使用NDFC 4.2在Nexus多站点交换矩阵上配置GPO

目录

简介

本文档介绍在运行NX-OS和NDFC 4.2的Nexus云扩展交换机上的VXLAN多站点交换矩阵中的GPO配置和验证。

先决条件

要求

思科建议您了解以下方面：

- 虚拟可扩展局域网(VXLAN)、以太网虚拟专用网(EVPN)和多站点交换矩阵技术
- Cisco Nexus云扩展交换机和NeXus操作系统(NX-OS)操作
- Nexus交换矩阵网络控制器(NDFC)4.2管理和部署工作流程
- 网络分段和安全策略概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

了解VXLAN EVPN交换矩阵中的GPO功能

组策略选项(GPO)是一种基于策略的分段机制，旨在根据逻辑身份而不是仅依赖IP地址、VLAN或子网来控制终端之间的通信。GPO的主要目的是简化安全策略实施，并在应用、服务器或工作负载之间提供可扩展的微分段。

一个简单的类比是假设一家酒店，其中每位宾客都属于特定类别或访问级别，某些区域仅允许特定宾客访问，并且访问权限取决于宾客的角色而不是房间号码。GPO的工作方式非常相似。GPO不是将终端完全视为IP地址，而是将其分类为安全组(SG)。 然后，在这些组之间应用策略，以确定允许或拒绝哪些通信。

例如：

- Web服务器可以属于一个安全组。
- 应用服务器可以属于另一个安全组。

- 数据库服务器可以属于受限制的安全组。

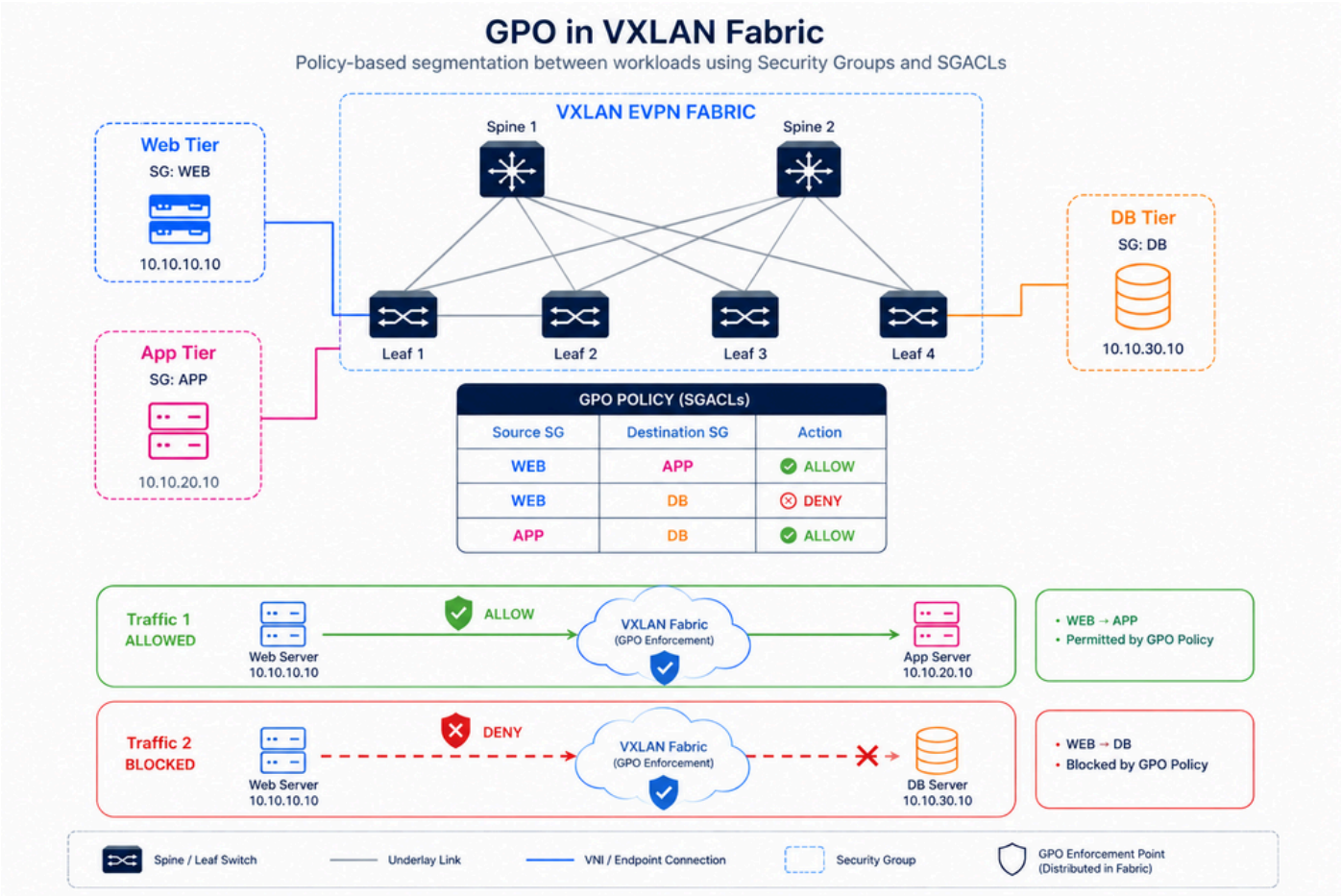
然后，策略可以定义：

- Web服务器可以与应用服务器通信。
- 应用程序服务器可以与数据库服务器通信。
- Web服务器无法与数据库服务器直接通信。

此方法简化了操作，因为管理员不再需要跨多个设备和VLAN维护大量ACL。

另一个主要优势是可扩展性。在大型环境中，工作负载经常移动、动态扩展或更改IP地址。即使端点位置发生变化，GPO也允许安全策略保持一致。在VXLAN EVPN交换矩阵内，GPO通过跨交换矩阵分发安全组信息以及在端点之间实施安全组ACL(SGACL)来扩展此概念。这在现代数据中心中变得尤为重要，因为工作负载之间的东 — 西流量通常代表最大的攻击面。GPO通过限制数据中心交换矩阵内不必要的通信路径来改善安全状况。

有关GPO架构、微分段概念和VXLAN策略实施的更深入技术了解，请参阅思科白皮书：使用 [VXLAN GPO通过微分段保护数据中心]



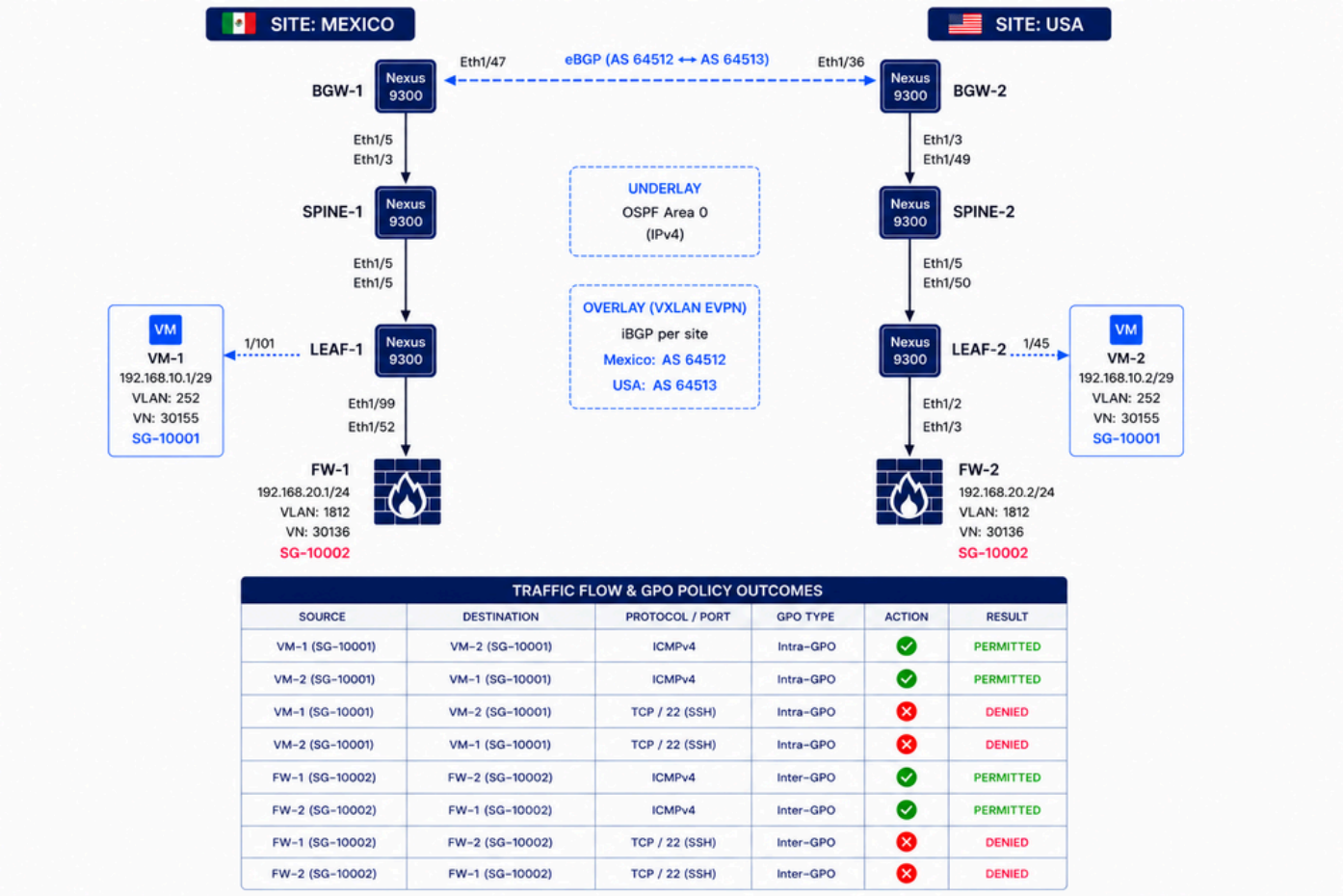
VxLAN交换矩阵中的GPO

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

此拓扑表示在两个地理上分散的站点上部署的VXLAN多站点交换矩阵：墨西哥和美国。每个站点都包含专用BGW、主干交换机、枝叶交换机、虚拟机和防火墙网段，这些网段在运行NX-OS 10.6(3)F的Cisco Nexus 9300交换机上运行。底层网络使用开放最短路径优先(OSPF)，而重叠控制平面在每个站点内使用iBGP，在BGW-1和BGW-2之间使用eBGP进行站点间VXLAN EVPN通信。由于此环境是实验室部署，因此墨西哥和美国站点通过两个BGW之间的直接连接链路互连，以简化多站点连接模型。

GPO用于在安全组(SG)之间实施基于策略的微分段，独立于IP编址或VLAN边界。根据连接策略表，允许从VM-1到VM-2、FW-1和FW-2的ICMP流量，而拒绝从VM-1到FW-1和FW-2的TCP端口22(SSH)流量。VM-1和VM-2之间的TCP端口22通信仍然被允许，因为两个终端属于同一安全组(SG-10001)。 此行为演示GPO如何在VXLAN多站点交换矩阵上的GPO内和GPO间通信之间动态实施不同的流量策略。

