NDFC 4.2를 사용하여 Nexus 멀티 사이트 패브릭에서 GPO 구성

목차

소개

이 문서에서는 NX-OS 및 NDFC 4.2를 실행하는 Nexus Cloud Scale 스위치의 VXLAN 멀티 사이트 패브릭에서 GPO 컨피그레이션 및 검증에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 영역에 대해 알고 있는 것이 좋습니다.

- VXLAN(Virtual Extensible Local Area Network), EVPN(Ethernet Virtual Private Network) 및 멀티 사이트 패브릭 기술
- Cisco Nexus Cloud Scale 스위치 및 Nexus NX-OS(Operating System) 운영
- Nexus NDFC(Fabric Network Controller) 4.2 관리 및 구축 워크플로
- 네트워크 세그멘테이션 및 보안 정책 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

VXLAN EVPN 패브릭의 GPO 기능 이해

GPO(Group Policy Option)는 IP 주소, VLAN 또는 서브넷에만 의존하지 않고 논리적 ID에 따라 엔드포인트 간 통신을 제어하도록 설계된 정책 기반 세그멘테이션 메커니즘입니다. GPO의 주요 목적은 보안 정책 시행을 간소화하고 애플리케이션, 서버 또는 워크로드 간에 확장 가능한 마이크로 세그멘테이션을 제공하는 것입니다.

간단한 비유는 모든 게스트가 특정 카테고리 또는 액세스 레벨에 속하고, 특정 영역은 특정 게스트만 액세스할 수 있으며, 액세스 권한은 객실 번호 대신 게스트의 역할에 따라 달라지는 호텔을 생각하는 것입니다. GPO는 매우 유사한 방식으로 작동합니다. GPO는 엔드포인트를 순수하게 IP 주소로 취급하는 대신 보안 그룹(SG)으로 분류합니다. 그런 다음 정책이 이러한 그룹 간에 적용되어 어떤 통신이 허용되거나 거부되는지 확인합니다.

예를 들면 다음과 같습니다.

- 웹 서버는 하나의 보안 그룹에 속할 수 있습니다.
- 애플리케이션 서버는 다른 보안 그룹에 속할 수 있습니다.
- 데이터베이스 서버는 제한된 보안 그룹에 속할 수 있습니다.

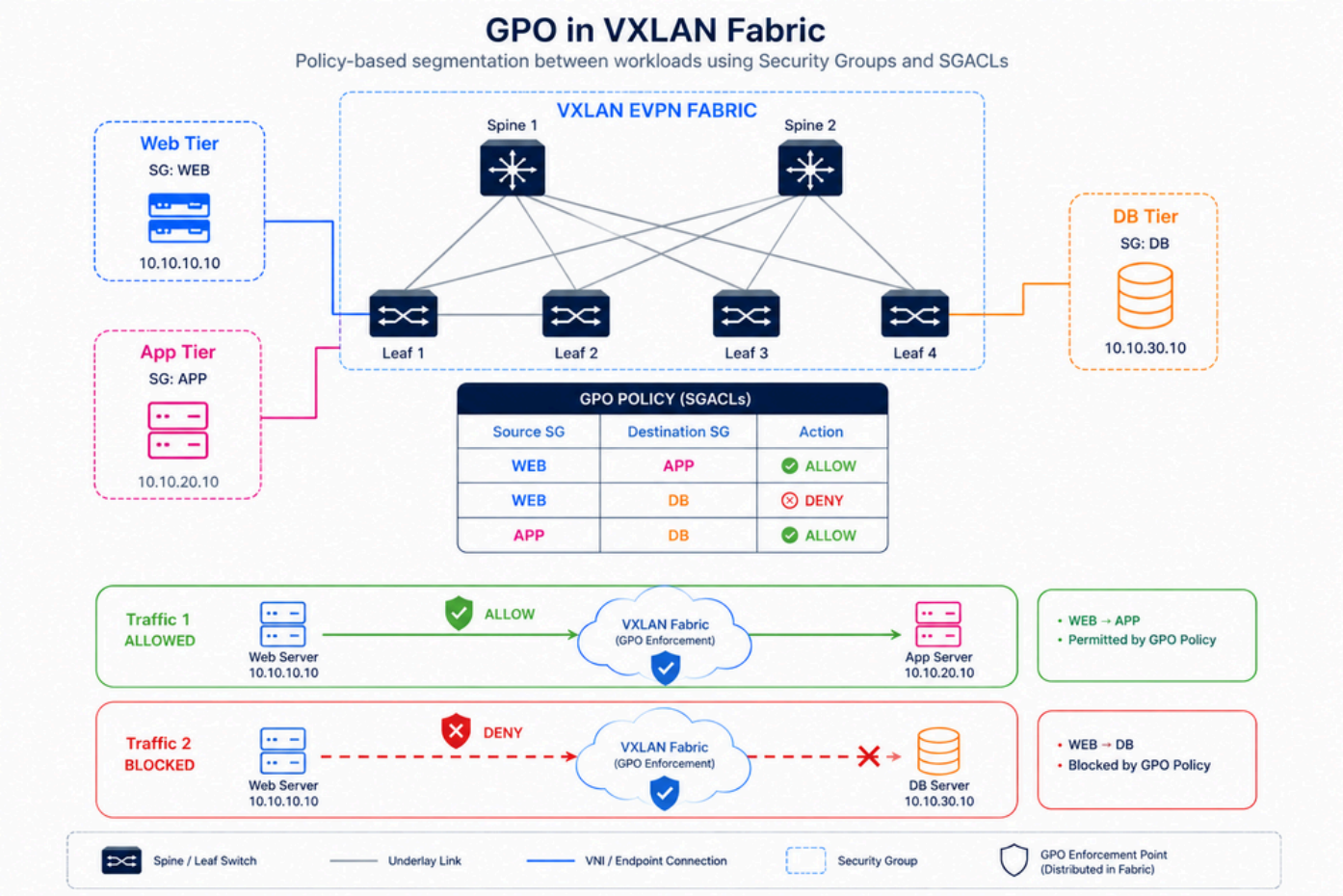
그러면 정책에서 다음을 정의할 수 있습니다.

- 웹 서버는 애플리케이션 서버와 통신할 수 있습니다.
- 애플리케이션 서버는 데이터베이스 서버와 통신할 수 있습니다.
- 웹 서버는 데이터베이스 서버와 직접 통신할 수 없습니다.

이 접근 방식은 관리자가 더 이상 여러 디바이스와 VLAN에서 많은 수의 ACL을 유지 관리할 필요가 없기 때문에 운영을 간소화합니다.

또 다른 주요 장점은 확장성입니다. 대규모 환경에서는 워크로드가 자주 이동하거나 동적으로 확장되거나 IP 주소가 변경됩니다. GPO를 사용하면 엔드포인트 위치가 변경되더라도 보안 정책이 일관되게 유지될 수 있습니다. VXLAN EVPN 패브릭 내에서 GPO는 패브릭 전체에 보안 그룹 정보를 배포하고 엔드포인트 간에 SGACL(Security Group ACL)을 적용하여 이러한 개념을 확장합니다. 워크로드 간의 동-서 트래픽이 가장 큰 공격 표면을 나타내는 경우가 많기 때문에, 이는 현대 데이터 센터에서 특히 중요합니다. GPO는 데이터 센터 패브릭 내부의 불필요한 통신 경로를 제한하여 보안 상태를 개선합니다.

GPO 아키텍처, 마이크로 세그멘테이션 개념 및 VXLAN 정책 시행에 대한 자세한 기술적 이해는 Cisco 백서, VXLAN GPO를 사용한 마이크로 세그멘테이션으로 데이터 센터 보안을 참조하십시오.



VxLAN 패브릭의 GPO

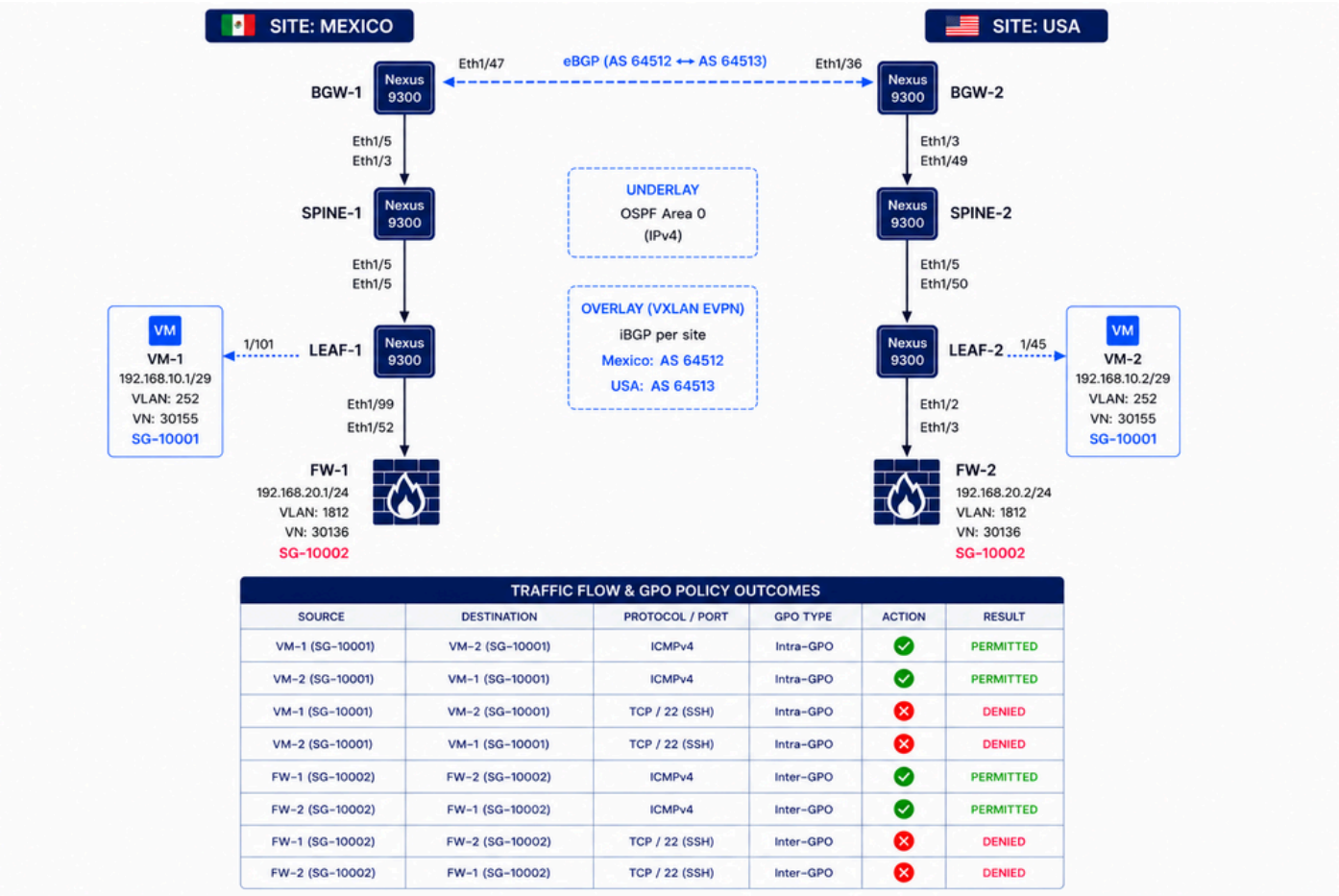
NDFC 4.2 및 NX-OS 10.6(3)F를 사용하는 VXLAN 멀티 사이트 GPO 구축 시나리오

이 토폴로지는 지리적으로 분산된 두 사이트에 구축된 VXLAN 멀티 사이트 패브릭을 나타냅니다. 멕시코와 미국. 각 사이트에는 전용 BGW, 스파인 스위치, 리프 스위치, 가상 머신, NX-OS 10.6(3)F가 포함된 Cisco Nexus 9300 스위치에서 실행되는 방화벽 세그먼트가 포함되어 있습니다. 언더레이 네트워크는 OSPF(Open Shortest Path First)를 사용하는 반면, 오버레이 컨트롤 플레인은 사이트 간 VXLAN EVPN 통신을 위해 각 사이트 내의 iBGP 및 BGW-1과 BGW-2 간의 eBGP를 사용합니다. 이 환경은 실험실 배치이므로, 다중 사이트 연결 모델을 간소화하기 위해 멕시코와 미국 사이트는 두 BGW 간에 직접 연결된 링크를 통해 상호 연결됩니다.

