NDFC 4.2を使用したNexusマルチサイトファブリックでのGPOの設定

内容

はじめに

このドキュメントでは、NX-OSおよびNDFC 4.2を実行しているNexus Cloud Scaleスイッチ上のVXLANマルチサイトファブリックにおけるGPOの設定と検証について説明します。

前提条件

要件

次の領域に関する知識があることが推奨されます。

- Virtual Extensible Local Area Network(VXLAN)、イーサネットVirtual Private Network(EVPN)、マルチサイトファブリックテクノロジー
- Cisco Nexus Cloud ScaleスイッチとNeXusオペレーティングシステム(NX-OS)の動作
- Nexusファブリックネットワークコントローラ(NDFC)4.2の管理および導入ワークフロー
- ネットワークのセグメント化とセキュリティポリシーの概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

VXLAN EVPNファブリックのGPO機能について

グループポリシーオプション(GPO)は、IPアドレス、VLAN、またはサブネットだけに依存するのではなく、論理アイデンティティに基づいてエンドポイント間の通信を制御するように設計された、ポリシーベースのセグメンテーションメカニズムです。GPOの主な目的は、セキュリティポリシーの適用を簡素化し、アプリケーション、サーバ、またはワークロード間のスケーラブルなマイクロセグメンテーションを提供することです。

たとえば、すべてのゲストが特定のカテゴリまたはアクセスレベルに属し、特定のエリアには特定のゲストのみがアクセスでき、アクセス権限は部屋番号ではなくゲストのロールに依存するホテルを考えてみましょう。GPOの動作もほぼ同じです。エンドポイントを純粋にIPアドレスとして扱う代わりに、GPOはエンドポイントをセキュリティグループ(SG)に分類します。 次に、これらのグループ間にポリシーを適用して、許可または拒否する通信を決定します。

例：

- Webサーバは、1つのセキュリティグループに属することができます。
- アプリケーションサーバは、別のセキュリティグループに属することができます。
- データベースサーバは、制限付きセキュリティグループに属することができます。

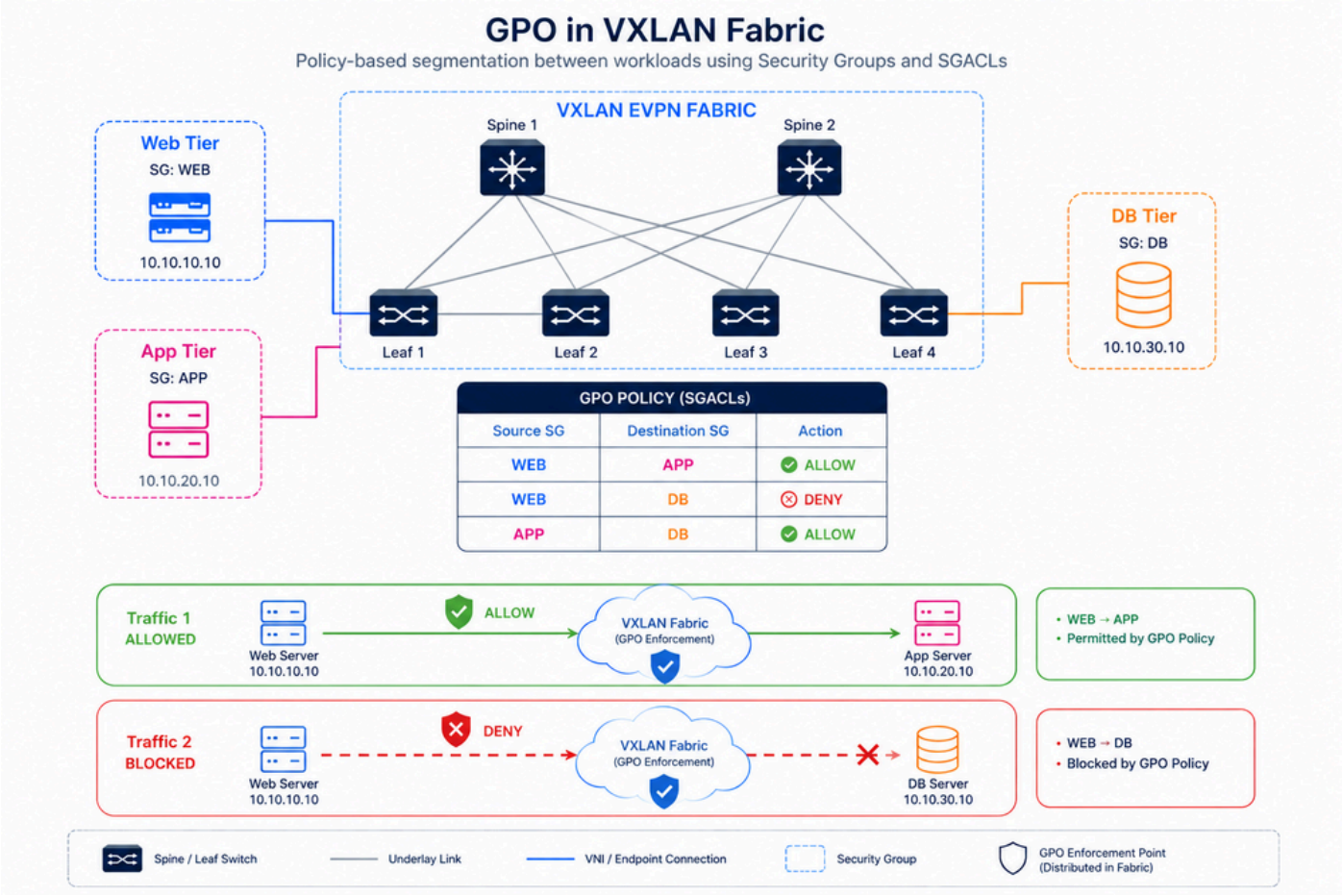
ポリシーでは次の項目を定義できます。

- Webサーバはアプリケーションサーバと通信できます。
- アプリケーションサーバはデータベースサーバと通信できます。
- Webサーバはデータベースサーバと直接通信できません。

このアプローチでは、管理者が複数のデバイスとVLANにわたって大量のACLを維持する必要がなくなるため、運用が簡素化されます。

もう1つの大きな利点は、拡張性です。大規模な環境では、ワークロードが頻繁に移動、動的な拡張、またはIPアドレスの変更を行います。 GPOを使用すると、エンドポイントの場所が変更されてもセキュリティポリシーの一貫性を維持できます。 VXLAN EVPNファブリック内では、GPOはセキュリティグループ情報をファブリック全体に分散し、エンドポイント間でセキュリティグループACL(SGACL)を適用することで、この概念を拡張します。ワークロード間の水平方向のトラフィックが最大の攻撃対象領域となることが多いため、これは現代のデータセンターでは特に重要です。GPOは、データセンターファブリック内の不要な通信パスを制限することにより、セキュリティポスチャを向上させます。

GPOアーキテクチャ、マイクロセグメンテーションの概念、およびVXLANポリシーの適用に関する技術的な詳細については、『Securing Data Centers with Microsegmentation using VXLAN GPO』に記載されているシスコホワイトペーパーを参照してください。



VxLANファブリック内のGPO

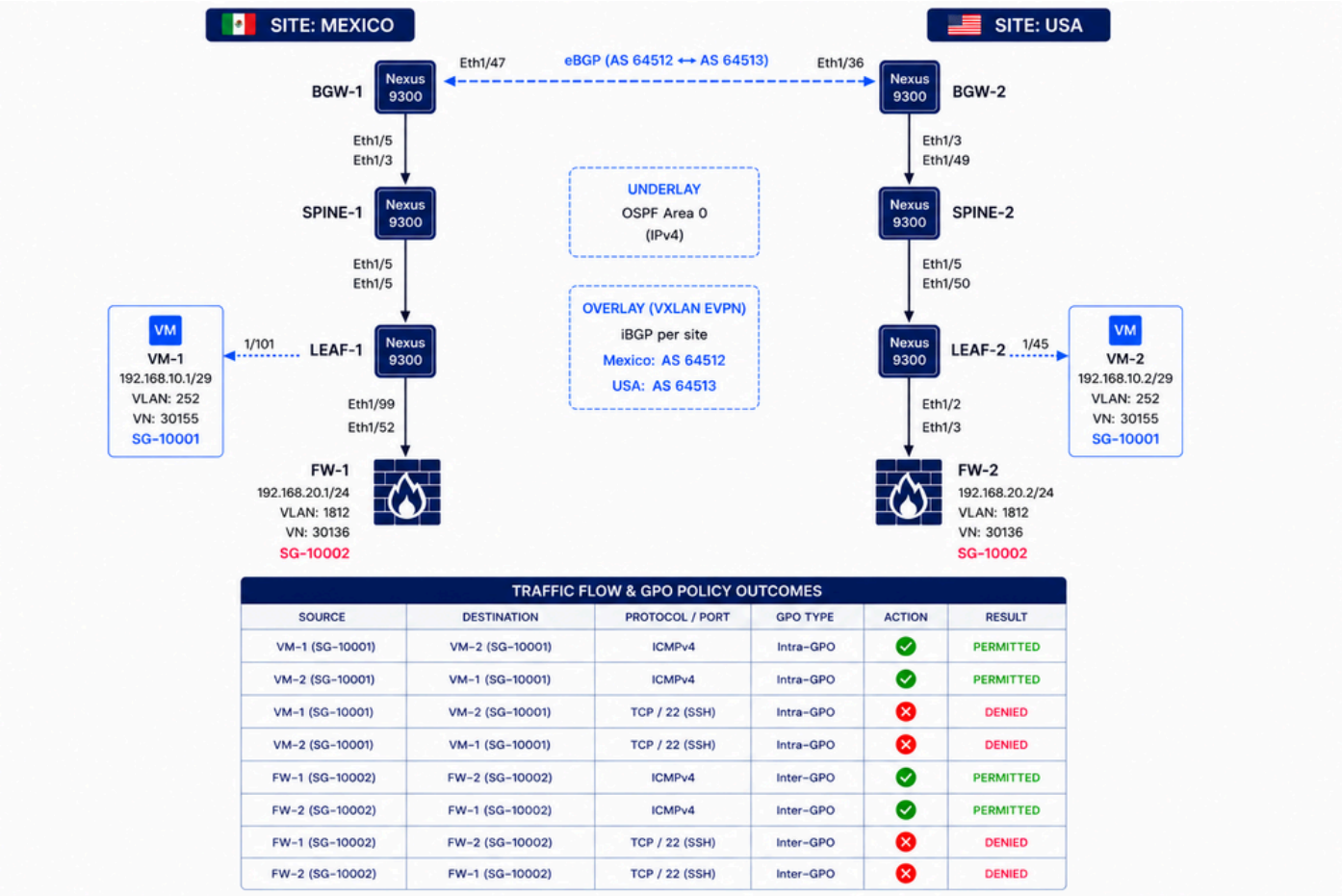
NDFC 4.2およびNX-OS 10.6(3)Fを使用したVXLANマルチサイトGPO展開のシナリオ

このトポロジは、地理的に分散した2つのサイト（メキシコと米国）に展開されたVXLANマルチサイトファブリックを表します。各サイトには、専用のBGW、スパインスイッチ、リーフスイッチ、仮想マシン、およびNX-OS 10.6(3)F搭載のCisco Nexus 9300スイッチで実行されるファイアウォールセグメントが含まれます。アンダーレイネットワークではOpen Shortest Path First(OSPF)が使用されますが、オーバーレイコントロールプレーンでは、サイト間VXLAN EVPN通信に各サイト内のiBGPとBGW-1とBGW-2間のeBGPが使用されます。この環境はラボ環境であるため、メキシコと米国のサイトは両方のBGW間で直接接続されたリンクを介して相互接続され、マルチサイト接続モデルが簡素化されます。

GPOは、IPアドレッシングやVLAN境界に関係なく、セキュリティグループ間でポリシーベースのマイクロセグメンテーションを適用するために使用されます。接続ポリシーテーブルに基づいて、VM-1からVM-2、FW-1、およびFW-2へのICMPトラフィックは許可され、VM-1からFW-1お

