Configurazione dell'oggetto Criteri di gruppo su Nexus Multi-Site Fabric con NDFC 4.2

Sommario

Introduzione

In questo documento viene descritta la configurazione e la convalida degli oggetti Criteri di gruppo in fabric VXLAN multisito su switch Nexus Cloud Scale che eseguono NX-OS e NDFC 4.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle seguenti aree:

- Tecnologie VXLAN (Virtual Extensible Local Area Network), EVPN (Virtual Private Network) Ethernet e fabric multisito
- Switch Cisco Nexus con scalabilità cloud e funzionamento del sistema operativo NetXus (NX-OS)
- Workflow di gestione e installazione Nexus Fabric Network Controller (NDFC) 4.2
- Nozioni fondamentali sulla segmentazione della rete e sui criteri di sicurezza

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Conoscenza delle funzionalità degli oggetti Criteri di gruppo nelle infrastrutture VPN VXLAN

L'opzione Criteri di gruppo è un meccanismo di segmentazione basato su criteri progettato per controllare la comunicazione tra endpoint in base all'identità logica anziché basarsi solo su indirizzi IP, VLAN o subnet. Lo scopo principale dell'oggetto Criteri di gruppo è semplificare l'applicazione delle policy di sicurezza e fornire una microsegmentazione scalabile tra applicazioni, server o carichi di lavoro.

Una semplice analogia consiste nel pensare a un hotel in cui ogni ospite appartiene a una categoria o a un livello di accesso specifico, alcune aree sono accessibili solo a ospiti specifici e i permessi di accesso dipendono dal ruolo dell'ospite invece che dal numero della stanza. L'oggetto Criteri di gruppo funziona in modo molto simile. Anziché considerare gli endpoint esclusivamente come indirizzi IP, l'oggetto Criteri di gruppo li classifica in gruppi di sicurezza. Vengono quindi applicati criteri tra questi gruppi per determinare quali comunicazioni sono consentite o negate.

Ad esempio:

- I server Web possono appartenere a un gruppo di sicurezza.
- I server applicazioni possono appartenere a un altro gruppo di sicurezza.
- I server di database possono appartenere a un gruppo di sicurezza con restrizioni.

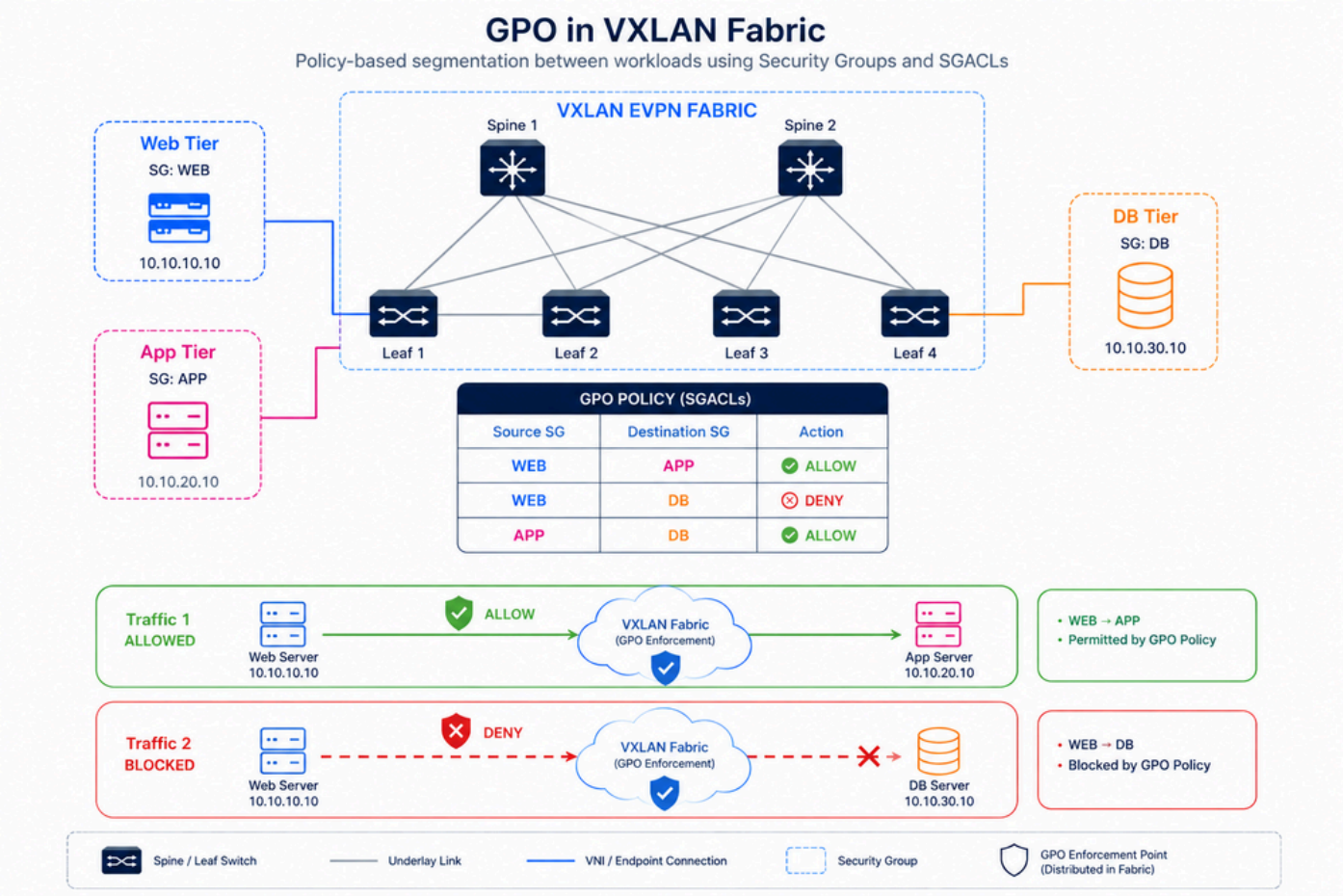
I criteri possono quindi definire:

- I server Web possono comunicare con i server applicazioni.
- I server applicazioni possono comunicare con i server di database.
- I server Web non possono comunicare direttamente con i server di database.

Questo approccio semplifica le operazioni in quanto gli amministratori non devono più mantenere un numero elevato di ACL su più dispositivi e VLAN.

Un altro importante vantaggio è la scalabilità. In ambienti di grandi dimensioni, i carichi di lavoro vengono spostati, ridimensionati dinamicamente o modificano gli indirizzi IP. L'oggetto Criteri di gruppo consente ai criteri di sicurezza di rimanere coerenti anche quando viene modificata la posizione dell'endpoint. All'interno delle strutture EVPN VXLAN, l'oggetto Criteri di gruppo estende questo concetto distribuendo le informazioni del gruppo di sicurezza nell'infrastruttura e applicando gli ACL del gruppo di sicurezza (SGACL) tra gli endpoint. Ciò diventa particolarmente importante nei moderni centri dati, in quanto il traffico est-ovest tra i carichi di lavoro rappresenta spesso la superficie di attacco più grande. L'oggetto Criteri di gruppo migliora la postura di sicurezza limitando i percorsi di comunicazione non necessari all'interno del fabric del centro dati.

Per una comprensione tecnica più approfondita dell'architettura degli oggetti Criteri di gruppo, dei concetti di microsegmentazione e dell'applicazione delle policy VXLAN, fare riferimento al white paper Cisco disponibile all'indirizzo: Secure Data Centers with Microsegmentation using VXLAN GPO (Protezione dei centri dati con microsegmentazione tramite VXLAN).



Oggetto Criteri di gruppo nell'infrastruttura VxLAN

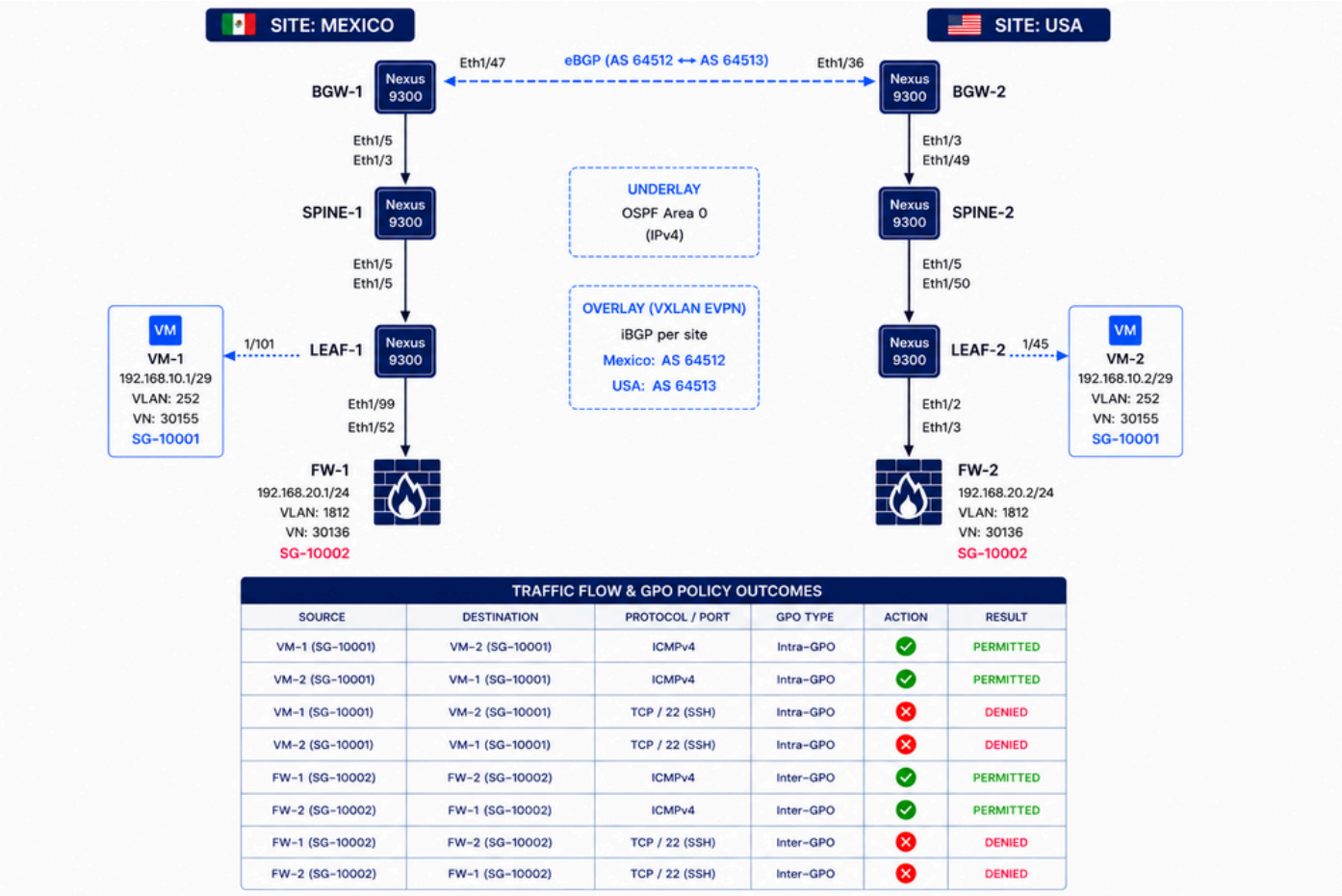
Scenario di distribuzione di oggetti Criteri di gruppo multisito VXLAN con NDFC 4.2 e NX-OS 10.6(3)F

Questa topologia rappresenta una struttura VXLAN multisito distribuita su due siti geograficamente distribuiti: Messico e Stati Uniti. Ciascun sito contiene BGW, switch Spine, switch Leaf, macchine virtuali e segmenti firewall dedicati eseguiti su switch Cisco Nexus 9300 con NX-OS 10.6(3)F. La rete sottostante utilizza Open Shortest Path First (OSPF), mentre il control plane di overlay utilizza iBGP all'interno di ciascun sito e eBGP tra BGW-1 e BGW-2 per la comunicazione VXLAN EVPN tra siti. Poiché questo ambiente è un'installazione di laboratorio, i siti in Messico e negli Stati Uniti sono interconnessi tramite un collegamento diretto tra entrambi i BGW per semplificare il modello di connettività multisito.

