Configuración de GPO en fabric multisitio Nexus con NDFC 4.2

Contenido

Introducción

Este documento describe la configuración y validación de GPO en fabrics multisitio VXLAN en

switches Nexus Cloud Scale que ejecutan NX-OS y NDFC 4.2.

Prerequisites

Requirements

Cisco recomienda que conozca estas áreas:

- Tecnologías de red de área local extensible virtual (VXLAN), red privada virtual Ethernet (EVPN) y fabric multisitio
- Funcionamiento de los switches Cisco Nexus Cloud Scale y del sistema operativo Nexus (NX-OS)
- Flujos de trabajo de gestión e implementación del controlador de red Nexus Fabric (NDFC) 4.2
- Segmentación de la red y conceptos de políticas de seguridad

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Comprensión de la funcionalidad GPO en estructuras VXLAN EVPN

La opción de directiva de grupo (GPO) es un mecanismo de segmentación basado en directivas diseñado para controlar la comunicación entre los extremos basándose en la identidad lógica en lugar de depender únicamente de direcciones IP, VLAN o subredes. El objetivo principal del GPO es simplificar la aplicación de políticas de seguridad y proporcionar microsegmentación escalable entre aplicaciones, servidores o cargas de trabajo.

Una simple analogía es pensar en un hotel donde cada huésped pertenece a una categoría o nivel de acceso específico, ciertas áreas son accesibles solo para huéspedes específicos, y los permisos de acceso dependen de la función del huésped en lugar del número de habitación. GPO funciona de una manera muy similar. En lugar de tratar los extremos exclusivamente como direcciones IP, el GPO los clasifica en grupos de seguridad (SG). A continuación, se aplican políticas entre estos grupos para determinar qué comunicaciones se permiten o deniegan.

Por ejemplo:

- Los servidores web pueden pertenecer a un grupo de seguridad.
- Los servidores de aplicaciones pueden pertenecer a otro grupo de seguridad.
- Los servidores de base de datos pueden pertenecer a un grupo de seguridad restringido.

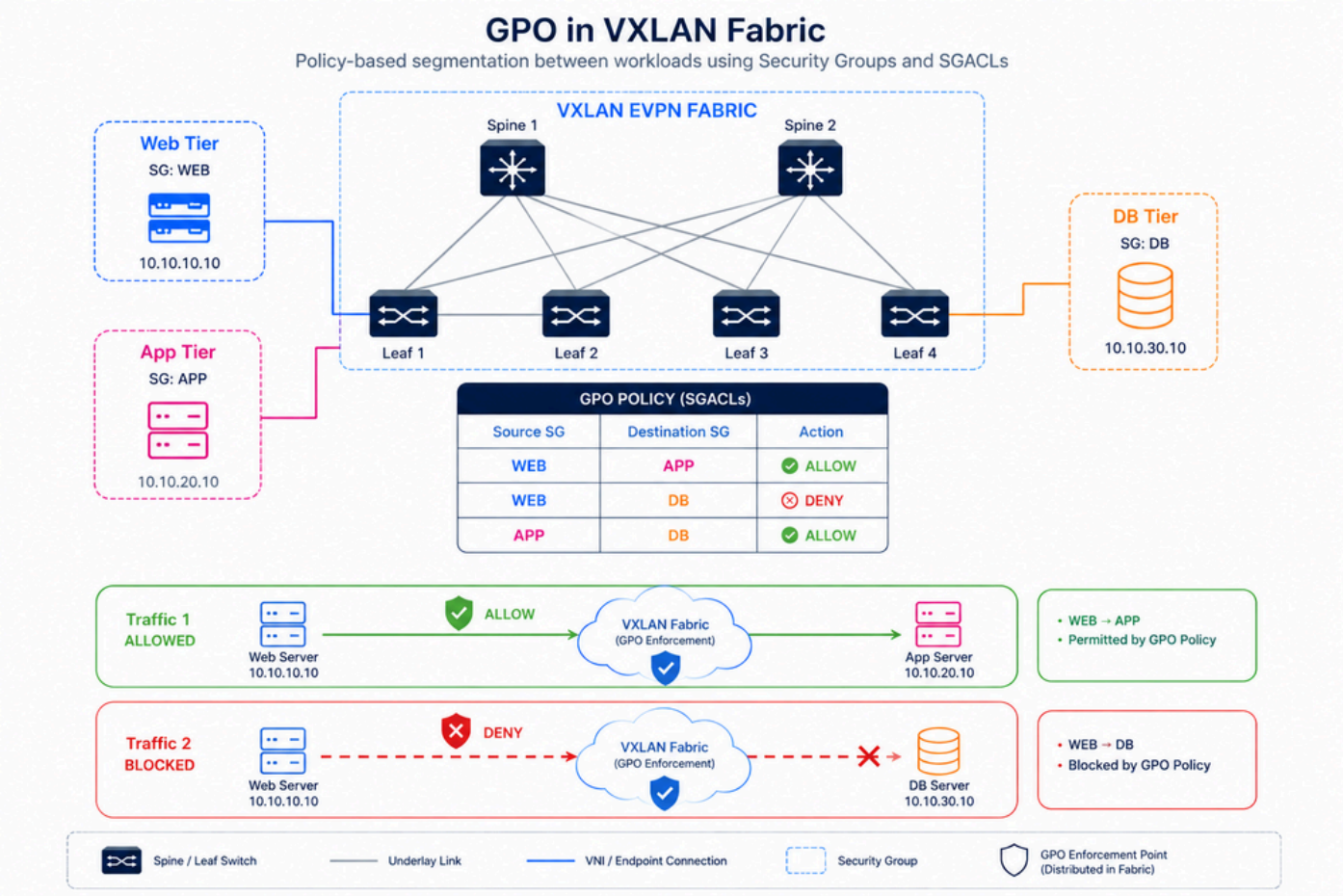
A continuación, las políticas pueden definir:

- Los servidores Web pueden comunicarse con los servidores de aplicaciones.
- Los servidores de aplicaciones pueden comunicarse con los servidores de bases de datos.
- Los servidores Web no pueden comunicarse directamente con los servidores de bases de datos.

Este enfoque simplifica las operaciones porque los administradores ya no necesitan mantener un gran número de ACL en varios dispositivos y VLAN.

Otra ventaja importante es la escalabilidad. En entornos de gran tamaño, las cargas de trabajo se mueven con frecuencia, se amplían dinámicamente o cambian las direcciones IP. El GPO permite que las políticas de seguridad sean coherentes incluso cuando cambia la ubicación del terminal. Dentro de los fabrics VXLAN EVPN, el GPO amplía este concepto distribuyendo la información del grupo de seguridad por el fabric y aplicando las ACL del grupo de seguridad (SGACL) entre los terminales. Esto es especialmente importante en los Data Centers modernos, ya que el tráfico horizontal entre cargas de trabajo suele representar la mayor superficie de ataque. El GPO mejora el estado de la seguridad al limitar las rutas de comunicación innecesarias dentro del fabric del Data Center.

Para obtener una comprensión técnica más profunda de la arquitectura de GPO, los conceptos de microsegmentación y la aplicación de políticas de VXLAN, consulte el informe técnico de Cisco disponible en: Protección de Data Centers con microsegmentación mediante GPO de VXLAN



GPO en fabric VxLAN

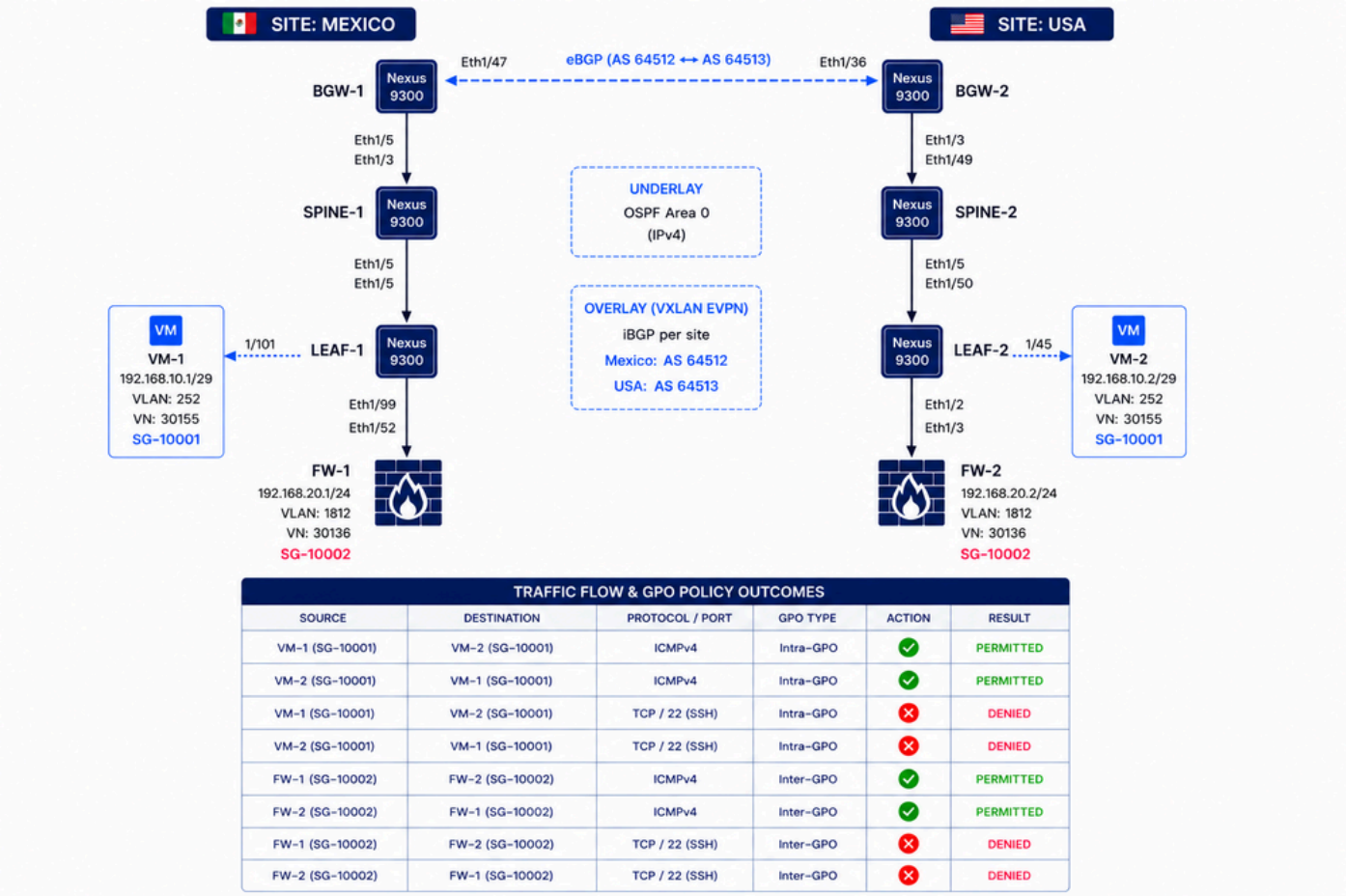
Escenario de implementación de GPO multisitio de VXLAN con NDFC 4.2 y NX-OS 10.6(3)F

Esta topología representa un fabric de varios sitios VXLAN implementado en dos sitios distribuidos geográficamente: México y Estados Unidos. Cada sitio contiene BGW dedicados, switches de columna, switches de hoja, máquinas virtuales y segmentos de firewall que se ejecutan en switches Cisco Nexus 9300 con NX-OS 10.6(3)F. La red subyacente utiliza Open Shortest Path First (OSPF), mientras que el plano de control de superposición utiliza iBGP dentro de cada sitio y eBGP entre BGW-1 y BGW-2 para la comunicación EVPN entre sitios VXLAN. Dado que este entorno es una implementación de laboratorio, las instalaciones de México y EE. UU. están interconectadas a través de un enlace conectado directamente entre ambos BGW para simplificar el modelo de conectividad multisitio.

