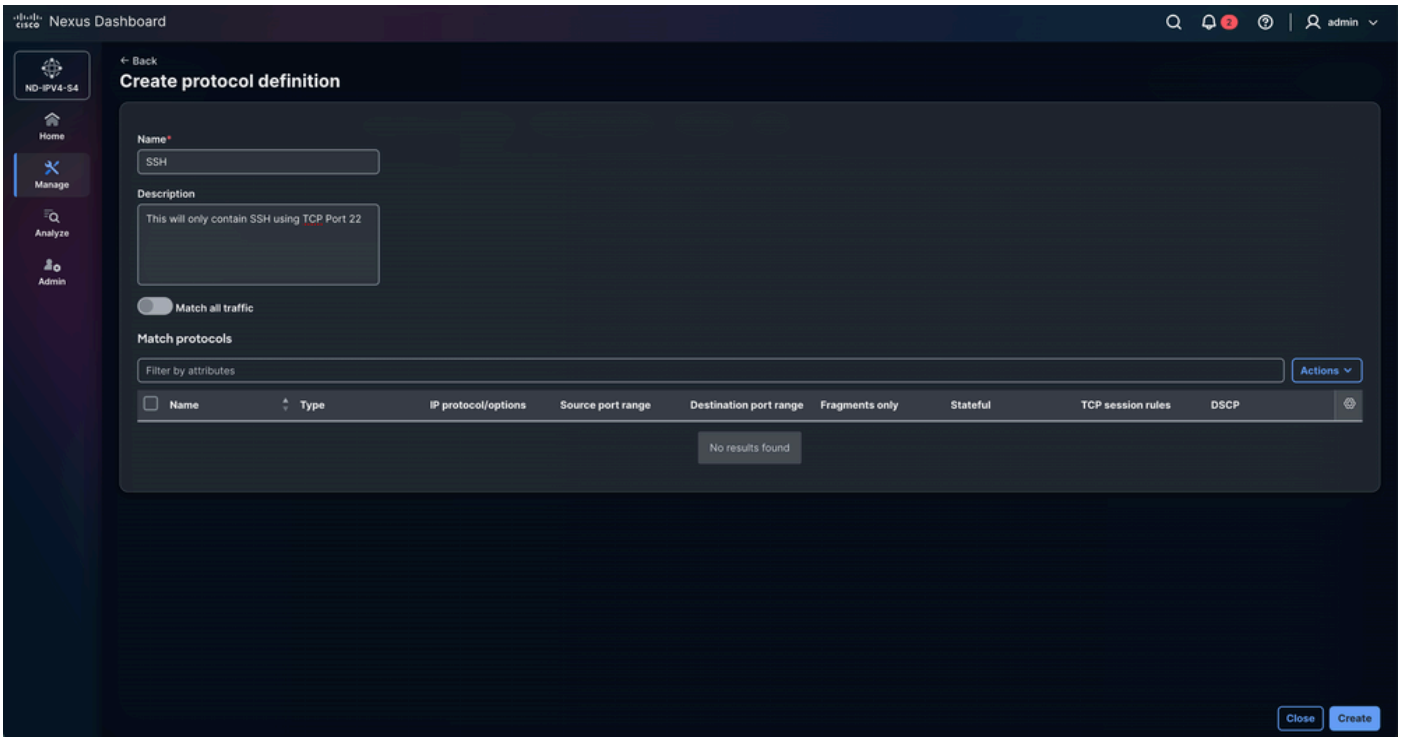
Stap 4. Protocoldefinities configureren

De optie Protocoldefinitie maken wordt gebruikt om de netwerkprotocolparameters en verkeerskenmerken te definiëren die overeenkomen met een groepsbeleidsobject (GPO). Hiermee kunnen beheerders criteria opgeven zoals protocoltype, poortnummers en andere pakketkenmerken, zodat het bijbehorende beleid kan worden toegepast op de gewenste verkeersstromen.

In dit scenario is het doel om alleen ICMP-verkeer toe te staan en expliciet TCP-verkeer op poort 22 (SSH) te blokkeren. Dit beleid zorgt ervoor dat het testen van de bereikbaarheid van het netwerk toegestaan blijft, terwijl onbevoegde of ongewenste SSH-toegang handmatig wordt beperkt.

Navigeer naar Beheer > Verbindingen > Verbindingsgroepen > DAVIDM3 > Segmentatie en beveiliging > Protocoldefinities > Acties > Protocoldefinitie maken.

Voer de naam en beschrijving in.



Navigeer naar Acties > Protocolvermelding maken.

- Naam: SSH
- Type: IPv4
    - IP en IPv6 zijn ook beschikbaar.
- IP-protocol/opties: TCP
    - Onder andere UDP, EIGRP en PIM worden ondersteund.

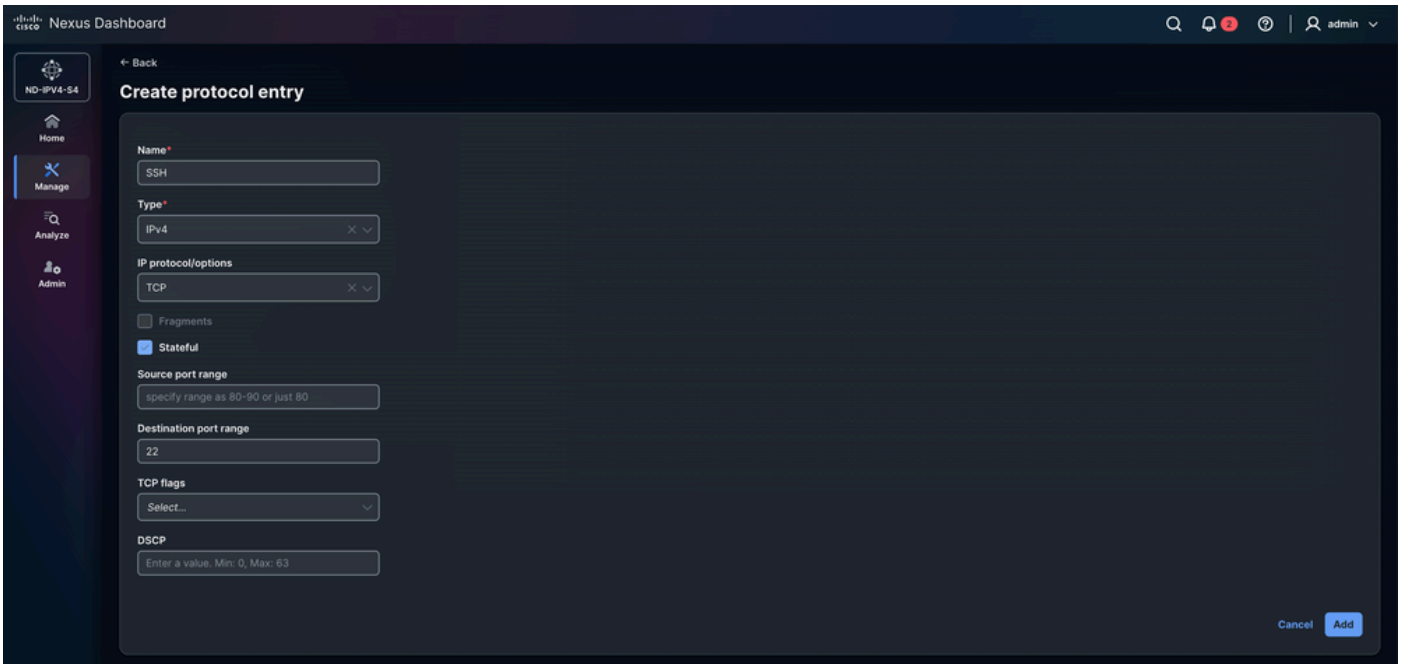
- Fragmenten: hiermee kan de regel overeenkomen met gefragmenteerde IP-pakketten. Dit is handig omdat grote pakketten kunnen worden opgesplitst in fragmenten bij overschrijding van de MTU van het netwerk. Door dit mogelijk te maken, wordt het beleid ook op die fragmenten toegepast.

