Configurar o GPO na malha de vários locais do Nexus com NDFC 4.2

Contents

Introdução

Este documento descreve a configuração e validação de GPO em malhas de vários locais VXLAN em switches Nexus Cloud Scale executando NX-OS e NDFC 4.2.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destas áreas:

- Virtual Extensible Local Area Network (VXLAN), Ethernet Virtual Private Network (EVPN) e tecnologias de malha em vários locais
- Switches de escala de nuvem Cisco Nexus e operação do sistema operacional NeXus (NX-OS)
- Fluxos de trabalho de gerenciamento e implantação do Nexus Fabric Network Controller (NDFC) 4.2
- Conceitos de segmentação de rede e política de segurança

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Entender a funcionalidade do GPO em estruturas EVPN VXLAN

A opção de política de grupo (GPO) é um mecanismo de segmentação baseado em políticas projetado para controlar a comunicação entre pontos finais com base na identidade lógica, em vez de depender apenas de endereços IP, VLANs ou sub-redes. O principal objetivo do GPO é simplificar a aplicação da política de segurança e fornecer microssegmentação escalável entre aplicativos, servidores ou cargas de trabalho.

Uma analogia simples é pensar em um hotel onde cada convidado pertence a uma categoria específica ou nível de acesso, certas áreas são acessíveis apenas a convidados específicos e as permissões de acesso dependem da função do convidado em vez do número do quarto. O GPO

funciona de maneira muito semelhante. Em vez de tratar os endpoints apenas como endereços IP, o GPO os classifica em Grupos de Segurança (SGs). As políticas são então aplicadas entre esses grupos para determinar quais comunicações são permitidas ou negadas.

Por exemplo:

- Os servidores Web podem pertencer a um Grupo de segurança.
- Os servidores de aplicativos podem pertencer a outro Grupo de segurança.
- Os servidores de banco de dados podem pertencer a um Grupo de Segurança restrito.

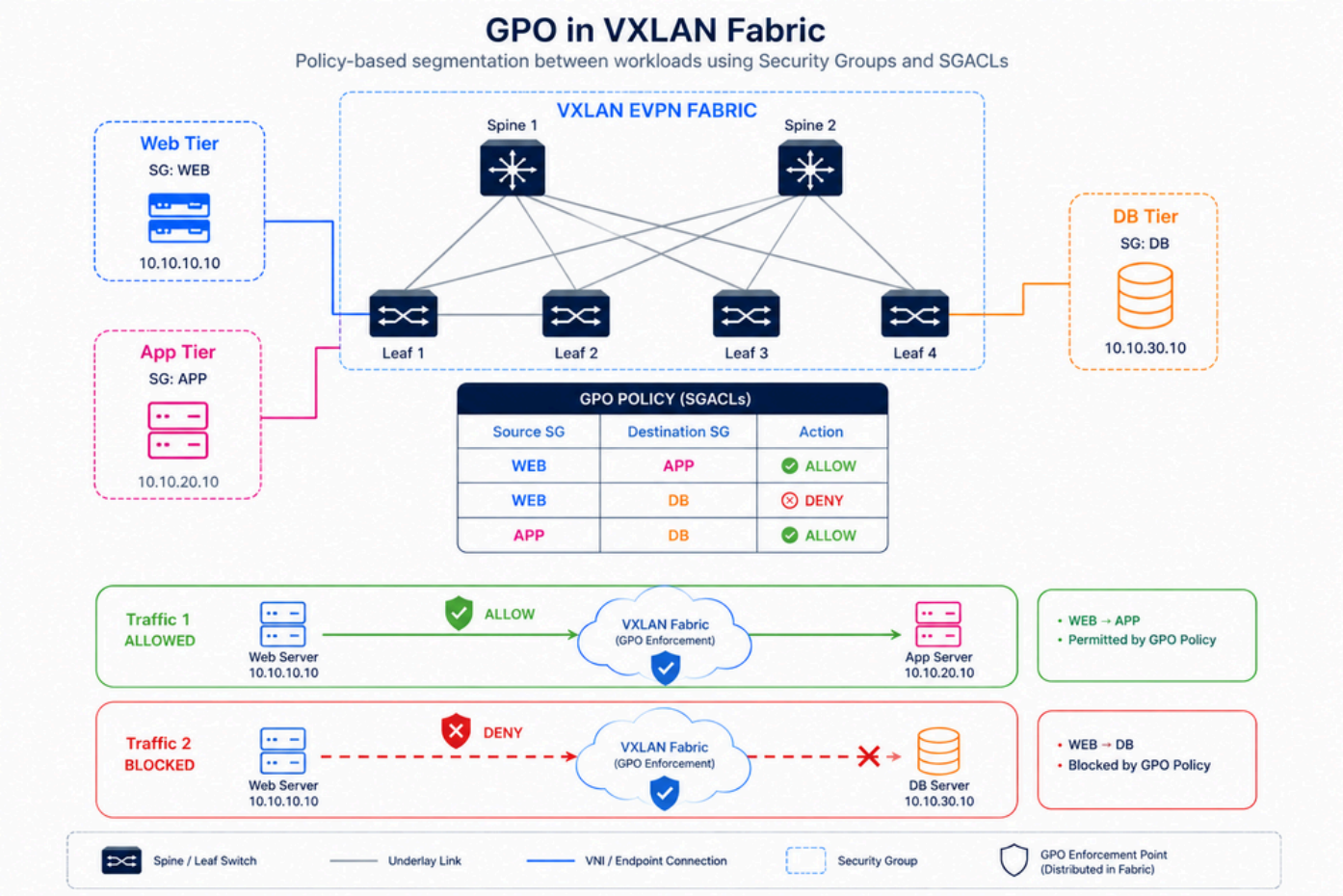
As políticas podem definir:

- Servidores Web podem se comunicar com servidores de aplicativos.
- Servidores de aplicativos podem se comunicar com servidores de bancos de dados.
- Os servidores Web não podem se comunicar diretamente com os servidores de banco de dados.

Essa abordagem simplifica as operações porque os administradores não precisam mais manter um grande número de ACLs em vários dispositivos e VLANs.

Outra grande vantagem é a escalabilidade. Em ambientes grandes, as cargas de trabalho frequentemente se movem, escalam dinamicamente ou alteram endereços IP. O GPO permite que as políticas de segurança permaneçam consistentes mesmo quando o local do ponto de extremidade é alterado. Dentro das estruturas VXLAN EVPN, o GPO estende esse conceito distribuindo informações do Grupo de Segurança na malha e impondo ACLs do Grupo de Segurança (SGACLs) entre os pontos de extremidade. Isso se torna especialmente importante nos data centers modernos, pois o tráfego de ponta a ponta entre as cargas de trabalho geralmente representa a maior superfície de ataque. O GPO melhora a postura de segurança limitando caminhos de comunicação desnecessários dentro da malha do data center.

Para obter um entendimento técnico mais profundo sobre a arquitetura de GPO, conceitos de microssegmentação e aplicação da política de VXLAN, consulte o white paper da Cisco disponível em: Proteção de data centers com microssegmentação usando VXLAN GPO



GPO na estrutura VxLAN

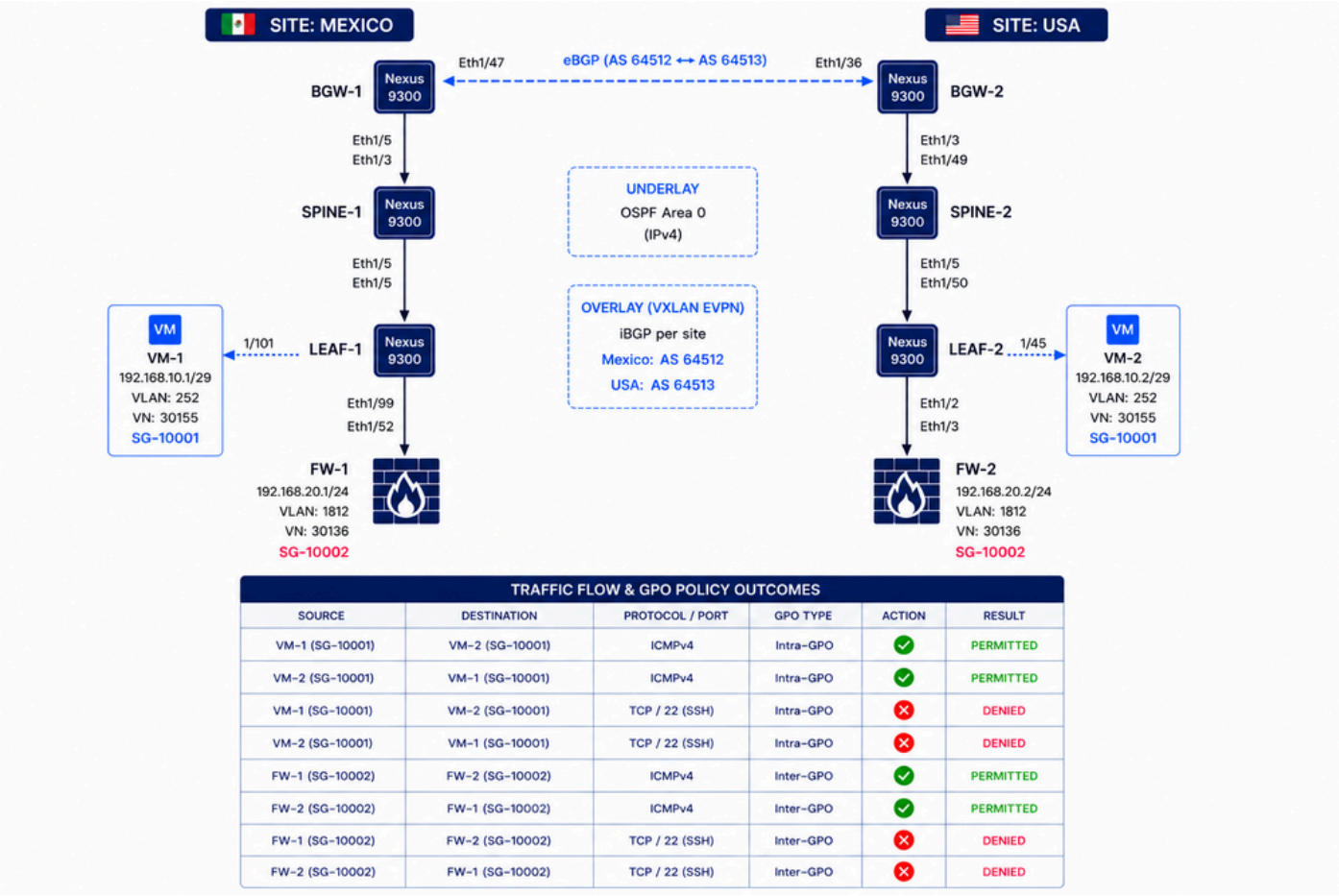
Cenário de implantação de GPO em vários locais de VXLAN usando NDFC 4.2 e NX-OS 10.6(3)F

Essa topologia representa uma malha de vários locais VXLAN implantada em dois locais geograficamente distribuídos: México e EUA. Cada site contém BGWs dedicados, switches Spine, switches Leaf, máquinas virtuais e segmentos de firewall executados em switches Cisco Nexus 9300 com NX-OS 10.6(3)F. A rede subjacente usa o Open Shortest Path First (OSPF), enquanto o plano de controle de sobreposição usa o iBGP dentro de cada site e o eBGP entre BGW-1 e BGW-2 para comunicação VXLAN EVPN entre sites. Como esse ambiente é uma implantação de laboratório, os sites do México e dos EUA são interconectados por meio de um link diretamente conectado entre ambos os BGWs para simplificar o modelo de conectividade Multi-Site.

O GPO é usado para aplicar a microssegmentação baseada em políticas entre Grupos de Segurança (SGs) independentemente do endereçamento IP ou dos limites de VLAN. Com base na tabela de política de conectividade, o tráfego ICMP de VM-1 para VM-2, FW-1 e FW-2 é

permitido, enquanto o tráfego da porta TCP 22 (SSH) de VM-1 para FW-1 e FW-2 é negado. A comunicação da porta TCP 22 entre VM-1 e VM-2 permanece permitida porque ambos os pontos finais pertencem ao mesmo Grupo de Segurança (SG-10001). Esse comportamento demonstra como o GPO aplica dinamicamente diferentes políticas de tráfego entre as comunicações dentro do GPO e entre GPO na malha de vários locais da VXLAN.

