Cisco TrustSec サブネットと SGT のマッピング

サブネットとセキュリティ グループ タグ（SGT）のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。

Cisco TrustSec サブネットと SGT のマッピングの制約事項

- /31 プレフィックスの IPv4 サブ ネットワークを拡張できません。
- サブネットホストアドレスは、**cts sxp mapping network-map** コマンドの *bindings* 引数が、指定されたサブネット内のサブネットホストの合計数より小さいか、バインド数が 0 の場合、SGT にバインドできません。
- SXP スピーカーおよびリスナーが SXPv3 以降のバージョンを実行している場合のみ、IPv6 拡張および伝播が実行されます。

Cisco TrustSec サブネットと SGT のマッピングに関する情報

IPv4 ネットワークでは、SXPv3 以降のバージョンは SXPv3 ピアからサブネットの network address/prefix ストリングを受信し、解析できます。SXP の以前のバージョンでは、SXP リス

ナー ピアにエクスポートする前に、サブネットのプレフィックスをホスト バインドのセットに変換します。

たとえば、IPv4 サブネット 198.1.1.0 /29 は次のように拡張されます（ホスト アドレスの 3 ビットのみ）。

- ホスト アドレス 198.1.1.1 から 198.1.1.7 はタグ付けされて SXP ピアに伝播します。
- ネットワーク、およびブロードキャスト アドレス 198.1.1.0 および 198.1.1.8 は、タグ付けされず、伝播しません。

（注） SXPv3 がエクスポートできるサブネットバインドの数を制限するには、**cts sxp mapping network-map** グローバル コンフィギュレーション コマンドを使用します。

サブネット バインディングは静的です。つまり、アクティブなホストは学習されません。これらは SGT インポジションおよび SGACL の適用にローカルで使用できます。サブネットと SGT のマッピングによってタグ付けされたパケットは、レイヤ 2 またはレイヤ 3 TrustSec リンクに伝播できます。

（注） IPv6 ネットワークの場合、SXPv3 は SXPv2 または SXPv1 ピアにサブネット バインディングをエクスポートできません。

Cisco TrustSec サブネットと SGT のマッピングの設定方法

サブネットと SGT のマッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp mapping network-map** *bindings*
4. **cts role-based sgt-map** *ipv4-address* **sgt** *number*
5. **cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number*
6. **exit**
7. **show running-config** | **include** *search-string*
8. **show cts sxp connections**
9. **show cts sxp sgt-map**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**cts sxp mapping network-map** *bindings* 例： `Device(config)# cts sxp mapping network-map 10000`	サブネットと SGT のマッピングのホスト数の制限を設定します。*bindings* 引数は、SGT にバインドされ、SXP リスナーにエクスポートできる、0 ～ 65,535 のサブネット IP ホストの最大数を指定します。デフォルトは 0（実行される拡張なし）です。
ステップ 4	**cts role-based sgt-map** *ipv4-address* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	（IPv4）CIDR 表記で IPv4 サブネットを指定します。 手順 3 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。**sgt** *number* キーワードペアでは、指定したサブネットの各ホストアドレスにバインドする SGT 番号を指定します。 • *ipv4-address*：ドット付き 10 進表記で IPv4 ネットワーク アドレスを指定します。 • *prefix*：（0 ～ 30）。ネットワーク アドレス内のビット数を指定します。 • **sgt** *number*：（0 ～ 65,535）。SGT 番号を指定します。
ステップ 5	**cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 2020::/64 sgt 1234`	（IPv6）16 進数表記で IPv6 サブネットを指定します。 手順 3 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。**sgt** *number* キーワードペアでは、指定したサブネットの各ホストアドレスにバインドする SGT 番号を指定します。 • *ipv6-address*：ドット付き 10 進表記で IPv4 ネットワーク アドレスを指定します。

	コマンドまたはアクション	目的
		• *prefix*：（0 ～ 30）。ネットワーク アドレス内のビット数を指定します。 • **sgt** *number*：（0 ～ 65,535）。SGT 番号を指定します。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

ステップ 7	**show running-config** | **include** *search-string*
	例：
	`Device# show running-config | include sgt 1234`
	`Device# show running-config | include network-map`
		cts role-based sgt-map コマンドと **cts sxp mapping network-map** コマンドが実行コンフィギュレーション内にあることを確認します。

