使用NDFC 4.2在Nexus多站點交換矩陣上配置GPO

目錄

簡介

本文檔介紹運行NX-OS和NDFC 4.2的Nexus雲擴展交換機上的VXLAN多站點交換矩陣中的GPO配置和驗證。

必要條件

需求

思科建議您瞭解以下領域：

- 虛擬可擴充區域網路(VXLAN)、乙太網路虛擬私人網路(EVPN)和多站點光纖技術
- Cisco Nexus Cloud Scale交換機和NeXus作業系統(NX-OS)操作
- Nexus交換矩陣網路控制器(NDFC)4.2管理和部署工作流程
- 網路分段和安全策略概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

瞭解VXLAN EVPN交換矩陣中的GPO功能

組策略選項(GPO)是一種基於策略的分段機制，旨在根據邏輯身份而不是僅依賴IP地址、VLAN或子網來控制終端之間的通訊。GPO的主要目的是簡化安全策略實施，並在應用程式、伺服器或工作負載之間提供可擴展的微細分段。

一個簡單的類比是設想一家酒店，其中每位客人都屬於特定類別或訪問級別，某些區域僅允許特定客人訪問，並且訪問許可權取決於訪客的角色而不是房間號碼。GPO的工作方式非常相似。GPO不是將端點完全視為IP地址，而是將它們分類為安全組(SG)。 然後，在這些組之間應用策略，以確定允許或拒絕哪些通訊。

舉例來說：

- Web伺服器可以屬於一個安全組。
- 應用程式伺服器可以屬於另一個安全組。

- 資料庫伺服器可以屬於受限制的安全組。

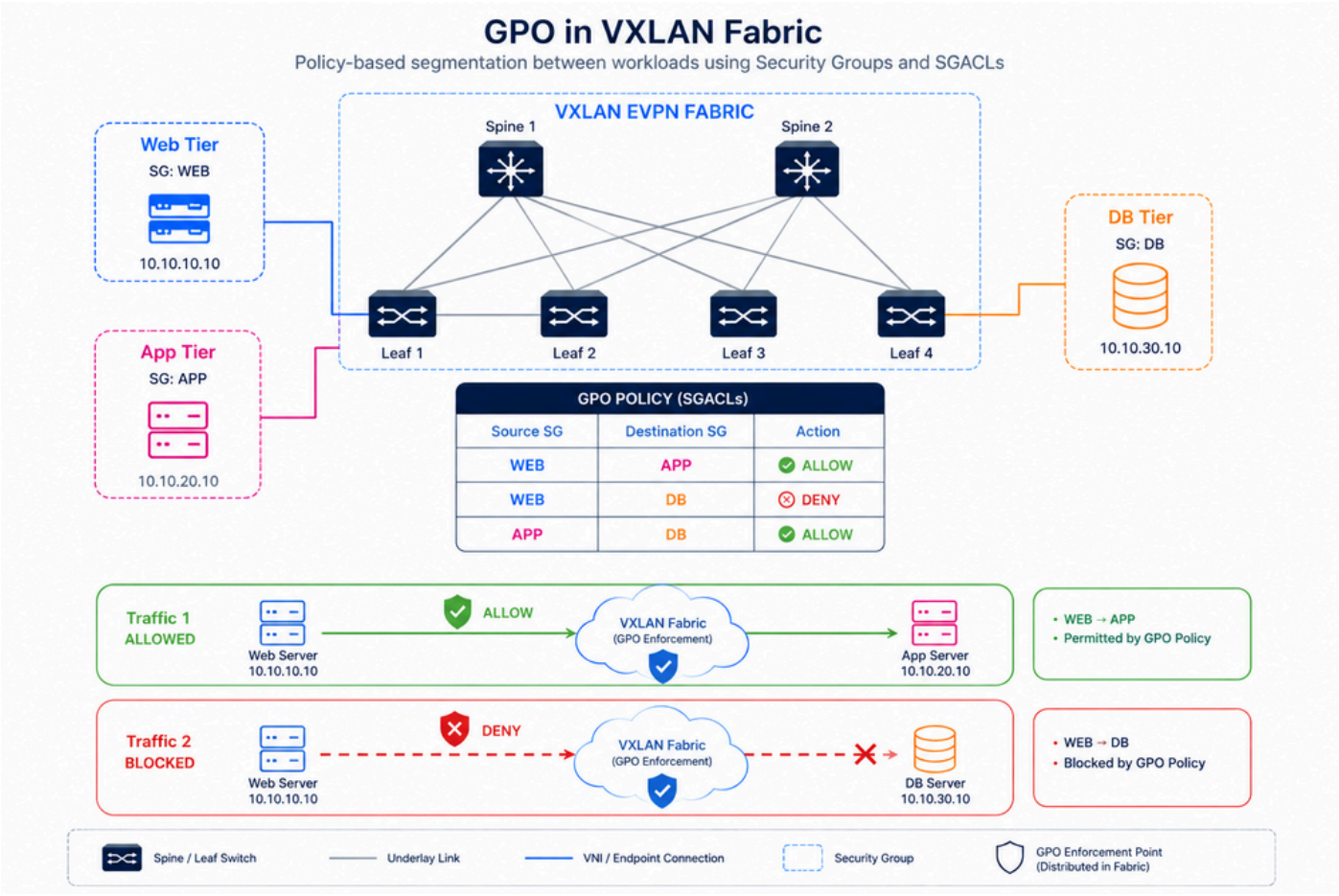
然後，策略可以定義：

- Web伺服器可以與應用伺服器通訊。
- 應用程式伺服器可以與資料庫伺服器通訊。
- Web伺服器無法與資料庫伺服器直接通訊。

此方法簡化了操作，因為管理員不再需要跨多個裝置和VLAN維護大量ACL。

另一個主要優勢是可擴充性。在大型環境中，工作負載經常移動、動態擴展或更改IP地址。即使在端點位置發生更改時，GPO也允許安全策略保持一致。在VXLAN EVPN結構中，GPO通過跨結構分發安全組資訊以及在端點之間實施安全組ACL(SGACL)來擴展此概念。這在現代資料中心中變得尤為重要，因為工作負載之間的東西流量通常代表最大的攻擊面。GPO通過限制資料中心交換矩陣內不必要的通訊路徑來改善安全狀態。

有關對GPO架構、微分段概念和VXLAN策略實施的更深入的技術瞭解，請參閱思科白皮書：《使用VXLAN GPO通過微分段保護資料中心》(Secure Data Center with Microsegmentation using VXLAN GPO)



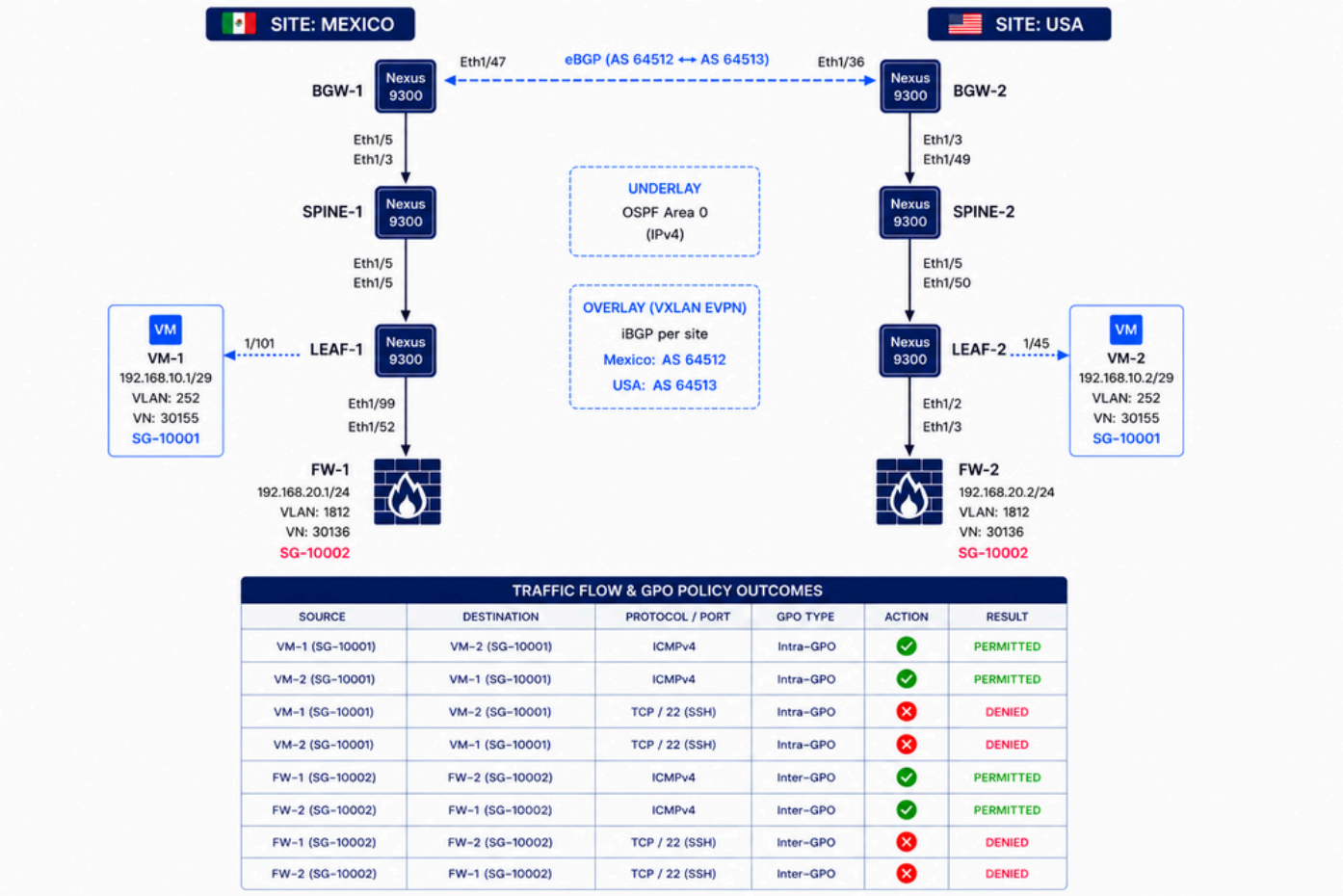
VxLAN交換矩陣中的GPO

使用NDFC 4.2和NX-OS 10.6(3)F的VXLAN多站點GPO部署方案

此拓撲表示在兩個地理上分散的站點上部署的VXLAN多站點交換矩陣：墨西哥和美國。每個站點都包含專用的BGW、主幹交換機、枝葉交換機、虛擬機器和運行在採用NX-OS 10.6(3)F的Cisco Nexus 9300交換機上的防火牆網段。底層網路使用開放最短路徑優先(OSPF)，而重疊控制平面使用每個站點內的iBGP和BGW-1和BGW-2之間的eBGP進行站點間VXLAN EVPN通訊。由於此環境是實驗室部署，因此墨西哥和美國站點通過兩個BGW之間的直接連線鏈路互連，以簡化多站點連線模式。

GPO用於在安全組(SG)之間實施基於策略的微分段，獨立於IP編址或VLAN邊界。根據連線策略表，允許從VM-1到VM-2、FW-1和FW-2的ICMP流量，但拒絕從VM-1到FW-1和FW-2的TCP埠22(SSH)流量。VM-1和VM-2之間的TCP埠22通訊仍然被允許，因為兩個終端屬於同一個安全組(SG-10001)。 此行為展示GPO如何通過VXLAN多站點交換矩陣在GPO內和GPO間通訊之間動態實施不同的流量策略。