L'oggetto Criteri di gruppo viene utilizzato per applicare la microsegmentazione basata su policy tra i gruppi di sicurezza (SG) indipendentemente dall'indirizzamento IP o dai limiti della VLAN. In base alla tabella dei criteri di connettività, è consentito il traffico ICMP da VM-1 a VM-2, FW-1 e

FW-2, mentre il traffico della porta TCP 2 (SSH) da VM-1 a FW-1 e FW-2 viene rifiutato. La comunicazione della porta TCP 2 tra VM-1 e VM-2 rimane consentita perché entrambi gli endpoint appartengono allo stesso gruppo di sicurezza (SG-10001). Questo comportamento dimostra come l'oggetto Criteri di gruppo applica in modo dinamico criteri di traffico diversi tra le comunicazioni tra oggetti Criteri di gruppo e tra oggetti Criteri di gruppo nell'infrastruttura VXLAN multisito.

Nota: Cisco NX-OS versione 10.6(3)F introduce la possibilità di limitare la comunicazione tra gli endpoint all'interno dello stesso ESG (noto anche come SG) utilizzando la funzione di isolamento intra-ESG. Questa funzione riduce al minimo il rischio di accesso non autorizzato all'interno di ESG e migliora la postura di sicurezza.



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

Configurazione dettagliata dell'oggetto Criteri di gruppo con NDFC 4.2 in fabric VXLAN VPN

Questi passaggi si applicano quando il fabric VXLAN multisito è già operativo e configurato con NDFC 4.2 e l'oggetto Criteri di gruppo deve essere implementato successivamente. La sezione Automazione tramite Nexus Dashboard in Protezione dei centri dati con microsegmentazione

tramite l'oggetto Criteri di gruppo VXLAN mostra la configurazione a partire dalla creazione di una struttura VXLAN per sito singolo.

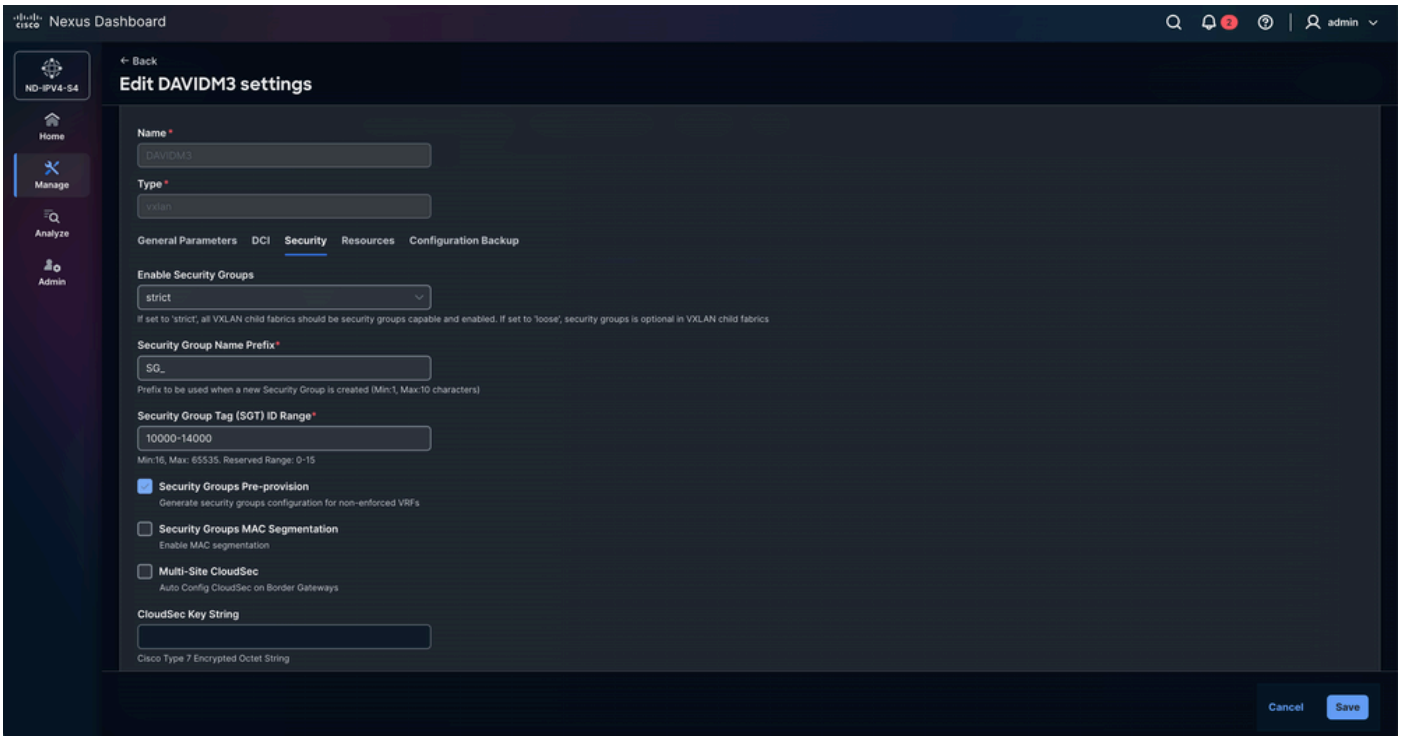
Attenzione: Quando l'oggetto Criteri di gruppo funziona in un'infrastruttura VXLAN VPN, la comunicazione viene eseguita solo se esiste la raggiungibilità della destinazione e i criteri di sicurezza consentono il traffico. L'applicazione delle policy si basa sulle informazioni IP, che richiedono le voci ARP e le SVI per le reti interne. Ciò significa che per la VLAN che appartiene al VRF tenant deve essere configurata una SVI. Di conseguenza, l'applicazione non si applica al traffico che contiene solo intestazioni di layer 2 e che pertanto non può essere utilizzato con l'estensione VXLAN Layer 2. NX-OS release 10.6(2)F introduce il supporto della microsegmentazione basata su MAC.

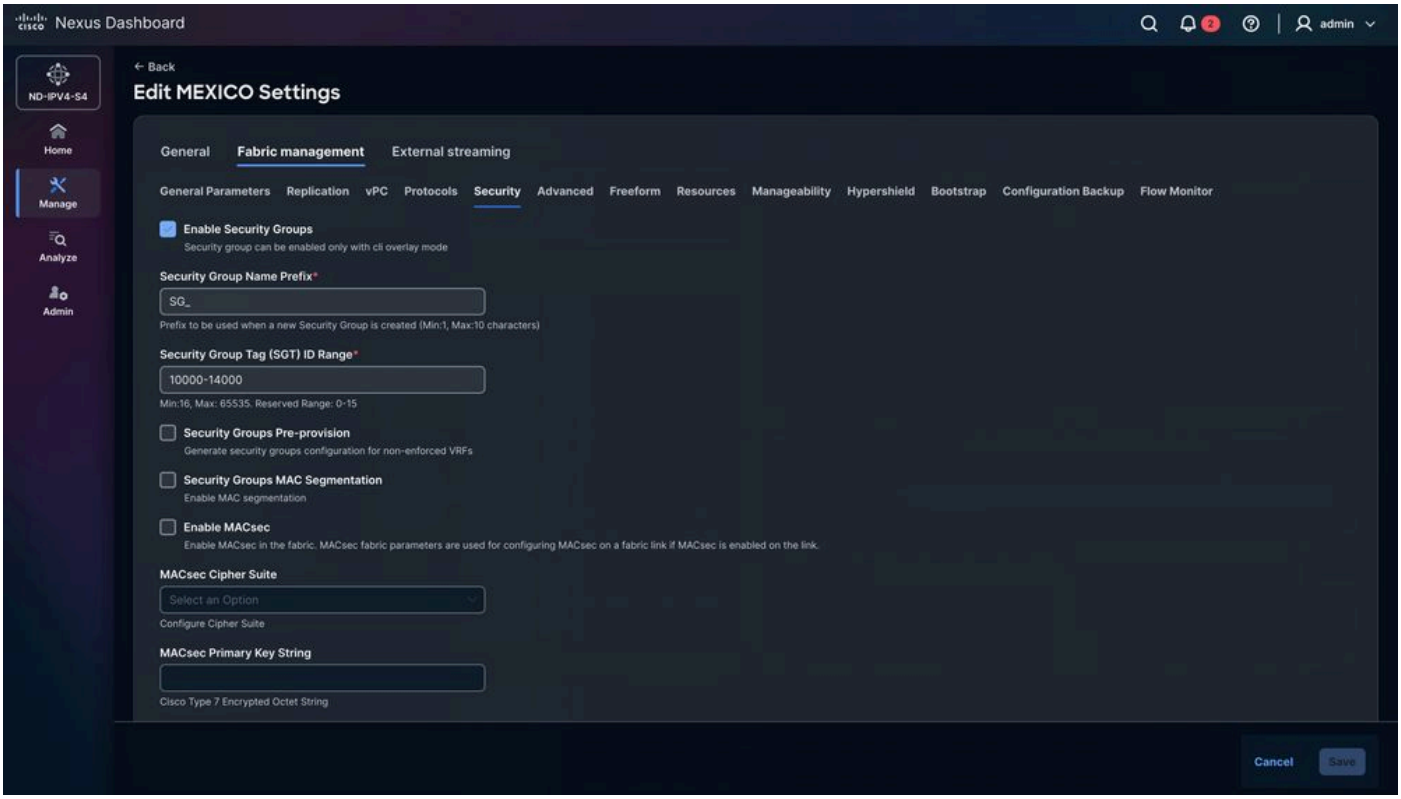
Passaggio 1. Abilitare i gruppi di sicurezza nell'infrastruttura padre

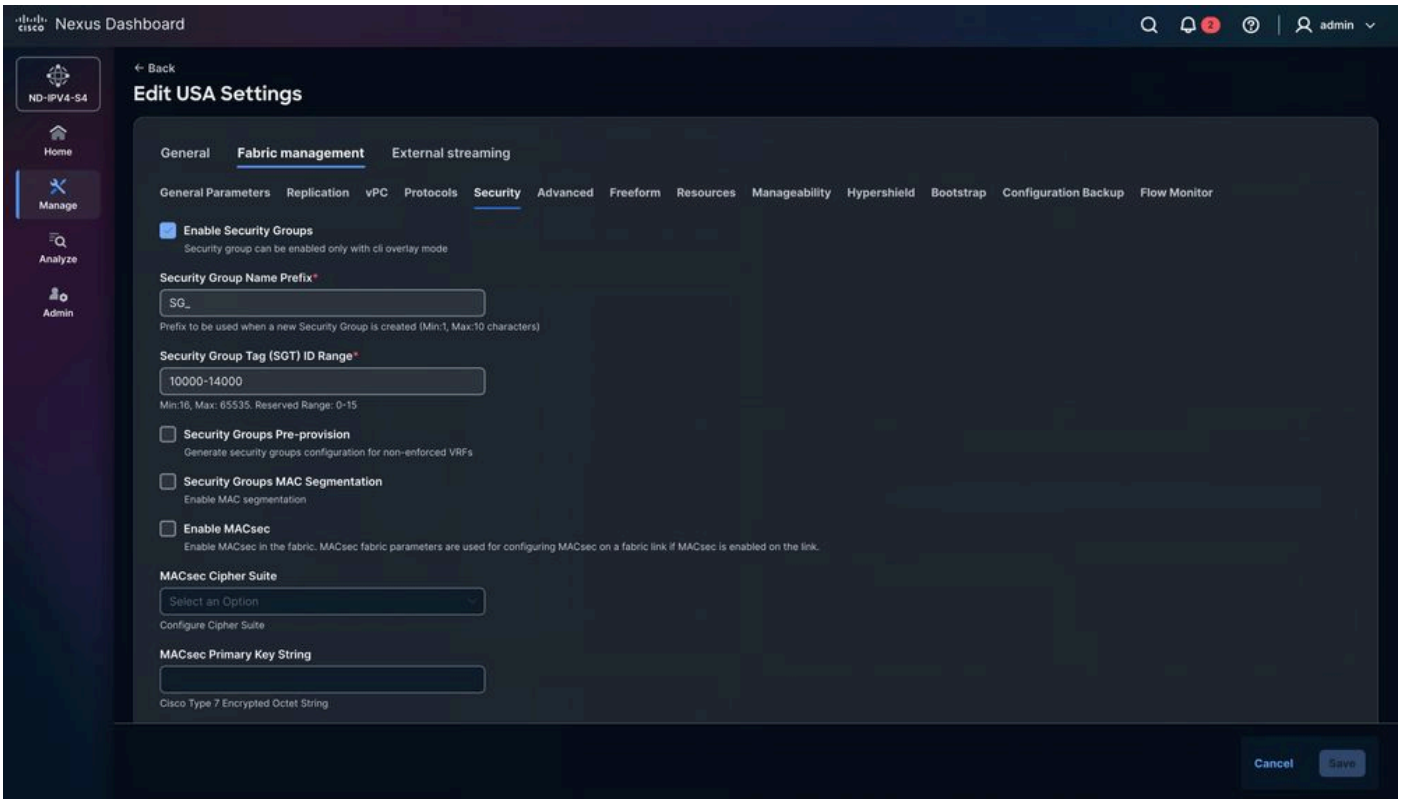
- Passare a Gestisci > Gruppi di fabric, selezionare il gruppo di fabric DAVIDM3, quindi scegliere Azioni > Modifica impostazioni gruppo di fabric. Nella sezione Sicurezza, abilitare i gruppi di sicurezza, impostare la modalità su Rigorosa e impostare i gruppi di sicurezza su Pre-provisioning.
  - Selezionare il gruppo fabric di interesse. Per questo esempio, il gruppo di fabric selezionato è denominato DAVIDM3, che è anche il nome della struttura multisito.
- Ripetere questi passaggi per ogni struttura figlio.
  - Passare a Gestisci > Infrastruttura, selezionare USA, quindi passare a Azioni > Modifica impostazioni gruppo infrastruttura. Nella sezione Sicurezza, abilitare i gruppi di sicurezza e impostare la modalità su Rigorosa.
  - Passare a Gestisci > Fabric, selezionare MEXICO, quindi passare a Azioni > Modifica impostazioni gruppo fabric. Nella sezione Sicurezza, abilitare i gruppi di sicurezza e impostare la modalità su Rigorosa.

