



## GPO を使用した VXLAN ファブリックのマイクロセグメンテーション

初版：2023 年 12 月 14 日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ [www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/) ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



## 目次

### Trademarks ?

---

はじめに :

はじめに v

対象読者 v

表記法 v

Cisco Nexus 9000 シリーズ スイッチの関連資料 vi

マニュアルに関するフィードバック vi

通信、サービス、およびその他の情報 vii

---

第 1 章

新機能および変更された機能に関する情報 1

新機能と更新情報 1

---

第 2 章

GPO を使用した VXLAN ファブリックのマイクロセグメンテーションの構成 3

概要 3

機能セキュリティ グループについて 4

注意事項と制約事項 5

GPO の構成 6

GPO の有効化 6

セキュリティ グループの作成 7

クラス マップの作成 8

ポリシー マップの作成 8

セキュリティ グループを使用したセキュリティ コントラクトの構成 9

GPO の構成例 9





## はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (v ページ)
- [表記法](#) (v ページ)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料](#) (vi ページ)
- [マニュアルに関するフィードバック](#) (vi ページ)
- [通信、サービス、およびその他の情報](#) (vii ページ)

## 対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

## 表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
<b>bold</b>	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x   y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x   y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y   z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

## Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

[http://www.cisco.com/en/US/products/ps13386/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html)

## マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

### Cisco バグ検索ツール

[Cisco Bug Search Tool \(BST\)](#) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。







# 第 1 章

## 新機能および変更された機能に関する情報

- [新機能と更新情報 \(1 ページ\)](#)

### 新機能と更新情報

表 1: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
グループポリシーオプションを使用した VXLAN ファブリックのマイクロセグメンテーション	グループポリシーオプション機能を使用した VXLAN ファブリックのマイクロセグメンテーションの追加	10.4(2)F	<a href="#">GPO を使用した VXLAN ファブリックのマイクロセグメンテーションの構成 (3 ページ)</a>





## 第 2 章

# GPO を使用した VXLAN ファブリックのマイクロセグメンテーションの構成

- [概要 \(3 ページ\)](#)
- [注意事項と制約事項 \(5 ページ\)](#)
- [GPO の構成 \(6 ページ\)](#)
- [GPO の構成例 \(9 ページ\)](#)

## 概要

従来のデータセンター環境では、アプリケーションまたはワークロードのセキュリティは、外部のデータセンターファブリックからのユーザーが入る境界または南北境界に実装されることがよくあります。これは、多くの場合、境界ファイアウォールやその他のセキュリティ検査デバイスを使用して実装されます。ただし、このアプローチは、最近の攻撃の高度な性質に対しては効果的ではありません。攻撃対象領域は、East-West および North-South フローを含むデータセンター全体に及ぶ。

セキュリティグループおよびセキュリティグループ ACL でマイクロセグメンテーションを使用すると、この機能は NX-OS プラットフォームのユーザーに効果的なソリューションを提供できます。マイクロセグメンテーションを使用すると、組織は、アプリケーションがネットワーク内のどこに常駐するかに関係なく、アプリケーションワークロードの通信方法を指定するアプリケーション固有のポリシーを提供できます。

グループポリシーオプション (GPO) が有効になっている VXLAN ネットワークでは、管理者はセキュリティグループを作成できます。これは、一意のセキュリティグループタグが適用されるネットワークリソースの論理的な集合です。セキュリティグループタグは IP アドレスから取得されます。送信元属性から派生したタグは送信元セキュリティグループタグ (SGT) と呼ばれ、接続先属性から派生したタグは接続先セキュリティグループタグ (DGT) と呼ばれます。セキュリティグループ間のトラフィックは、セキュリティグループアクセスコントロールリスト (SGACL) (セキュリティコントラクトとも呼ばれる) によって制御できます。これは、セキュリティグループタグによって送信元と接続先のセキュリティグループを照合します。

GPO は VXLAN の下位互換性のある拡張機能であり、セキュリティポリシーを適用するために VXLAN ヘッダーにセキュリティグループタグを追加します。

VXLAN 環境では、GPO を使用すると、管理者はアプリケーション属性などの特定の基準に基づいてポリシーを定義し、ネットワークトポロジに関係なく、それらのポリシーをネットワークリソースの特定のグループに適用できます。セキュリティポリシーを設定する場合、GPO は従来の汎用アクセス制御リスト (ACL) よりも柔軟性が高く、複雑さが軽減されます。

リーフスイッチは、適用デバイスとして機能します。ほとんどの適用は入力であり、タグは送信元タグ情報とポリシー適用ビットの両方を伝送します。設定すると、出力の適用を回避できます。送信元タグは、ポリシー適用ビットが設定されていない場合、出力の適用に役立ちません。