附註：Cisco NX-OS版本10.6(3)F引入了使用ESG內隔離功能限制同一ESG（也稱為SG）內終端之間的通訊。此功能可最大程度降低ESG內未經授權訪問的風險，並增強安全狀況。



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

在VXLAN EVPN結構中使用NDFC 4.2逐步配置GPO

當VXLAN多站點交換矩陣已運行並配置了NDFC 4.2，並且以後需要實施GPO時，將應用這些步驟。使用Nexus儀表板的自動化使用VXLAN GPO通過微分段保護資料中心一節顯示了從建立VXLAN單站點交換矩陣開始的配置。

⚠ 注意：當GPO在VXLAN EVPN交換矩陣中運行時，僅當存在目標可達性且安全策略允許流量時，才會進行通訊。策略實施依賴於IP資訊，這些資訊需要內部網路的ARP條目和SVI。這意味著屬於租戶VRF的VLAN必須配置SVI。因此，實施不適用於僅包含第2層報頭的流量，因此不能用於VXLAN第2層擴展。NX-OS版本10.6(2)F引入了基於MAC的微分段支援。

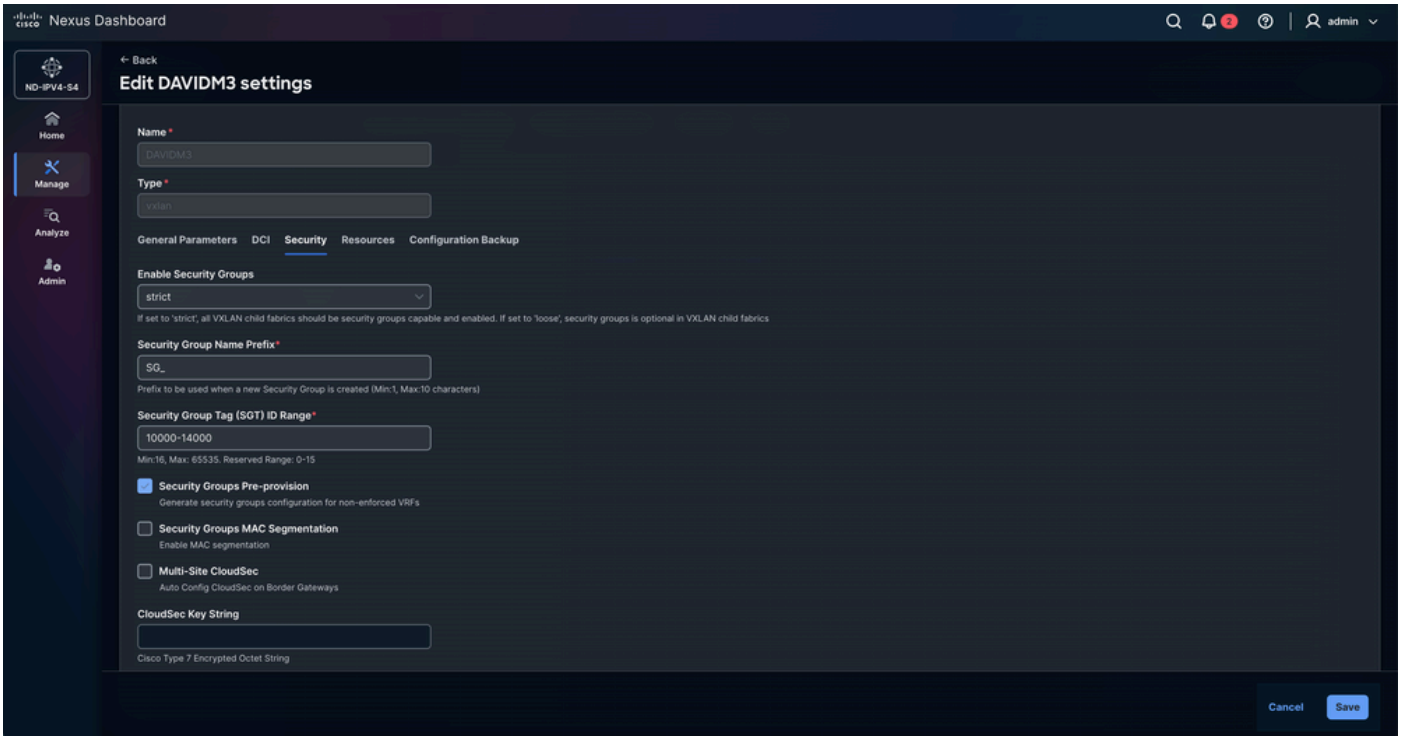
步驟1.在父交換矩陣中啟用安全組

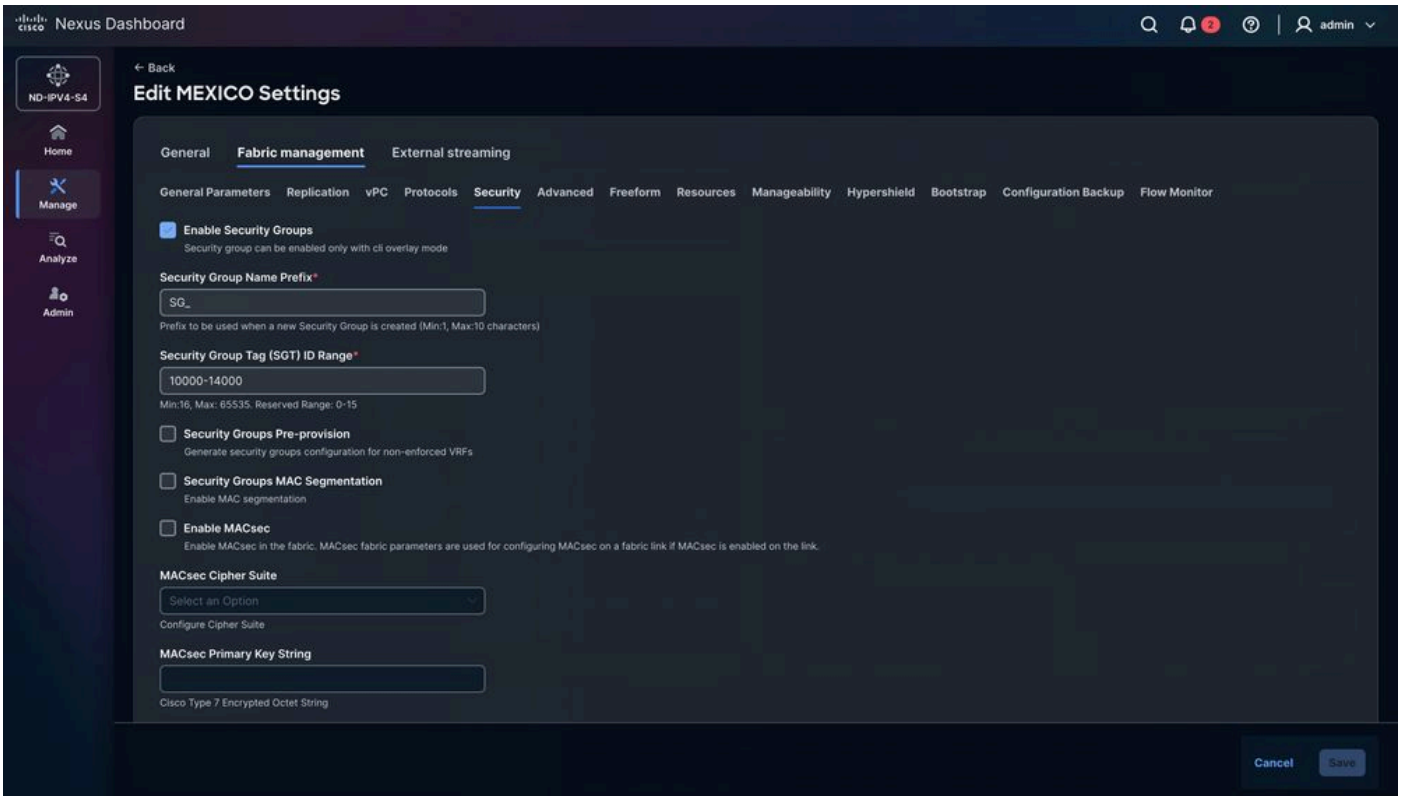
- 導航到Manage > Fabric Groups，選擇交換矩陣組DAVIDM3，然後選擇Actions > Edit Fabric Group Settings。在「安全」部分中，啟用Security Groups，將模式設定為Strict，並設定Security GroupsPre-provision。
  - 選擇感興趣的交換矩陣組。在本示例中，選定的交換矩陣組稱為DAVIDM3，它也是多站點交換矩陣的名稱。

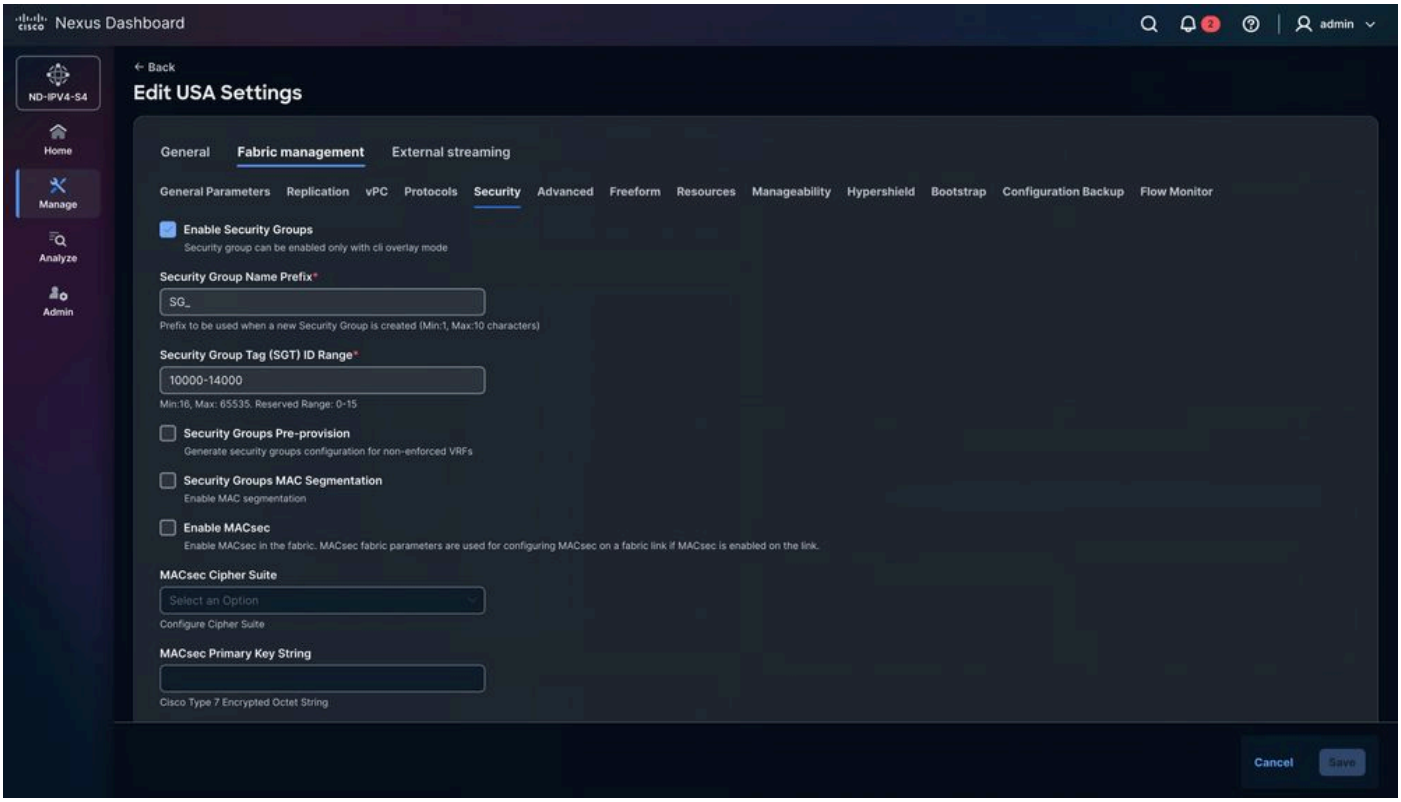
- 對每個子交換矩陣重複這些步驟。
  - 導航到管理>交換矩陣，選擇USA，然後導航到操作>編輯交換矩陣組設定。在Security部分中，啟用Security Groups並將模式設定為Strict。
  - 導覽至Manage > Fabric，選擇MEXICO，然後導覽至Actions > Edit Fabric Group Settings。在Security部分中，啟用Security Groups並將模式設定為Strict。