注意：Cisco NX-OS版本10.6(3)F引入了使用ESG内隔离功能限制同一ESG（也称为SG）内终端之间的通信。此功能可最大程度降低ESG内未经授权的访问风险，并增强安全状态。



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交换矩阵中使用NDFC 4.2分步配置GPO

当VXLAN多站点交换矩阵已运行并配置了NDFC 4.2，并且以后需要实施GPO时，将应用这些步骤。使用Nexus控制面板的使用VXLAN GPO通过微分段保护数据中心部分显示了从创建VXLAN单站点交换矩阵开始的配置。

⚠ 警告：当GPO在VXLAN EVPN交换矩阵中运行时，仅当存在目标可达性且安全策略允许流量时，才会进行通信。策略实施依赖IP信息，IP信息需要ARP条目和SVI才能用于内部网络。这意味着属于租户VRF的VLAN必须配置SVI。因此，实施不适用于仅包含第2层报头的流量，因此不能与VXLAN第2层扩展一起使用。NX-OS版本10.6(2)F引入了基于MAC的微分段支持。

步骤1.在父交换矩阵中启用安全组

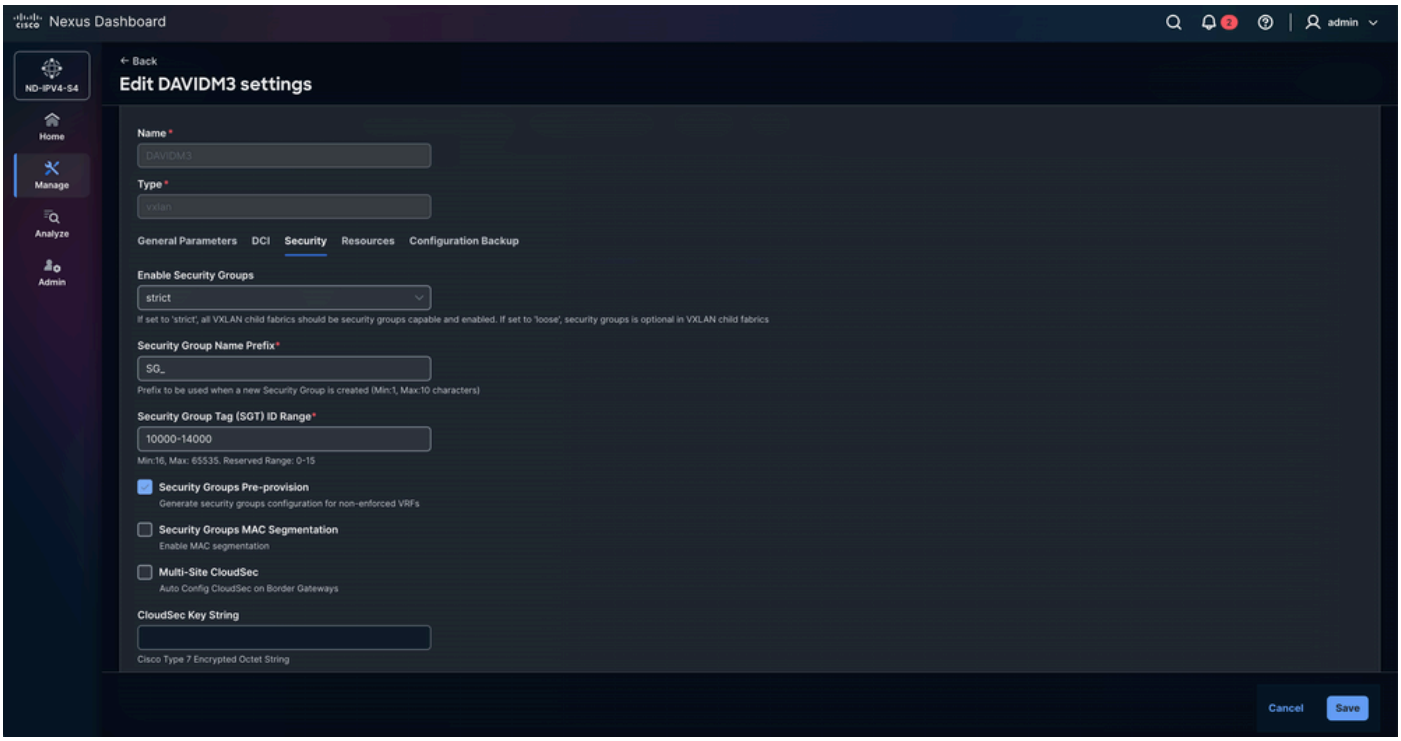
- 导航到Manage > Fabric Groups，选择交换矩阵组DAVIDM3，然后选择Actions > Edit Fabric Group Settings。在Security部分中，启用Security Groups，将模式设置为Strict，并设置Security Groups预调配。
  - 选择关注的交换矩阵组。在本示例中，所选交换矩阵组称为DAVIDM3，它也是多站点交

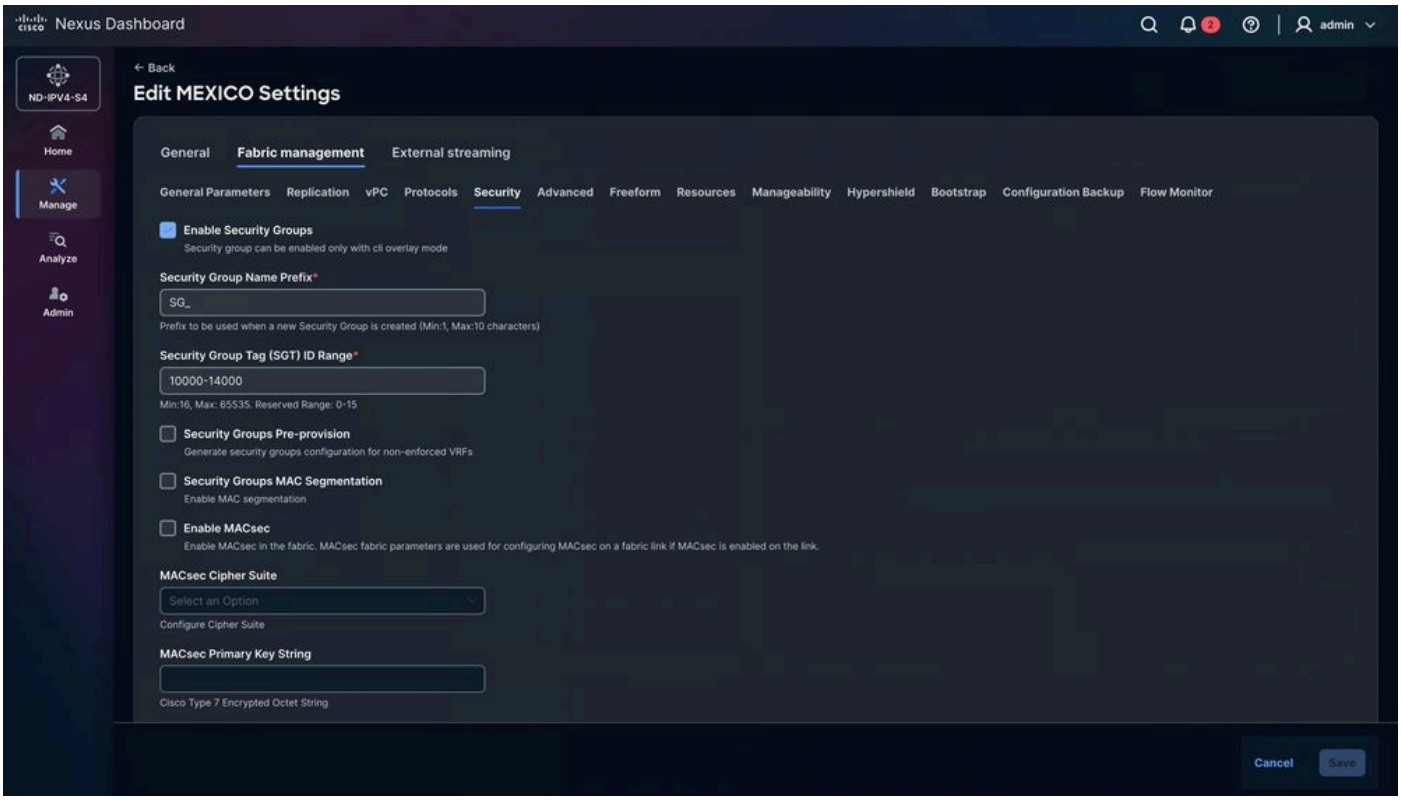
换矩阵的名称。

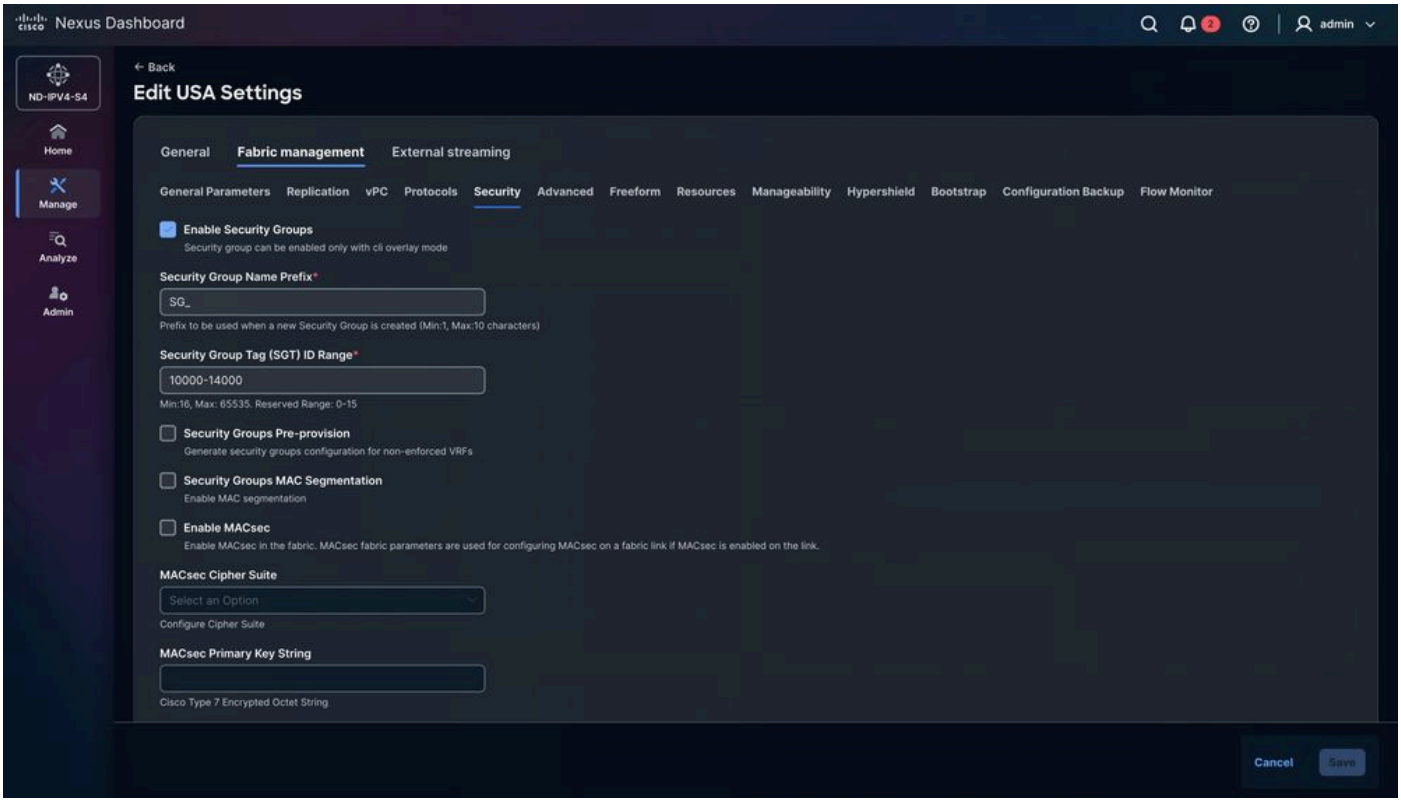
- 对每个子交换矩阵重复这些步骤。
  - 导航到管理>交换矩阵，选择USA，然后导航到操作>编辑交换矩阵组设置。在Security部分中，启用Security Groups并将模式设置为Strict。
  - 导航到管理>交换矩阵，选择MEXICO，然后导航到操作>编辑交换矩阵组设置。在Security部分中，启用Security Groups并将模式设置为Strict。