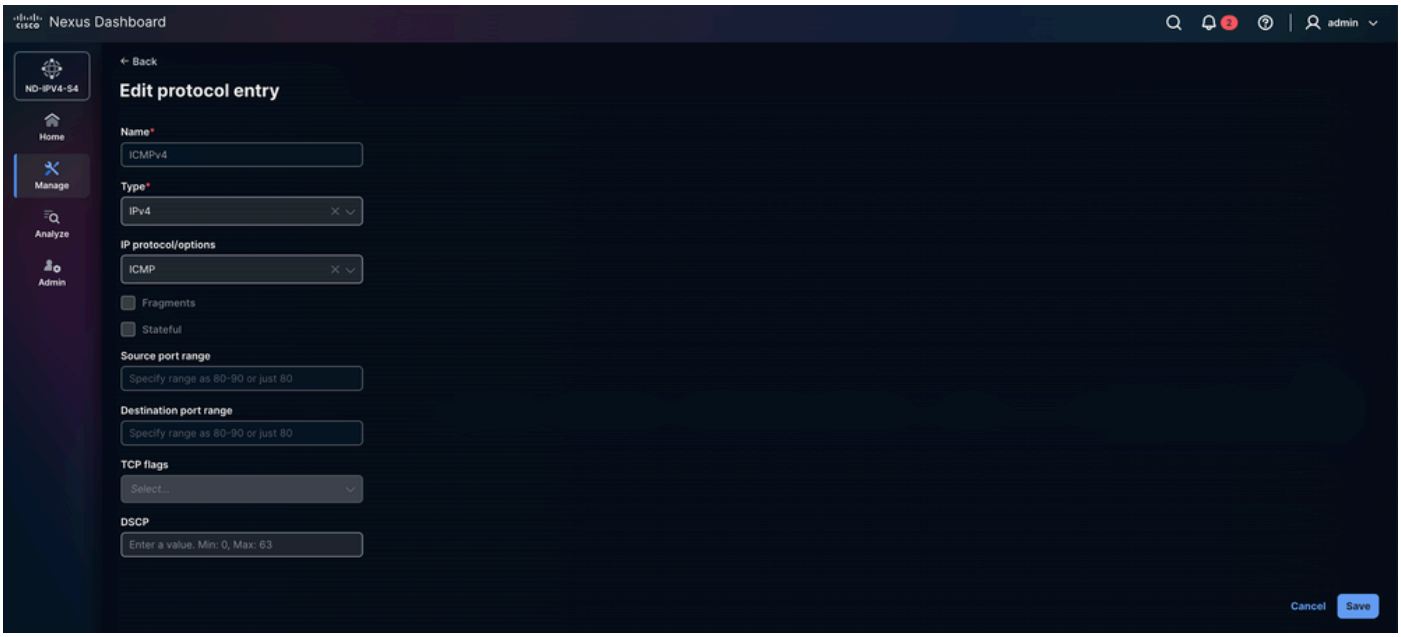
- Stateful: Een proces dat stateful is, betekent dat het alle veranderingen of interacties bijhoudt die in het verleden zijn gebeurd, en een huidig proces wordt uitgevoerd met een context van die eerdere processen. In dit geval houdt TCP gebieden bij zoals het aantal pakketten dat moet worden overgedragen, de volgorde van de pakketten en of de ontvanger een pakket heeft ontvangen of niet. Als de optie Stateful is geselecteerd, wordt deze informatie opgeslagen als een status in TCP.

- Bronpoortbereik: Deze optie is alleen beschikbaar als u TCP of UDP hebt geselecteerd in het veld IP-protocol/opties hierboven.
- Doelpoortbereik: Deze optie is alleen beschikbaar als u TCP of UDP hebt geselecteerd in het veld IP-protocol/opties.
- TCP-vlaggen

    - Deze optie is alleen beschikbaar als TCP is geselecteerd in het veld IP-protocol/opties.

- Hiermee kunt u de TCP-vlaggen definiëren die door het beveiligingsprotocol worden gebruikt.
- TCP-vlaggen maken deel uit van de TCP-header en worden gebruikt om het tot stand brengen, onderhouden en beëindigen van verbindingen te regelen.
- Beschikbare opties:
    - ACK (Bevestiging): geeft de bevestiging van ontvangen gegevens of synchronisatiepakketten aan.
    - EST (Vastgesteld): Verwijst naar reeds bestaande TCP-verbindingen. Als deze optie is ingeschakeld, kunnen geen andere TCP-vlaggen worden geselecteerd.
    - FIN (Voltooien): Wordt gebruikt om een TCP-verbinding sierlijk te sluiten.
    - RST (Reset): beëindigt onmiddellijk de verbinding en verwijdert alle gegevens die nog worden verzonden.
    - SYN (Synchronisatie): Gebruikt tijdens het initiëren en tot stand brengen van een TCP-verbinding.





