Konfigurieren des Gruppenrichtlinienobjekts auf einer Nexus-Multi-Site-Fabric mit NDFC 4.2

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration und Validierung von Gruppenrichtlinienobjekten in

VXLAN Multi-Site-Fabrics auf Nexus Cloud Scale-Switches mit NX-OS und NDFC 4.2 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Virtual Extensible Local Area Network (VXLAN), Ethernet Virtual Private Network (EVPN) und Fabric-Technologien für mehrere Standorte
- Cisco Nexus Cloud Scale-Switches und NeXus-Betriebssystem (NX-OS)
- Nexus Fabric Network Controller (NDFC) 4.2 Management- und Bereitstellungs-Workflows
- Konzepte für Netzwerksegmentierung und Sicherheitsrichtlinien

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Analyse der GPO-Funktionalität in VXLAN-EVPN-Fabrics

Die Gruppenrichtlinienoption (Group Policy Option, GPO) ist ein richtlinienbasierter Segmentierungsmechanismus, der die Kommunikation zwischen Endpunkten auf der Grundlage logischer Identität steuert, anstatt sich nur auf IP-Adressen, VLANs oder Subnetze zu verlassen. Der Hauptzweck von GPO besteht in der Vereinfachung der Durchsetzung von Sicherheitsrichtlinien und der Bereitstellung einer skalierbaren Mikrosegmentierung zwischen Anwendungen, Servern oder Workloads.

Eine einfache Analogie ist ein Hotel, in dem jeder Gast zu einer bestimmten Kategorie oder Zugriffsebene gehört, bestimmte Bereiche nur für bestimmte Gäste zugänglich sind und die Zugriffsberechtigungen von der Rolle des Gastes statt der Zimmernummer abhängen. GPO funktioniert sehr ähnlich. Endpunkte werden nicht mehr nur als IP-Adressen behandelt, sondern vom GPO in Sicherheitsgruppen (Security Groups, SGs) klassifiziert. Anschließend werden Richtlinien zwischen diesen Gruppen angewendet, um zu bestimmen, welche Kommunikation zugelassen oder verweigert wird.

Beispiele:

- Webserver können einer Sicherheitsgruppe angehören.
- Anwendungsserver können einer anderen Sicherheitsgruppe angehören.
- Datenbankserver können einer eingeschränkten Sicherheitsgruppe angehören.

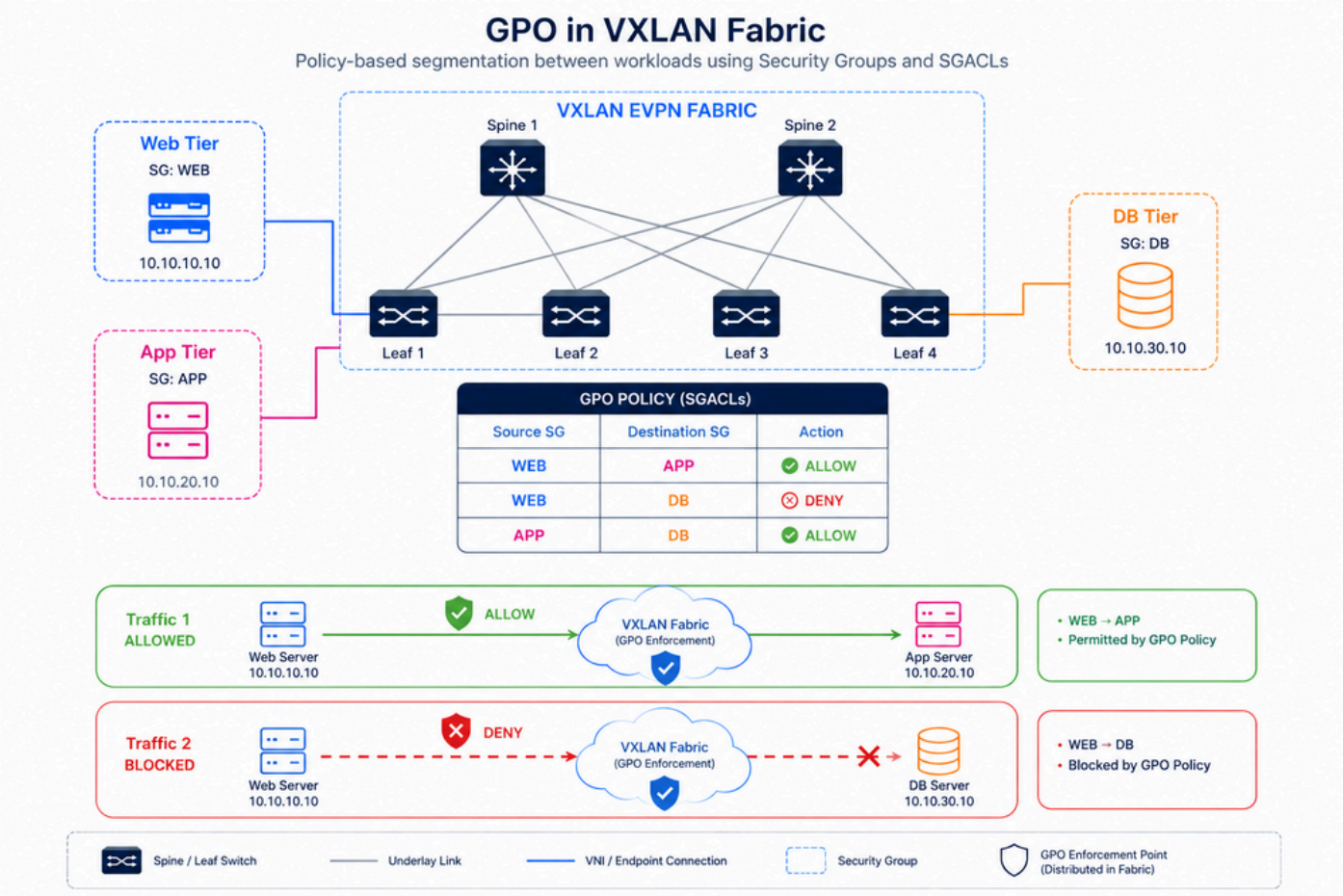
Richtlinien können dann Folgendes definieren:

- Webserver können mit Anwendungsservern kommunizieren.
- Anwendungsserver können mit Datenbankservern kommunizieren.
- Webserver können nicht direkt mit Datenbankservern kommunizieren.

Dieser Ansatz vereinfacht den Betrieb, da Administratoren nicht mehr eine große Anzahl von ACLs über mehrere Geräte und VLANs verwalten müssen.

Ein weiterer wichtiger Vorteil ist die Skalierbarkeit. In großen Umgebungen werden Workloads häufig verschoben, dynamisch skaliert oder die IP-Adressen geändert. Mithilfe von GPOs können Sicherheitsrichtlinien selbst dann konsistent bleiben, wenn sich der Endpunktstandort ändert. Innerhalb von VXLAN EVPN-Fabrics erweitert GPO dieses Konzept, indem Sicherheitsgruppeninformationen über die Fabric verteilt werden und Sicherheitsgruppen-ACLs (SGACLs) zwischen Endpunkten durchgesetzt werden. Dies ist besonders in modernen Rechenzentren wichtig, da der Ost-West-Datenverkehr zwischen den Workloads oft die größte Angriffsfläche darstellt. GPO verbessert den Sicherheitsstatus, indem unnötige Kommunikationspfade innerhalb der Rechenzentrums-Fabric eingeschränkt werden.

Weitere technische Informationen zur GPO-Architektur, zu Mikrosegmentierungskonzepten und zur Durchsetzung von VXLAN-Richtlinien finden Sie im Cisco Whitepaper unter: Sicherung von Rechenzentren mit Mikrosegmentierung mithilfe von VXLAN GPO.



GPO in VxLAN-Fabric

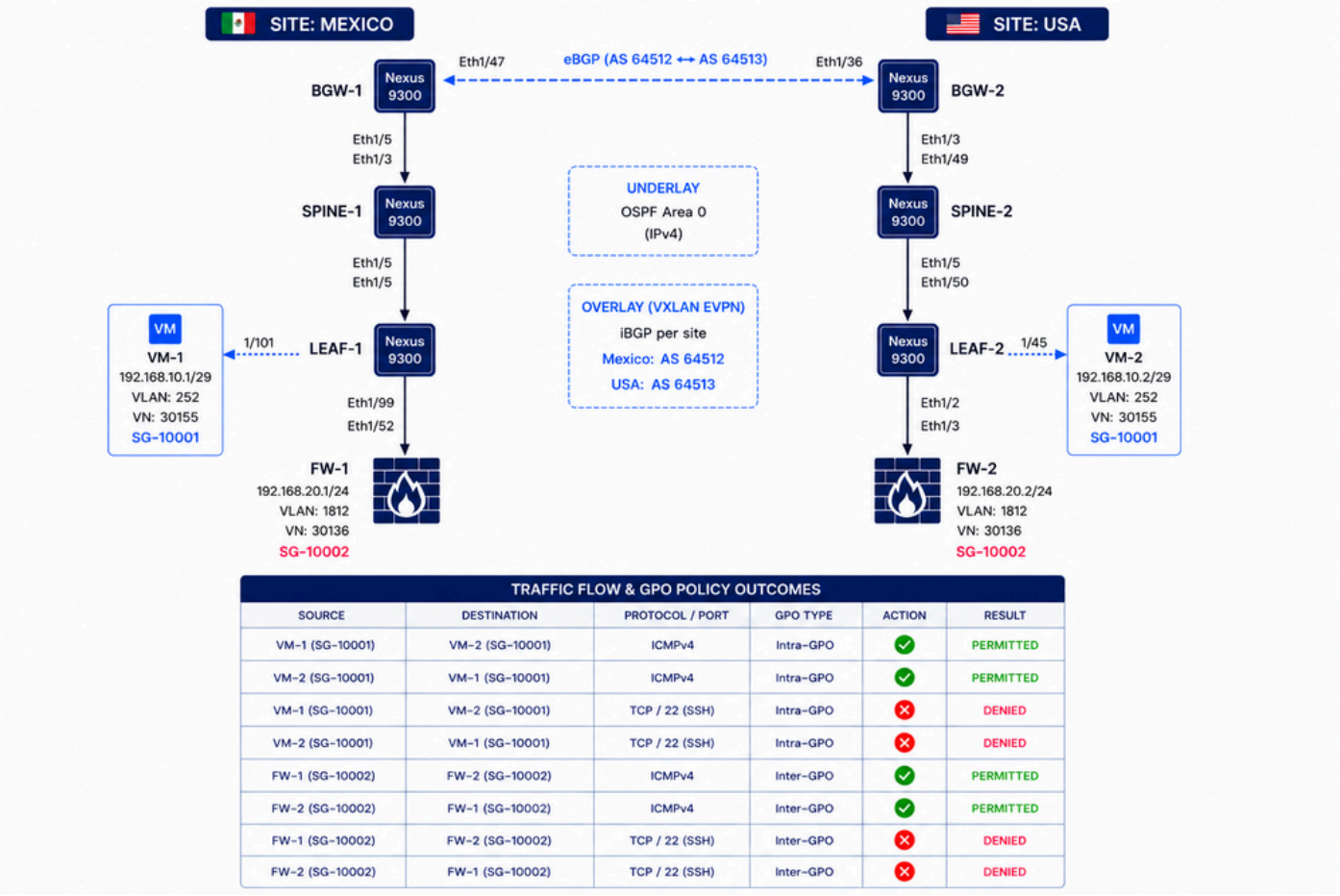
VXLAN-Szenario für die GPO-Bereitstellung an mehreren Standorten mit NDFC 4.2 und NX-OS 10.6(3)F

Diese Topologie stellt eine VXLAN-Fabric mit mehreren Standorten dar, die an zwei geografisch verteilten Standorten bereitgestellt wird: Mexiko und USA. Jeder Standort enthält dedizierte BGWs, Spine-Switches, Leaf-Switches, virtuelle Systeme und Firewall-Segmente, die auf Cisco Nexus 9300-Switches mit NX-OS 10.6(3)F ausgeführt werden. Das Underlay-Netzwerk verwendet Open Shortest Path First (OSPF), während die Overlay-Kontrollebene iBGP an jedem Standort und eBGP zwischen BGW-1 und BGW-2 für die standortübergreifende VXLAN-EVPN-Kommunikation verwendet. Da es sich bei dieser Umgebung um eine Laborumgebung handelt, sind die Standorte in Mexiko und den USA über eine direkt verbundene Verbindung zwischen den beiden BGWs miteinander verbunden, um das Modell der standortübergreifenden Vernetzung zu vereinfachen.