附註：如果設定為strict，則所有VXLAN子結構都必須支援並啟用安全組。如果設定為鬆散，則安全組在VXLAN子結構中是可選的。

提示：要保持清晰的可見性，請在父交換矩陣和所有子交換矩陣中使用相同的安全組標籤(SGT)ID範圍。父交換矩陣範圍必須覆蓋所有子交換矩陣使用的範圍。







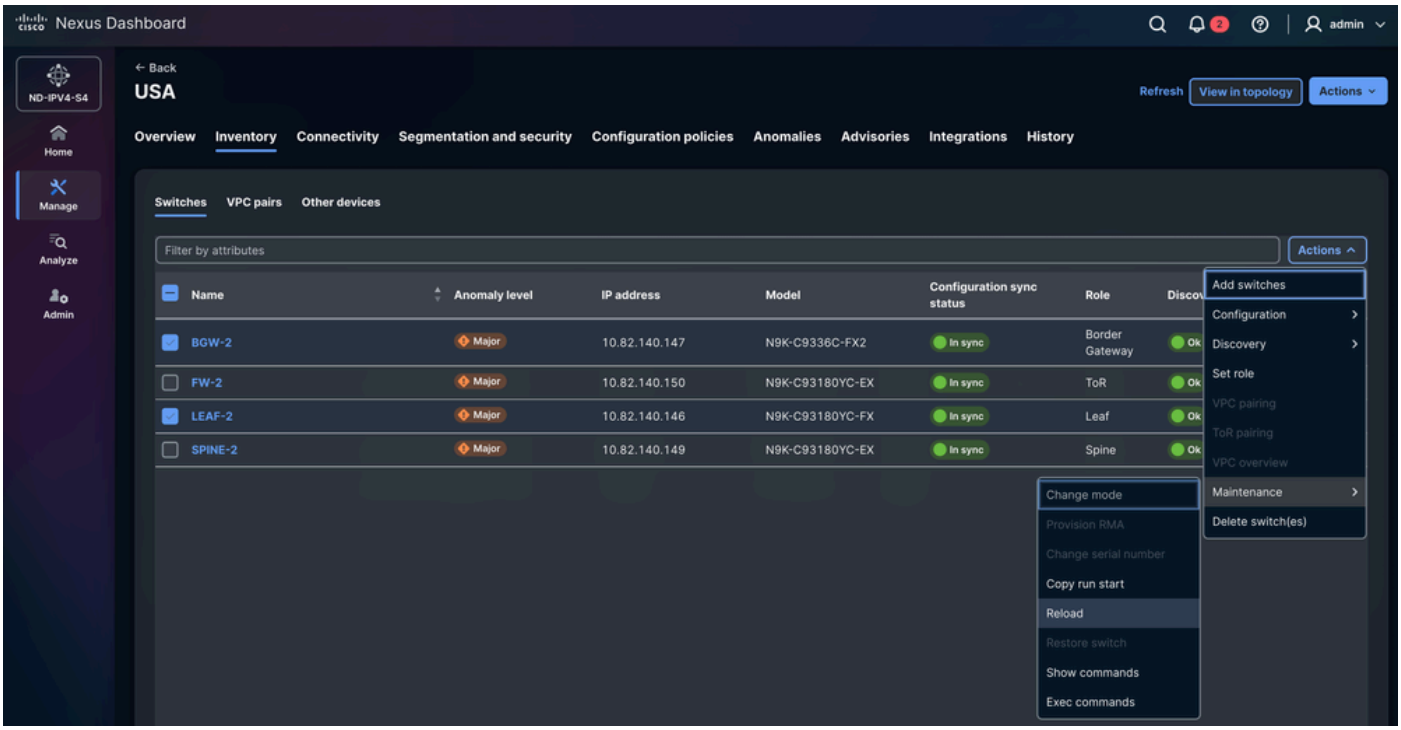
步驟2.為GPO部署重新計算交換矩陣配置並重新載入交換機

NDFC會根據特定的Nexus交換機的角色自動提示您重新載入該組。在本示例中，必須重新載入LEAF-1、LEAF-2、BGW-1和BGW-2。此操作必須由網路管理員手動執行。需要重新載入，並且無法跳過該重新載入，因為GPO需要TCAM雕刻。

附註：如果未重新載入裝置，TCAM更改可能出現在運行配置中；但是，由於交換機尚未重新啟動，因此該設定不會應用於硬體記憶體。因此，該功能無法按預期運行。

要重新載入Nexus交換機：

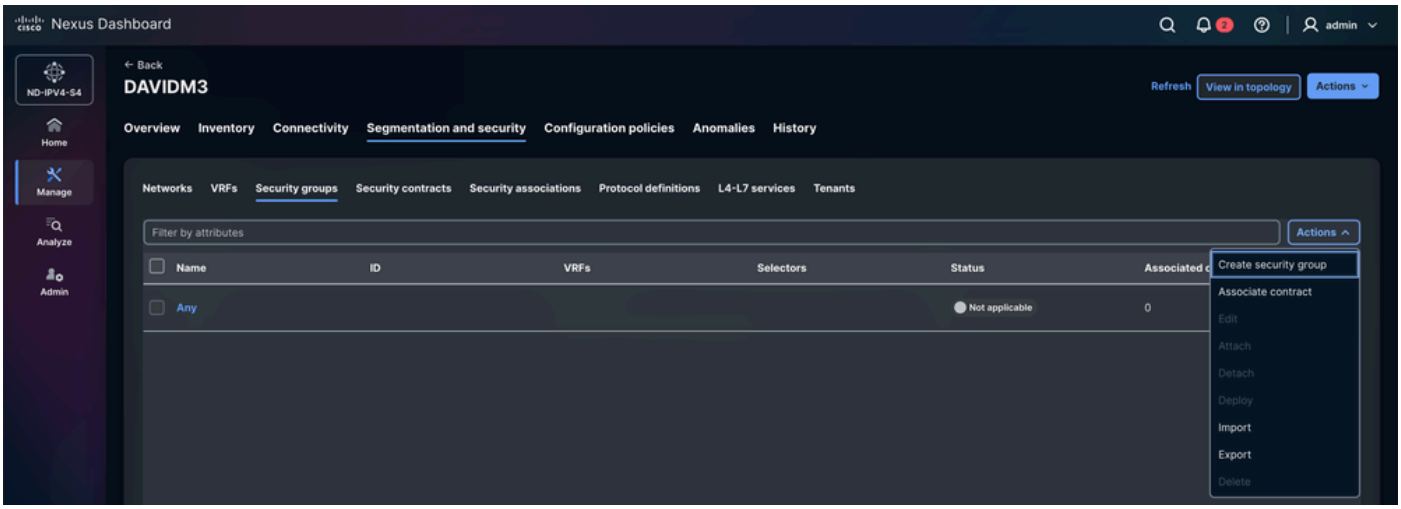
導航到Manage > Fabric > MEXICO/USA > Inventory > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions > Maintenance > Reload。



步驟3.建立安全組

為每個端點定義安全組。VXLAN交換矩陣中的每個端點可以有一個安全組。這種方法不能有效擴展。全域性分組終端（虛擬機器、防火牆、TCP最佳化程式等）。

導航到Manage > Fabric > Fabric groups > DAVIDM3 > Segmentation and security > Security Groups > Actions > Create security group。



步驟3.1配置安全組名稱

- NDFC自動分配一個隨機名稱，該名稱可以更改；建議使用易於端點識別的代表性名稱。
- 在此情況中：
  - VM -> SG_VM
  - 防火牆 — > SG_FW

第3.2步配置VRF

- 選擇終端所屬的租戶(VRF)。
- 在此情況中：VM和防火牆屬於CISCO-TAC租戶。

可選，建立VRF。

預設情況下，新建立的租戶VRF將策略實施模式設定為Unenforced。在此狀態下，即使配置安全組之間的分類標準和SGACL，也不會執行任何策略。要啟用SGACL實施，必須在實施模式下顯式配置VRF。

當VRF在強制模式下運行時，會定義預設策略行為：

- 拒絕：除非允許規則明確允許，否則所有單播流量都會被丟棄。
- 允許：除非被拒絕規則明確阻止，否則允許所有單播流量。

屬於同一安全組的端點可以相互通訊，而不需要SGACL規則。SGACL僅在不同的安全組之間定義安全策略。

Cisco NX-OS版本10.6(3)F引入了限制同一GPO內終端之間通訊的功能，也稱為GPO內隔離功能。

在此版本之前，應用於同一安全組內端點的規則會被忽略，並且預設情況下允許流量。

步驟3.3配置安全組標籤ID

NDFC自動從交換矩陣配置中的預定義範圍內分配隨機標籤ID。雖然可以手動選擇標籤ID，但它必須位於為子交換矩陣和父交換矩陣定義的範圍內。

在此情況中：

- VM-1和VM-2:10001
- FW-1和FW-2:10002

第3.4步配售

如果未啟用Attach選項，則安全組不會應用於CISCO-TAC租戶。

步驟3.5配置選擇器

- 選擇器確定哪些端點和外部IP地址與特定安全組相關聯。

NDFC 4.2本地支援三種型別的選擇器：

1)IP選擇器：IP選擇器根據IP資訊將終端或IP子網與安全組相關聯。

a. 連線端點 — 標識直接連線到交換矩陣的端點，例如虛擬機器、伺服器或連線到枝葉交換機的物理主機。
b. 外部子網 — 將外部IP字首與安全組相關聯。此型別用於VXLAN交換矩陣之外的網路，例如外部資料中心、WAN網段或面向網際網路的網路。來源或目的地為這些字首的流量使用已配置的安全組進行分類。