よびFW-2へのTCPポート22(SSH)トラフィックは拒否されます。VM-1とVM-2の間のTCPポート22通信は、両方のエンドポイントが同じセキュリティグループ(SG-10001)に属しているため、引き続き許可されます。 この動作は、VXLANマルチサイトファブリック全体で、GPO内およびGPO間の通信の間で異なるトラフィックポリシーがGPOによってどのように動的に適用されるかを示しています。

注:Cisco NX-OSリリース10.6(3)Fでは、ESG内アイソレーション機能を使用して、同じESG（SGとも呼ばれる）内のエンドポイント間の通信を制限できるようになりました。この機能により、ESG内での不正アクセスのリスクが最小限に抑えられ、セキュリティ体制が強化されます。



TRAFFIC FLOW & GPO POLICY OUTCOMES

SOURCE	DESTINATION	PROTOCOL / PORT	GPO TYPE	ACTION	RESULT
VM-1 (SG-10001)	VM-2 (SG-10001)	ICMPv4	Intra-GPO	✓	PERMITTED
VM-2 (SG-10001)	VM-1 (SG-10001)	ICMPv4	Intra-GPO	✓	PERMITTED
VM-1 (SG-10001)	VM-2 (SG-10001)	TCP / 22 (SSH)	Intra-GPO	✗	DENIED
VM-2 (SG-10001)	VM-1 (SG-10001)	TCP / 22 (SSH)	Intra-GPO	✗	DENIED
FW-1 (SG-10002)	FW-2 (SG-10002)	ICMPv4	Inter-GPO	✓	PERMITTED
FW-2 (SG-10002)	FW-1 (SG-10002)	ICMPv4	Inter-GPO	✓	PERMITTED
FW-1 (SG-10002)	FW-2 (SG-10002)	TCP / 22 (SSH)	Inter-GPO	✗	DENIED
FW-2 (SG-10002)	FW-1 (SG-10002)	TCP / 22 (SSH)	Inter-GPO	✗	DENIED

VXLAN EVPNファブリックでのNDFC 4.2を使用したGPOの段階的設定

これらの手順は、VXLANマルチサイトファブリックがすでに動作しており、NDFC 4.2を使用して設定されている場合に適用されます。その後、GPOを実装する必要があります。「VXLAN GPOを使用したマイクロセグメンテーションによるデータセンターのセキュリティ保護」の「

Nexusダッシュボードを使用した自動化」セクションでは、VXLANシングルサイトファブリックの作成から始まる設定について説明しています。

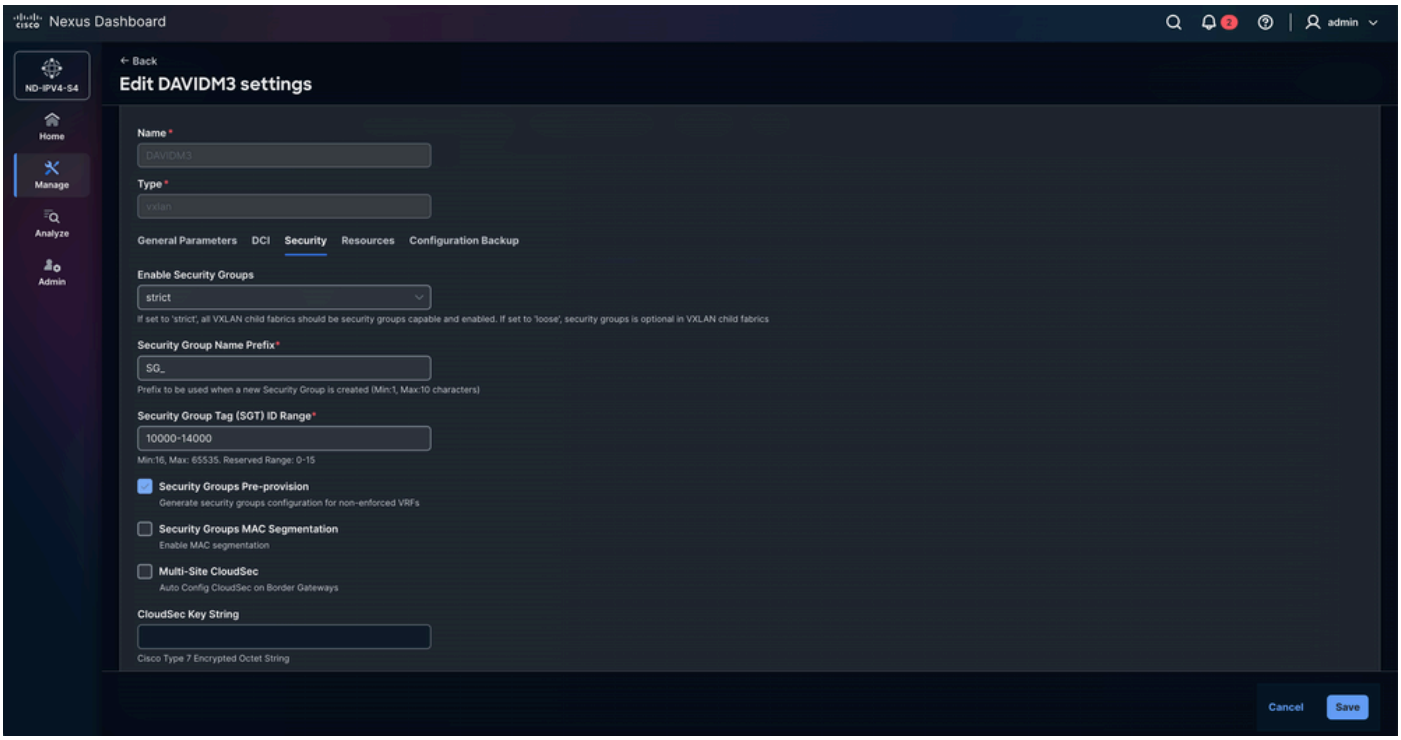
注意:GPOがVXLAN EVPNファブリックで動作している場合、通信は宛先の到達可能性が存在し、セキュリティポリシーでトラフィックが許可されている場合にのみ行われます。ポリシーの適用はIP情報に依存するため、内部ネットワークにはARPエントリとSVIが必要です。つまり、テナントVRFに属するVLANにはSVIが設定されている必要があります。したがって、レイヤ2ヘッダーのみを含むトラフィックには適用されず、VXLANレイヤ2拡張では使用できません。 NX-OSリリース10.6(2)Fでは、MACベースのマイクロセグメンテーションのサポートが導入されています。