ステップ 8	**show cts sxp connections** 例： `Device# show cts sxp connections`	SXP スピーカーとリスナーの接続と、動作ステータスを表示します。
ステップ 9	**show cts sxp sgt-map** 例： `Device# show cts sxp sgt-map`	SXP リスナーにエクスポートした IP と SGT のバインディングを表示します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

Cisco TrustSec サブネットと SGT のマッピング：例

次の例は、SXPv3 を実行している 2 つのデバイス（Device 1 と Device 2）間の IPv4 サブネットと SGT のマッピングを設定する方法を示します。

Device 1（10.1.1.1）と Device 2（10.2.2.2）間の SXP スピーカー/リスナー ピアリングを設定します。

```
Device1# configure terminal
Device1(config)# cts sxp enable
Device1(config)# cts sxp default source-ip 10.1.1.1
Device1(config)# cts sxp default password 1syzygy1
Device1(config)# cts sxp connection peer 10.2.2.2 password default mode local speaker
```

Device 1 の SXP リスナーとして Device 2 を設定します。

```
Device2(config)# cts sxp enable
Device2(config)# cts sxp default source-ip 10.2.2.2
Device2(config)# cts sxp default password 1syzygy1
Device2(config)# cts sxp connection peer 10.1.1.1 password default mode local listener
```

Device 2 で、SXP 接続が動作していることを確認してください。

```
Device2# show cts sxp connections brief | include 10.1.1.1

     10.1.1.1          10.2.2.2          On                3:22:23:18 (dd:hr:mm:sec)
```

サブネットワークが Device 1 に拡張されるように設定します。

```
Device1(config)# cts sxp mapping network-map 10000
Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Device1(config)# cts role-based sgt-map 10.11.11.0/29 sgt 11111
Device1(config)# cts role-based sgt-map 172.168.1.0/28 sgt 65000
```

Device 2 で、Device 1 からのサブネットと SGT の拡張を確認します。ここには、10.10.10.0/30 サブネットワーク用の拡張が 2 個、10.11.11.0/29 サブネットワーク用の拡張が 6 個、172.168.1.0/28 サブネットワーク用の拡張が 14 個存在する必要があります。

```
Device2# show cts sxp sgt-map brief | include 101|11111|65000

IPv4,SGT: <10.10.10.1 , 101>
IPv4,SGT: <10.10.10.2 , 101>
IPv4,SGT: <10.11.11.1 , 11111>
IPv4,SGT: <10.11.11.2 , 11111>
IPv4,SGT: <10.11.11.3 , 11111>
IPv4,SGT: <10.11.11.4 , 11111>
IPv4,SGT: <10.11.11.5 , 11111>
IPv4,SGT: <10.11.11.6 , 11111>
IPv4,SGT: <172.168.1.1 , 65000>
IPv4,SGT: <172.168.1.2 , 65000>
IPv4,SGT: <172.168.1.3 , 65000>
IPv4,SGT: <172.168.1.4 , 65000>
IPv4,SGT: <172.168.1.5 , 65000>
IPv4,SGT: <172.168.1.6 , 65000>
IPv4,SGT: <172.168.1.7 , 65000>
IPv4,SGT: <172.168.1.8 , 65000>
IPv4,SGT: <172.168.1.9 , 65000>
IPv4,SGT: <172.168.1.10 , 65000>
IPv4,SGT: <172.168.1.11 , 65000>
IPv4,SGT: <172.168.1.12 , 65000>
IPv4,SGT: <172.168.1.13 , 65000>
IPv4,SGT: <172.168.1.14 , 65000>
```

Device 1 の拡張数を確認します。

```
Device1# show cts sxp sgt-map

IP-SGT Mappings expanded:22
There are no IP-SGT Mappings
```

Device 1 と Device 2 の設定を保存して、グローバル コンフィギュレーション モードを終了します。

```
Device1(config)# copy running-config startup-config
Device1(config)# exit

Device2(config)# copy running-config startup-config
Device2(config)# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
Cisco TrustSec と SXP の設定	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』
IPsec の設定	『Configuring Security for VPNs with IPsec』
IKEv2 の設定	『Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site』
Cisco Secure Access Control Server	『Configuration Guide for the Cisco Secure ACS』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec サブネットと SGT のマッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : Cisco TrustSec* サブネットと *SGT* のマッピングの機能情報

機能名	リリース	機能情報
Cisco TrustSec サブネットと SGT のマッピング		サブネットとセキュリティ グループ タグ（SGT）のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。 次のコマンドが導入されました：**cts sxp mapping network-map**

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。