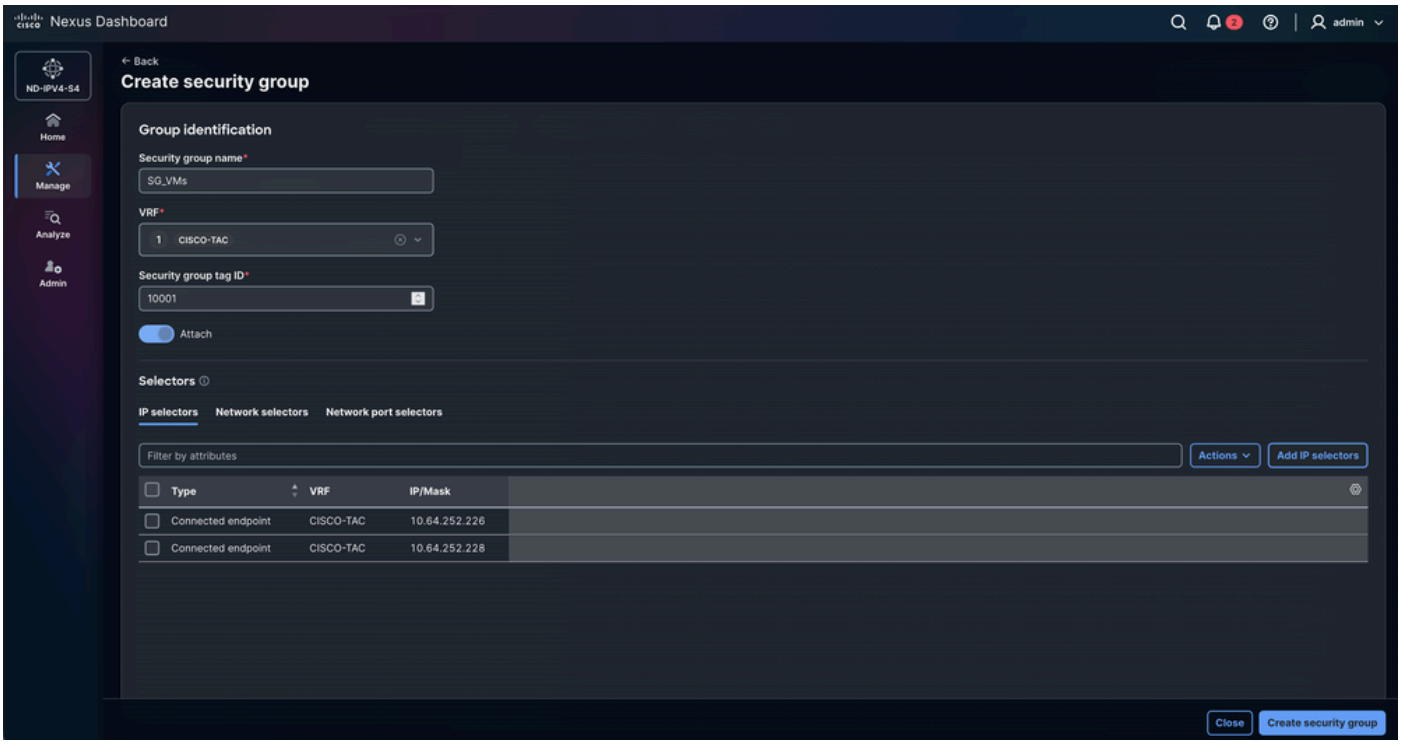
2)網路選擇器：網路選擇器將安全組與特定VXLAN網段相關聯。基於網路識別符號(L2VNI)應用分類。 屬於該網路的所有終端都繼承分配的安全組，這樣當多個終端共用同一網段時，可以簡化策略部署。

3)網路埠選擇器：網路埠選擇器根據流量進入交換矩陣的物理交換機介面對流量進行分類。可將安全組分配給在特定埠或介面上接收的流量。此方法通常用於通過外部網路、服務裝置或基礎設施鏈路連線的裝置，在這些裝置中，終端IP分類不可行。

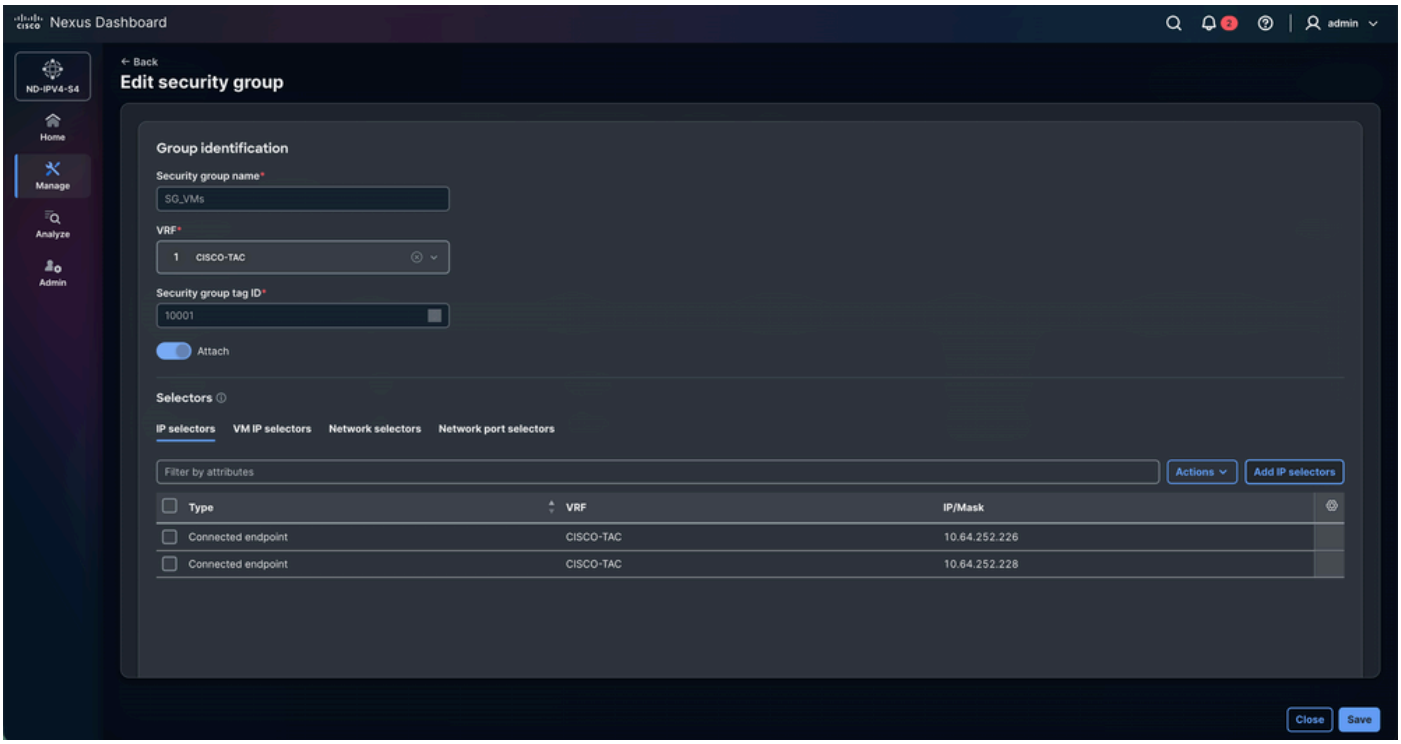
安全組配置摘要

裝置	安全組名稱	VRF	安全組標籤ID	選擇器
VM-1	SG_VM	CISCO-TAC	10001	IP選擇器
VM-2	SG_VM	CISCO-TAC	10001	IP選擇器
FW-1	SG_FW	CISCO-TAC	10002	IP選擇器
FW-2	SG_FW	CISCO-TAC	10002	IP選擇器

VM的安全組配置



防火牆的安全組配置



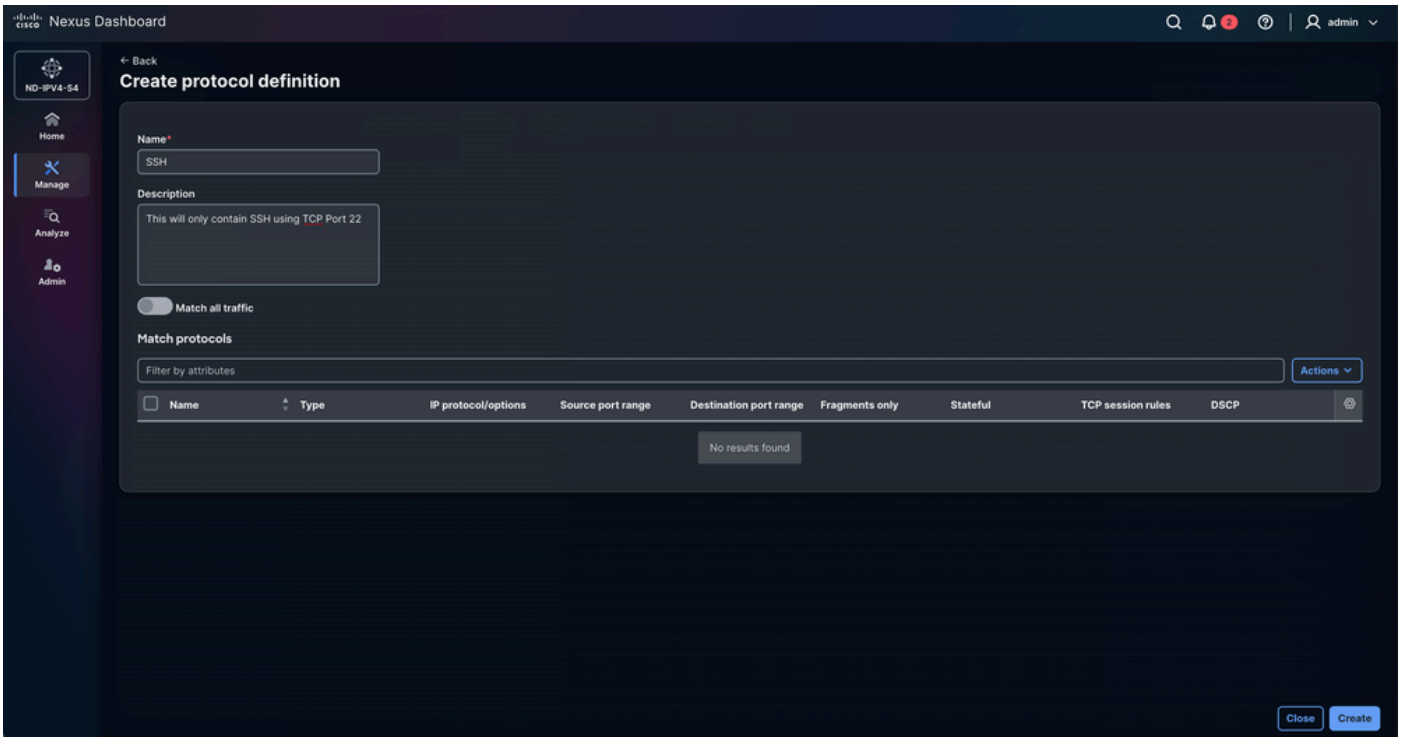
步驟4.配置協定定義

Create Protocol Definition選項用於定義與組策略對象(GPO)匹配的網路協定引數和流量特性。 它允許管理員指定諸如協定型別、埠號和其他資料包屬性等標準，以便將相應的策略應用於所需的通訊流。