El GPO se utiliza para aplicar una microsegmentación basada en políticas entre grupos de seguridad (SG) independientemente del direccionamiento IP o los límites de VLAN. Según la tabla

de políticas de conectividad, se permite el tráfico ICMP de VM-1 a VM-2, FW-1 y FW-2, mientras que se deniega el tráfico del puerto TCP 22 (SSH) de VM-1 a FW-1 y FW-2. La comunicación del puerto TCP 22 entre VM-1 y VM-2 sigue estando permitida porque ambos terminales pertenecen al mismo grupo de seguridad (SG-10001). Este comportamiento demuestra cómo el GPO aplica dinámicamente diferentes políticas de tráfico entre las comunicaciones entre GPO y entre GPO a través del entramado de varios sitios de VXLAN.

Nota: Cisco NX-OS Release 10.6(3)F introduce que puede restringir la comunicación entre los terminales dentro del mismo ESG (también conocido como SG) mediante la función de aislamiento intra-ESG. Esta función minimiza el riesgo de acceso no autorizado dentro de ESG y mejora el estado de la seguridad.



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

Configuración paso a paso de GPO con NDFC 4.2 en estructuras VPN VXLAN

Estos pasos se aplican cuando el entramado multisitio VXLAN ya está operativo y configurado con NDFC 4.2, y el GPO debe implementarse posteriormente. La sección Automatización con el

panel de Nexus en Protección de Data Centers con microsegmentación mediante GPO VXLAN muestra la configuración a partir de la creación de un fabric de sitio único VXLAN.

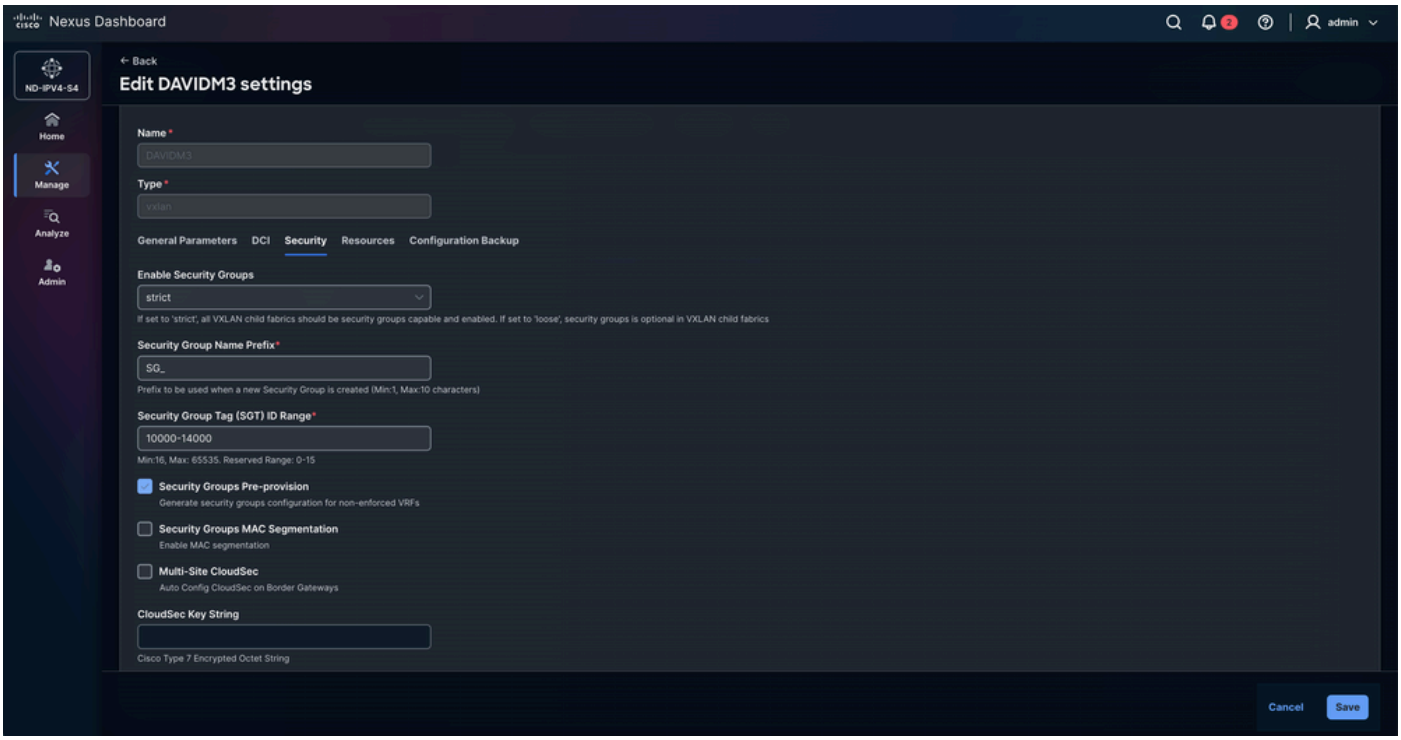
Precaución: Cuando el GPO funciona en un fabric VXLAN EVPN, la comunicación se produce sólo si existe disponibilidad de destino y la política de seguridad permite el tráfico. La aplicación de políticas se basa en la información de IP, que requiere entradas ARP y SVI para las redes internas. Esto significa que la VLAN que pertenece al VRF de arrendatario debe tener una SVI configurada. En consecuencia, la aplicación no se aplica al tráfico que contiene solo encabezados de capa 2 y, por lo tanto, no se puede utilizar con la extensión de capa 2 de VXLAN. NX-OS Release 10.6(2)F introduce la compatibilidad con microsegmentación basada en MAC.

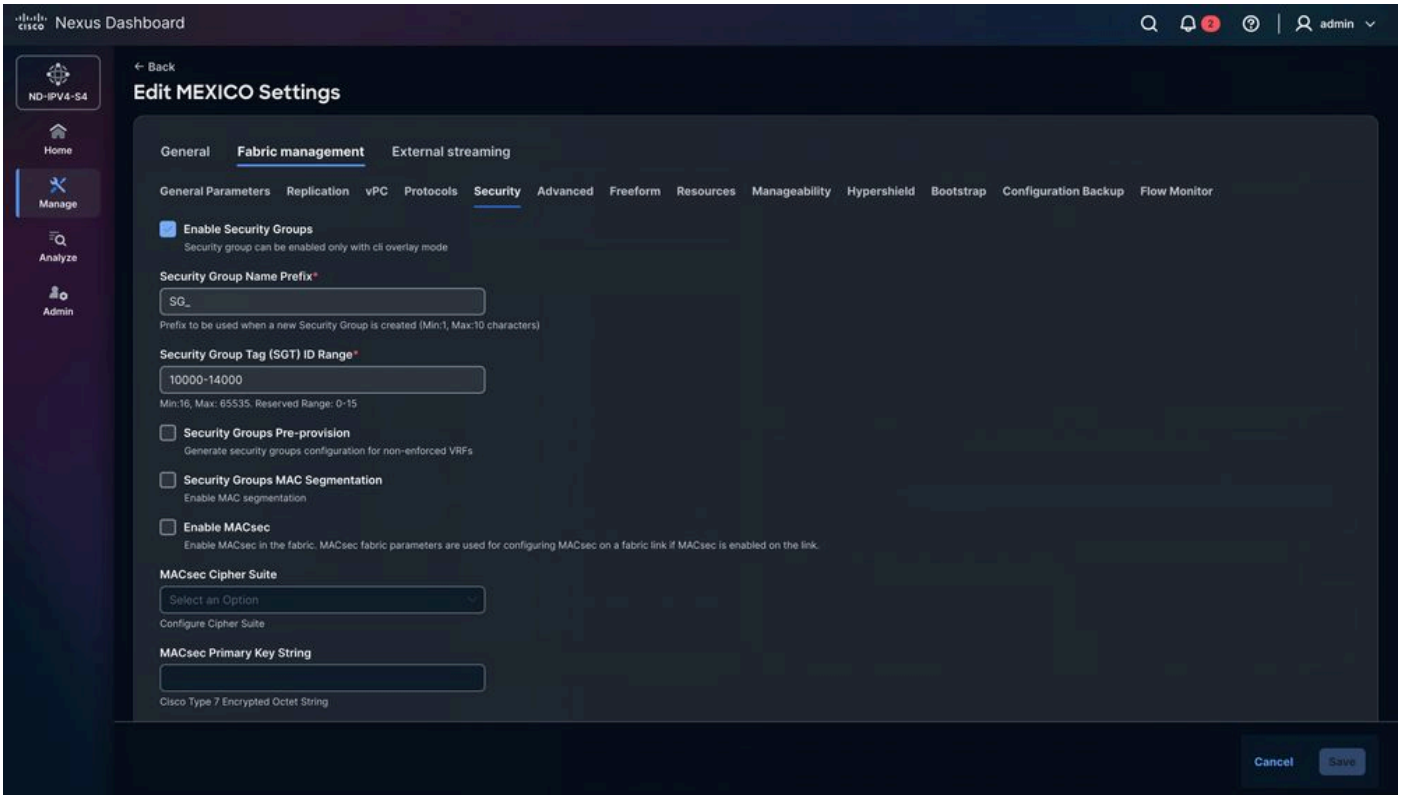
Paso 1. Habilitación de grupos de seguridad en el fabric principal

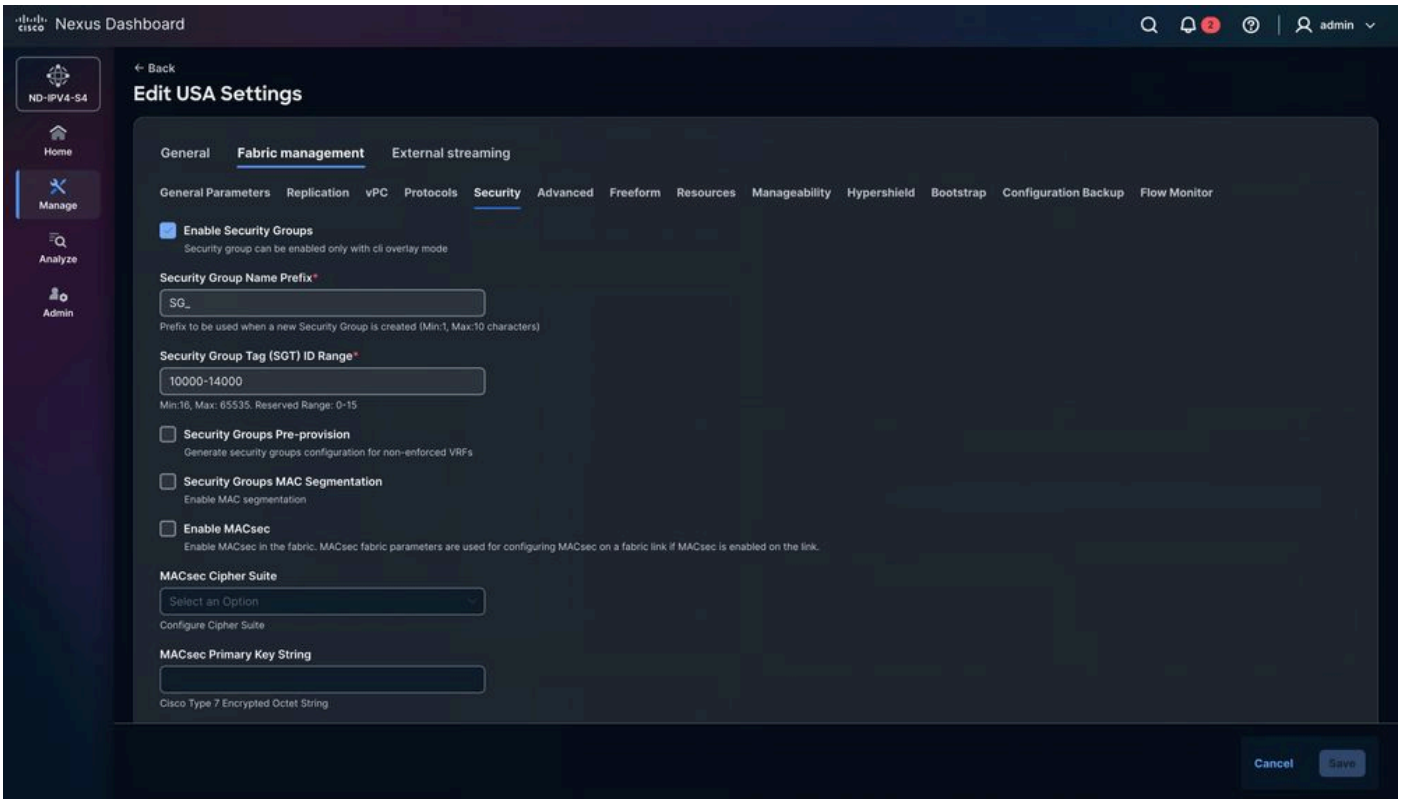
- Navegue hasta Administrar > Grupos de entramado, seleccione el grupo de entramado DAVIDM3, luego elija Acciones > Editar configuración de grupo de entramado. En la sección Seguridad, habilite Security Groups, establezca el modo en Estricto y establezca Security Groups Pre-provision.
  - Seleccione el grupo de interés del fabric. En este ejemplo, el grupo de fabric seleccionado se denomina DAVIDM3, que también es el nombre del fabric multisitio.
- Repita estos pasos para cada tejido secundario.
  - Vaya a Manage > Fabric, seleccione USA, luego vaya a Actions > Edit Fabric Group Settings. En la sección Seguridad, habilite Grupos de Seguridad y establezca el modo en Estricto.
  - Navegue hasta Administrar > Fabric, seleccione MÉXICO, luego navegue hasta Acciones > Editar configuración de grupo de fabric. En la sección Seguridad, habilite Grupos de Seguridad y establezca el modo en Estricto.