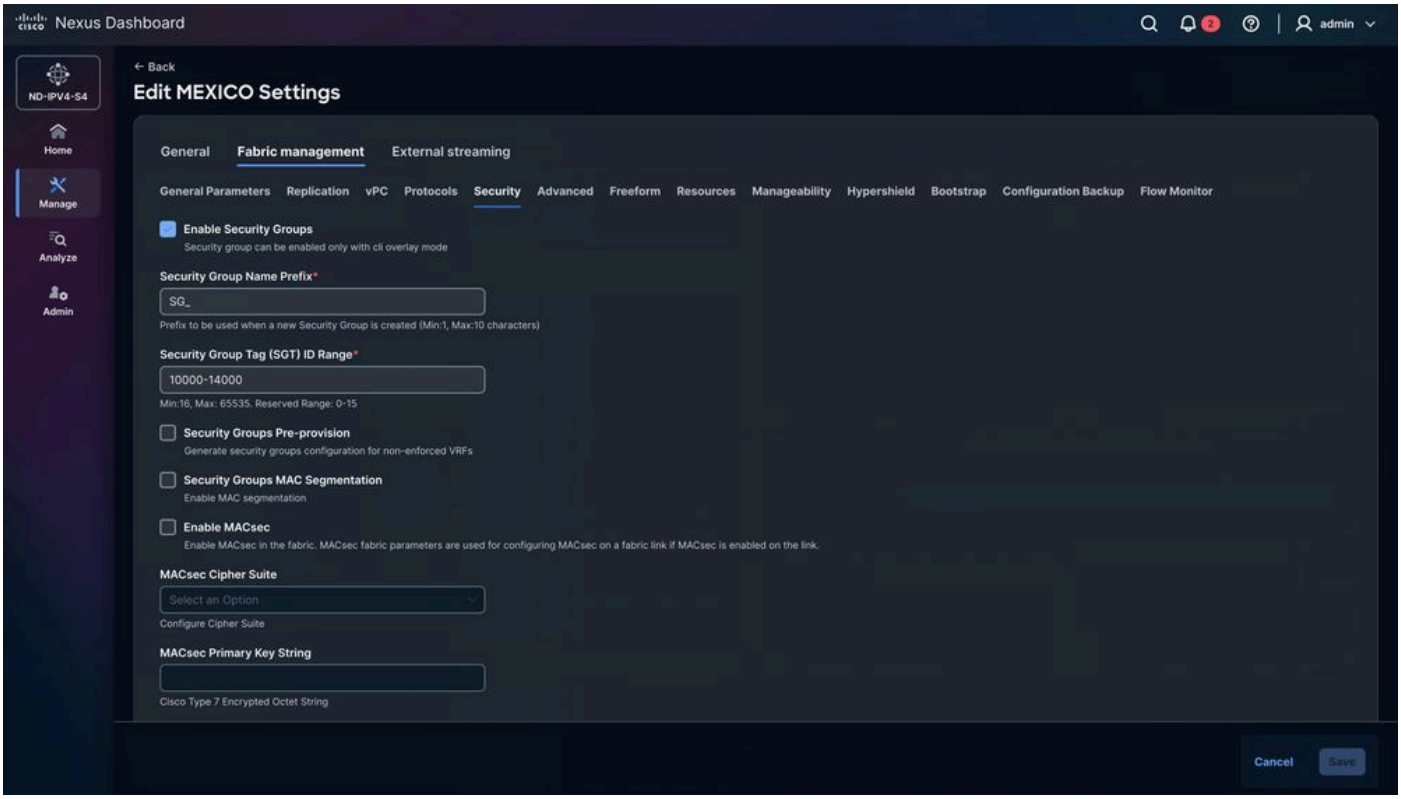
ステップ 1：親ファブリックでセキュリティグループを有効にする

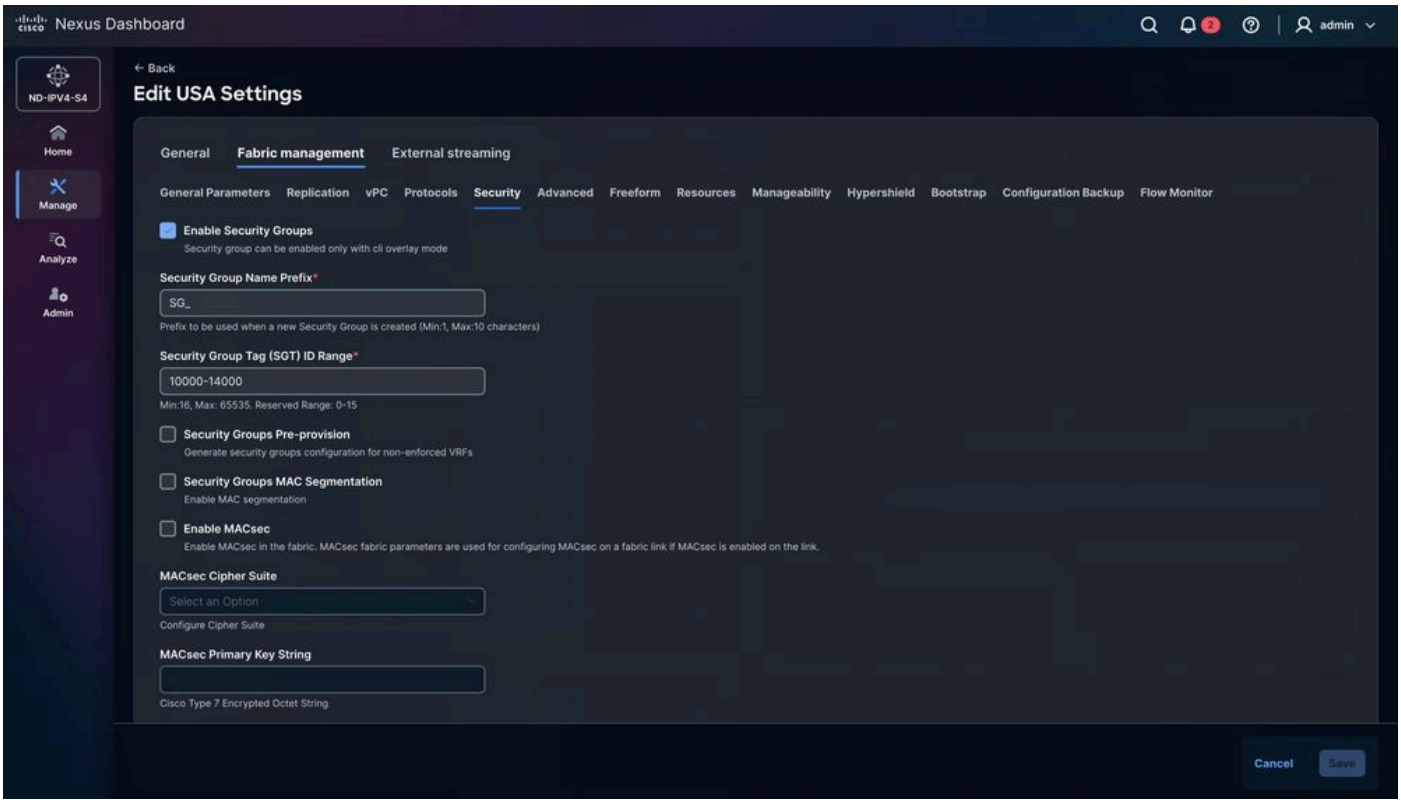
- Manage > Fabric Groupsの順に移動し、ファブリックグループDAVIDM3を選択してから、Actions > Edit Fabric Group Settingsの順に選択します。Securityセクションで、Security Groupsをイネーブルにし、モードをStrictに設定し、Security Groups Pre-provisionを設定します。
  - 対象のファブリックグループを選択します。この例では、選択したファブリックグループの名前はDAVIDM3で、これはマルチサイトファブリックの名前でもあります。
- 各子ファブリックに対して、これらの手順を繰り返します。
  - Manage > Fabricの順に移動し、USAを選択してから、Actions > Edit Fabric Group Settingsの順に移動します。Securityセクションで、Security Groupsをイネーブルにして、モードをStrictに設定します。
  - Manage > Fabricの順に移動し、MEXICOを選択してから、Actions > Edit Fabric Group Settingsの順に移動します。Securityセクションで、Security Groupsをイネーブルにして、モードをStrictに設定します。

注：strictに設定すると、すべてのVXLAN子ファブリックはセキュリティグループ対応で有効になっている必要があります。looseに設定した場合、VXLAN子ファブリックではセキュリティグループはオプションです。

ヒント：クリアな可視性を維持するには、親ファブリックとすべての子ファブリックで同じセキュリティグループタグ(SGT)ID範囲を使用します。親ファブリックの範囲は、すべての子ファブリックで使用される範囲をカバーする必要があります。


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



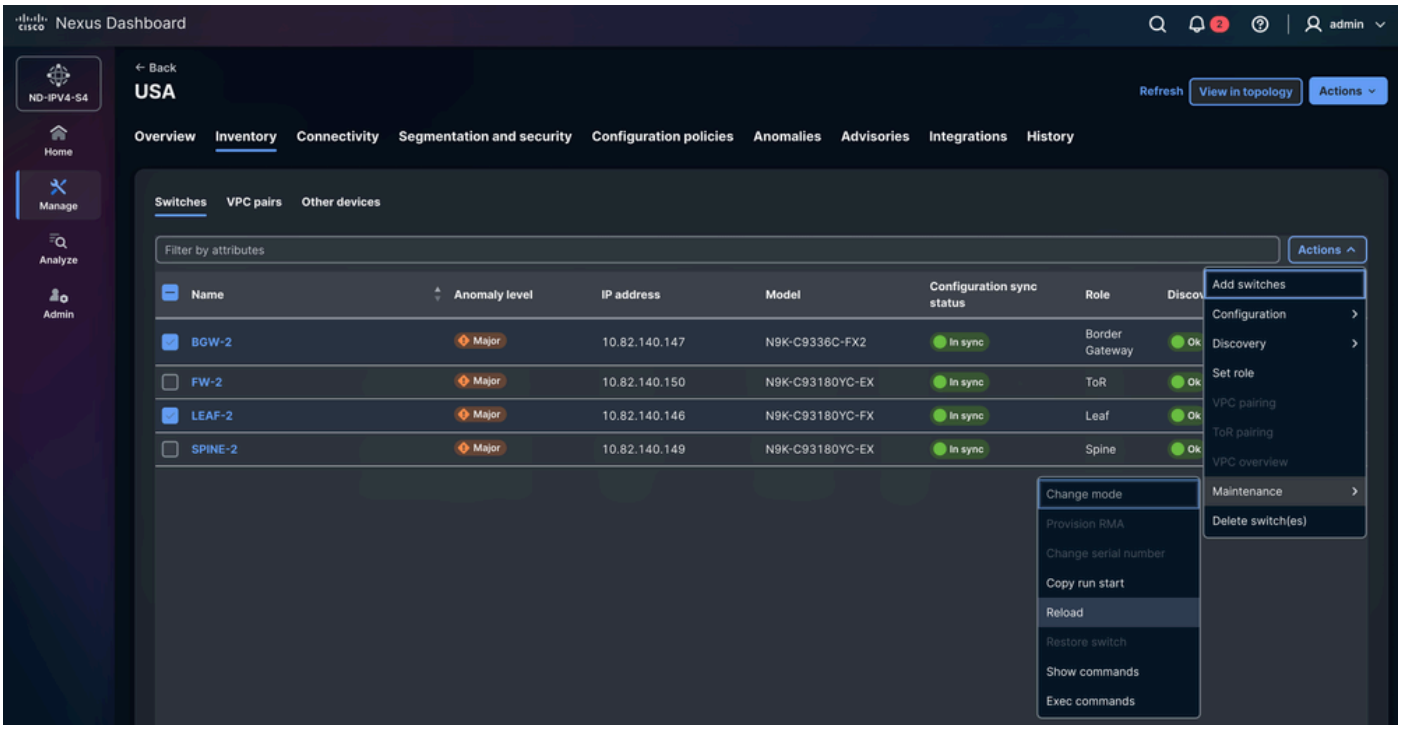
ステップ 2GPO展開のためのファブリック構成の再計算とスイッチのリロード

NDFCでは、Nexusスイッチの役割に基づいて、特定のグループをリロードするように求めるメッセージが自動的に表示されます。この例では、LEAF-1、LEAF-2、BGW-1、およびBGW-2をリロードする必要があります。このアクションは、ネットワーク管理者が手動で実行する必要があります。GPOにはTCAMの分割が必要なので、リロードは必要で、スキップできません。

注：デバイスをリロードしないと、TCAMの変更が実行コンフィギュレーションに反映される場合があります。ただし、スイッチはリブートされていないため、この設定はハードウェアメモリには適用されません。その結果、この機能は期待どおりに機能しません。

Nexusスイッチをリロードするには、次の手順を実行します。

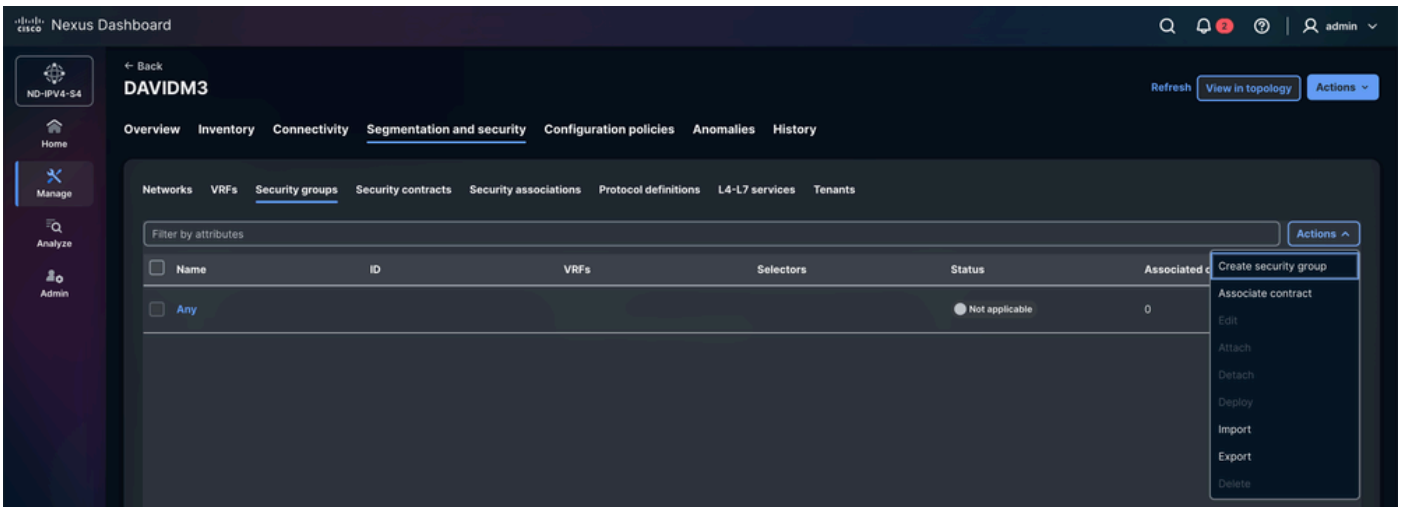
Manage > Fabrics > MEXICO/USA > Inventory > Switches > LEAF-1 / LEAF-2 / BGW-1 / BGW-2 > Actions > Maintenance > Reloadの順に移動します。



ステップ 3セキュリティグループの作成

各エンドポイントのセキュリティグループを定義します。VXLANファブリック内の各エンドポイントは、1つのセキュリティグループを持つことができます。このアプローチは効率的に拡張できません。エンドポイントをグローバルにグループ化します（仮想マシン、ファイアウォール、TCPオプティマイザなど）。

Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security Groups > Actions > Create security groupの順に選択します。



手順3.1セキュリティグループ名の設定

- NDFCは、ランダムな名前を自動的に割り当てます。 名前は変更できます。エンドポイントが識別しやすい代表名を使用することをお勧めします。
- このシナリオでは次のようになっています。
  - VM -> SG_VM
  - FW -> SG_FW

手順3.2 VRFの設定

- エンドポイントが属するテナント(VRF)を選択します。
- このシナリオでは、VMとファイアウォールはCISCO-TACテナントに属します。

オプションで、VRFを作成します。

デフォルトでは、新しく作成されたテナントVRFのポリシー適用モードは未適用に設定されています。この状態では、セキュリティグループ間の分類基準とSGACLが設定されていても、ポリシーは適用されません。SGACL強制をアクティブにするには、VRFを強制モードで明示的に設定する必要があります。

VRFが強制モードで動作している場合は、デフォルトのポリシー動作が定義されます。

- Deny：許可ルールによって明示的に許可されていない限り、すべてのユニキャストトラフィックは廃棄されます。
- 許可：拒否ルールによって明示的にブロックされない限り、すべてのユニキャストトラフィックが許可されます。

同じセキュリティグループに属するエンドポイントは、SGACLルールを必要とせずに相互に通信できます。SGACLは、異なるセキュリティグループ間でのみセキュリティポリシーを定義します。

Cisco NX-OSリリース10.6(3)Fには、同じGPO内(GPO内の分離とも呼ばれる)のエンドポイント間の通信を制限する機能が導入されています。このリリース以前は、同じセキュリティグループ内のエンドポイントに適用されたルールは無視され、デフォルトでトラフィックが許可されていました。

手順3.3セキュリティグループタグIDの設定

NDFCは、ファブリック構成で事前定義された範囲からランダムなタグIDを自動的に割り当てます。タグIDは手動で選択できますが、子ファブリックと親ファブリックの両方に定義された範囲内である必要があります。