Note: O Cisco NX-OS versão 10.6(3)F introduz que você pode restringir a comunicação entre os endpoints dentro do mesmo ESG (também conhecido como SG) usando o recurso de isolamento intraESG. Esse recurso minimiza o risco de acesso não autorizado no ESG e melhora a postura de segurança.



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

Configurar o GPO Passo a Passo com NDFC 4.2 em Estruturas VXLAN EVPN

Essas etapas se aplicam quando a estrutura de vários locais VXLAN já está operacional e configurada com NDFC 4.2, e o GPO precisa ser implementado posteriormente. A seção Automação usando o painel do Nexus em Proteção de data centers com microssegmentação

usando VXLAN GPO mostra a configuração a partir da criação de uma estrutura de site único VXLAN.

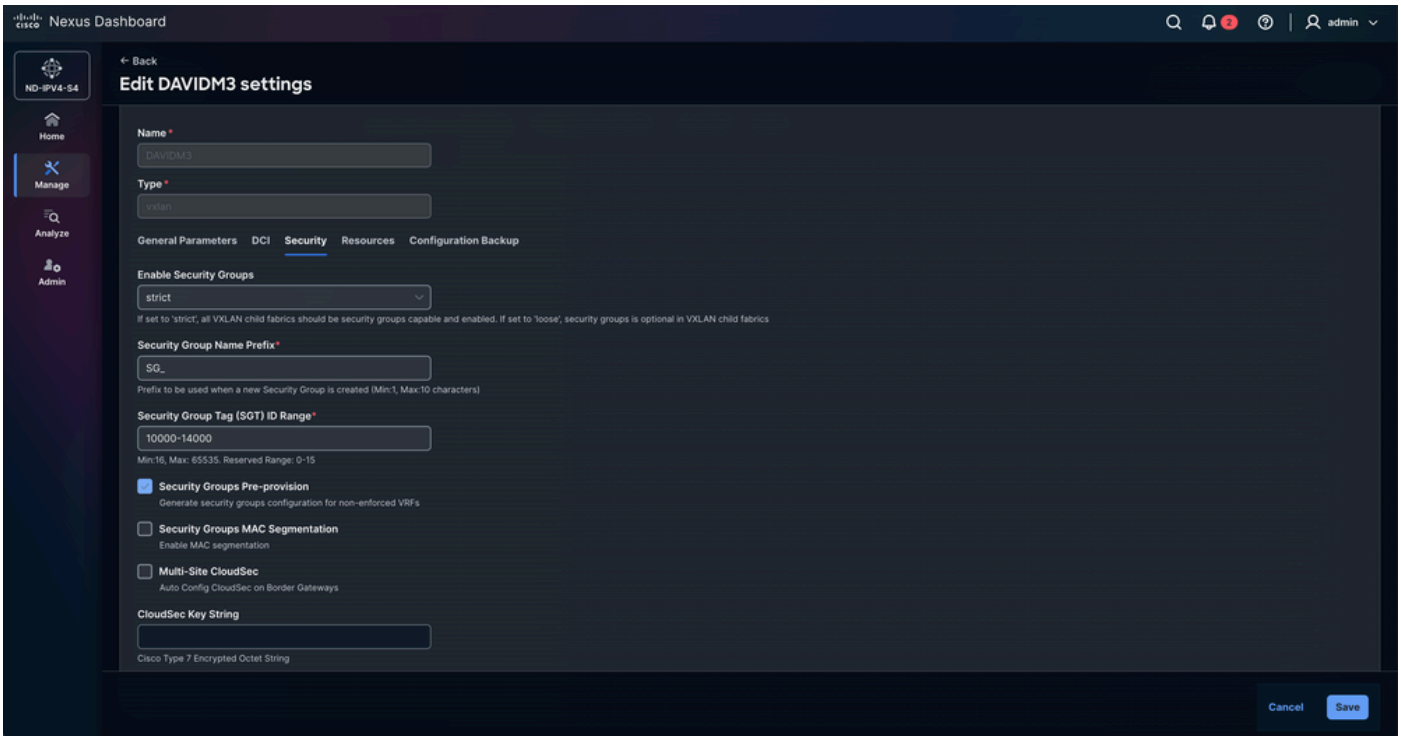
Caution: Quando o GPO opera em uma estrutura VXLAN EVPN, a comunicação ocorre somente se o alcance do destino existir e a política de segurança permitir o tráfego. A aplicação da política depende das informações de IP, que exigem entradas ARP e SVIs para redes internas. Isso significa que a VLAN que pertence ao locatário VRF deve ter um SVI configurado. Consequentemente, a aplicação não se aplica ao tráfego que contém apenas cabeçalhos da Camada 2 e, portanto, não pode ser usado com a extensão da Camada 2 de VXLAN. O NX-OS Versão 10.6(2)F introduz o suporte à microssegmentação baseada em MAC.

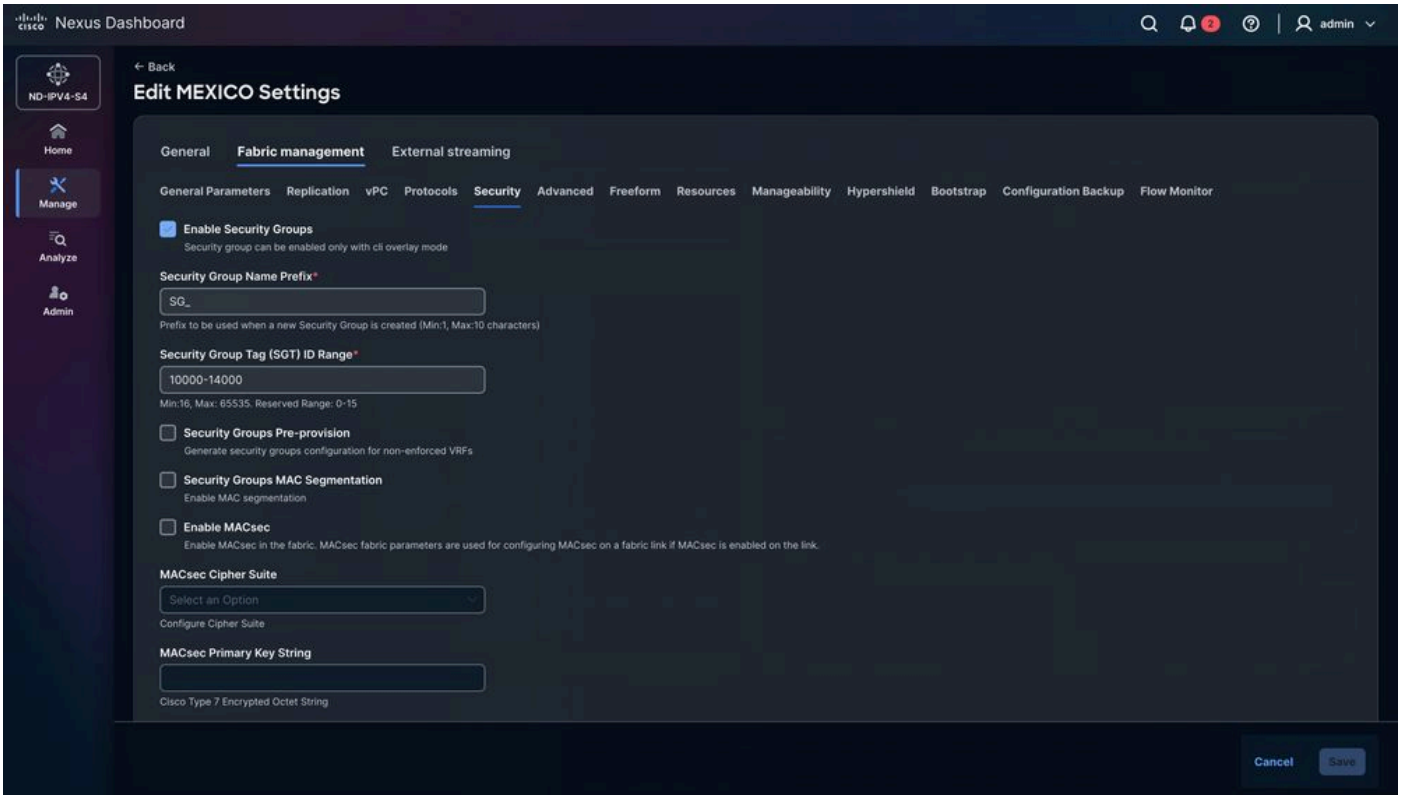
Etapa 1. Ativar grupos de segurança na malha pai

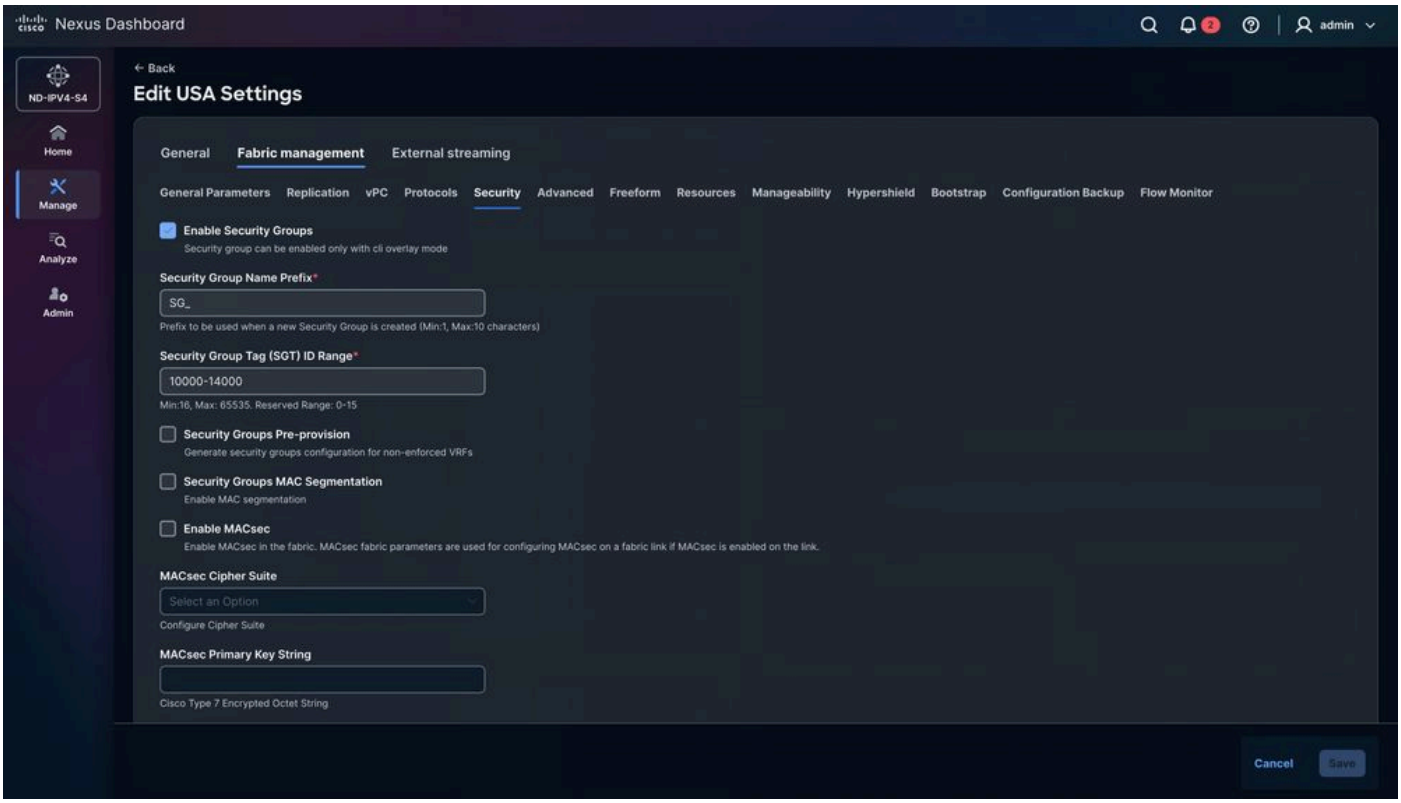
- Navegue para Gerenciar > Grupos de estrutura, selecione o grupo de estrutura DAVIDM3 e escolha Ações > Editar configurações do grupo de estrutura. Na seção Segurança, ative Segurança Grupos, defina o modo como Estrito e defina Segurança Grupos Pré-provisionamento.
    - Selecione o grupo de estrutura de interesse. Para este exemplo, o grupo de malha selecionado é chamado de DAVIDM3, que também é o nome da Malha de vários sites.
- Repita essas etapas para cada malha filho.
    - Navegue até Manage > Fabric, selecione USA e navegue até Actions > Edit Fabric Group Settings. Na seção Segurança, ative Grupos de segurança e defina o modo como Estrito.
    - Navegue até Manage > Fabric, selecione MEXICO e navegue até Actions > Edit Fabric Group Settings. Na seção Segurança, ative Grupos de segurança e defina o modo como Estrito.