GPO は、Cisco NX-OS リリース 10.4(2) 以降で使用可能です。

## 機能セキュリティグループについて

VXLAN EVPN ファブリックにセキュリティグループを作成し、ネットワーク構造やその他の属性を使用してアプリケーション中心のセグメンテーションを定義できます。小規模で分離されたアプリケーションセグメントを定義することで、アプリケーション階層間およびアプリケーション間のネットワークトラフィックのフローをより適切に制御できるマイクロセグメンテーションポリシーを展開できます。マイクロセグメンテーションにより、サービスが必要な場所のみ適用され、アプリケーションとワークロードのセキュリティが向上し、セキュリティ体制が向上します。

マイクロセグメンテーションには、次の 2 つの主要な原則があります。

- **ESG** : エンドポイントセキュリティグループ。属性/セクタに基づいて分類される物理または仮想ネットワークエンドポイントのコレクションを含む論理エンティティです。
- **SGACL** : セキュリティグループ ACL は、L4 フィルタとともに照合にセキュリティタグを使用する ACL です。タグは、IP、MAC、VLAN、ポート/VLAN、VM 属性から取得されます。このリリースでは、IPv4 および IPv6 セクタに基づいてタグを取得できます。

セキュリティグループを使用したマイクロセグメンテーションの機能は次のとおりです。

- 各セキュリティグループは、VRF インスタンスに関連付けられます。セキュリティグループセクタは、VRF インスタンス内のどのエンドポイントと外部 IP がセキュリティグループに属するかを定義します。
- デフォルトでは、VRF は非適用モードで作成されます。つまり、SGACL コントラクトは VRF で適用されません。SGACL を使用するには、VRF モードを適用するように設定する必要があります。

デフォルトで作成されたすべての VRF は、SGACL 適用モードを **UnEnforced** として取得します。これは、VRF で処理されるトラフィックに対して SGACL コントラクトが適用されないことを意味します。VRF で SGACL の適用を有効にするには、VRF を [強制 (**Enforced**)] モードで明示的に設定する必要があります。

- 適用 VRF モードを設定する場合、デフォルトの動作を次のいずれかに定義できます。

- [拒否 (Deny) ]: 許可リストで許可されていない限り、すべてのユニキャストパケットフローがドロップされます。
- [許可 (Permit) ]: 拒否リストによって拒否されない限り、すべてのユニキャストパケットフローが許可されます。
- ESG内のホストは、明示的なSGACLなしで自由に通信できます。VRFモードが適用されている場合、すべてのESG間通信にSGACLが必要です。
- SGACLはセキュリティルールのみを作成します。ESGは、サブネット展開やルートリークなどのネットワーク展開には使用されません。

## 注意事項と制約事項

GPOには、次の注意事項と制限事項があります。

- GPOには、Cisco Nexus リリース 10.4(2) 以降が必要です。
- GPOは、次のプラットフォームでのみサポートされます。
  - N9K-93180YC-FX3
  - N9K-93180YC-FX3S
  - N9K-93600CD-GX
  - N9K-9364C-GX
  - N9K-9316D-GX
  - N9K-9364D-GX2A
  - N9K-9332D-GX2B
- SGACLはVXLAN EVPN展開のコンテキストでのみサポートされ、VRF (テナント)にのみ適用されます。
- SGACLは、単一サイト内でのみサポートされます。
- GPOには下位互換性があり、GPO拡張機能をサポートしていないVTEPは、VXLANヘッダー内の関連する予約済みビットを無視します。ただし、この機能をサポートしているピアまたは有効になっているピアのGPO拡張のみを含める方が、運用上安全で保守的です。同様に、受信側では、着信VXLANカプセル化パケットのGPO関連フィールドは、GPOをサポートしていることがわかっているピアからのみ処理する必要があります。
- SGACLはBUMおよびマルチキャストトラフィックには適用されません。

## GPO の構成

### GPO の有効化

グループ ポリシー オプション機能を有効にするには、次の手順を実行します。

この機能を初めて有効にする場合は、ルーティング テンプレートを **system routing template-security-groups** に構成し、スイッチをリロードする必要があります。機能セキュリティ グループのその後の無効化と再有効化は、リロードなしで実行できます。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>system routing template-security-groups</b> 例 : <pre>switch(config-if)# system routing template-security-groups</pre>	スイッチのルーティング プロファイルを変更します。 (注) この手順では、 <b>copy running-config startup-config</b> の後にリロードが必要です。
ステップ 3	<b>[no] feature security-group</b> 例 : <pre>switch(config-if)# feature security-group</pre>	グループ ポリシー オプション (GPO) 機能を有効にします。機能を無効にするには、「no」プレフィックスを使用します。GPO 機能は、実行時に無効または有効にできます。
ステップ 4	<b>show nve peers detail</b> 例 : <pre>switch(config-if)# show nve peers detail Details of nve Peers: ----- Peer-IP: 1.1.1.1   NVE Interface      : nve1   Peer State         : Up   Peer Uptime        : 1d12h   Router-Mac         : 5292.ca60.1b08   Peer First VNI     : 101   Time since Create  : 1d12h   Configured VNIs    : 100-101,200-201   Provision State    : peer-add-complete   Learnt CP VNIs     : 100-101,200-201   vni assignment mode : SYMMETRIC   Peer Location      : FABRIC   Group policy option : yes -----</pre>	グループ ポリシー オプションが有効になっていることを確認します。