注意：如果设置为strict，则所有VXLAN子交换矩阵都必须支持并启用安全组。如果设置为松散，则安全组在VXLAN子交换矩阵中是可选的。

提示：要保持清晰的可视性，请在父交换矩阵和所有子交换矩阵中使用相同的安全组标记(SGT)ID范围。父交换矩阵范围必须涵盖所有子交换矩阵使用的范围。







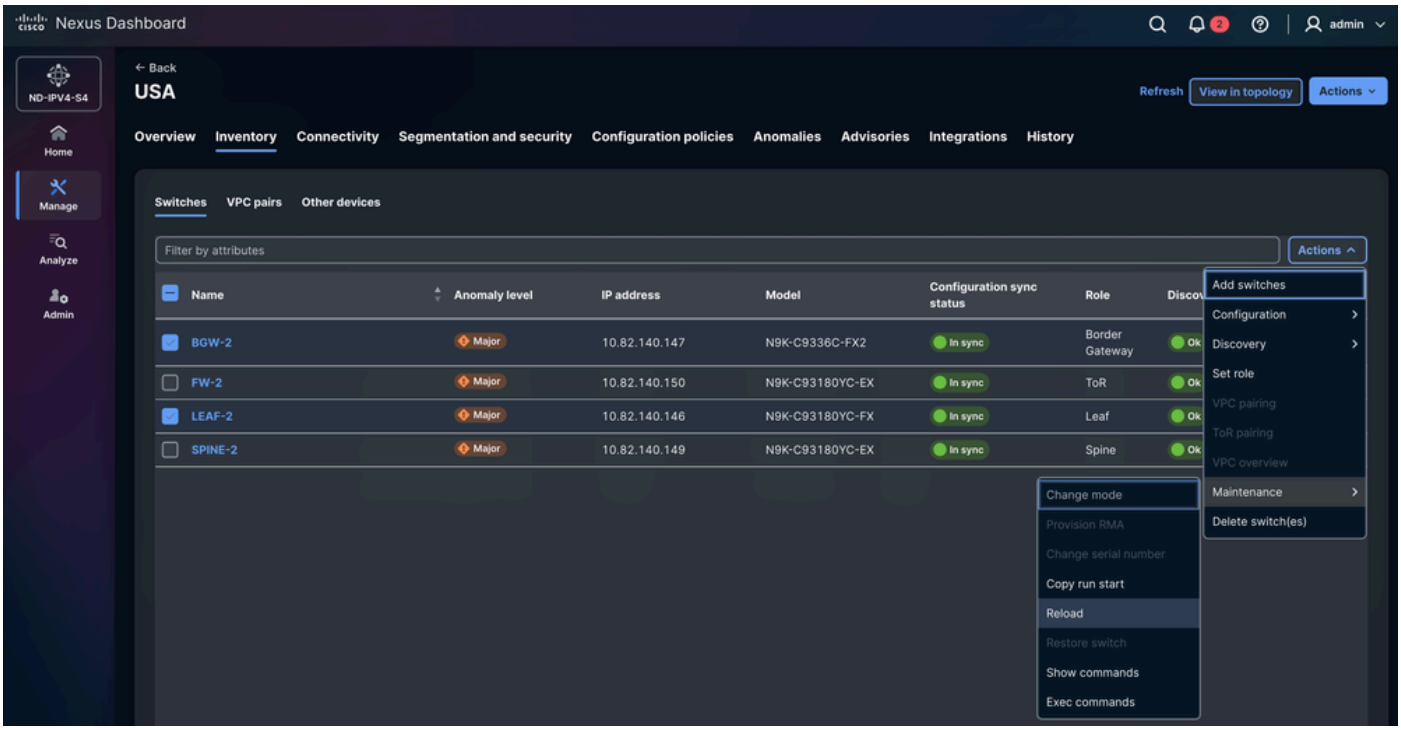
步骤2.重新计算交换矩阵配置并重新加载GPO部署的交换机

NDFC会根据特定Nexus交换机的角色自动提示您重新加载该组。在本示例中，必须重新加载LEAF-1、LEAF-2、BGW-1和BGW-2。此操作必须由网络管理员手动执行。需要重新加载，无法跳过重新加载，因为GPO需要TCAM刻划。

注意：如果设备未重新加载，TCAM更改可能出现在运行配置中；但是，由于交换机尚未重新启动，因此该设置不会应用于硬件内存。因此，该功能无法按预期运行。

要重新加载Nexus交换机，请执行以下操作：

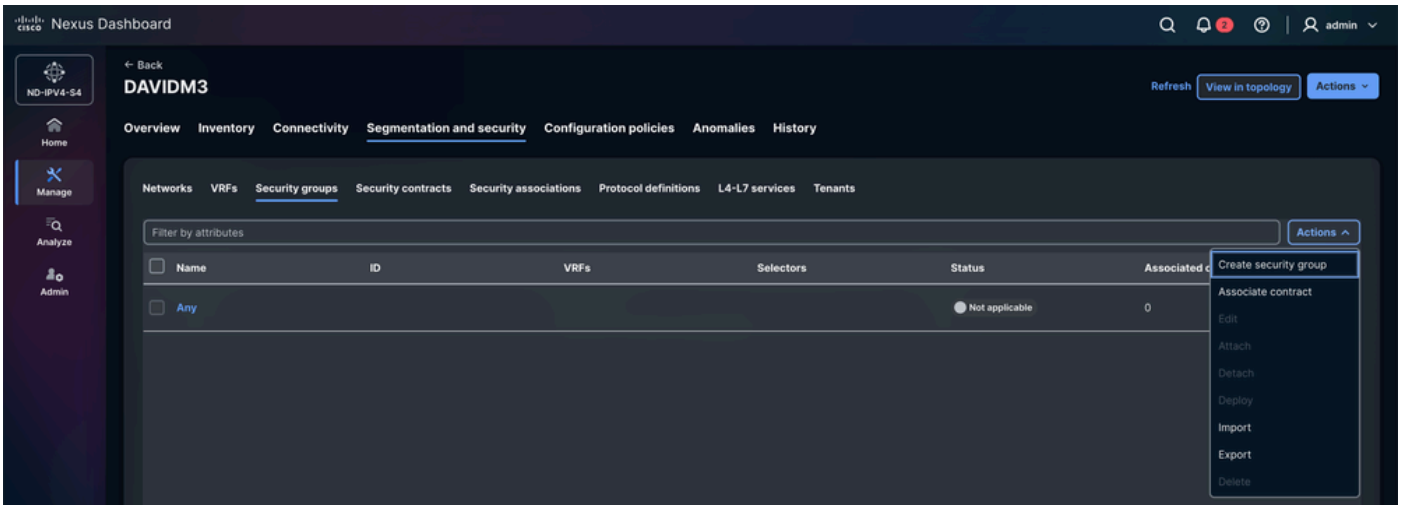
导航到管理>交换矩阵>墨西哥/美国>资产>交换机> LEAF-1 / LEAF-2 / BGW-1 / BGW-2 >操作>维护>重新加载。



步骤3.创建安全组

定义每个终端的安全组。VXLAN交换矩阵中的每个终端可以有一个安全组。这种方法不能有效扩展。对终端进行全局分组（虚拟机、防火墙、TCP优化器等）。

导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >分段和安全>安全组>操作>创建安全组。



第3.1步配置安全组名称

- NDFC自动分配一个随机名称，名称可以更改；建议使用便于终端识别的代表性名称。
- 在这种情况下：
  - VM -> SG_VM
  - FW -> SG_FWs

第3.2步配置VRF

- 选择终端所属的租户(VRF)。
- 在这种情况下：虚拟机和防火墙属于CISCO-TAC租户。

可选，创建VRF。

默认情况下，新创建的租户VRF将策略实施模式设置为Unenforced。在此状态下，即使配置安全组之间的分类标准和SGACL，也不会执行策略。要激活SGACL实施，必须在实施模式下显式配置VRF。

当VRF在强制模式下运行时，会定义默认策略行为：

- 拒绝：除非允许规则明确允许，否则会丢弃所有单播流量。
- 允许：除非拒绝规则明确阻止，否则允许所有单播流量。

属于同一安全组的终端可以相互通信，无需SGACL规则。SGACL仅在不同的安全组之间定义安全策略。

Cisco NX-OS版本10.6(3)F引入了限制同一GPO内终端之间通信的功能，也称为GPO内隔离功能。

在此版本之前，将忽略应用于同一安全组内终端的规则，默认情况下允许流量。

第3.3步配置安全组标记ID

NDFC自动从交换矩阵配置中的预定义范围分配随机标记ID。虽然可以手动选择标记ID，但它必须位于为子交换矩阵和父交换矩阵定义的范围内。

在这种情况下：

- VM-1和VM-2:10001
- FW-1和FW-2:10002

第3.4步配售

如果未启用Attach选项，则安全组不会应用于CISCO-TAC租户。

第3.5步配置选择器

- 选择器确定哪些终端和外部IP地址与特定安全组关联。

NDFC 4.2本地支持三种类型的选择器：

1)IP选择器：IP选择器根据IP信息将终端或IP子网与安全组相关联。

a. 连接的终端 — 标识直接连接到交换矩阵的终端，例如虚拟机、服务器或连接到枝叶交换机的物理主机。
b. 外部子网 — 将外部IP前缀与安全组关联。此类型用于存在于VXLAN交换矩阵之外的网络，例如外部数据中心、WAN网段或面向互联网的网络。源自或发往这些前缀的流量使用已配置的安全组进行分类。