Note: Se definido como estrito, todas as estruturas secundárias VXLAN devem ser compatíveis com grupos de segurança e ativadas. Se definido como solto, os grupos de segurança são opcionais nas malhas secundárias VXLAN.

Tip: Para manter uma visibilidade clara, use os mesmos intervalos de ID de Security Group Tag (SGT) na malha principal e em todas as malhas secundárias. A gama de tecidos pai deve abranger as gamas utilizadas por todos os tecidos filhos.


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



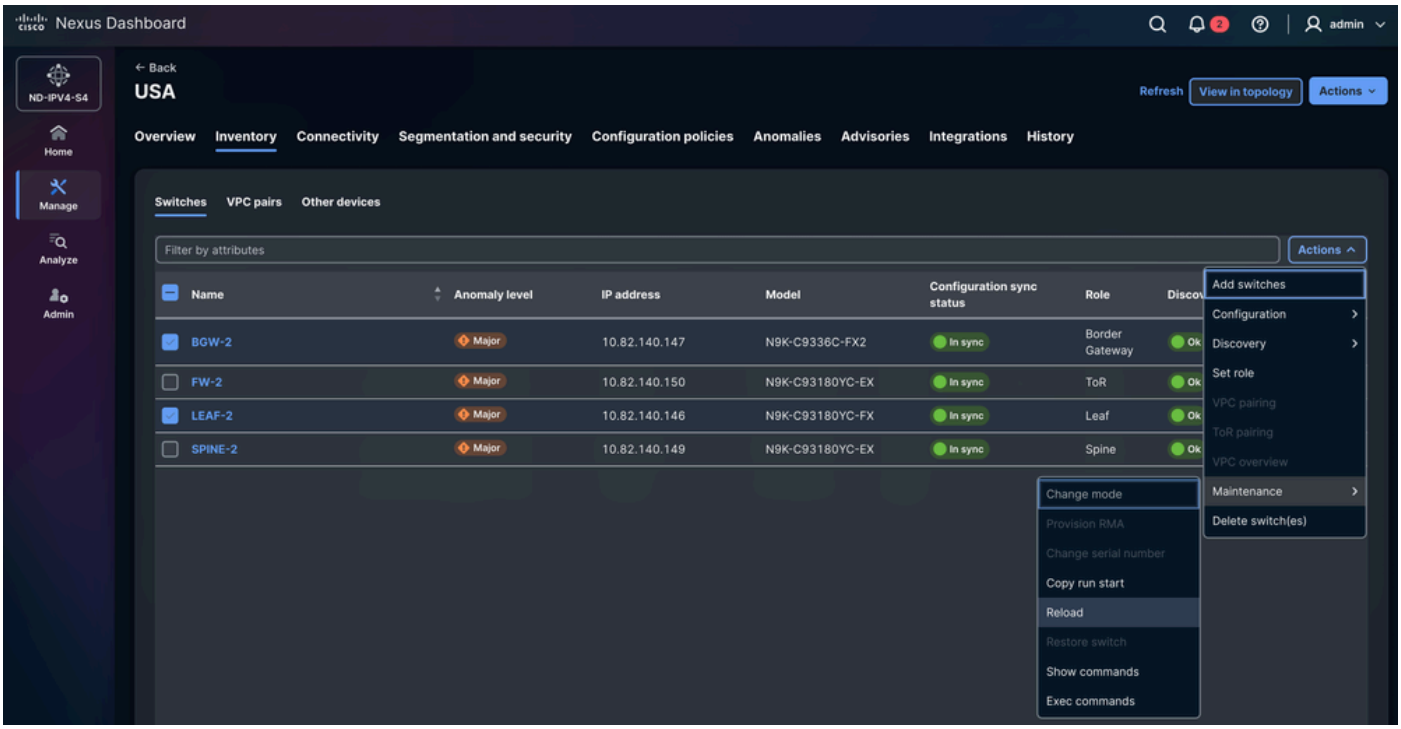
Etapa 2. Recalcular a configuração de estrutura e recarregar switches para implantação de GPO

O NDFC solicita automaticamente que você recarregue um grupo específico de switches Nexus com base em sua função. Neste exemplo, LEAF-1, LEAF-2, BGW-1 e BGW-2 devem ser recarregados. Esta ação deve ser executada manualmente pelo administrador da rede. O recarregamento é necessário e não pode ser ignorado porque o GPO requer gravação TCAM.

Note: Se o dispositivo não for recarregado, a alteração de TCAM pode aparecer na configuração de execução; no entanto, como o switch não foi reinicializado, a configuração não é aplicada à memória de hardware. Como resultado, o recurso não pode funcionar como esperado.

Para recarregar os switches Nexus:

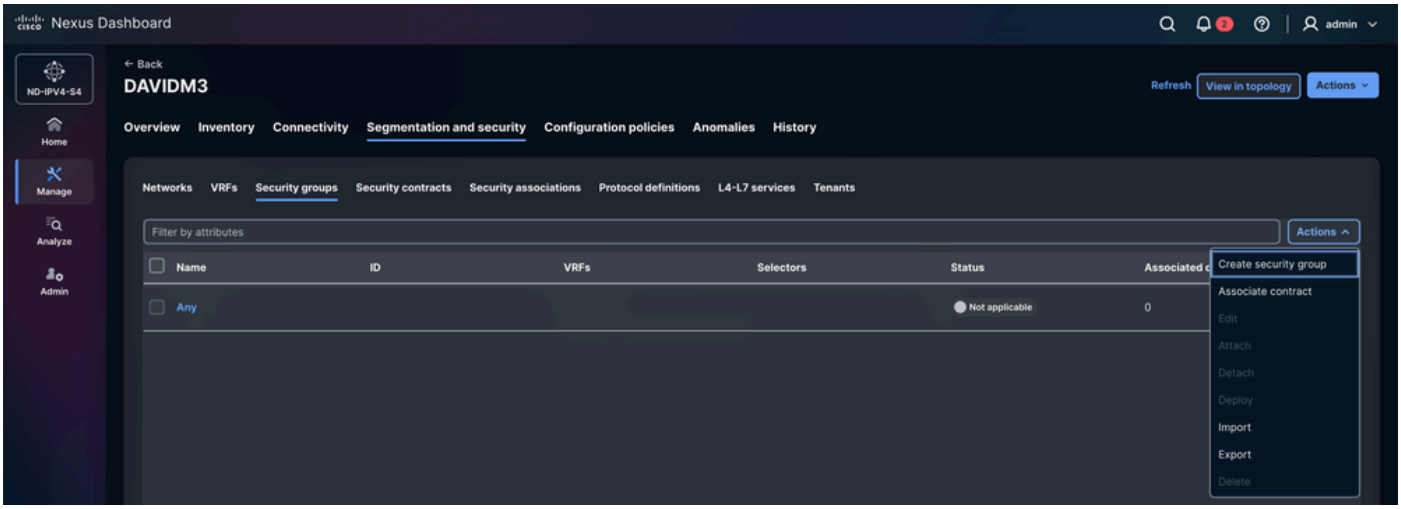
Navegue até Manage > Fabrics > MEXICO/USA > Inventory > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions > Maintenance > Reload.



Etapa 3. Criar Grupo de Segurança

Defina os Grupos de Segurança para cada endpoint. Cada endpoint nas estruturas VXLAN pode ter um único Grupo de Segurança. Essa abordagem não é escalável com eficiência. Agrupe endpoints globalmente (máquinas virtuais, firewalls, otimizadores de TCP, entre outros).

Navegue para Gerenciar > Estruturas > Grupos de estrutura > DAVIDM3 > Segmentação e segurança > Grupos de segurança > Ações > Criar grupo de segurança.



Etapa 3.1 Configurar o nome do grupo de segurança

- A NDFC atribui automaticamente um nome aleatório. O nome pode ser alterado; é recomendável usar um nome representativo que seja fácil para os endpoints identificarem.
- Neste cenário:
    - VMs -> SG_VMs
    - FWs -> SG_FWs

Etapa 3.2 Configurar o VRF

- Selecione o locatário (VRF) ao qual os endpoints pertencem.
- Neste cenário: As VMs e os Firewalls pertencem ao locatário do CISCO-TAC.

Opcional, Criar VRF.

Por padrão, um VRF de locatário recém-criado tem o modo de aplicação de política definido como Não aplicado. Nesse estado, mesmo que os critérios de classificação e SGACLs entre grupos de segurança estejam configurados, não ocorre aplicação de política. Para ativar a aplicação de SGACL, o VRF deve ser explicitamente configurado no modo Enforced.

Quando o VRF opera no modo Enforced, um comportamento de política padrão é definido:

- Negar: Todo o tráfego unicast é descartado a menos que seja explicitamente permitido por uma regra de permissão.
- Permitir: Todo o tráfego unicast é permitido, a menos que seja explicitamente bloqueado por uma regra deny.

Os endpoints que pertencem ao mesmo grupo de segurança podem se comunicar entre si sem a necessidade de regras SGACL. Os SGACLs definem políticas de segurança apenas entre diferentes grupos de segurança.

O Cisco NX-OS versão 10.6(3)F introduz a capacidade de restringir a comunicação entre os endpoints dentro do mesmo GPO, também conhecido como recurso de isolamento dentro do GPO. Antes desta versão, as regras aplicadas aos endpoints dentro do mesmo Grupo de segurança são ignoradas e o tráfego é permitido por padrão.

Etapa 3.3 Configurar ID da tag do grupo de segurança

O NDFC atribui automaticamente um ID de tag aleatório do intervalo predefinido na configuração de estrutura. Embora um ID de tag possa ser selecionado manualmente, ele deve estar dentro do intervalo definido para as malhas filho e pai.

Neste cenário:

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

Etapa 3.4 Anexar

Se a opção Attach não estiver habilitada, o Security Group não será aplicado ao locatário do CISCO-TAC.

Etapa 3.5 Configurar os seletores

- Os seletores determinam quais endpoints e endereços IP externos estão associados a um grupo de segurança específico.

O NDFC 4.2 suporta originalmente três tipos de seletores:

1) Seletores de IP: os seletores de IP associam endpoints ou sub-redes IP a um grupo de segurança com base nas informações de IP.

a. Endpoint conectado - identifica endpoints diretamente conectados à malha, como máquinas virtuais, servidores ou hosts físicos conectados a switches leaf.
b. Sub-rede Externa - Associa prefixos IP externos a um Grupo de Segurança. Esse tipo é usado para redes que existem fora da estrutura de VXLAN, como data centers externos, segmentos de WAN ou redes voltadas para a Internet. O tráfego originado ou destinado a esses prefixos é classificado com o Grupo de segurança configurado.