GPO는 IP 주소 지정 또는 VLAN 경계와는 독립적으로 SG(Security Group) 간에 정책 기반 마이크로 세그멘테이션을 적용하는 데 사용됩니다. 연결 정책 테이블에 따라 VM-1에서 VM-2, FW-1 및 FW-2로의 ICMP 트래픽이 허용되며, VM-1에서 FW-1 및 FW-2로의 TCP 포트 22(SSH) 트래픽은 거부됩니다. 두 엔드포인트가 동일한 보안 그룹(SG-10001)에 속하므로 VM-1과 VM-2 간의 TCP 포

트 22 통신은 계속 허용됩니다. 이 동작은 GPO가 VXLAN 멀티 사이트 패브릭 전체에서 GPO 내 통신과 GPO 간 통신 간에 서로 다른 트래픽 정책을 동적으로 적용하는 방법을 보여줍니다.

참고: Cisco NX-OS Release 10.6(3)F에서는 ESG 내 격리 기능을 사용하여 동일한 ESG(SG라고도 함) 내의 엔드포인트 간 통신을 제한할 수 있습니다. 이 기능은 ESG 내에서 무단 액세스의 위험을 최소화하고 보안 상태를 강화합니다.



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

VXLAN EVPN 패브릭에서 NDFC 4.2로 GPO를 단계별로 구성

이 단계는 VXLAN 멀티 사이트 패브릭이 이미 작동 중이고 NDFC 4.2로 구성되어 있으며 이후에 GPO를 구현해야 하는 경우에 적용됩니다. Automation Using Nexus Dashboard in Securing Data Centers with Microsegmentation Using VXLAN GPO(VXLAN GPO를 사용한 마이크로 세그멘테이션으로 데이터 센터 보안의 자동화) 섹션에서는 VXLAN 단일 사이트 패브릭 생성부터 시작하는 컨피그레이션을 보여줍니다.

⚠

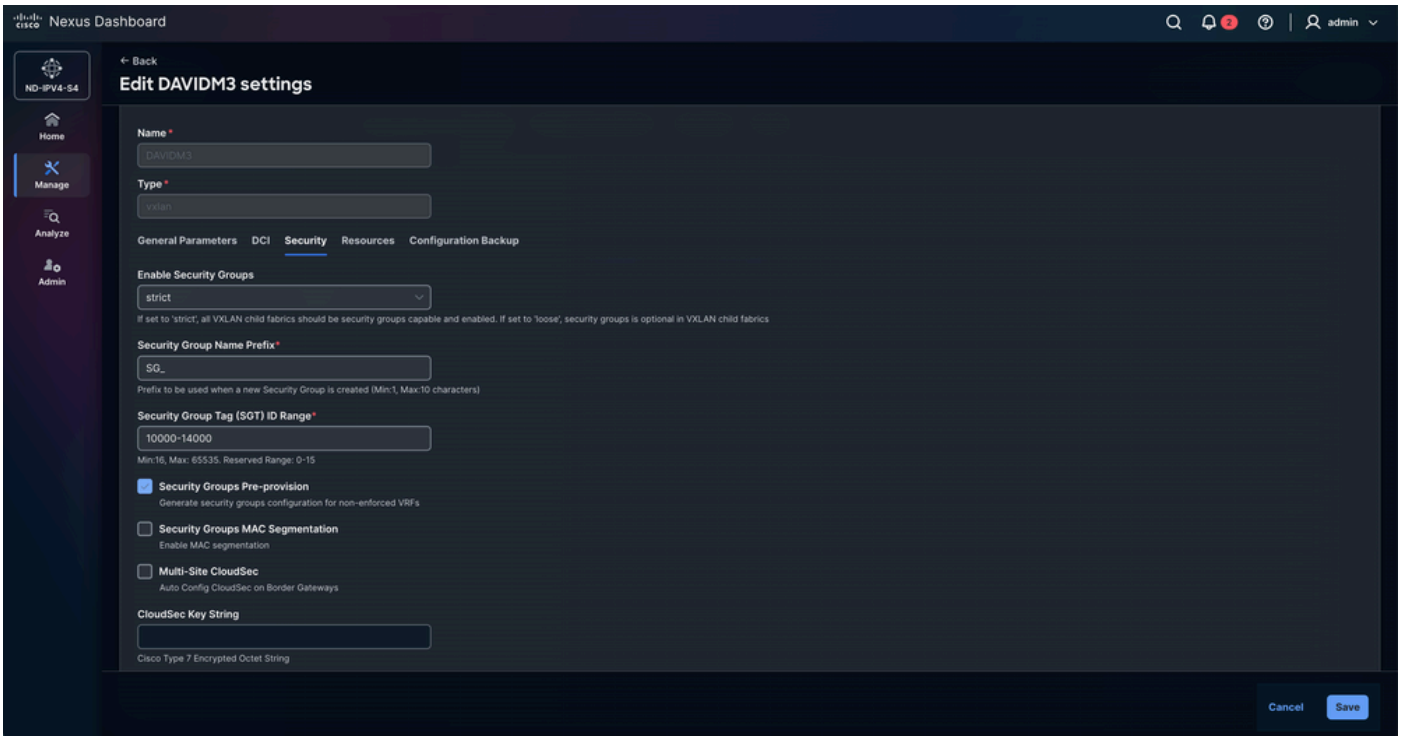
주의: GPO가 VXLAN EVPN 패브릭에서 작동하는 경우, 대상 연결이 존재하고 보안 정책이 트래픽을 허용하는 경우에만 통신이 발생합니다. 정책 시행은 IP 정보에 의존하므로 내부 네트워크에 ARP 항목 및 SVI가 필요합니다. 즉, 테넌트 VRF에 속하는 VLAN에는 SVI가 구성되어 있어야 합니다. 따라서 레이어 2 헤더만 포함된 트래픽에는 적용이 적용되지 않으므로 VXLAN 레이어 2 확장에서 사용할 수 없습니다. NX-OS Release 10.6(2)F에서는 MAC 기반 마이크로세그멘테이션 지원을 도입합니다.

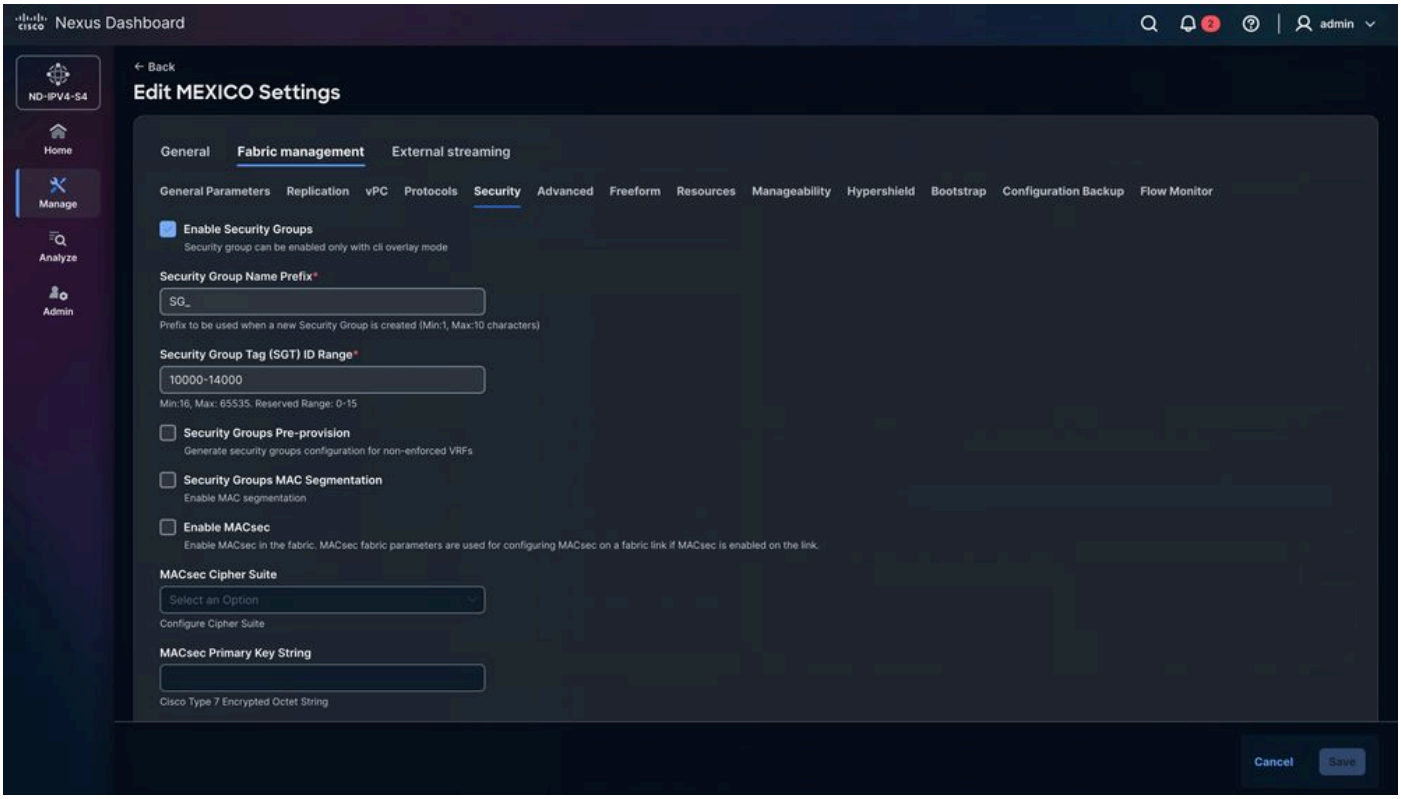
1단계. 상위 패브릭에서 보안 그룹 활성화

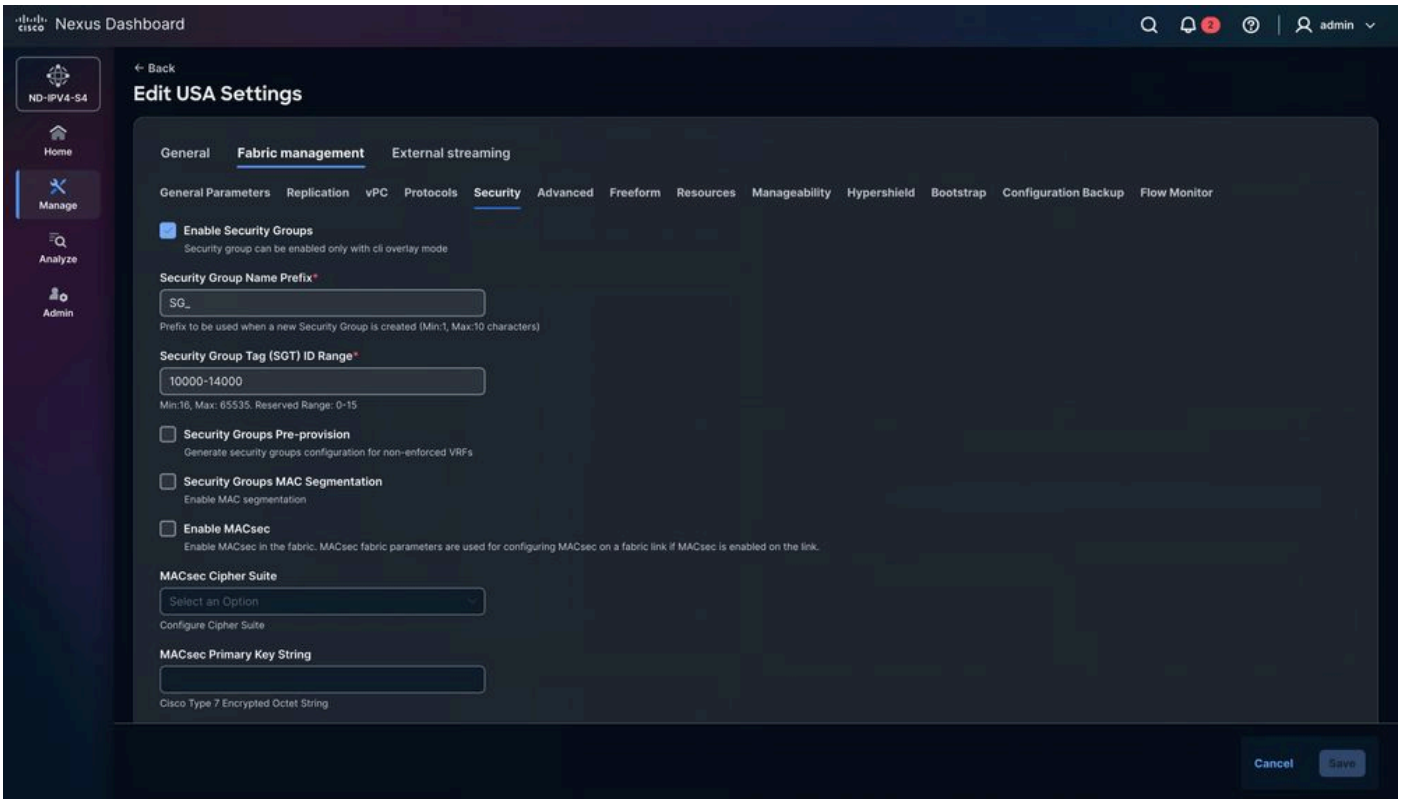
- Manage(관리) > Fabric Groups(패브릭 그룹)로 이동하고 패브릭 그룹 DAVIDM3를 선택한 다음 Actions(작업) > Edit Fabric Group Settings(패브릭 그룹 설정 편집)를 선택합니다. Security(보안) 섹션에서 Security Groups(보안 그룹)를 활성화하고 Strict(엄격)로 설정하고 Security Groups(보안 그룹) Pre-provision(사전 프로비저닝)으로 설정합니다.
  - 원하는 패브릭 그룹을 선택합니다. 이 예에서 선택한 패브릭 그룹을 DAVIDM3라고 하며, 이는 멀티 사이트 패브릭의 이름이기도 합니다.
- 각 하위 패브릭에 대해 이 단계를 반복합니다.
  - Manage(관리) > Fabric(패브릭)으로 이동하고, USA를 선택한 다음 Actions(작업) > Edit Fabric Group Settings(패브릭 그룹 설정 수정)로 이동합니다. Security(보안) 섹션에서 Security Groups(보안 그룹)를 활성화하고 모드를 Strict(엄격)로 설정합니다.
  - Manage(관리) > Fabric(패브릭)으로 이동하고 MEXICO(멕시코)를 선택한 다음 Actions(작업) > Edit Fabric Group Settings(패브릭 그룹 설정 편집)로 이동합니다. Security(보안) 섹션에서 Security Groups(보안 그룹)를 활성화하고 모드를 Strict(엄격)로 설정합니다.