Nota: Se l'opzione è impostata su strict, tutti i fabric figlio VXLAN devono essere gruppi di sicurezza compatibili e abilitati. Se l'opzione è impostata su loose, i gruppi di sicurezza sono facoltativi nei fabric figlio VXLAN.

Suggerimento: Per mantenere una chiara visibilità, utilizzare gli stessi intervalli di ID SGT (Security Group Tag) nell'infrastruttura padre e in tutte le strutture figlio. L'intervallo di fabric padre deve coprire gli intervalli utilizzati da tutti i fabric figlio.


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



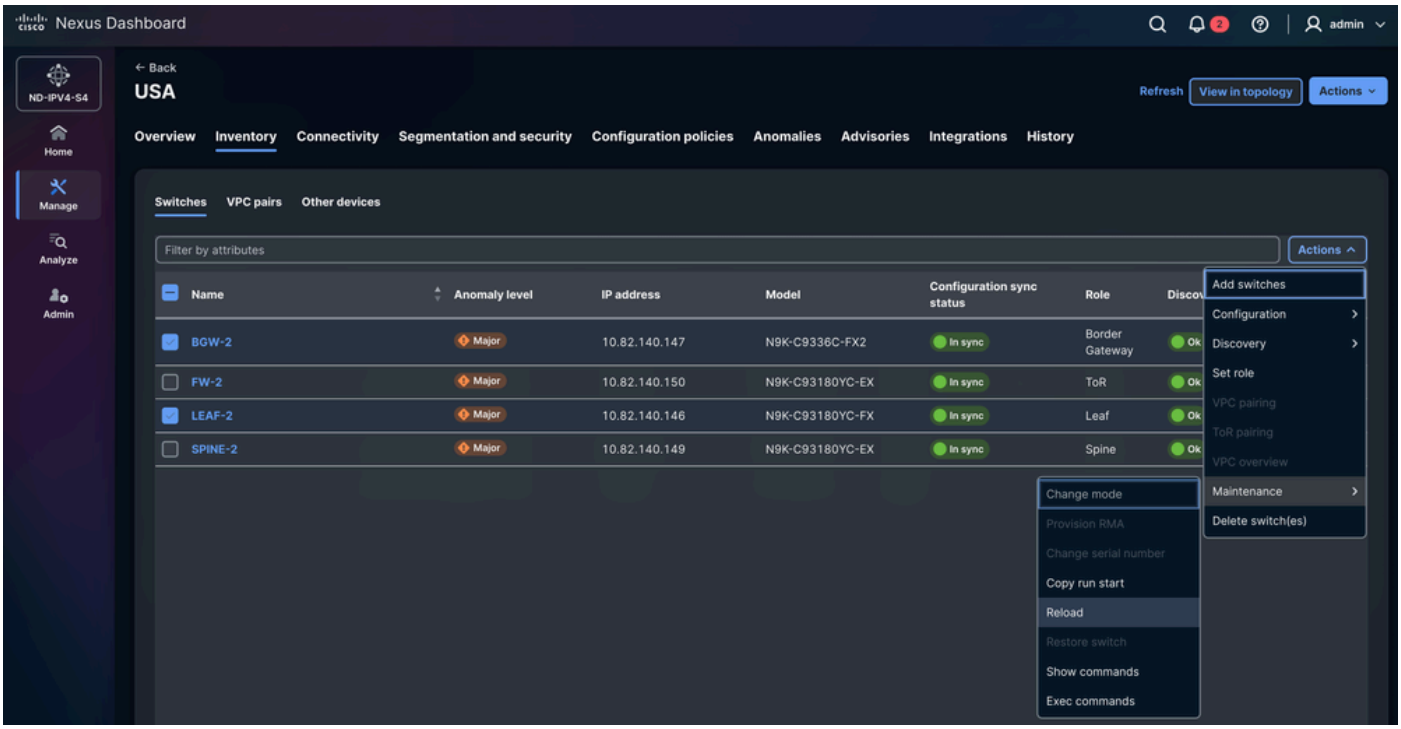
Passaggio 2. Ricalcolare la configurazione dell'infrastruttura e ricaricare gli switch per la distribuzione dell'oggetto Criteri di gruppo

L'NDFC chiede automaticamente di ricaricare un gruppo specifico di switch Nexus in base al ruolo. Nell'esempio, è necessario ricaricare LEAF-1, LEAF-2, BGW-1 e BGW-2. Questa azione deve essere eseguita manualmente dall'amministratore di rete. Il ricaricamento è necessario e non può essere ignorato perché l'oggetto Criteri di gruppo richiede l'archiviazione TCAM.

Nota: Se il dispositivo non viene ricaricato, la modifica TCAM può essere visualizzata nella configurazione corrente; tuttavia, poiché lo switch non è stato riavviato, l'impostazione non viene applicata alla memoria hardware. Di conseguenza, la feature non può funzionare come previsto.

Per ricaricare gli switch Nexus:

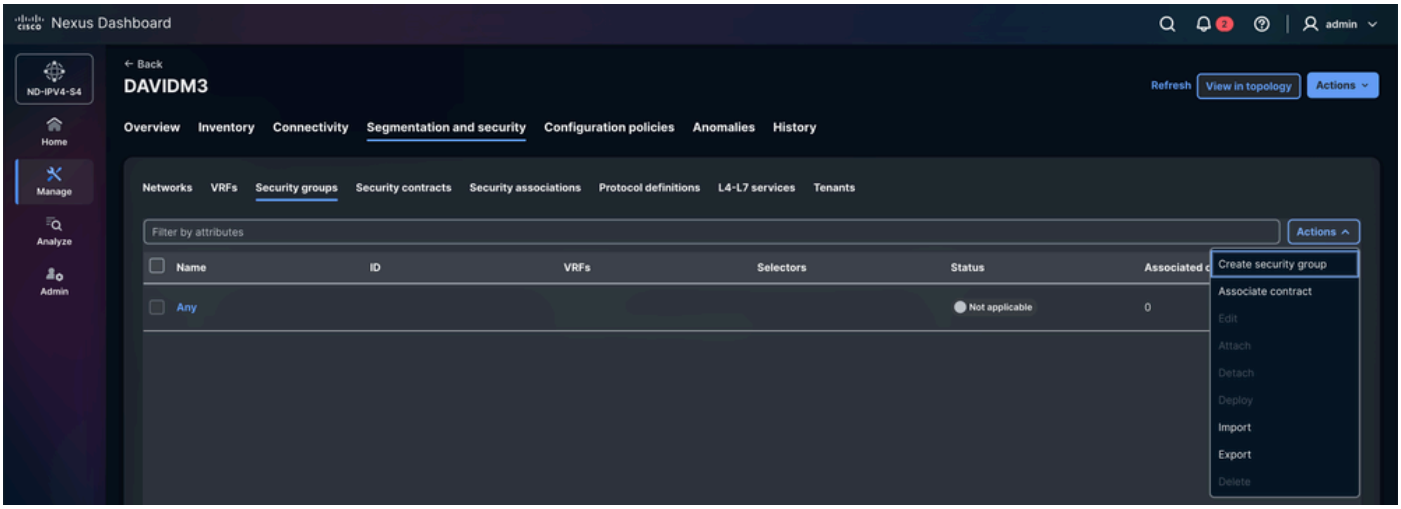
Selezionare Gestisci > Fabric > MESSICO/USA > Inventario > Switch > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Azioni > Manutenzione > Ricarica.



Passaggio 3. Creazione del gruppo di sicurezza

Definire i gruppi di sicurezza per ciascun endpoint. Ogni endpoint nelle fabric VXLAN può avere un singolo gruppo di sicurezza. Questo approccio non è scalabile in modo efficiente. Raggruppare gli endpoint a livello globale (macchine virtuali, firewall, ottimizzatori TCP e così via).

Passare a Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Segmentazione e sicurezza > Gruppi di sicurezza > Azioni > Crea gruppo di sicurezza.



Passaggio 3.1 Configurazione del nome del gruppo di sicurezza

- NDFC assegna automaticamente un nome casuale. Il nome può essere modificato. si consiglia di utilizzare un nome rappresentativo che sia facile da identificare per gli endpoint.
- In questo scenario:
    - VM -> SG_VM
    - FW -> SG_FW

Passaggio 3.2 Configurazione di VRF

- Selezionare il tenant (VRF) a cui appartengono gli endpoint.
- In questo scenario: Le VM e i firewall appartengono al tenant CISCO-TAC.

Facoltativo, creare VRF.

Per impostazione predefinita, per un VRF tenant appena creato la modalità di applicazione dei criteri è impostata su Non imposto. In questo stato, anche se i criteri di classificazione e gli SGACL tra i gruppi di sicurezza sono configurati, non viene applicata alcuna policy. Per attivare l'imposizione SGACL, il VRF deve essere configurato in modo esplicito in modalità Imposta.

Quando il VRF funziona in modalità Imposta, viene definito un comportamento predefinito del criterio:

- Nega: Tutto il traffico unicast viene eliminato a meno che non sia esplicitamente consentito da una regola di autorizzazione.
- Autorizza: Tutto il traffico unicast è consentito a meno che non sia esplicitamente bloccato da una regola di negazione.

Gli endpoint che appartengono allo stesso gruppo di sicurezza possono comunicare tra loro senza la necessità di regole SGACL. Gli SGACL definiscono i criteri di sicurezza solo tra gruppi di sicurezza diversi.

Cisco NX-OS versione 10.6(3)F introduce la funzionalità per limitare la comunicazione tra endpoint all'interno dello stesso oggetto Criteri di gruppo, nota anche come funzionalità di isolamento intra-GPO. Nelle versioni precedenti, le regole applicate agli endpoint all'interno dello stesso gruppo di sicurezza vengono ignorate e il traffico è autorizzato per impostazione predefinita.

Passaggio 3.3 Configurazione dell'ID del tag del gruppo di sicurezza

NDFC assegna automaticamente un ID tag casuale dall'intervallo predefinito nella configurazione fabric. Sebbene sia possibile selezionare manualmente un ID tag, questo deve essere compreso

nell'intervallo definito per i fabric figlio e padre.

In questo scenario:

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

Passaggio 3.4 Collegamento

Se l'opzione Attach (Connetti) non è abilitata, il gruppo di sicurezza non viene applicato al tenant CISCO-TAC.

Passaggio 3.5 Configurazione dei selettori

- I selettori determinano gli endpoint e gli indirizzi IP esterni associati a un gruppo di sicurezza specifico.