GPO wird verwendet, um eine richtlinienbasierte Mikrosegmentierung zwischen

Sicherheitsgruppen unabhängig von der IP-Adressierung oder VLAN-Grenzen durchzusetzen. Basierend auf der Verbindungsrichtlinientabelle wird ICMP-Datenverkehr von VM-1 zu VM-2, FW-1 und FW-2 zugelassen, während TCP-Port 22 (SSH)-Datenverkehr von VM-1 zu FW-1 und FW-2 abgelehnt wird. Die TCP-Port 22-Kommunikation zwischen VM-1 und VM-2 bleibt zulässig, da beide Endpunkte derselben Sicherheitsgruppe angehören (SG-10001). Dieses Verhalten zeigt, wie GPO dynamisch unterschiedliche Datenverkehrsrichtlinien zwischen Intra-GPO- und Inter-GPO-Kommunikation über die VXLAN Multi-Site-Fabric durchsetzt.

Anmerkung: Mit der Cisco NX-OS-Version 10.6(3)F können Sie die Kommunikation zwischen Endgeräten innerhalb derselben ESG (auch als SG bezeichnet) mithilfe der Intra-ESG-Isolationsfunktion einschränken. Diese Funktion minimiert das Risiko nicht autorisierter Zugriffe innerhalb von ESG und verbessert den Sicherheitsstatus.



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

Konfigurieren des GPO Schritt für Schritt mit NDFC 4.2 in VXLAN-EVPN-Fabrics

Diese Schritte gelten, wenn die VXLAN Multi-Site-Fabric bereits betriebsbereit und mit NDFC 4.2

konfiguriert ist und GPO anschließend implementiert werden muss. Der Abschnitt "Automatisierung mit dem Nexus Dashboard in Sichern von Rechenzentren mit Mikrosegmentierung mithilfe von VXLAN-GPO" zeigt die Konfiguration, die bei der Erstellung einer VXLAN Single-Site-Fabric beginnt.

Vorsicht: Wenn das GPO in einer VXLAN-EVPN-Fabric ausgeführt wird, erfolgt die Kommunikation nur, wenn die Zielerreichbarkeit gegeben ist und die Sicherheitsrichtlinie den Datenverkehr zulässt. Die Richtliniendurchsetzung basiert auf IP-Informationen, die ARP-Einträge und SVIs für interne Netzwerke erfordern. Das bedeutet, dass für das VLAN, das zur Tenant-VRF-Instanz gehört, eine SVI konfiguriert sein muss. Daher gilt die Durchsetzung nicht für Datenverkehr, der nur Layer-2-Header enthält und daher nicht mit der VXLAN-Layer-2-Erweiterung verwendet werden kann. Mit NX-OS Version 10.6(2)F wird die MAC-basierte Mikrosegmentierung unterstützt.

Schritt 1: Aktivieren von Sicherheitsgruppen in der übergeordneten Fabric

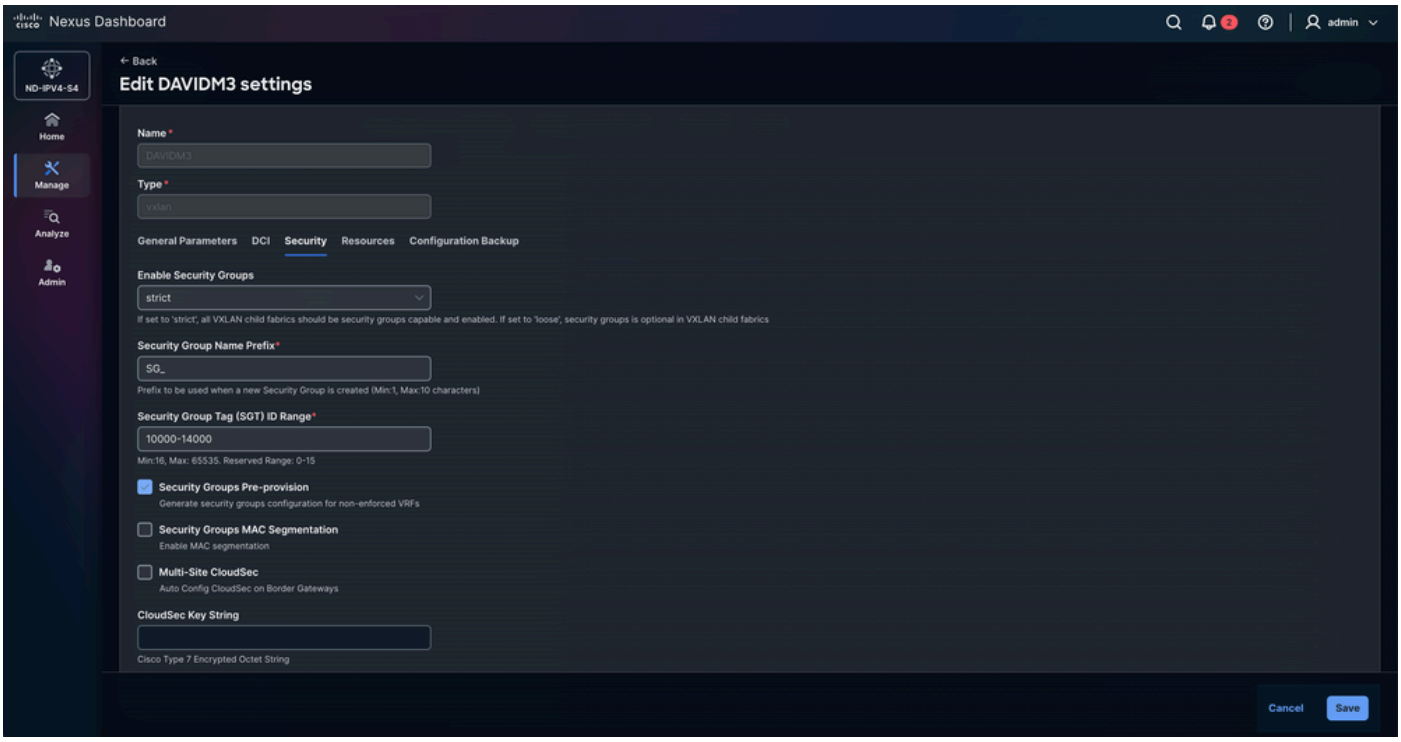
- Navigieren Sie zu Verwalten > Fabric-Gruppen, wählen Sie die Fabric-Gruppe DAVIDM3 aus, und wählen Sie dann Aktionen > Fabric-Gruppeneinstellungen bearbeiten aus. Aktivieren Sie im Abschnitt Sicherheit die Option Sicherheitsgruppen, legen Sie den Modus auf Strict (Strict) fest, und legen Sie Security Groups Pre-provisionfest fest.
  - Wählen Sie die gewünschte Fabric-Gruppe aus. In diesem Beispiel wird die ausgewählte Fabric-Gruppe DAVIDM3 genannt. Dies ist auch der Name der Multi-Site-Fabric.
- Wiederholen Sie diese Schritte für jede untergeordnete Fabric.
  - Navigieren Sie zu Verwalten > Fabric, wählen Sie USA aus, und navigieren Sie dann zu Aktionen > Fabric-Gruppeneinstellungen bearbeiten. Aktivieren Sie im Abschnitt Sicherheit die Option Sicherheitsgruppen, und legen Sie den Modus auf Strikte fest.
  - Navigieren Sie zu Verwalten > Fabric, wählen Sie MEXICO aus, und navigieren Sie dann zu Aktionen > Fabric-Gruppeneinstellungen bearbeiten. Aktivieren Sie im Abschnitt Sicherheit die Option Sicherheitsgruppen, und legen Sie den Modus auf Strikte fest.

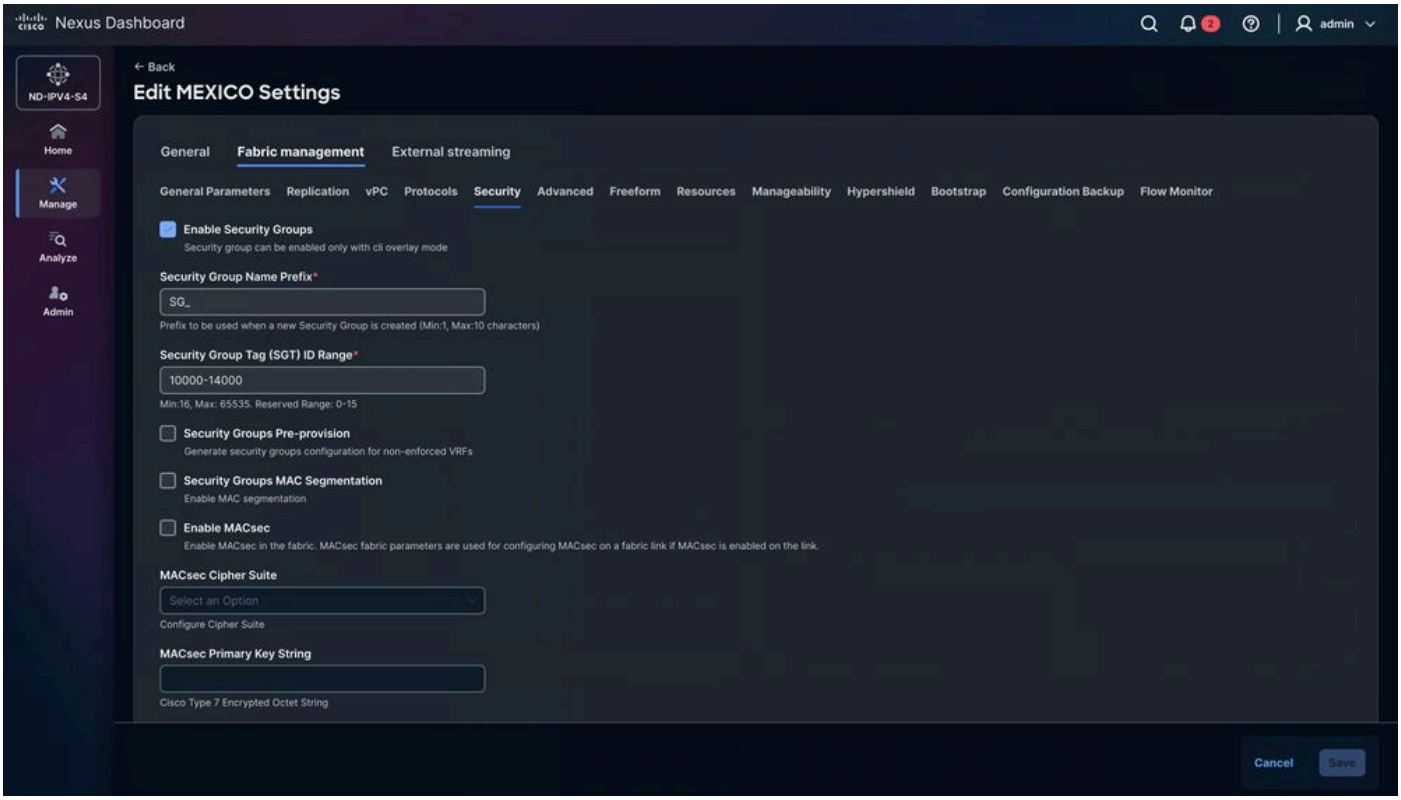
Anmerkung: Bei der Festlegung auf strict müssen alle untergeordneten VXLAN-Fabrics sicherheitsgruppenfähig und aktiviert sein. Wenn diese Option auf "Loose" gesetzt ist, sind Sicherheitsgruppen in untergeordneten VXLAN-Fabrics optional.