참고: strict로 설정된 경우 모든 VXLAN 하위 패브릭이 보안 그룹을 지원하고 활성화되어야 합니다. loose로 설정된 경우 VXLAN 하위 패브릭에서 보안 그룹은 선택 사항입니다.

팁: 명확한 가시성을 유지하려면 상위 패브릭과 모든 하위 패브릭에서 동일한 SGT(Security Group Tag) ID 범위를 사용합니다. 상위 패브릭 범위는 모든 하위 패브릭에서 사용하는 범위를 포함해야 합니다.


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



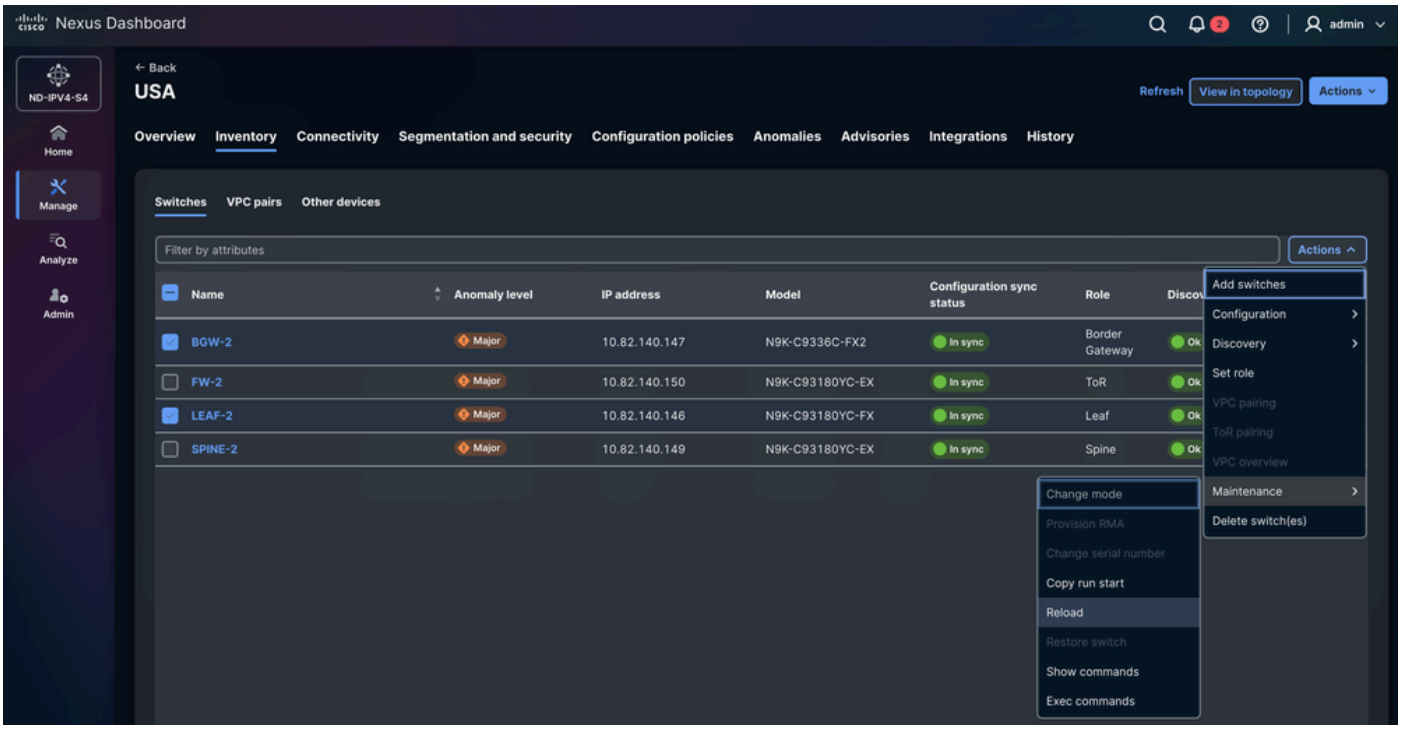
2단계. 패브릭 컨피그레이션 재계산 및 GPO 구축을 위한 스위치 다시 로드

NDFC는 역할에 따라 특정 Nexus 스위치 그룹을 다시 로드하라는 메시지를 자동으로 표시합니다. 이 예에서는 LEAF-1, LEAF-2, BGW-1 및 BGW-2를 다시 로드해야 합니다. 이 작업은 네트워크 관리자가 수동으로 실행해야 합니다. 다시 로드는 필요하며 GPO에 TCAM 조각이 필요하므로 건너뛸 수 없습니다.

참고: 디바이스가 다시 로드되지 않은 경우 TCAM 변경 사항이 실행 중인 컨피그레이션에 나타날 수 있습니다. 그러나 스위치가 재부팅되지 않았으므로 하드웨어 메모리에 설정이 적용되지 않습니다. 따라서 기능이 예상대로 작동하지 않습니다.

Nexus 스위치를 다시 로드하려면

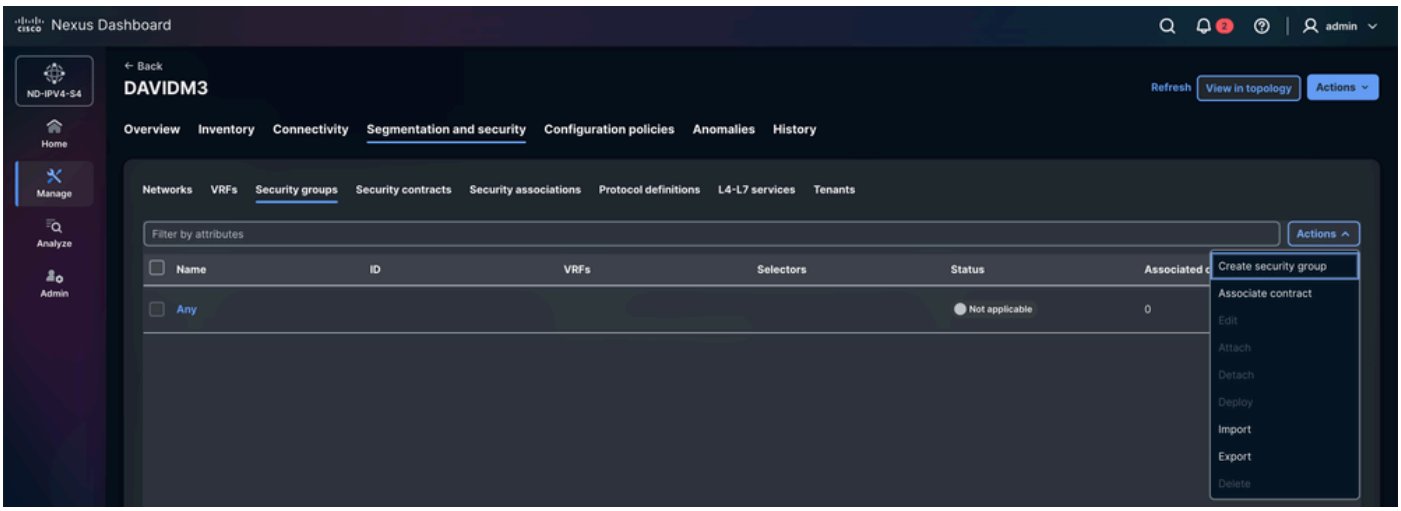
Manage(관리) > Fabrics(패브릭) > MEXICO/USA > Inventory(인벤토리) > Switches(스위치) > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions(작업) > Maintenance(유지 관리) > Reload(다시 로드)로 이동합니다.



3단계. 보안 그룹 생성

각 엔드포인트의 보안 그룹을 정의합니다. VXLAN 패브릭의 각 엔드포인트는 단일 보안 그룹을 가질 수 있습니다. 이 접근 방식은 확장성이 효율적이지 않습니다. 엔드포인트를 전역으로 그룹화합니다(가상 머신, 방화벽, TCP 최적기 등).

Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Segmentation and security(세그멘테이션 및 보안) > Security Groups(보안 그룹) > Actions(작업) > Create security group(보안 그룹 생성)으로 이동합니다.



3.1단계 보안 그룹 이름 구성

- NDFC에서 자동으로 임의의 이름을 할당합니다. 이름을 변경할 수 있습니다. 엔드포인트가 식별하기 쉬운 대표 이름을 사용하는 것이 좋습니다.
- 이 시나리오에서:
  - VM -> SG_VM
  - FW -> SG_FW

3.2단계 VRF 구성

- 엔드포인트가 속한 테넌트(VRF)를 선택합니다.
- 이 시나리오에서: VM 및 방화벽은 CISCO-TAC 테넌트에 속합니다.

선택 사항, VRF를 생성합니다.

기본적으로 새로 생성된 테넌트 VRF는 정책 시행 모드가 Unenforced(미시행)로 설정되어 있습니다. 이 상태에서는 보안 그룹 간 분류 기준 및 SGACL이 구성된 경우에도 정책 시행이 발생하지 않습니다. SGACL 시행을 활성화하려면 Enforced 모드에서 VRF를 명시적으로 구성해야 합니다.

VRF가 Enforced 모드에서 작동할 때 기본 정책 동작이 정의됩니다.

- 거부: 허용 규칙에서 명시적으로 허용하지 않는 한 모든 유니캐스트 트래픽은 삭제됩니다.
- 허용: 거부 규칙에 의해 명시적으로 차단되지 않는 한 모든 유니캐스트 트래픽은 허용됩니다.

동일한 보안 그룹에 속한 엔드포인트는 SGACL 규칙 없이도 서로 통신할 수 있습니다. SGACL은 서로 다른 보안 그룹 간에만 보안 정책을 정의합니다.

Cisco NX-OS Release 10.6(3)F에는 동일한 GPO 내의 엔드포인트 간 통신을 제한하는 기능이 도입되었으며 이는 intra-GPO 격리 기능이라고도 합니다. 이 릴리스 이전에는 동일한 보안 그룹 내의 엔드포인트에 적용되는 규칙이 무시되며, 기본적으로 트래픽이 허용됩니다.

3.3단계 보안 그룹 태그 ID 구성

NDFC는 패브릭 컨피그레이션에서 미리 정의된 범위에서 임의의 Tag ID를 자동으로 할당합니다. 태그 ID는 수동으로 선택할 수 있지만 하위 패브릭과 상위 패브릭 모두에 대해 정의된 범위에 속해야 합니다.

이 시나리오에서:

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

3.4단계 추가

Attach 옵션이 활성화되지 않으면 보안 그룹이 CISCO-TAC 테넌트에 적용되지 않습니다.

3.5단계 선택기 구성

- 선택기는 어떤 엔드포인트와 외부 IP 주소가 특정 보안 그룹과 연결되는지 결정합니다.