在此案例中，目標是只允許ICMP流量，同時明確封鎖連線埠22(SSH)上的TCP流量。 此策略確保允許網路連通性測試，同時手動限制未經授權或不希望的SSH訪問。

導航到Manage > Fabric > Fabric groups > DAVIDM3 > Segmentation and security > Protocol definitions > Actions > Create protocol definition。

輸入名稱和說明。



導航到操作>建立協定條目。

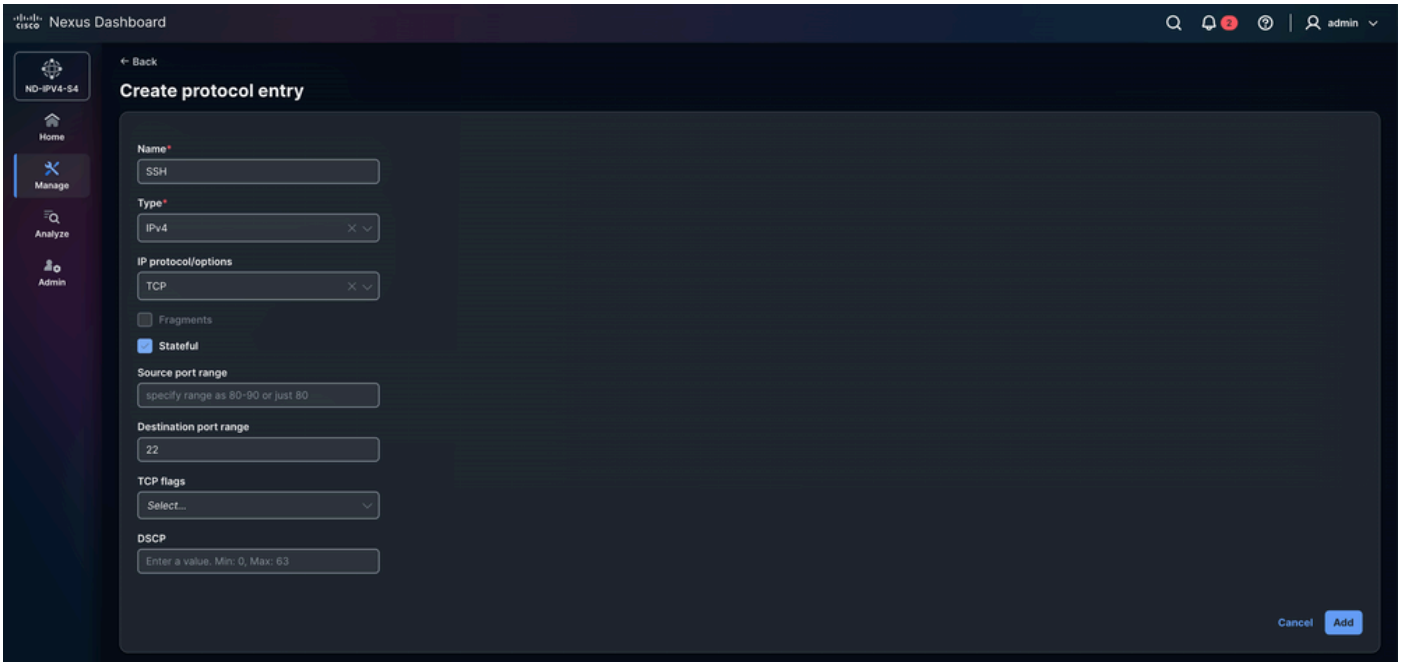
- 名稱:SSH
- 型別：IPv4
    - IP和IPv6也可用。
- IP協定/選項：TCP
    - 支援UDP、EIGRP和PIM等。

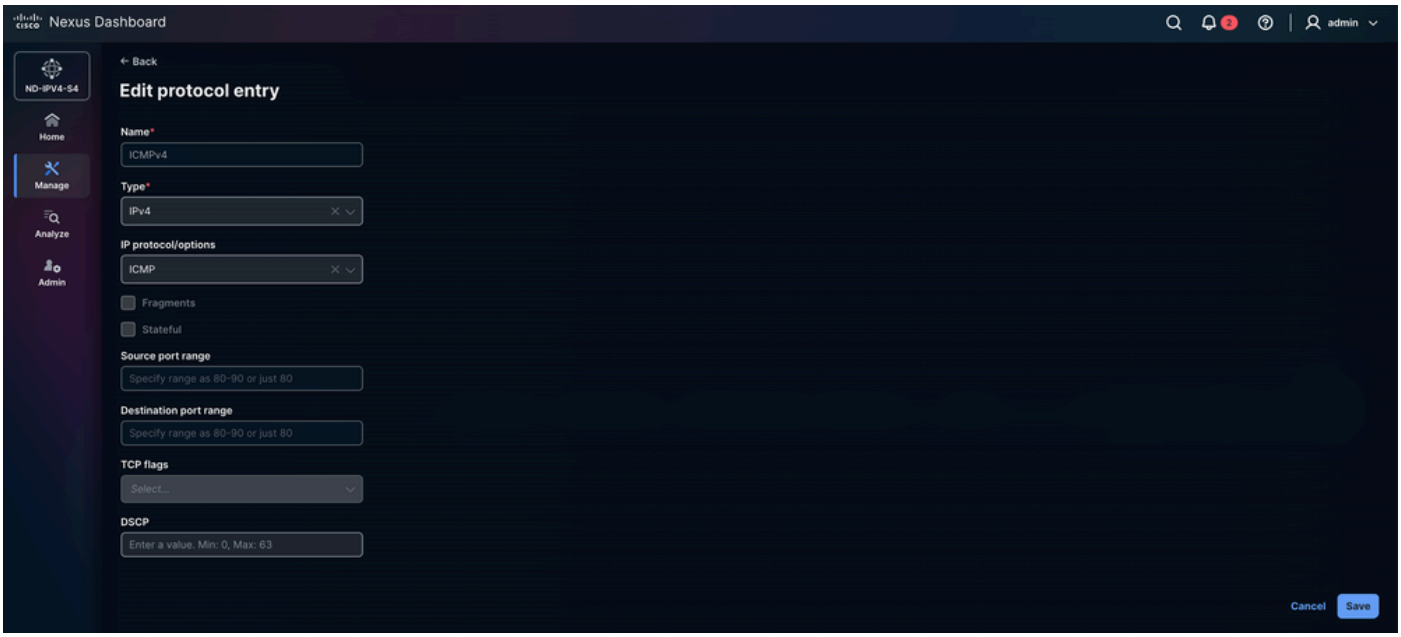
- 片段：允許規則匹配分段的IP資料包。這非常有用，因為超過網路MTU時，大型封包可能會分割為片段。啟用此選項可確保策略也適用於這些片段。

- 有狀態：有狀態進程意味著它跟蹤過去發生的所有更改或互動，並且當前進程是在這些以前的進程的情況下執行的。在這種情況下，TCP會跟蹤一些區域，例如要傳輸的資料包數量、資料包的順序以及接收方是否收到資料包。選擇Stateful選項後，此資訊將儲存為TCP中的狀態。

- 源埠範圍：只有在以上IP協定/選項欄位中選擇了TCP或UDP時，此選項才可用。
- 目的地連線埠範圍：只有在「IP通訊協定/選項」欄位中選擇了TCP或UDP時，此選項才可用。
- TCP標誌
    - 只有在「IP協定/選項」欄位中選擇TCP時，此選項才可用。
    - 它允許您定義安全協定使用的TCP標誌。
    - TCP標誌是TCP報頭的一部分，用於控制連線的建立、維護和終止。
    - 可用選項：
        - ACK（確認）：表示確認接收的資料或同步資料包。

- EST（已建立）：表示已建立的TCP連線。啟用此選項後，不能選擇其他TCP標誌。
- FIN（完成）：用於正常關閉TCP連線。
- RST（重置）：立即終止連線並丟棄所有仍在傳輸的資料。
- SYN（同步）：在TCP連線的發起和建立期間使用。