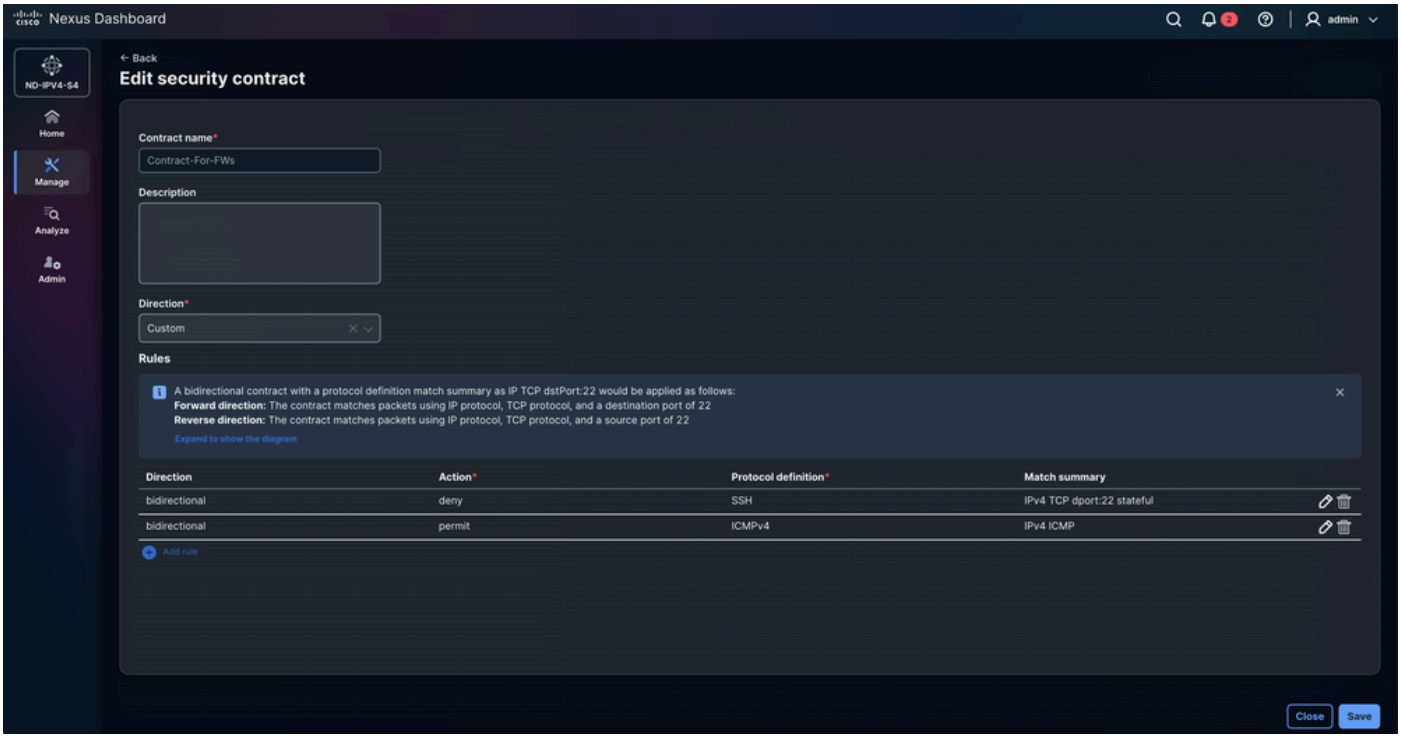
Stap 5. Beveiligingscontracten configureren

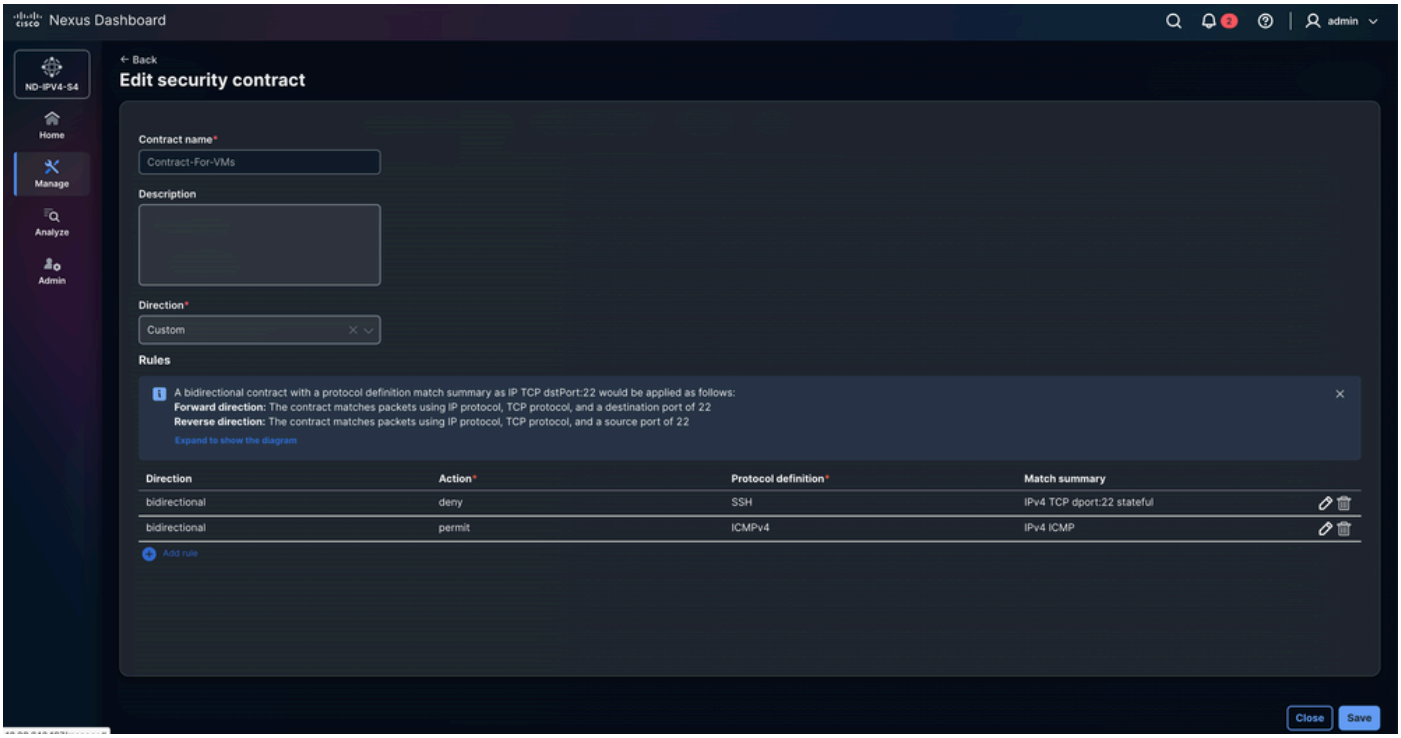
Het Contract definieert de communicatieregels tussen eindpuntgroepen door aan te geven welk verkeer is toegestaan of geweigerd op basis van de bijbehorende beleidsdefinities. Het fungeert als het handhavingsmechanisme dat de geconfigureerde protocolregels, filters en acties toepast en ervoor zorgt dat het verkeer tussen bron- en doelgroepen voldoet aan het beoogde beveiligings- en segmentatiebeleid.

Navigeer naar Beheer > Stoffen > Verbindingsgroepen > DAVIDM3 > Segmentatie en beveiliging > Beveiligingscontracten > Acties > Beveiligingscontract maken.