NDFC 4.2는 기본적으로 세 가지 유형의 선택기를 지원합니다.

1) IP Selectors: IP Selectors는 IP 정보를 기준으로 엔드포인트 또는 IP 서브넷을 보안 그룹에 연결합니다.

a. Connected Endpoint(연결된 엔드포인트) - 가상 머신, 서버 또는 리프 스위치에 연결된 물리적 호스트와 같이 패브릭에 직접 연결된 엔드포인트를 식별합니다.
b. 외부 서브넷 - 외부 IP 접두사를 보안 그룹에 연결합니다. 이 유형은 외부 데이터 센터, WAN 세그먼트 또는 인터넷 연결 네트워크와 같이 VXLAN 패브릭 외부에 있는 네트워크에 사용됩니다. 이러한 접두사로부터 소싱되거나 이러한 접두사로 향하는 트래픽은 구성된 보안 그룹으로 분류됩니다.

2) 네트워크 선택기: 네트워크 선택기는 보안 그룹을 특정 VXLAN 네트워크 세그먼트와 연결합니다. 분류는 네트워크 식별자(L2VNI)를 기반으로 적용된다. 해당 네트워크에 속한 모든 엔드포인트는 할당된 보안 그룹을 상속하며, 이는 여러 엔드포인트가 동일한 세그먼트를 공유할 때 정책 구축을 간소화합니다.

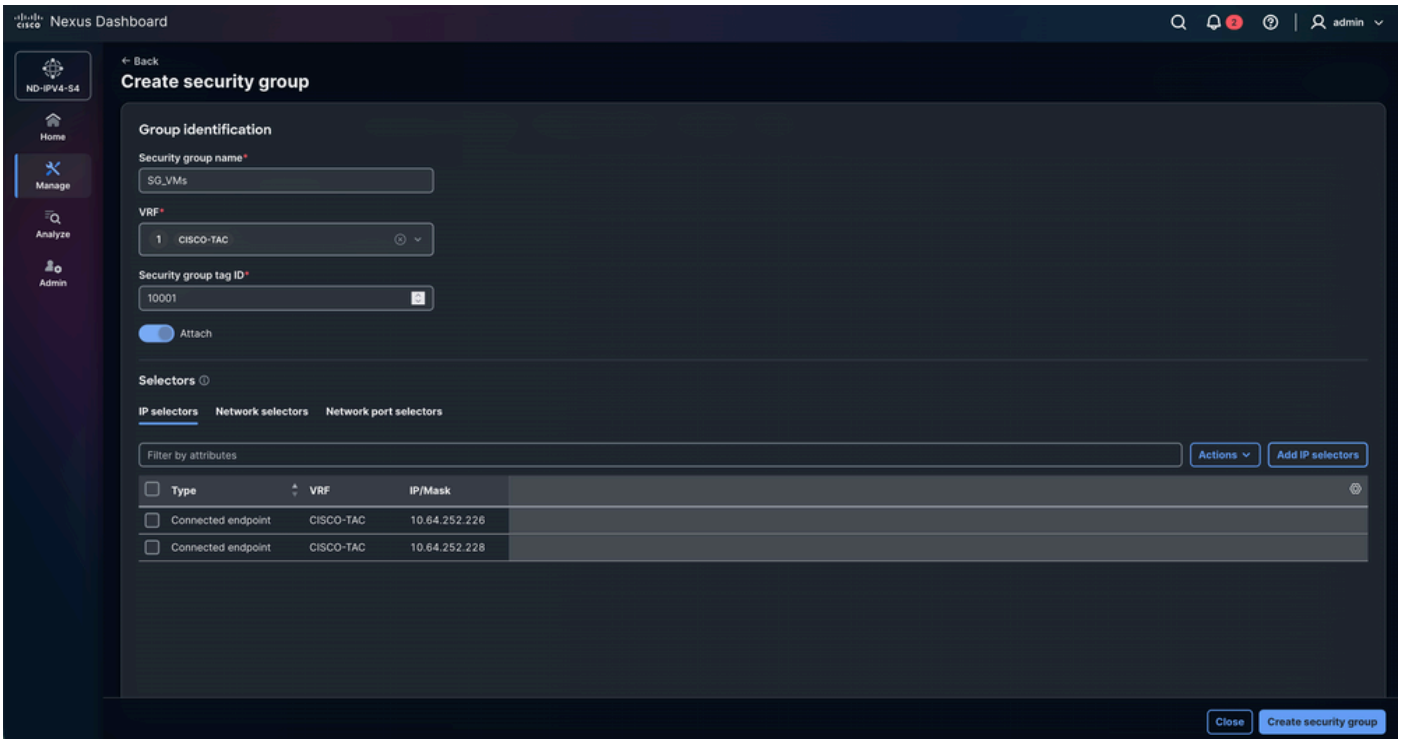
3) 네트워크 포트 선택기: 네트워크 포트 선택기는 트래픽이 패브릭으로 들어오는 물리적 스위치 인터페이스를 기반으로 트래픽을 분류합니다. 특정 포트 또는 인터페이스에서 수신된 트래픽에 보안 그룹을 할당할 수 있습니다. 이 접근 방식은 일반적으로 엔드포인트 IP 분류가 불가능한 외부 네트워크, 서비스 어플라이언스 또는 인프라 링크를 통해 연결된 디바이스에 사용됩니다.

보안 그룹 컨피그레이션 요약

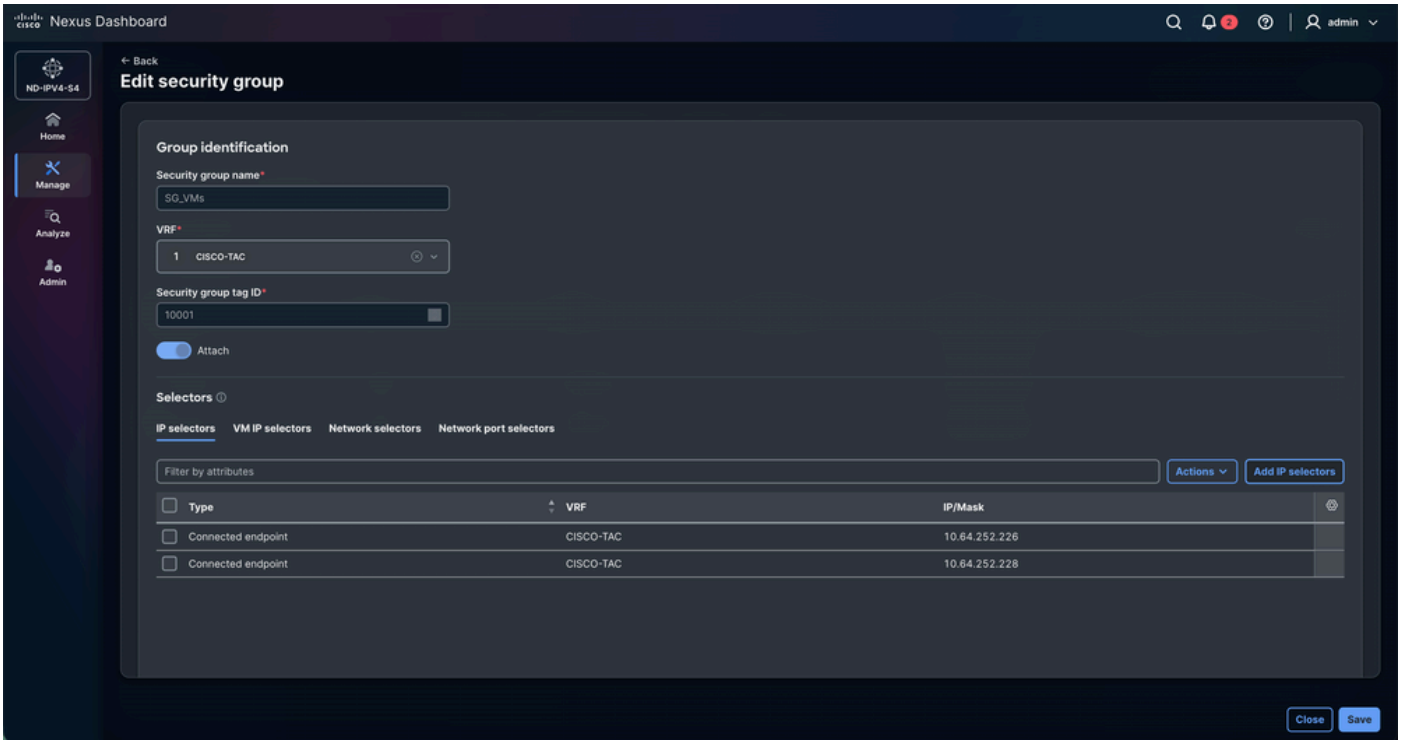
디바이스	보안 그룹 이름	VRF	보안 그룹 태그 ID	선택기
VM-1	SG_VM	시스코-TAC	10001	IP 선택기
VM-2	SG_VM	시스코-TAC	10001	IP 선택기

FW 1	SG_FW	시스코-TAC	10002	IP 선택기
FW 2	SG_FW	시스코-TAC	10002	IP 선택기

VM에 대한 보안 그룹 컨피그레이션



FW용 보안 그룹 컨피그레이션



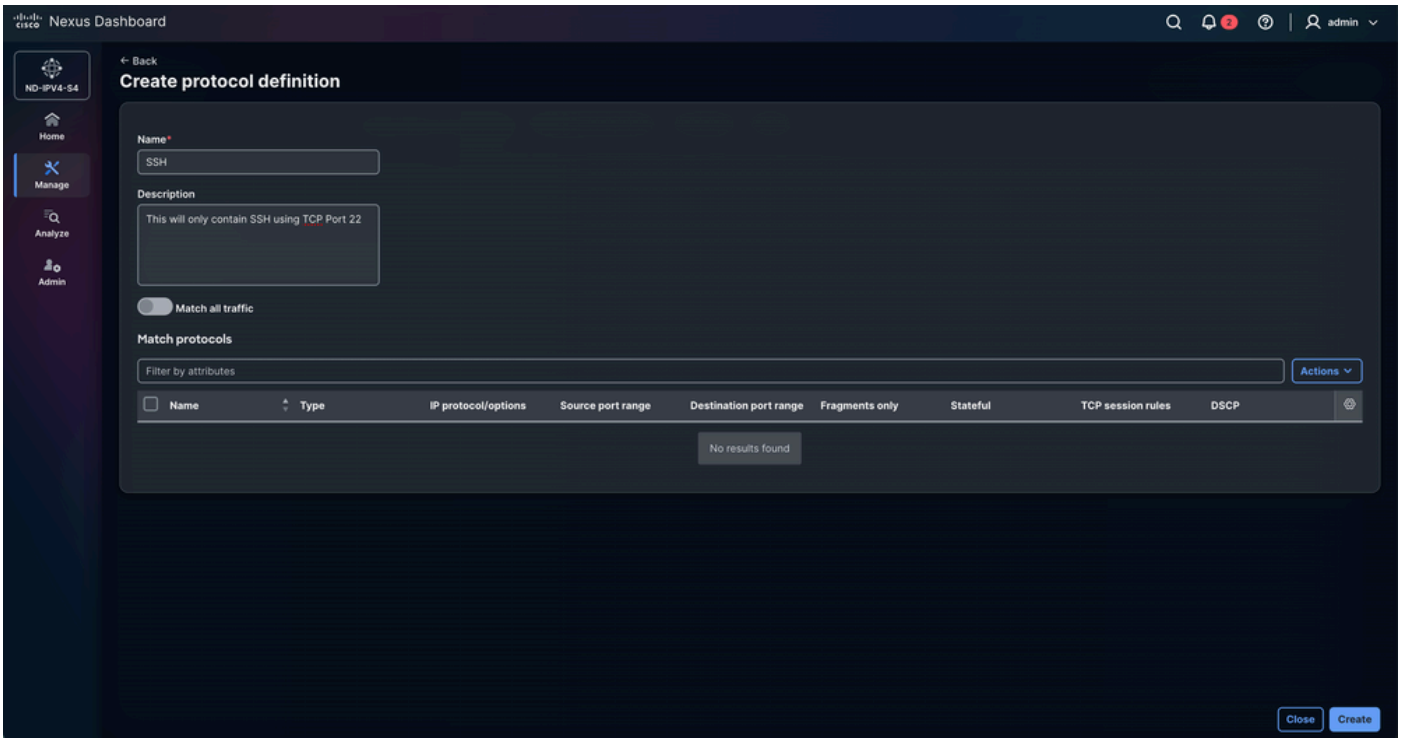
4단계. 프로토콜 정의 구성

Create Protocol Definition 옵션은 GPO(Group Policy Object)에서 일치하는 네트워크 프로토콜 매개변수 및 트래픽 특성을 정의하는 데 사용됩니다. 관리자는 프로토콜 유형, 포트 번호 및 기타 패킷 특성과 같은 기준을 지정하여 해당 정책을 원하는 트래픽 흐름에 적용할 수 있습니다.