Nota: Si se establece en strict, todos los fabrics secundarios VXLAN deben ser capaces y habilitados para grupos de seguridad. Si se establece en flexible, los grupos de seguridad son opcionales en los fabrics secundarios VXLAN.

Consejo: Para mantener una visibilidad clara, utilice los mismos intervalos de ID de etiquetas de grupos de seguridad (SGT) en el fabric principal y en todos los fabric secundarios. La gama de tejidos principales debe cubrir las gamas utilizadas por todos los tejidos secundarios.


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



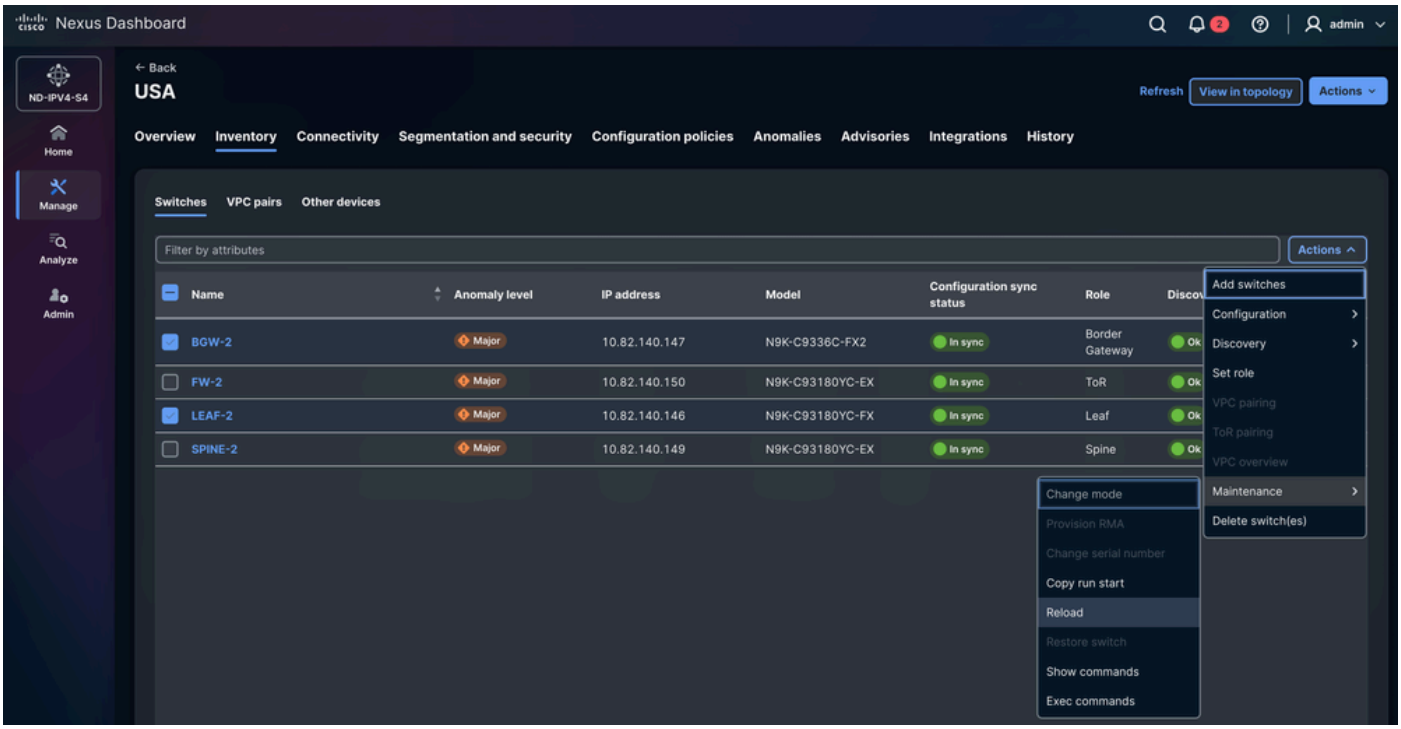
Paso 2. Recalcular la configuración del fabric y recargar switches para la implementación de GPO

NDFC solicita automáticamente que se vuelva a cargar un grupo específico de switches Nexus en función de su función. En este ejemplo, LEAF-1, LEAF-2, BGW-1 y BGW-2 deben volver a cargarse. El administrador de la red debe ejecutar esta acción manualmente. La recarga es necesaria y no se puede omitir porque el GPO requiere la división TCAM.

Nota: Si el dispositivo no se recarga, el cambio TCAM puede aparecer en la configuración en ejecución; sin embargo, dado que el switch no se ha reiniciado, la configuración no se aplica a la memoria de hardware. Como resultado, la función no puede funcionar como se esperaba.

Para volver a cargar los switches Nexus:

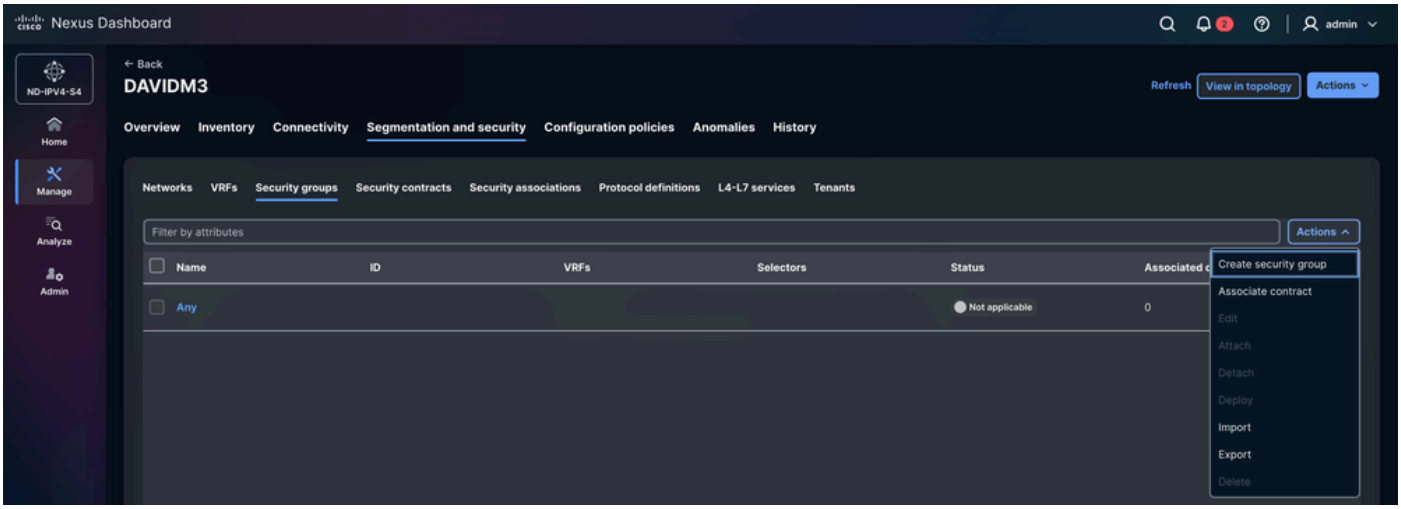
Vaya a Manage > Fabrics > MEXICO/USA > Inventory > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions > Maintenance > Reload.



Paso 3. Crear grupo de seguridad

Defina los grupos de seguridad para cada terminal. Cada terminal de los fabrics VXLAN puede tener un único grupo de seguridad. Este enfoque no es escalable de manera eficiente. Agrupe los terminales de forma global (máquinas virtuales, firewalls, optimizadores TCP, entre otros).

Vaya a Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security Groups > Actions > Create security group.



Paso 3.1 Configuración del nombre del grupo de seguridad

- NDFC asigna automáticamente un nombre aleatorio. El nombre se puede cambiar; se recomienda utilizar un nombre representativo que sea fácil de identificar para los terminales.
- En esta situación:
    - VM -> SG_VM
    - FW -> SG_FW

Paso 3.2 Configuración de VRF

- Seleccione el arrendatario (VRF) al que pertenecen los terminales.
- En esta situación: Las VM y los firewalls pertenecen al arrendatario de CISCO-TAC.

Opcional, Crear VRF.

De forma predeterminada, un VRF de arrendatario recién creado tiene el modo de aplicación de políticas establecido en Sin aplicar. En este estado, incluso si se configuran los criterios de clasificación y las SGACL entre los grupos de seguridad, no se aplica ninguna política. Para activar la aplicación de SGACL, el VRF se debe configurar explícitamente en el modo Enforced.

Cuando el VRF funciona en el modo Enforced, se define un comportamiento de la política por defecto:

- Denegar: Todo el tráfico de unidifusión se descarta a menos que lo permita explícitamente una regla de permiso.
- Permitir: Se permite todo el tráfico de unidifusión a menos que una regla de denegación lo bloquee explícitamente.

Los terminales que pertenecen al mismo grupo de seguridad pueden comunicarse entre sí sin necesidad de reglas SGACL. Las SGACL definen las políticas de seguridad solo entre grupos de seguridad diferentes.

Cisco NX-OS versión 10.6(3)F introduce la capacidad de restringir la comunicación entre terminales dentro del mismo GPO, también conocida como función de aislamiento dentro del GPO. Antes de esta versión, las reglas aplicadas a los terminales dentro del mismo grupo de seguridad se ignoran y el tráfico se permite de forma predeterminada.

Paso 3.3 Configuración de ID de etiqueta de grupo de seguridad

NDFC asigna automáticamente un ID de etiqueta aleatorio del intervalo predefinido en la configuración de fabric. Aunque se puede seleccionar manualmente un ID de etiqueta, debe estar comprendido en el intervalo definido para los tejidos principal y secundario.

En esta situación:

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

Paso 3.4 Adhesión

Si la opción Adjuntar no está habilitada, el grupo de seguridad no se aplica al arrendatario CISCO-TAC.

Paso 3.5 Configuración de selectores

- Los selectores determinan qué extremos y direcciones IP externas están asociados con un grupo de seguridad específico.

NDFC 4.2 admite de forma nativa tres tipos de selectores:

1) Selectores IP: los selectores IP asocian extremos o subredes IP a un grupo de seguridad en función de la información IP.

a. Terminal conectado: identifica los terminales conectados directamente al fabric, como máquinas virtuales, servidores o hosts físicos conectados a switches de hoja.
b. Subred externa: Asocia prefijos IP externos a un grupo de seguridad. Este tipo se utiliza para redes que existen fuera del fabric VXLAN, como Data Centers externos, segmentos WAN o redes con conexión a Internet. El tráfico originado o destinado a estos prefijos se clasifica con el grupo de seguridad configurado.