NDFC 4.2 supporta in modo nativo tre tipi di selettori:

1) Selettori IP: i selettori IP associano gli endpoint o le subnet IP a un gruppo di sicurezza basato sulle informazioni IP.

a. Connected Endpoint: identifica gli endpoint collegati direttamente al fabric, ad esempio macchine virtuali, server o host fisici connessi a switch foglia.
b. Subnet esterna: associa i prefissi IP esterni a un gruppo di sicurezza. Questo tipo viene utilizzato per le reti che esistono al di fuori della struttura VXLAN, ad esempio centri dati esterni, segmenti WAN o reti connesse a Internet. Il traffico originato da o destinato a questi prefissi viene classificato con il gruppo di sicurezza configurato.

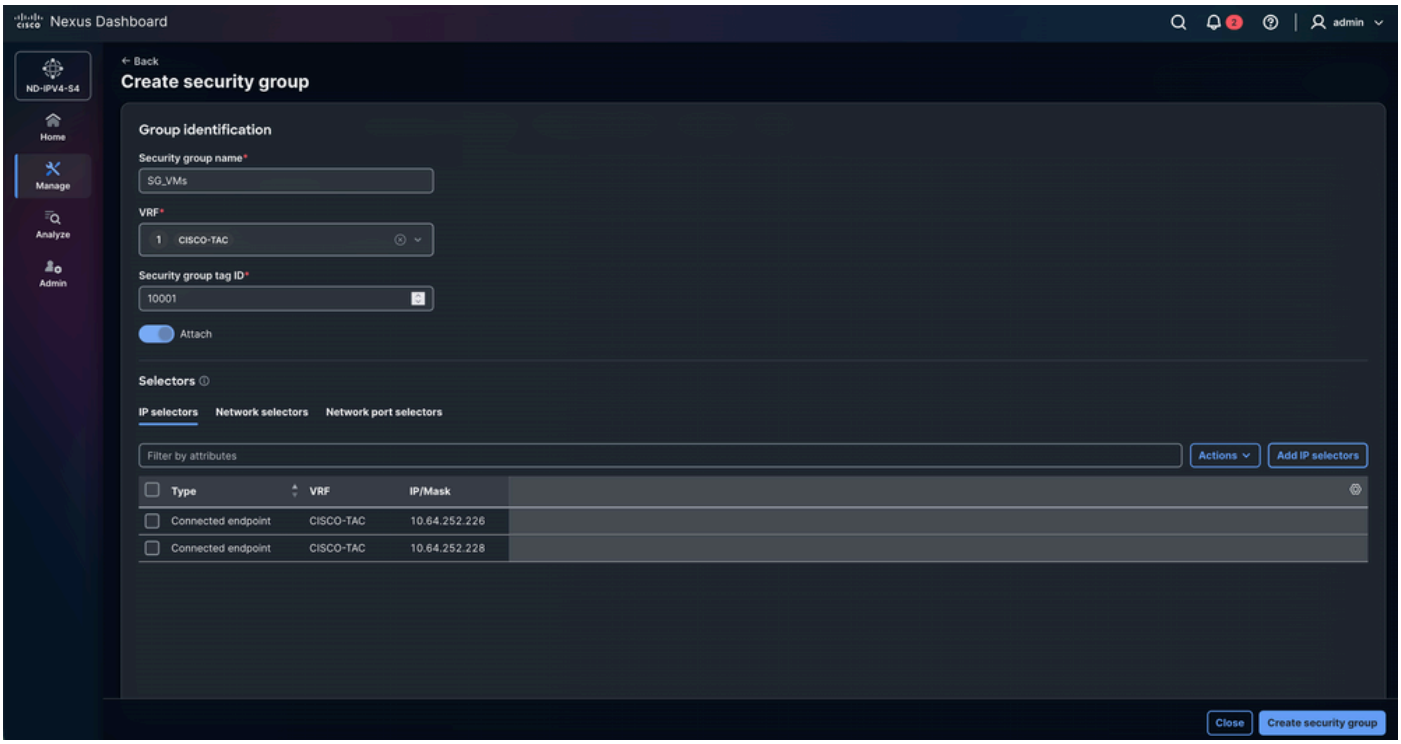
2) Selettori di rete: i selettori di rete associano un gruppo di sicurezza a un segmento di rete VXLAN specifico. La classificazione viene applicata in base all'identificatore di rete (L2VNI). Tutti gli endpoint appartenenti alla rete ereditano il gruppo di sicurezza assegnato, semplificando la distribuzione dei criteri quando più endpoint condividono lo stesso segmento.

3) Selettori porte di rete: i selettori delle porte di rete classificano il traffico in base all'interfaccia dello switch fisico attraverso cui il traffico entra nella struttura. È possibile assegnare un gruppo di sicurezza al traffico ricevuto su una porta o un'interfaccia specifica. Questo approccio viene in genere utilizzato per i dispositivi connessi tramite reti esterne, appliance di servizio o collegamenti a infrastrutture in cui la classificazione IP degli endpoint non è fattibile.

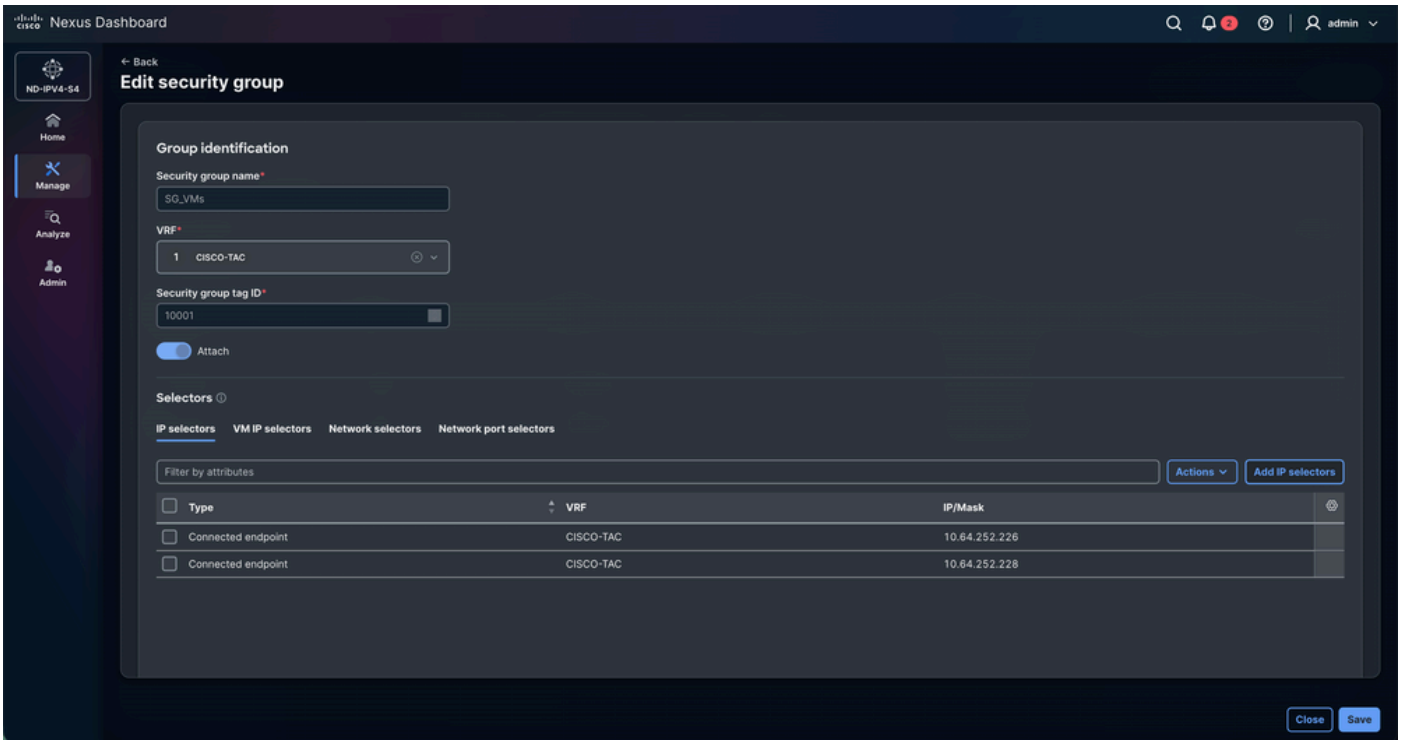
Riepilogo della configurazione del gruppo di sicurezza

Sul dispositivo bootflash o slot0:	Nome gruppo di sicurezza	VRF	ID tag gruppo di sicurezza	Selettori
VM-1	SG_VM	CISCO-TAC	10001	Selettori IP
VM-2	SG_VM	CISCO-TAC	10001	Selettori IP
FW-1	SG_FW	CISCO-TAC	10002	Selettori IP
FW-2	SG_FW	CISCO-TAC	10002	Selettori IP

Configurazione del gruppo di sicurezza per le macchine virtuali



Configurazione del gruppo di sicurezza per i firmware



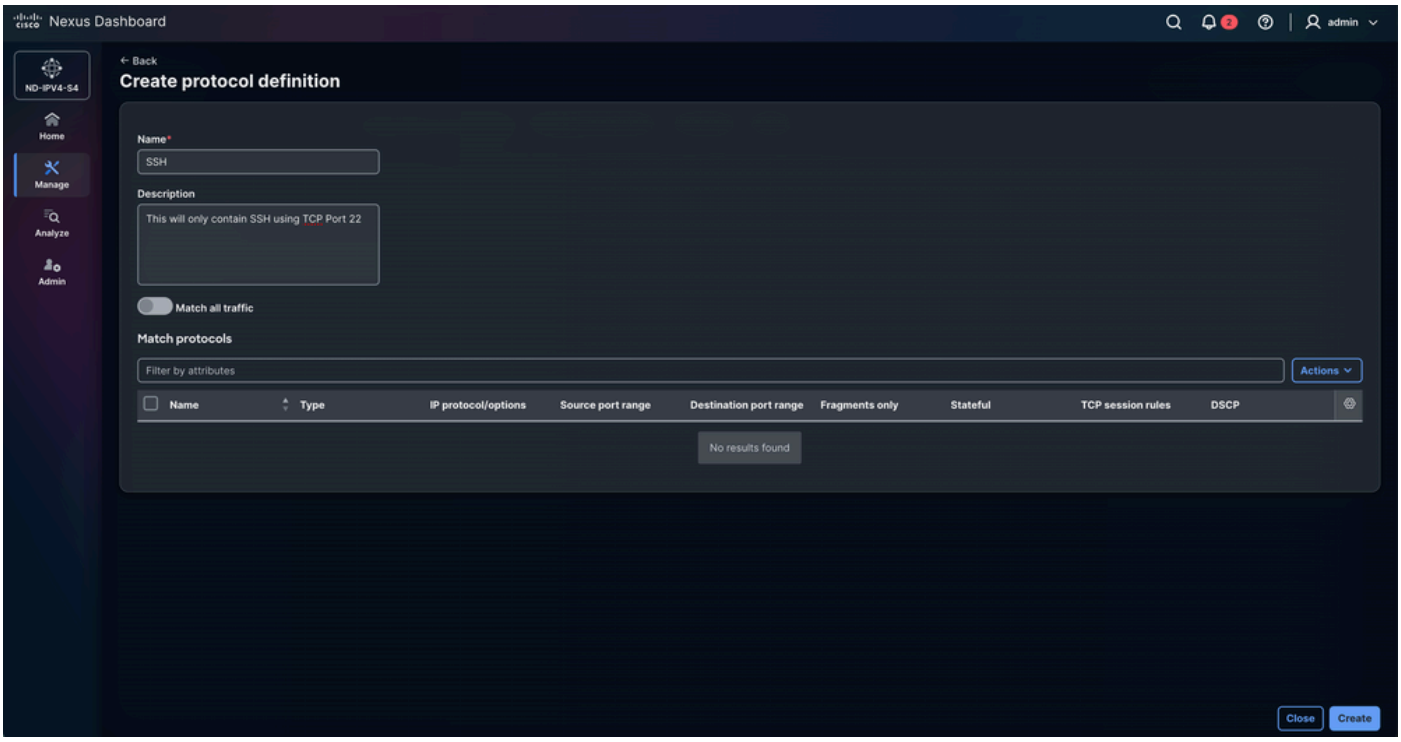
Passaggio 4. Configurazione delle definizioni di protocollo

L'opzione Crea definizione protocollo consente di definire i parametri del protocollo di rete e le caratteristiche del traffico corrispondenti a un oggetto Criteri di gruppo. Consente agli amministratori di specificare criteri quali il tipo di protocollo, i numeri di porta e altri attributi del pacchetto in modo che il criterio corrispondente possa essere applicato ai flussi di traffico desiderati.