이 시나리오에서는 ICMP 트래픽만 허용하면서 포트 22(SSH)에서 TCP 트래픽을 명시적으로 차단하는 것이 목적입니다. 이 정책은 네트워크 연결 가능성 테스트가 계속 허용되고 무단 또는 원하지 않는 SSH 액세스가 수동으로 제한되도록 보장합니다.

Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Segmentation and security(세그멘테이션 및 보안) > Protocol definitions(프로토콜 정의) > Actions(작업) > Create protocol definition(프로토콜 정의 생성)으로 이동합니다.

Name(이름)과 Description(설명)을 입력합니다.



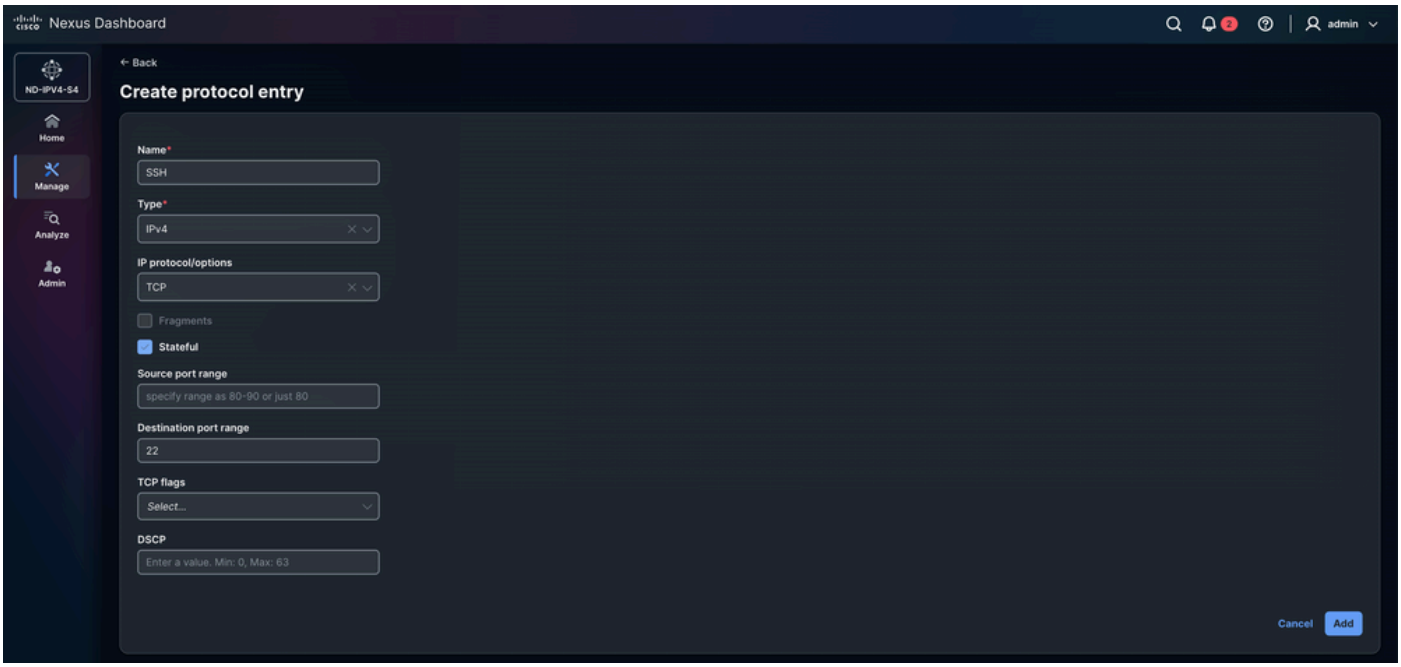
Actions(작업) > Create protocol entry(프로토콜 항목 생성)로 이동합니다.

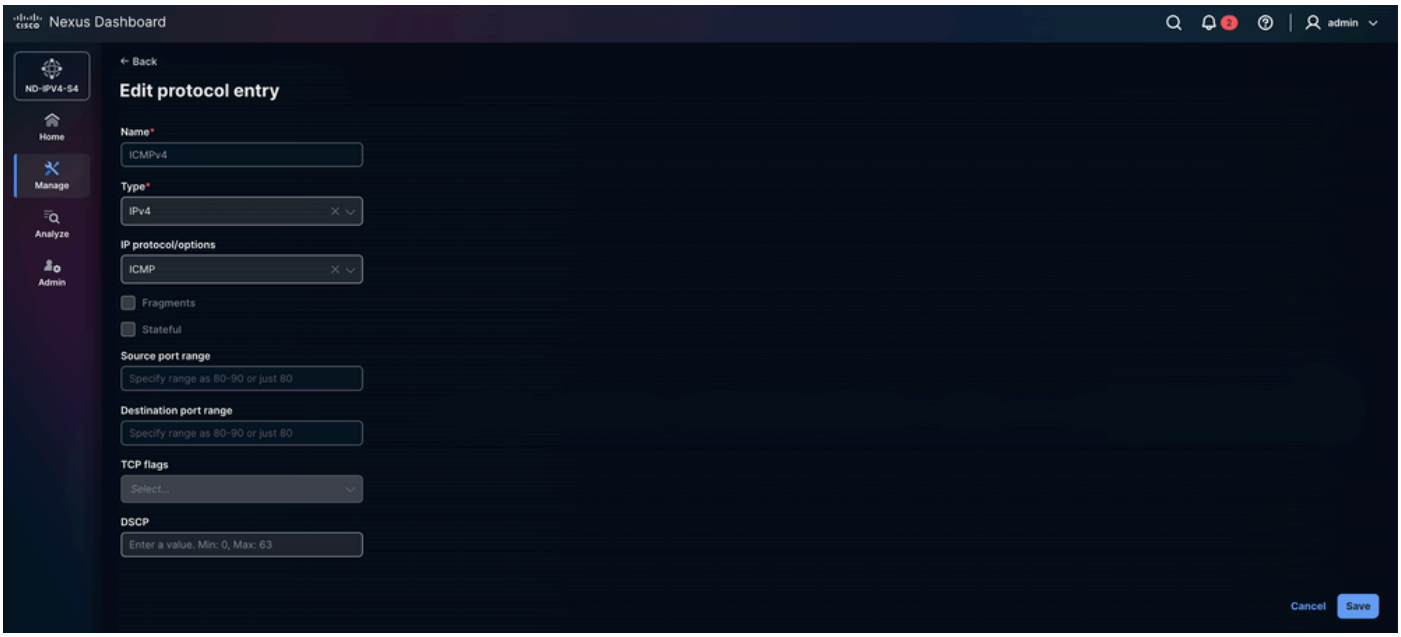
- 이름: SSH
- 유형: IPv4
  - IP 및 IPv6도 사용할 수 있습니다.
- IP 프로토콜/옵션: TCP
  - UDP, EIGRP, PIM 등이 지원됩니다.

- 조각: 규칙이 프래그먼트된 IP 패킷을 매칭할 수 있습니다. 이는 네트워크 MTU를 초과할 때 큰 패킷을 프래그먼트로 분할할 수 있으므로 유용합니다. 이를 활성화하면 해당 프래그먼트에도 정책이 적용됩니다.

- 상태 저장: 스테이트풀 프로세스란 과거에 발생한 모든 변경 사항 또는 상호 작용을 추적하며, 현재 프로세스는 이전 프로세스의 컨텍스트로 수행됩니다. 이 경우 TCP는 전송할 패킷의 수, 패킷의 순서 및 수신자가 패킷을 수신했는지 여부와 같은 영역을 추적합니다. Stateful 옵션을 선택하면 이 정보가 TCP의 상태로 저장됩니다.

- 소스 포트 범위: 이 옵션은 위의 IP Protocol/Options 필드에서 TCP 또는 UDP를 선택한 경우에만 사용할 수 있습니다.
- 대상 포트 범위: 이 옵션은 IP Protocol/Options 필드에서 TCP 또는 UDP를 선택한 경우에만 사용할 수 있습니다.
- TCP 플래그
    - 이 옵션은 IP Protocol/Options(IP 프로토콜/옵션) 필드에서 TCP를 선택한 경우에만 사용할 수 있습니다.
    - 보안 프로토콜에서 사용하는 TCP 플래그를 정의할 수 있습니다.
    - TCP 플래그는 TCP 헤더의 일부로서 연결의 설정, 유지 관리 및 종료를 제어하는 데 사용됩니다.
    - 사용 가능한 옵션:
        - ACK(승인): 수신된 데이터 또는 동기화 패킷에 대한 확인 응답을 나타냅니다.
        - EST(설정): 이미 설정된 TCP 연결을 나타냅니다. 이 옵션이 활성화된 경우 다른 TCP 플래그를 선택할 수 없습니다.
        - FIN(마침): TCP 연결을 정상적으로 닫는 데 사용됩니다.
        - RST(재설정): 연결을 즉시 종료하고 전송 중인 모든 데이터를 버립니다.
        - SYN(동기화): TCP 연결을 시작하고 설정하는 동안 사용됩니다.