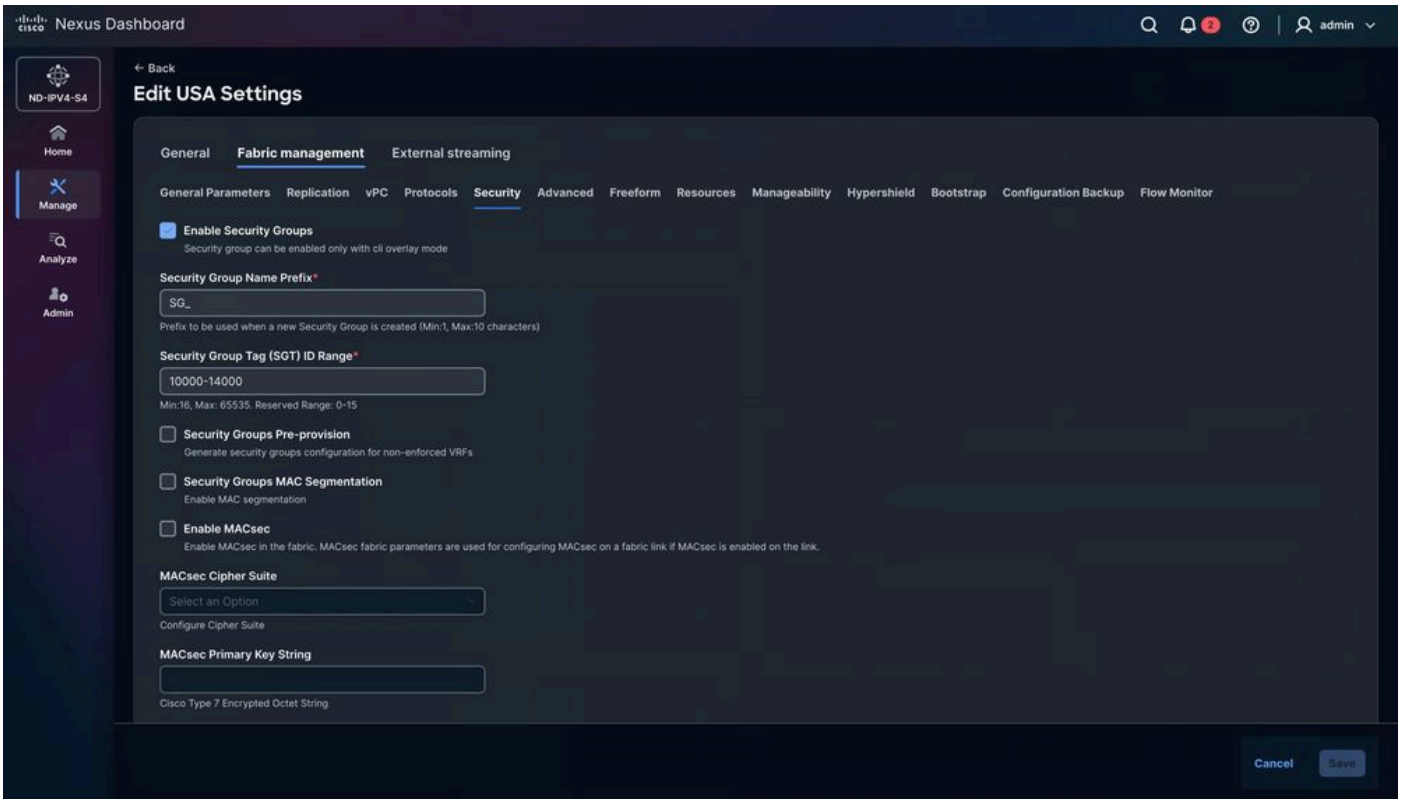
Tipp: Um eine klare Transparenz zu gewährleisten, verwenden Sie dieselben SGT-ID-Bereiche (Security Group Tag) in der übergeordneten Fabric und in allen untergeordneten

---

Fabrics. Der übergeordnete Fabric-Bereich muss die von allen untergeordneten Fabrics verwendeten Bereiche abdecken.







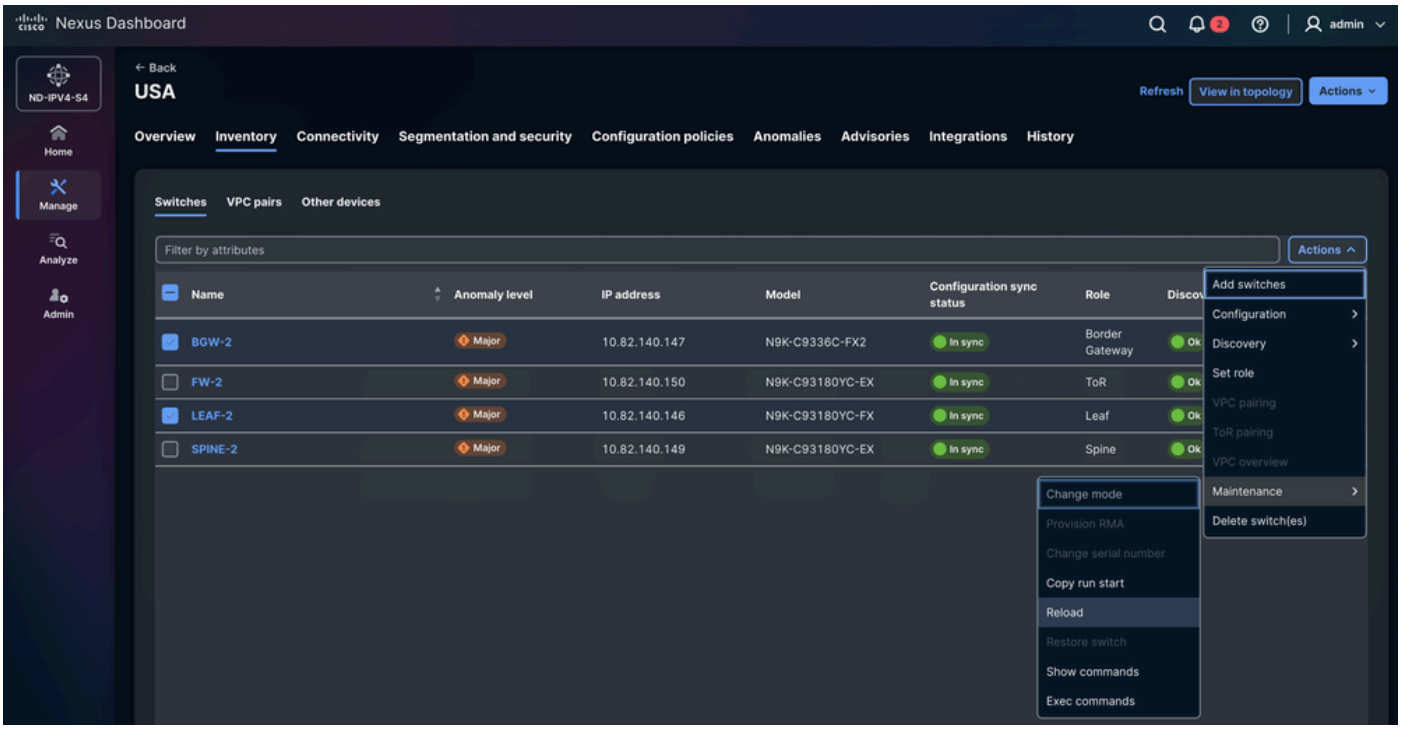
Schritt 2: Neuberechnung der Fabric-Konfiguration und Neuladen von Switches für die GPO-Bereitstellung

NDFC fordert Sie automatisch auf, eine bestimmte Gruppe von Nexus-Switches aufgrund ihrer Rolle neu zu laden. In diesem Beispiel müssen LEAF-1, LEAF-2, BGW-1 und BGW-2 neu geladen werden. Diese Aktion muss manuell vom Netzwerkadministrator ausgeführt werden. Das erneute Laden ist erforderlich und kann nicht übersprungen werden, da für das GPO eine TCAM-Partitionierung erforderlich ist.

Anmerkung: Wenn das Gerät nicht neu geladen wird, kann die TCAM-Änderung in der aktuellen Konfiguration angezeigt werden. Da der Switch jedoch nicht neu gestartet wurde, wird die Einstellung nicht auf den Hardwarespeicher angewendet. Daher kann die Funktion nicht wie erwartet funktionieren.

So laden Sie die Nexus Switches neu:

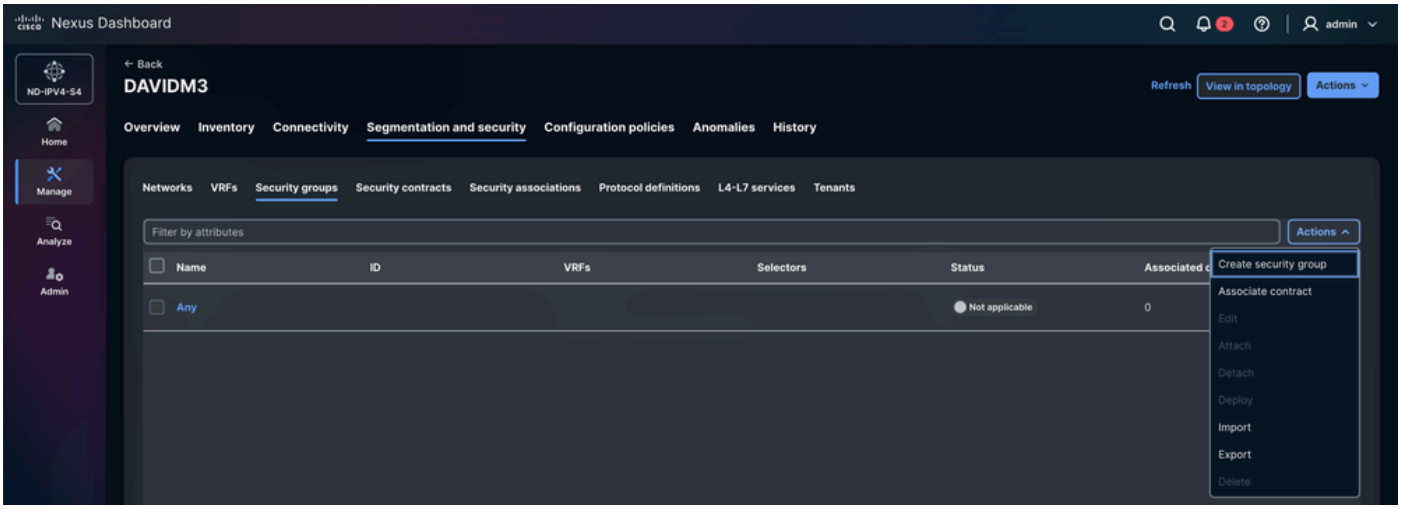
Navigieren Sie zu Manage > Fabrics > MEXICO/USA > Inventory > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions > Maintenance > Reload.



Schritt 3: Sicherheitsgruppe erstellen

Definieren Sie die Sicherheitsgruppen für die einzelnen Endpunkte. Jeder Endpunkt in den VXLAN-Fabrics kann über eine einzige Sicherheitsgruppe verfügen. Dieser Ansatz ist nicht effizient skalierbar. Gruppieren Sie Endpunkte global (z. B. virtuelle Systeme, Firewalls, TCP-Optimierer).

Navigieren Sie zu Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security Groups > Actions > Create security group.



Schritt 3.1 Konfigurieren des Sicherheitsgruppennamen

- NDFC weist automatisch einen zufälligen Namen zu. Der Name kann geändert werden. Es wird empfohlen, einen repräsentativen Namen zu verwenden, der für Endpunkte leicht zu identifizieren ist.
- In diesem Szenario gilt:
    - VMs -> SG_VMs
    - FWs -> SG_FWs

Schritt 3.2 Konfigurieren von VRF

- Wählen Sie den Tenant (VRF) aus, zu dem die Endgeräte gehören.
- In diesem Szenario gilt: Die VMs und Firewalls gehören zum CISCO-TAC-Tenant.

Optional: Erstellen Sie VRF.

Standardmäßig ist für eine neu erstellte Tenant-VRF-Instanz der Modus zur Richtliniendurchsetzung auf Nicht durchgesetzt festgelegt. In diesem Zustand erfolgt keine Richtliniendurchsetzung, selbst wenn Klassifizierungskriterien und SGACLs zwischen Sicherheitsgruppen konfiguriert sind. Um die SGACL-Durchsetzung zu aktivieren, muss die VRF-Instanz explizit im erzwungenen Modus konfiguriert werden.

Wenn die VRF-Instanz im erzwungenen Modus arbeitet, wird ein standardmäßiges Richtlinienverhalten definiert:

- Ablehnen: Der gesamte Unicast-Datenverkehr wird verworfen, es sei denn, dies wird durch eine Zulassungsregel explizit zugelassen.
- Zulassen: Sämtlicher Unicast-Datenverkehr ist zulässig, sofern er nicht explizit durch eine Deny-Regel blockiert wird.

Endpunkte, die derselben Sicherheitsgruppe angehören, können miteinander kommunizieren, ohne dass SGACL-Regeln erforderlich sind. SGACLs definieren Sicherheitsrichtlinien nur zwischen verschiedenen Sicherheitsgruppen.

Die Cisco NX-OS-Version 10.6(3)F bietet die Möglichkeit, die Kommunikation zwischen Endpunkten innerhalb desselben Gruppenrichtlinienobjekts einzuschränken. Dies wird auch als Intra-Gruppenrichtlinienobjekt-Isolationsfunktion bezeichnet. Vor dieser Version werden Regeln, die auf Endpunkte innerhalb derselben Sicherheitsgruppe angewendet werden, ignoriert, und der Datenverkehr ist standardmäßig zulässig.

Schritt 3.3 Sicherheitsgruppen-Tag-ID konfigurieren

NDFC weist automatisch eine zufällige Tag-ID aus dem vordefinierten Bereich in der Fabric-Konfiguration zu. Obwohl eine Tag-ID manuell ausgewählt werden kann, muss sie in den Bereich fallen, der sowohl für die untergeordnete als auch für die übergeordnete Fabric definiert ist.

In diesem Szenario gilt:

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

Schritt 3.4 Anhängen

Wenn die Option "Attach" (Hinzufügen) nicht aktiviert ist, wird die Sicherheitsgruppe nicht auf den CISCO-TAC-Tenant angewendet.

Schritt 3.5 Konfigurieren von Auswahlen

- Die Selektoren bestimmen, welche Endpunkte und externen IP-Adressen einer bestimmten Security Group zugeordnet sind.