In questo scenario, l'obiettivo è consentire solo il traffico ICMP e bloccare in modo esplicito il traffico TCP sulla porta 22 (SSH). Questa policy garantisce che i test di raggiungibilità della rete rimangano consentiti, mentre l'accesso SSH non autorizzato o indesiderato viene limitato manualmente.

Selezionare Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Segmentazione e sicurezza > Definizioni protocollo > Azioni > Crea definizione protocollo.

Inserire il nome e la descrizione.



Passare a Azioni > Crea voce di protocollo.

- Nome: SSH
- Tipo: IPv4
    - Sono inoltre disponibili IP e IPv6.
- Opzioni/protocollo IP: TCP
    - Sono supportati, tra gli altri, UDP, EIGRP e PIM.

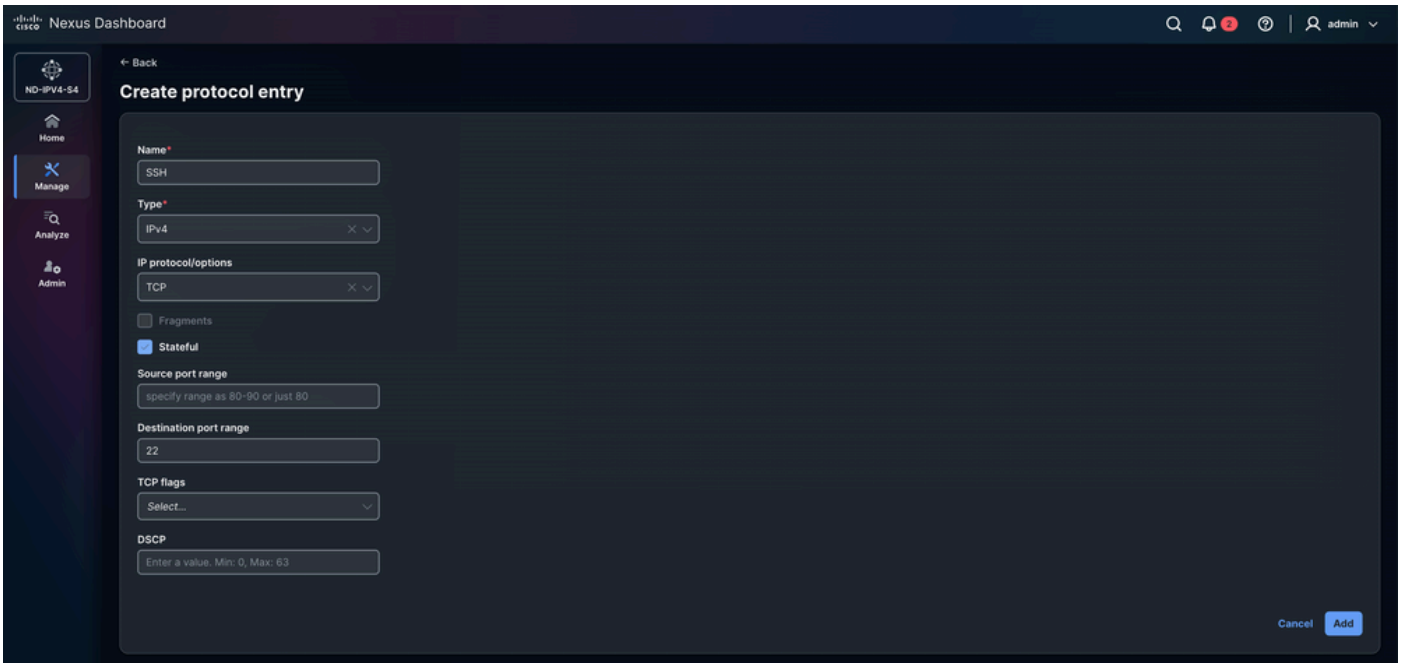
- Frammenti: Consente alla regola di corrispondere ai pacchetti IP frammentati. Questa opzione è utile perché i pacchetti di grandi dimensioni possono essere suddivisi in frammenti quando si supera l'MTU della rete. In questo modo, il criterio viene applicato anche ai frammenti selezionati.

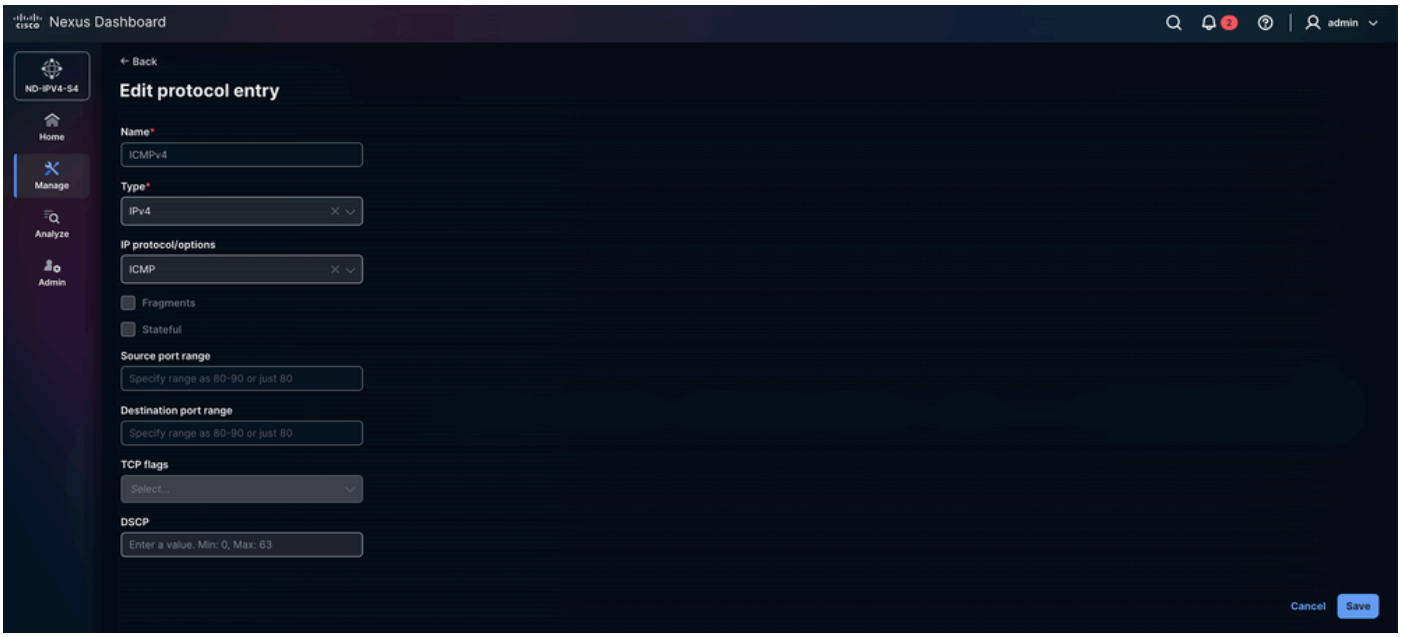
- Con stato: Un processo con conservazione dello stato consente di tenere traccia di tutte le modifiche o interazioni avvenute in passato e viene eseguito un processo corrente con un contesto di tali processi precedenti. In questo caso, il protocollo TCP tiene traccia di aree come il numero di pacchetti da trasferire, l'ordine dei pacchetti e se il destinatario ha ricevuto o meno un pacchetto. Se l'opzione Stateful è selezionata, queste informazioni vengono archiviate come stato in TCP.

- Intervallo porte di origine: Questa opzione è disponibile solo se è stato selezionato TCP o UDP nel campo Opzioni protocollo IP sopra riportato.
- Intervallo porte di destinazione: questa opzione è disponibile solo se è stato selezionato TCP o UDP nel campo Opzioni/protocollo IP.
- Flag TCP

    - Questa opzione è disponibile solo quando nel campo Opzioni/protocollo IP è selezionato TCP.

- Consente di definire i flag TCP utilizzati dal protocollo di sicurezza.
- I flag TCP fanno parte dell'intestazione TCP e vengono utilizzati per controllare la creazione, la manutenzione e la terminazione delle connessioni.
- Opzioni disponibili:
    - ACK (riconoscimento): Indica la conferma dei dati ricevuti o dei pacchetti di sincronizzazione.
    - EST (stabilito): Fa riferimento a connessioni TCP già stabilite. Quando questa opzione è abilitata, non è possibile selezionare altri flag TCP.
    - FIN (Fine): Utilizzato per chiudere normalmente una connessione TCP.
    - RST (Reimposta): Interrompe immediatamente la connessione e scarta tutti i dati ancora in transito.
    - SYN (sincronizzazione): Utilizzato durante l'avvio e la connessione TCP.





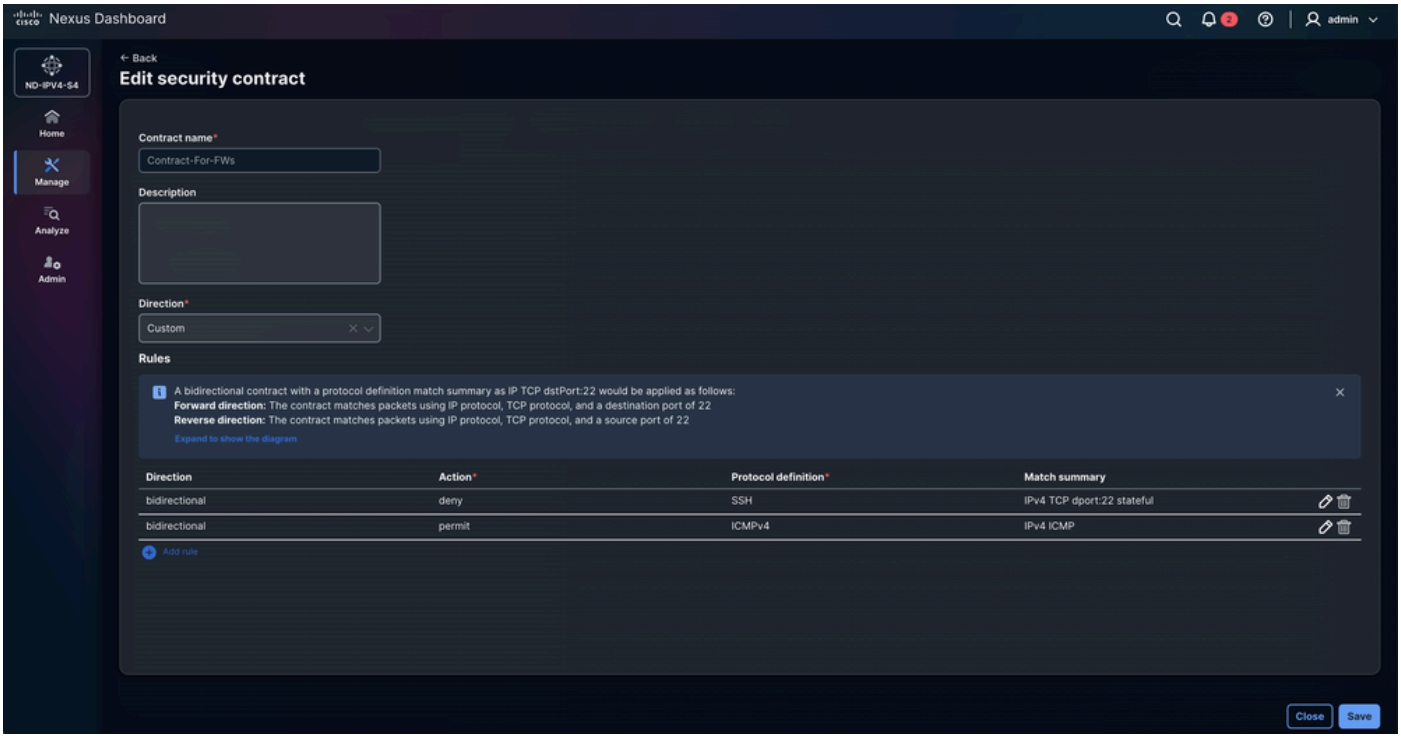
Passaggio 5. Configurare i contratti di sicurezza