- Selecteer Regel toevoegen en configureer richting, actie en protocoldefinitie.
    - Bidirectioneel:
        - Het bidirectionele contract is als volgt van toepassing met een overeenkomende samenvatting van de protocoldefinitie als IP TCP-poort 22.
            - Doorsturen: Het contract komt overeen met pakketten met IP-protocol, TCP-protocol en een bestemmingspoort van 22
            - Omgekeerde richting: Het contract komt overeen met pakketten met behulp van IP-protocol, TCP-protocol en een bronpoort van 22.
            - Dit geldt ongeacht de herkomst of bestemming.
    - Unidirectioneel:
        - Unidirectioneel in een GPO-beveiligingscontract betekent dat het beleid slechts in

één richting van de verkeersstroom wordt afgedwongen, waardoor communicatie van de bronbeveiligingsgroep naar de bestemmingsbeveiligingsgroep wordt toegestaan of geweigerd zonder automatisch dezelfde regel in omgekeerde richting toe te passen.

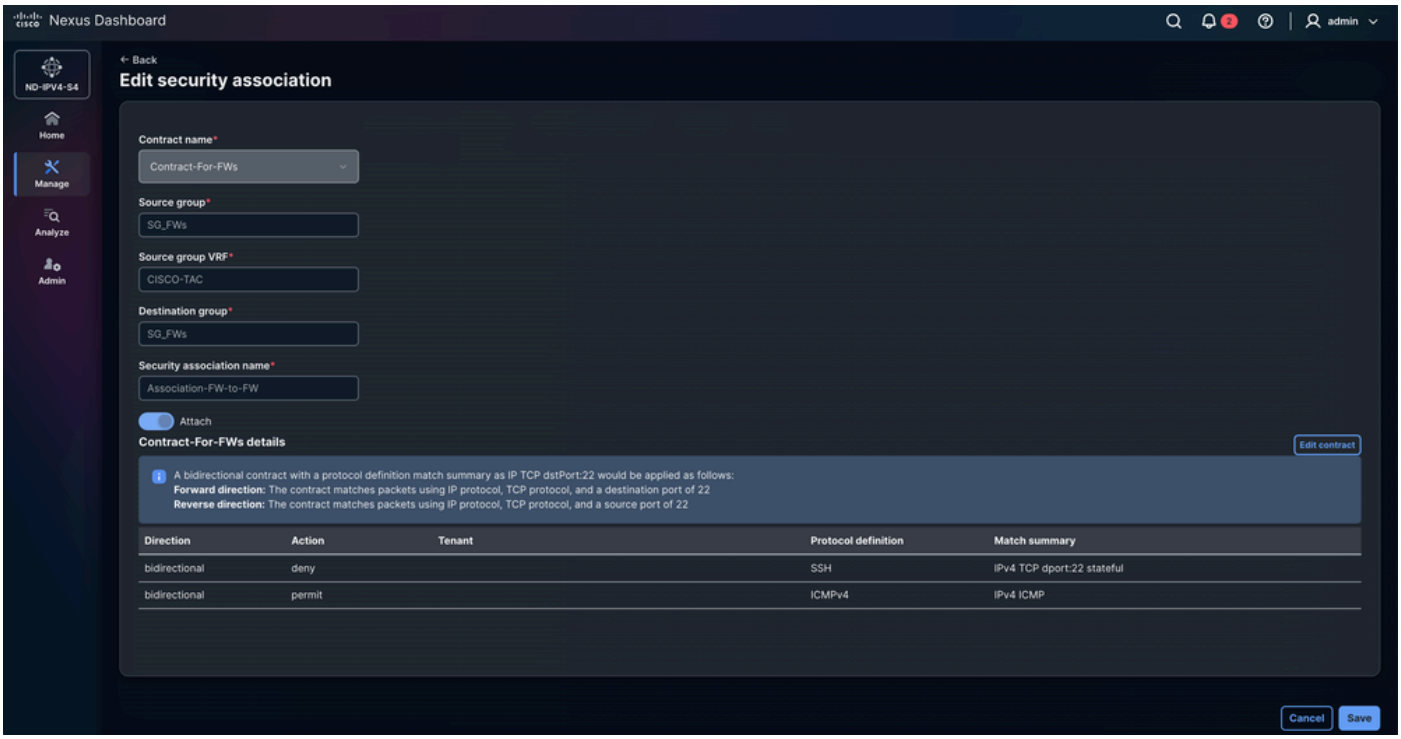


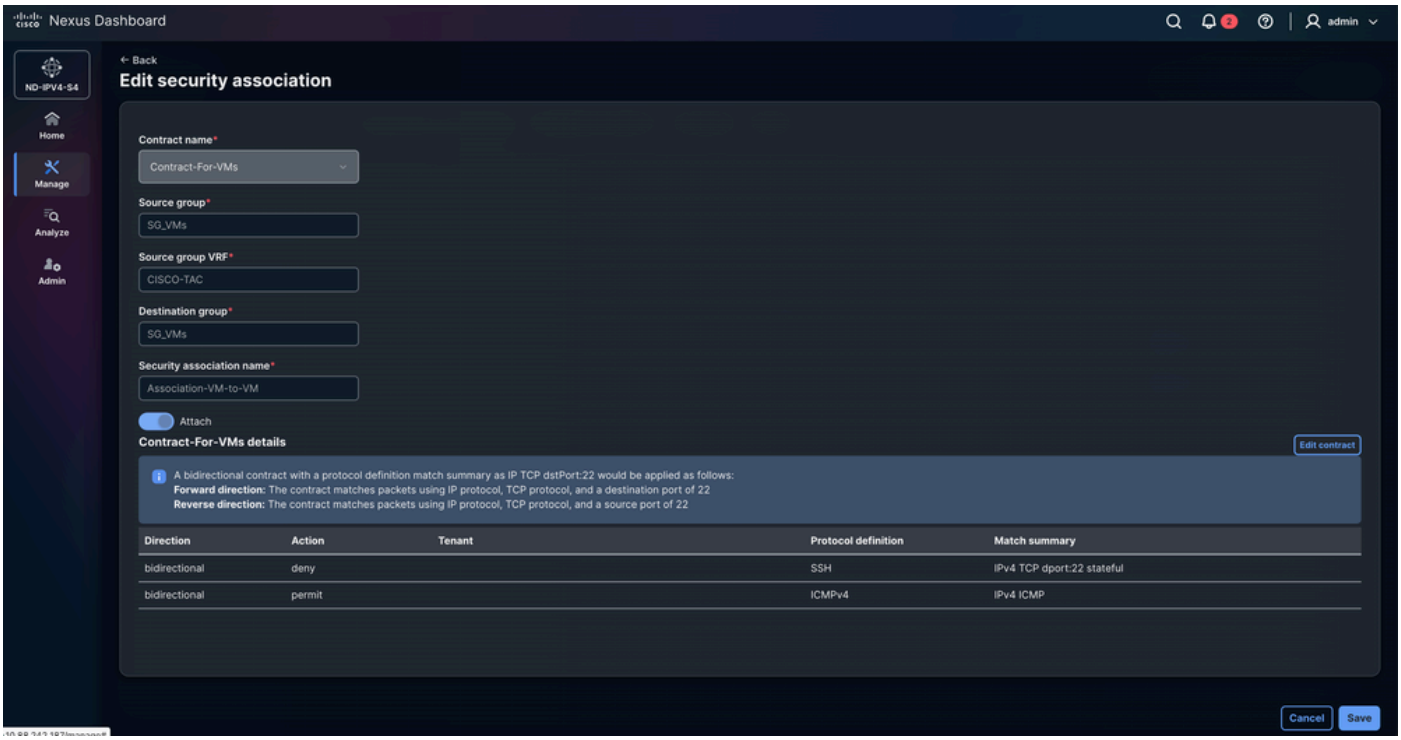


Stap 6. Beveiligingsassociaties configureren

Navigeer naar Beheer > Verbindingen > Verbindingsgroepen > DAVIDM3 > Segmentatie en beveiliging > Beveiligingsassociaties > Acties > Beveiligingsassociatie maken.

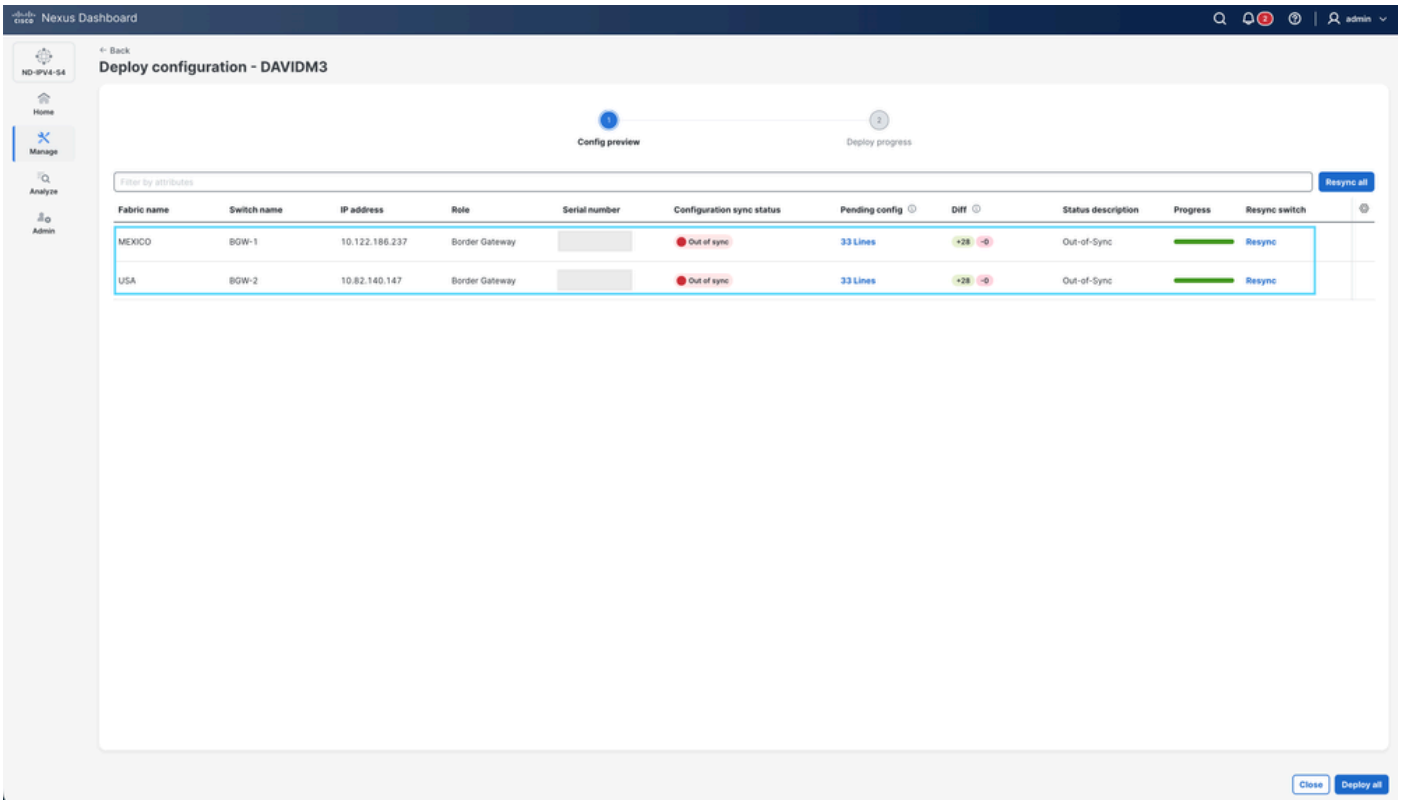
In Beveiligingsassociaties configureren wordt het beleidsmodel gedefinieerd door beveiligingsgroepen, protocoldefinities en beveiligingscontracten te koppelen. Beveiligingsgroepen classificeren eindpunten, protocoldefinities specificeren de verkeerstypen (zoals protocollen of poorten) en beveiligingscontracten definiëren het beleid dat wordt toegepast tussen bron- en bestemmingsbeveiligingsgroepen met behulp van die protocolregels. Beveiligingsassociaties vertegenwoordigen de relatie die deze elementen met elkaar verbindt, zodat de structuur het gedefinieerde beveiligingsbeleid kan afdwingen.