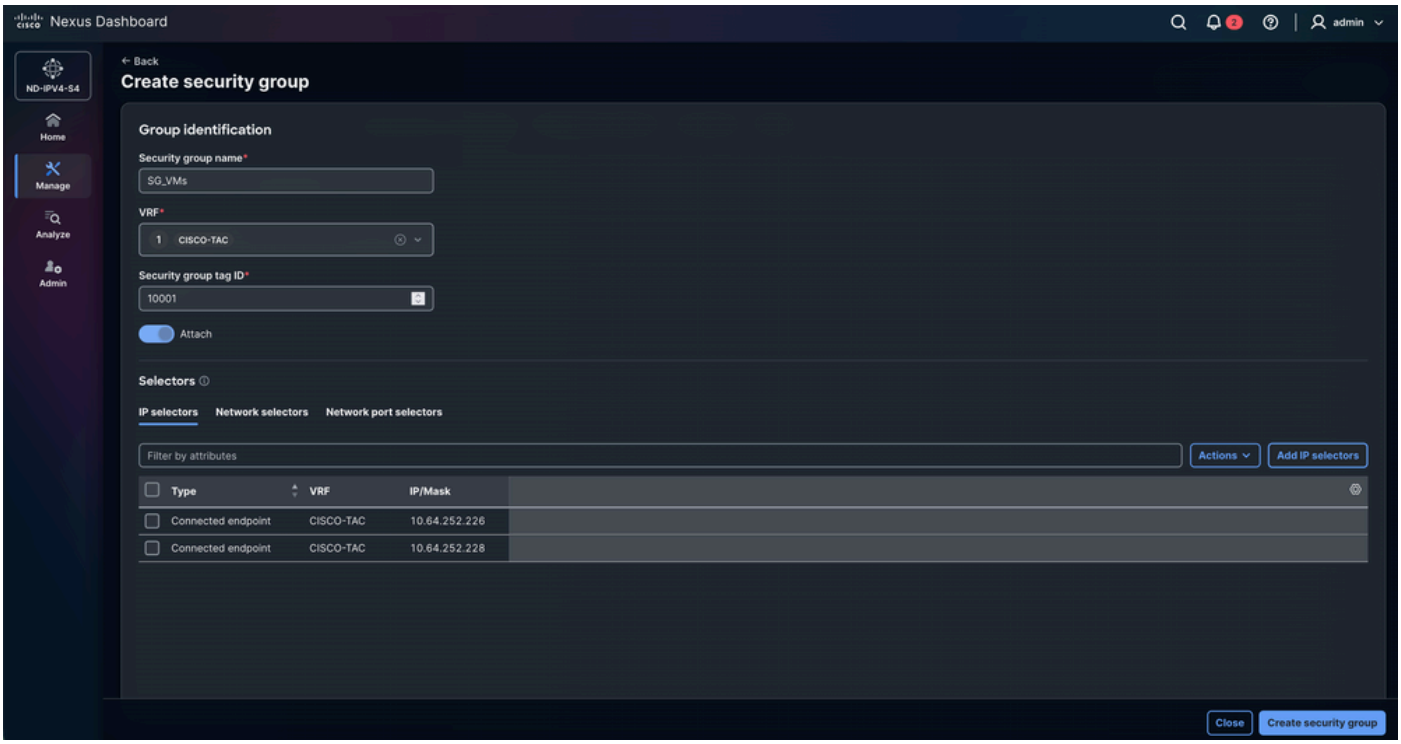
2)网络选择器：网络选择器将安全组与特定VXLAN网段关联。基于网络标识符(L2VNI)应用分类。属于该网络的所有终端都继承分配的安全组，这样当多个终端共享同一网段时，可以简化策略部署。

3)网络端口选择器：网络端口选择器根据流量进入交换矩阵的物理交换机接口对流量进行分类。可将安全组分配给在特定端口或接口上接收的流量。此方法通常用于通过外部网络、服务设备或基础设施链路连接的设备，在这些设备上终端IP分类不可行。

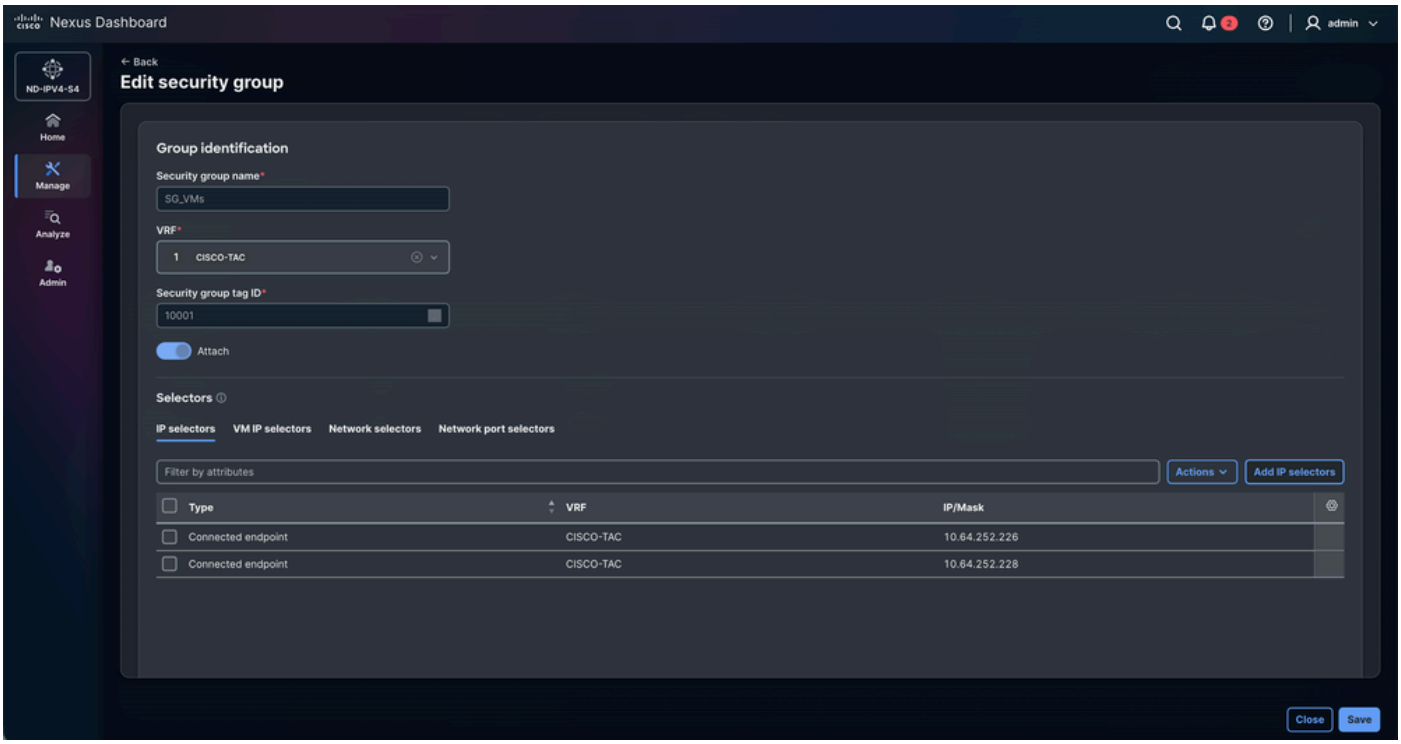
安全组配置摘要

设备	安全组名称	VRF	安全组标记ID	选择器
VM-1	SG_VM	CISCO-TAC	10001	IP选择器
VM-2	SG_VM	CISCO-TAC	10001	IP选择器
FW-1	SG_FWs	CISCO-TAC	10002	IP选择器
FW-2	SG_FWs	CISCO-TAC	10002	IP选择器

VM的安全组配置



防火墙的安全组配置



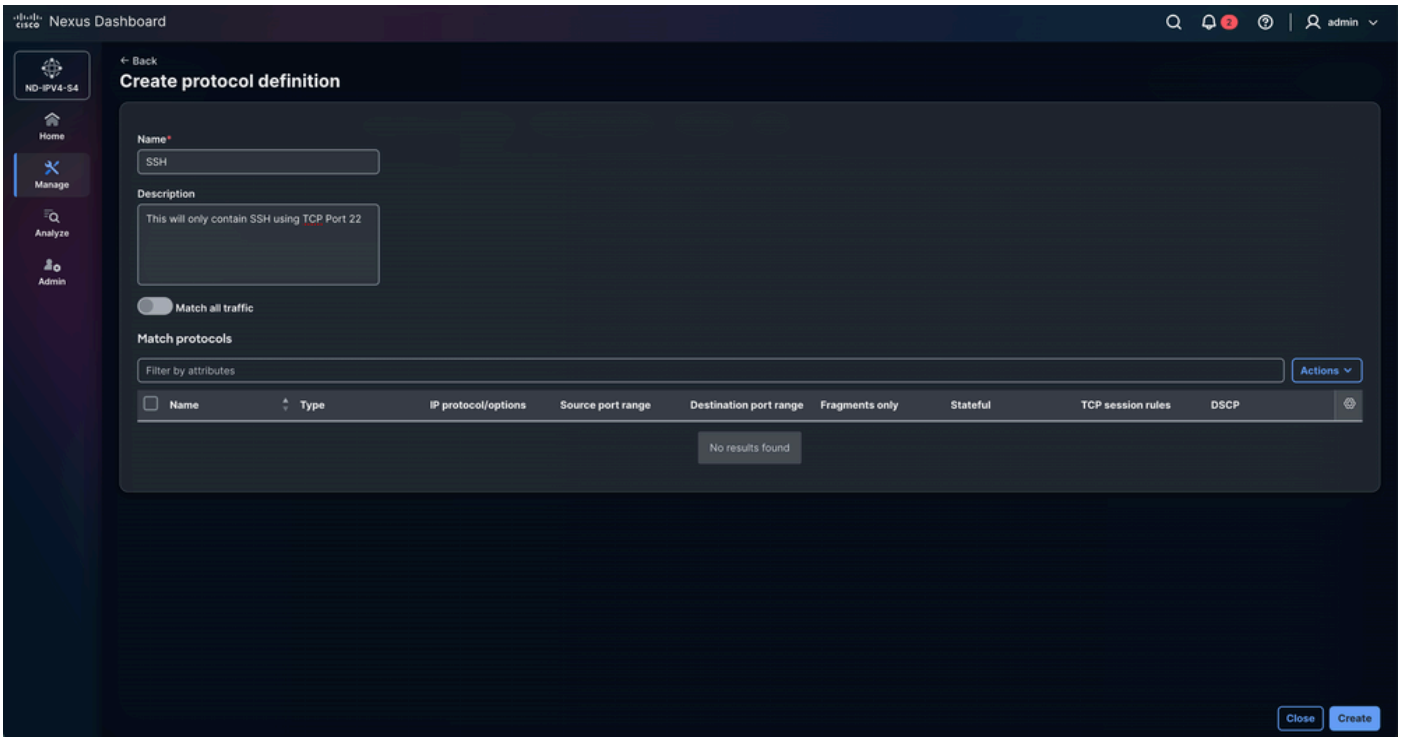
步骤4.配置协议定义

Create Protocol Definition选项用于定义与组策略对象(GPO)匹配的网络协议参数和流量特征。 它允许管理员指定协议类型、端口号和其他数据包属性等条件，以便可以将相应的策略应用于所需的流量。