このシナリオでは次のようになっています。

- VM-1およびVM-2:10001
- FW-1およびFW-2:10002

ステップ3.4添付

Attachオプションが有効でない場合、セキュリティグループはCISCO-TACテナントに適用されません。

手順3.5セレクタの設定

- セレクタは、特定のセキュリティグループに関連付けられているエンドポイントと外部IPアドレスを決定します。

NDFC 4.2では、次の3種類のセレクタがネイティブでサポートされています。

1) IPセレクタ：IPセレクタは、IP情報に基づいて、エンドポイントまたはIPサブネットをセキュリティグループに関連付けます。

a. 接続エンドポイント：仮想マシン、サーバ、リーフスイッチに接続された物理ホストなど、ファブリックに直接接続されているエンドポイントを特定します。
b. 外部サブネット：外部IPプレフィックスをセキュリティグループに関連付けます。このタイプは、外部データセンター、WANセグメント、インターネットに面したネットワークなど、VXLANファブリックの外部に存在するネットワークに使用されます。これらのプレフィクスを送信元または宛先とするトラフィックは、設定済みのセキュリティグループで分類されます。

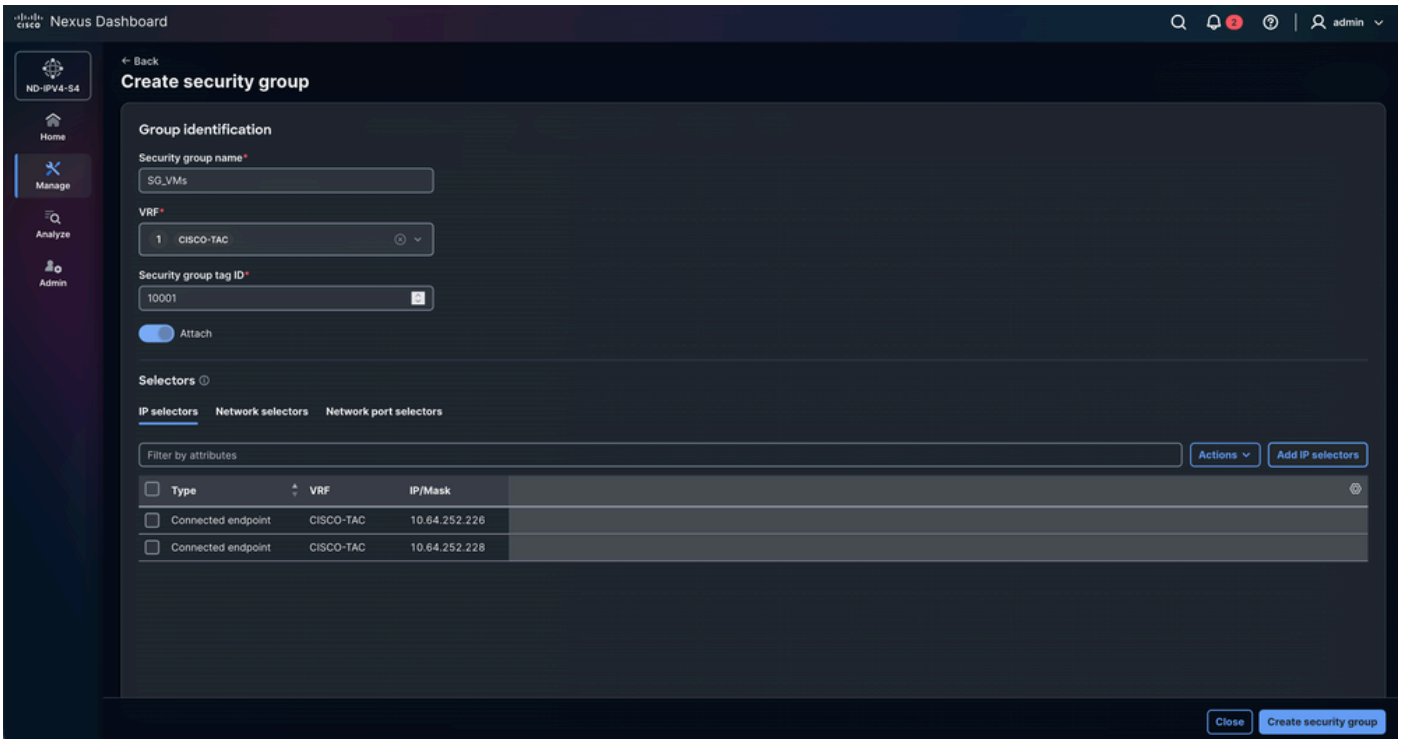
2)ネットワークセレクタ：ネットワークセレクタは、セキュリティグループを特定のVXLANネットワークセグメントに関連付けます。分類は、ネットワークID(L2VNI)に基づいて適用されます。そのネットワークに属するすべてのエンドポイントは、割り当てられたセキュリティグループを継承します。これにより、複数のエンドポイントが同じセグメントを共有する場合のポリシー展開が簡素化されます。

3)ネットワークポートセレクタ：ネットワークポートセレクタは、トラフィックがファブリックに入る物理スイッチインターフェイスに基づいてトラフィックを分類します。セキュリティグループは、特定のポートまたはインターフェイスで受信されたトラフィックに割り当てることができます。このアプローチは、通常、外部ネットワーク、サービスアプライアンス、またはエンドポイントIP分類が不可能なインフラストラクチャリンク経由で接続されているデバイスに使用されます。

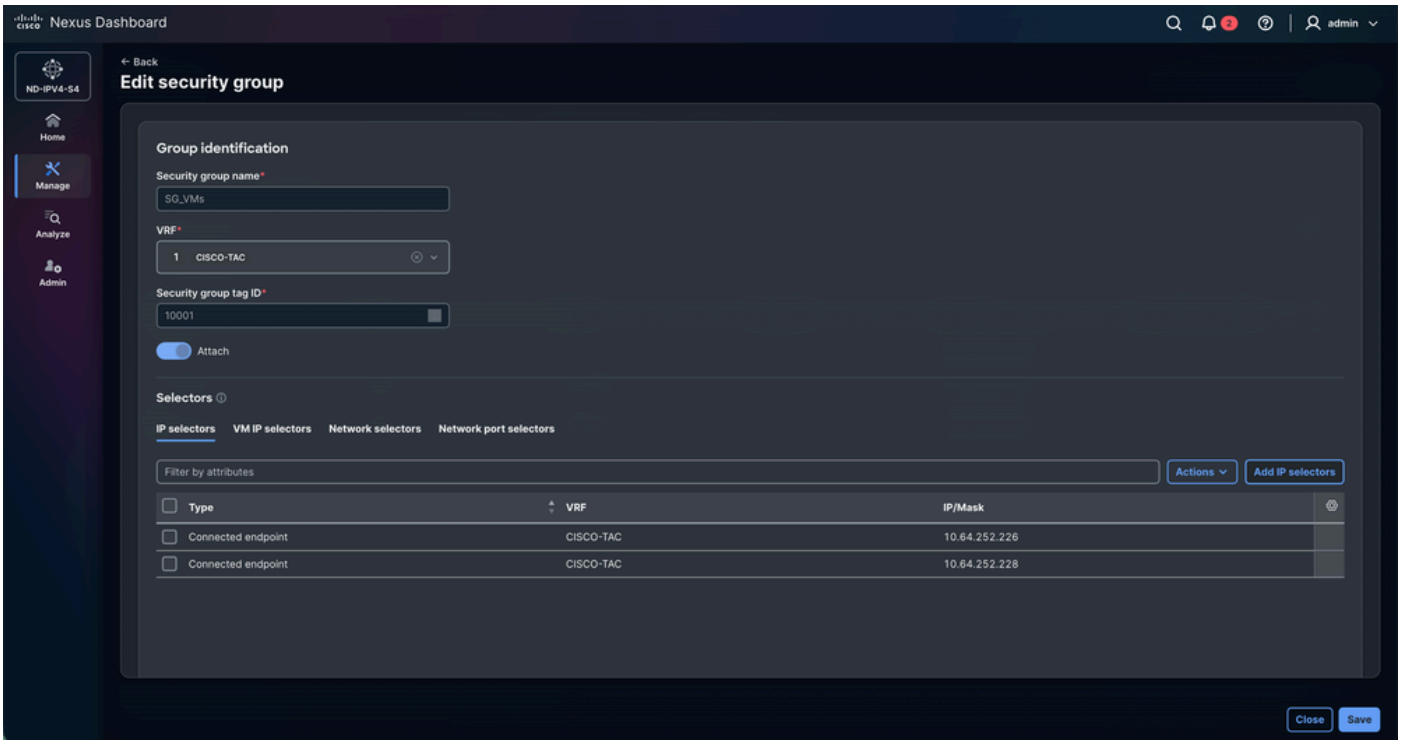
セキュリティグループ構成の概要

デバイス	セキュリティグループ名	VRF	セキュリティグループタグID	セレクタ
VM-1	SG_VM	シスコとTAC	10001	IPセレクタ
VM-2	SG_VM	シスコとTAC	10001	IPセレクタ
FW-1	SG_FW	シスコとTAC	10002	IPセレクタ
FW-2	SG_FW	シスコとTAC	10002	IPセレクタ

VMのセキュリティグループの設定



FW用のセキュリティグループ設定



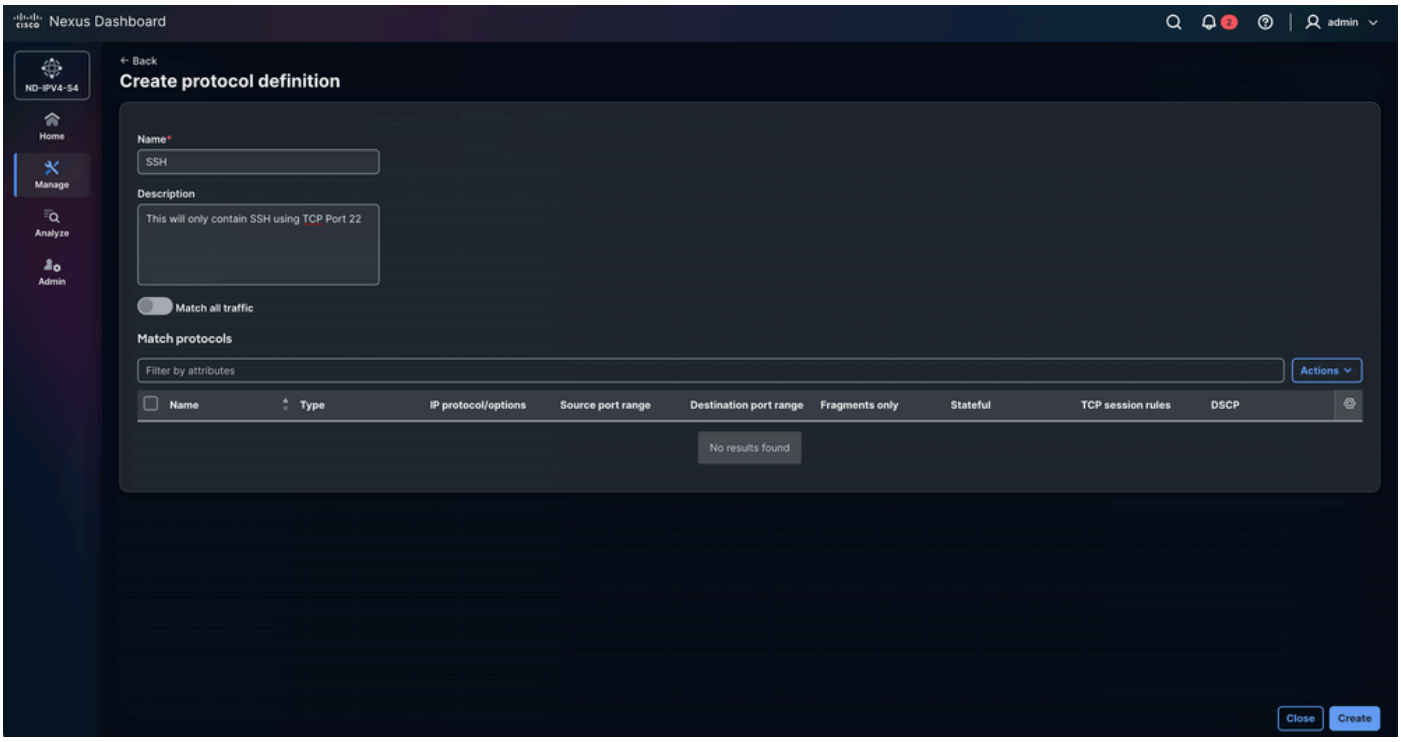
ステップ 4プロトコル定義の設定

Create Protocol Definitionオプションは、グループポリシーオブジェクト(GPO)によって一致されるネットワークプロトコルパラメータとトラフィック特性を定義するために使用されます。 管理者は、プロトコルタイプ、ポート番号、その他のパケット属性などの基準を指定して、対応するポリシーを目的のトラフィックフローに適用できます。