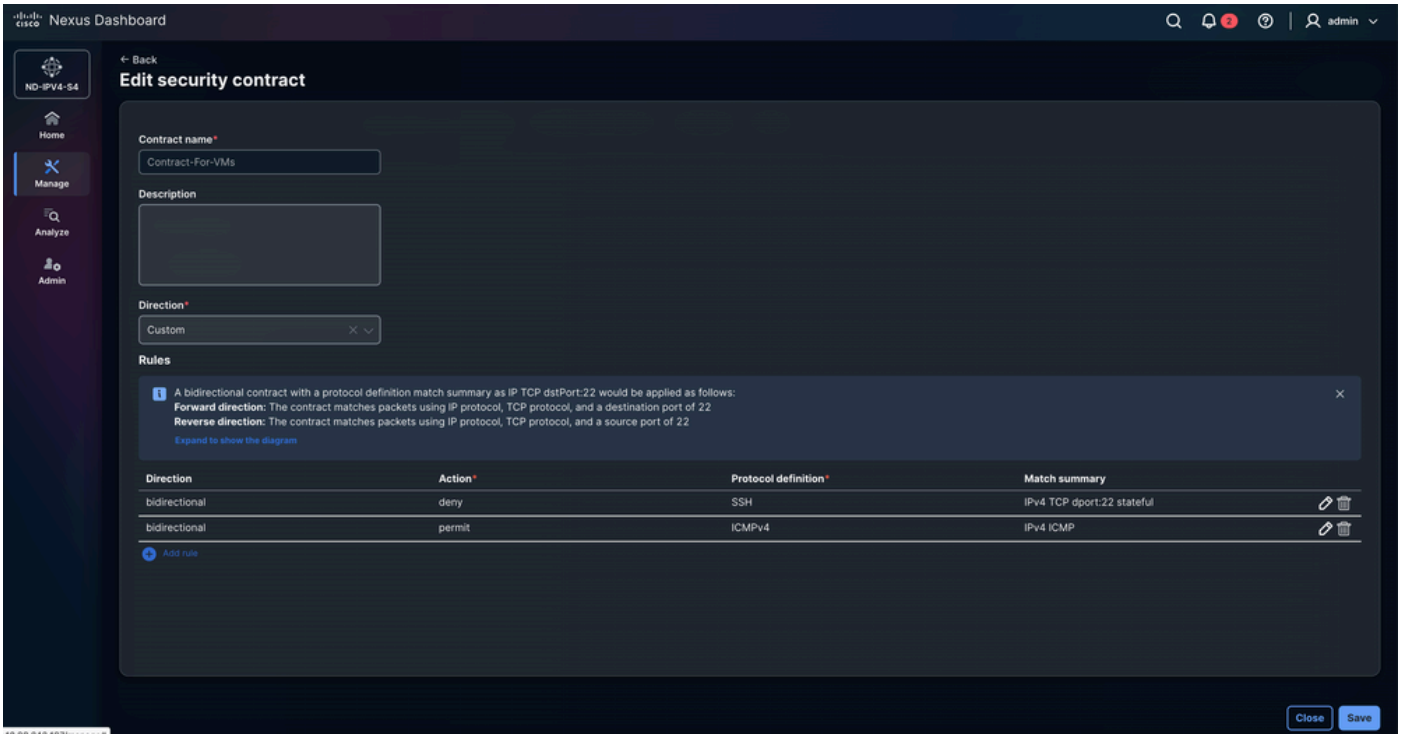
Il contratto definisce le regole di comunicazione tra i gruppi di endpoint specificando il traffico consentito o negato in base alle definizioni dei criteri associati. Funge da meccanismo di applicazione che applica le regole, i filtri e le azioni del protocollo configurati, garantendo che il traffico tra i gruppi di origine e di destinazione sia conforme ai criteri di sicurezza e segmentazione previsti.

Passare a Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Segmentazione e sicurezza > Contratti di sicurezza > Azioni > Crea contratto di sicurezza.

- Selezionare Aggiungi regola e configurare Direzione, Azione e Definizione protocollo.
    - Bidirezionale:
        - Il contratto bidirezionale si applica come segue con un riepilogo delle corrispondenze di definizione del protocollo come porta TCP IP 22.
            - Direzione in avanti: Il contratto determina la corrispondenza dei pacchetti usando il protocollo IP, il protocollo TCP e una porta di destinazione di 22
            - Inverti direzione: Il contratto stabilisce la corrispondenza dei pacchetti usando il protocollo IP, il protocollo TCP e una porta di origine di 22.
            - Ciò si applica indipendentemente dall'origine o dalla destinazione.
    - Unidirezionale:
        - Unidirezionale in un contratto di sicurezza dell'oggetto Criteri di gruppo significa

che i criteri vengono applicati solo in una direzione del flusso di traffico, consentendo o negando la comunicazione dal gruppo di sicurezza di origine al gruppo di sicurezza di destinazione senza applicare automaticamente la stessa regola nella direzione inversa.

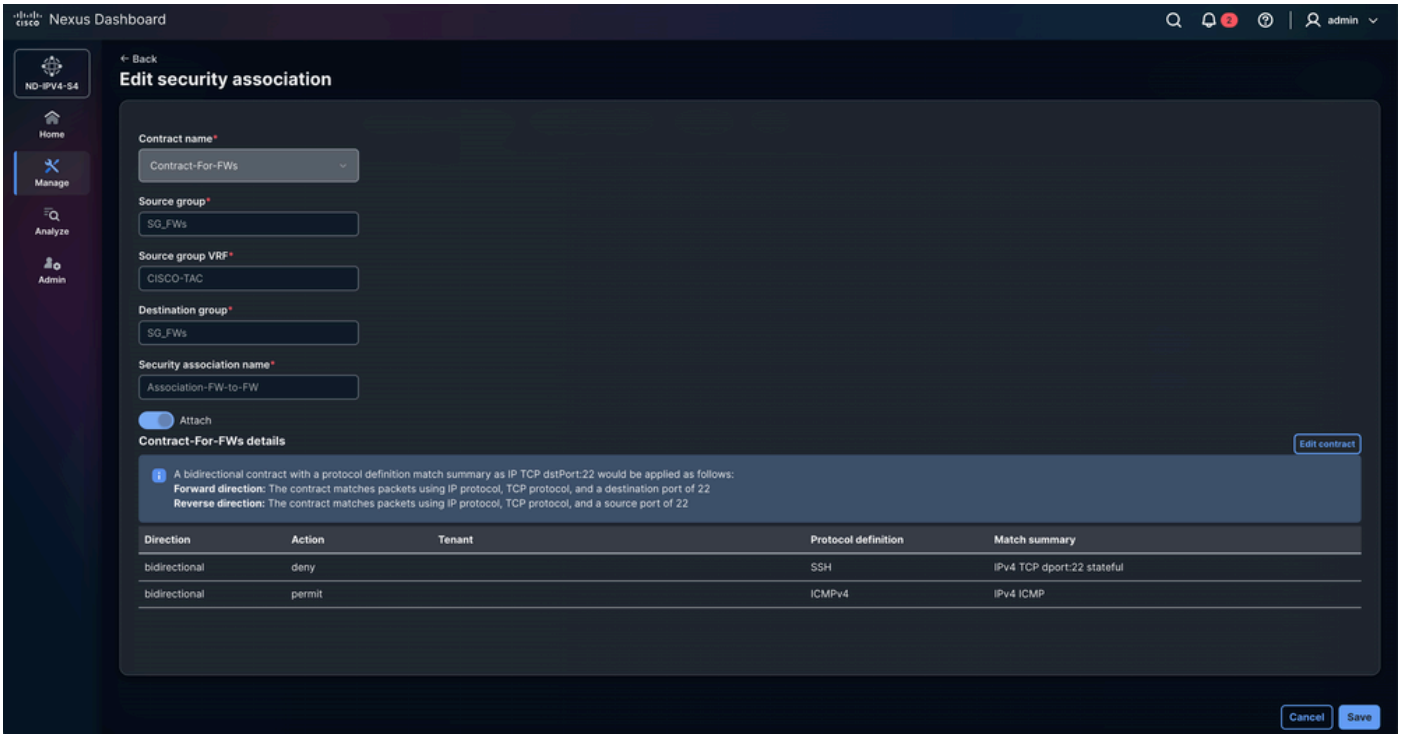


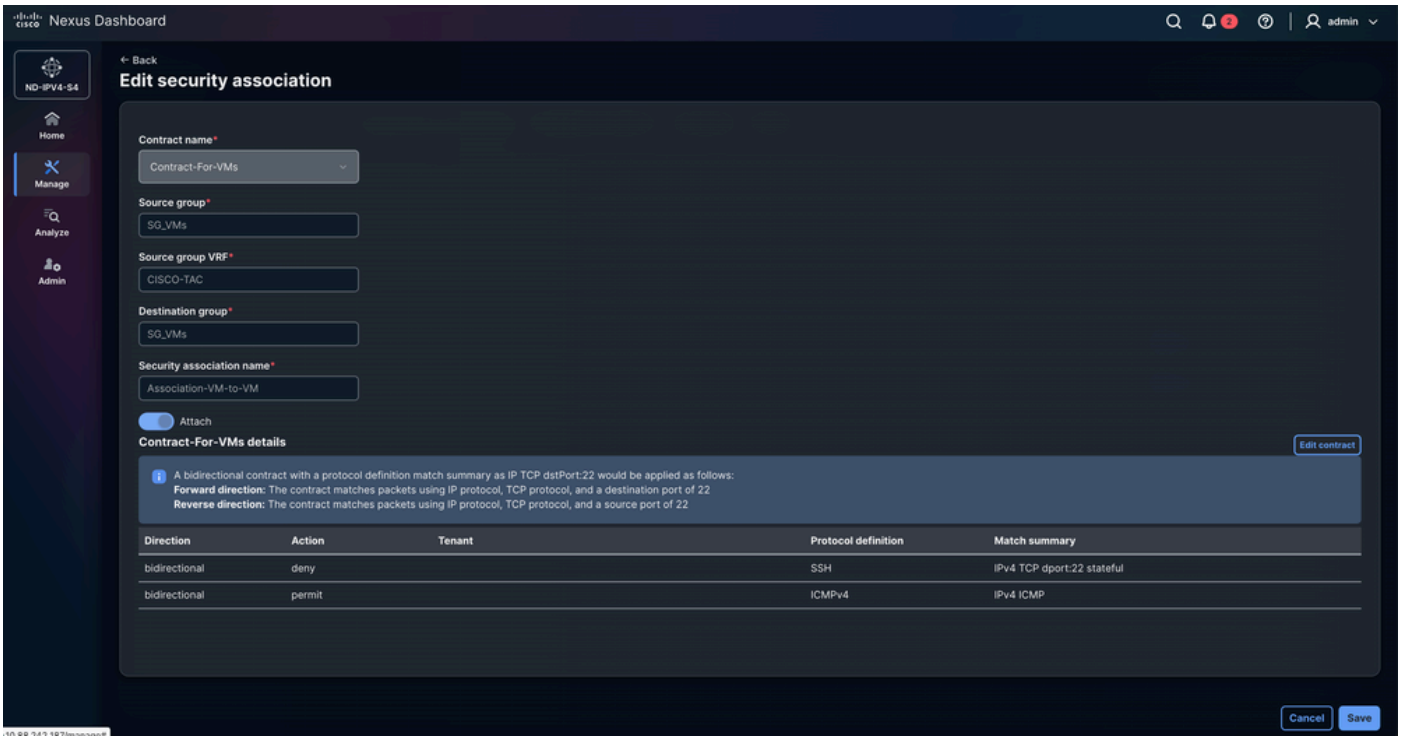


Passaggio 6. Configurare le associazioni di sicurezza

Passare a Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Segmentazione e sicurezza > Associazioni di sicurezza > Azioni > Crea associazione di sicurezza.