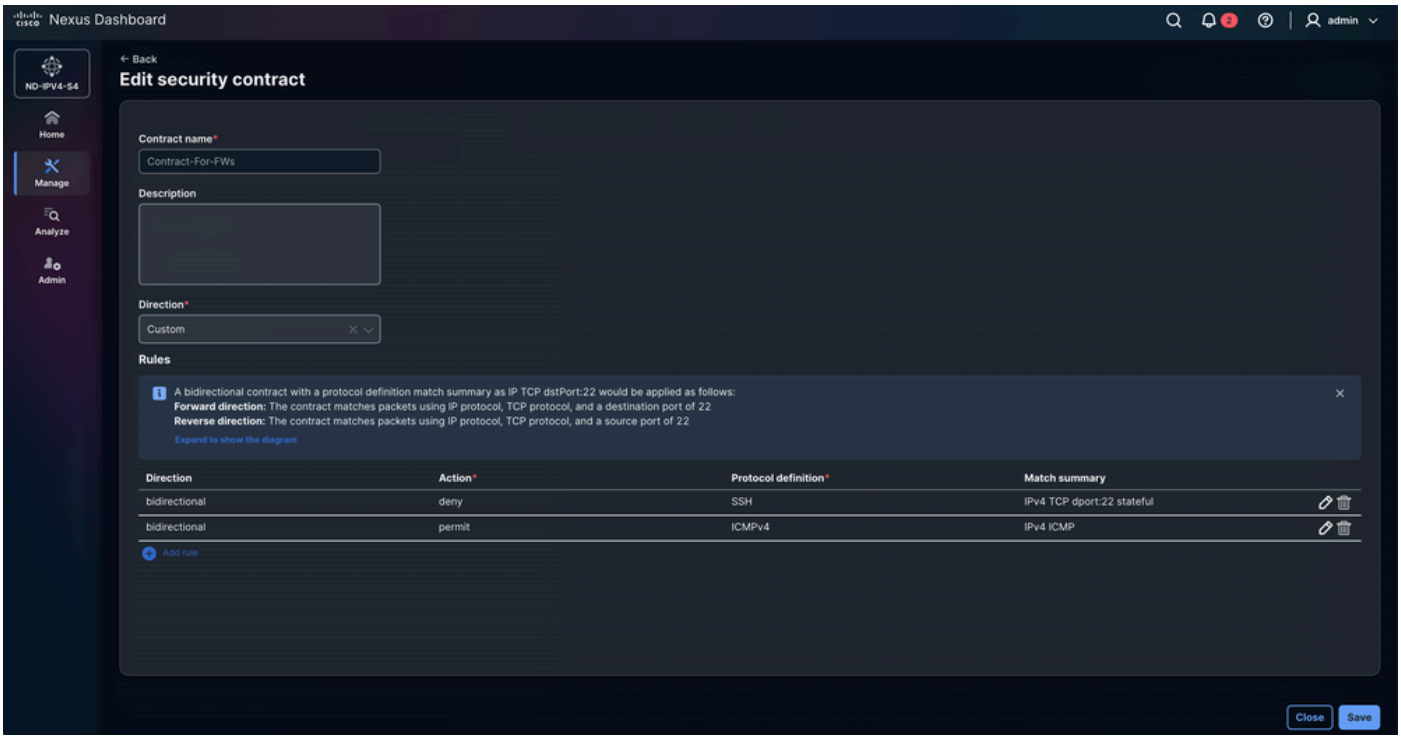


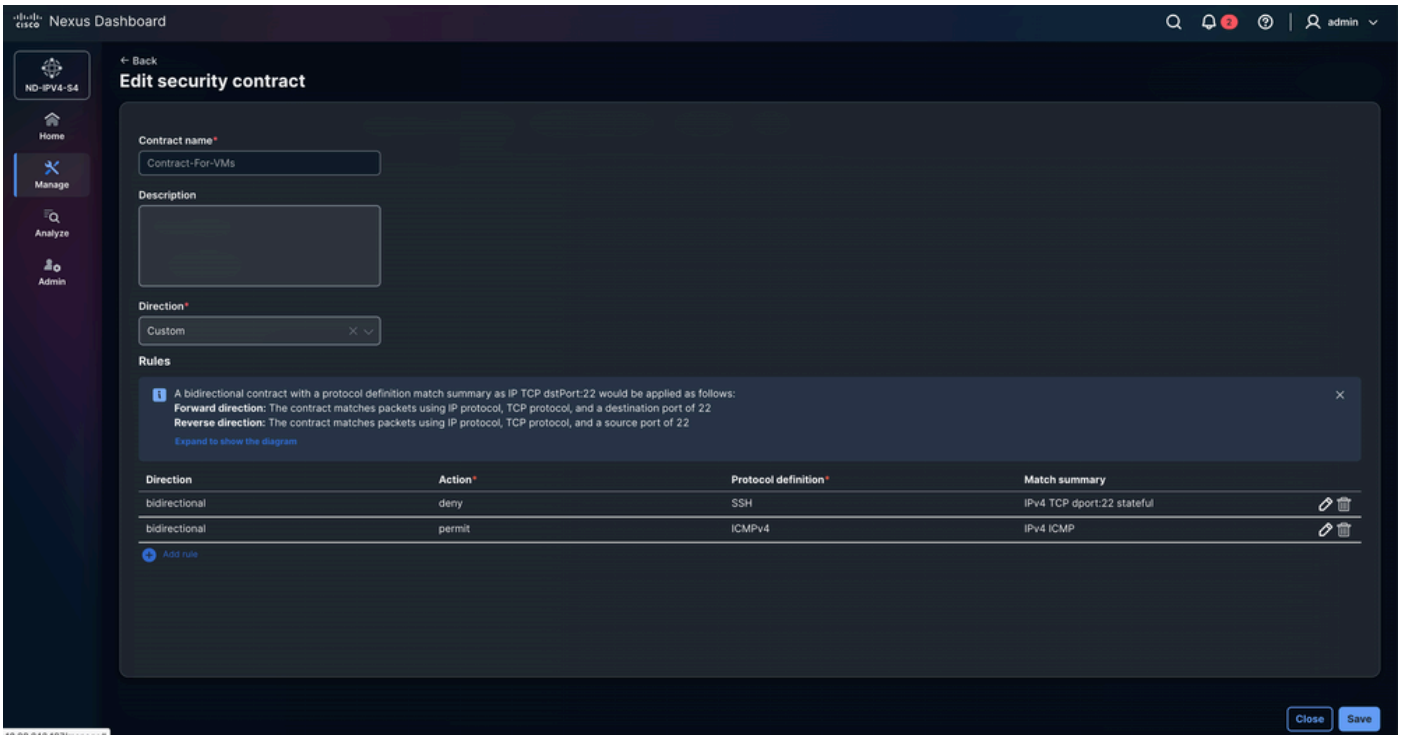
步驟5.設定安全合約

通過根據關聯的策略定義指定允許或拒絕哪些流量，合約定義了終端組之間的通訊規則。它充當實施機制，應用已配置的協定規則、過濾器和操作，確保源組和目標組之間的流量符合預期的安全性和分段策略。

導航到管理>結構>結構組> DAVIDM3 >分段和安全>安全合約>操作>建立安全合約。

- 選擇Add rule並配置Direction、Action和Protocol定義。
  - 雙向：
    - 雙向合約應用如下，協定定義匹配摘要作為IP TCP埠22。
      - Forward direction:合約使用IP協定、TCP協定和目的地埠22匹配資料包
      - 反向方向：合約使用IP協定、TCP協定和源埠22匹配資料包。
      - 這適用於任何來源或目的地。
  - 單向：
    - GPO安全合約中的單向表示僅在資料流的一個方向上實施策略，允許或拒絕從源安全組到目標安全組的通訊，而不在相反方向自動應用同一規則。

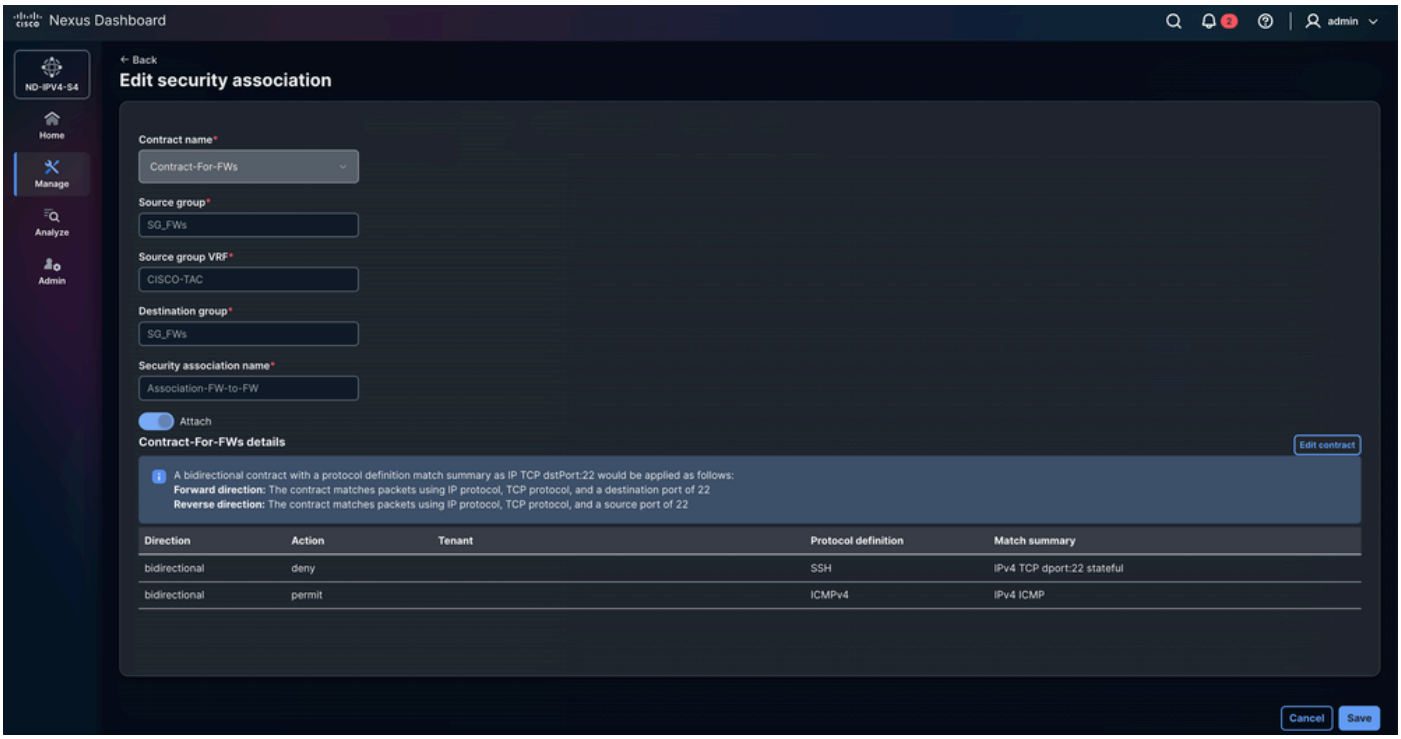


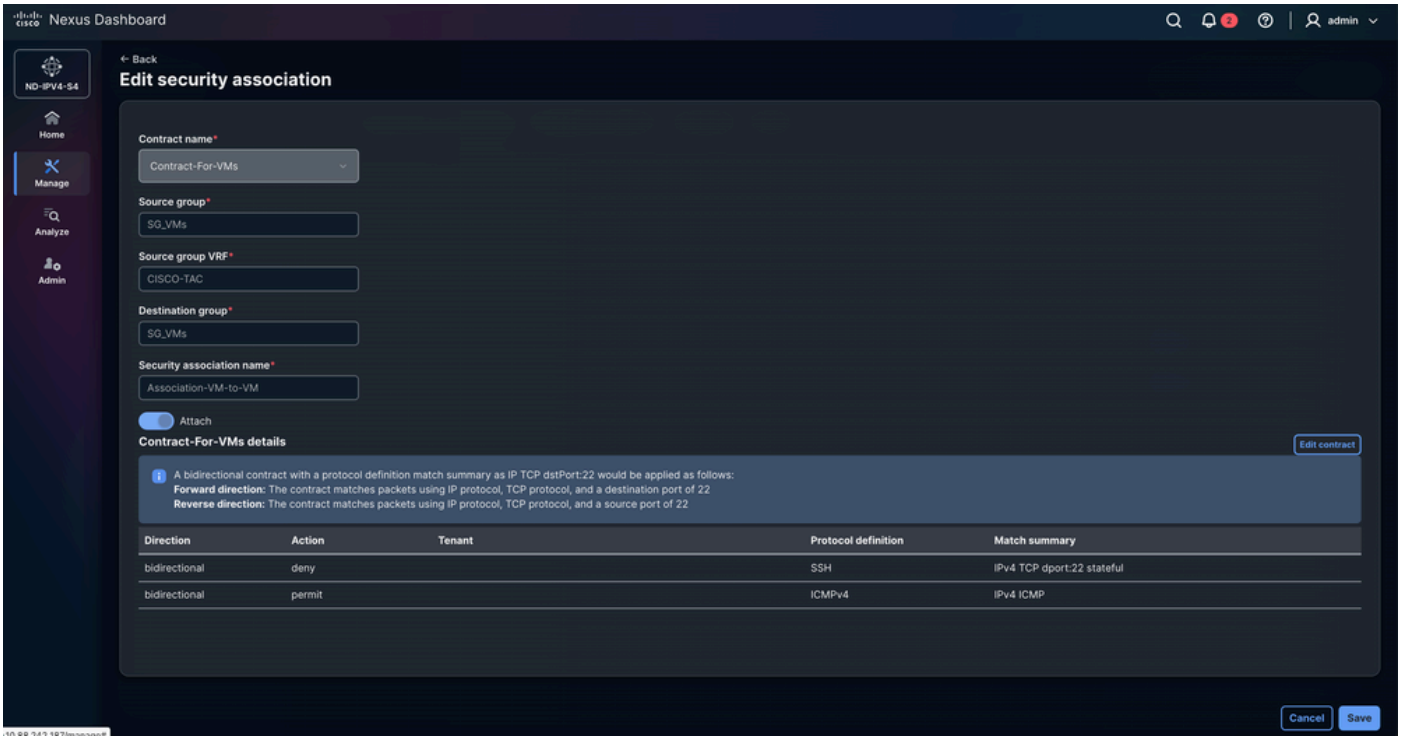


步驟6.配置安全關聯

導航到Manage > Fabric > Fabric groups > DAVIDM3 > Segmentation and security > Security associations > Actions > Create security association。

在配置安全關聯中，通過連結安全組、協定定義和安全合約來定義策略模型。安全組對終端進行分類，協定定義指定流量型別（如協定或埠），安全合約使用這些協定規則定義在源安全組和目標安全組之間應用的策略。安全關聯表示將這些元素繫結在一起的關係，以便交換矩陣可以實施定義的安全策略。