このシナリオの目的は、ポート22(SSH)でTCPトラフィックを明示的にブロックしながら、ICMPトラフィックのみを許可することです。 このポリシーにより、ネットワーク到達可能性テストは許可されたままになりますが、不正または望ましくないSSHアクセスは手動で制限されます。

Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Protocol definitions > Actions > Create protocol definitionの順に選択します。

[Name] と [Description] を入力します。



Actions > Create protocol entryの順に移動します。

- 名前：SSH
- タイプ：IPv4
    - IPおよびIPv6も使用できます。
- IPプロトコル/オプション：TCP
    - UDP、EIGRP、PIMなどがサポートされます。

- フラグメント：フラグメント化されたIPパケットにルールを照合できます。ネットワークMTUを超えると大きなパケットがフラグメントに分割されることがあるため、この機能は便利です。これを有効にすると、ポリシーがこれらのフラグメントにも適用されます。

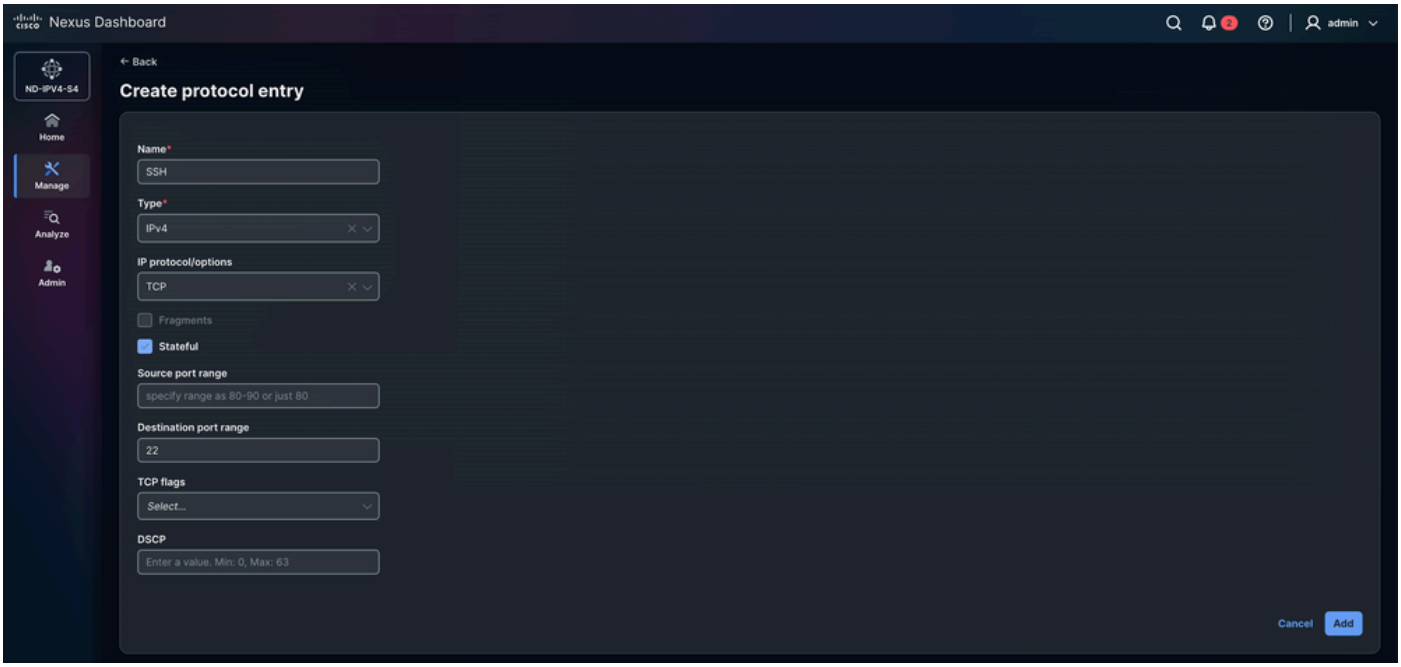
- ステートフル：ステートフルなプロセスとは、過去に発生したすべての変更やインタラクションを追跡し、現在のプロセスをそれらの以前のプロセスのコンテキストで実行することを意味します。この場合、TCPは、転送されるパケットの数、パケットの順序、受信者がパケットを受信したかどうかなどのエリアを追跡します。Statefulオプションを選択すると、この情報は状態としてTCPに保存されます。

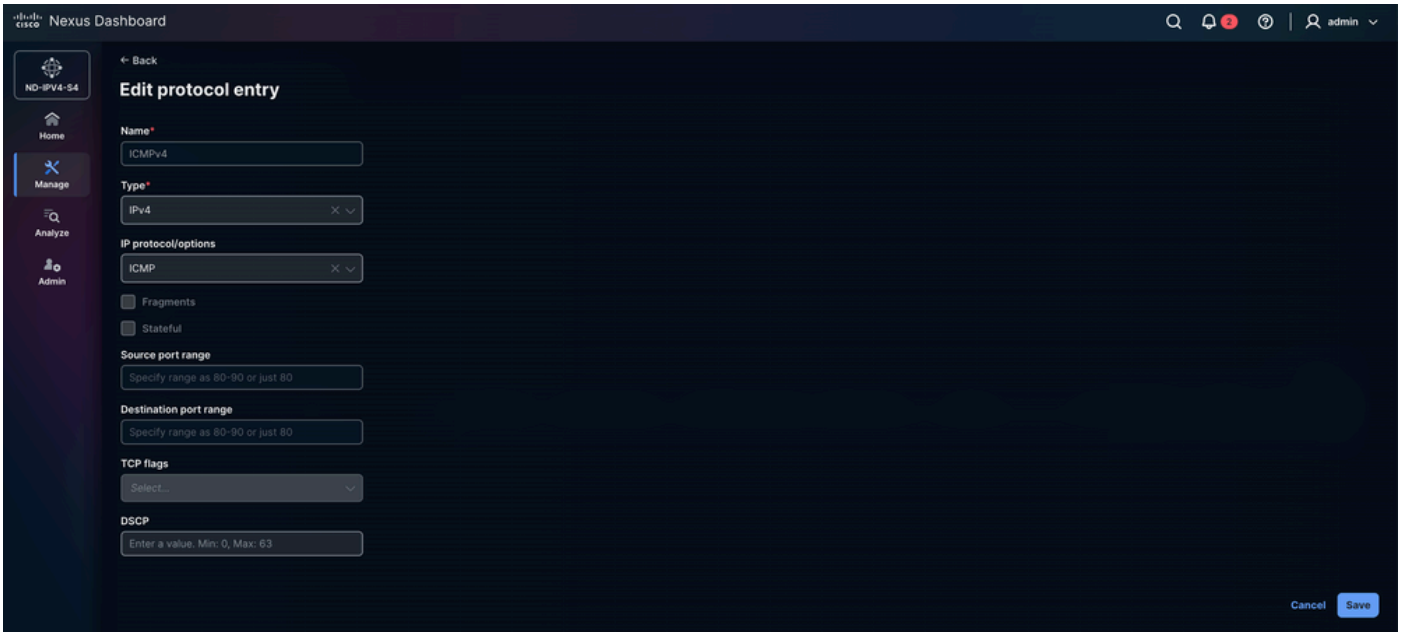
- 送信元ポート範囲：このオプションは、上記のIP Protocol/Optionsフィールドで TCPまたはUDPを選択した場合にのみ使用できます。
- 宛先ポート範囲：このオプションは、[IPプロトコル/オプション]フィールドで[TCP]または[UDP]を選択した場合にのみ使用できます。
- TCPフラグ

    - このオプションは、IP Protocol/OptionsフィールドでTCPが選択されている場合にのみ使用できます。

    - セキュリティプロトコルで使用されるTCPフラグを定義できます。

- TCPフラグはTCPヘッダーの一部であり、接続の確立、メンテナンス、および終了を制御するために使用されます。
- 利用可能なオプション：
    - ACK(Acknowledgment)：受信したデータまたは同期パケットの確認応答を示します。
    - EST(Established)：すでに確立されているTCP接続を指します。このオプションを有効にすると、他のTCPフラグを選択できなくなります。
    - FIN(Finish):TCP接続を正常に閉じるために使用します。
    - RST（リセット）：接続を即時に終了し、転送中のデータを破棄します。
    - SYN（同期）:TCP接続の開始および確立時に使用されます。