在此场景中，目标是仅允许ICMP流量，同时明确阻止端口22(SSH)上的TCP流量。 此策略可确保允许网络连通性测试，同时手动限制未经授权或不想要的SSH访问。

导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >分段和安全>协议定义>操作>创建协议定义。

输入名称和说明。



导航到操作>创建协议条目。

- 名称：SSH
- 类型：IPv4
  - IP和IPv6也可用。
- IP协议/选项：TCP
  - 支持UDP、EIGRP和PIM等。

- 分段：允许规则匹配分段的IP数据包。这很有用，因为当超过网络MTU时，大型数据包可以拆分为多个分段。启用此选项可确保策略也适用于这些分段。

- 有状态：有状态的进程意味着它跟踪过去发生的所有更改或交互，当前进程是在与这些以前的进程相关的环境中执行的。在这种情况下，TCP会跟踪一些区域，例如要传输的数据包数量、数据包的顺序以及接收方是否收到数据包。选择Stateful选项后，此信息将存储为TCP中的状态。

- 源端口范围：仅当在上面的IP协议/选项字段中选择了TCP或UDP时，此选项才可用。
- 目标端口范围：只有在IP协议/选项(IP Protocol/Options)字段中选择TCP或UDP时，此选项才可用。
- TCP 标记

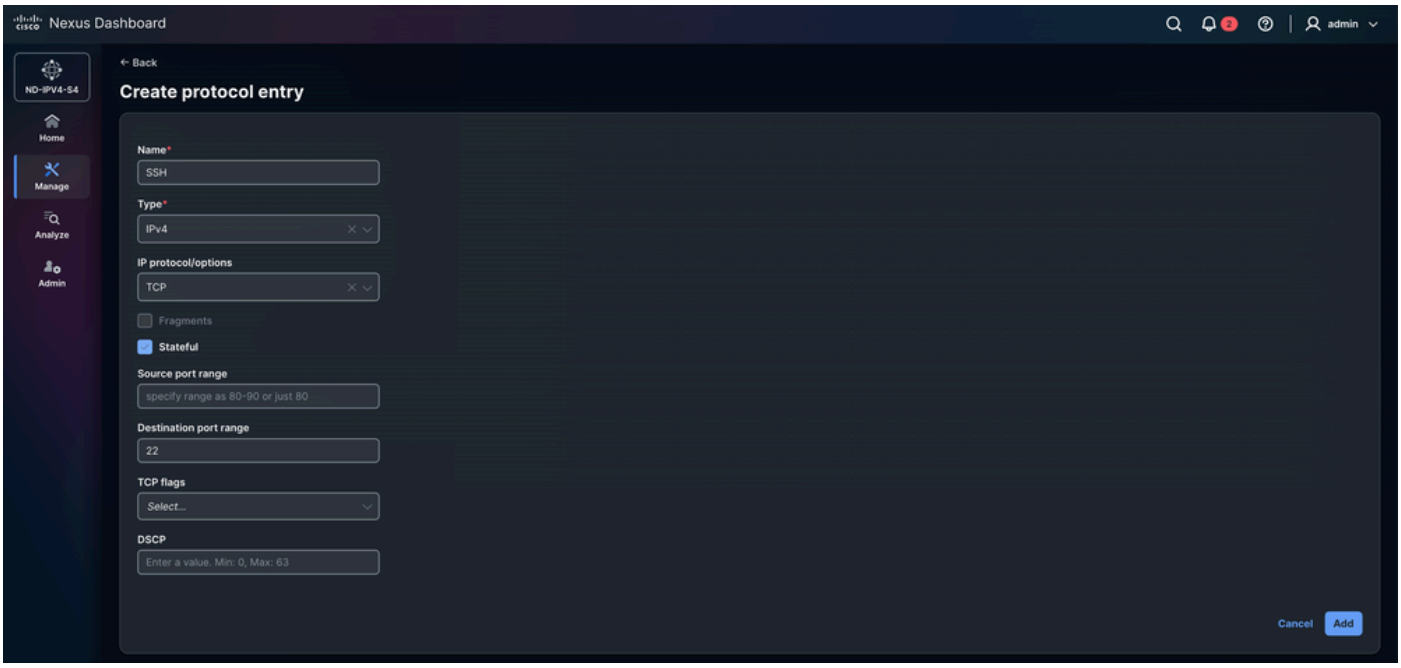
  - 此选项仅在IP协议/选项(IP Protocol/Options)字段中选择TCP时可用。

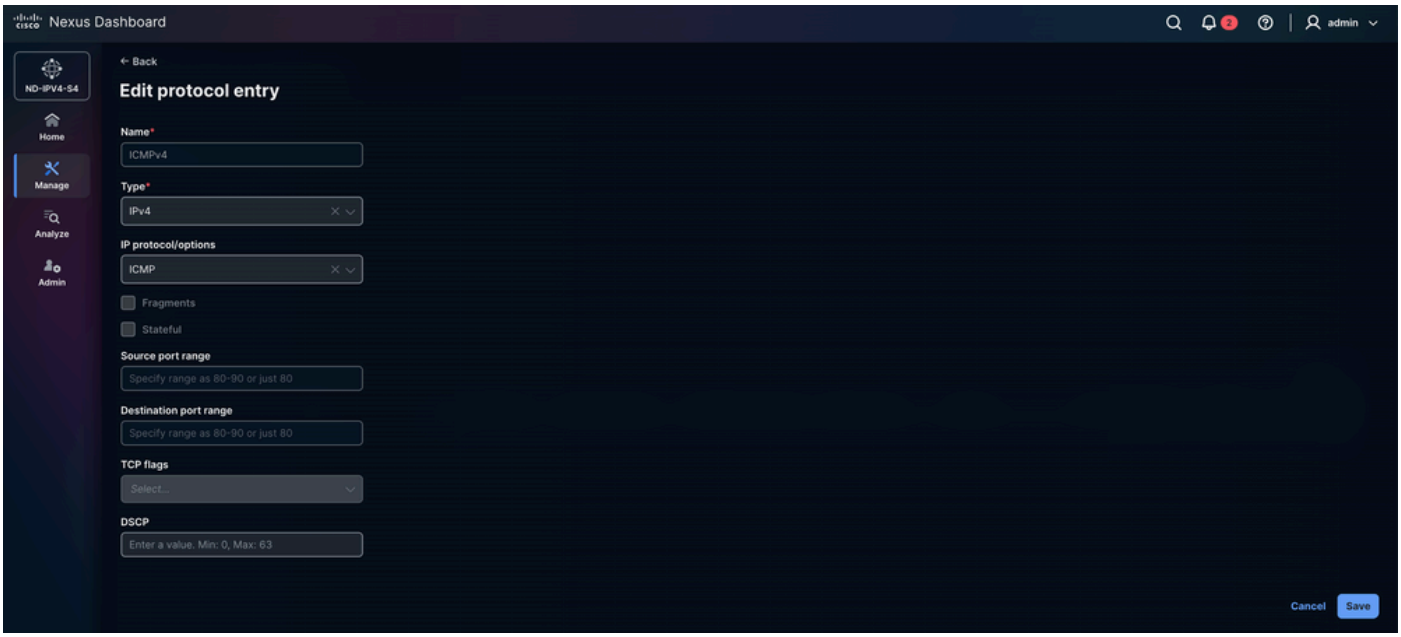
  - 它允许您定义安全协议使用的TCP标志。

  - TCP标志是TCP报头的一部分，用于控制连接的建立、维护和终止。

  - 可用选项:

- ACK（确认）：表示已接收数据或同步数据包的确认。
- EST（已建立）：表示已建立的TCP连接。启用此选项后，不能选择其他TCP标志。
- FIN（结束）：用于正常关闭TCP连接。
- RST（重置）：立即终止连接并丢弃所有仍在传输的数据。
- SYN（同步）：在TCP连接的启动和建立期间使用。