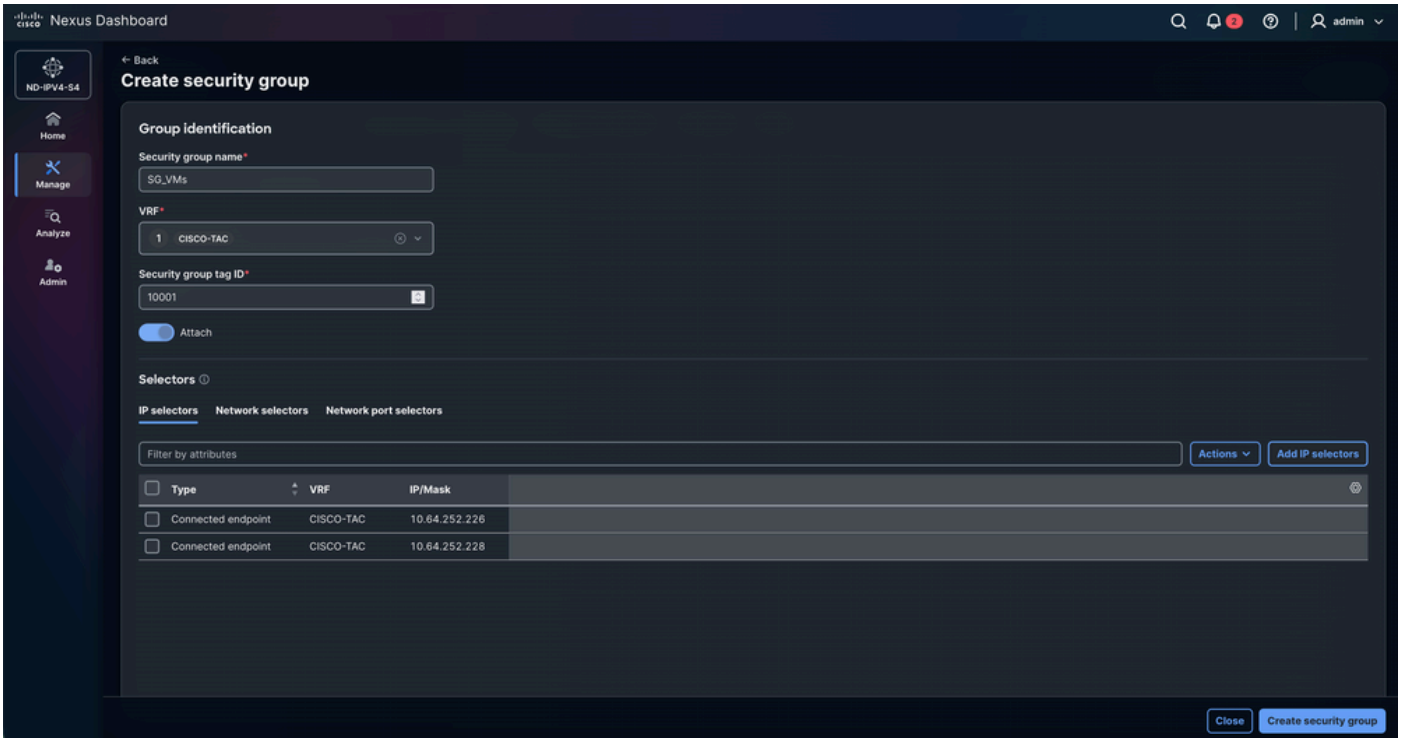
2) Seletores de rede: os seletores de rede associam um Grupo de segurança a um segmento de rede VXLAN específico. A classificação é aplicada com base no identificador de rede (L2VNI). Todos os endpoints pertencentes a essa rede herdam o Grupo de Segurança atribuído, que simplifica a implantação de políticas quando vários endpoints compartilham o mesmo segmento.

3) Seletores de porta de rede: os seletores de porta de rede classificam o tráfego com base na interface física do switch por meio da qual o tráfego entra na estrutura. Um Grupo de segurança pode ser atribuído ao tráfego recebido em uma porta ou interface específica. Essa abordagem é normalmente usada para dispositivos conectados por redes externas, dispositivos de serviço ou links de infraestrutura onde a classificação IP do endpoint não é viável.

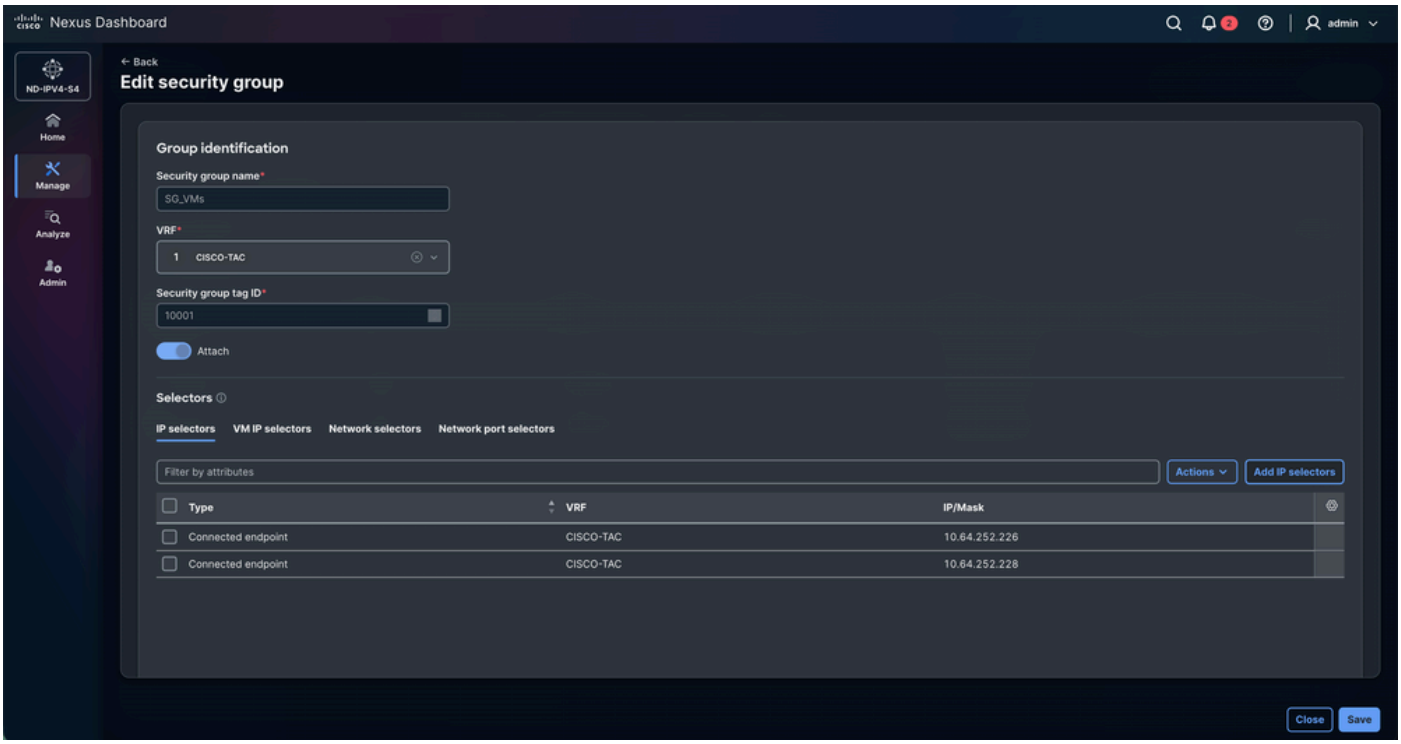
Resumo da configuração do grupo de segurança

Dispositivo	Security Group Name	VRF	ID da tag do grupo de segurança	Seletores
VM-1	SG_VMs	CISCO-TAC	10001	Seletores de IP
VM-2	SG_VMs	CISCO-TAC	10001	Seletores de IP
FW-1	SG_FWs	CISCO-TAC	10002	Seletores de IP
FW-2	SG_FWs	CISCO-TAC	10002	Seletores de IP

Configuração do grupo de segurança para VMs



Configuração do grupo de segurança para FWs



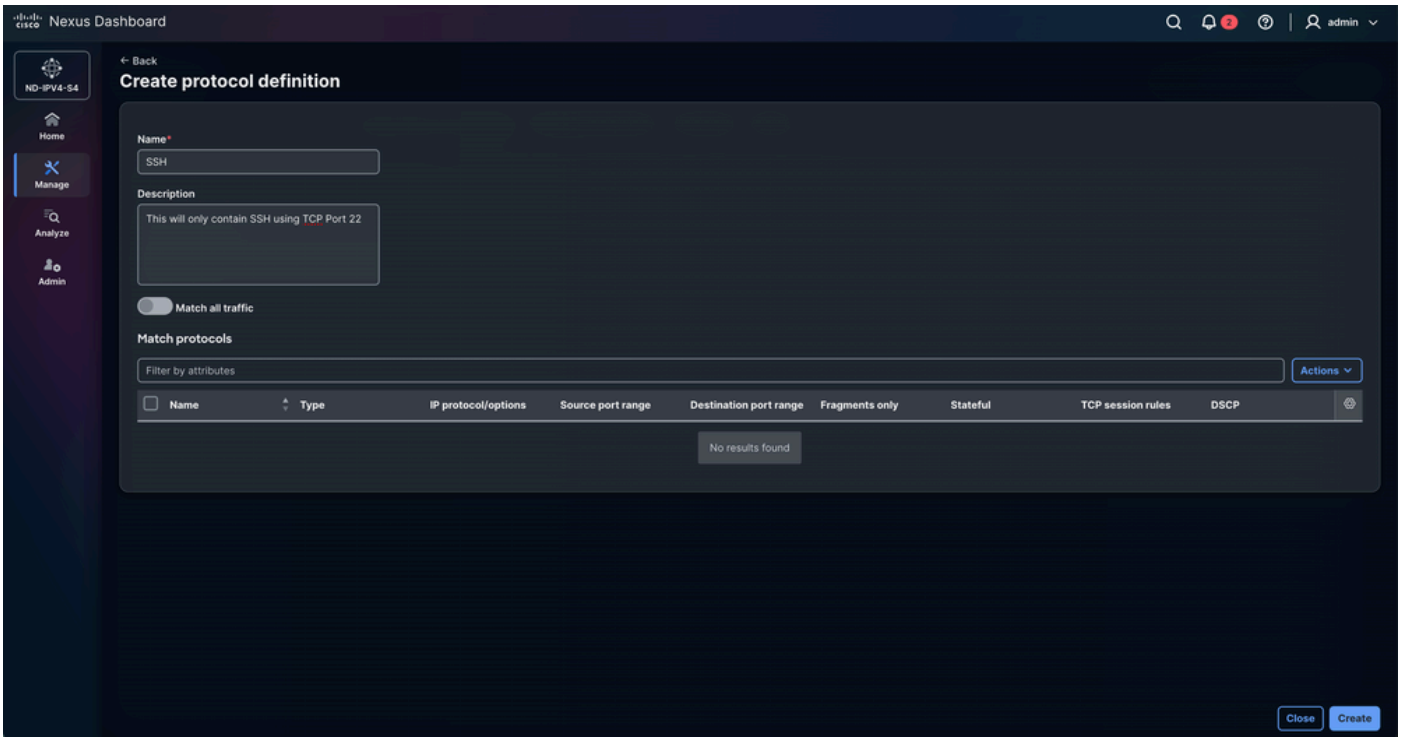
Etapa 4. Configurar Definições de Protocolo

A opção Criar definição de protocolo é usada para definir os parâmetros de protocolo de rede e as características de tráfego que são correspondidos por um Objeto de Diretiva de Grupo (GPO). Ele permite que os administradores especifiquem critérios como tipo de protocolo, números de porta e outros atributos de pacote para que a política correspondente possa ser aplicada aos fluxos de tráfego desejados.

Neste cenário, o objetivo é permitir somente o tráfego ICMP enquanto bloqueia explicitamente o tráfego TCP na porta 22 (SSH). Essa política garante que o teste de acessibilidade da rede permaneça permitido, enquanto o acesso SSH não autorizado ou indesejado é manualmente restrito.

Navegue para Gerenciar > Estruturas > Grupos de estrutura > DAVIDM3 > Segmentação e segurança > Definições de protocolo > Ações > Criar definição de protocolo.

Insira o Nome e a Descrição.



Navegue até Ações > Criar entrada de protocolo.