## 次のタスク

セキュリティ グループ セレクタを構成して、グループを作成します。

## セキュリティ グループの作成

セキュリティグループを作成または更新し、メンバー選択基準を設定するには、次の手順を実行します。グループメンバーを選択するには、次の属性を任意に組み合わせて指定できます。

- 接続されたエンドポイントと外部サブネットの IPv4 アドレスまたはサブネット。
- 接続されたエンドポイントと外部サブネットの IPv6 アドレスまたはサブネット。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>security-group <i>sg-id</i> name <i>sg-name</i></b> 例： switch(config)# security-group 100 name webserver	一意の ID が <i>sg-id</i> で名前が <i>sg-name</i> であるセキュリティグループを作成（または既存を選択）します。
ステップ 3	<b>[no] match [connected-endpoints   external-subnets] vrf <i>vrf-name</i> [ipv4   ipv6] <i>ip-prefix</i></b> 例： switch(config-security-group)# match connected-endpoints vrf vrf_blue ipv4 61.1.1.141/32 switch(config-security-group)# match external-subnets vrf vrf_blue ipv4 10.0.0.0/8 switch(config-security-group)# match connected-endpoints vrf vrf_blue ipv6 61:1:1:2:1::141/128 switch(config-security-group)# match external-subnets vrf vrf_blue ipv6 10:11:12:13::/64	このコマンドは、ホスト（接続されたエンドポイント）または外部（外部サブネット）リソースの IPv4-VRF または IPv6-VRF セレクタです。  機能を無効にするには、「no」プレフィックスを使用します。
ステップ 4	<b>show security-group id <i>sg-id</i></b> 例： switch(config-if)# show security-group id 100 Security Group ID 100 , Name 100 Selector Type : External IPv4 Selector VRF-Name IPv4-Address/mask-len  blue 10.1.1.3/32 blue 10.1.1.4/32 Selector Type : Host IPv4 Selector	グループ ポリシー セレクタを確認します。

## ■ クラス マップの作成

	コマンドまたはアクション	目的
	VRF-Name                      IPv4-Address/mask-len blue                            10.1.1.3/32 blue                            10.1.1.4/32	

## クラス マップの作成

クラス マップを作成するには、次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **class-map type security match-any web-class match ip**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>class-map type security match-any web-class match ip</b> 例 : switch# class-map type security match-any web-class2 match ipv4 udp sport 399 to 402 dport 400 to 403 match ipv6 udp sport 399 to 402 dport 400 to 403	クラス マップを作成します。

## ポリシー マップの作成

ポリシー マップを作成するには、次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **policy-map type security policy-map class web-class [permit | deny]**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : switch# configure terminal	グローバル コンフィギュレーション モードを開始します。



	コマンドまたはアクション	目的
ステップ 2	<b>policy-map type security</b> <i>policy-map class web-class</i> [permit   deny]	ポリシー マップを作成します。

## セキュリティ グループを使用したセキュリティ コントラクトの構成

この手順では、セキュリティ グループを適用する SGACL (コントラクト) を作成します。

始める前に

セキュリティ グループを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>vrf context</b> <i>vrf-name</i> 例： switch(config)# vrf context blue	指定した VRF の構成モードを開始します。
ステップ 3	<b>security enforce tag</b> <i>sg-id default</i> [permit   deny] 例： switch(config-vrf)# security enforce tag 100 default deny	VRF の強制を有効にします。
ステップ 4	<b>security contract source</b> [ <i>sg-id / any</i> ] <b>destination</b> [ <i>sg-id / any</i> ] <b>policy</b> <i>policy-map-name</i> [ <i>bidir / unidir</i> ] 例： switch(config-vrf)# security contract source 100 destination 200 policy policyMap1 bidir	指定したセキュリティグループの強制を有効にします。