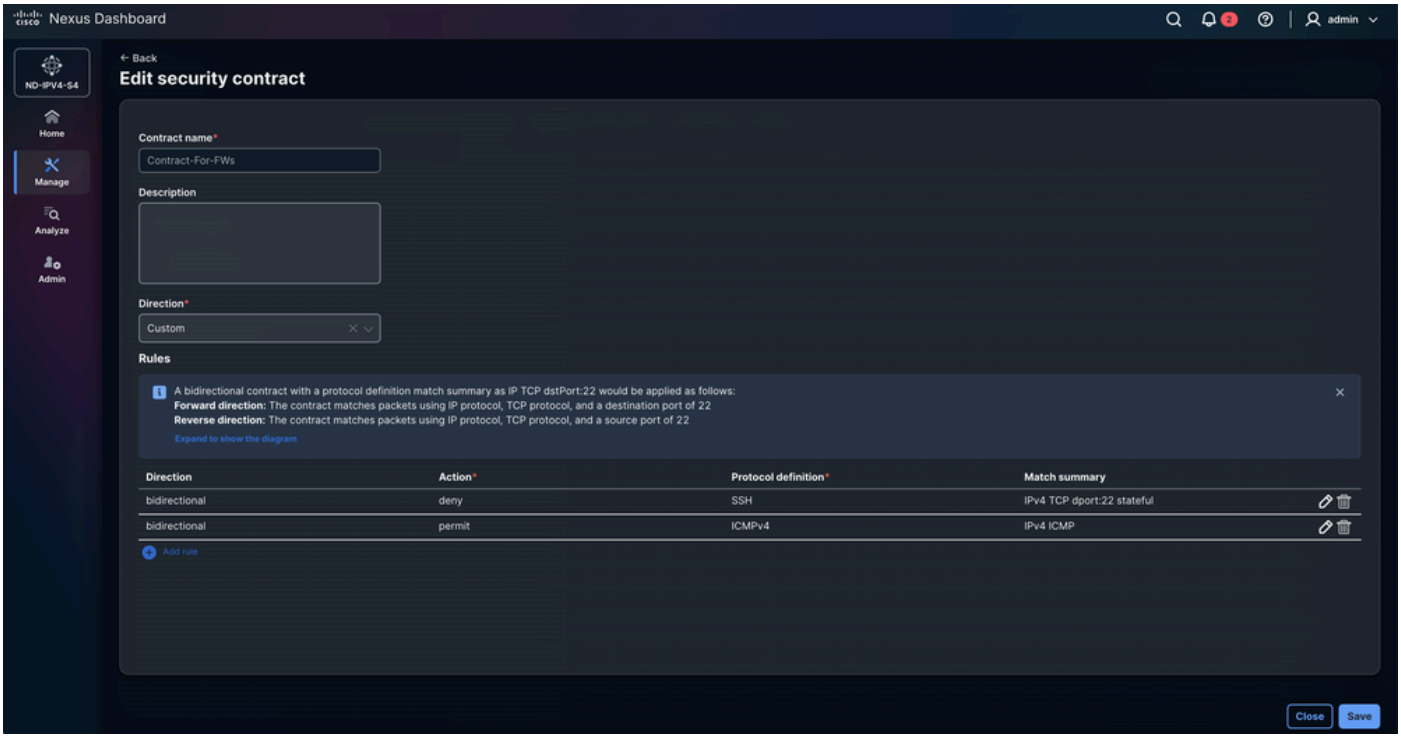
5단계. 보안 계약 구성

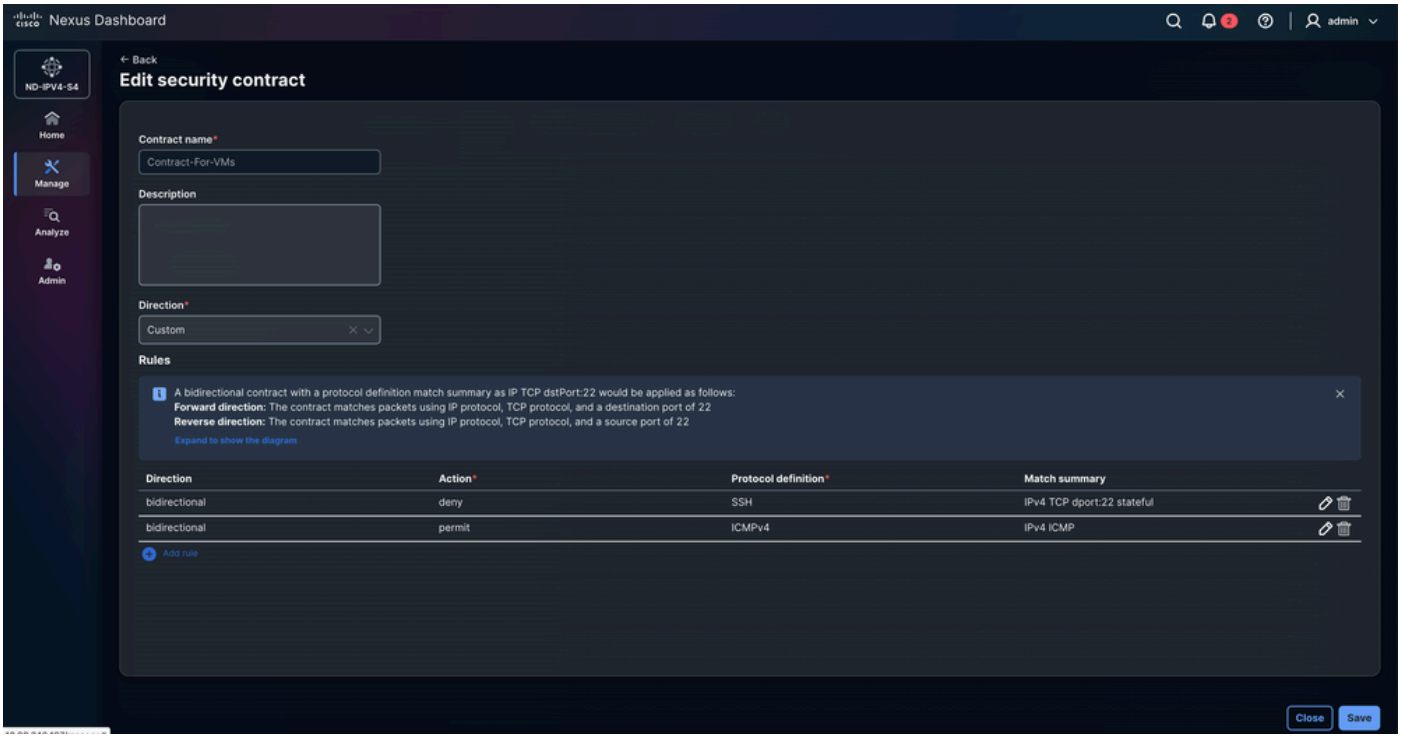
Contract(계약)는 연결된 정책 정의에 따라 허용 또는 거부되는 트래픽을 지정하여 엔드포인트 그룹 간의 통신 규칙을 정의합니다. 또한 구성된 프로토콜 규칙, 필터 및 작업을 적용하는 시행 메커니즘으로 작동하여 소스와 대상 그룹 간의 트래픽이 의도된 보안 및 세그멘테이션 정책을 준수하도록 보장합니다.

Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Segmentation and Security(분할 및 보안) > Security contracts(보안 계약) > Actions(작업) > Create security contract(보안 계약 생성)로 이동합니다.

- Add rule을 선택하고 Direction, Action 및 Protocol 정의를 구성합니다.
  - 양방향:
    - 양방향 계약은 프로토콜 정의 일치 요약을 IP TCP 포트 22로 사용하여 다음과 같이 적용됩니다.
      - 전달 방향: 계약은 IP 프로토콜, TCP 프로토콜, 목적지 포트 22를 사용하여 패킷을 확인합니다
      - 역방향: 계약은 IP 프로토콜, TCP 프로토콜, 소스 포트 22를 사용하여 패킷을 확인합니다.
      - 이는 소스 또는 대상에 관계없이 적용됩니다.
  - 단방향:
    - GPO 보안 계약의 단방향 정책은 트래픽 흐름의 한 방향으로만 적용되므로 동일한

규칙을 반대 방향으로 자동으로 적용하지 않고 소스 보안 그룹에서 대상 보안 그룹으로의 통신을 허용하거나 거부합니다.



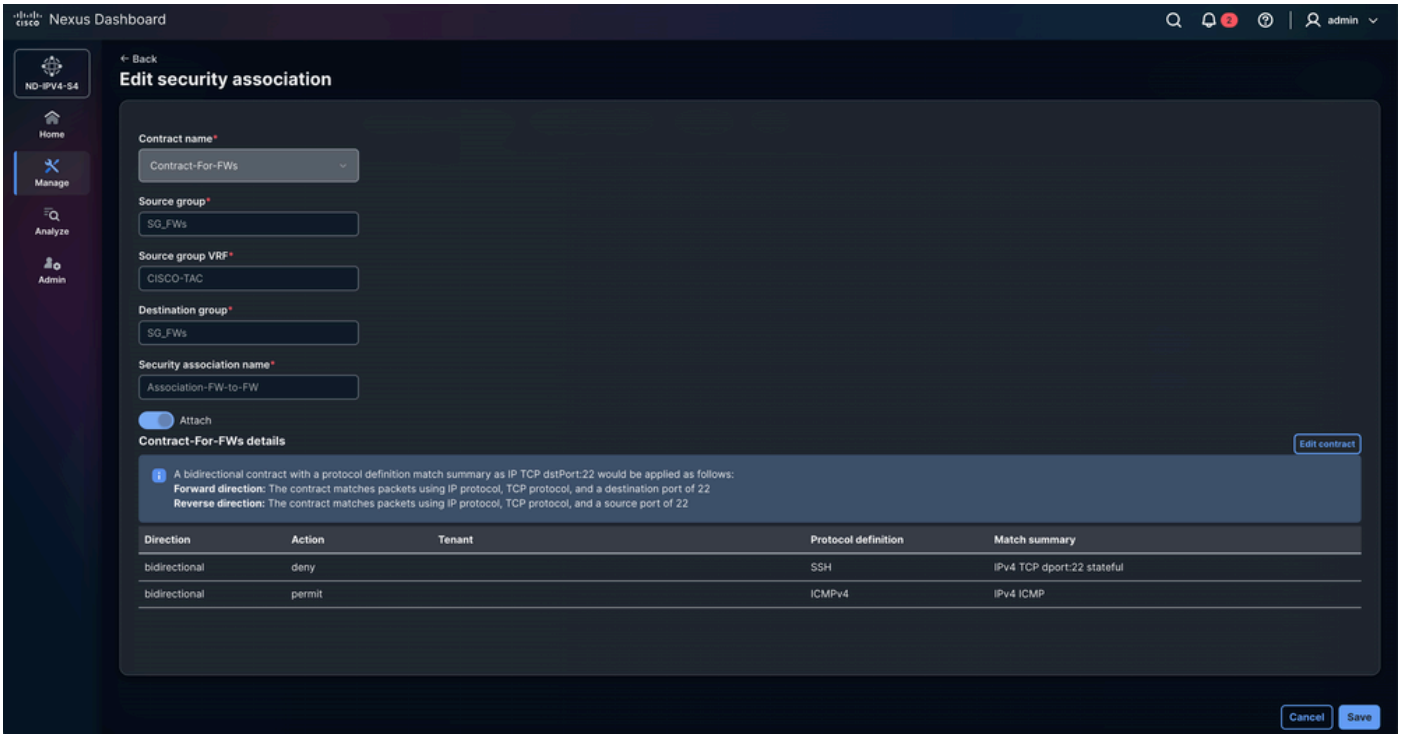


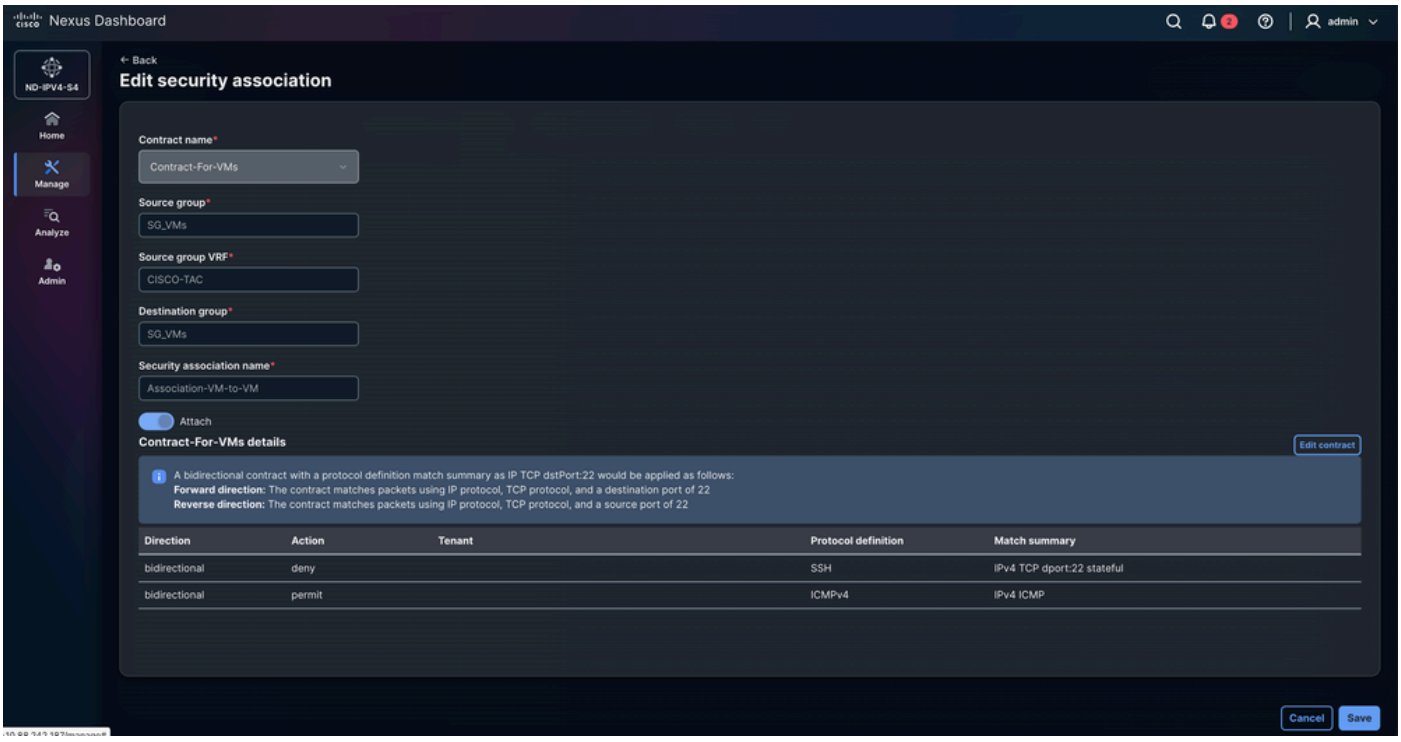
6단계. 보안 연결 구성

Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Segmentation and

Security(분할 및 보안) > Security associations(보안 연계) > Actions(작업) > Create security association(보안 연계 생성)으로 이동합니다.