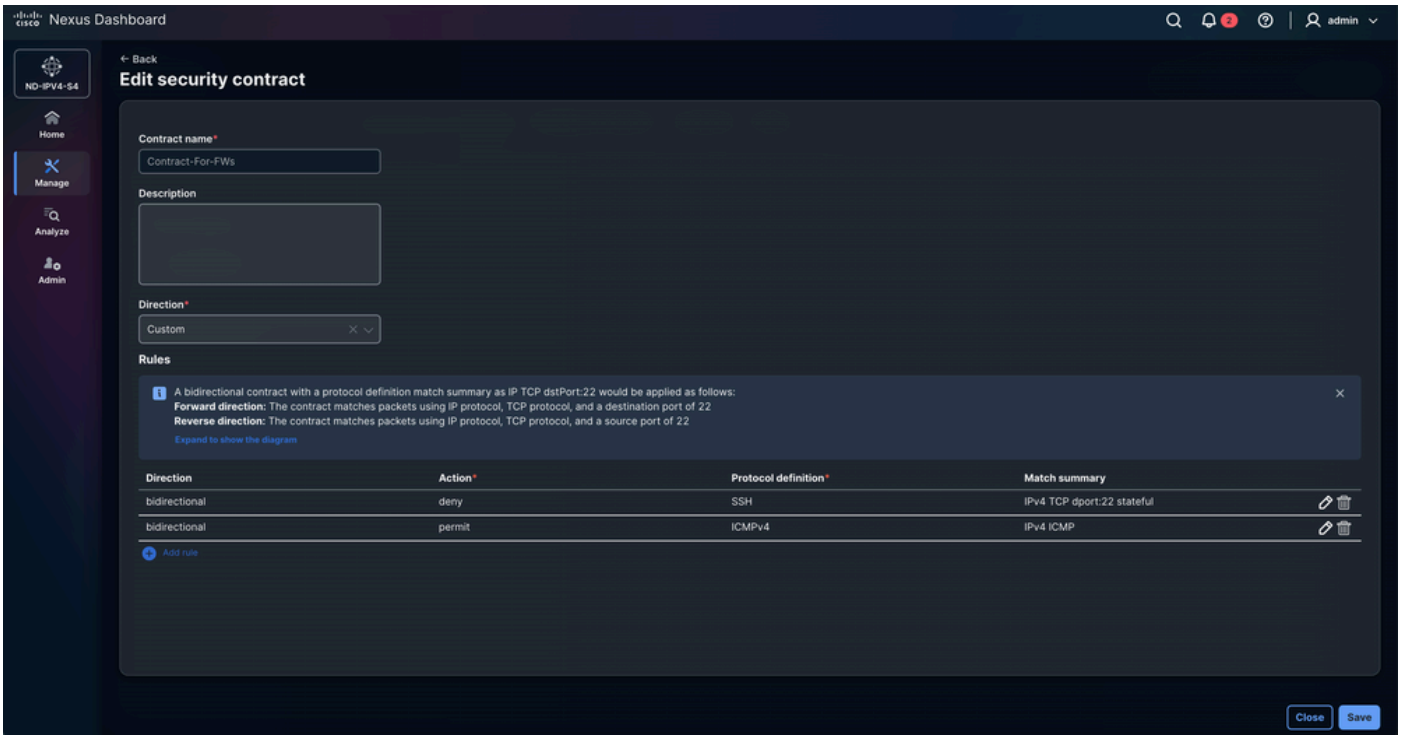
步骤5.配置安全合同

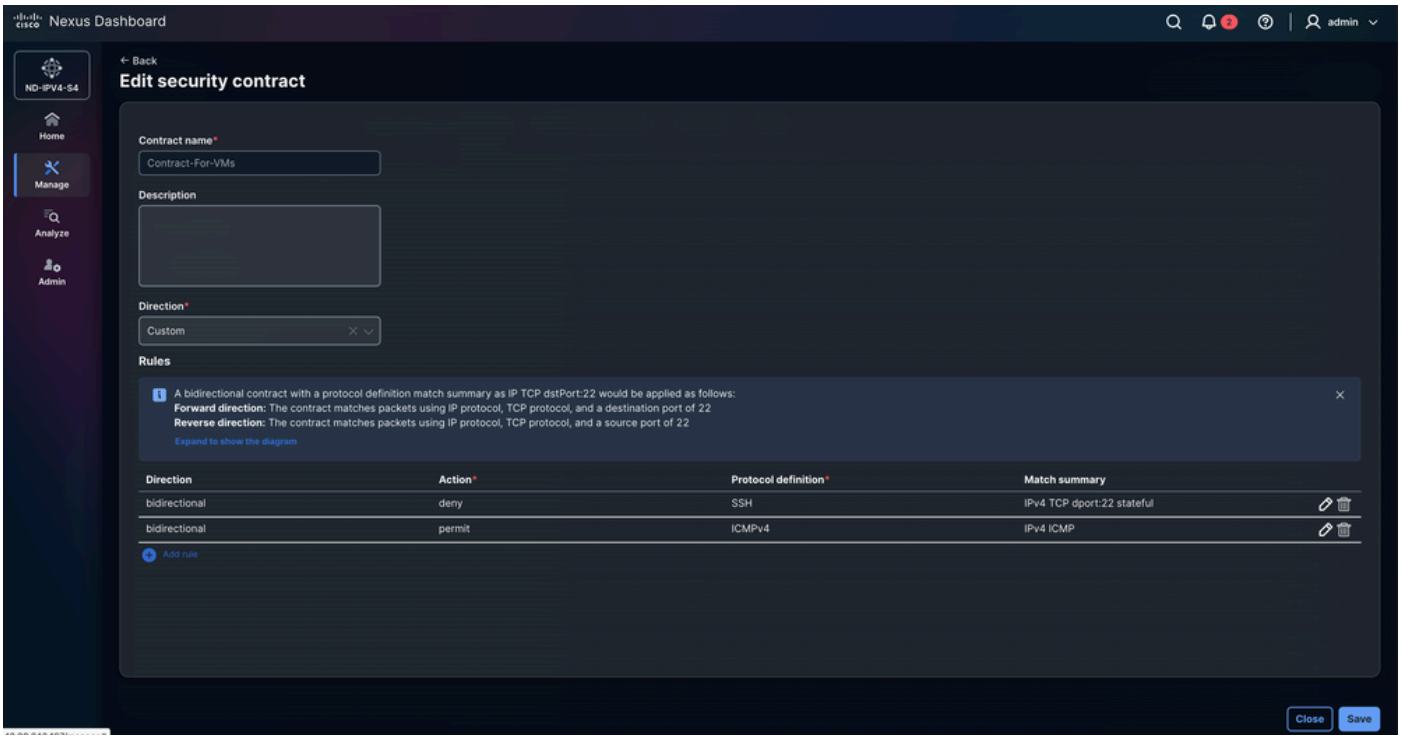
合同通过根据关联的策略定义指定允许或拒绝哪些流量来定义终端组之间的通信规则。它充当实施机制，应用已配置的协议规则、过滤器和操作，确保源组和目标组之间的流量符合预期的安全和分

段策略。

导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >分段和安全>安全合同>操作>创建安全合同。

- 选择Add rule并配置Direction、Action和Protocol definition。
  - 双向：
    - 双向合同应用如下，协议定义匹配摘要作为IP TCP端口22。
      - 转发方向：合同使用IP协议、TCP协议和目的端口22匹配数据包
      - 反向方向：合同使用IP协议、TCP协议和源端口22匹配数据包。
      - 无论源或目标如何，这都适用。
  - 单向:
    - GPO安全合同中的单向表示仅在流量流的一个方向上实施策略，允许或拒绝从源安全组到目标安全组的通信，而不在相反方向上自动应用同一规则。

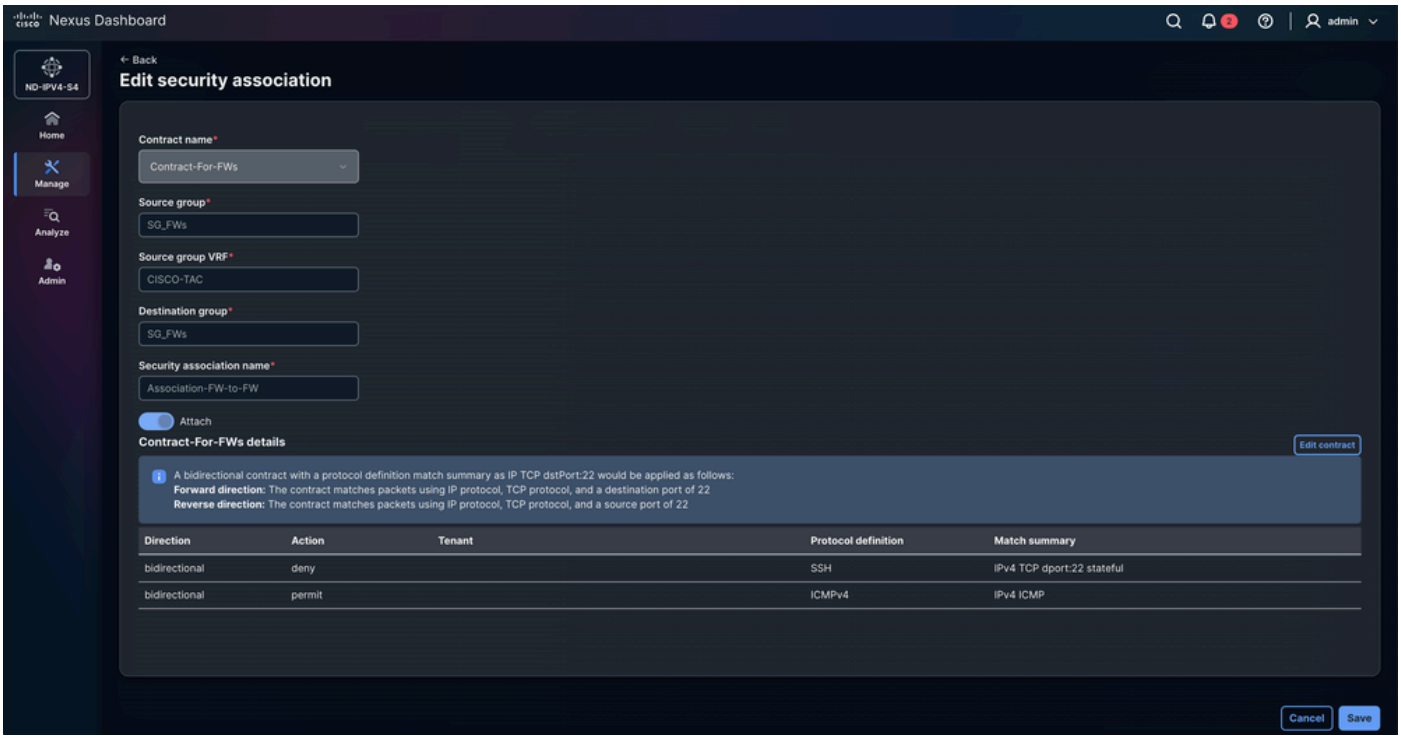


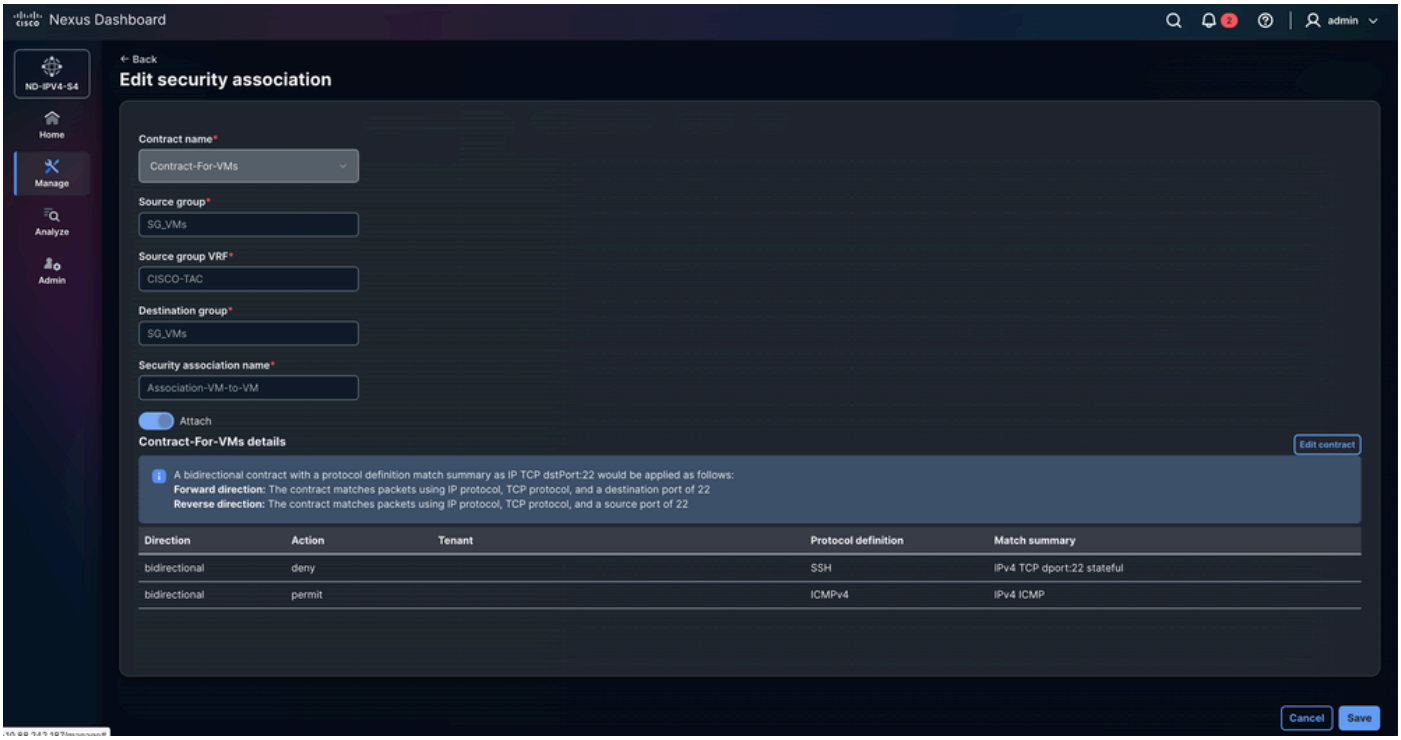


步骤6.配置安全关联

导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >分段和安全>安全关联>操作>创建安全关联。

在配置安全关联中，通过链接安全组、协议定义和安全合同来定义策略模型。安全组对终端进行分类，协议定义指定流量类型（例如协议或端口），安全合同使用这些协议规则定义在源安全组和目标安全组之间应用的策略。安全关联表示将这些元素绑定在一起的关系，以便交换矩阵可以实施定义的安全策略。