- Nome: SSH
- Tipo: IPv4
    - IP e IPv6 também estão disponíveis.
- Protocolo IP/opções: TCP
    - UDP, EIGRP e PIM, entre outros, são suportados.

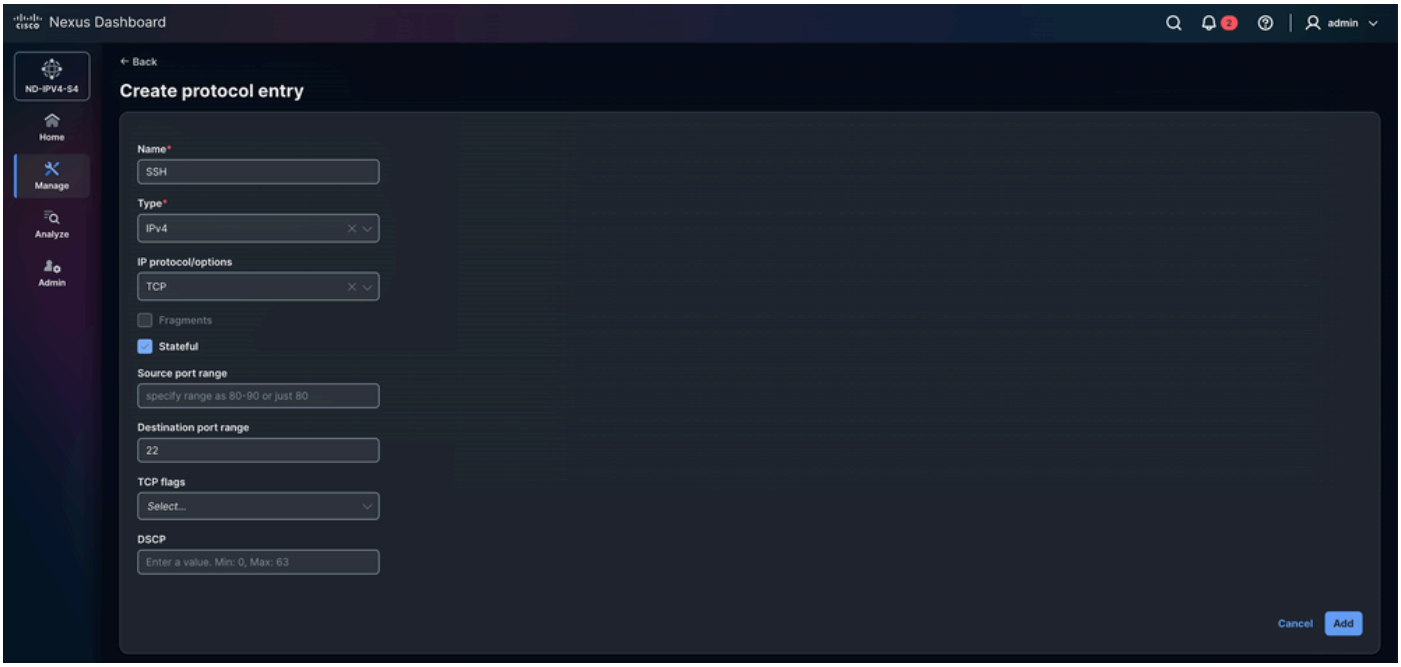
- Fragmentos: Permite que a regra corresponda a pacotes IP fragmentados. Isso é útil porque pacotes grandes podem ser divididos em fragmentos quando excedem o MTU da rede. Habilitar isso garante que a política também se aplique a esses fragmentos.

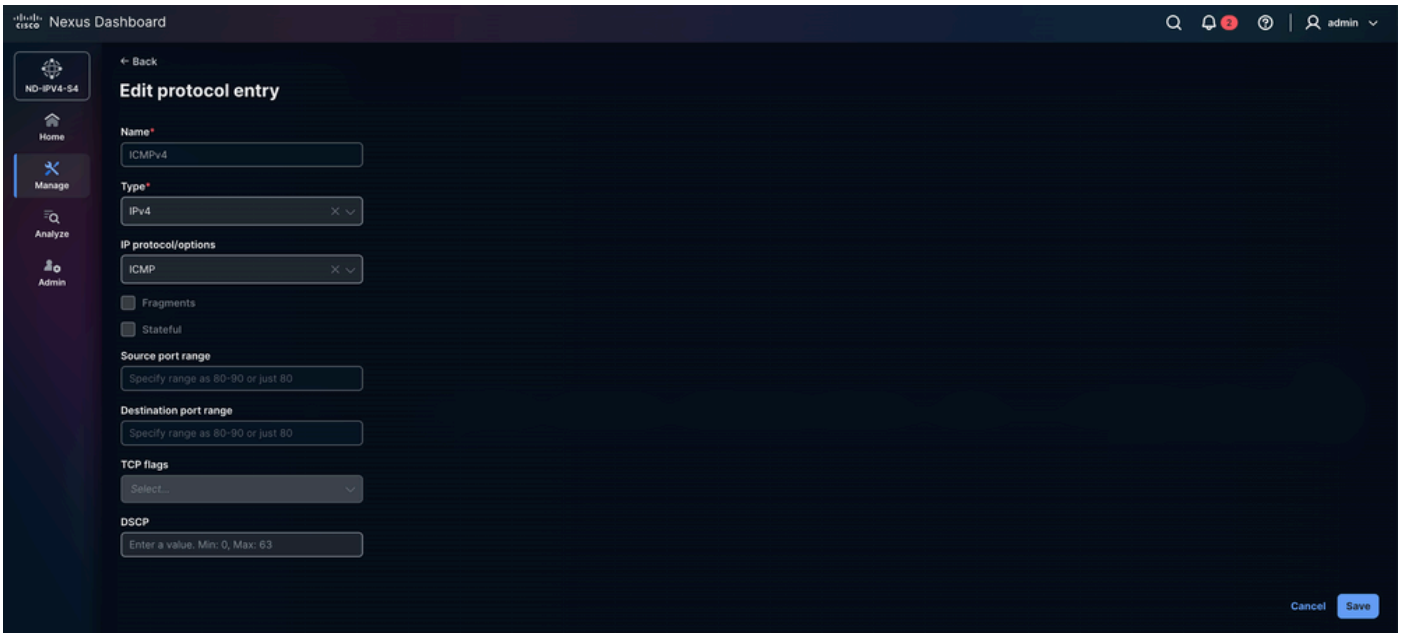
- Com estado: Um processo com informações de estado significa que ele controla todas as alterações ou interações que ocorreram no passado, e um processo atual é executado com um contexto desses processos anteriores. Nesse caso, o TCP rastreia áreas como o número de pacotes a serem transferidos, a ordem dos pacotes e se o receptor recebeu ou não um pacote. Com a opção Stateful selecionada, essas informações são armazenadas como um estado no TCP.

- Intervalo de portas de origem: Essa opção estará disponível apenas se você tiver selecionado TCP ou UDP no campo Protocolo IP/Opções acima.
- Intervalo de portas de destino: essa opção estará disponível somente se você tiver selecionado TCP ou UDP no campo Protocolo IP/Opções.
- Sinalizadores TCP

    - Essa opção está disponível somente quando o TCP é selecionado no campo Protocolo IP/Opções.

- Permite definir os flags TCP usados pelo protocolo de segurança.
- As flags TCP são parte do cabeçalho TCP e são usadas para controlar o estabelecimento, a manutenção e o término de conexões.
- Opções disponíveis:
    - ACK (Confirmação): Indica confirmação de dados recebidos ou pacotes de sincronização.
    - EST (Estabelecido): Refere-se a conexões TCP já estabelecidas. Quando esta opção está habilitada, nenhuma outra flag TCP pode ser selecionada.
    - FIN (Concluir): Usado para fechar uma conexão TCP normalmente.
    - RST (Redefinir): Encerra imediatamente a conexão e descarta todos os dados ainda em trânsito.
    - SYN (sincronização): Usado durante o início e o estabelecimento de uma conexão TCP.





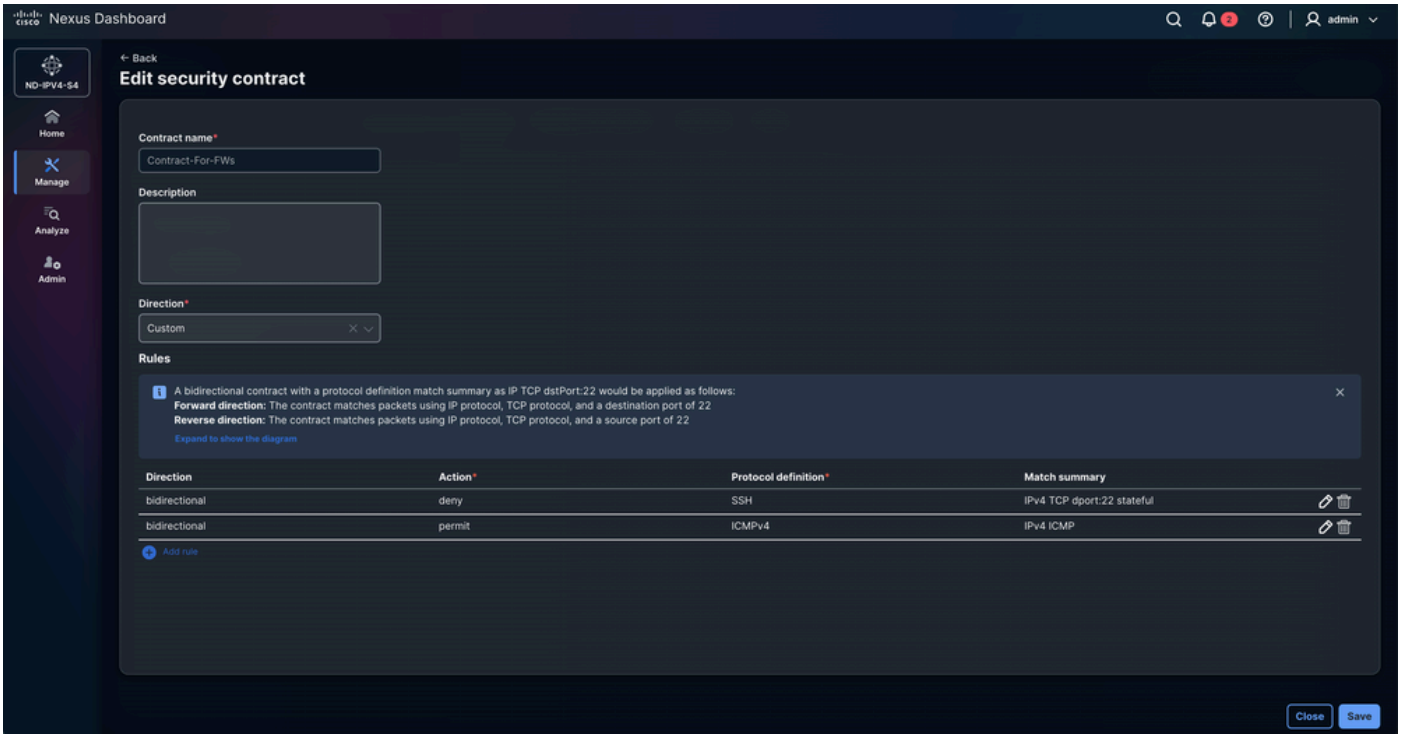
Etapa 5. Configurar Contratos de Segurança