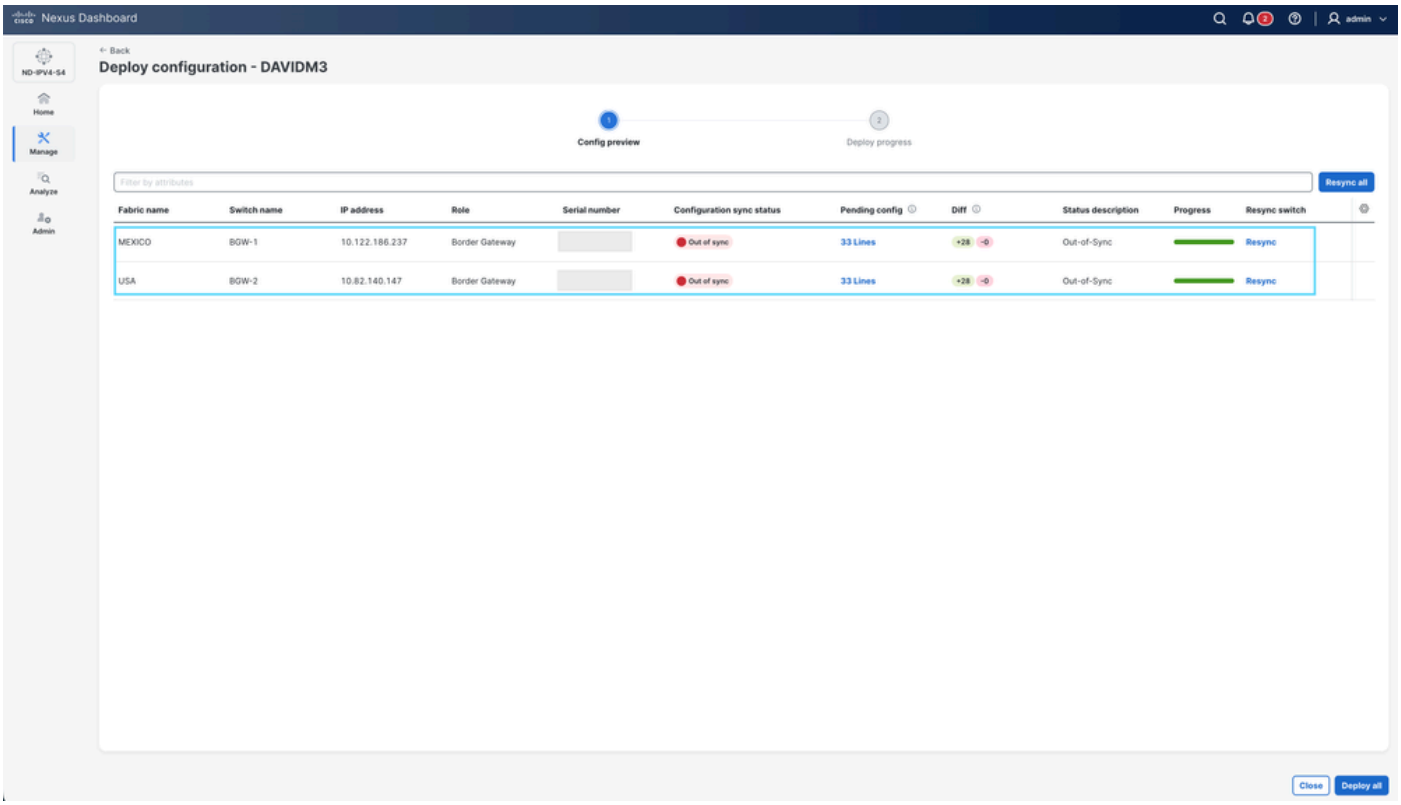


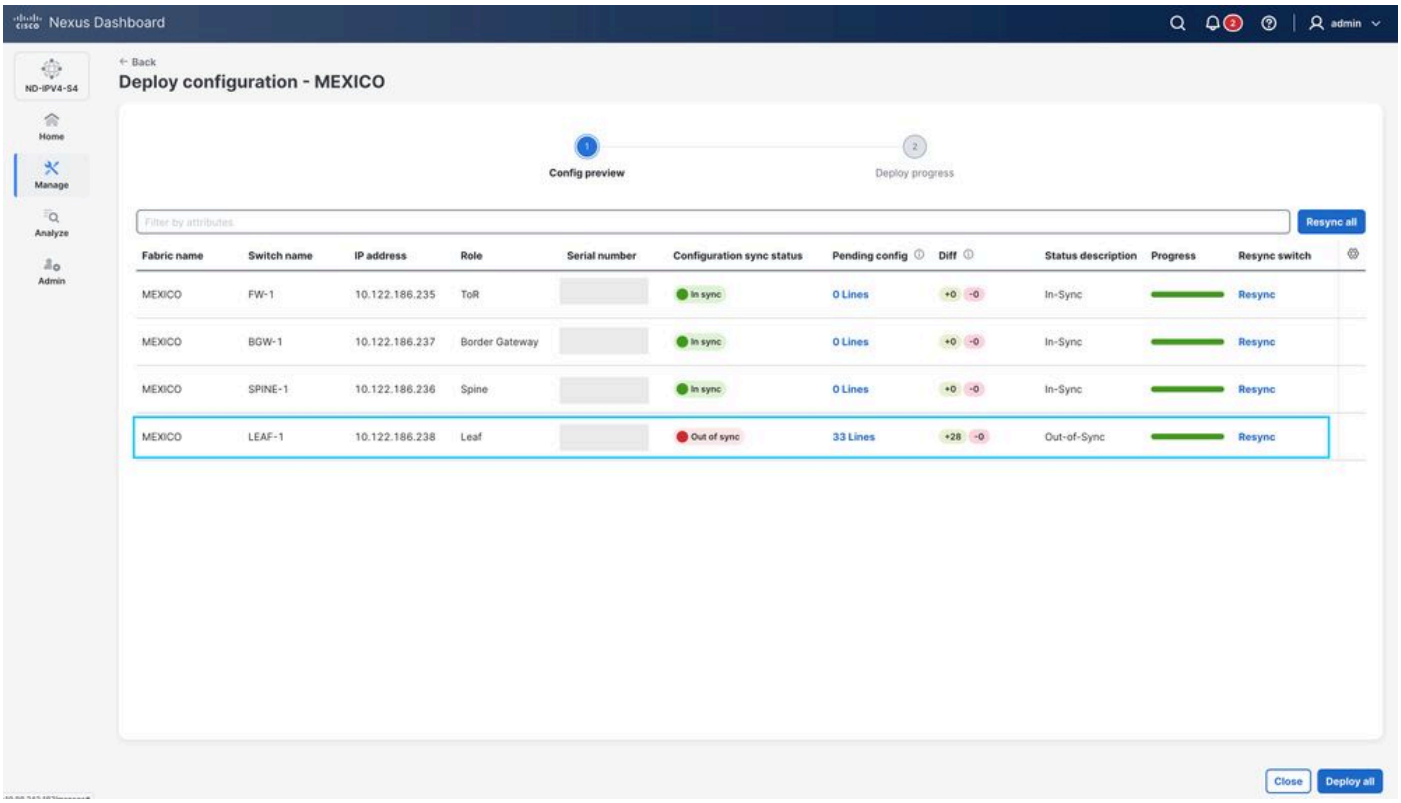


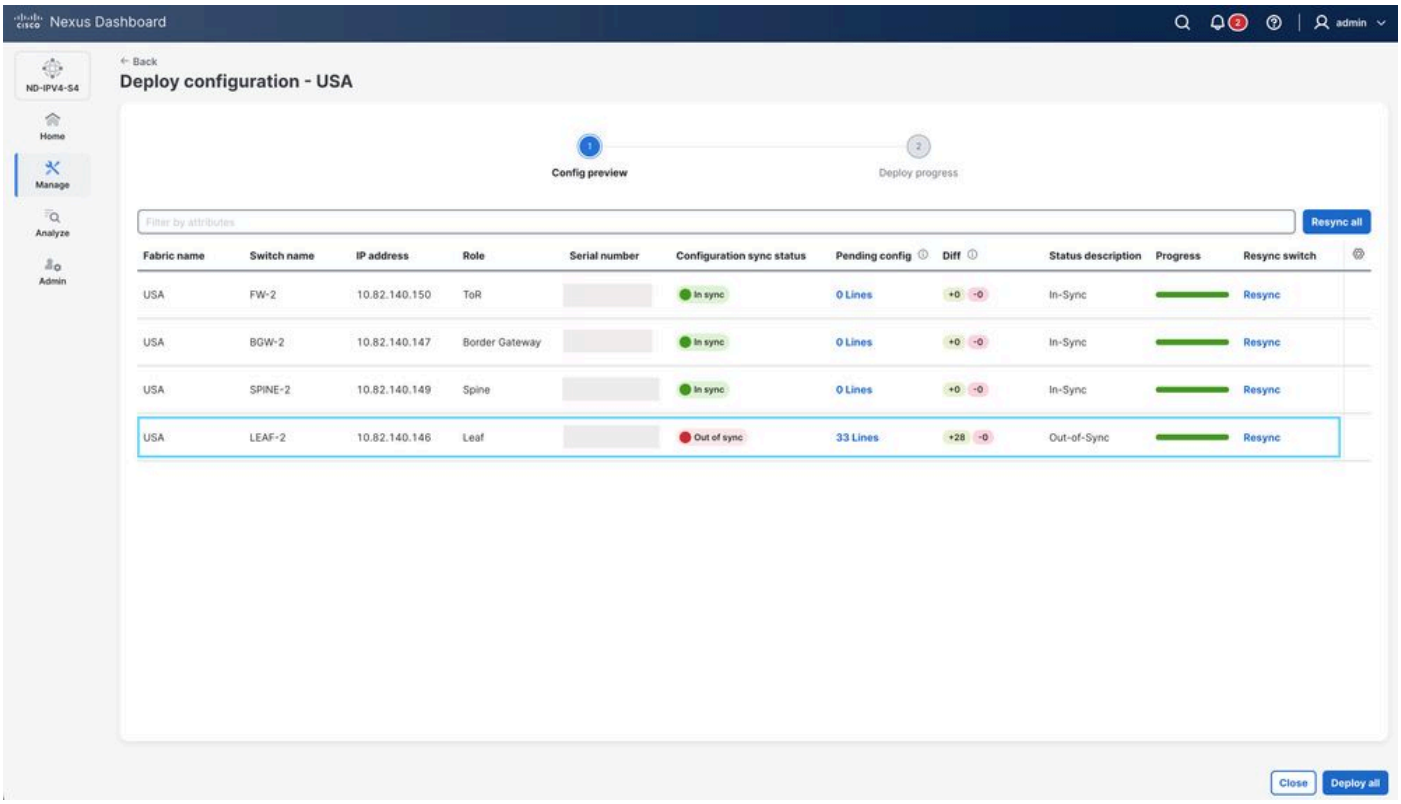
步驟7.驗證GPO配置

- 導航到Manage > Fabric > Fabric groups > DAVIDM3 > Actions > Recalculate and deploy。
  - GPO配置從父交換矩陣交換機推送到邊界網關。點選待處理的配置行數，檢視並驗證可以部署到裝置的配置。必須為每個子交換矩陣重複此過程。
  - 導航到Manage > Fabric > Fabric groups > DAVIDM3 > Inventory > Member fabric > MEXICO > Actions > Recalculate and deploy。
  - 導航到Manage > Fabric > Fabric groups > DAVIDM3 > Inventory > Member fabric >