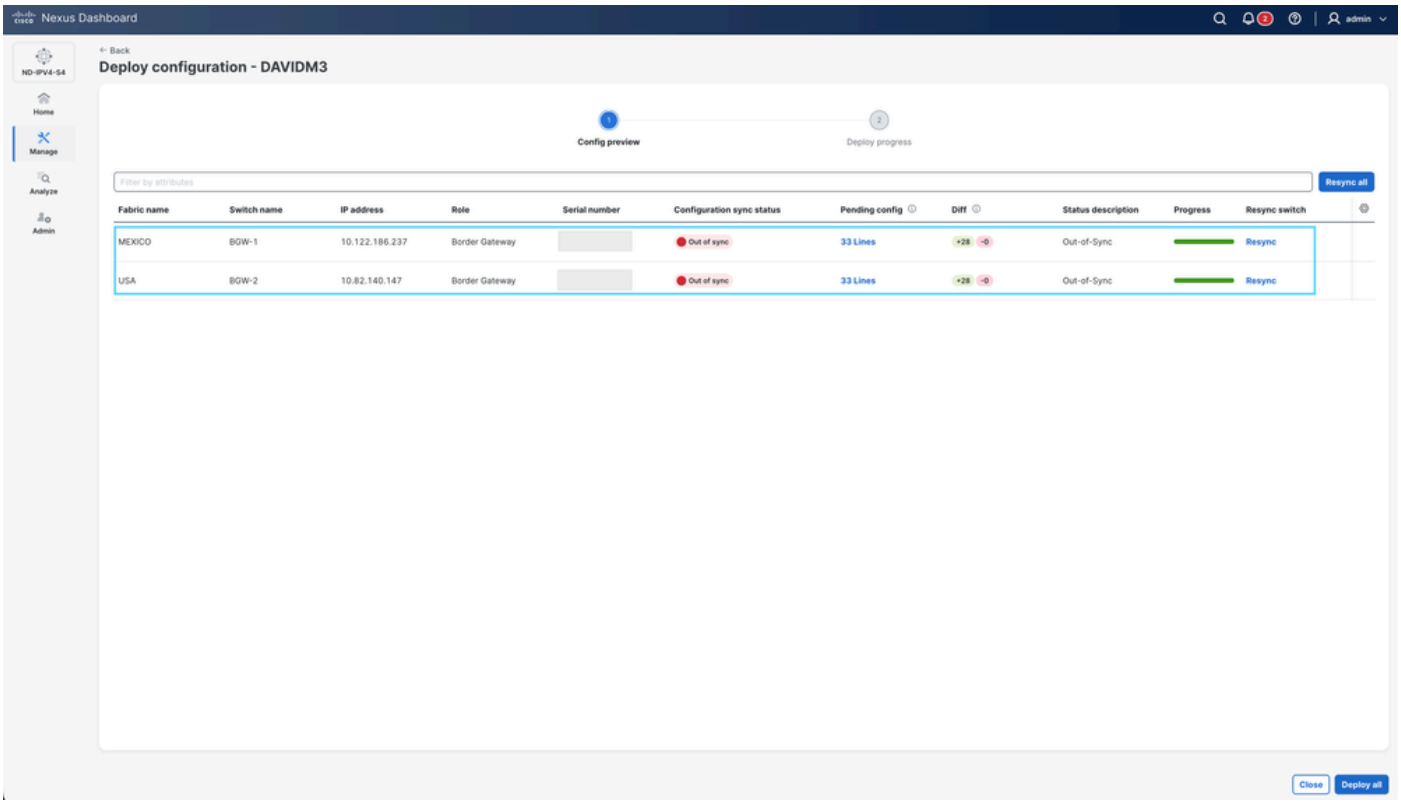
보안 연결 구성에서는 보안 그룹, 프로토콜 정의 및 보안 계약을 연결하여 정책 모델을 정의합니다. 보안 그룹은 엔드포인트를 분류하고, 프로토콜 정의는 트래픽 유형(예: 프로토콜 또는 포트)을 지정하며, 보안 계약은 이러한 프로토콜 규칙을 사용하여 소스 및 대상 보안 그룹 간에 적용되는 정책을 정의합니다. 보안 연결은 패브릭에서 정의된 보안 정책을 시행할 수 있도록 이러한 요소를 함께 바인딩하는 관계를 나타냅니다.

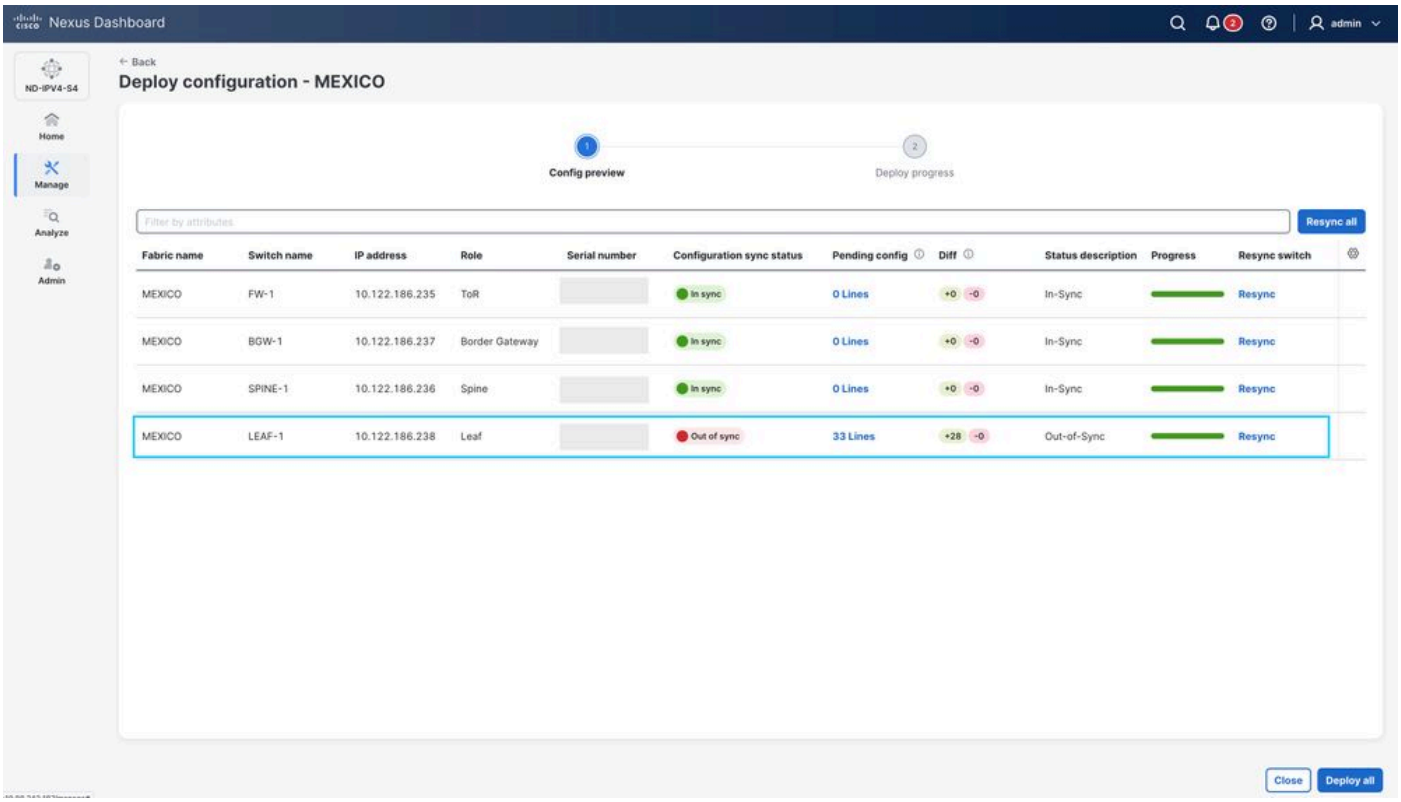


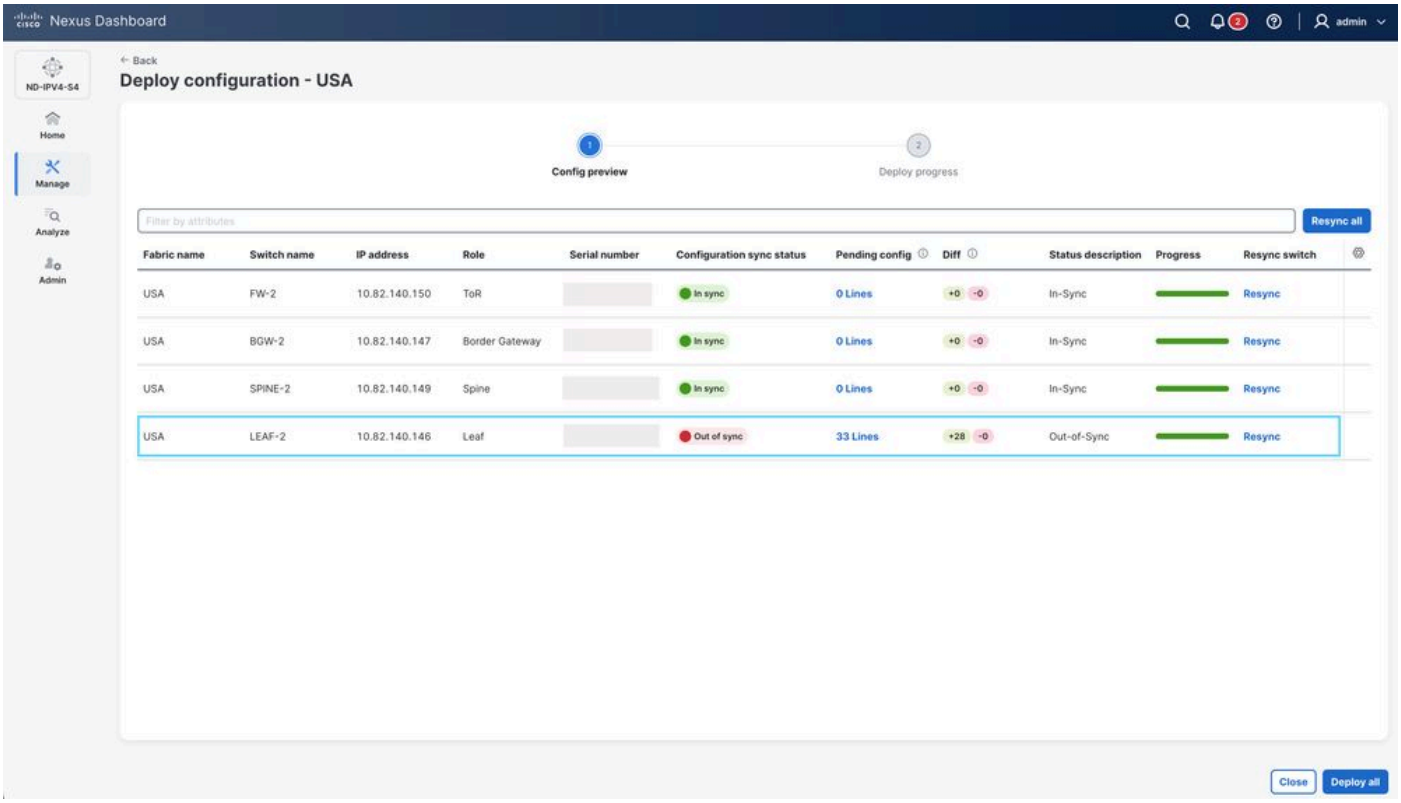


7단계. GPO 구성 검증

- Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Actions(작업) > Recalculate and deploy(다시 계산 및 구축)로 이동합니다.
  - GPO 컨피그레이션은 상위 패브릭 스위치에서 보더 게이트웨이로 푸시됩니다. 디바이스에 구축할 수 있는 컨피그레이션을 검토하고 검증하려면 보류 중인 컨피그레이션 행의 수를 클릭합니다. 이 프로세스는 각 하위 패브릭에 대해 반복되어야 합니다.
  - Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Inventory(인벤토리) > Member fabrics(멤버 패브릭) > MEXICO > Actions(작업) > Recalculate and deploy(다시 계산 및 구축)로 이동합니다.
  - Manage(관리) > Fabrics(패브릭) > Fabric groups(패브릭 그룹) > DAVIDM3 > Inventory(인벤토리) > Member Fabrics(멤버 패브릭) > USA > Actions(작업) > Recalculate and deploy(다시 계산 및 구축)로 이동합니다.