NDFC 4.2 unterstützt nativ drei Auswahltypen:

1) IP-Selektoren: IP-Selektoren verknüpfen Endpunkte oder IP-Subnetze mit einer Sicherheitsgruppe, basierend auf IP-Informationen.

a. Verbundene Endpunkte - Identifiziert direkt mit der Fabric verbundene Endpunkte, z. B. virtuelle Systeme, Server oder physische Hosts, die mit Leaf-Switches verbunden sind.
b. Externes Subnetz - Ordnet externe IP-Präfixe einer Sicherheitsgruppe zu. Dieser Typ wird für Netzwerke außerhalb der VXLAN-Fabric verwendet, z. B. externe Rechenzentren, WAN-Segmente oder Netzwerke mit Internetanbindung. Datenverkehr, der von diesen Präfixen stammt oder für diese bestimmt ist, wird mit der konfigurierten Sicherheitsgruppe klassifiziert.

2) Network Selectors (Netzwerkauswahl): Netzwerkselektoren ordnen einem bestimmten VXLAN-Netzwerksegment eine Sicherheitsgruppe zu. Die Klassifizierung erfolgt anhand der Netzwerkkennung (L2VNI). Alle Endgeräte, die zu diesem Netzwerk gehören, übernehmen die zugewiesene Sicherheitsgruppe, was die Bereitstellung von Richtlinien vereinfacht, wenn mehrere Endgeräte dasselbe Segment nutzen.

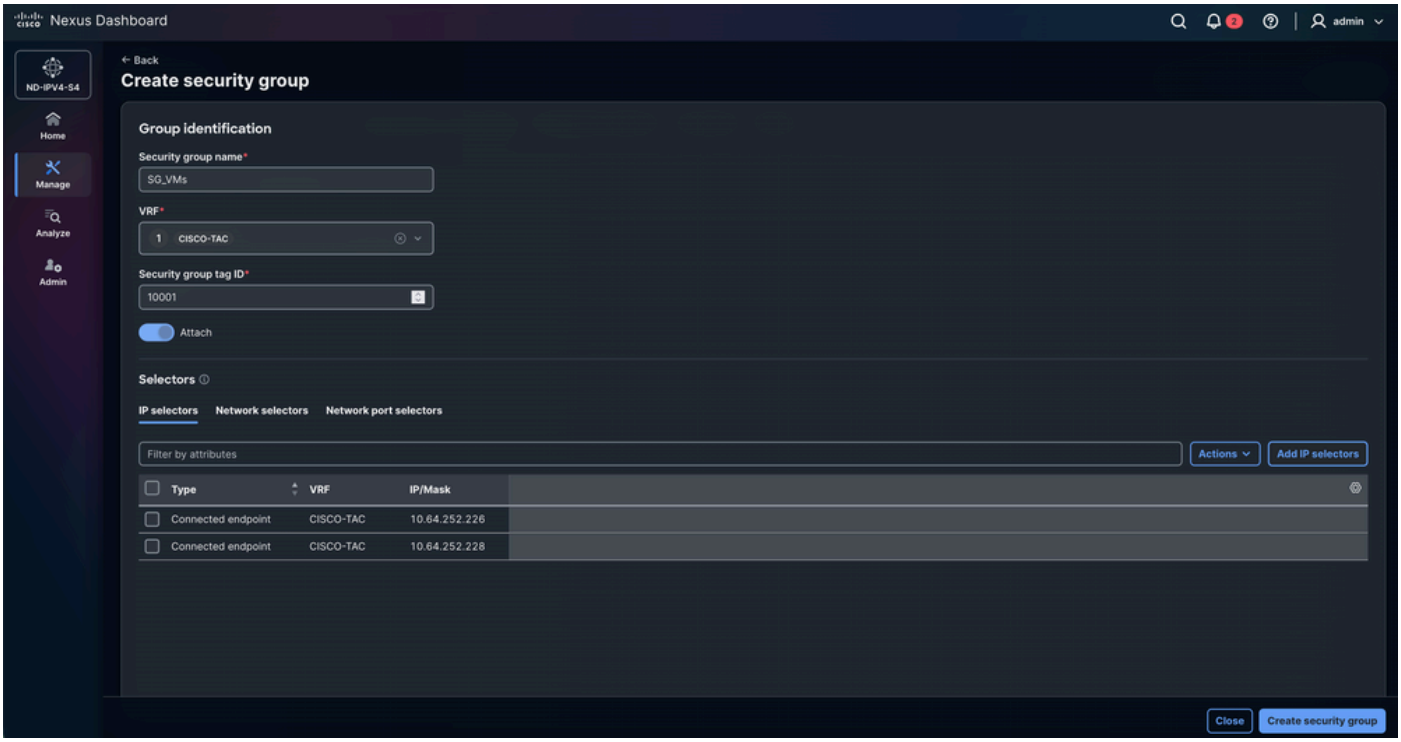
3) Network Port Selectors: Network Port Selectors klassifizieren den Datenverkehr basierend auf der physischen Switch-Schnittstelle, über die der Datenverkehr in die Fabric eingeht. Eine

Sicherheitsgruppe kann dem Datenverkehr zugewiesen werden, der über einen bestimmten Port oder eine Schnittstelle empfangen wird. Dieser Ansatz wird in der Regel für Geräte verwendet, die über externe Netzwerke, Service-Appliances oder Infrastrukturverbindungen verbunden sind, wenn eine IP-Klassifizierung der Endgeräte nicht möglich ist.

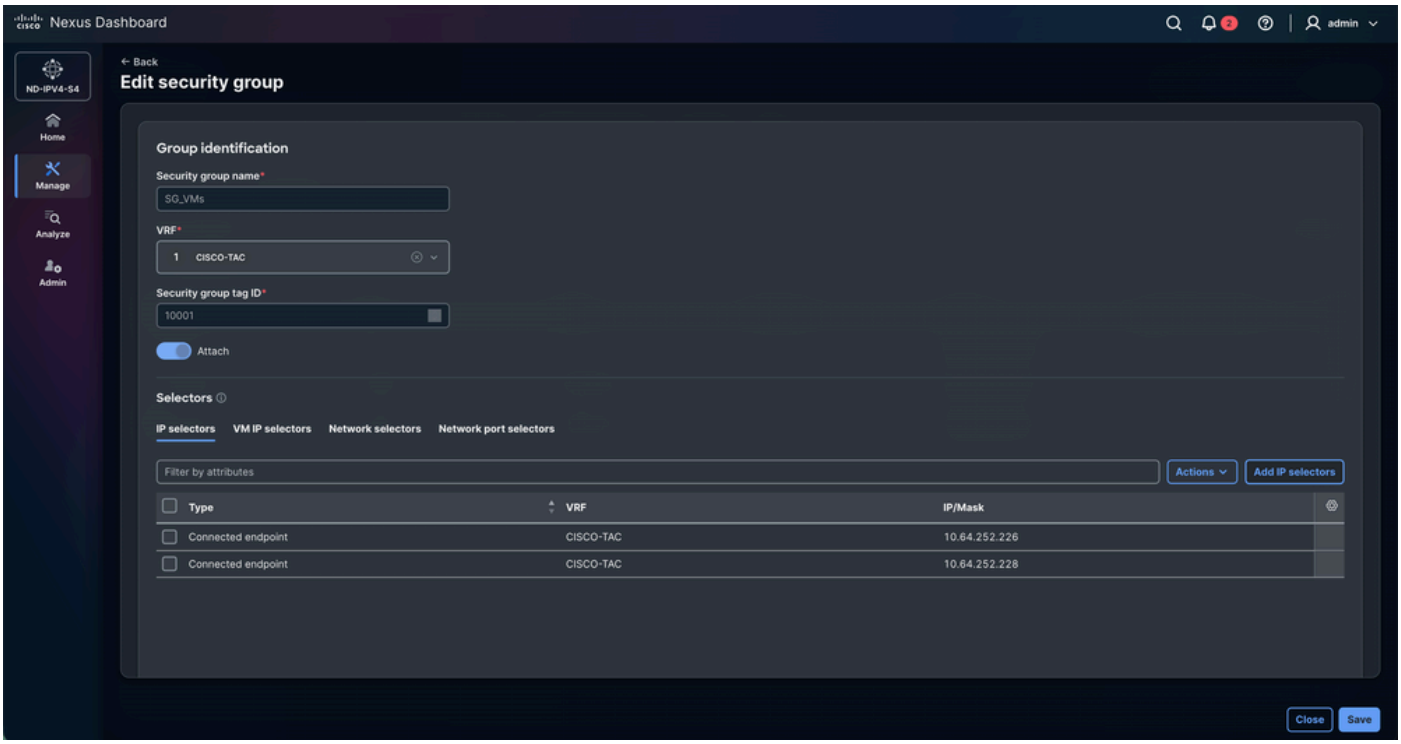
Zusammenfassung der Konfiguration der Sicherheitsgruppe

"Slot0:"	Name der Sicherheitsgruppe	VRF	Security Group Tag-ID	Selektoren
VM-1	SG_VMs	CISCO TAC	10001	IP-Selektoren
VM-2	SG_VMs	CISCO TAC	10001	IP-Selektoren
FW-1	SG_FWs	CISCO TAC	10002	IP-Selektoren
FW-2	SG_FWs	CISCO TAC	10002	IP-Selektoren

Security Group Configuration für VMs



Sicherheitsgruppenkonfiguration für FWs



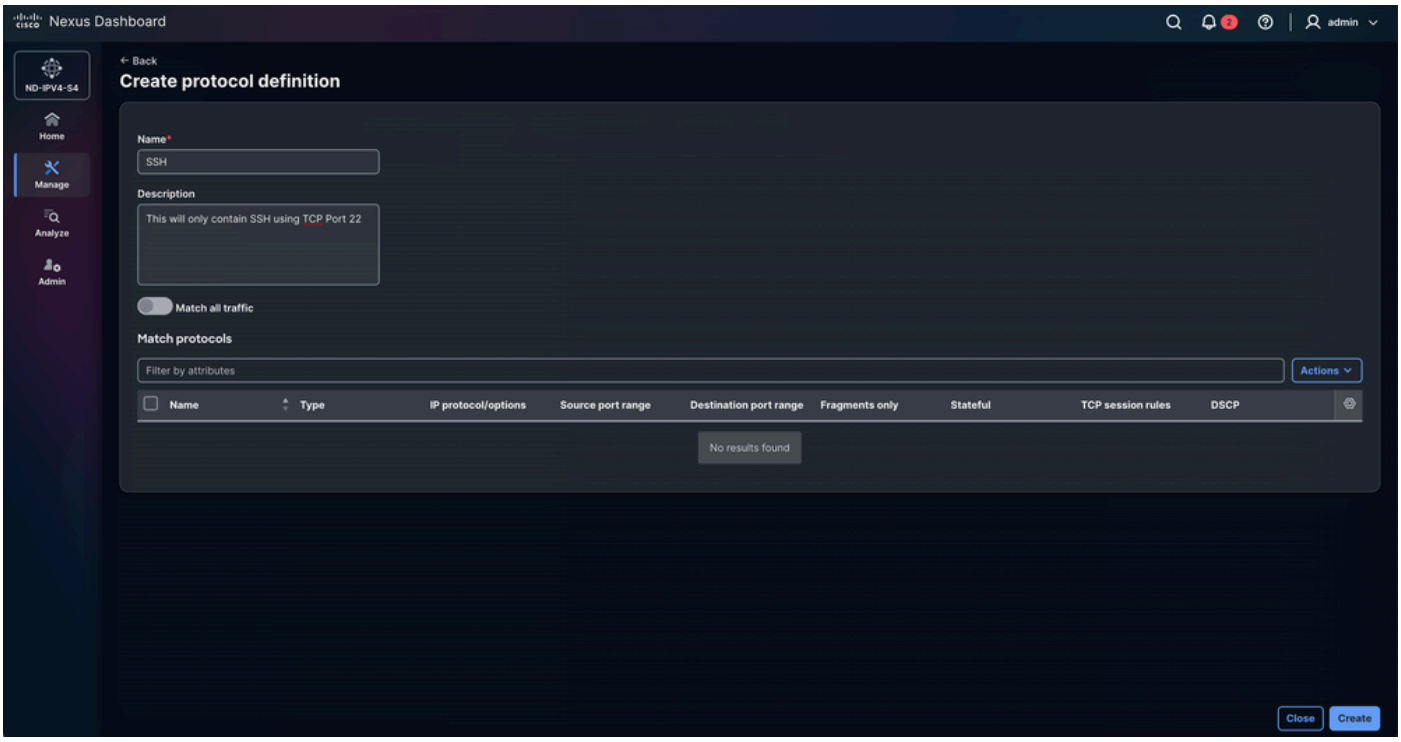
Schritt 4: Konfigurieren von Protokolldefinitionen

Mit der Option Create Protocol Definition (Protokolldefinition erstellen) werden die Netzwerkprotokollparameter und Datenverkehrseigenschaften definiert, denen ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) entspricht. Administratoren können Kriterien wie Protokolltyp, Portnummern und andere Paketattribute festlegen, sodass die entsprechende Richtlinie auf den gewünschten Datenverkehr angewendet werden kann.