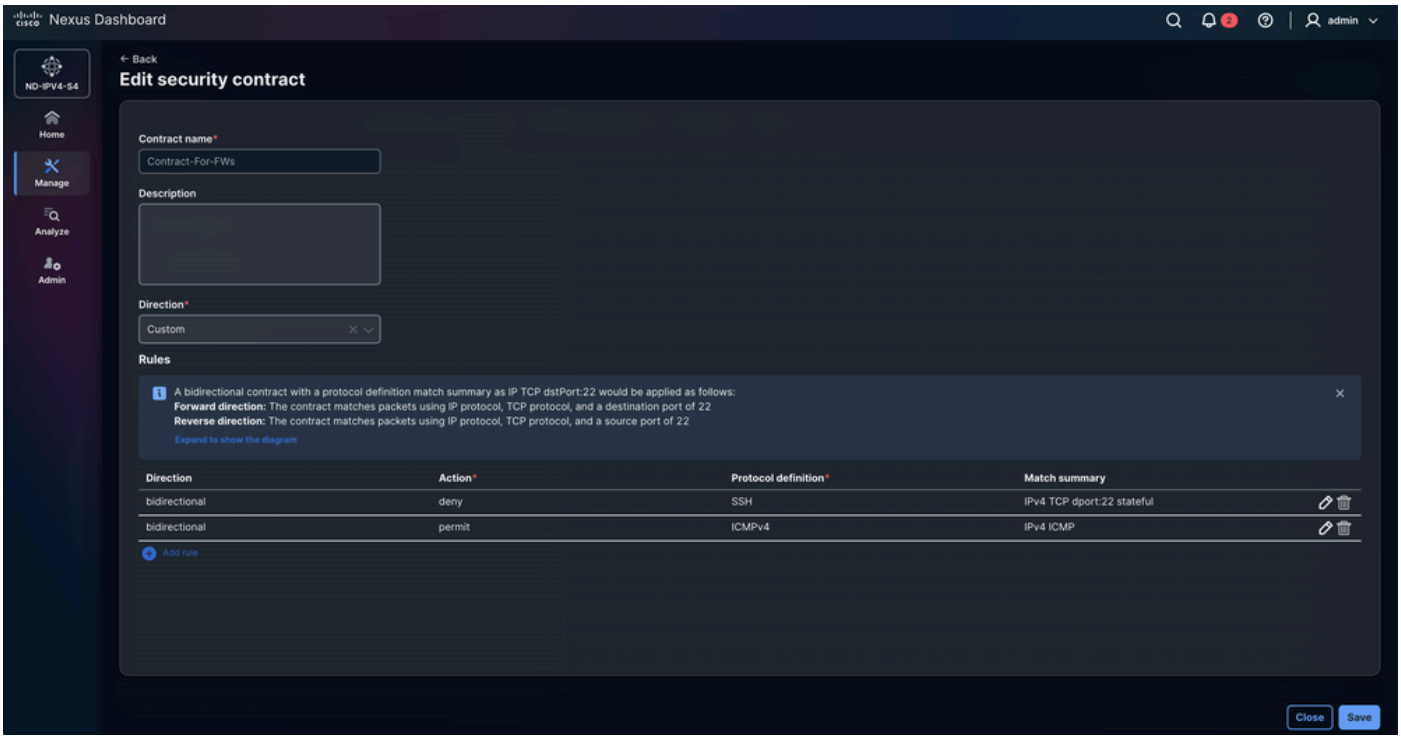


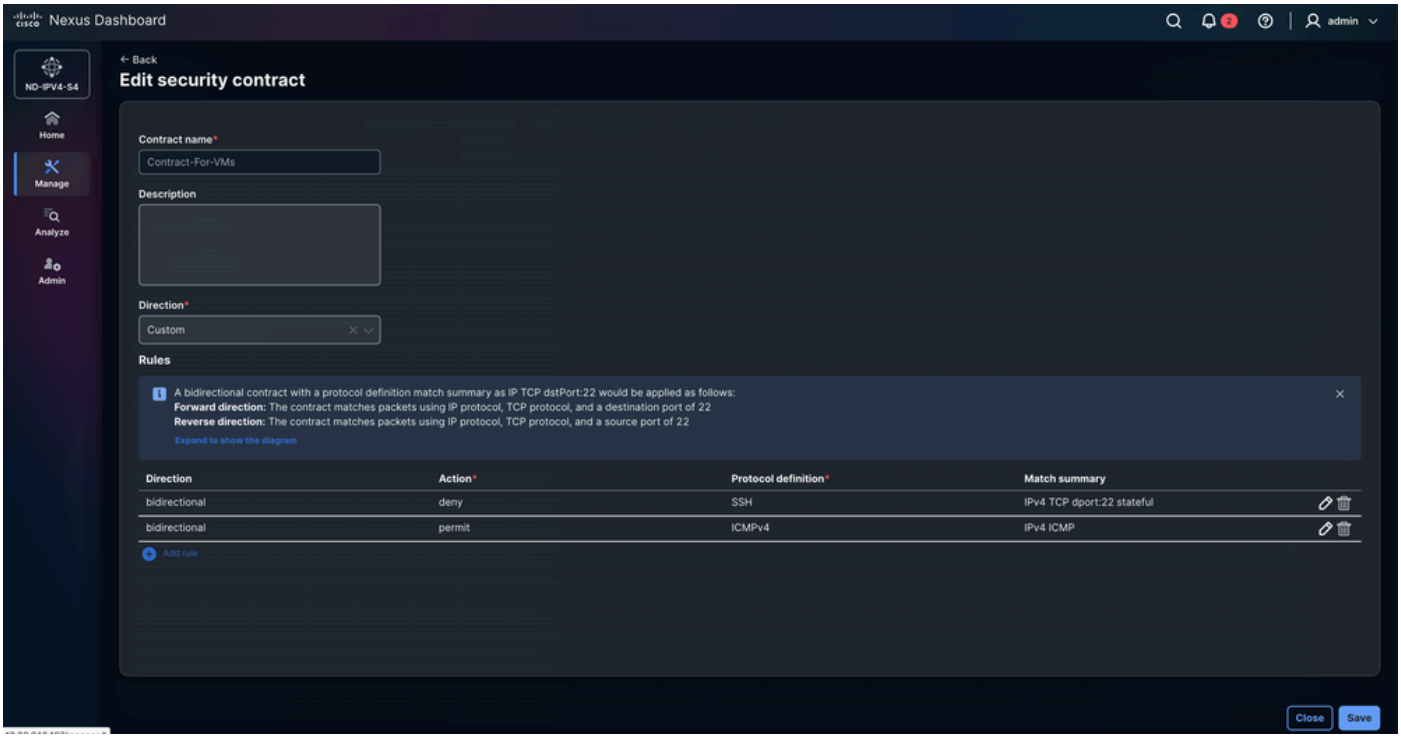
ステップ 5セキュリティコントラクトの設定

コントラクトは、関連するポリシー定義に基づいて許可または拒否するトラフィックを指定することで、エンドポイントグループ間の通信ルールを定義します。この機能は、設定済みのプロトコルルール、フィルタ、およびアクションを適用する強制メカニズムとして機能し、送信元グループと宛先グループ間のトラフィックが目的のセキュリティポリシーおよびセグメンテーションポリシーに確実に準拠するようにします。

Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security contracts > Actions > Create security contractの順に選択します。

- Add ruleを選択し、Direction、Action、およびProtocol definitionを設定します。
    - 双方向：
        - 双方向コントラクトは、IP TCPポート22としてプロトコル定義の一致要約を使用して、次のように適用されます。
            - 順方向：コントラクトは、IPプロトコル、TCPプロトコル、および宛先ポート22を使用してパケットを照合します
            - 逆方向：コントラクトは、IPプロトコル、TCPプロトコル、および送信元ポート22を使用してパケットを照合します。
            - これは、送信元または宛先に関係なく適用されます。
    - 単方向:
        - GPOセキュリティコントラクトにおける単方向とは、ポリシーがトラフィックフローの一方向のみに適用されることを意味し、逆方向に同じルールを自動的に適用することなく、送信元のセキュリティグループから宛先のセキュリティグループへの通信を許可または拒否します。



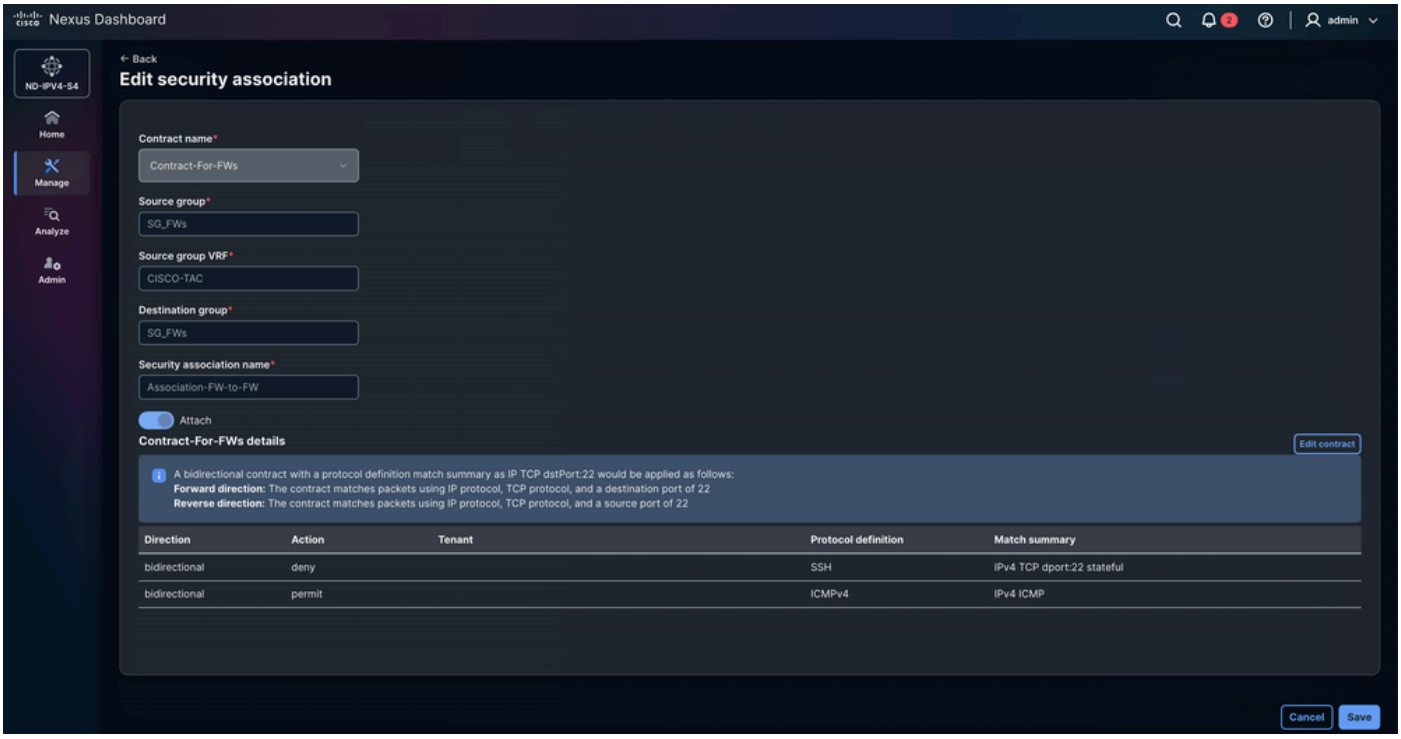


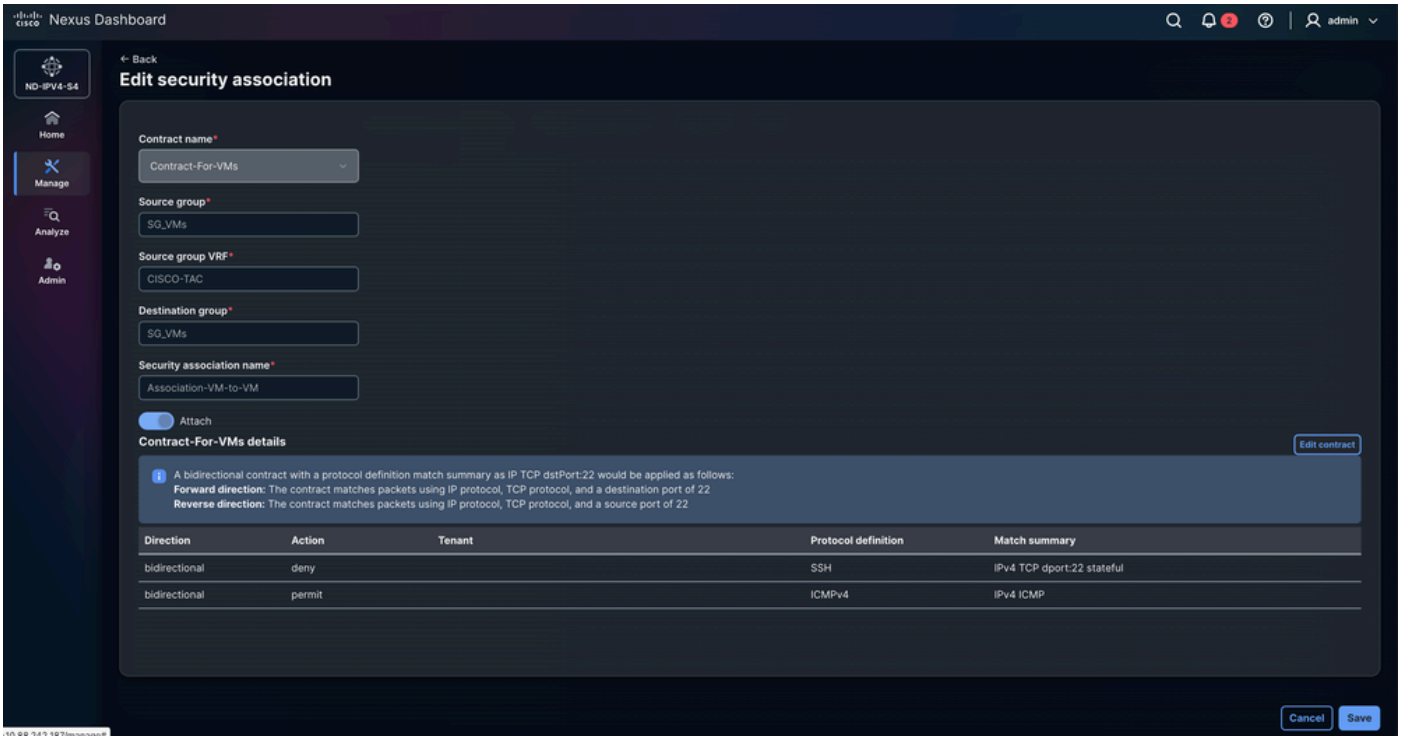
ステップ 6セキュリティアソシエーションの設定

Manage > Fabrics > Fabric groups > DAVIDM3 > Segmentation and security > Security associations > Actions > Create security associationの順に選択します。

「セキュリティアソシエーションの設定」では、ポリシーモデルはセキュリティグループ、プロトコル定義、およびセキュリティコントラクトをリンクすることで定義されます。セキュリティ