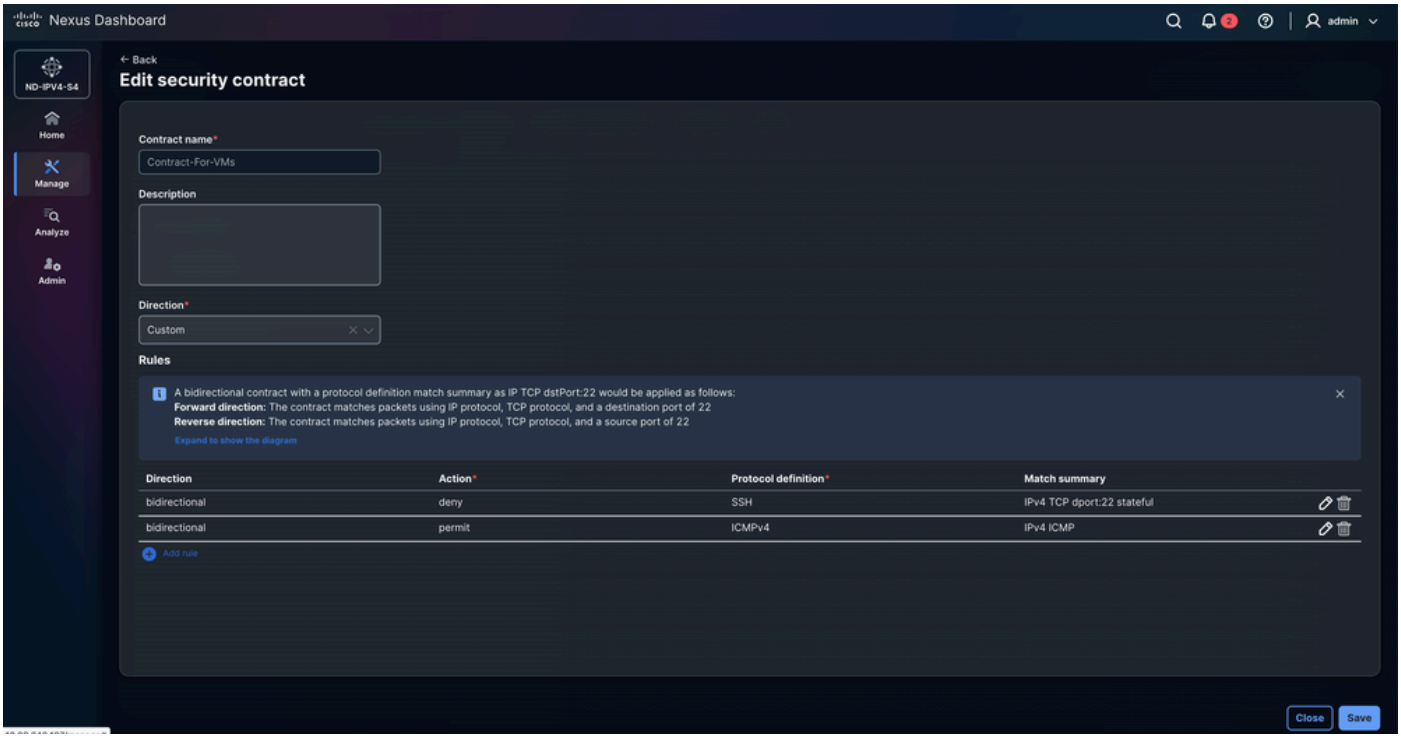
O Contrato define as regras de comunicação entre grupos de endpoint especificando qual tráfego é permitido ou negado com base nas definições de política associadas. Ele atua como o mecanismo de aplicação que aplica as regras, os filtros e as ações do protocolo configurado, garantindo que o tráfego entre os grupos de origem e destino esteja em conformidade com as políticas de segurança e segmentação desejadas.

Navegue para Gerenciar > Estruturas > Grupos de estrutura > DAVIDM3 > Segmentação e segurança > Contratos de segurança > Ações > Criar contrato de segurança.

- Selecione Add rule e configure Direction, Action e Protocol definition.
    - Bidirecional:
        - O contrato bidirecional se aplica da seguinte maneira com um resumo de correspondência de definição de protocolo como IP TCP Port 22.
            - Direção de encaminhamento: O contrato combina pacotes usando protocolo IP, protocolo TCP e uma porta destino de 22
            - Direção inversa: O contrato combina pacotes usando o protocolo IP, o protocolo TCP e uma porta origem de 22.
            - Isso se aplica independentemente da origem ou do destino.
    - Unidirecional:
        - Unidirecional em um Contrato de segurança de GPO significa que a política é

aplicada em apenas uma direção do fluxo de tráfego, permitindo ou negando a comunicação do Grupo de segurança de origem para o Grupo de segurança de destino sem aplicar automaticamente a mesma regra na direção inversa.

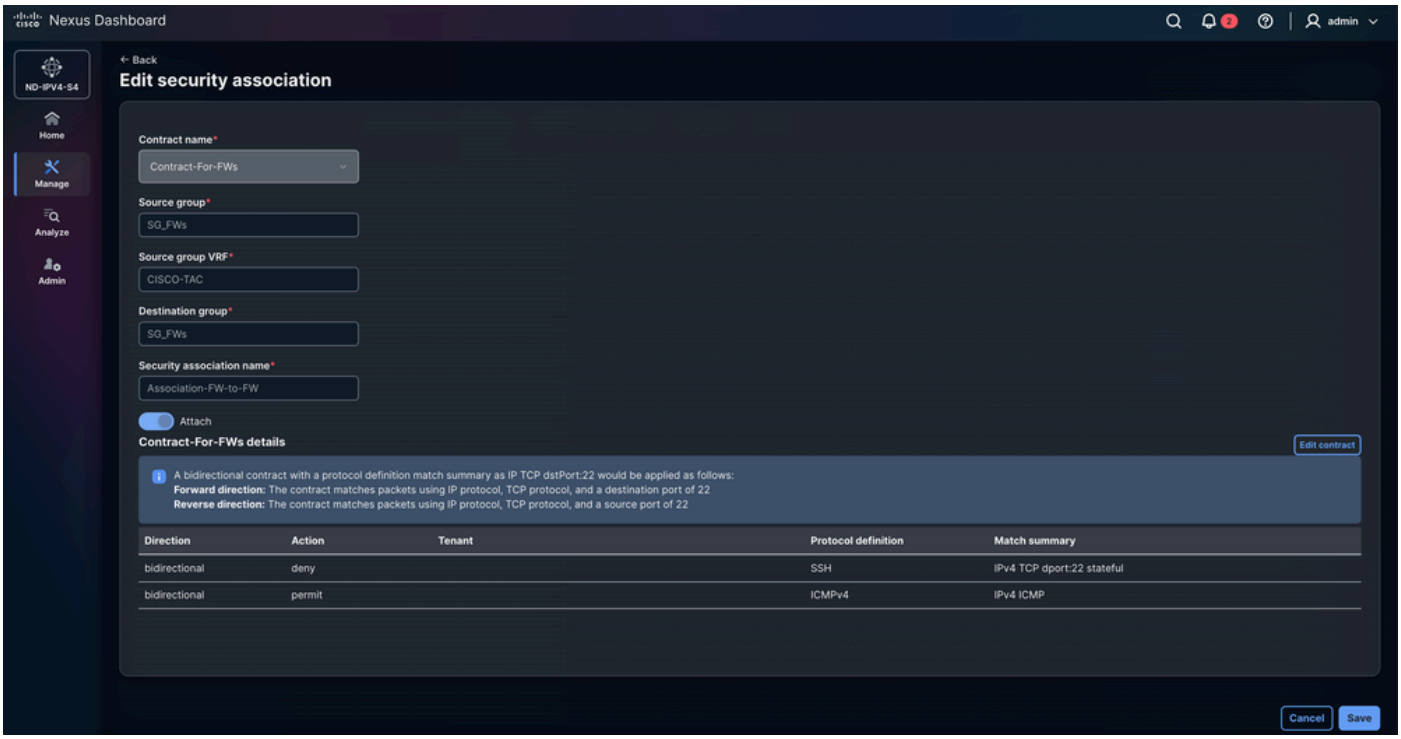


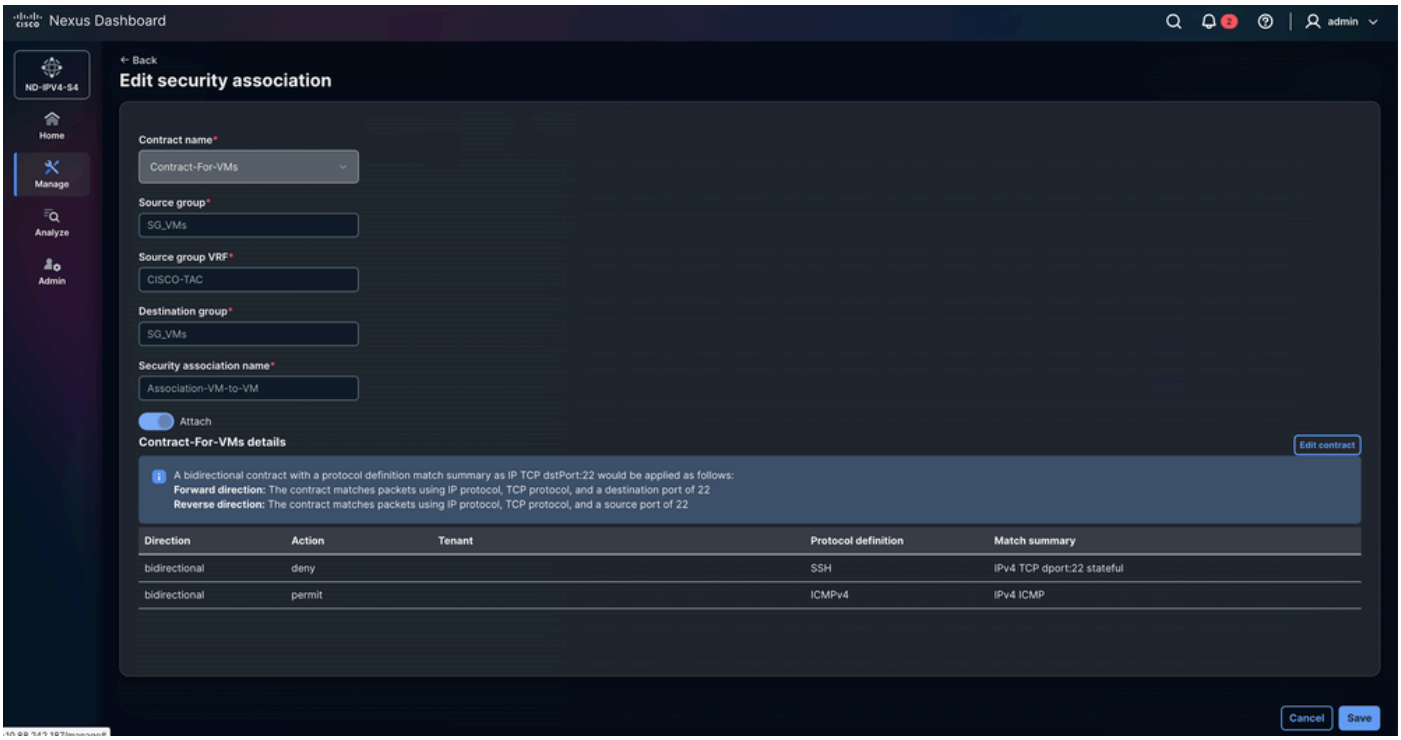


Etapa 6. Configurar Associações de Segurança

Navegue para Gerenciar > Estruturas > Grupos de estrutura > DAVIDM3 > Segmentação e segurança > Associações de segurança > Ações > Criar associação de segurança.