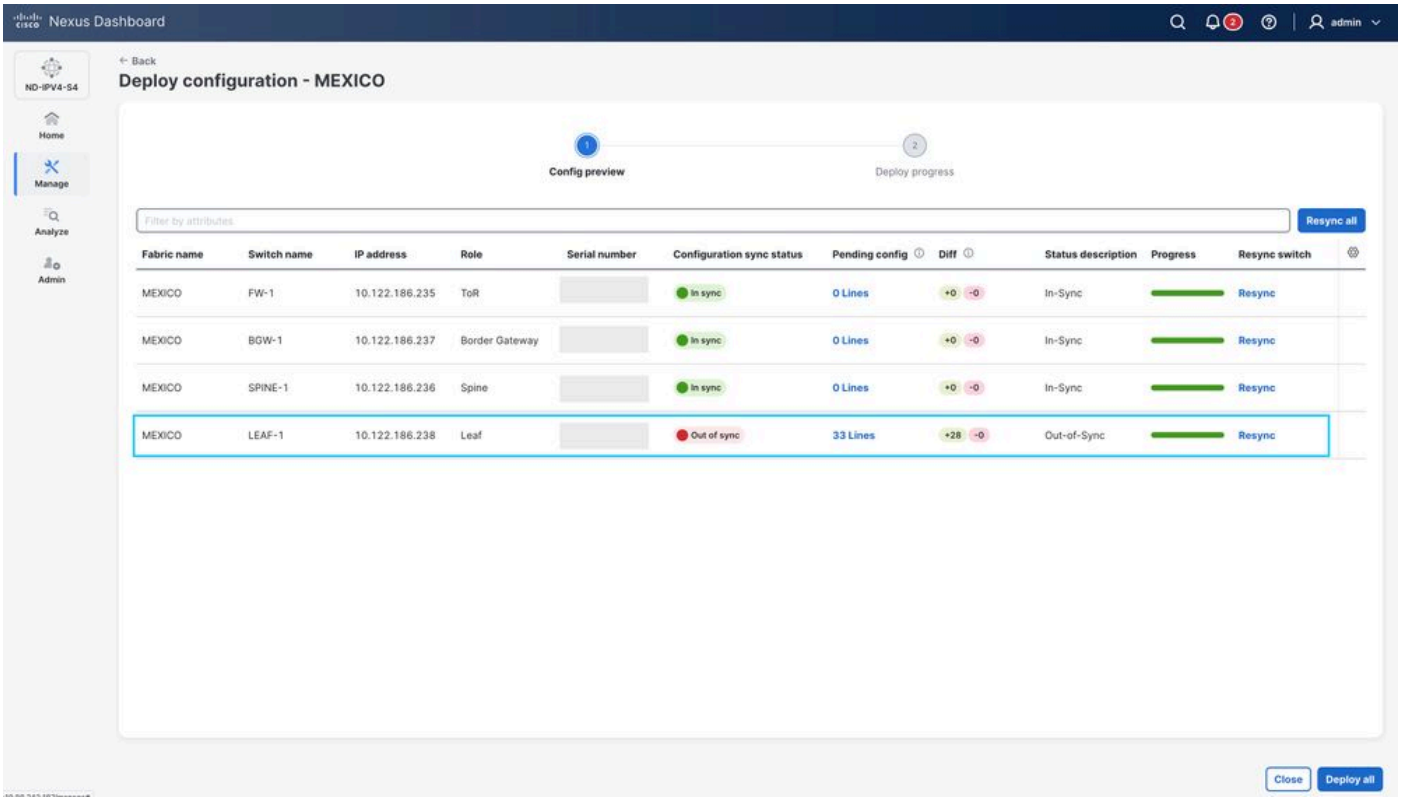


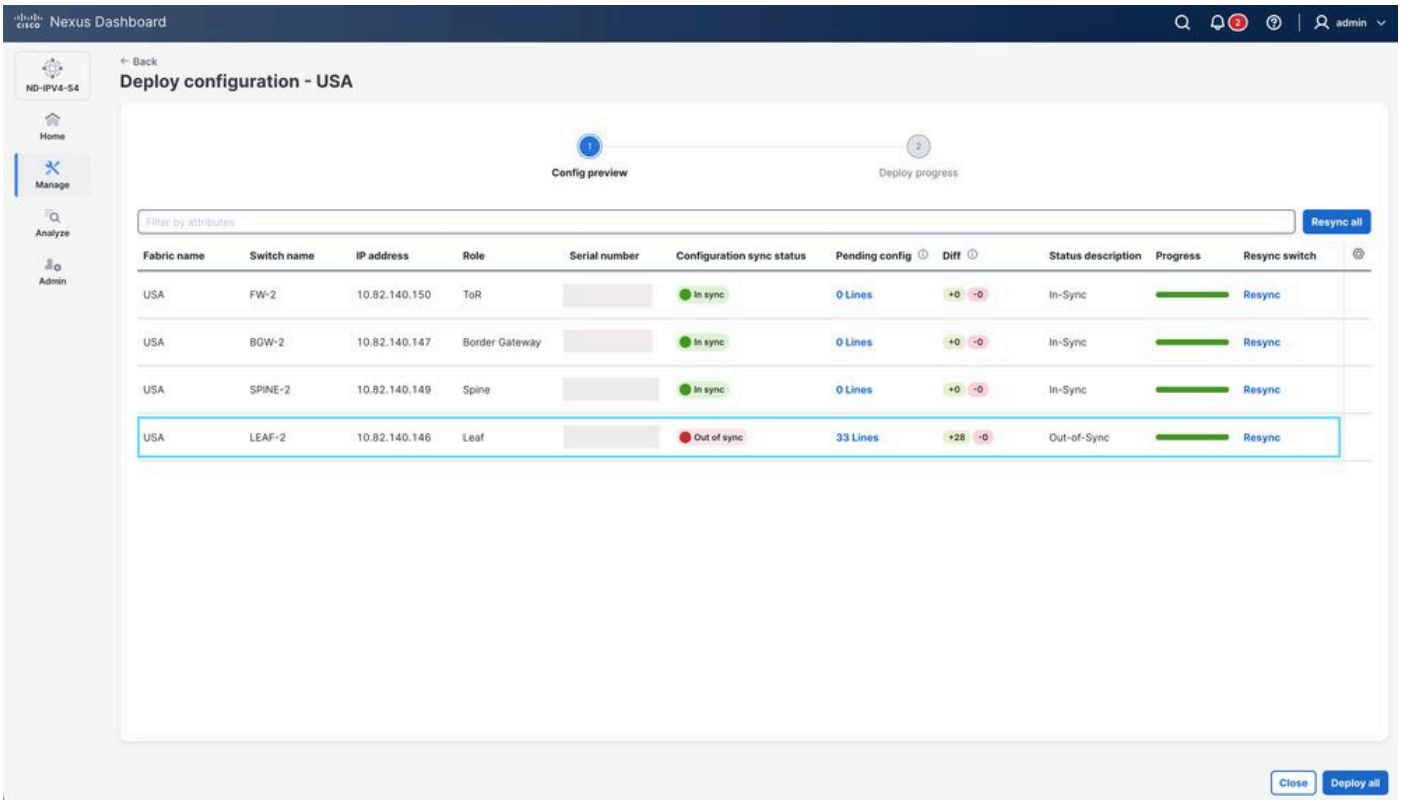


Stap 7. GPO-configuratie valideren

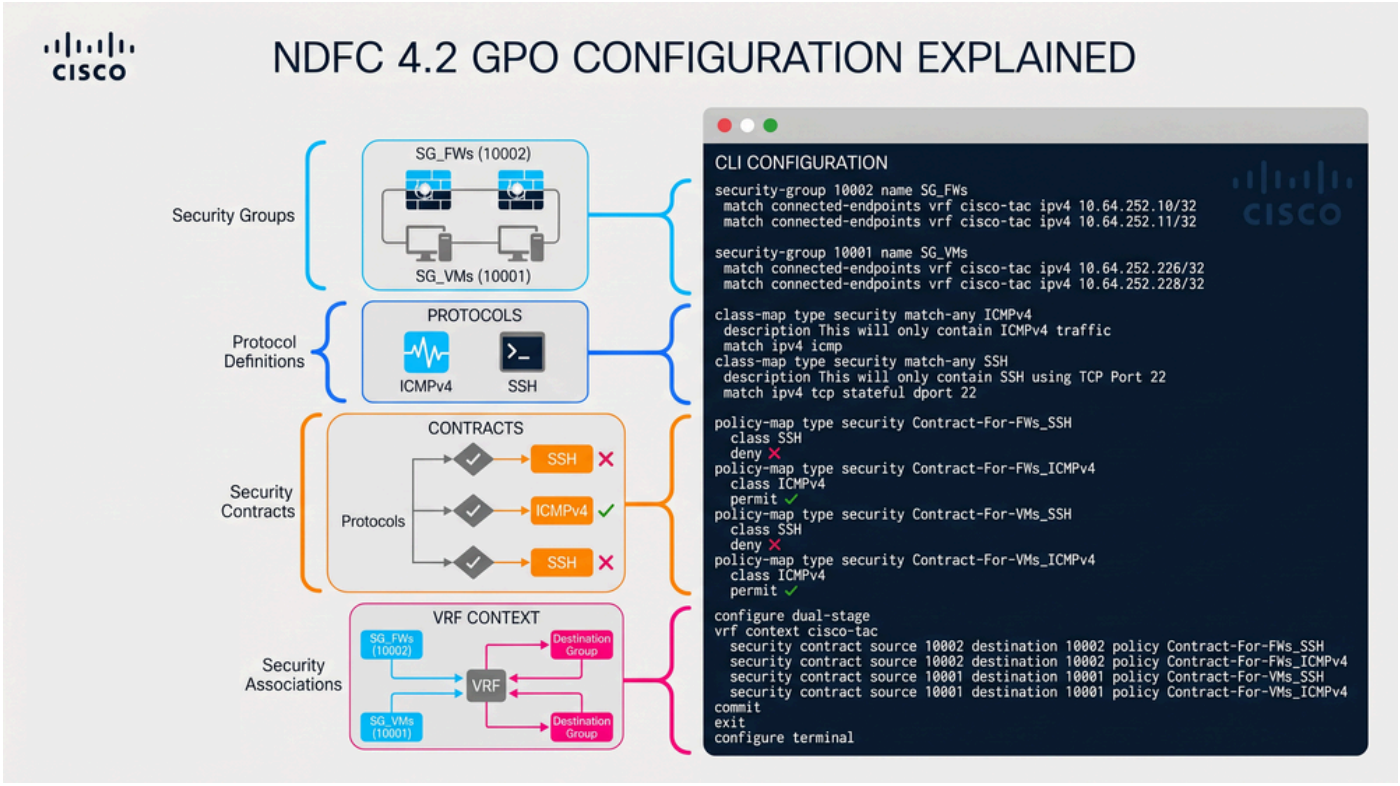
- Navigeer naar Beheer > Verbindingen > Verbindingsgroepen > DAVIDM3 > Acties > Opnieuw berekenen en implementeren.
  - De GPO-configuratie wordt vanuit de bovenliggende fabric-switch naar de Border Gateways gepusht. Klik op het aantal openstaande configuratielijnen om de configuratie te bekijken en te valideren die op de apparaten kan worden geïmplementeerd. Dit proces moet worden herhaald voor elk kind stof.
  - Navigeer naar Beheer > Verbindingen > Verbindingsgroepen > DAVIDM3 > Inventaris > Verbindingen van leden > MEXICO > Acties > Herberekenen en implementeren.
  - Navigeer naar Beheer > Verbindingen > Verbindingsgroepen > DAVIDM3 > Inventarisatie > Verbindingen voor leden > VS > Acties > Herberekenen en implementeren.


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



- De afbeelding toont de GPO-configuratie voor BGW-1, BGW-2, LEAF-1 en LEAF-2. De indeling is op alle switches gelijk. NDFC 4.2 past de configuratie niet toe in de exacte volgorde die wordt weergegeven. Dit gedeelte illustreert de logische volgorde van de CLI-opdrachten.



Problemen met VXLAN GPO-operabiliteit oplossen

Stap 1. De status van de functies van de beveiligingsgroep controleren

Controleer of de beveiligingsgroepfunctie is ingeschakeld op de switch. VXLAN GPO is afhankelijk van deze functie omdat hiermee de SGACL-infrastructuur (Security Group Tag) wordt geactiveerd die vereist is voor de classificatie van eindpunten, de handhaving van contracten en de programmering van SGACL-hardware.

<#root>

```
BGW-1#

show feature | i i security-group


security-group 1 enabled
```

Stap 2. De routeringsmodus van het systeem controleren