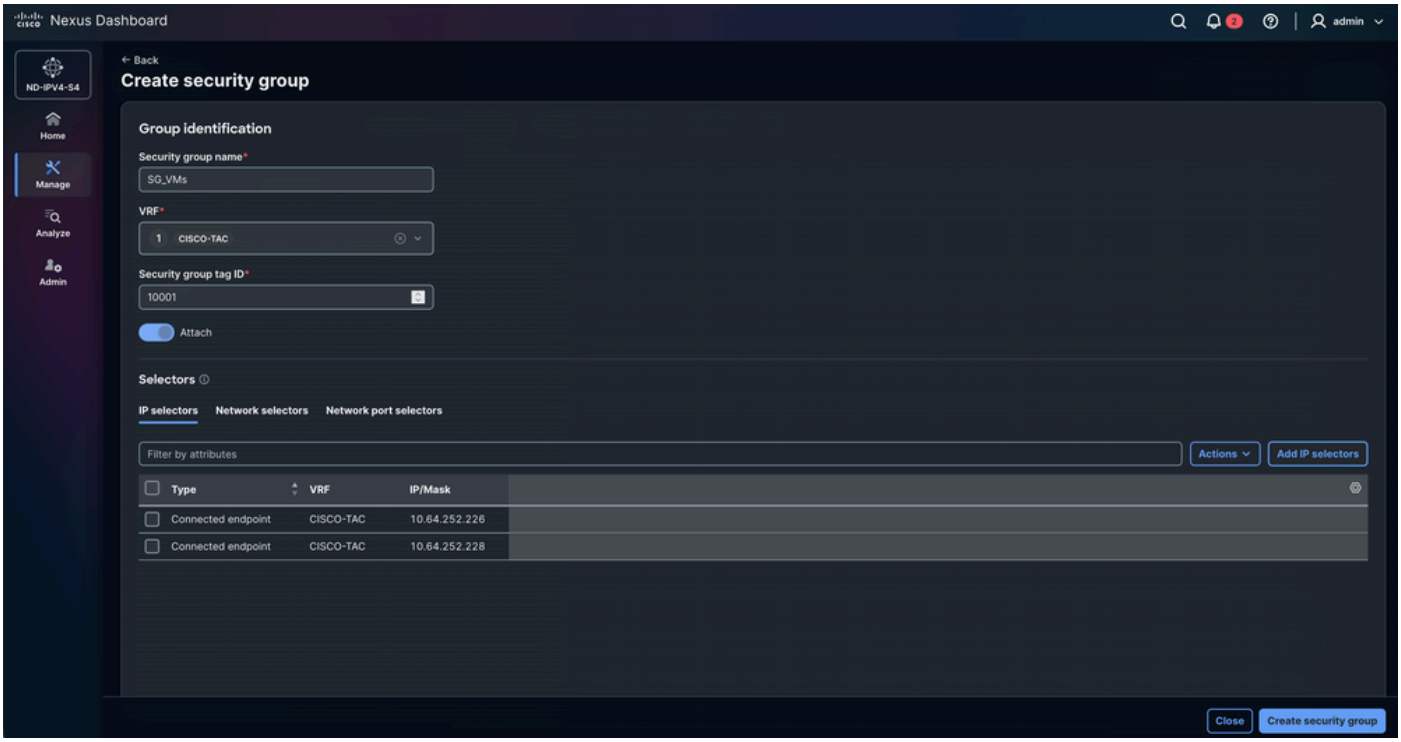
2) Selectores de red: los selectores de red asocian un grupo de seguridad a un segmento de red VXLAN específico. La clasificación se aplica en función del identificador de red (L2VNI). Todos los terminales que pertenecen a esa red heredan el grupo de seguridad asignado, lo que simplifica la implementación de políticas cuando varios terminales comparten el mismo segmento.

3) Selectores de puertos de red: los selectores de puertos de red clasifican el tráfico en función de la interfaz física del switch a través de la cual el tráfico entra en el fabric. Un grupo de seguridad se puede asignar al tráfico recibido en un puerto o interfaz específicos. Este enfoque se utiliza normalmente para dispositivos conectados a través de redes externas, dispositivos de servicio o enlaces de infraestructura en los que la clasificación IP de terminales no es viable.

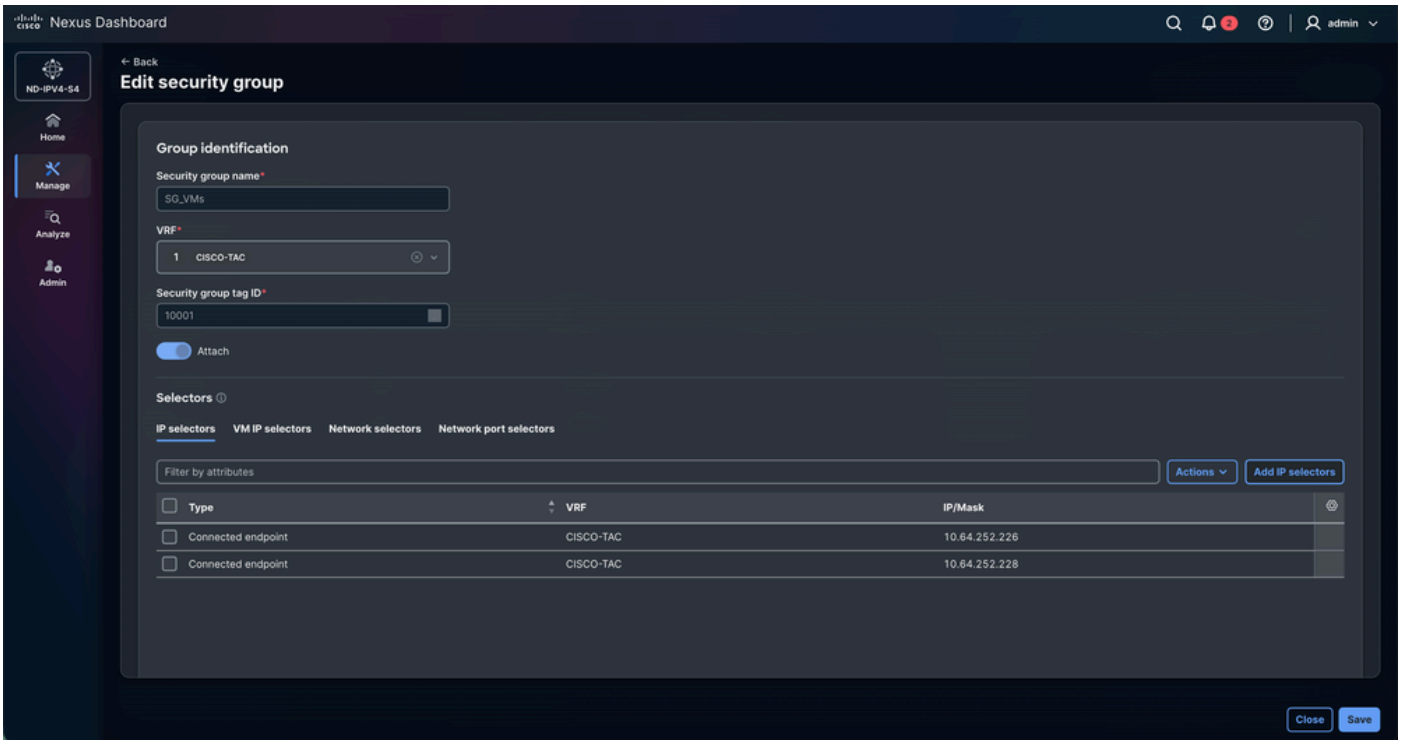
Resumen de configuración del grupo de seguridad

Dispositivo	Nombre del grupo de seguridad	VRF	ID de etiqueta de grupo de seguridad	Selectores
VM-1	SG_VM	CISCO-TAC	10001	Selectores IP
VM-2	SG_VM	CISCO-TAC	10001	Selectores IP
FW-1	SG_FW	CISCO-TAC	10002	Selectores IP
FW-2	SG_FW	CISCO-TAC	10002	Selectores IP

Configuración de grupos de seguridad para VM



Configuración del grupo de seguridad para FW



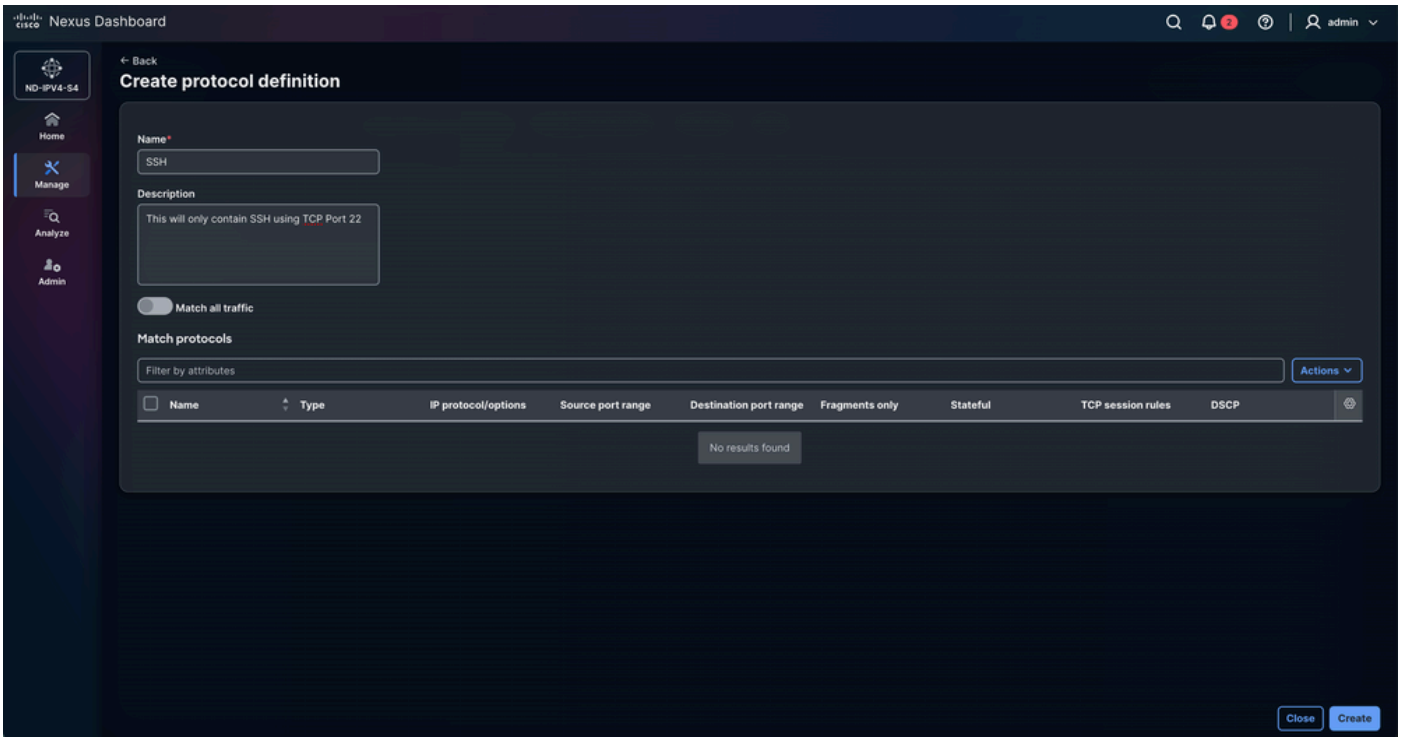
Paso 4. Configuración de definiciones de protocolo

La opción Crear definición de protocolo se utiliza para definir los parámetros del protocolo de red y las características de tráfico que coinciden con un objeto de directiva de grupo (GPO). Permite a los administradores especificar criterios como el tipo de protocolo, los números de puerto y otros atributos de paquete para que la política correspondiente se pueda aplicar a los flujos de tráfico deseados.

En esta situación, el objetivo es permitir solamente el tráfico ICMP mientras se bloquea explícitamente el tráfico TCP en el puerto 22 (SSH). Esta política garantiza que las pruebas de disponibilidad de la red permanezcan permitidas, mientras que el acceso SSH no autorizado o no deseado se restringe manualmente.

Vaya a Administrar > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Protocol definition > Actions > Create protocol definition.

Introduzca el nombre y la descripción.



Navegue hasta Acciones > Crear entrada de protocolo.

- Nombre: SSH
- Tipo: IPv4
    - IP e IPv6 también están disponibles.
- Protocolo/opciones IP: TCP
    - UDP, EIGRP y PIM, entre otros, son compatibles.