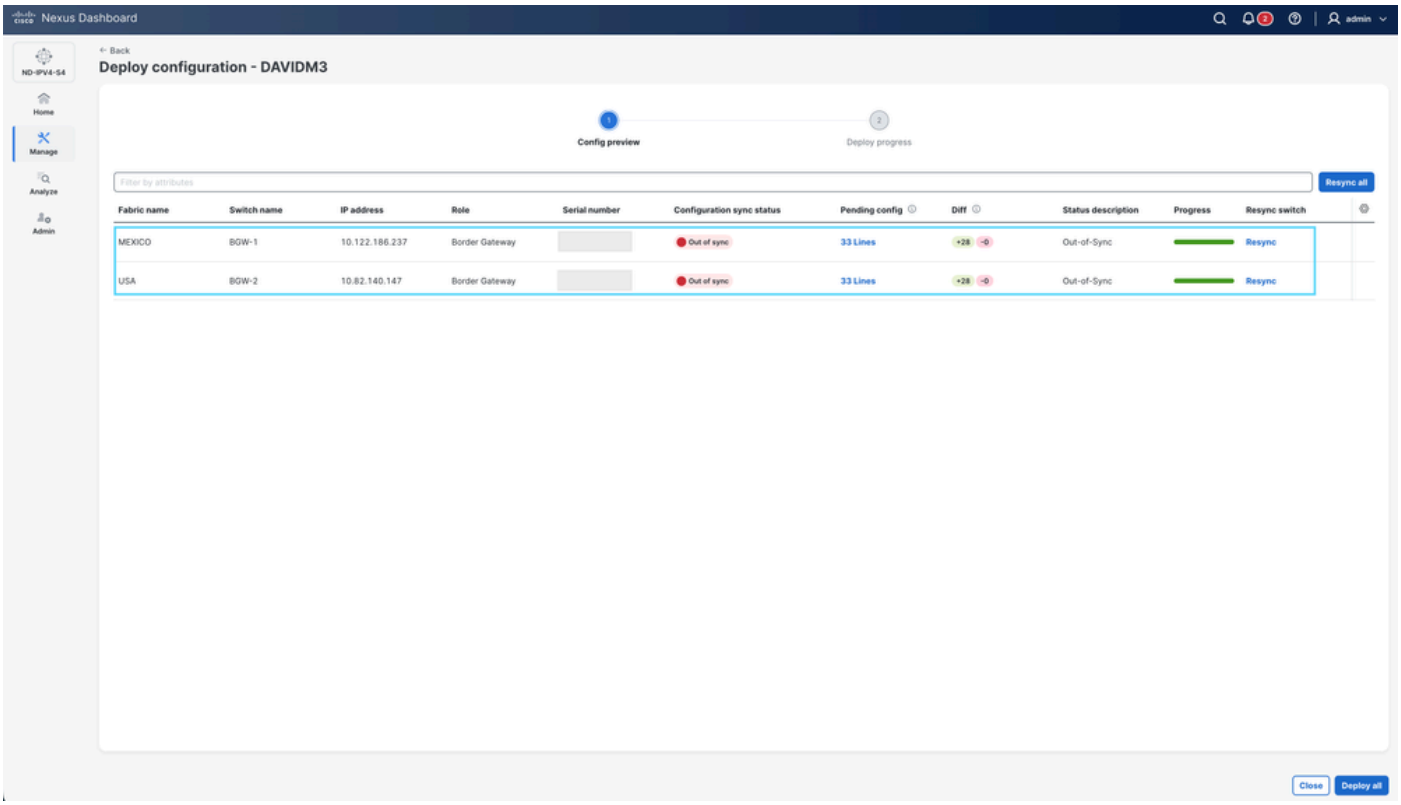


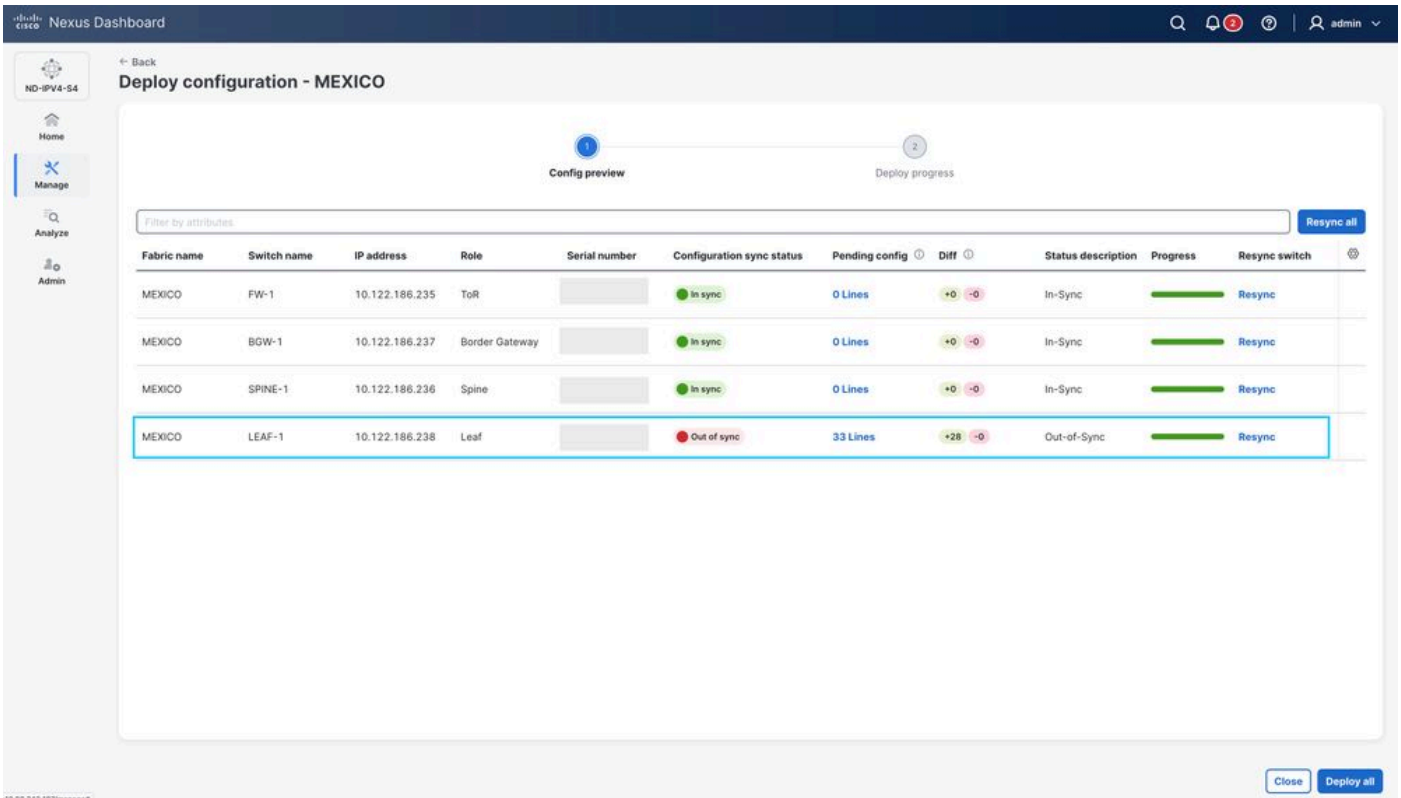


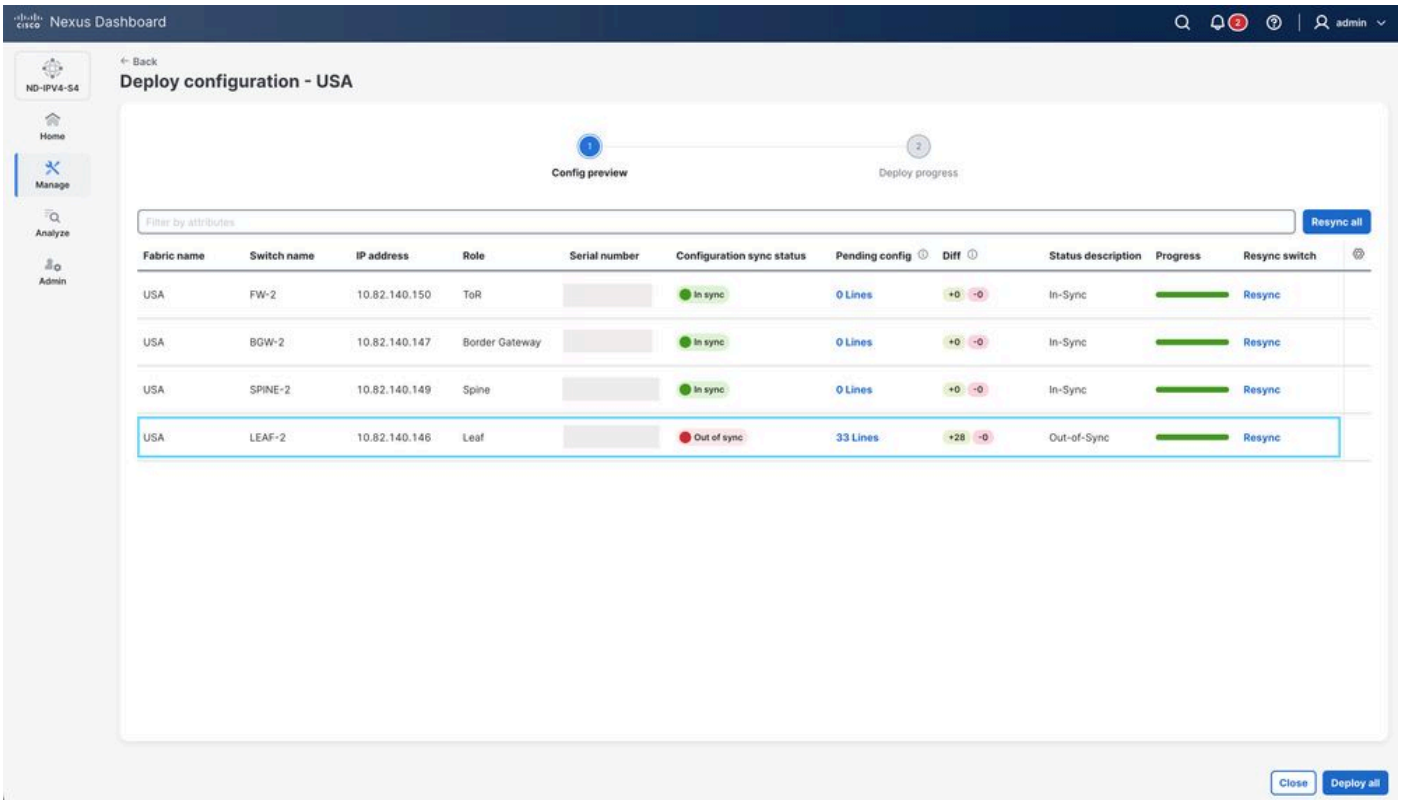
步骤7.验证GPO配置

- 导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >操作>重新计算和部署。
  - GPO配置从父交换矩阵交换机推送到边界网关。点击待处理的配置行数，查看并验证可部署到设备的配置。必须为每个子交换矩阵重复此过程。
  - 导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >资产>成员交换矩阵> MEXICO >操作>重新计算和部署。
  - 导航到管理>交换矩阵>交换矩阵组> DAVIDM3 >资产>成员交换矩阵> USA >操作>重新