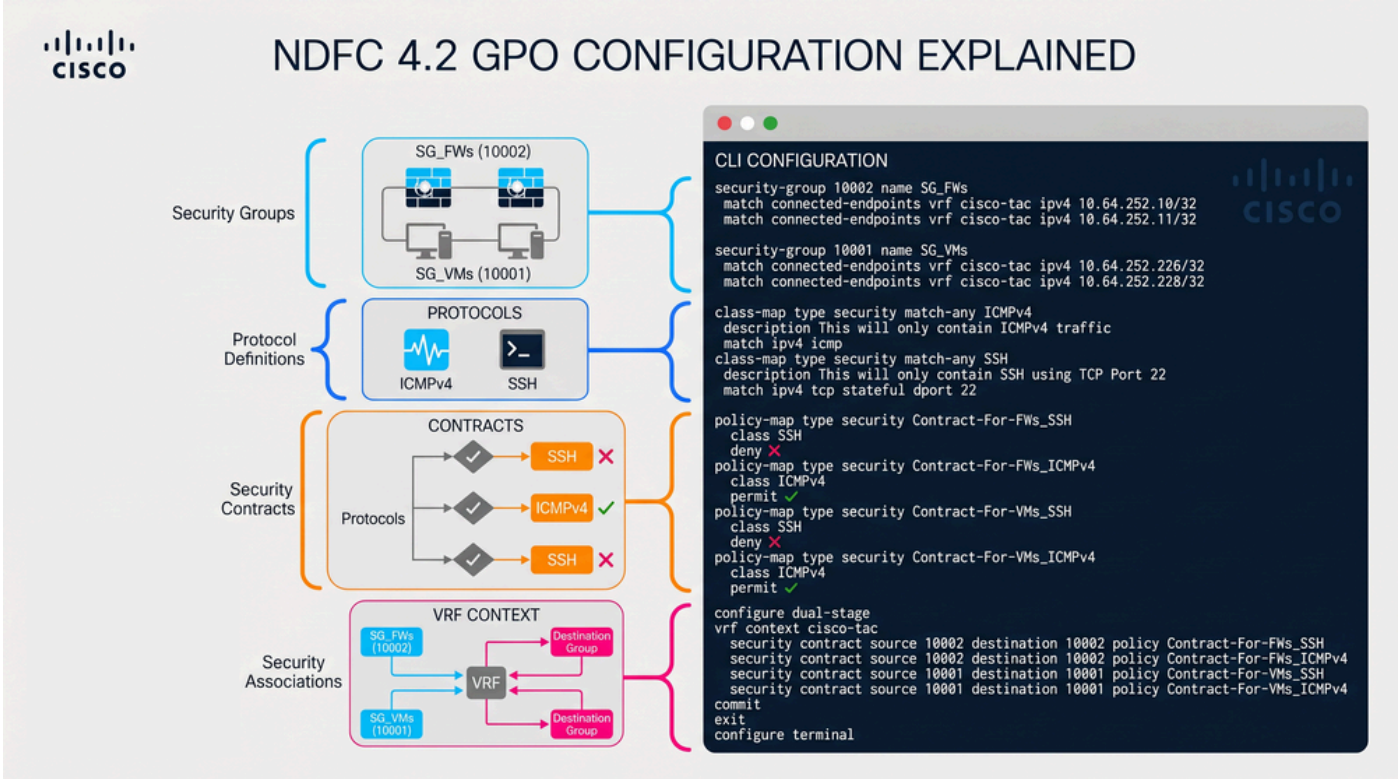
USA > Actions > Recalate and deploy。







- 該圖顯示了BGW-1、BGW-2、LEAF-1和LEAF-2的GPO配置。所有交換機上的配置都相同。NDFC 4.2不按所示確切順序應用配置。本節說明CLI命令的邏輯順序。



疑難排解VXLAN GPO可操作性

步驟1.驗證安全組功能狀態

驗證交換器上是否已啟用安全組功能。VXLAN GPO依賴於此功能，因為它啟用終端分類、合約實施和SGACL硬體程式設計所需的安全組標籤(SGT)基礎設施。

<#root>

BGW-1#

show feature | i i security-group

security-group 1 enabled

步驟2.檢驗系統路由模式

驗證交換機上已配置和運行的系統路由模式。VXLAN GPO需要安全組支援路由模式，因為SGACL實施會消耗ASIC管道內的專用硬體轉發資源。

<#root>

BGW-1#

show system routing mode

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

步驟3.驗證VXLAN NVE對等點建立和GPO功能

- 驗證本地交換矩陣裝置和遠端多站點對等體之間的VXLAN NVE對等體建立。VXLAN GPO資訊通過VXLAN EVPN控制平面傳播，因此跨交換矩陣的安全組標籤(SGT)學習和合約同步需要穩定的NVE鄰接。
- 具有欄位組策略功能是此命令中最重要的指示之一，因為它確認遠端VTEP是否支援跨VXLAN EVPN多站點域的SGT傳播和SGACL合約實施所需的VXLAN組策略擴展。

<#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


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

步驟4.驗證安全組學習和終端分類

驗證終端是否已正確分類為安全組(SGT)。VXLAN GPO實施取決於準確的終端到SGT對映。

<#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
```

步驟5.驗證安全合約和策略實施

驗證VXLAN GPO合約是否正確安裝且可操作。合約定義在安全組之間實施的通訊規則，並代表VXLAN GPO用於微區劃分的核心策略機制。

<#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
```

步驟6.檢驗VRF安全實施狀態

驗證交換機上配置的所有VRF的VXLAN GPO實施狀態。此命令確認SGACL策略和安全組合約是否在租戶VRF中主動實施。

輸出確認cisco-tac VRF正在主動參與VXLAN GPO實施，並且模式設定為強制實施。實施標籤13648用於標識已程式設計到此VRF硬體的內部SGACL策略上下文。預設操作deny log表示未明確允許通過安全組合約的任何流量都會遭到拒絕和記錄，從而實施預設拒絕微分段策略。相反，預設的egress-loadbalance-resolution-management和管理VRF在非強制模式下運行，這意味著這些VRF中不應用VXLAN GPO策略，並且預設情況下允許流量。

欄位Stats跟蹤與VRF安全策略匹配的流量。cisco-tac VRF下的值0表示在執行命令時，沒有不匹配的流量觸發預設拒絕行為，而預設VRF下的計數器值4364表示不執行VXLAN GPO的VRF中的流量活動。

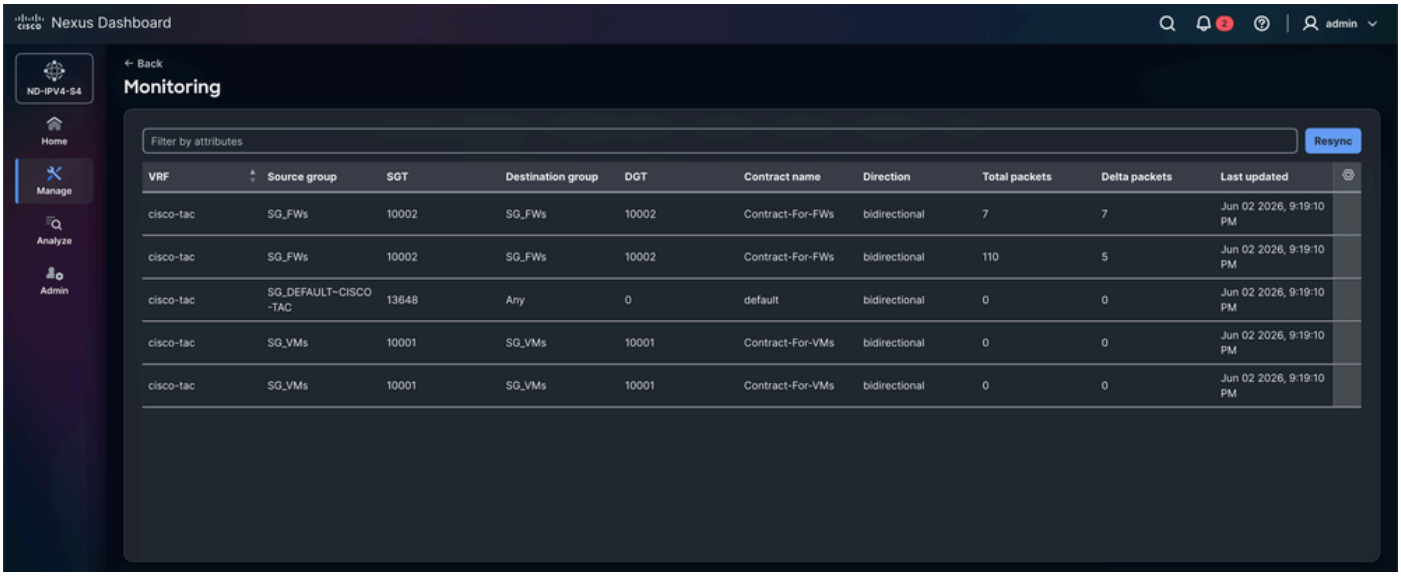
```
<#root>

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
```

步驟7.檢驗VRF安全實施狀態

- 從NDFC GUI驗證VXLAN GPO合約的流量匹配統計資訊。此驗證可確認流量是否主動匹配已配置的安全組合約，以及SGACL實施是否可在VXLAN EVPN多站點交換矩陣間正常運行。
- 在NDFC GUI中，導航至Manage > Fabric > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoring。
  - 此部分提供安全組通訊流、合約命中統計、允許和拒絕操作以及終端組之間的操作合約活動的可視性。
  - 監控統計資訊會在每個監控統計資訊中單獨顯示。

- 來自NDFC的監控統計資訊提供操作驗證層，該層通過確認交換矩陣中的即時策略實施和流量匹配行為來補充基於CLI的故障排除。

附註：第一次嘗試檢視NDFC 4.2中的流量統計資訊時，監控部分最初可能顯示為空。在這種情況下，按Resync按鈕以觸發來自VXLAN交換矩陣的合約統計資訊的同步。同步過程運行時,GUI會顯示消息Resync status:In progress.同步完成後，按Ok按鈕刷新監控檢視。重新同步完成後，與每個安全組合約關聯的流量統計資訊將在監控部分中顯示。若要驗證即時流量匹配行為，請在端點之間生成流量，然後再次按Resync按鈕以更新NDFC中顯示的合約統計資訊。



- 在上一個場景中，終端之間成功允許ICMPv4流量。但是，如果已建立SSH作業階段，則連線會逾時，因為VXLAN GPO合約明確拒絕目的地為連線埠22的TCP流量。

<#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
```

相關資訊

Cisco Nexus 9000系列NX-OS VXLAN配置指南，版本10.6(x)

使用VXLAN GPO通過微分段保護資料中心

使用VXLAN組策略選項(GPO)在Cisco NX-OS VXLAN EVPN交換矩陣中部署微分段

使用組策略選項(GPO)和Nexus控制面板在VXLAN EVPN交換矩陣中自動執行微分段和部署第4-7層服務

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。