In diesem Szenario soll nur ICMP-Datenverkehr zugelassen werden, während TCP-Datenverkehr auf Port 22 (SSH) explizit blockiert wird. Diese Richtlinie stellt sicher, dass Netzwerkerreichbarkeitstests zugelassen bleiben, während der nicht autorisierte oder unerwünschte SSH-Zugriff manuell eingeschränkt wird.

Navigieren Sie zu Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Protocol definitions > Actions > Create protocol definition.

Geben Sie den Namen und die Beschreibung ein.



Navigieren Sie zu Aktionen > Protokolleintrag erstellen.

- Name: SSH
- Typ: IPv4
    - IP und IPv6 sind ebenfalls verfügbar.
- IP-Protokoll/Optionen: TCP
    - Neben anderen werden UDP, EIGRP und PIM unterstützt.

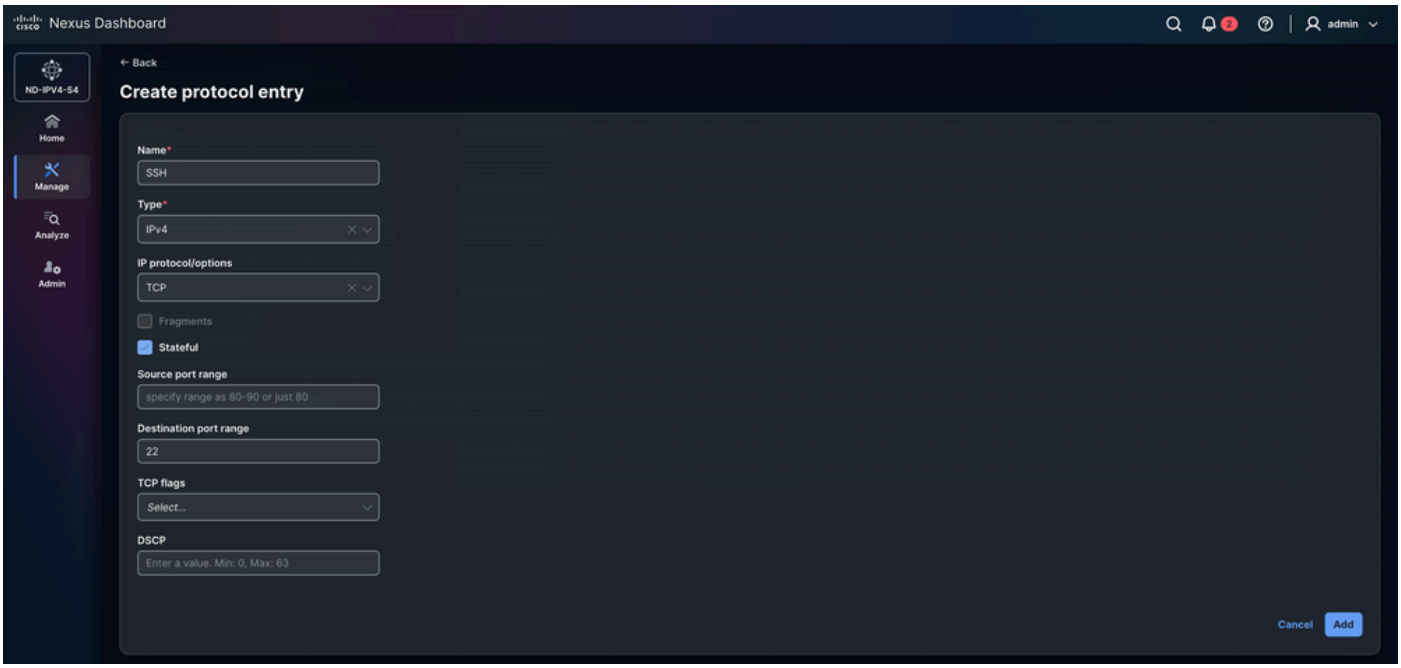
- Fragmente: Ermöglicht die Übereinstimmung der Regel mit fragmentierten IP-Paketen. Dies ist nützlich, da große Pakete bei Überschreiten der Netzwerk-MTU in Fragmente aufgeteilt werden können. Durch Aktivieren dieser Option wird sichergestellt, dass die Richtlinie auch für diese Fragmente gilt.

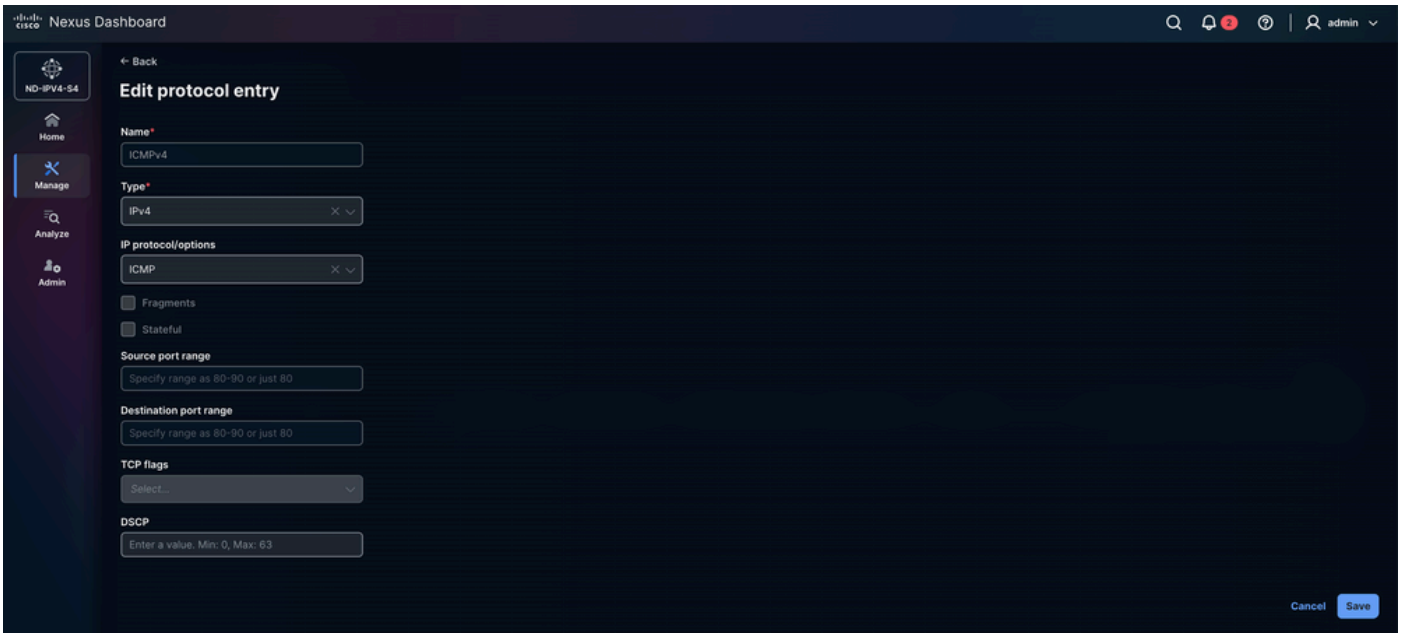
- Stateful: Ein Prozess ist zustandsbehaftet, d. h. er verfolgt alle Änderungen oder Interaktionen, die in der Vergangenheit stattgefunden haben, und ein aktueller Prozess wird mit einem Kontext dieser vorherigen Prozesse ausgeführt. In diesem Fall verfolgt TCP Bereiche wie die Anzahl der zu übertragenden Pakete, die Reihenfolge der Pakete und ob der Empfänger ein Paket empfangen hat oder nicht. Bei aktivierter Stateful-Option werden diese Informationen als Status in TCP gespeichert.

- Quellportbereich: Diese Option ist nur verfügbar, wenn Sie TCP oder UDP im Feld IP-Protokoll/Optionen oben ausgewählt haben.
- Zielportbereich: Diese Option ist nur verfügbar, wenn Sie TCP oder UDP im Feld "IP Protocol/Options" (IP-Protokoll/Optionen) ausgewählt haben.
- TCP-Flags

    - Diese Option ist nur verfügbar, wenn im Feld IP-Protokoll/Optionen TCP ausgewählt ist.

- Es ermöglicht Ihnen, die vom Sicherheitsprotokoll verwendeten TCP-Flags zu definieren.
- TCP-Flags sind Teil des TCP-Headers und werden verwendet, um den Aufbau, die Wartung und die Beendigung von Verbindungen zu steuern.
- Verfügbare Optionen:
    - ACK (Bestätigung): Gibt die Bestätigung empfangener Daten oder Synchronisierungspakete an.
    - EST (etabliert): Bezieht sich auf bereits hergestellte TCP-Verbindungen. Wenn diese Option aktiviert ist, können keine anderen TCP-Flags ausgewählt werden.
    - FIN (Ende): Wird verwendet, um eine TCP-Verbindung ordnungsgemäß zu schließen.
    - RST (Zurücksetzen): Beendet die Verbindung sofort und verwirft alle Daten, die noch übertragen werden.
    - SYN (Synchronisierung): Wird während des Aufbaus einer TCP-Verbindung verwendet.





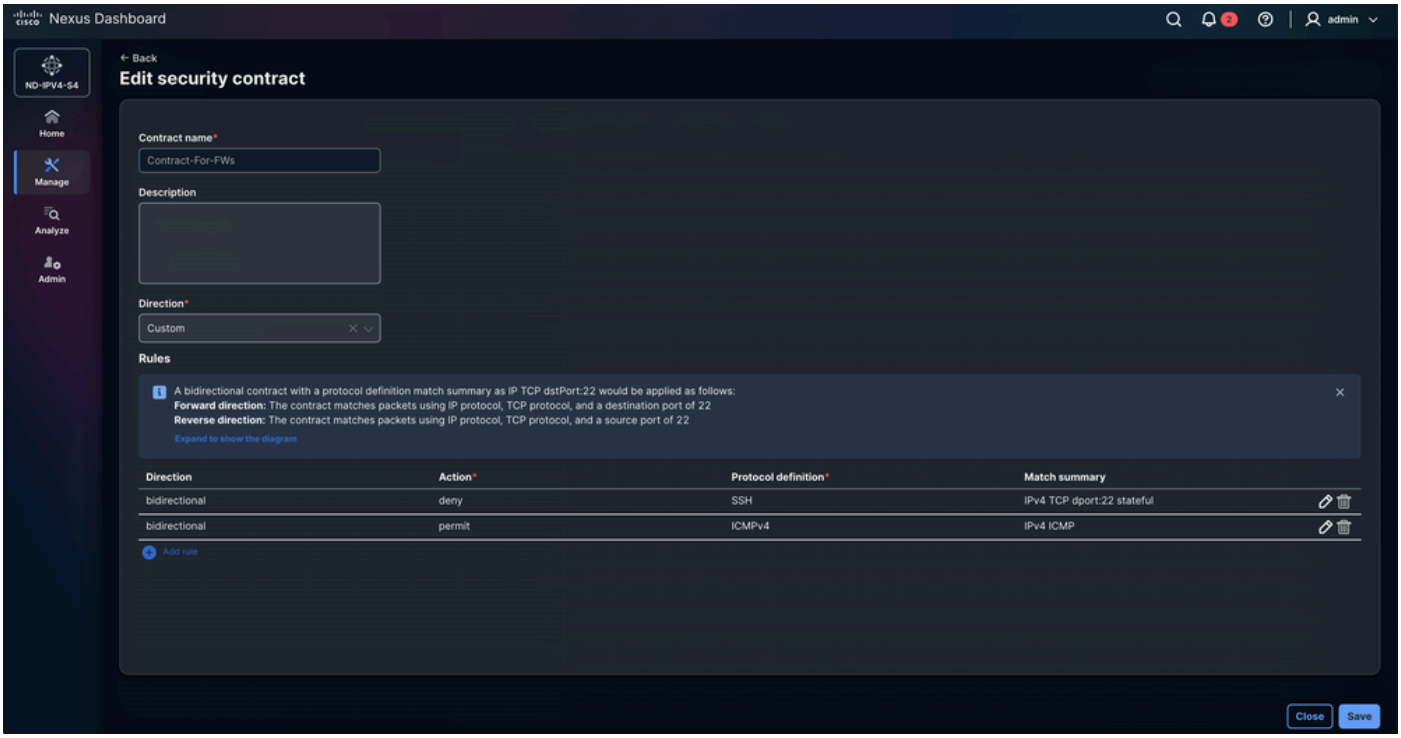
Schritt 5: Sicherheitsverträge konfigurieren