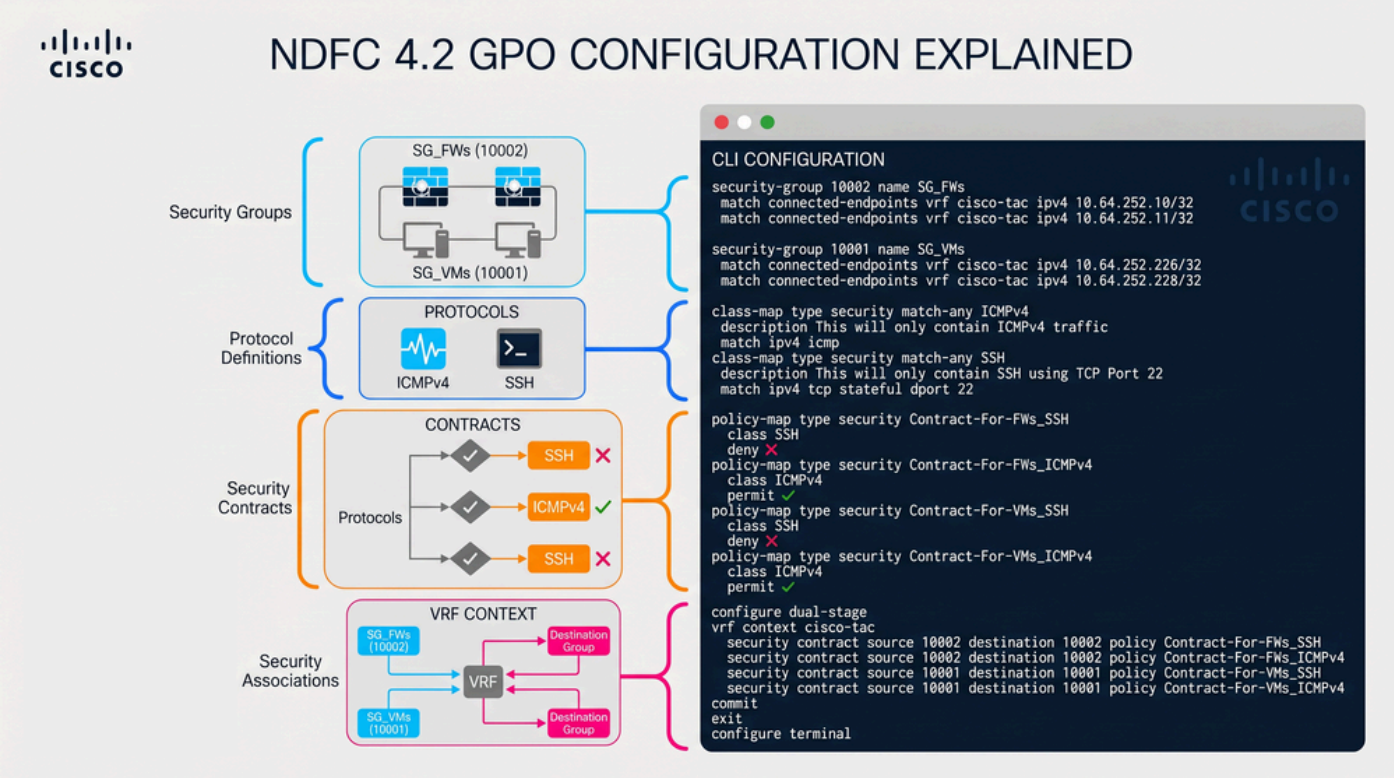






- 이 그림에서는 BGW-1, BGW-2, LEAF-1 및 LEAF-2에 대한 GPO 컨피그레이션을 보여 줍니

다. 컨피그레이션은 모든 스위치에서 동일합니다. NDFC 4.2는 표시된 정확한 순서대로 컨피그레이션을 적용하지 않습니다. 이 섹션에서는 CLI 명령의 논리적 순서를 설명합니다.



VXLAN GPO 작동 문제 해결

1단계. 보안 그룹 기능 상태 확인

스위치에서 보안 그룹 기능이 활성화되어 있는지 확인합니다. VXLAN GPO는 엔드포인트 분류, 계약 적용 및 SGACL 하드웨어 프로그래밍에 필요한 SGT(Security Group Tag) 인프라를 활성화하므로 이 기능에 따라 달라집니다.

<#root>

BGW-1#

show feature | i i security-group

security-group 1 enabled

2단계. 시스템 라우팅 모드 확인

스위치에서 구성된 운영 체제 라우팅 모드를 확인합니다. SGACL 시행은 ASIC 파이프라인 내에서 전용 하드웨어 포워딩 리소스를 사용하기 때문에 VXLAN GPO에는 Security-Groups Support 라우팅 모드가 필요합니다.

<#root>

BGW-1#

show system routing mode

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

3단계. VXLAN NVE 피어 설정 및 GPO 기능 확인

- 로컬 패브릭 디바이스와 원격 멀티 사이트 피어 간의 VXLAN NVE 피어 설정을 검증합니다. VXLAN GPO 정보는 VXLAN EVPN 컨트롤 플레인을 통해 전파되므로 패브릭 전체에서 SGT(Security Group Tag) 학습 및 계약 동기화에 안정적인 NVE 인접성이 필요합니다.
- 원격 VTEP가 VXLAN EVPN 멀티 사이트 도메인 전반의 SGT 전파 및 SGACL 계약 시행에 필요한 VXLAN 그룹 정책 확장을 지원하는지 확인하기 때문에 이 명령에서 가장 중요한 지표 중 하나가 그룹 정책을 사용할 수 있습니다.

<#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

4단계. 보안 그룹 학습 및 엔드포인트 분류 확인

엔드포인트가 SGT(Security Group)로 올바르게 분류되었는지 확인합니다. VXLAN GPO 시행은 정확한 엔드포인트-SGT 매핑에 따라 달라집니다.

<#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
```

5단계. 보안 계약 및 정책 적용 확인

VXLAN GPO 계약이 올바르게 설치되고 작동하는지 확인합니다. 계약은 보안 그룹 간에 적용되는 통신 규칙을 정의하며 마이크로 세그멘테이션을 위해 VXLAN GPO에서 사용되는 핵심 정책 메커니즘을 나타냅니다.

<#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
```

6단계. VRF 보안 적용 상태 확인

스위치에 구성된 모든 VRF에 대한 VXLAN GPO 시행 상태를 확인합니다. 이 명령은 SGACL 정책 및 보안 그룹 계약이 테넌트 VRF 내에서 적극적으로 적용되는지 확인합니다.

출력에서는 cisco-tac VRF가 Enforced(시행)로 설정된 모드를 통해 VXLAN GPO 시행에 적극적으로 참여하고 있음을 확인합니다. 시행 태그(13648)는 이 VRF를 위해 하드웨어에 프로그래밍된 내부 SGACL 정책 컨텍스트를 식별합니다. 기본 작업 거부 로그는 보안 그룹 계약을 통해 명시적으로 허용되지 않은 모든 트래픽이 거부 및 로깅되어 기본 거부 마이크로 세그멘테이션 정책을 구현함을 나타냅니다. 이와 달리, 기본 VRF, 이그레스-로드밸런스-해상도-관리 및 관리 VRF는 미시행 모드에서 작동하므로 VXLAN GPO 정책이 해당 VRF 내에 적용되지 않으며 기본적으로 트래픽이 허용됩니다.

Stats 필드는 VRF 보안 정책과 일치하는 트래픽을 추적합니다. cisco-tac VRF의 값 0은 명령이 실행될 때 일치하지 않는 트래픽이 기본 거부 동작을 트리거하지 않았음을 나타내고, 기본 VRF의 카운터 값 4364는 VXLAN GPO 시행 없이 작동하는 VRF 내의 트래픽 활동을 나타냅니다.

<#root>

BGW-1#

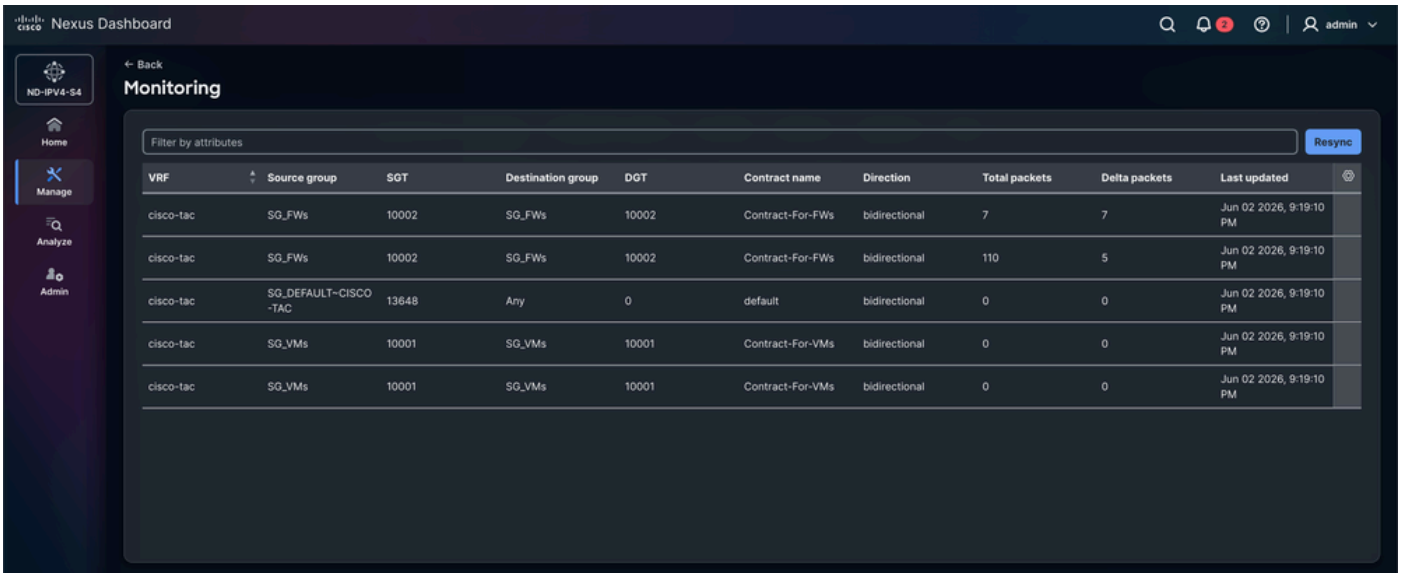
show vrf all security

```
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
```

7단계. VRF 보안 적용 상태 확인

- NDFC GUI에서 VXLAN GPO 계약에 대한 트래픽 일치 통계를 검증합니다. 이 확인은 트래픽이 구성된 보안 그룹 계약과 적극적으로 일치하는지 여부와 SGACL 시행이 VXLAN EVPN 멀티 사이트 패브릭 전체에서 작동하는지를 확인합니다.
- NDFC GUI에서 Manage(관리) > Fabrics(패브릭) > Fabric Groups(패브릭 그룹) > USA/MEXICO(미국/멕시코) > Segmentation and Security(세그멘테이션 및 보안) > Security Associations(보안 연계) > Monitoring(모니터링)으로 이동합니다.
  - 이 섹션에서는 보안 그룹 통신 흐름, 계약 적중 통계, 허용 및 거부 작업, 엔드포인트 그룹 간 운영 계약 활동에 대한 가시성을 제공합니다.
  - 모니터링 통계는 각각 내부에 개별적으로 표시됩니다.
  - NDFC의 모니터링 통계는 패브릭 전반의 실시간 정책 시행 및 트래픽 매칭 동작을 확인하여 CLI 기반 문제 해결을 보완하는 운영 검증 계층을 제공합니다.

참고: NDFC 4.2에서 트래픽 통계를 검토하려는 첫 번째 시도에서 모니터링 섹션이 처음에는 빈 상태로 표시될 수 있습니다. 이 경우 Resync(재동기화) 버튼을 눌러 VXLAN 패브릭에서 계약 통계의 동기화를 트리거합니다. 동기화 프로세스가 실행되는 동안 GUI에 Resync status(재동기화 상태) 메시지가 표시됩니다. 진행 중입니다. 동기화가 완료되면 Ok(확인) 버튼을 눌러 모니터링 뷰를 새로 고칩니다. 재동기화가 완료되면 각 보안 그룹 계약과 연결된 트래픽 통계가 모니터링 섹션에 표시됩니다. 라이브 트래픽 일치 동작을 검증하려면 엔드포인트 간 트래픽을 생성한 다음 Resync 버튼을 다시 눌러 NDFC에 표시된 계약 통계를 업데이트합니다.



- 이전 시나리오에서는 엔드포인트 간에 ICMPv4 트래픽이 성공적으로 허용되었습니다. 그러나 SSH 세션이 설정되면 VXLAN GPO 계약이 포트 22로 향하는 TCP 트래픽을 명시적으로 거부하므로 연결이 시간 초과됩니다.

<#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
```

관련 정보

[Cisco Nexus 9000 Series NX-OS VXLAN 컨피그레이션 가이드, 릴리스 10.6(x)]

VXLAN GPO를 사용한 마이크로 세그멘테이션으로 데이터 센터 보안

VXLAN GPO(Group Policy Option)를 사용한 Cisco NX-OS VXLAN EVPN 패브릭의 마이크로 세그멘테이션 구축

GPO(Group Policy Option) 및 Nexus 대시보드를 사용하여 VXLAN EVPN 패브릭에서 마이크로 세그멘테이션 자동화 및 레이어 4-7 서비스 구축

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.