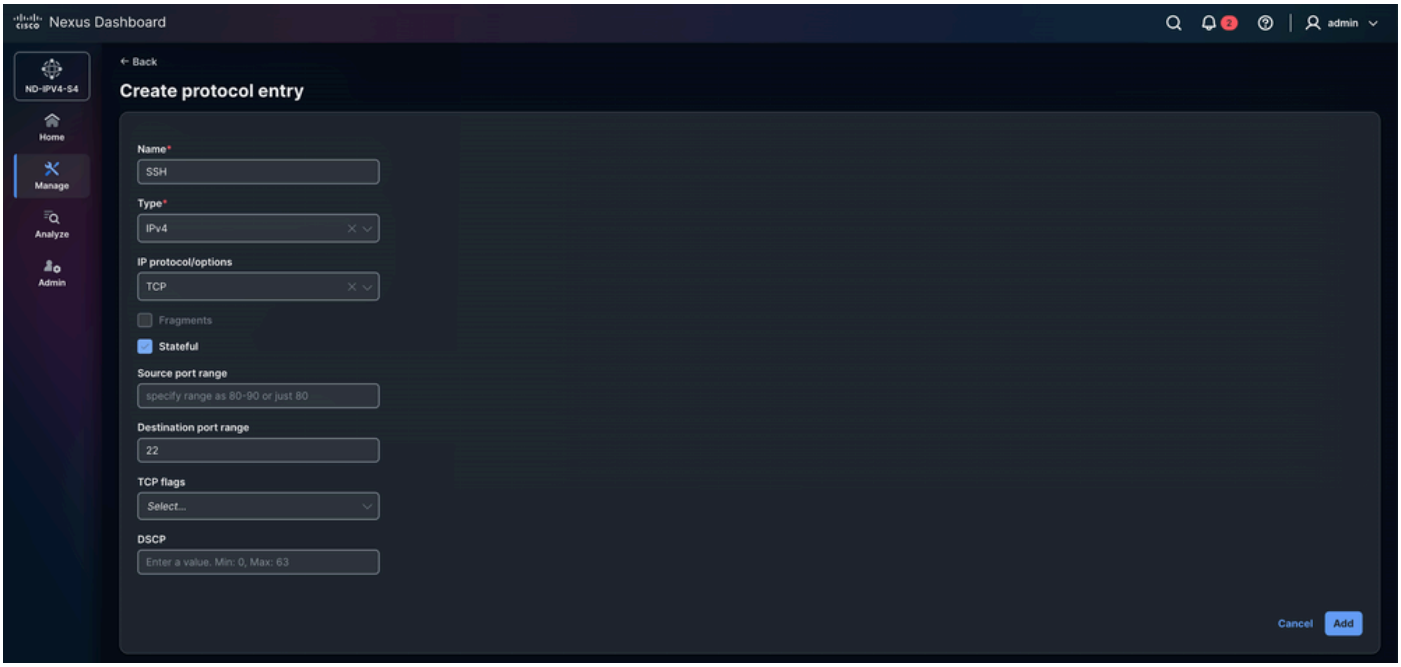
- Fragmentos: Permite que la regla coincida con los paquetes IP fragmentados. Esto es útil porque los paquetes grandes se pueden dividir en fragmentos cuando se excede la MTU de la red. Si activa esta opción, la política también se aplicará a esos fragmentos.

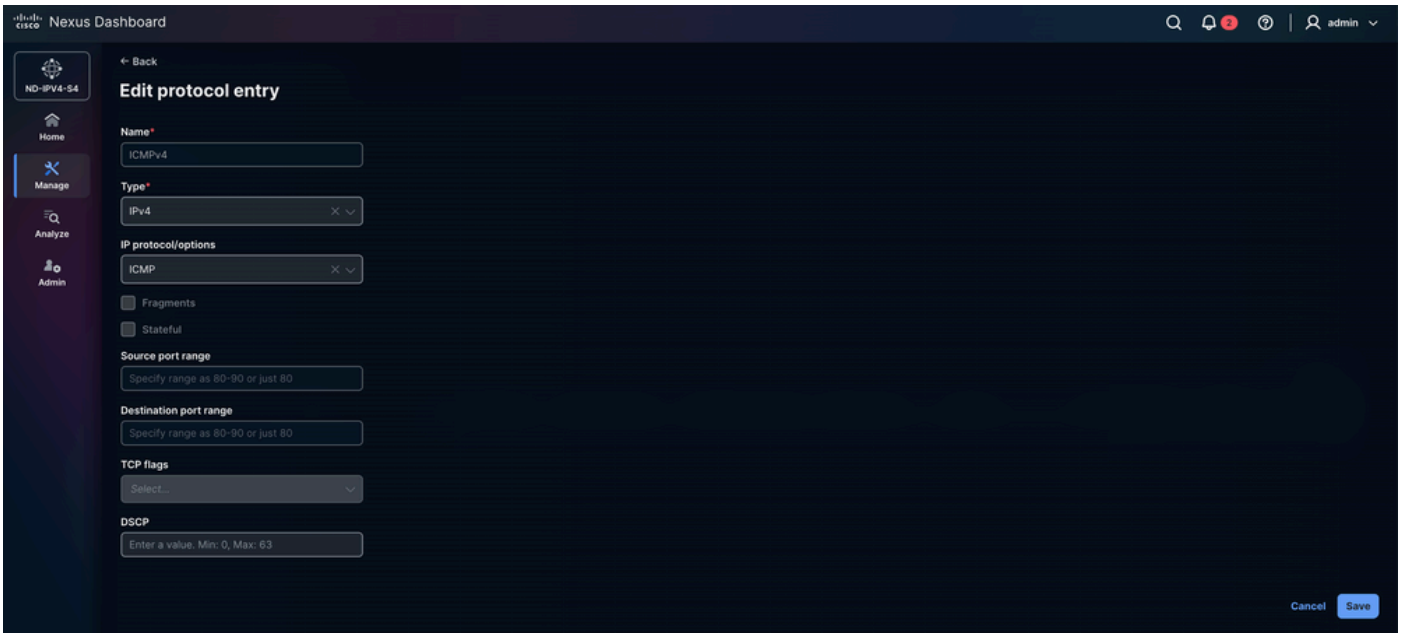
- Con estado: Un proceso con estado significa que realiza un seguimiento de todos los cambios o interacciones que ocurrieron en el pasado, y un proceso actual se realiza con un contexto de esos procesos anteriores. En este caso, TCP realiza un seguimiento de áreas tales como el número de paquetes que se van a transferir, el orden de los paquetes y si el receptor ha recibido un paquete o no. Con la opción Stateful seleccionada, esta información se almacena como un estado en TCP.

- Intervalo de puertos de origen: Esta opción sólo está disponible si ha seleccionado TCP o UDP en el campo IP Protocol/Options (Opciones/Protocolo IP) anterior.
- Intervalo de puertos de destino: esta opción sólo está disponible si ha seleccionado TCP o UDP en el campo IP Protocol/Options (Opciones/Protocolo IP).
- Indicadores TCP

    - Esta opción sólo está disponible cuando se selecciona TCP en el campo IP Protocol/Options (Opciones/Protocolo IP).

- Permite definir los indicadores TCP que utiliza el protocolo de seguridad.
- Los indicadores TCP forman parte del encabezado TCP y se utilizan para controlar el establecimiento, el mantenimiento y la terminación de las conexiones.
- Opciones disponibles:
    - ACK (confirmación): Indica la confirmación de los datos recibidos o los paquetes de sincronización.
    - EST (establecido): Hace referencia a conexiones TCP ya establecidas. Cuando esta opción está habilitada, no se puede seleccionar ningún otro indicador TCP.
    - FIN (fin): Se utiliza para cerrar correctamente una conexión TCP.
    - RST (Reinicio): Finaliza inmediatamente la conexión y descarta los datos que aún estén en tránsito.
    - SYN (sincronización): Se utiliza durante el inicio y el establecimiento de una conexión TCP.





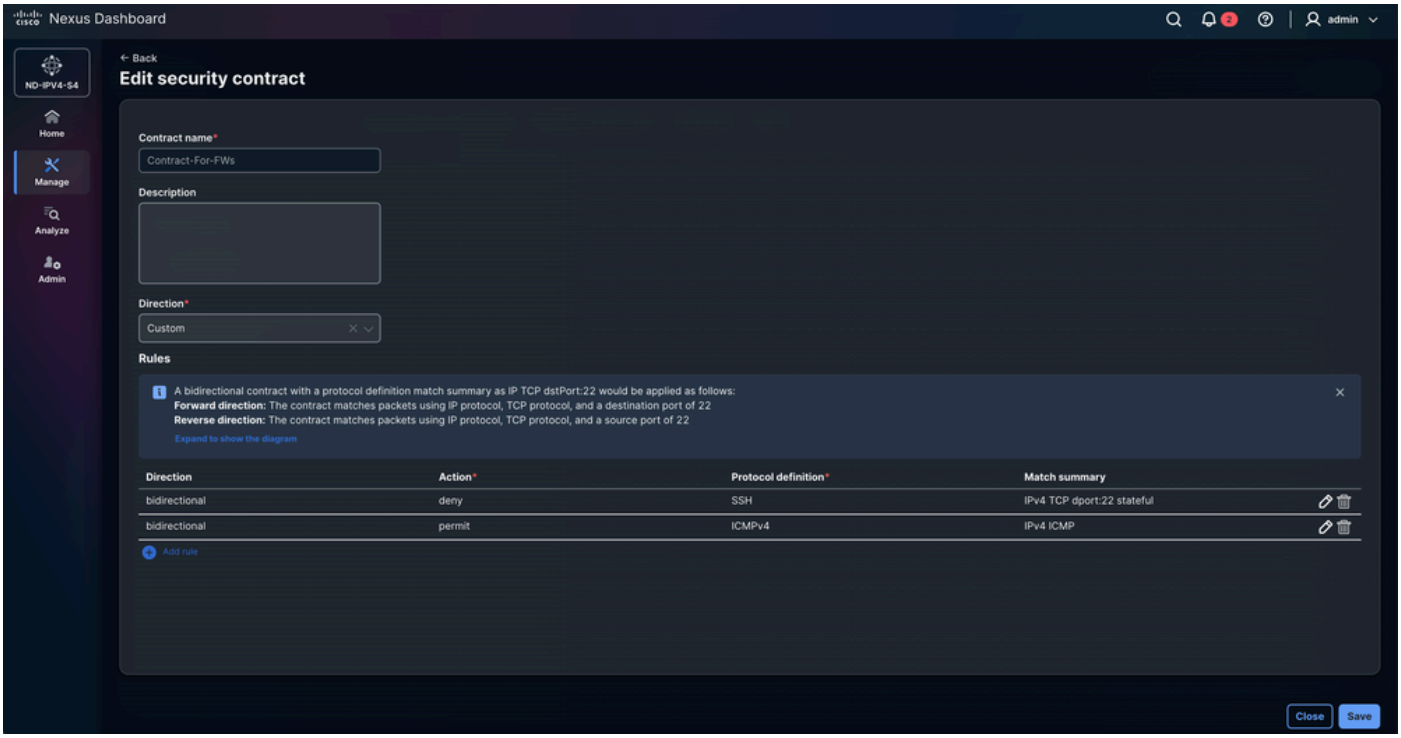
Paso 5. Configuración de los contratos de seguridad