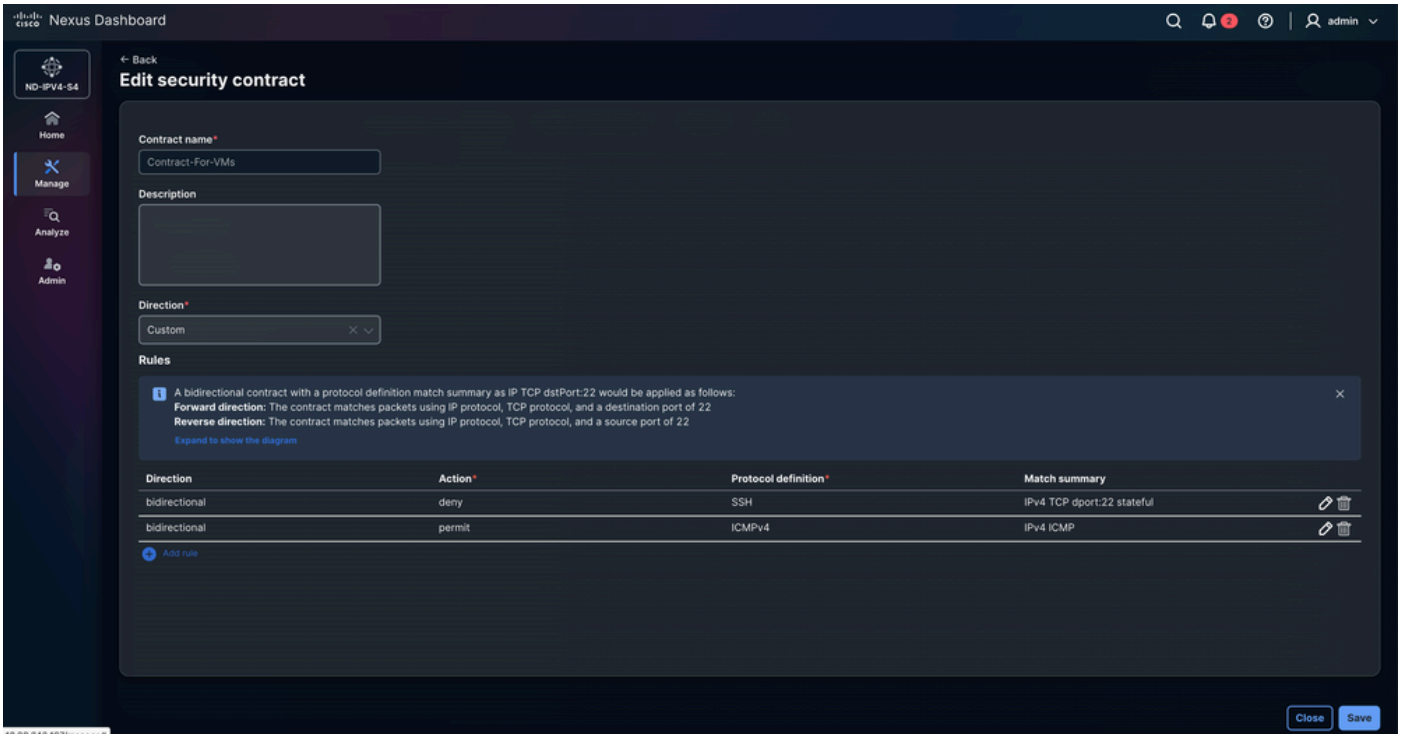
Der Vertrag definiert die Kommunikationsregeln zwischen Endpunktgruppen, indem er festlegt, welcher Datenverkehr auf der Grundlage der zugeordneten Richtliniendefinitionen zulässig oder abgelehnt ist. Sie dient als Durchsetzungsmechanismus, der die konfigurierten Protokollregeln, Filter und Aktionen anwendet und sicherstellt, dass der Datenverkehr zwischen Quell- und Zielgruppen den beabsichtigten Sicherheits- und Segmentierungsrichtlinien entspricht.

Navigieren Sie zu Verwalten > Fabrics > Fabric groups > DAVIDM3 > Segmentierung und Sicherheit > Sicherheitsverträge > Aktionen > Sicherheitsvertrag erstellen.

- Wählen Sie Regel hinzufügen und konfigurieren Sie Richtung, Aktion und Protokolldefinition.
    - Bidirektional:
        - Der bidirektionale Vertrag gilt wie folgt, mit einer Zusammenfassung der Protokolldefinitionsübereinstimmungen als IP-TCP-Port 22.
            - Weiterleitungsrichtung: Der Vertrag vergleicht Pakete mit IP- und TCP-Protokoll und einem Ziel-Port von 22.
            - Umgekehrte Richtung: Der Vertrag gleicht Pakete mit IP-Protokoll, TCP-Protokoll und einem Quell-Port von 22 ab.
            - Dies gilt unabhängig von der Quelle oder dem Ziel.
    - Unidirektional:
        - Unidirektional in einem Gruppenrichtlinienobjekt-Sicherheitsvertrag bedeutet,

dass die Richtlinie nur in eine Richtung des Datenverkehrsflusses durchgesetzt wird, sodass die Kommunikation von der Quellsicherheitsgruppe zur Zielsicherheitsgruppe zugelassen oder verweigert wird, ohne dass automatisch dieselbe Regel in umgekehrter Richtung angewendet wird.

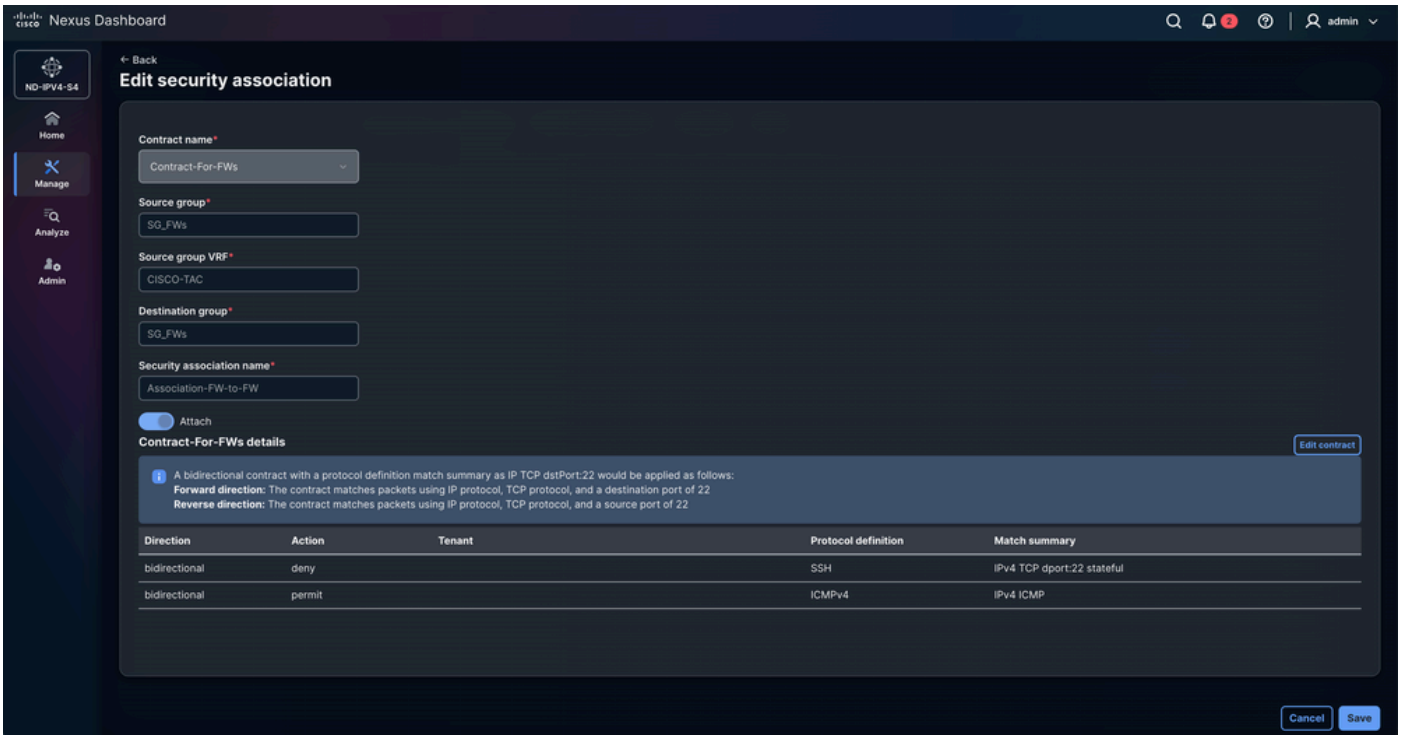


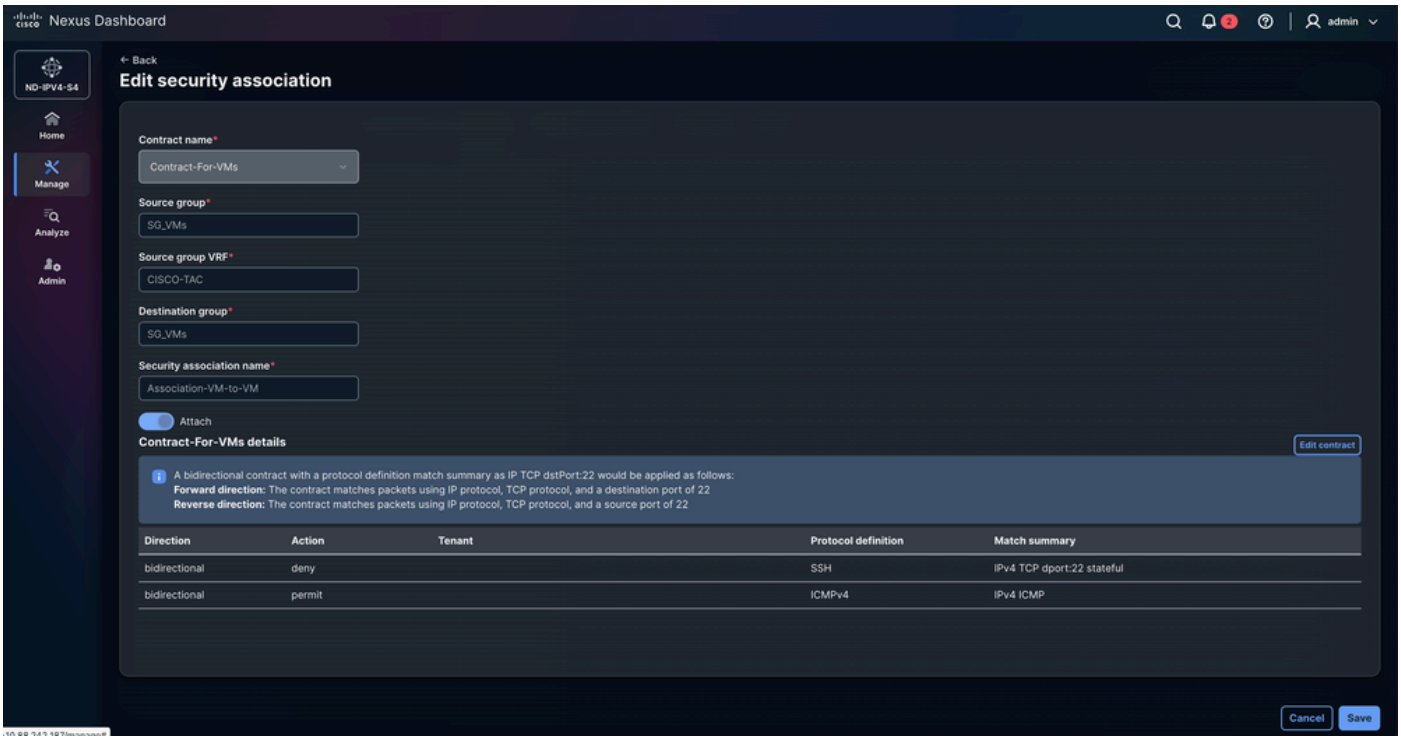


Schritt 6: Sicherheitszuordnungen konfigurieren

Navigieren Sie zu Verwalten > Strukturen > Fabric-Gruppen > DAVIDM3 > Segmentierung und Sicherheit > Sicherheitszuordnungen > Aktionen > Sicherheitszuordnung erstellen.