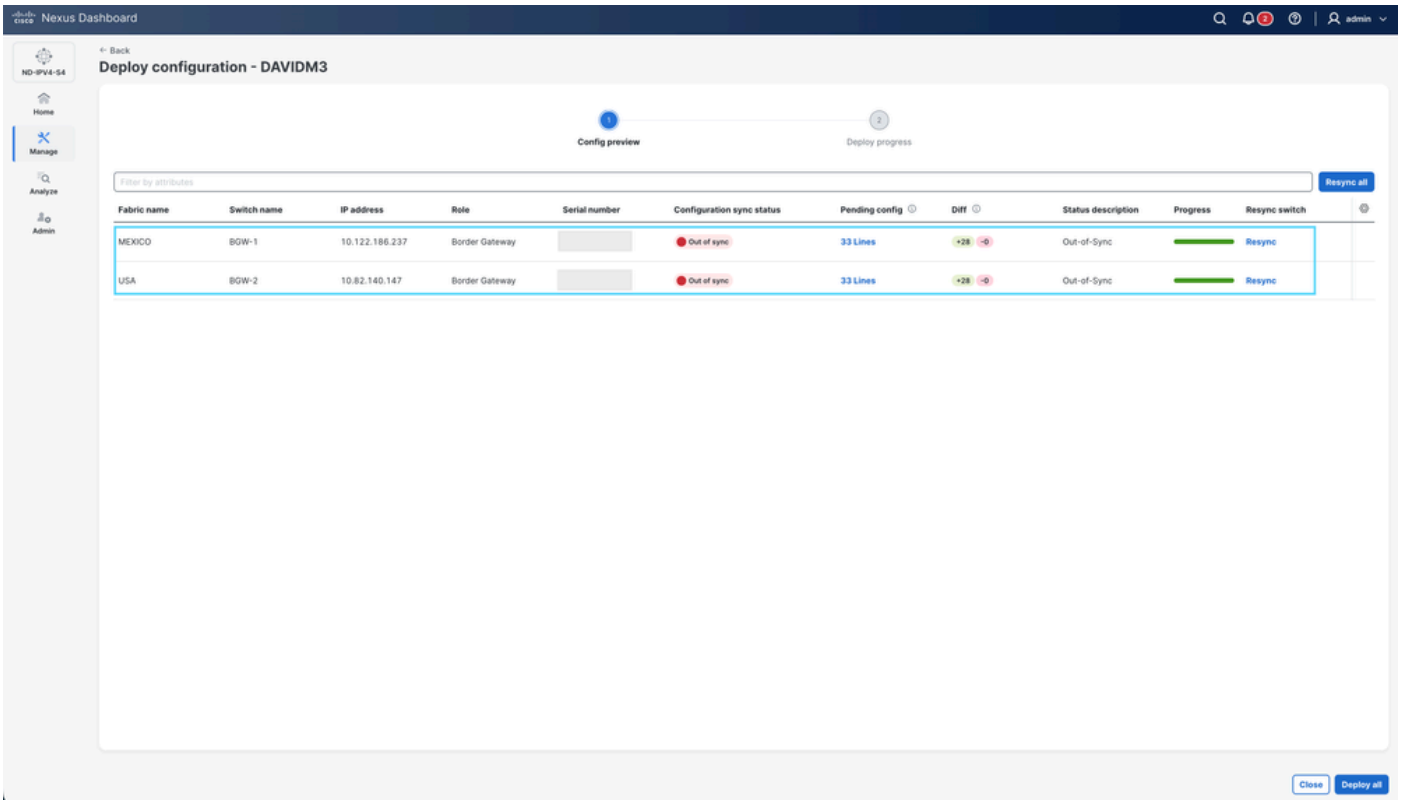
In Configura associazioni di sicurezza il modello di criteri viene definito collegando gruppi di sicurezza, definizioni di protocollo e contratti di sicurezza. I gruppi di sicurezza classificano gli endpoint, le definizioni di protocollo specificano i tipi di traffico (ad esempio protocolli o porte) e i contratti di sicurezza definiscono il criterio applicato tra i gruppi di sicurezza di origine e di destinazione utilizzando tali regole di protocollo. Le associazioni di sicurezza rappresentano la relazione che associa questi elementi in modo che l'infrastruttura possa applicare i criteri di sicurezza definiti.