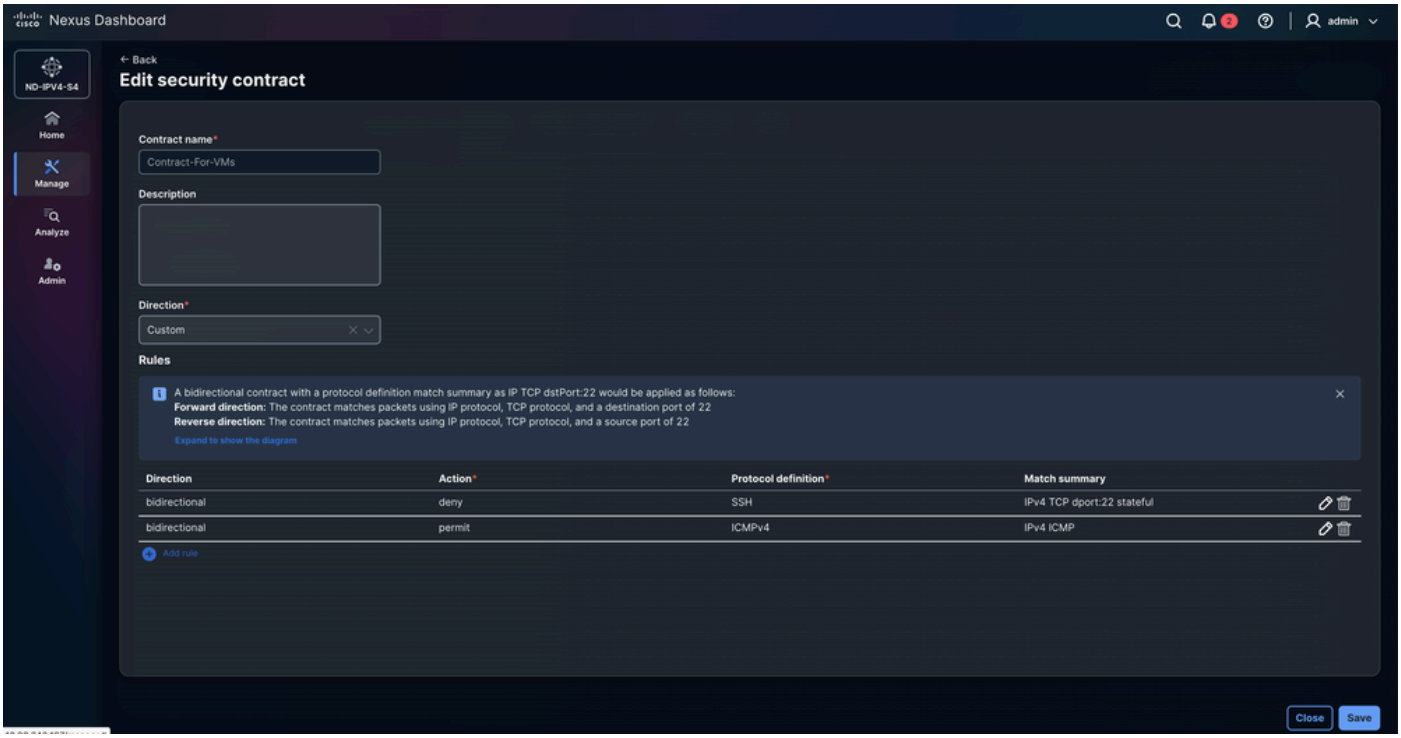
El contrato define las reglas de comunicación entre los grupos de terminales especificando qué tráfico se permite o se deniega en función de las definiciones de políticas asociadas. Actúa como el mecanismo de aplicación que aplica las reglas, filtros y acciones de protocolo configuradas, garantizando que el tráfico entre los grupos de origen y de destino cumple con las políticas de segmentación y seguridad deseadas.

Vaya a Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security Contracts > Actions > Create security contract.

- Seleccione Agregar regla y configure Dirección, Acción y Definición de protocolo.
    - Bidireccionales:
        - El contrato bidireccional se aplica de la siguiente manera con un resumen de coincidencia de definición de protocolo como Puerto TCP IP 22.
            - Dirección hacia adelante: El contrato hace coincidir los paquetes mediante el protocolo IP, el protocolo TCP y un puerto de destino de 22
            - Dirección inversa: El contrato hace coincidir los paquetes mediante el protocolo IP, el protocolo TCP y un puerto de origen de 22.
            - Esto se aplica independientemente del origen o el destino.
    - Unidireccional:
        - Unidireccional en un contrato de seguridad de GPO significa que la política se

aplica en una sola dirección del flujo de tráfico, lo que permite o deniega la comunicación del grupo de seguridad de origen al grupo de seguridad de destino sin aplicar automáticamente la misma regla en la dirección inversa.

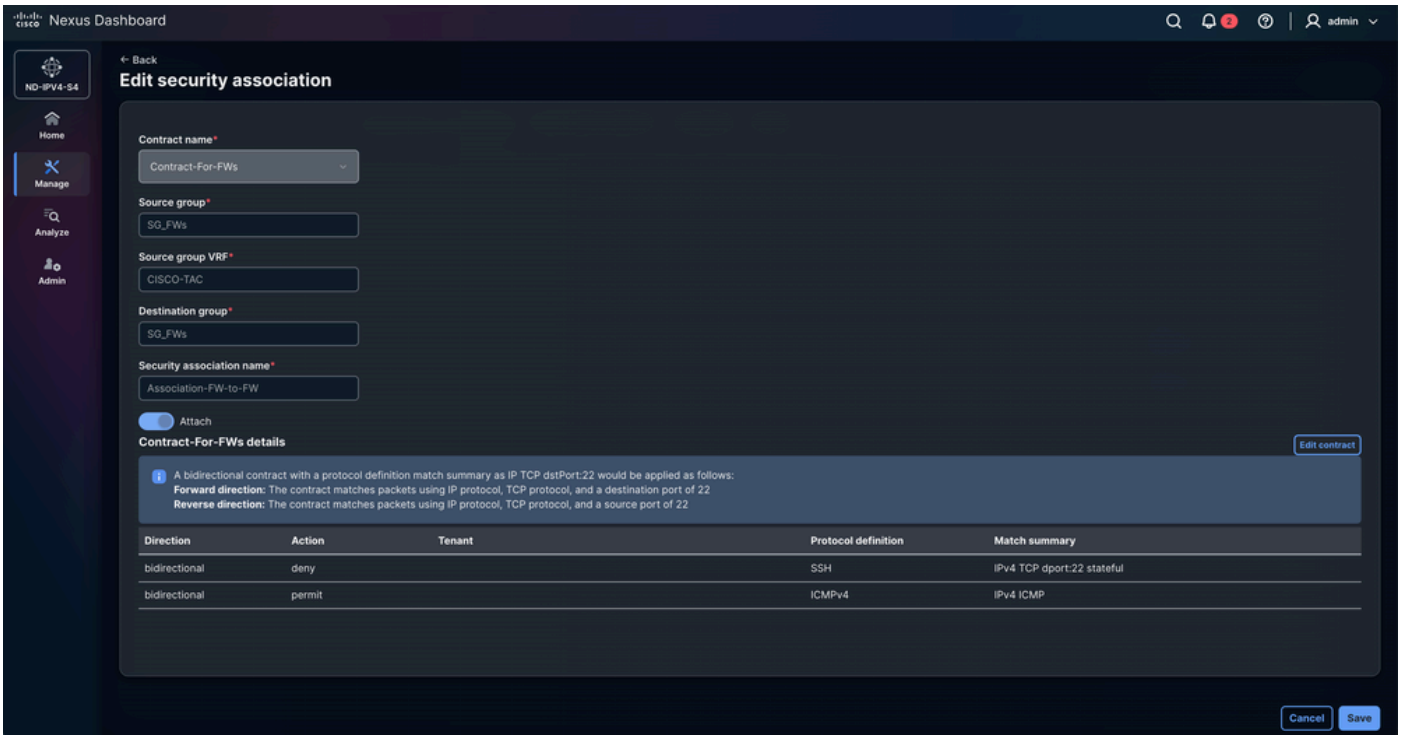


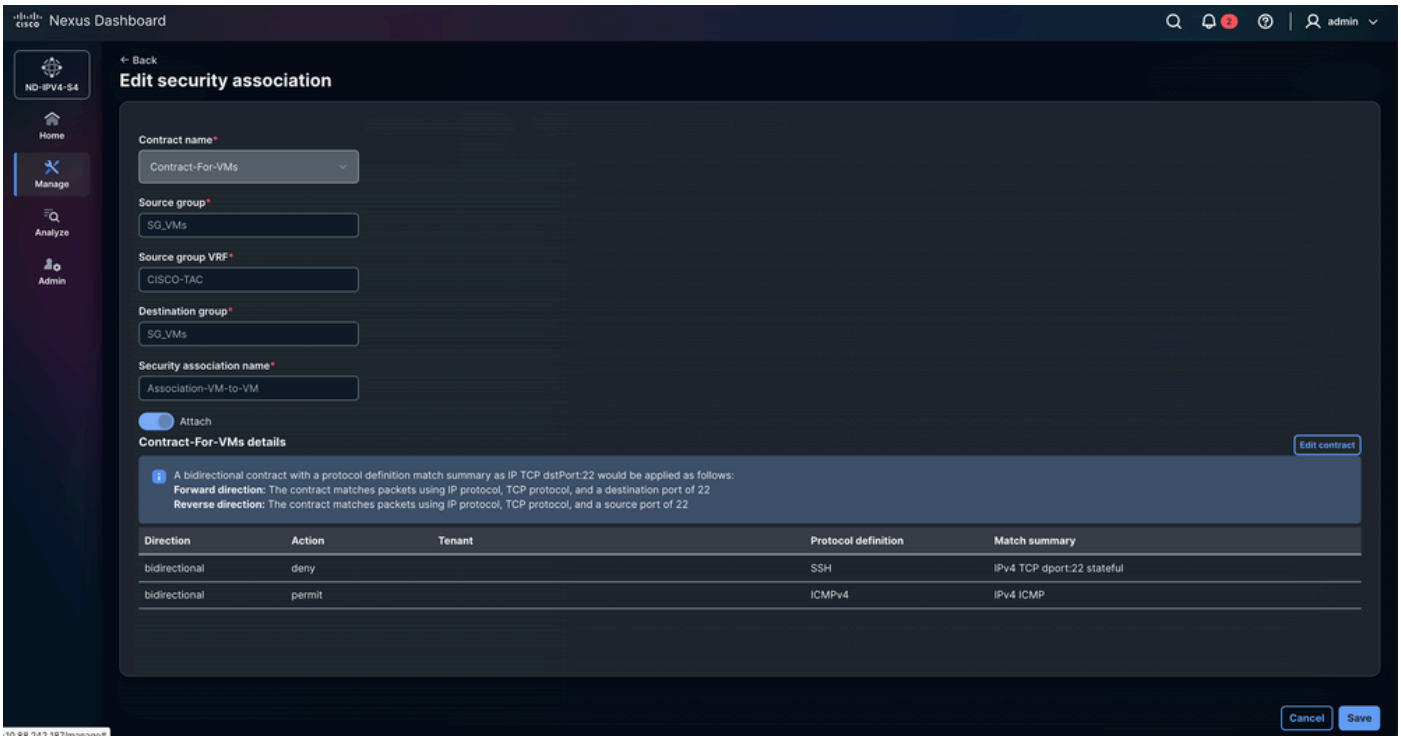


Paso 6. Configurar asociaciones de seguridad

Vaya a Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security associations > Actions > Create security association.