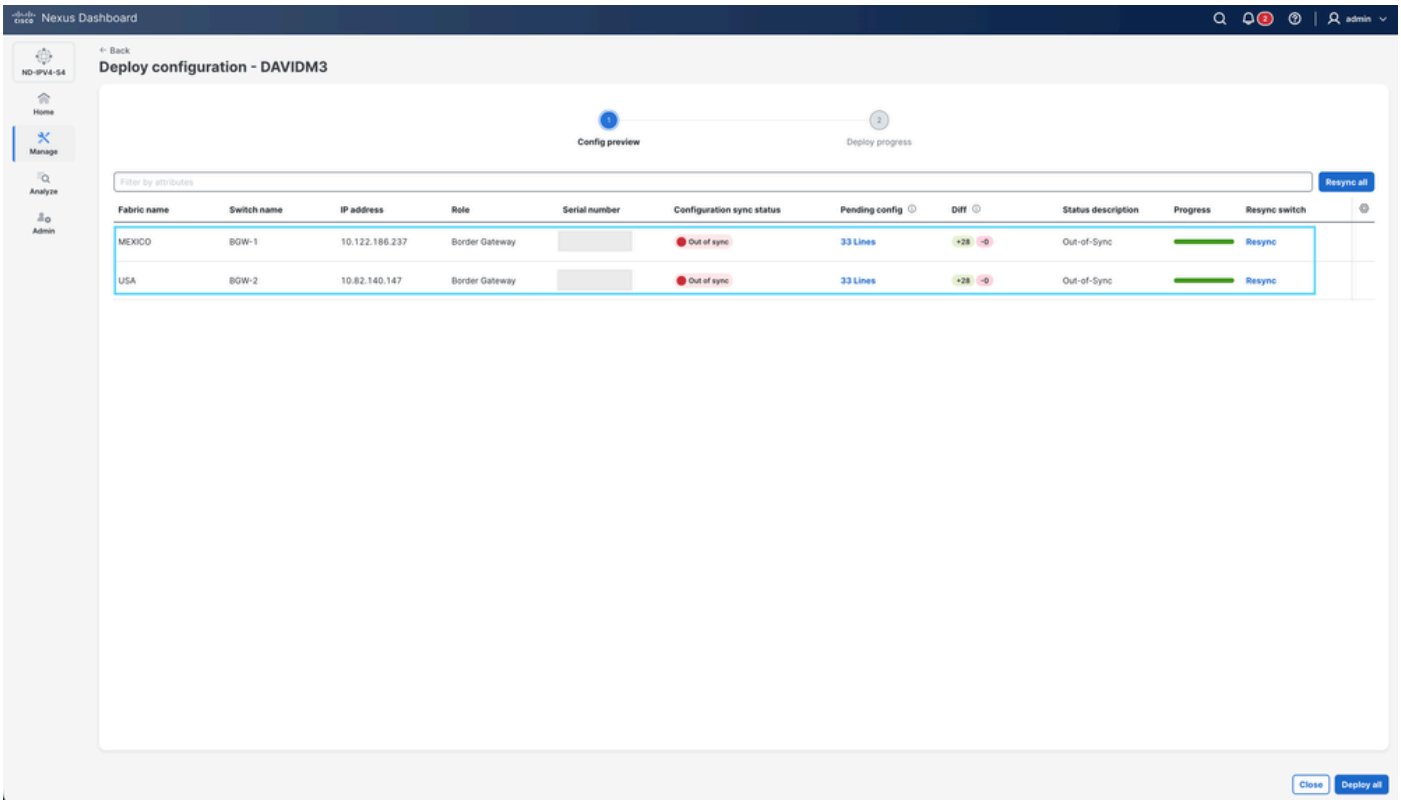
In Sicherheitszuordnungen konfigurieren wird das Richtlinienmodell durch Verknüpfen von Sicherheitsgruppen, Protokolldefinitionen und Sicherheitsverträgen definiert. Sicherheitsgruppen klassifizieren Endpunkte, Protokolldefinitionen geben die Datenverkehrstypen an (z. B. Protokolle oder Ports), und Sicherheitsverträge definieren die Richtlinie, die zwischen Quell- und Ziel-Sicherheitsgruppen mithilfe dieser Protokollregeln angewendet wird. Sicherheitszuordnungen stellen die Beziehung dar, die diese Elemente miteinander verbindet, sodass die Fabric die definierten Sicherheitsrichtlinien durchsetzen kann.

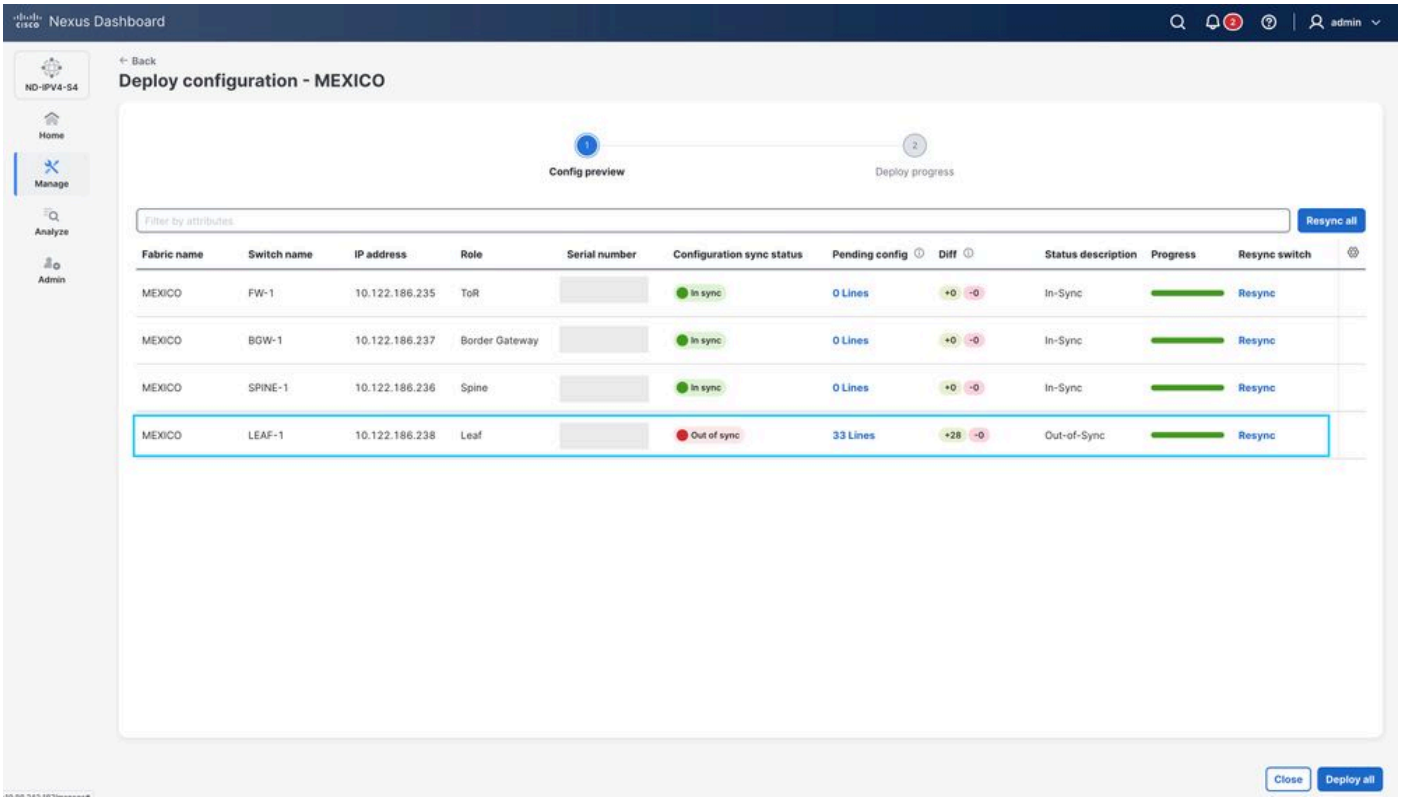


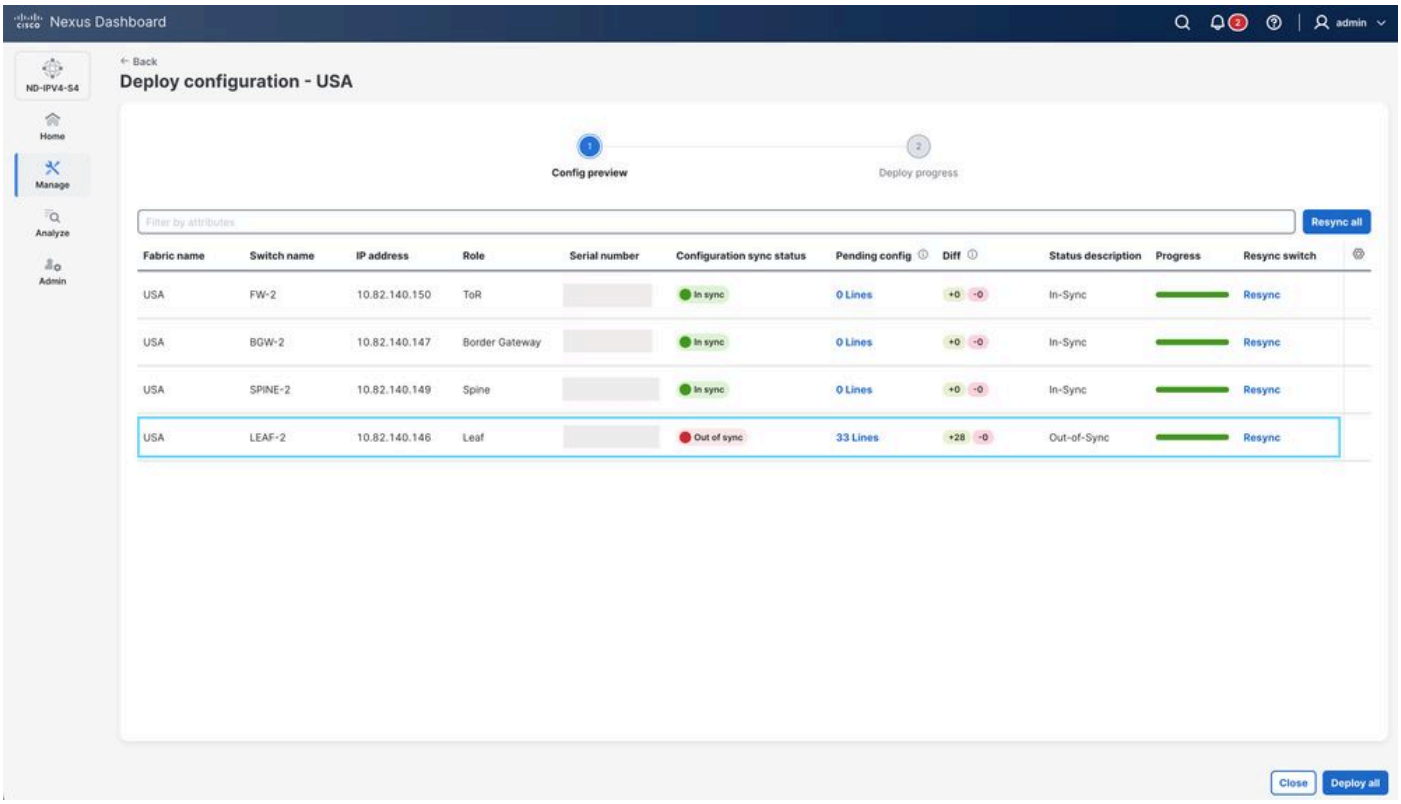


Schritt 7: Gruppenrichtlinienobjektkonfiguration validieren

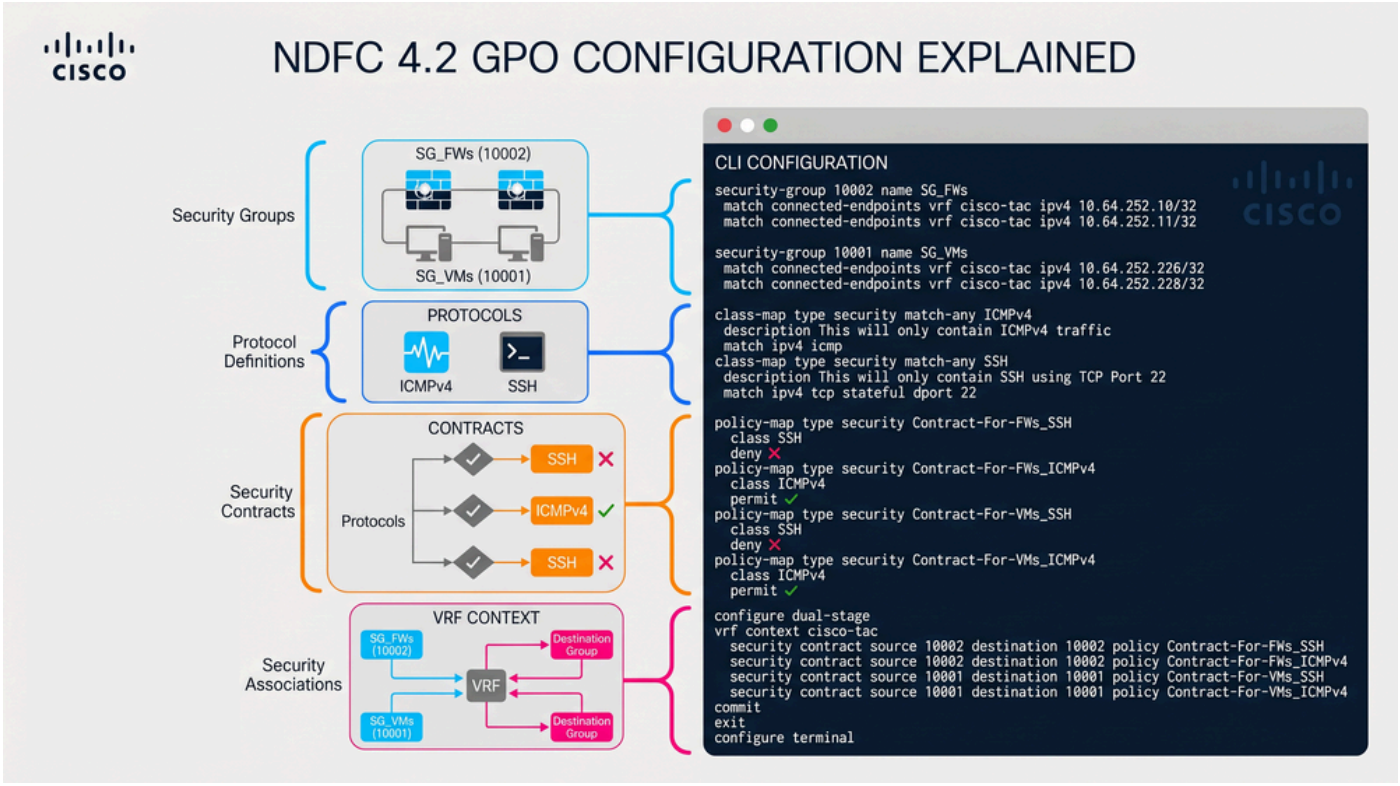
- Navigieren Sie zu Verwalten > Fabrics > Fabric groups > DAVIDM3 > Aktionen > Neu berechnen und bereitstellen.
  - Die GPO-Konfiguration wird vom übergeordneten Fabric-Switch an die Border Gateways übertragen. Klicken Sie auf die Anzahl der ausstehenden Konfigurationsposten, um die Konfiguration zu überprüfen und zu validieren, die auf den Geräten bereitgestellt werden kann. Dieser Prozess muss für jedes untergeordnete Fabric wiederholt werden.
  - Navigieren Sie zu Verwalten > Fabrics > Fabric Groups > DAVIDM3 > Inventory > Member Fabrics > MEXICO > Actions > Recalculate and deploy.
  - Navigieren Sie zu 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