## GPO の構成例

次に、GPO 構成に関連するいくつかの show コマンドを示します。

- 次の show コマンドは、セキュリティ グループを構成する方法を示しています。

```
switch(config)# show security-group id 1000
Security Group ID 1000 , Name webservers
Selector Type : External IPv4 Subnets
  VRF-Name                               IPv4-Address/mask-len
  vrf_blue                               10.0.0.0/8
Selector Type : Connected IPv4 Endpoints
```

```

VRF-Name                IPv4-Address/mask-len
vrf_blue                 61.1.1.141/32
Selector Type : External IPv6 Subnets
VRF-Name                IPv6-Address/mask-len
vrf_blue                 10:11:12:13::/64
Selector Type : Connected IPv6 Endpoints
VRF-Name                IPv6-Address/mask-len
vrf_blue                 61:1:1:2:1::141/128 switch(config)
switch(config)

switch(config)# show security-group vrf vrf_blue ipv4
Security Group ID 1000 , Name webservers
Selector Type : External IPv4 Subnets
VRF-Name                IPv4-Address/mask-len
vrf_blue                 10.0.0.0/8
Selector Type : Connected IPv4 Endpoints
VRF-Name                IPv4-Address/mask-len
vrf_blue                 61.1.1.141/32
switch(config)

switch(config)# show security-group vrf vrf_blue ipv6
Security Group ID 1000 , Name webservers
Selector Type : External IPv6 Subnets
VRF-Name                IPv6-Address/mask-len
vrf_blue                 10:11:12:13::/64
Selector Type : Connected IPv6 Endpoints
VRF-Name                IPv6-Address/mask-len
vrf_blue                 61:1:1:2:1::141/128
switch(config)#

switch(config)# show security-group name webservers
Security Group ID 1000 , Name webservers
Selector Type : External IPv4 Subnets
VRF-Name                IPv4-Address/mask-len
vrf_blue                 10.0.0.0/8
Selector Type : Connected IPv4 Endpoints
VRF-Name                IPv4-Address/mask-len
vrf_blue                 61.1.1.141/32
Selector Type : External IPv6 Subnets
VRF-Name                IPv6-Address/mask-len
vrf_blue                 10:11:12:13::/64
Selector Type : Connected IPv6 Endpoints
VRF-Name                IPv6-Address/mask-len
vrf_blue                 61:1:1:2:1::141/128
switch(config)#

```

- 次の show コマンドは、セキュリティ契約関連の情報を表示します。

```

switch(config)# show contracts

VRF          SGT  DGT  Policy          Dir  Stats  Class
Action      OperSt
-----
blue        1000  200  policyMap1      bidir  0      web-class1
permit      enabled
switch(config)

switch(config) show contracts sgt 1000

VRF          SGT  DGT  Policy          Dir  Stats  Class
Action      OperSt
-----
blue        1000  200  policyMap1      bidir  0      web-class1
permit      enabled
switch(config)

```

```
switch(config) sh contracts dgt 2000
```

VRF	SGT	DGT	Policy	Dir	Stats	Class
Action	OperSt					
vrf_blue	1000	2000	policyMap1	bidir	0	web-class1
permit	enabled					

```
switch(config)
```

```
switch(config)# show contracts detail
```

```
VRF: blue
  Contract source group 1000 dest group 200
  Policy: policyMap1 Direction: bidir
  Stats: 0
  Class: web-class1
  match ip
  Action: permit
  OperSt: enabled
switch(config)
```

```
switch(config)show contracts policy policyMap1
```

VRF	SGT	DGT	Policy	Dir	Stats	Class
Action	OperSt					
blue	1000	200	policyMap1	bidir	0	web-class1
permit	enabled					

```
switch(config)
```

```
switch(config)show contracts vrf vrf_blue
```

VRF	SGT	DGT	Policy	Dir	Stats	Class
Action	OperSt					
vrf_blue	1000	200	policyMap1	bidir	0	web-class1
permit	enabled					

```
switch(config)
```

```
switch(config)# show run security-group
```

```
!Command: show running-config security-group
!Running configuration last done at: Fri Dec 8 12:23:52 2023
!Time: Fri Dec 8 12:27:09 2023
```

```
version 10.4(2) Bios:version 05.50
```

```
feature security-group
```

```
security-group 1000 name webservers
  match external-subnets vrf vrf_blue ipv4 10.0.0.0/8
  match external-subnets vrf vrf_blue ipv6 10:11:12:13::/64
  match connected-endpoints vrf vrf_blue ipv4 61.1.1.141/32
  match connected-endpoints vrf vrf_blue ipv6 61:1:1:2:1::141/128
class-map type security match-any web-class1
  match ip
class-map type security match-any web-class2
  match ipv4 udp sport 399 to 402 dport 400 to 403

  match ipv6 udp sport 399 to 402 dport 400 to 403
policy-map type security policyMap1
  class web-class1
```

```
vrf context vrf_blue
  security contract source 1000 destination 2000 policy policyMap1
  security enforce tag 100 default deny

switch(config)
```

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。