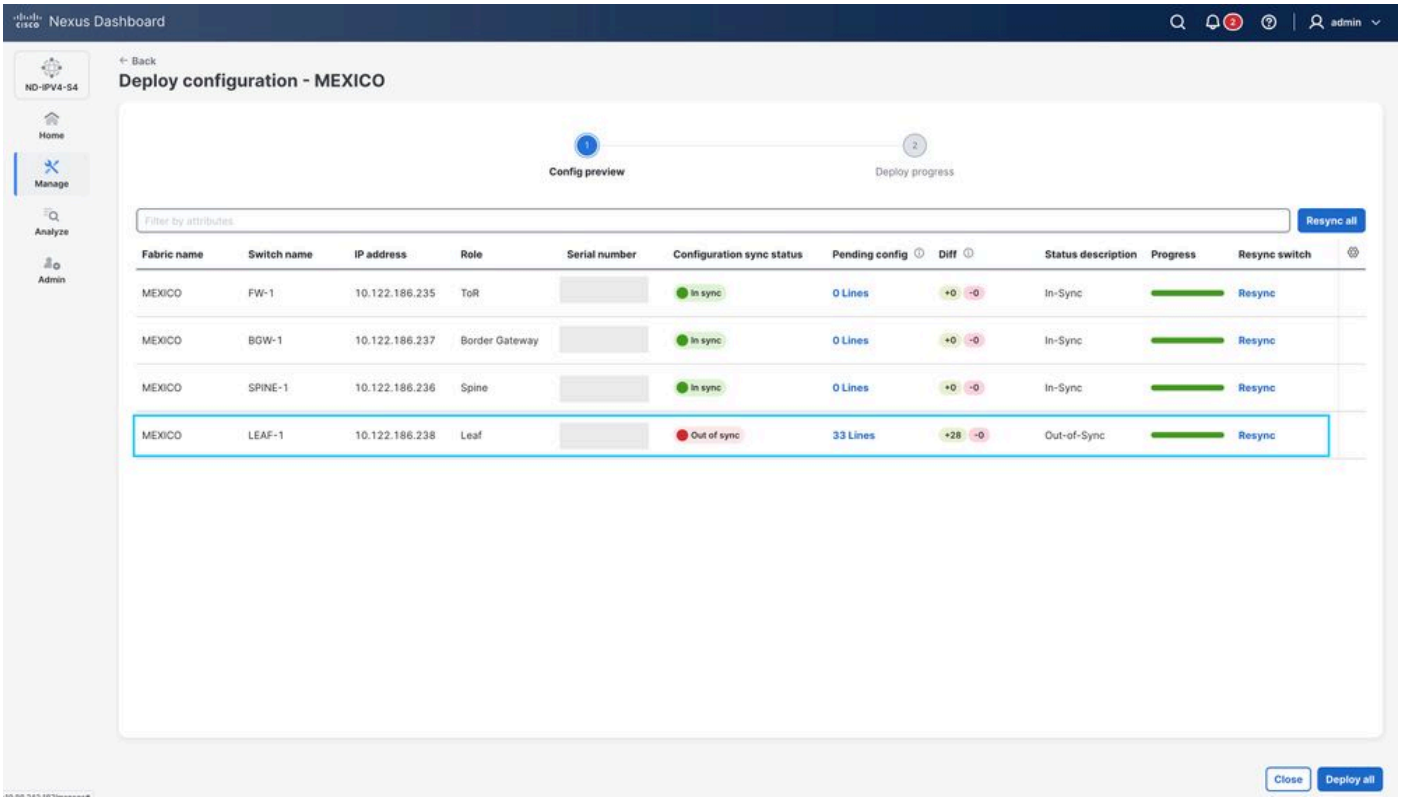


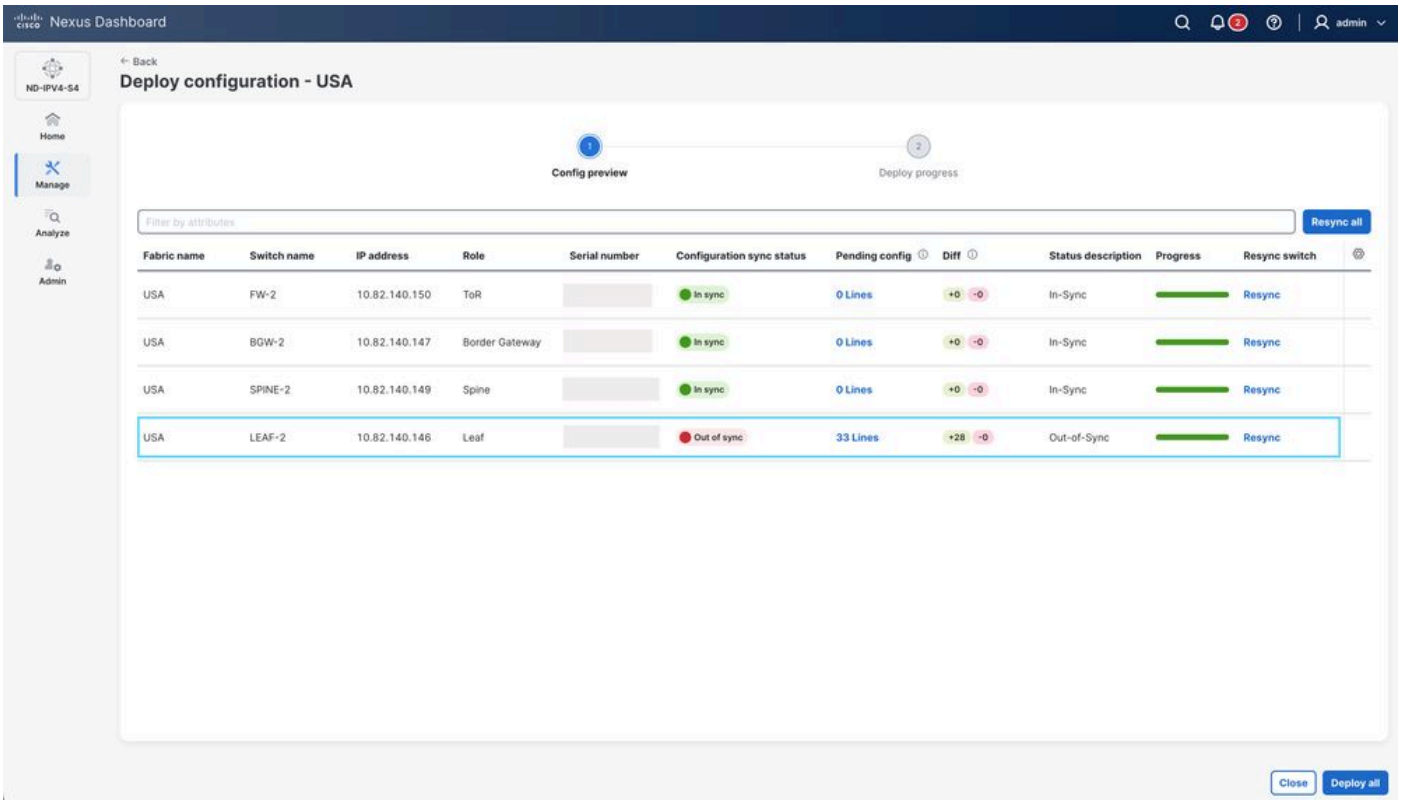


Passaggio 7. Convalida della configurazione dell'oggetto Criteri di gruppo

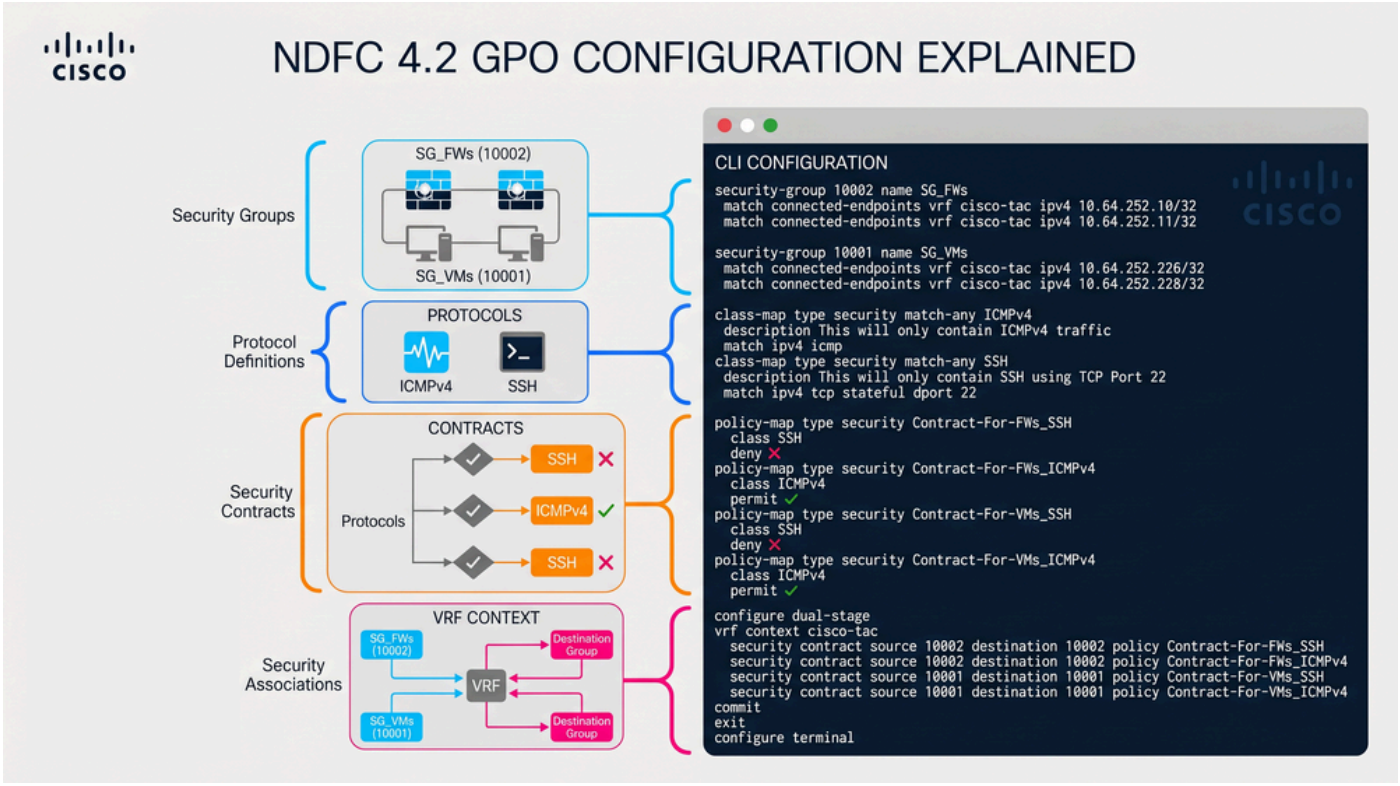
- Passare a Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Azioni > Ricalcola e distribuisci.
  - Push della configurazione dell'oggetto Criteri di gruppo nei gateway del bordo dallo switch dell'infrastruttura padre. Fare clic sul numero di righe di configurazione in sospeso per esaminare e convalidare la configurazione che può essere distribuita ai dispositivi. Questo processo deve essere ripetuto per ogni struttura secondaria.
  - Passare a Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Inventario > Tessuti membri > MESSICO > Azioni > Ricalcola e distribuisci.
  - Passare a Gestisci > Fabric > Gruppi fabric > DAVIDM3 > Inventario > Tessuti membri > USA > Azioni > Ricalcola e distribuisci.


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



- L'immagine mostra la configurazione dell'oggetto Criteri di gruppo per BGW-1, BGW-2, LEAF-1 e LEAF-2. La configurazione è identica su tutti gli switch. NDFC 4.2 non applica la configurazione nell'ordine esatto mostrato. Questa sezione illustra la sequenza logica dei comandi CLI.



Risoluzione dei problemi di operabilità dell'oggetto Criteri di gruppo VXLAN

Passaggio 1. Verificare lo stato della funzionalità del gruppo di sicurezza

Verificare se la funzionalità del gruppo di sicurezza è abilitata sullo switch. L'oggetto Criteri di gruppo VXLAN dipende da questa funzionalità perché attiva l'infrastruttura SGT (Security Group Tag) necessaria per la classificazione degli endpoint, l'applicazione dei contratti e la programmazione dell'hardware SGACL.

<#root>

```
BGW-1#

show feature | i i security-group


security-group 1 enabled
```

Passaggio 2. Verificare la modalità di instradamento del sistema

Convalidare la modalità di routing del sistema configurata e operativa sullo switch. L'oggetto Criteri di gruppo VXLAN richiede la modalità di routing del supporto dei gruppi di sicurezza perché l'imposizione SGACL utilizza risorse di inoltro hardware dedicate all'interno della pipeline ASIC.

<#root>

```
BGW-1#

show system routing mode


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

Passaggio 3. Verificare la funzionalità NVE Peer Establishment e GPO di VXLAN

- Convalida della creazione di peer VXLAN NVE tra dispositivi fabric locali e peer remoti multisito. Poiché le informazioni sugli oggetti Criteri di gruppo VXLAN si propagano attraverso il control-plane VXLAN EVPN, per l'apprendimento SGT (Security Group Tag) e la

sincronizzazione dei contratti nell'infrastruttura sono necessarie adiacenze NVE stabili.
- Il campo Funzionalità Criteri di gruppo è uno degli indicatori più importanti di questo comando perché conferma se il VTEP remoto supporta le estensioni Criteri di gruppo VXLAN necessarie per la propagazione SGT e l'applicazione del contratto SGACL nel dominio VXLAN VPN multisito.

<#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

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

Passaggio 4. Verifica dell'apprendimento del gruppo di sicurezza e della classificazione degli endpoint

Verificare che gli endpoint siano classificati correttamente nei gruppi di sicurezza (SGT). L'imposizione dell'oggetto Criteri di gruppo VXLAN dipende da mapping accurati da endpoint 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
```

Passaggio 5. Verificare i contratti di sicurezza e l'applicazione delle policy

Verificare che i contratti dell'oggetto Criteri di gruppo VXLAN siano installati e operativi correttamente. I contratti definiscono le regole di comunicazione applicate tra i gruppi di sicurezza e rappresentano il meccanismo di policy principale utilizzato dall'oggetto Criteri di gruppo VXLAN per la microsegmentazione.

<#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
```

Passaggio 6. Verificare lo stato di applicazione della sicurezza VRF

Verificare lo stato di imposizione dell'oggetto Criteri di gruppo VXLAN per tutte le VRF configurate sullo switch. Questo comando conferma se i criteri SGACL e i contratti del gruppo di sicurezza sono applicati attivamente nel VRF del tenant.

L'output conferma che il VRF cisco-tac sta partecipando attivamente all'imposizione dell'oggetto Criteri di gruppo VXLAN con la modalità impostata su enforced (imposto). Il tag di imposizione 13648 identifica il contesto interno dei criteri SGACL programmato nell'hardware per questo VRF. Il log di negazione dell'azione predefinito indica che qualsiasi traffico non esplicitamente autorizzato tramite un contratto del gruppo di sicurezza viene rifiutato e registrato, implementando un criterio di micro-segmentazione di negazione predefinito. Al contrario, i VRF predefiniti, gestione-bilanciamento-carico-uscita-risoluzione e gestione operano in modalità non applicata, ovvero le policy VXLAN GPO non vengono applicate all'interno di tali VRF e il traffico è autorizzato per impostazione predefinita.

Il campo Stats consente di tenere traccia del traffico corrispondente al criterio di protezione VRF. Il valore 0 in VRF cisco-tac indica che non è stato generato alcun traffico non corrispondente al comportamento di negazione predefinito al momento dell'esecuzione del comando, mentre il valore del contatore 4364 in VRF predefinito indica un'attività di traffico in un VRF che funziona senza l'applicazione dell'oggetto Criteri di gruppo VXLAN.

```
<#root>

BGW-1#
```

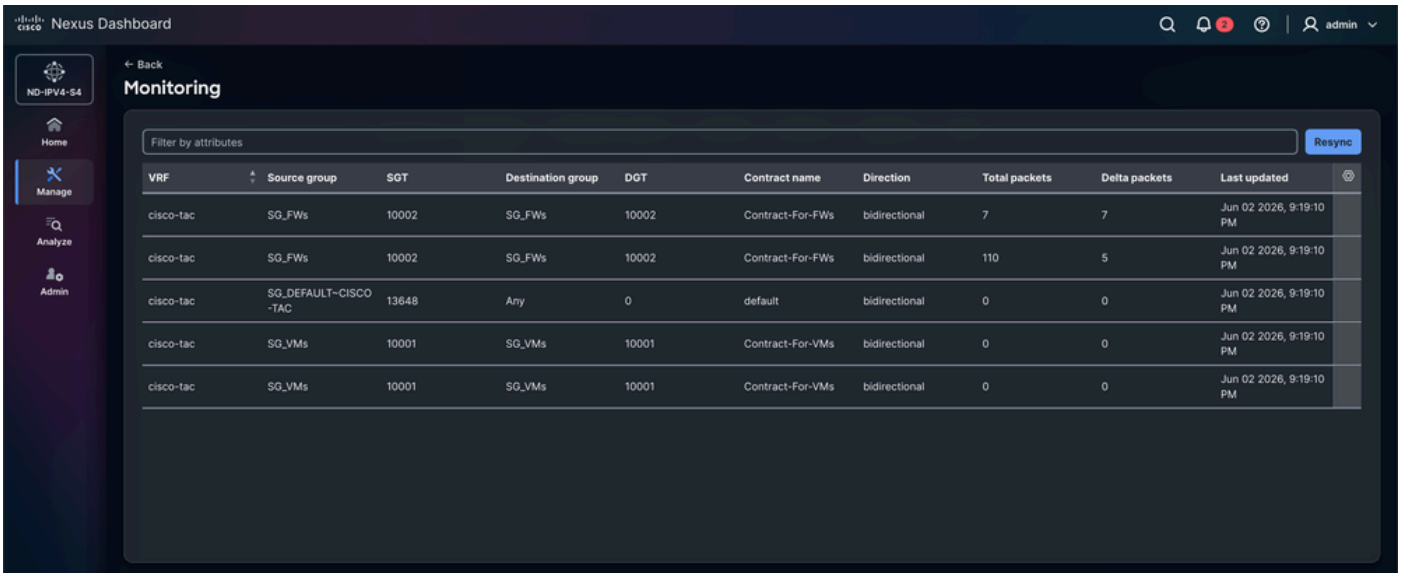
```
show vrf all security
```

```
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
```

Passaggio 7. Verificare lo stato di applicazione della sicurezza VRF

- Convalidare le statistiche di corrispondenza del traffico per i contratti dell'oggetto Criteri di gruppo VXLAN dalla GUI NDFC. Questa verifica conferma se il traffico corrisponde attivamente ai contratti del gruppo di sicurezza configurati e se l'applicazione SGACL è operativa nell'infrastruttura VXLAN EVPN multisito.
- Nell'interfaccia utente di NDFC, selezionare Manage > Fabrics > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoring (Gestione fabric > Gruppi di fabric > USA / MESSICO > Segmentazione e sicurezza > Associazioni di sicurezza > Monitoraggio).
    - In questa sezione viene fornita la visibilità dei flussi di comunicazione del gruppo di sicurezza, delle statistiche relative agli accessi ai contratti, delle azioni di autorizzazione e rifiuto e dell'attività operativa sui contratti tra i gruppi di endpoint.
    - Le statistiche di monitoraggio vengono visualizzate singolarmente all'interno di ciascuna tabella.
    - Le statistiche di monitoraggio dell'NDFC forniscono un livello di convalida operativo che integra la risoluzione dei problemi basata sulla CLI confermando l'applicazione delle policy in tempo reale e il comportamento di corrispondenza del traffico nell'infrastruttura.

Nota: Al primo tentativo di rivedere le statistiche sul traffico nella NDFC 4.2, la sezione di monitoraggio può inizialmente apparire vuota. In questo caso, premere il pulsante Resync per avviare la sincronizzazione delle statistiche dei contratti dal fabric VXLAN. Mentre il processo di sincronizzazione è in esecuzione, l'interfaccia grafica visualizza il messaggio Resync status: In corso. Al termine della sincronizzazione, premere il pulsante Ok per aggiornare la visualizzazione di monitoraggio. Al termine della risincronizzazione, le statistiche del traffico associate a ciascun contratto del gruppo di sicurezza diventano visibili nella sezione di monitoraggio. Per convalidare il comportamento di corrispondenza del traffico in tempo reale, generare il traffico tra gli endpoint, quindi premere di nuovo il pulsante Resync per aggiornare le statistiche dei contratti visualizzate in NDFC.



- Nello scenario precedente, il traffico ICMPv4 tra gli endpoint è stato autorizzato. Tuttavia, se viene stabilita una sessione SSH, la connessione scade perché il contratto dell'oggetto Criteri di gruppo VXLAN nega esplicitamente il traffico TCP destinato alla porta 2.

<#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
```

Informazioni correlate

[Guida alla configurazione di Cisco Nexus serie 9000 NX-OS VXLAN, versione 10.6(x)]

Protezione dei centri dati con la microsegmentazione tramite l'oggetto Criteri di gruppo VXLAN

Implementazione della microsegmentazione nei fabric VXLAN EVPN Cisco NX-OS con opzione Criteri di gruppo VXLAN

Automazione della microsegmentazione e distribuzione dei servizi di layer 4-7 nei fabric VPN VXLAN tramite l'opzione Criteri di gruppo e il dashboard Nexus

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).