- Das Bild zeigt die GPO-Konfiguration für BGW-1, BGW-2, LEAF-1 und LEAF-2. Die Konfiguration ist auf allen Switches identisch. NDFC 4.2 wendet die Konfiguration nicht in der angegebenen Reihenfolge an. In diesem Abschnitt wird die logische Reihenfolge der CLI-Befehle veranschaulicht.



Fehlerbehebung: Betrieb des VXLAN GPO

Schritt 1: Überprüfen des Sicherheitsgruppen-Funktionsstatus

Überprüfen Sie, ob die Sicherheitsgruppenfunktion auf dem Switch aktiviert ist. Das VXLAN-GPO hängt von dieser Funktion ab, da es die SGT-Infrastruktur (Security Group Tag) aktiviert, die für die Endpunktklassifizierung, die Vertragsdurchsetzung und die SGACL-Hardwareprogrammierung erforderlich ist.

<#root>

```
BGW-1#

show feature | i i security-group


security-group 1 enabled
```

Schritt 2: Überprüfen des System-Routing-Modus

Validieren Sie den konfigurierten und betriebsbereiten System-Routing-Modus auf dem Switch. Für das VXLAN-GPO ist der Routing-Modus "Security-Groups Support" erforderlich, da die SGACL-Durchsetzung dedizierte Hardware-Weiterleitungsressourcen innerhalb der ASIC-Pipeline belegt.

<#root>

```
BGW-1#

show system routing mode


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

Schritt 3: Überprüfung der VXLAN NVE-Peer-Einrichtung und der GPO-Funktion

- Validierung der VXLAN NVE-Peer-Einrichtung zwischen lokalen Fabric-Geräten und Remote-Multi-Site-Peers Da die VXLAN-GPO-Informationen über die VXLAN-EVPN-Kontrollebene weitergeleitet werden, sind stabile NVE-Nachbarschaften für das Security

Group Tag (SGT)-Learning und die Vertragssynchronisierung in der gesamten Fabric erforderlich.
- Die Feldgruppenrichtlinien-Funktion ist einer der wichtigsten Indikatoren in diesem Befehl, da sie bestätigt, ob das Remote-VTEP VXLAN-Gruppenrichtlinienerweiterungen unterstützt, die für die SGT-Propagierung und die SGACL-Vertragsdurchsetzung in der VXLAN-EVPN-Multi-Site-Domäne erforderlich sind.

<#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

Schritt 4: Sicherheitsgruppenlernen und Endpunktklassifizierung überprüfen

Überprüfen der korrekten Klassifizierung von Endpunkten in Sicherheitsgruppen (SGTs) Die VXLAN-GPO-Durchsetzung hängt von der genauen Zuordnung von Endpunkt zu SGT ab.

<#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
```

Schritt 5: Sicherheitsverträge und Richtliniendurchsetzung überprüfen

Überprüfen Sie, ob die VXLAN-GPO-Verträge korrekt installiert und betriebsbereit sind. Verträge definieren die Kommunikationsregeln, die zwischen Sicherheitsgruppen durchgesetzt werden, und stellen den Kernrichtlinienmechanismus dar, der von VXLAN GPO für die Mikrosegmentierung verwendet wird.

<#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
```

Schritt 6: Überprüfen des VRF-Sicherheitsdurchsetzungsstatus

Validieren Sie den VXLAN-GPO-Erzwingungsstatus für alle auf dem Switch konfigurierten VRFs. Mit diesem Befehl wird bestätigt, ob SGACL-Richtlinien und Security Group Contracts innerhalb der Tenant-VRF-Instanz aktiv durchgesetzt werden.

Die Ausgabe bestätigt, dass das cisco-tac-VRF aktiv an der VXLAN-GPO-Durchsetzung beteiligt ist, wobei der Modus auf "enforced" (Erzwungen) gesetzt ist. Das Durchsetzungs-Tag 13648 identifiziert den internen SGACL-Richtlinienkontext, der für diese VRF-Instanz in die Hardware programmiert wurde. Die Standardaktion "deny log" (Protokoll ablehnen) gibt an, dass jeglicher Datenverkehr, der nicht explizit über einen Security Group-Vertrag zulässig ist, abgelehnt und protokolliert wird. Dabei wird eine Standardrichtlinie für die Mikrosegmentierung "deny" (Verweigern) implementiert. Die Standard-, Egress-LoadBalancing-Resolution-Management- und Management-VRFs hingegen arbeiten im nicht erzwungenen Modus, d. h., VXLAN-GPO-Richtlinien werden innerhalb dieser VRFs nicht angewendet, und der Datenverkehr ist standardmäßig zulässig.

Das Feld "Stats" (Statistiken) verfolgt den Datenverkehr entsprechend der VRF-Sicherheitsrichtlinie. Der Wert 0 unter der VRF-Instanz cisco-tac gibt an, dass zum Zeitpunkt der Ausführung des Befehls kein nicht übereinstimmender Datenverkehr das standardmäßige Ablehnungsverhalten ausgelöst hat, während der Zählerwert 4364 unter der VRF-Standardeinstellung die Datenverkehrsaktivität innerhalb einer VRF-Instanz angibt, die ohne VXLAN-GPO-Durchsetzung funktioniert.

```
<#root>

BGW-1#
```

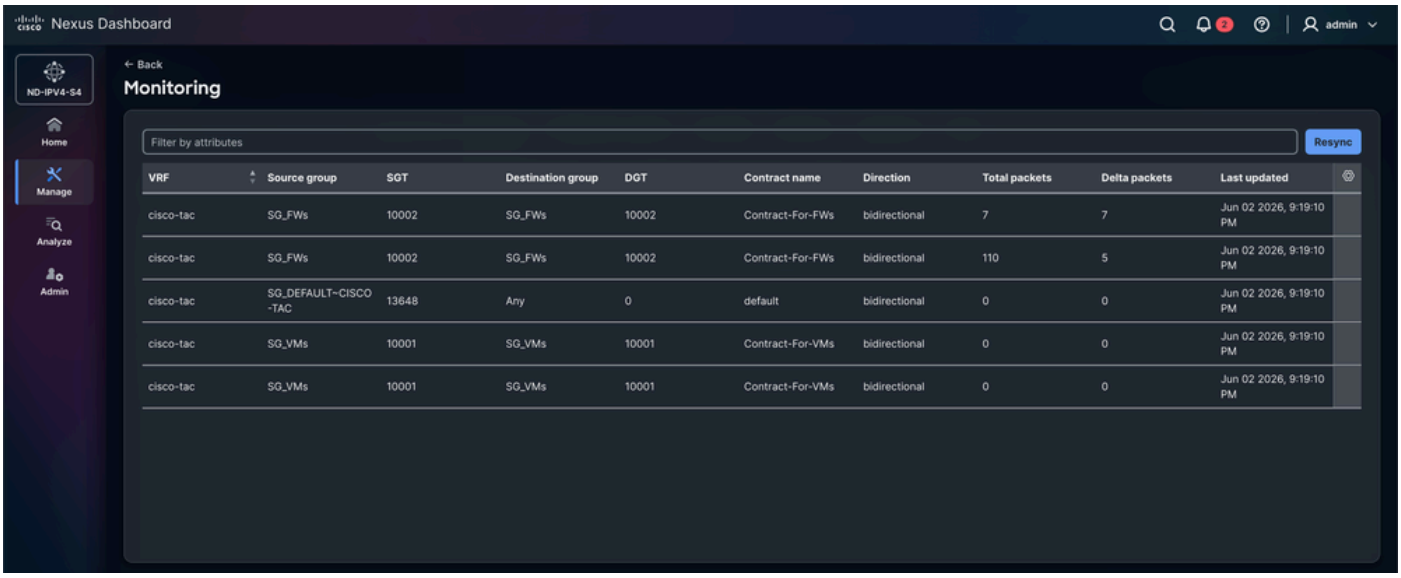
```
show vrf all security
```

```
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
```

Schritt 7: Überprüfen des VRF-Sicherheitsdurchsetzungsstatus

- Validieren Sie die Statistiken zum Datenverkehrsabgleich für VXLAN-Gruppenrichtlinienobjekte über die NDFC-GUI. Diese Überprüfung bestätigt, ob der Datenverkehr aktiv mit den konfigurierten Security Group Contracts übereinstimmt und ob die SGACL-Durchsetzung in der gesamten VXLAN EVPN Multi-Site-Fabric funktioniert.
- Navigieren Sie in der NDFC-GUI zu Manage > Fabrics > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoring.
    - Dieser Abschnitt bietet Einblick in Kommunikationsflüsse von Sicherheitsgruppen, Statistiken zu Vertragsergebnissen, Zulassen und Ablehnen von Aktionen sowie betriebliche Vertragsaktivitäten zwischen Endpunktgruppen.
    - Die Überwachungsstatistiken werden in jedem Fenster einzeln angezeigt.
    - Die Überwachung von Statistiken über NDFC bietet eine betriebliche Validierungsebene, die die CLI-basierte Fehlerbehebung ergänzt, indem sie die Durchsetzung von Richtlinien in Echtzeit und das Verhalten beim Abgleich des Datenverkehrs in der gesamten Fabric bestätigt.

Anmerkung: Beim ersten Versuch, die Datenverkehrsstatistik in NDFC 4.2 zu überprüfen, kann der Überwachungsabschnitt zunächst leer erscheinen. In diesem Fall drücken Sie die Taste Resync (Neu synchronisieren), um die Synchronisierung der Vertragsstatistiken aus der VXLAN-Fabric zu starten. Während der Synchronisierung zeigt die GUI die Meldung Resync status: In progress. Wenn die Synchronisierung abgeschlossen ist, drücken Sie die Taste Ok, um die Überwachungsansicht zu aktualisieren. Nach Abschluss der Resynchronisierung werden die mit den einzelnen Sicherheitsgruppenverträgen verknüpften Datenverkehrsstatistiken im Überwachungsabschnitt angezeigt. Um das Abgleichverhalten für Live-Datenverkehr zu validieren, generieren Sie Datenverkehr zwischen den Endpunkten, und drücken Sie dann erneut die Taste Resync (Neu synchronisieren), um die in NDFC angezeigten Vertragsstatistiken zu aktualisieren.



- Aus dem vorherigen Szenario wird ICMPv4-Datenverkehr zwischen den Endpunkten zugelassen. Wenn jedoch eine SSH-Sitzung hergestellt wird, läuft die Verbindung ab, da der VXLAN-GPO-Vertrag den an Port 22 gerichteten TCP-Datenverkehr explizit ablehnt.

<#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
```

Zugehörige Informationen

[Cisco Nexus Serie 9000 NX-OS VXLAN Konfigurationsleitfaden, Version 10.6(x)]

Sicherung von Rechenzentren mit Mikrosegmentierung mithilfe von VXLAN GPO

Bereitstellung von Mikrosegmentierung in Cisco NX-OS VXLAN EVPN Fabrics mit VXLAN Group Policy Option (GPO)

Automatisierung der Mikrosegmentierung und Bereitstellung von Layer-4-7-Services in VXLAN-EVPN-Fabrics mit Group Policy Option (GPO) und Nexus Dashboard

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.