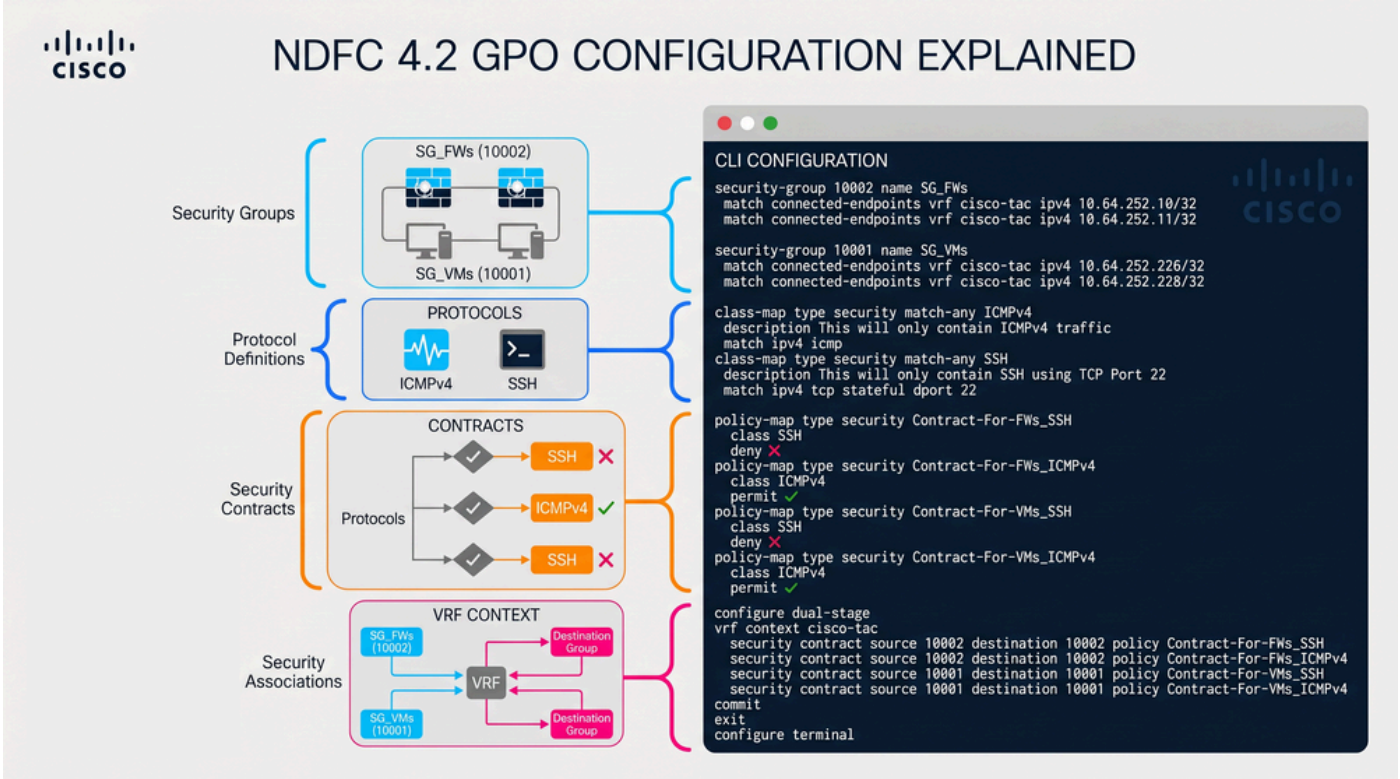
计算和部署。


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



- 该图显示了BGW-1、BGW-2、LEAF-1和LEAF-2的GPO配置。所有交换机上的配置都相同。NDFC 4.2不按所示确切顺序应用配置。本节说明CLI命令的逻辑顺序。



排除VXLAN GPO可操作性故障

步骤1.检验安全组功能状态

验证交换机上是否启用了安全组功能。VXLAN GPO依赖于此功能，因为它激活终端分类、合同实施和SGACL硬件编程所需的安全组标记(SGT)基础设施。

<#root>

BGW-1#

show feature | i i security-group

security-group 1 enabled

步骤2.检验系统路由模式

验证交换机上已配置和运行的系统路由模式。VXLAN GPO需要安全组支持路由模式，因为SGACL实施会消耗ASIC管道内的专用硬件转发资源。

<#root>

BGW-1#

show system routing mode

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

步骤3.验证VXLAN NVE对等体建立和GPO功能

- 验证本地交换矩阵设备和远程多站点对等体之间的VXLAN NVE对等体建立。VXLAN GPO信息通过VXLAN EVPN控制平面传播，因此，在整个交换矩阵中进行安全组标记(SGT)学习和合同同步需要稳定的NVE邻接。
- 支持字段组策略是此命令中最重要的指示符之一，因为它确认远程VTEP是否支持跨VXLAN EVPN多站点域的SGT传播和SGACL合同实施所需的VXLAN组策略扩展。

<#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


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

步骤4.检验安全组学习和终端分类

验证终端是否正确分类为安全组(SGT)。VXLAN GPO实施取决于准确的终端到SGT映射。

<#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
```

步骤5.检验安全合同和策略实施

验证VXLAN GPO合同是否正确安装且运行正常。合同定义在安全组之间实施的通信规则，并代表VXLAN GPO用于微分段的核心策略机制。

<#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
```

步骤6.检验VRF安全实施状态

验证交换机上配置的所有VRF的VXLAN GPO实施状态。此命令确认SGACL策略和安全组合同是否在租户VRF内主动实施。

输出确认cisco-tac VRF主动参与VXLAN GPO实施，模式设置为实施。实施标记13648用于标识编程到此VRF硬件的内部SGACL策略情景。默认操作deny log表示拒绝并记录未明确允许通过安全组合同的任何流量，从而实施默认拒绝微分段策略。相反，默认VRF（出口负载均衡解析管理）和管理VRF在非实施模式下运行，这意味着这些VRF中不应用VXLAN GPO策略，并且默认情况下允许流量。

Stats字段跟踪与VRF安全策略匹配的流量。cisco-tac VRF下的值0表示在执行命令时，没有不匹配的流量触发默认拒绝行为，而默认VRF下的计数器值4364表示不执行VXLAN GPO的VRF中的流量活动。

<#root>

BGW-1#

show vrf all security

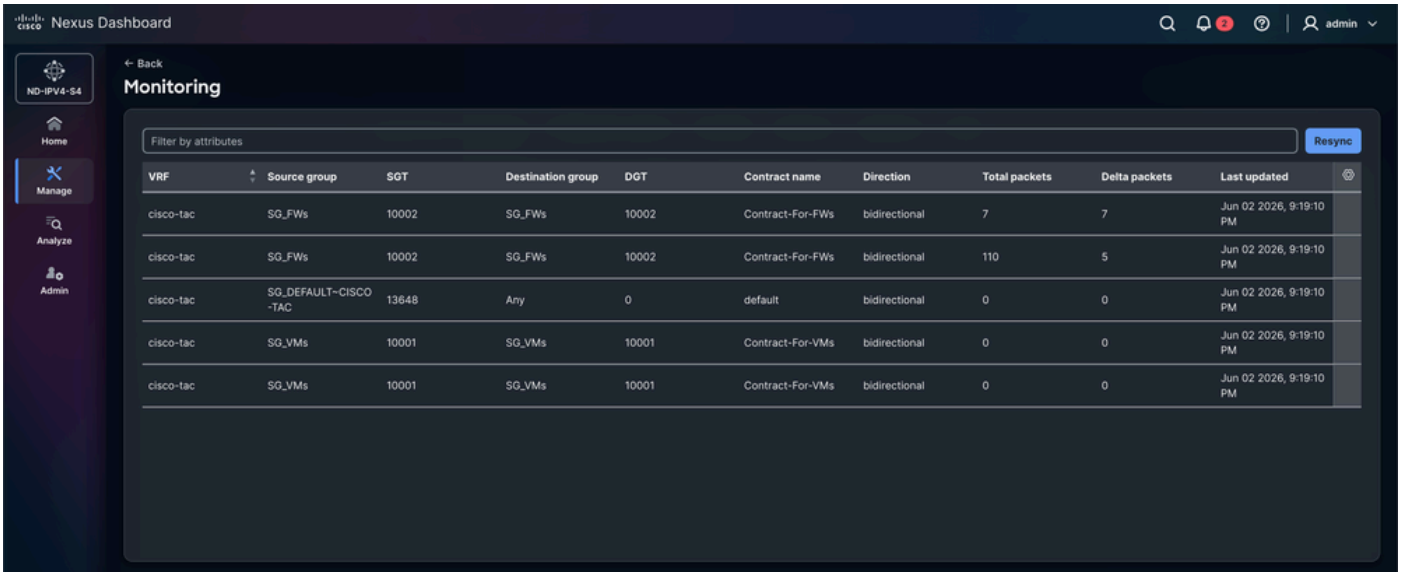
```
VRF                                Mode         TAG     Action     Scope   Stats
-------------------------------------------------------------------------------------
cisco-tac                          enforced     13648   deny,log   4       0
default                            unenforced   -   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

步骤7.检验VRF安全实施状态

- 从NDFC GUI验证VXLAN GPO合同的流量匹配统计信息。此验证确认流量是否主动匹配已配置的安全组合同，以及SGACL实施是否可在VXLAN EVPN多站点交换矩阵中正常运行。
- 在NDFC GUI中，导航至管理>交换矩阵>交换矩阵组> USA / MEXICO >分段和安全>安全关联>监控。
  - 此部分提供对安全组通信流、合同命中统计信息、允许和拒绝操作以及终端组之间的操作合同活动的可视性。
  - 监控统计信息会单独显示在每个监控统计信息内。

- NDFC的监控统计信息提供操作验证层，该层通过确认交换矩阵中的实时策略实施和流量匹配行为来补充基于CLI的故障排除。

注意：第一次尝试查看NDFC 4.2中的流量统计信息时，监控部分最初可能显示为空白。在这种情况下，按Resync按钮以触发来自VXLAN交换矩阵的合同统计信息的同步。同步进程运行时,GUI显示消息Resync status:正在进行中.同步完成后，按Ok按钮刷新监控视图。重新同步完成后，与每个安全组合同关联的流量统计信息将在监控部分显示。要验证实时流量匹配行为，请在终端之间生成流量，然后再次按Resync按钮以更新NDFC中显示的合同统计信息。



- 在前一个场景中，终端之间成功允许ICMPv4流量。但是，如果建立SSH会话，连接将超时，因为VXLAN GPO合同明确拒绝发往端口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
```

相关信息

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

使用VXLAN GPO通过微分段保护数据中心

使用VXLAN组策略选项(GPO)在Cisco NX-OS VXLAN EVPN交换矩阵中部署微分段

使用组策略选项(GPO)和Nexus控制面板在VXLAN EVPN交换矩阵中自动执行微分段和部署第4-7层服务

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。