De geconfigureerde en operationele routeringsmodus van het systeem op de switch valideren. Voor VXLAN GPO is de routeringsmodus voor ondersteuning van beveiligingsgroepen vereist, omdat de SGACL-handhaving speciale doorstuurmiddelen voor hardware binnen de ASIC-pijplijn verbruikt.

<#root>

```
BGW-1#

show system routing mode


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

Stap 3. VXLAN NVE Peer Establishment and GPO Capability controleren

- Valideren van VXLAN NVE-peer-establishment tussen lokale fabric-apparaten en externe peers voor meerdere sites. VXLAN GPO-informatie verspreidt zich via het VXLAN EVPN-besturingsvlak en daarom zijn stabiele NVE-aansluitingen vereist voor het leren van de

Security Group Tag (SGT) en de synchronisatie van contracten in de fabric.

- Het veld Groepspolitiek geschikt is een van de belangrijkste indicatoren in deze opdracht, omdat het bevestigt of de externe VTEP ondersteunt VXLAN Group Policy extensies die nodig zijn voor SGT propagatie en SGACL contract handhaving in de VXLAN EVPN Multi-Site domein.

<#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

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

Stap 4. Beveiligingsgroepsleren en eindpuntclassificatie verifiëren

Valideren dat eindpunten correct zijn geclassificeerd in beveiligingsgroepen (SGT's). VXLAN GPO-handhaving is afhankelijk van nauwkeurige endpoint-to-SGT-mappings.

<#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
```

Stap 5. Beveiligingscontracten en beleidshandhaving controleren

Valideren dat VXLAN GPO-contracten correct zijn geïnstalleerd en operationeel zijn. Contracten definiëren de communicatieregels die worden afgedwongen tussen beveiligingsgroepen en vertegenwoordigen het belangrijkste beleidsmechanisme dat door VXLAN GPO wordt gebruikt voor micro-segmentatie.