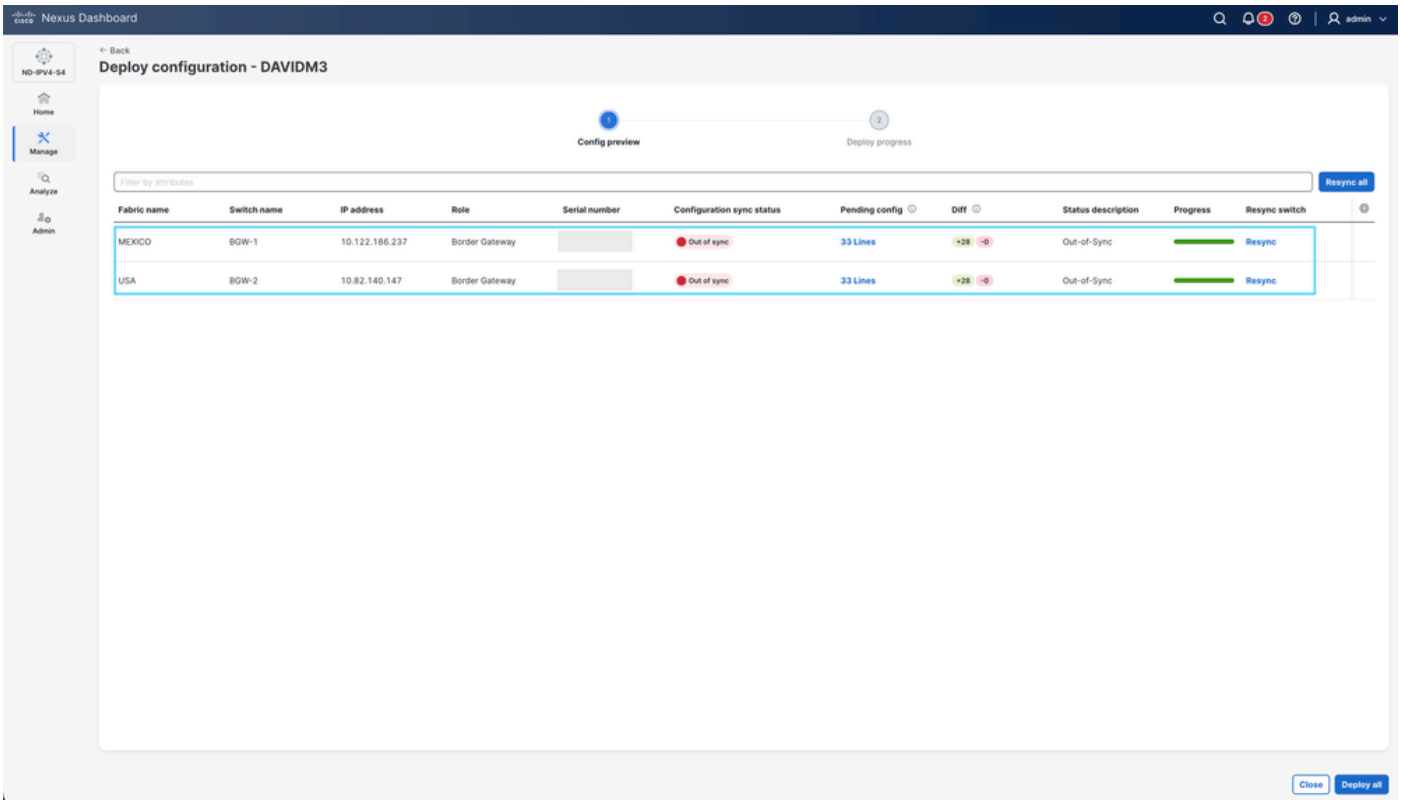
En Configurar asociaciones de seguridad, el modelo de políticas se define vinculando grupos de seguridad, definiciones de protocolo y contratos de seguridad. Los grupos de seguridad clasifican los terminales, las definiciones de protocolo especifican los tipos de tráfico (como protocolos o puertos) y los contratos de seguridad definen la política aplicada entre los grupos de seguridad de origen y de destino utilizando esas reglas de protocolo. Las asociaciones de seguridad representan la relación que une a estos elementos para que el fabric pueda aplicar las políticas de seguridad definidas.

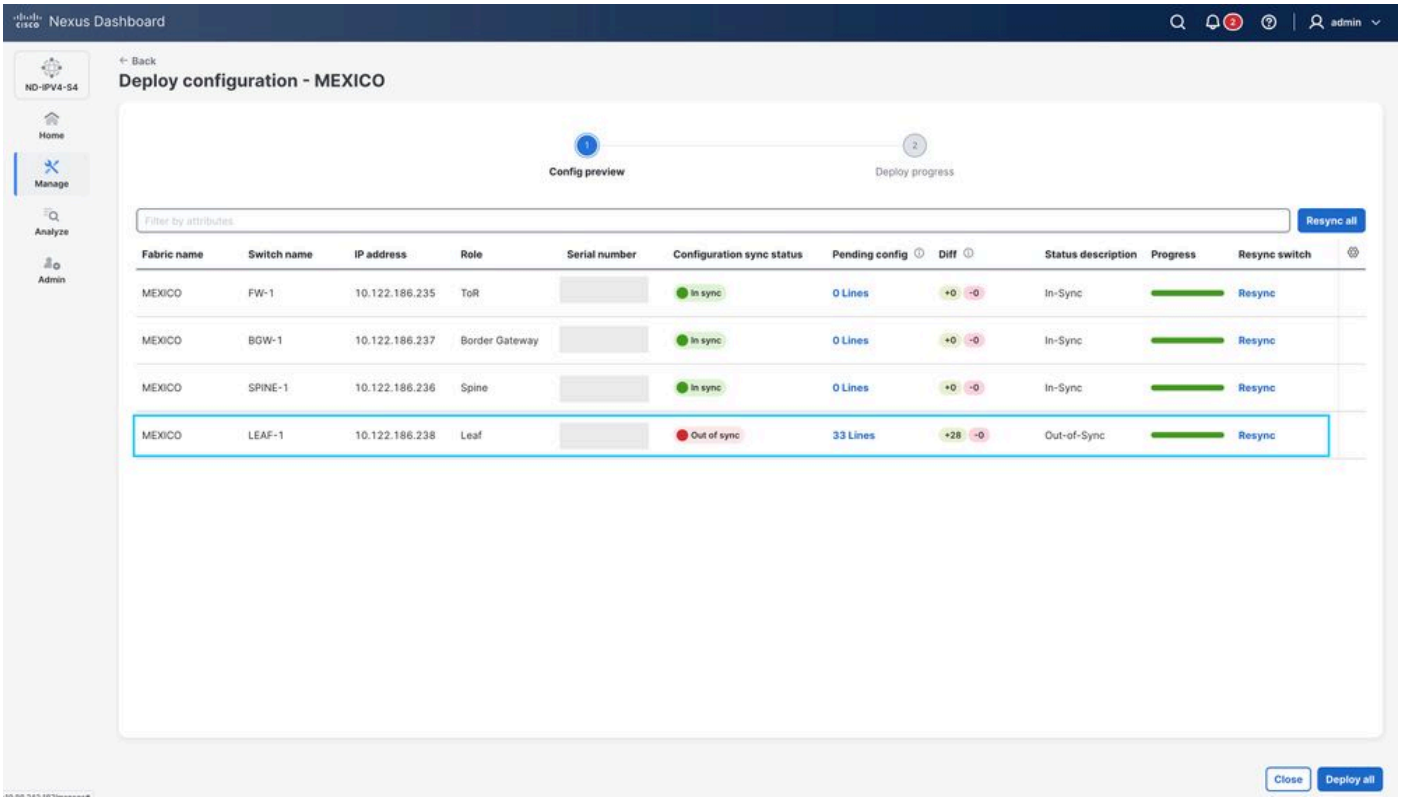


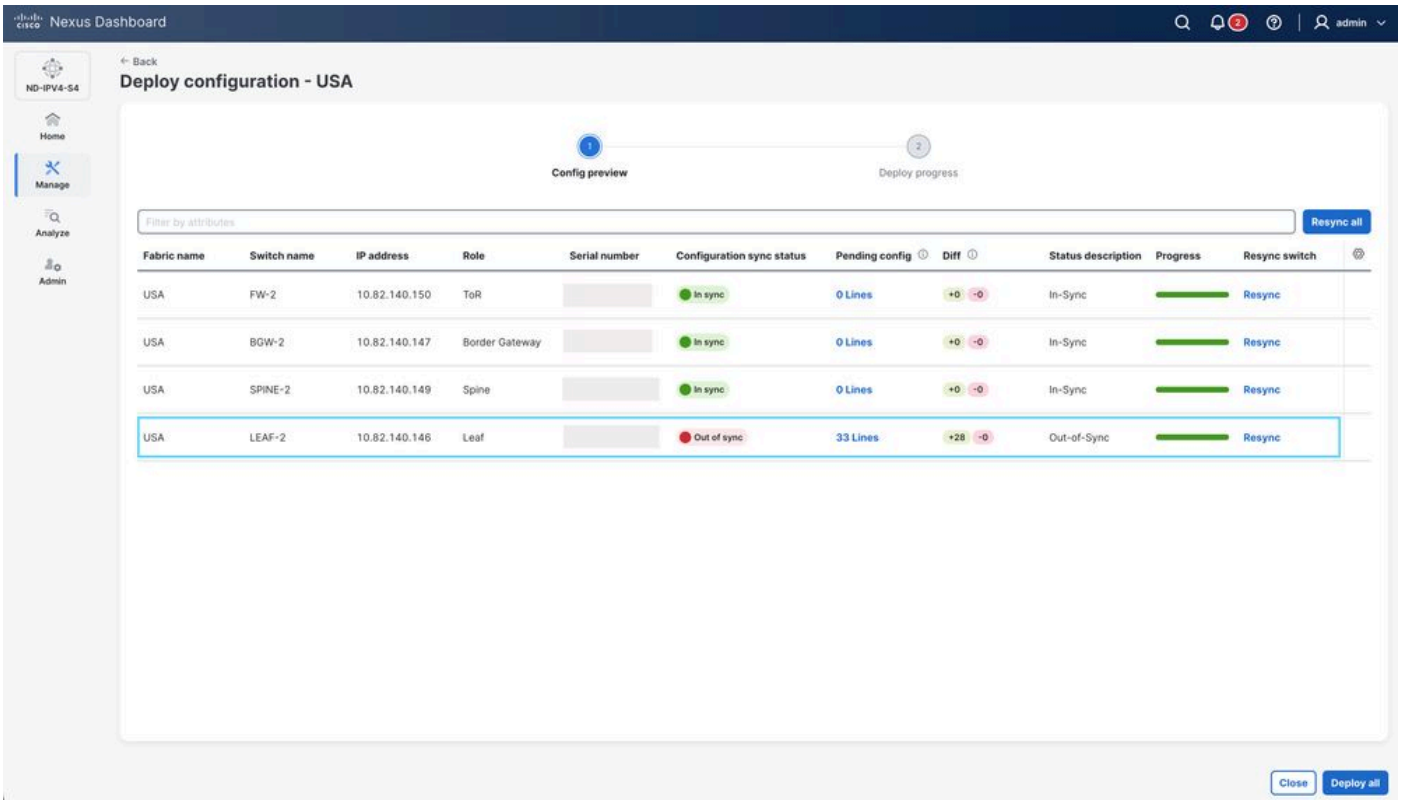


Paso 7. Validar configuración GPO

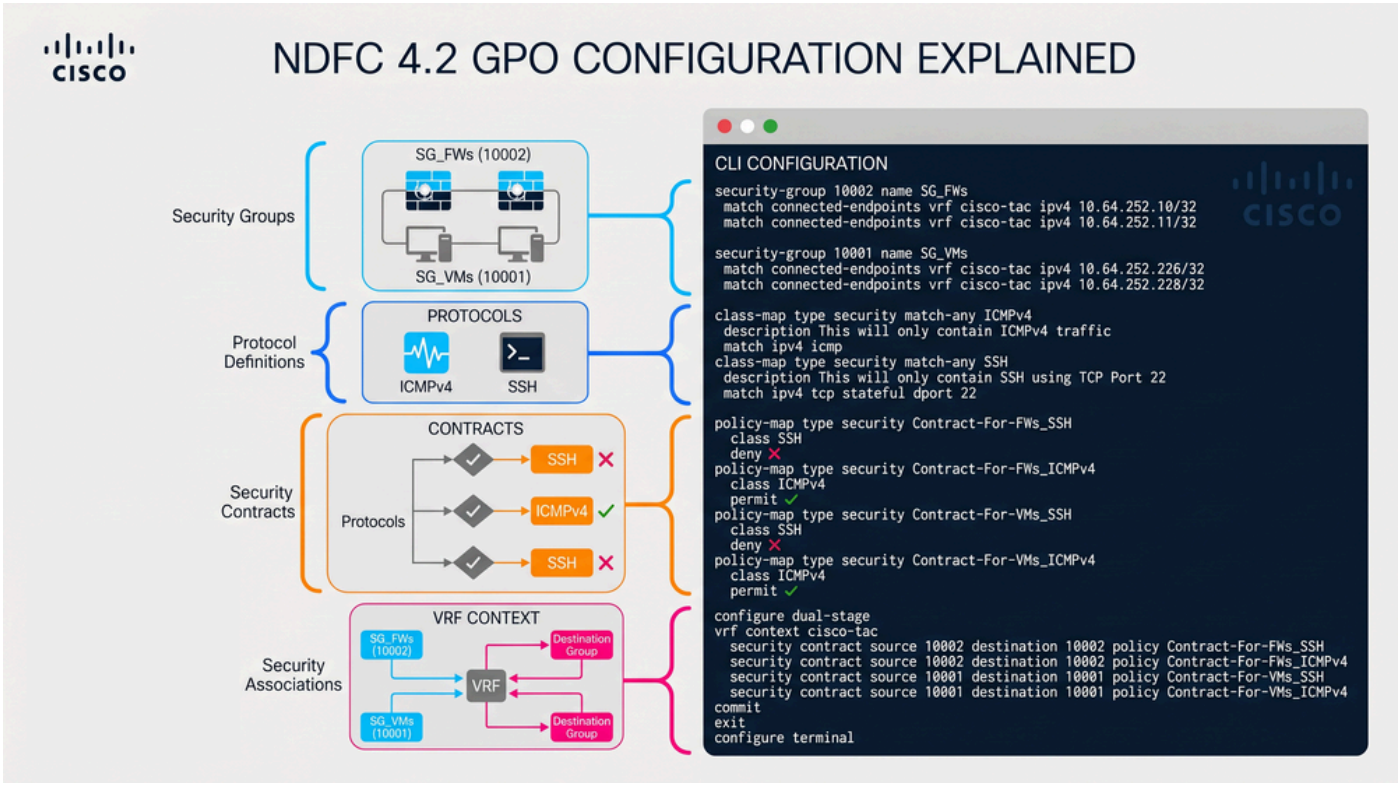
- Vaya a Manage > Fabrics > Fabric groups > DAVIDM3 > Actions > Recalculate and deploy.
  - La configuración de GPO se envía a los gateways de borde desde el switch de fabric principal. Haga clic en el número de líneas de configuración pendientes para revisar y validar la configuración que se puede implementar en los dispositivos. Este proceso debe repetirse para cada tejido secundario.
  - Vaya a Manage > Fabrics > Fabric groups > DAVIDM3 > Inventory > Member fabrics > MEXICO > Actions > Recalculate and deploy.
  - Vaya a Manage > Fabrics > Fabric groups > DAVIDM3 > Inventory > Member fabrics > USA > Actions > Recalculate and deploy.