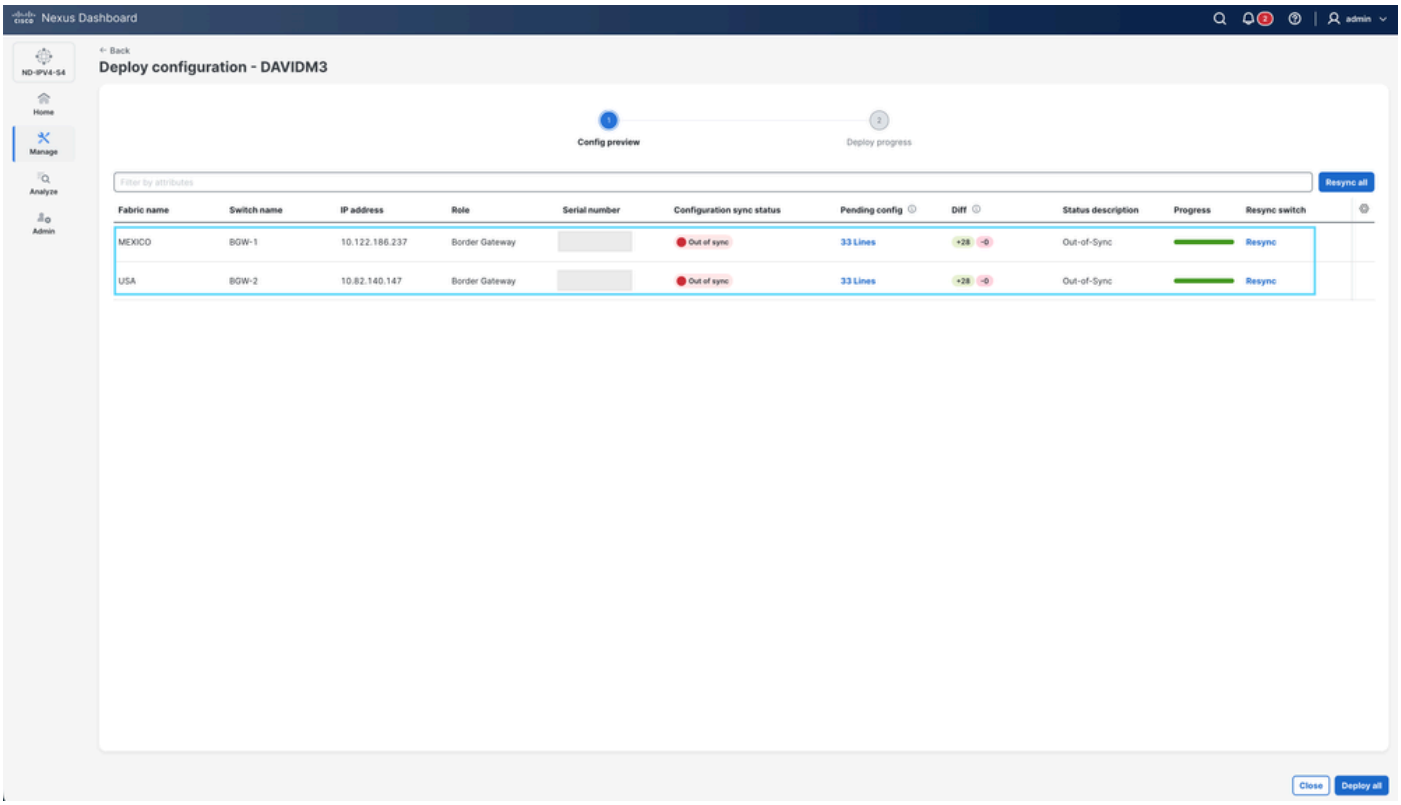
グループはエンドポイントを分類し、プロトコル定義はトラフィックタイプ（プロトコルやポートなど）を指定します。セキュリティコントラクトは、これらのプロトコルルールを使用して送信元セキュリティグループと宛先セキュリティグループ間で適用されるポリシーを定義します。セキュリティアソシエーションは、ファブリックが定義済みのセキュリティポリシーを適用できるように、これらの要素をバインドする関係を表します。

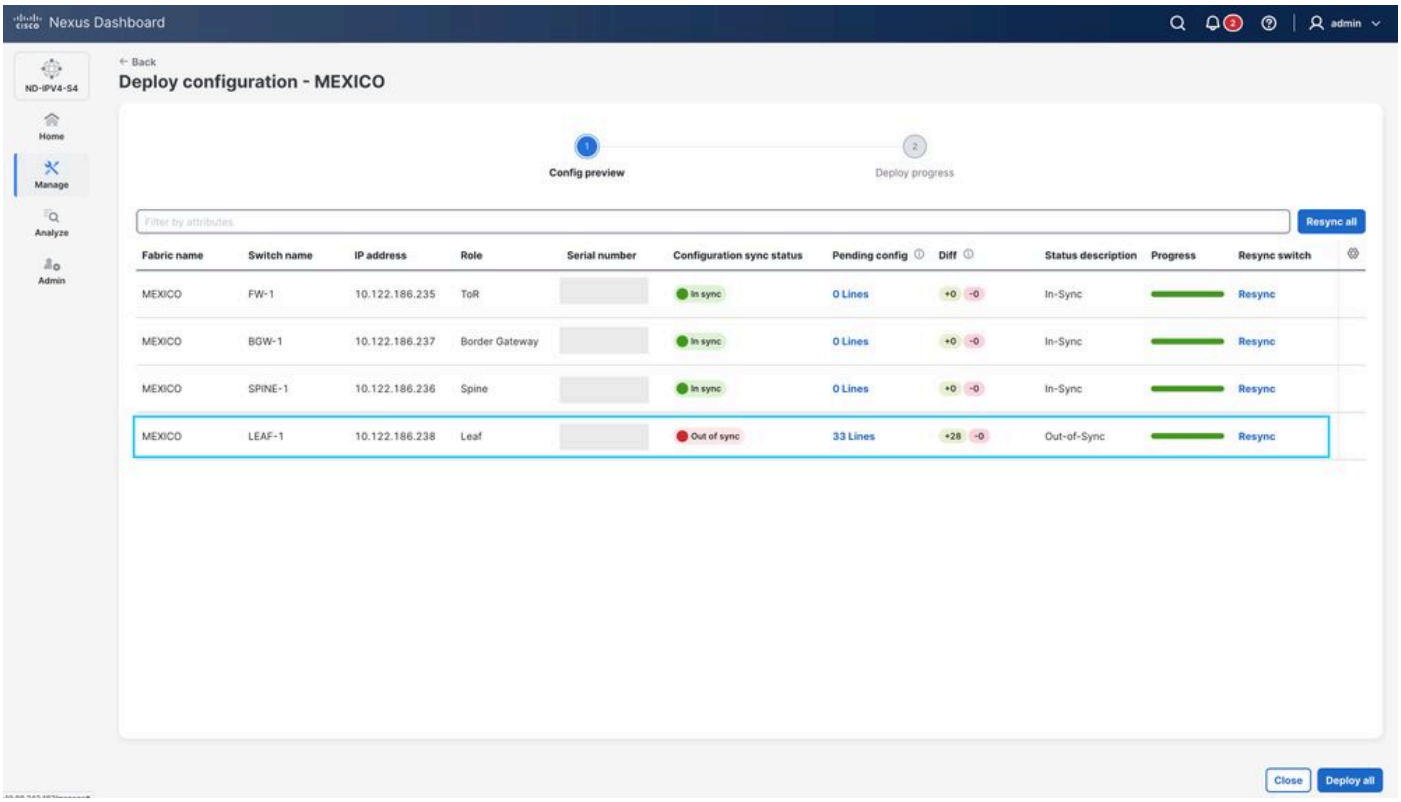


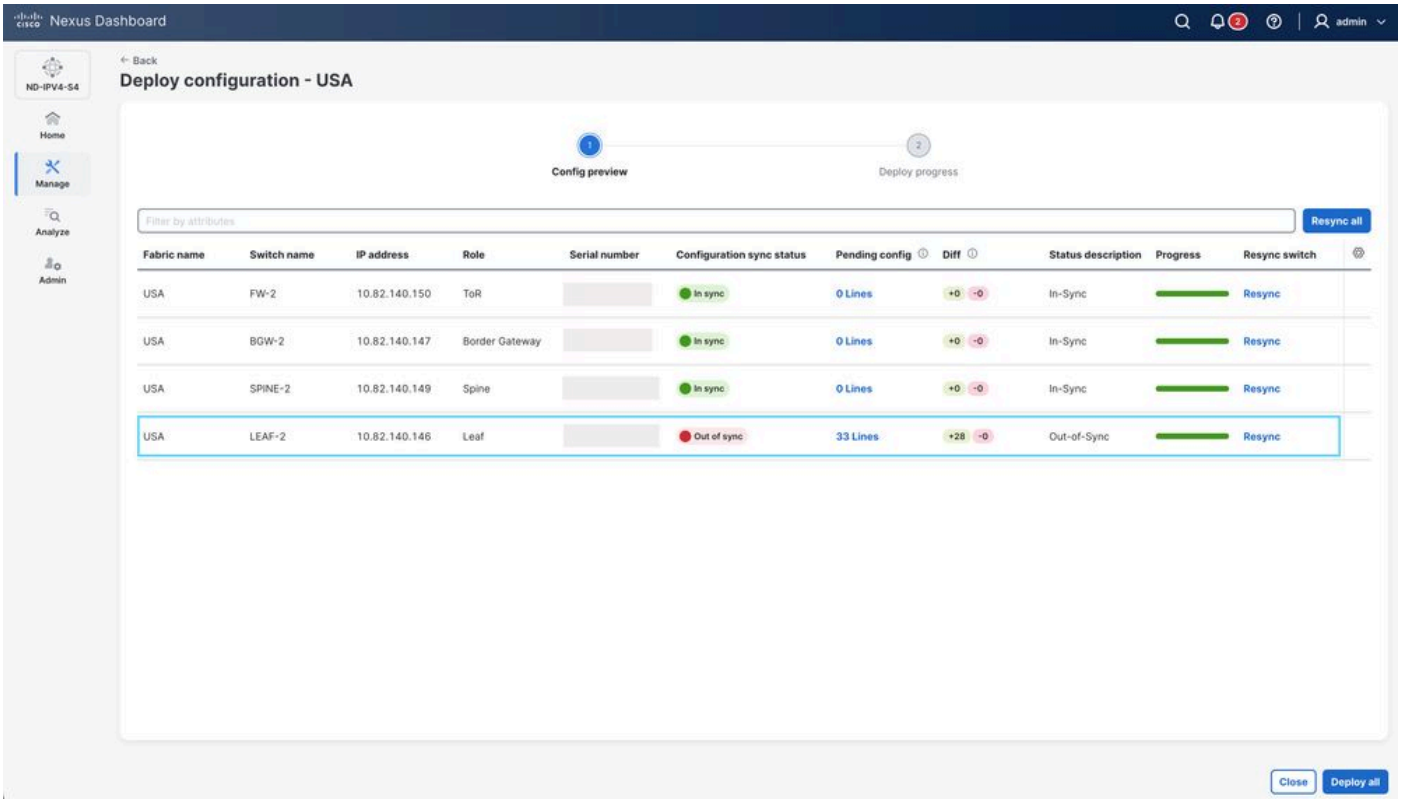


ステップ 7GPO構成の検証

- Manage > Fabrics > Fabric groups > DAVIDM3 > Actions > Recalculate and deployの順に選択します。
  - GPO設定は、親ファブリックスイッチからボーダーゲートウェイにプッシュされます。保留中の設定行の数をクリックして、デバイスに展開できる設定を確認および検証します。このプロセスは、子ファブリックごとに繰り返す必要があります。
  - Manage > Fabrics > Fabric groups > DAVIDM3 > Inventory > Member fabrics > MEXICO > Actions > Recalculate and deployの順に選択します。
  - Manage > Fabrics > Fabric groups > DAVIDM3 > Inventory > Member fabrics > USA > Actions > Recalculate and deployの順に選択します。