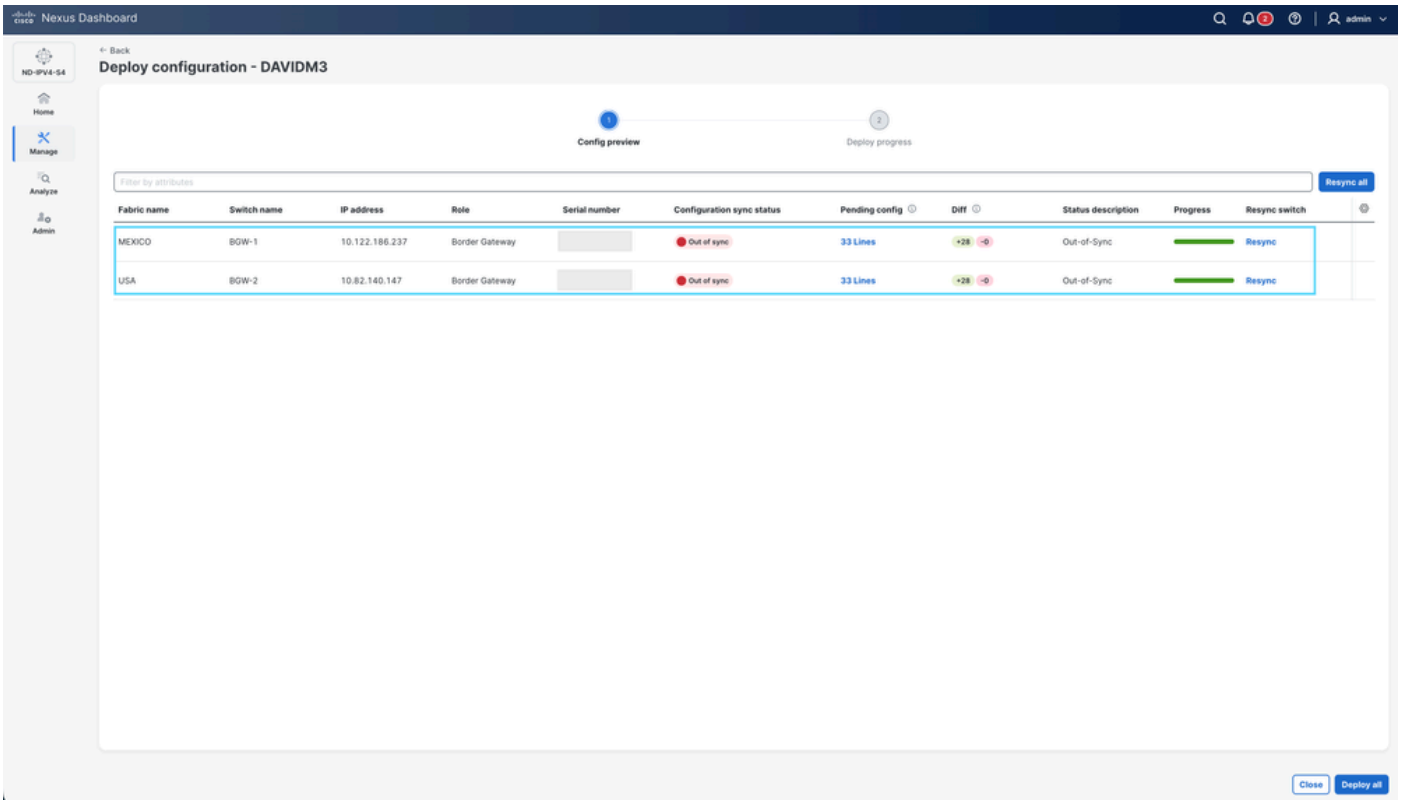
Em Configurar Associações de Segurança, o modelo de política é definido vinculando Grupos de Segurança, Definições de Protocolo e Contratos de Segurança. Os grupos de segurança classificam pontos finais, as definições de protocolo especificam os tipos de tráfego (como protocolos ou portas) e os contratos de segurança definem a política aplicada entre os grupos de segurança de origem e destino usando essas regras de protocolo. As associações de segurança representam a relação que une esses elementos para que a malha possa aplicar as políticas de segurança definidas.