<#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
```

Stap 6. VRF-beveiligingsstatus controleren

De VXLAN GPO-handhavingsstatus valideren voor alle VRF's die op de switch zijn geconfigureerd. Deze opdracht bevestigt of het SGACL-beleid en de contracten van de beveiligingsgroep actief worden gehandhaafd binnen de tenant VRF.

De uitvoer bevestigt dat de Cisco-tac VRF actief deelneemt aan VXLAN GPO-handhaving met de modus ingesteld op afgedwongen. De handhavingstag 13648 identificeert de interne SGACL-beleidscontext die is geprogrammeerd in hardware voor deze VRF. Het standaard actie-weigeringslogboek geeft aan dat verkeer dat niet expliciet is toegestaan via een contract van de beveiligingsgroep, wordt geweigerd en geregistreerd, waarbij een standaard micro-segmentatiebeleid wordt geïmplementeerd. De standaard, regress-loadbalance-resolution-management en beheer-VRF's werken daarentegen in niet-afgedwongen modus, wat betekent dat VXLAN GPO-beleid niet wordt toegepast binnen die VRF's en dat verkeer standaard is toegestaan.

Het veld Status volgt verkeer dat overeenkomt met het VRF-beveiligingsbeleid. De waarde 0 onder de cisco-tac VRF geeft aan dat geen ongeëvenaard verkeer het standaard weigergedrag heeft geactiveerd op het moment dat de opdracht werd uitgevoerd, terwijl de tegenwaarde 4364 onder de standaard VRF verkeersactiviteit aangeeft binnen een VRF die werkt zonder VXLAN GPO-handhaving.

<#root>

```
BGW-1#
```

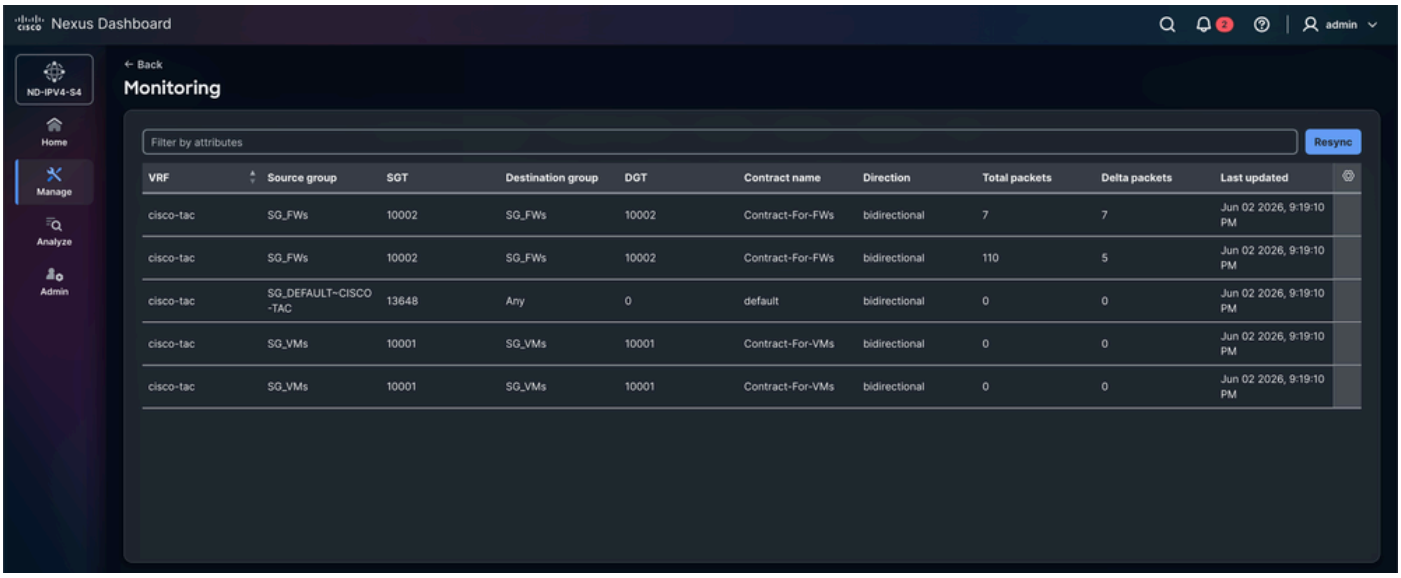
show vrf all security

```
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
```

Stap 7. VRF-beveiligingsstatus controleren

- Valideer statistieken voor het matchen van verkeer voor VXLAN GPO-contracten vanuit de NDFC GUI. Deze verificatie bevestigt of het verkeer actief overeenkomt met de geconfigureerde contracten van de beveiligingsgroep en of de SGACL-handhaving operationeel is voor de VXLAN EVPN Multi-Site Fabric.
- Navigeer in de NDFC GUI naar Beheer > Fabrics > Fabric Groups > USA / MEXICO > Segmentatie en beveiliging > Security Associations > Monitoring.
    - Deze sectie biedt inzicht in de communicatiestromen van de beveiligingsgroep, de statistieken van de hit-contracten, de machtigings- en weigeringsacties en de operationele contractactiviteit tussen eindpuntgroepen.
    - De controlestatistieken worden binnen elk afzonderlijk weergegeven.
    - Monitoringstatistieken van NDFC bieden een operationele validatielaag die een aanvulling vormt op CLI-gebaseerde probleemoplossing door real-time beleidshandhaving en gedrag voor verkeersafstemming in de fabric te bevestigen.

Opmerking: Bij de eerste poging om verkeersstatistieken in NDFC 4.2 te bekijken, kan het bewakingsgedeelte aanvankelijk leeg worden weergegeven. Druk in deze situatie op de knop Resync om de synchronisatie van contractstatistieken vanuit de VXLAN-structuur te activeren. Terwijl het synchronisatieproces wordt uitgevoerd, geeft de GUI het bericht Resync status: In progress weer. Nadat de synchronisatie is voltooid, drukt u op de knop OK om de bewakingsweergave te vernieuwen. Nadat de hersynchronisatie is voltooid, worden de verkeersstatistieken die aan elk contract van de beveiligingsgroep zijn gekoppeld, zichtbaar in het bewakingsgedeelte. Om het matchingsgedrag van het live verkeer te valideren, genereert u verkeer tussen de eindpunten en drukt u vervolgens nogmaals op de knop Resync om de contractstatistieken die in NDFC worden weergegeven bij te werken.



- In het vorige scenario is ICMPv4-verkeer tussen de eindpunten met succes toegestaan. Als er echter een SSH-sessie wordt ingesteld, wordt de verbinding vertraagd omdat het VXLAN GPO-contract expliciet TCP-verkeer weigert dat is bestemd voor poort 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
```

Gerelateerde informatie

[Cisco Nexus 9000 Series NX-OS VXLAN Configuratiegids, versie 10.6(x)]

Datacenters beveiligen met microsegmentatie met behulp van VXLAN GPO

Implementatie van microsegmentatie in Cisco NX-OS VXLAN EVPN-verbindingen met VXLAN Group Policy Option (GPO)

Micro-segmentatie automatiseren en Layer 4-7-services implementeren in VXLAN EVPN-verbindingen met behulp van Group Policy Option (GPO) en Nexus Dashboard

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.