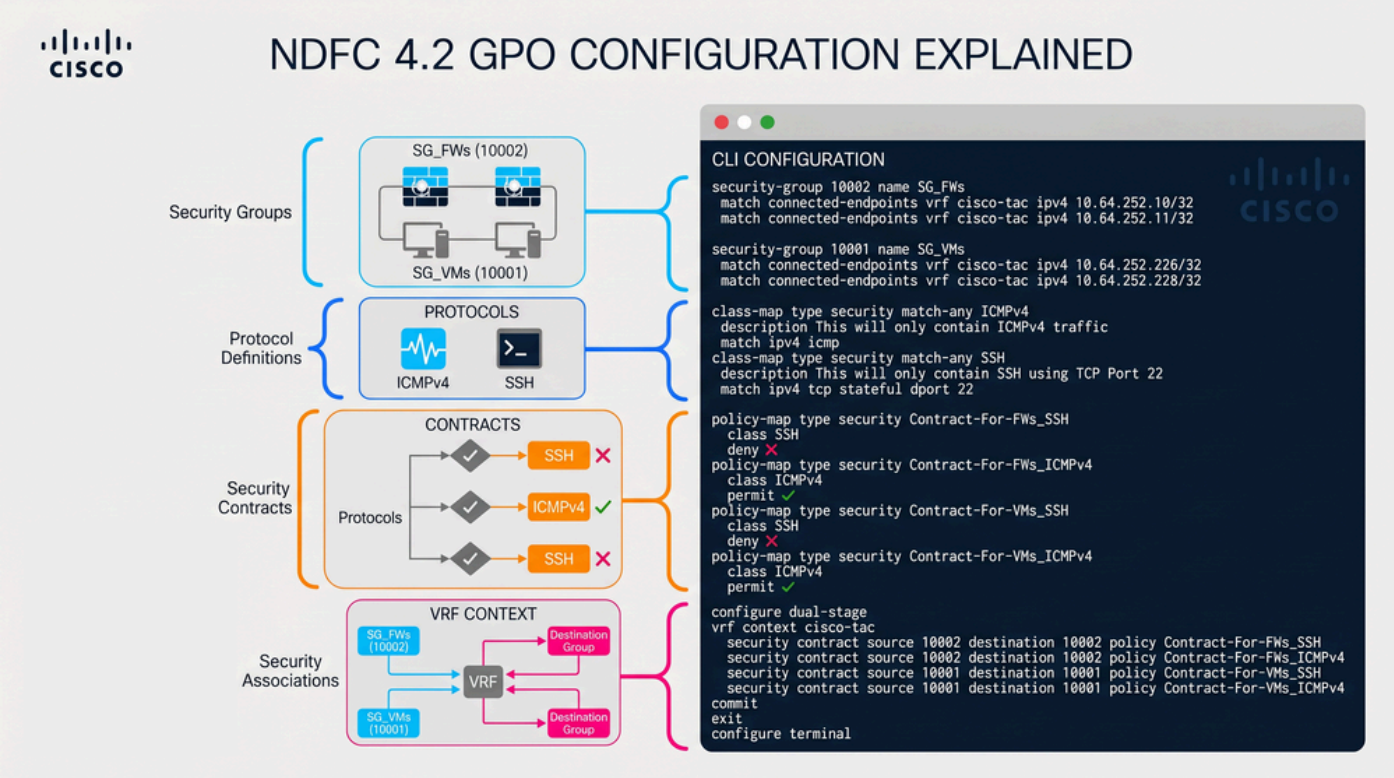






- この図は、BGW-1、BGW-2、LEAF-1、およびLEAF-2のGPO設定を示しています。設定は

すべてのスイッチで同じです。NDFC 4.2では、この設定は示されている順序どおりに適用されません。このセクションでは、CLIコマンドの論理的な順序を示しています。



VXLAN GPOの運用性に関するトラブルシューティング

ステップ 1：セキュリティグループ機能の状態の確認

スイッチでセキュリティグループ機能が有効になっているかどうかを検証します。VXLAN GPOは、エンドポイントの分類、契約の適用、およびSGACLハードウェアプログラミングに必要なセキュリティグループタグ(SGT)インフラストラクチャをアクティブ化するため、この機能に依存しています。

<#root>

BGW-1#

show feature | i i security-group

security-group 1 enabled

ステップ 2システムルーティングモードの確認

スイッチ上で設定されているシステムのルーティングモードと動作しているシステムのルーティングモードを検証します。SGACLの適用ではASICパイプライン内の専用ハードウェア転送リソースを消費するため、VXLAN GPOにはSecurity-Groups Supportルーティングモードが必要です。

<#root>

BGW-1#

show system routing mode

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

ステップ 3VXLAN NVEピアの確立とGPO機能の確認

- ローカルファブリックデバイスとリモートマルチサイトピアの間のVXLAN NVEピアの確立を検証します。VXLAN GPO情報はVXLAN EVPNコントロールプレーンを通じて伝搬されるため、ファブリック全体でのセキュリティグループタグ(SGT)の学習とコントラクトの同期には安定したNVE隣接関係が必要です。
- Group Policy capableフィールドは、VXLAN EVPNマルチサイトドメイン全体でのSGT伝搬とSGACLコントラクトの適用に必要なVXLANグループポリシー拡張をリモートVTEPがサポートしているかどうかを確認するため、このコマンドで最も重要なインジケータの1つです。

<#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

ステップ 4セキュリティグループ学習とエンドポイント分類の確認

エンドポイントがセキュリティグループ(SGT)に正しく分類されていることを検証します。
VXLAN GPOの適用は、エンドポイントからSGTへの正確なマッピングに依存します。

<#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
```

ステップ 5セキュリティ契約とポリシー適用の確認

VXLAN GPOコントラクトが正しくインストールされ、動作していることを検証します。コントラクトは、セキュリティグループ間で適用される通信ルールを定義し、マイクロセグメンテーションのためにVXLAN GPOによって使用されるコアポリシーメカニズムを表します。

<#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
```

ステップ 6VRFセキュリティ適用状態の確認

スイッチに設定されているすべてのVRFについて、VXLAN GPOの強制状態を検証します。このコマンドは、SGACLポリシーとセキュリティグループコントラクトがテナントVRF内でアクティブに適用されているかどうかを確認します。

出力から、cisco-tac VRFが、モードがenforcedに設定されたVXLAN GPOの適用にアクティブに参加していることが確認できます。エンフォースメントタグ13648は、このVRF用にハードウェアにプログラムされた内部SGACLポリシーコンテキストを識別します。デフォルトのアクション「deny log」は、セキュリティグループコントラクトで明示的に許可されていないトラフィックが拒否されてログに記録されることを示し、デフォルトの「deny micro-segmentation」ポリシーが実装されます。これに対して、デフォルト、egress-loadbalance-resolution-management、および管理VRFは、未実施モードで動作します。つまり、VXLAN GPOポリシーはこれらのVRF内では適用されず、トラフィックはデフォルトで許可されます。

フィールドStatsは、VRFセキュリティポリシーに一致するトラフィックを追跡します。cisco-tac VRFの下の値0は、コマンドが実行された時点で一致しないトラフィックによってデフォルトの拒否動作がトリガーされていないことを示し、デフォルトVRFの下のカウンタ値4364は、VXLAN GPOが適用されずに動作しているVRF内のトラフィックアクティビティを示しています。

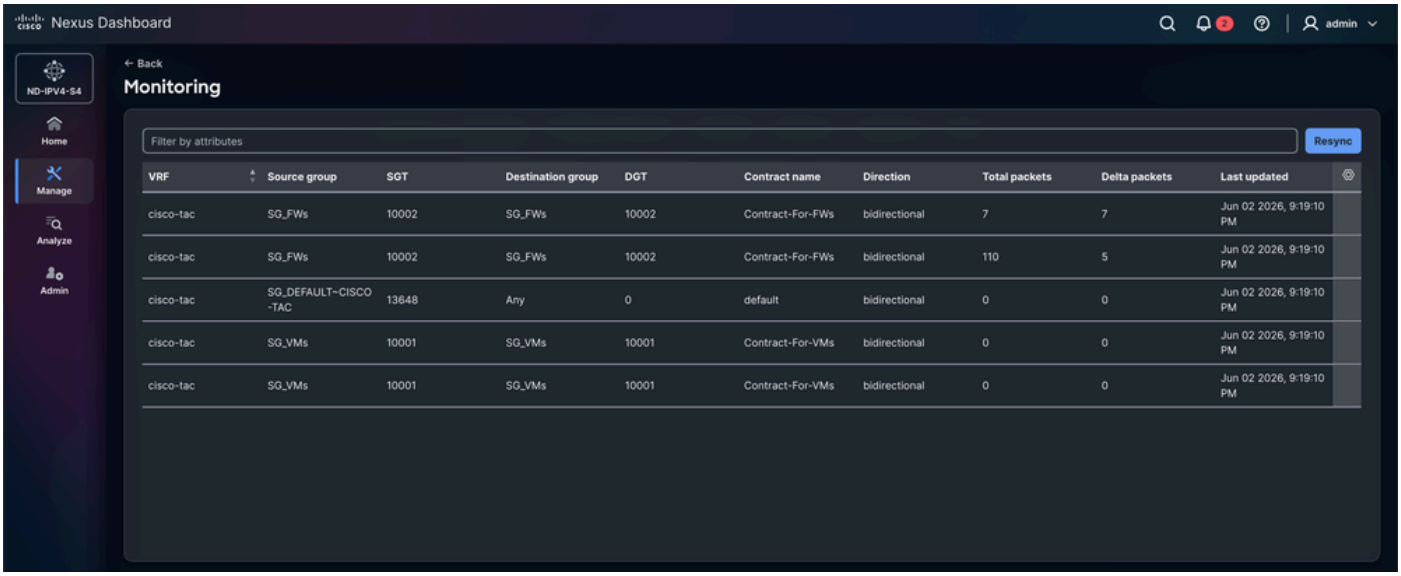
<#root>

```
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
```

ステップ 7VRFセキュリティ適用状態の確認

- NDFC GUIからVXLAN GPOコントラクトのトラフィック一致統計情報を検証します。この検証により、トラフィックが設定済みのセキュリティグループ契約にアクティブに一致しているかどうか、およびSGACLの適用がVXLAN EVPNマルチサイトファブリックで動作しているかどうかが確認されます。
- NDFC GUIで、Manage > Fabrics > Fabric Groups > USA / MEXICO > Segmentation and Security > Security Associations > Monitoringの順に選択します。
  - このセクションでは、セキュリティグループの通信フロー、契約ヒット統計、許可アクションと拒否アクション、およびエンドポイントグループ間の運用契約アクティビティを可視化します。
  - モニタリング統計情報は、それぞれの内部に個別に表示されます。
  - NDFCからの統計情報のモニタリングにより、リアルタイムのポリシー適用とファブリック全体でのトラフィック照合動作を確認することで、CLIベースのトラブルシューティングを補完する運用検証レイヤが提供されます。

注: NDFC 4.2のトラフィック統計情報を初めて確認したときに、モニタリングセクションが最初は空と表示される場合があります。この場合は、Resyncボタンを押して、VXLANファブリックからのコントラクト統計情報の同期をトリガーします。同期プロセスの実行中、GUIに「Resync status: In progress」というメッセージが表示されます。同期が完了したら、Okボタンを押してモニタリングビューを更新します。再同期が完了すると、各セキュリティグループコントラクトに関連付けられたトラフィック統計情報がモニタリングセクションに表示されるようになります。ライブトラフィックの照合動作を検証するには、エンドポイント間でトラフィックを生成し、再度Resyncボタンを押して、NDFCに表示される契約統計を更新します。



- 前のシナリオから、ICMPv4トラフィックはエンドポイント間で正常に許可されます。ただし、SSHセッションが確立されると、VXLAN GPOコントラクトによってポート22を宛先とするTCPトラフィックが明示的に拒否されるため、接続はタイムアウトします。

<#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
```

関連情報

Cisco Nexus 9000シリーズNX-OS VXLANコンフィギュレーションガイド、リリース10.6(x)

VXLAN GPOを使用したマイクロセグメンテーションによるデータセンターの保護

VXLANグループポリシーオプション(GPO)を使用したCisco NX-OS VXLAN EVPNファブリックでのマイクロセグメンテーションの導入

グループポリシーオプション(GPO)とNexusダッシュボードを使用した、VXLAN EVPNファブリックでのマイクロセグメンテーションの自動化とレイヤ4 ~ 7サービスの導入

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。