Nexus Dashboard
admin
ND-IPV4-S4
Home
Manage
Analyze
Admin
Back
Deploy configuration - DAVIDM3
1
Config preview
2
Deploy progress
Filter by attributes
Resync all
Fabric name
Switch name
IP address
Role
Serial number
Configuration sync status
Pending config
Diff
Status description
Progress
Resync switch
MEXICO
BGW-1
10.122.186.237
Border Gateway
Out of sync
33 Lines
+28
-0
Out-of-Sync
Resync
USA
BGW-2
10.82.140.147
Border Gateway
Out of sync
33 Lines
+28
-0
Out-of-Sync
Resync
Close
Deploy all


Nexus Dashboard
admin
ND-IPV4-S4
Home
Manage
Analyze
Admin
Back
Deploy configuration - MEXICO
1
Config preview
2
Deploy progress
Filter by attributes
Resync all
Fabric name
Switch name
IP address
Role
Serial number
Configuration sync status
Pending config
Diff
Status description
Progress
Resync switch
MEXICO
FW-1
10.122.186.235
ToR
In sync
0 Lines
+0
-0
In-Sync
Resync
MEXICO
BGW-1
10.122.186.237
Border Gateway
In sync
0 Lines
+0
-0
In-Sync
Resync
MEXICO
SPINE-1
10.122.186.236
Spine
In sync
0 Lines
+0
-0
In-Sync
Resync
MEXICO
LEAF-1
10.122.186.238
Leaf
Out of sync
33 Lines
+28
-0
Out-of-Sync
Resync
Close
Deploy all



- La imagen muestra la configuración GPO para BGW-1, BGW-2, LEAF-1 y LEAF-2. La configuración es idéntica en todos los switches. NDFC 4.2 no aplica la configuración en el orden exacto que se muestra. Esta sección ilustra la secuencia lógica de los comandos CLI.



Solución de problemas de funcionalidad GPO VXLAN

Paso 1. Verificar el Estado de la Función Security-Group

Valide si la función de grupo de seguridad está habilitada en el switch. El GPO de VXLAN depende de esta característica porque activa la infraestructura de Security Group Tag (SGT) necesaria para la clasificación de terminales, la aplicación de contratos y la programación de hardware de SGACL.

<#root>

```
BGW-1#

show feature | i i security-group


security-group 1 enabled
```

Paso 2. Verificar el Modo de Ruteo del Sistema

Valide el modo de ruteo del sistema configurado y operativo en el switch. El GPO de VXLAN requiere el modo de enrutamiento Security-Groups Support porque la aplicación de SGACL consume recursos de reenvío de hardware dedicados en la canalización ASIC.

<#root>

```
BGW-1#

show system routing mode


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

Paso 3. Verificar el establecimiento de pares VXLAN NVE y la capacidad de GPO

- Validar el establecimiento de pares VXLAN NVE entre los dispositivos de fabric locales y los pares remotos multisitio. La información de GPO de VXLAN se propaga a través del plano de control de VXLAN EVPN, por lo que se requieren adyacencias NVE estables para el aprendizaje de Security Group Tag (SGT) y la sincronización de contratos en el fabric.

- El campo con capacidad para políticas de grupo es uno de los indicadores más importantes de este comando, ya que confirma si VTEP remoto admite extensiones de políticas de grupo de VXLAN necesarias para la propagación de SGT y la aplicación de contratos SGACL en el dominio multisitio 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

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

Paso 4. Verificar el aprendizaje del grupo de seguridad y la clasificación de terminales

Valide que los terminales están correctamente clasificados en grupos de seguridad (SGT). La aplicación de GPO de VXLAN depende de asignaciones exactas de punto final a 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
```

Paso 5. Verificar los contratos de seguridad y la aplicación de políticas

Valide que los contratos GPO de VXLAN estén correctamente instalados y en funcionamiento. Los contratos definen las reglas de comunicación aplicadas entre los grupos de seguridad y representan el mecanismo de política principal utilizado por el GPO de VXLAN para la microsegmentación.

<#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
```

Paso 6. Verificar el Estado de Aplicación de Seguridad VRF

Valide el estado de aplicación de GPO de VXLAN para todos los VRF configurados en el switch. Este comando confirma si las políticas SGACL y los contratos del grupo de seguridad se aplican activamente dentro del VRF del arrendatario.

El resultado confirma que el VRF de Cisco-Tac participa activamente en la aplicación de GPO de VXLAN con el modo establecido en forzado. La etiqueta de aplicación 13648 identifica el contexto de política SGACL interno programado en el hardware para este VRF. El registro de denegación de acciones predeterminado indica que se deniega y registra todo el tráfico no permitido explícitamente a través de un contrato de grupo de seguridad, lo que implementa una política de microsegmentación de denegación predeterminada. Por el contrario, los VRF predeterminados de gestión, resolución y equilibrio de carga de salida y gestión funcionan en modo no aplicado, lo que significa que las políticas de GPO de VXLAN no se aplican dentro de esos VRF y el tráfico está permitido de forma predeterminada.

El campo Stats realiza un seguimiento del tráfico que coincide con la política de seguridad VRF. El valor 0 bajo el VRF cisco-tac indica que ningún tráfico sin coincidencia activó el comportamiento de negación predeterminado en el momento en que se ejecutó el comando, mientras que el valor del contador 4364 bajo el VRF predeterminado indica actividad de tráfico dentro de un VRF que funciona sin la aplicación del GPO de VXLAN.

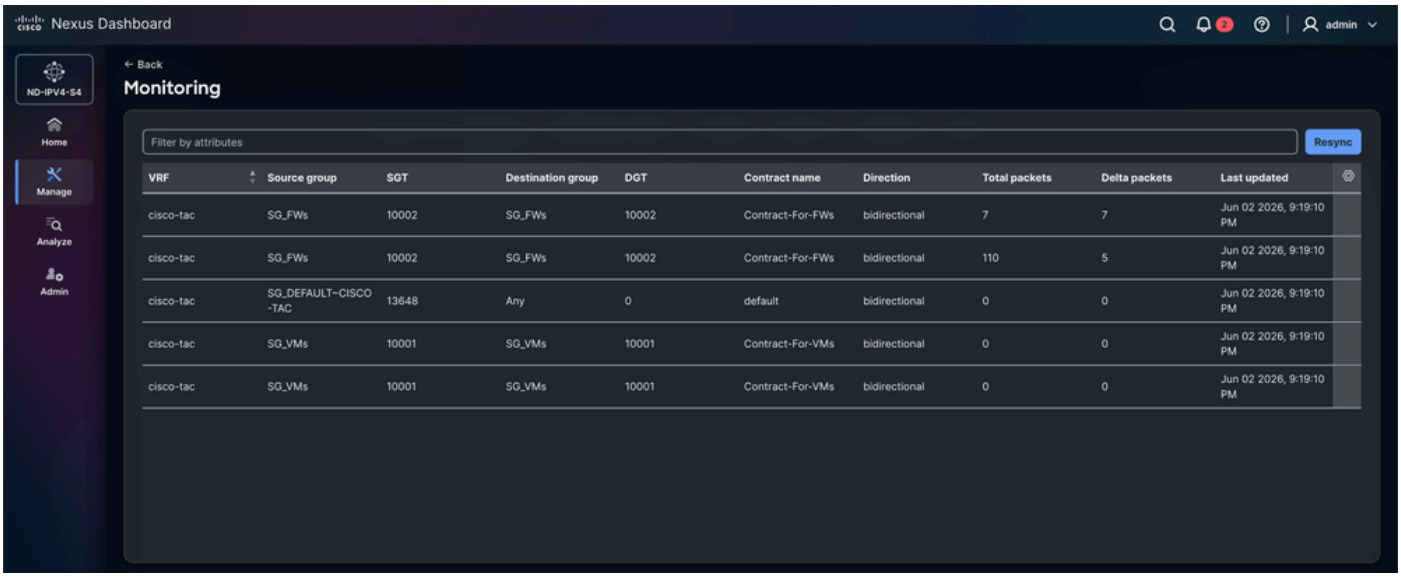
```
<#root>

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
```

Paso 7. Verificar el Estado de Aplicación de Seguridad VRF

- Valide las estadísticas de coincidencia de tráfico para los contratos GPO de VXLAN desde la GUI de NDFC. Esta verificación confirma si el tráfico coincide activamente con los contratos de grupo de seguridad configurados y si la aplicación de SGACL está operativa en el fabric multisitio de VXLAN EVPN.
- En la GUI de NDFC, vaya a Manage > Fabrics > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoring.
    - Esta sección proporciona visibilidad de los flujos de comunicación del grupo de seguridad, las estadísticas de aciertos de los contratos, las acciones de permiso y denegación y la actividad de los contratos operativos entre los grupos de terminales.
    - Las estadísticas de supervisión se muestran de forma individual dentro de cada una.
    - Las estadísticas de supervisión de NDFC proporcionan una capa de validación operativa que complementa la solución de problemas basada en CLI mediante la confirmación de la aplicación de políticas en tiempo real y el comportamiento de coincidencia de tráfico en todo el fabric.

Nota: En el primer intento de revisar las estadísticas de tráfico en NDFC 4.2, la sección de monitoreo puede aparecer inicialmente vacía. En esta situación, pulse el botón Resync para activar la sincronización de las estadísticas de contrato desde el fabric VXLAN. Mientras se ejecuta el proceso de sincronización, la GUI muestra el mensaje Resync status: En curso. Una vez completada la sincronización, presione el botón Ok para actualizar la vista de monitoreo. Una vez finalizada la resincronización, las estadísticas de tráfico asociadas a cada contrato de grupo de seguridad se vuelven visibles en la sección de supervisión. Para validar el comportamiento de coincidencia de tráfico en vivo, genere tráfico entre los terminales y luego presione el botón Resync nuevamente para actualizar las estadísticas de contrato mostradas en NDFC.



- En el escenario anterior, el tráfico ICMPv4 se permite correctamente entre los terminales. Sin embargo, si se establece una sesión SSH, la conexión se desconecta porque el contrato GPO de VXLAN niega explícitamente el tráfico TCP destinado al puerto 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
```

Información Relacionada

[Guía de configuración de VXLAN NX-OS para Cisco Nexus serie 9000, versión 10.6(x)]

Protección de Data Centers con microsegmentación mediante GPO VXLAN

Implementación de microsegmentación en estructuras VXLAN EVPN de Cisco NX-OS con la opción de política de grupo (GPO) de VXLAN

Automatización de la microsegmentación e implementación de servicios de nivel 4-7 en estructuras VXLAN EVPN mediante la opción de política de grupo (GPO) y el panel de Nexus

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).