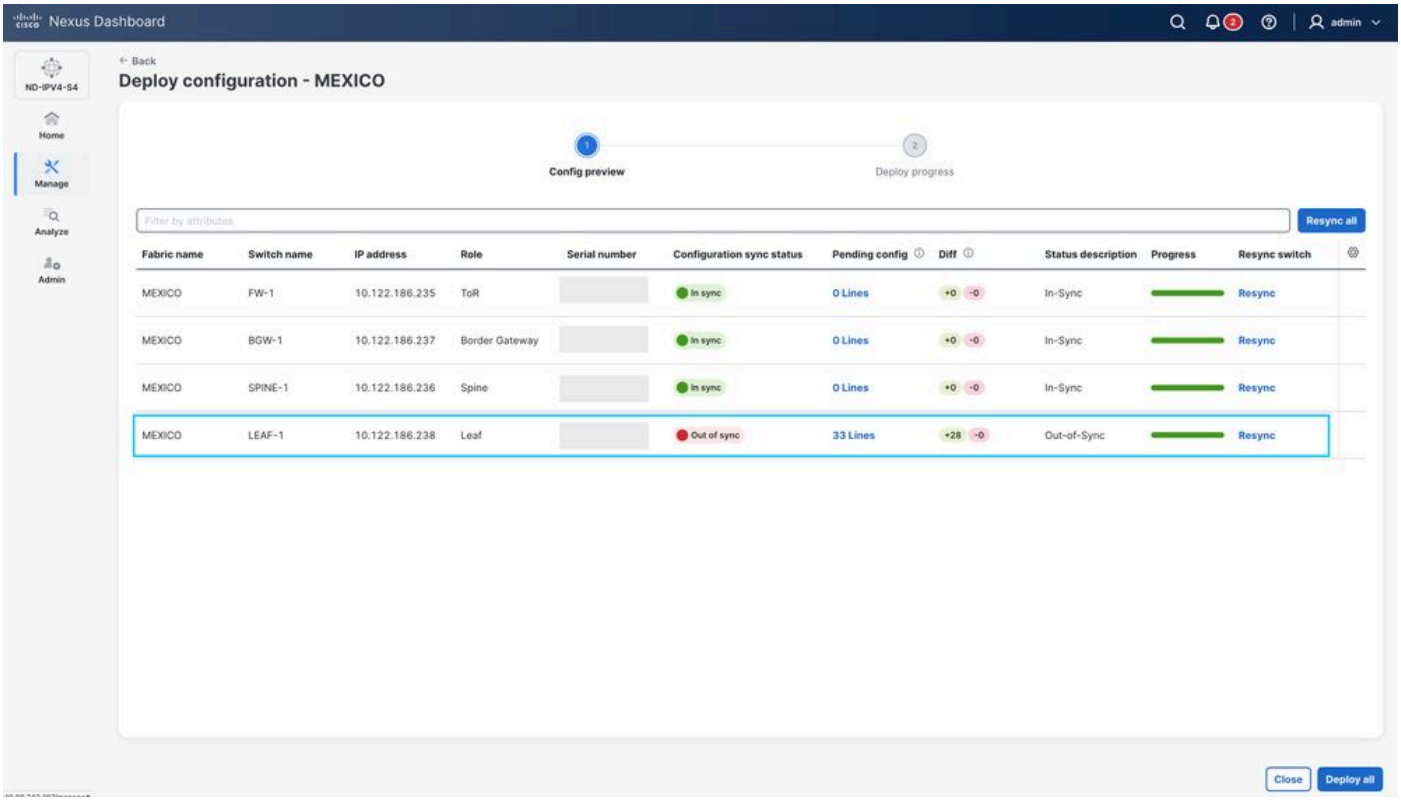


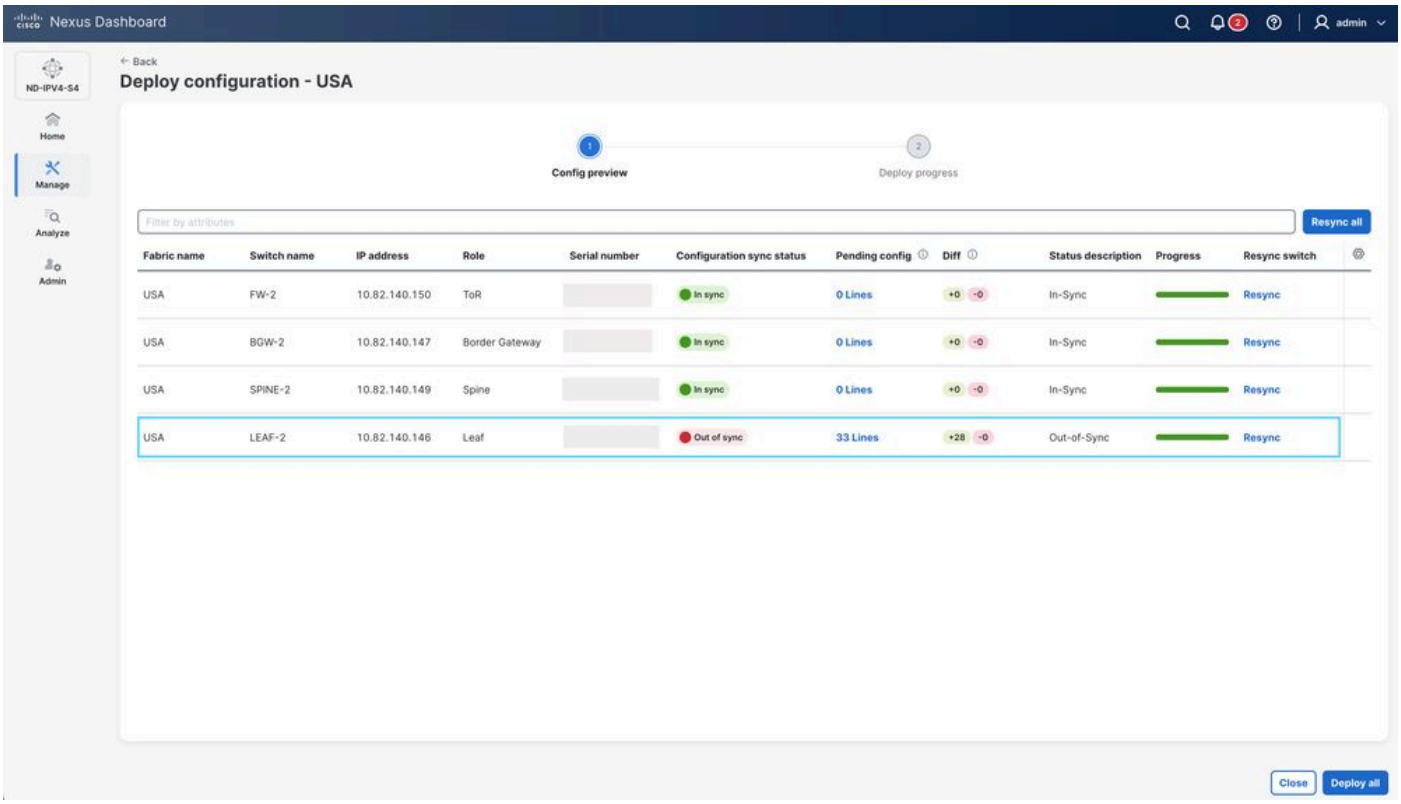


Etapa 7. Validar a configuração do GPO

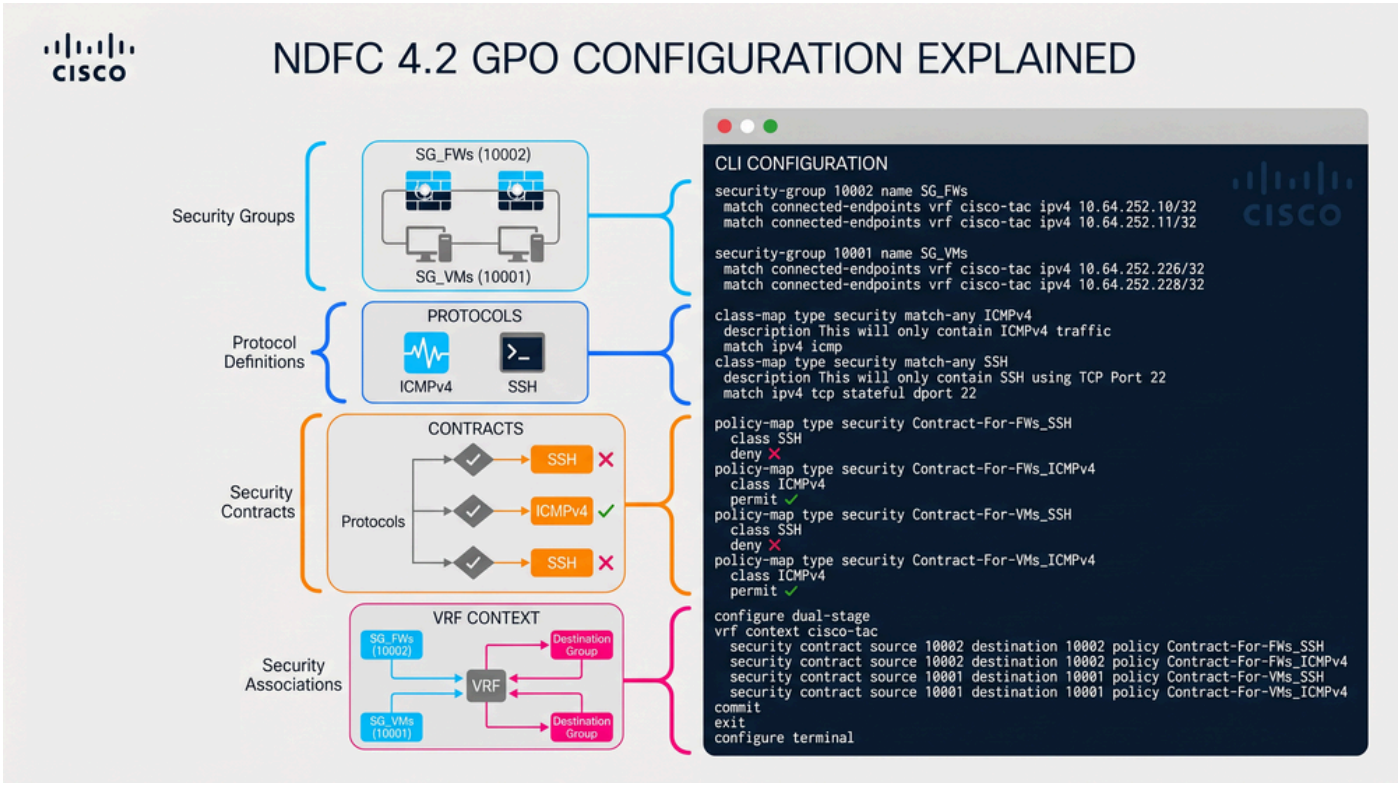
- Navegue até Manage > Fabrics > Fabric groups > DAVIDM3 > Actions > Recalculate and deploy.
  - A configuração do GPO é enviada para os Border Gateways a partir do switch de malha pai. Clique no número de linhas de configuração pendentes para revisar e validar a configuração que pode ser implantada nos dispositivos. Esse processo deve ser repetido para cada malha filho.
  - Navegue para Gerenciar > Estruturas > Grupos de estrutura > DAVIDM3 > Inventário > Estruturas membro > MÉXICO > Ações > Recalcular e implantar.
  - Navegue para Gerenciar > Estruturas > Grupos de estrutura > DAVIDM3 > Inventário > Estruturas membro > EUA > Ações > Recalcular e implantar.


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



- A imagem mostra a configuração de GPO para BGW-1, BGW-2, LEAF-1 e LEAF-2. A configuração é idêntica em todos os switches. O NDFC 4.2 não aplica a configuração na ordem exata mostrada. Esta seção ilustra a sequência lógica dos comandos CLI.



Troubleshooting de Operabilidade de GPO de VXLAN

Etapa 1. Verificar o estado do recurso do grupo de segurança

Valide se o recurso de grupo de segurança está habilitado no switch. O GPO da VXLAN depende desse recurso porque ativa a infraestrutura da Security Group Tag (SGT) necessária para classificação de endpoint, execução de contrato e programação de hardware da SGACL.

<#root>

```
BGW-1#

show feature | i i security-group


security-group 1 enabled
```

Etapa 2. Verificar o modo de roteamento do sistema

Valide o modo de roteamento do sistema operacional configurado no switch. O GPO de VXLAN requer o modo de roteamento de suporte a grupos de segurança porque a aplicação de SGACL consome recursos dedicados de encaminhamento de hardware dentro do pipeline de ASIC.

<#root>

```
BGW-1#

show system routing mode


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

Etapa 3. Verificar o estabelecimento de pares VXLAN NVE e a capacidade do GPO

- Valide o estabelecimento de pares VXLAN NVE entre dispositivos de estrutura local e pares remotos de vários locais. As informações de GPO de VXLAN se propagam através do plano de controle de EVPN de VXLAN, portanto, são necessárias adjacências NVE estáveis para o aprendizado de Security Group Tag (SGT) e sincronização de contrato através da malha.
- O campo Capacidade da política de grupo é um dos indicadores mais importantes neste

comando porque confirma se o VTEP remoto suporta extensões da política de grupo de VXLAN necessárias para propagação de SGT e execução de contrato de SGACL através do domínio de vários sites de VXLAN EVPN.

<#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

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

Etapa 4. Verificar o aprendizado do grupo de segurança e a classificação do endpoint

Valide se os pontos de extremidade estão corretamente classificados em Grupos de Segurança (SGTs). A aplicação de GPO de VXLAN depende de mapeamentos precisos de endpoint para SGT.

<#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
```

Etapa 5. Verificar os contratos de segurança e a aplicação de políticas

Valide se os contratos de GPO de VXLAN estão corretamente instalados e operacionais. Os contratos definem as regras de comunicação impostas entre os grupos de segurança e representam o mecanismo de política central usado pelo VXLAN GPO para microssegmentação.

<#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
```

Etapa 6. Verificar o estado de aplicação da segurança do VRF

Valide o estado de aplicação do GPO de VXLAN para todos os VRFs configurados no switch. Esse comando confirma se as políticas de SGACL e os contratos do Grupo de segurança são aplicados ativamente no VRF do locatário.

A saída confirma que o VRF do cisco-tac está participando ativamente da aplicação do GPO de VXLAN com o modo definido como aplicado. A tag de aplicação 13648 identifica o contexto de política SGACL interno programado no hardware para esse VRF. O registro de negação de ação padrão indica que qualquer tráfego não permitido explicitamente por meio de um contrato do Grupo de segurança é negado e registrado, implementando uma política de microssegmentação de negação padrão. Por outro lado, os VRFs padrão, de gerenciamento de resolução de balanceamento de carga de saída e de gerenciamento operam no modo não imposto, o que significa que as políticas de GPO de VXLAN não são aplicadas dentro desses VRFs e o tráfego é permitido por padrão.

O campo Stats rastreia o tráfego correspondente à política de segurança do VRF. O valor 0 no VRF do cisco-tac indica que nenhum tráfego sem correspondência acionou o comportamento de negação padrão no momento em que o comando foi executado, enquanto o valor do contador 4364 no VRF padrão indica atividade de tráfego em um VRF operando sem aplicação de GPO de VXLAN.

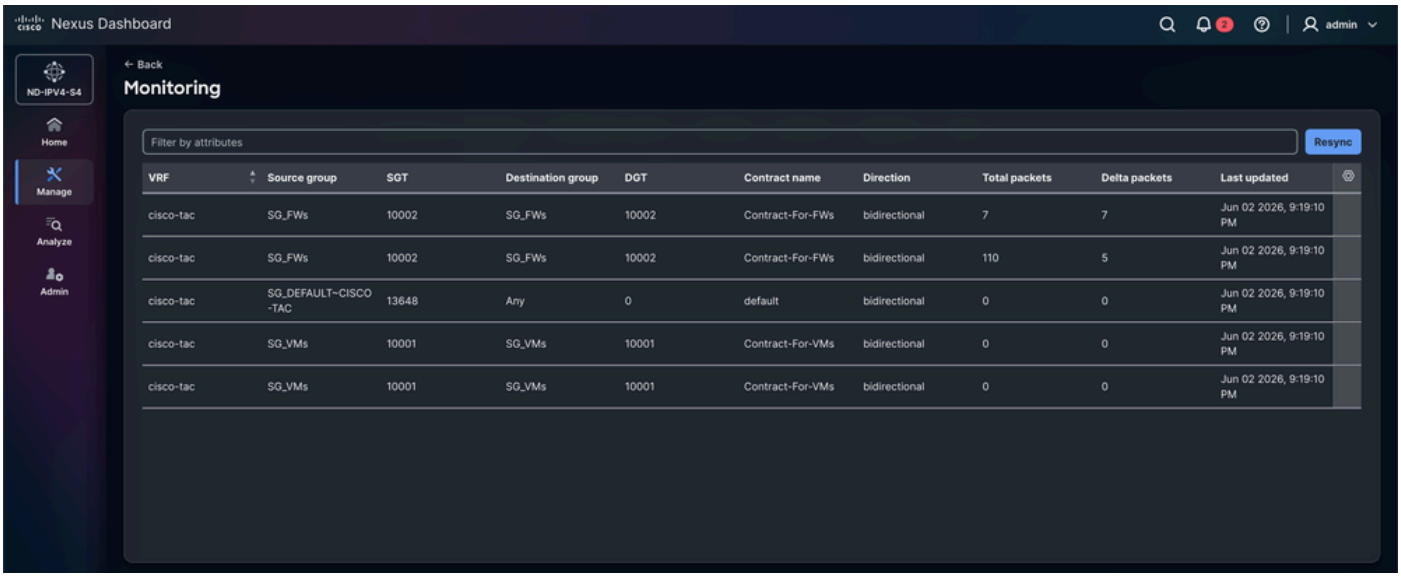
```
<#root>

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
```

Etapa 7. Verificar o estado de aplicação da segurança do VRF

- Valide as estatísticas de correspondência de tráfego para contratos de GPO de VXLAN da GUI da NDFC. Essa verificação confirma se o tráfego está correspondendo ativamente aos contratos configurados do Grupo de Segurança e se a aplicação de SGACL está operacional através da estrutura de vários locais EVPN VXLAN.
- Na GUI da NDFC, navegue para Manage > Fabrics > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoring.
    - Esta seção fornece visibilidade dos fluxos de comunicação do Grupo de segurança, estatísticas de acerto de contrato, ações de permissão e negação e atividade de contrato operacional entre grupos de endpoint.
    - As estatísticas de monitoramento são exibidas individualmente dentro de cada uma delas.
    - O monitoramento de estatísticas do NDFC fornece uma camada de validação operacional que complementa a solução de problemas com base em CLI, confirmando a aplicação de políticas em tempo real e o comportamento de correspondência de tráfego na malha.

Note: Na primeira tentativa de analisar estatísticas de tráfego na NDFC 4.2, a seção de monitoramento pode parecer inicialmente vazia. Nessa situação, pressione o botão Resync para acionar a sincronização das estatísticas do contrato da estrutura VXLAN. Enquanto o processo de sincronização é executado, a GUI exibe a mensagem Resync status: Em andamento. Após a conclusão da sincronização, pressione o botão Ok para atualizar a exibição de monitoramento. Após o término da ressincronização, as estatísticas de tráfego associadas a cada contrato do Grupo de Segurança tornam-se visíveis na seção de monitoramento. Para validar o comportamento de correspondência de tráfego ao vivo, gere tráfego entre os endpoints e pressione o botão Resync novamente para atualizar as estatísticas do contrato exibidas no NDFC.



- A partir do cenário anterior, o tráfego ICMPv4 é permitido com êxito entre os endpoints. No entanto, se uma sessão SSH for estabelecida, a conexão expira porque o contrato de GPO da VXLAN nega explicitamente o tráfego TCP destinado à porta 22.

<#root>

```
FW-1#

ping 10.64.252.11


PING 10.64.252.11 (10.64.252.11): 56 data bytes
64 bytes from 10.64.252.11: icmp_seq=0 ttl=254 time=1.131 ms
64 bytes from 10.64.252.11: icmp_seq=1 ttl=254 time=0.694 ms
64 bytes from 10.64.252.11: icmp_seq=2 ttl=254 time=0.675 ms
64 bytes from 10.64.252.11: icmp_seq=3 ttl=254 time=0.657 ms
64 bytes from 10.64.252.11: icmp_seq=4 ttl=254 time=0.648 ms

--- 10.64.252.11 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.648/0.761/1.131 ms
FW-1#

ssh admin@10.64.252.11


ssh: connect to host 10.64.252.11 port 22: Connection timed out
```

Informações Relacionadas

[Guia de configuração do Cisco Nexus 9000 Series NX-OS VXLAN, versão 10.6(x)]

Proteção de data centers com microssegmentação usando VXLAN GPO

Implantação de microssegmentação em estruturas Cisco NX-OS VXLAN EVPN com VXLAN Group Policy Option (GPO)

Automatização da microssegmentação e implantação de serviços das camadas 4 a 7 em estruturas EVPN VXLAN usando Group Policy Option (GPO) e Nexus Dashboard

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.