



IP プレフィックスと SGT ベースの SXP フィルタリング

セキュリティグループタグ (SGT) 交換プロトコル (SXP) は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。SXP は、パケットのタグ付け機能がないネットワークデバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティサービスは、アクセスデバイスから学習したユーザアイデンティティ情報を伝えることができます。

IP プレフィックスと SGT ベースの SXP フィルタリング機能を使用すると、IP と SGT のバインドをエクスポートまたはインポートするときにフィルタリングできます。このフィルタリングは、IP プレフィックス、SGT、またはその両方の組み合わせに基づいて実行できます。

- [IP プレフィックスとセキュリティグループタグ \(SGT\) ベースのセキュリティ交換プロトコル \(SXP\) フィルタリングの制約事項 \(1 ページ\)](#)
- [IP プレフィックスと SGT ベースの SXP フィルタリングに関する情報 \(2 ページ\)](#)
- [IP プレフィックスと SGT ベースの SXP フィルタリングの設定方法 \(3 ページ\)](#)
- [IP プレフィックスと SGT ベースの SXP フィルタリングの設定例 \(8 ページ\)](#)
- [IP プレフィックスと SGT ベースの SXP フィルタリングの確認 \(9 ページ\)](#)
- [SXP フィルタリングの syslog メッセージ \(11 ページ\)](#)
- [IP プレフィックスと SGT ベースの SXP フィルタリングの機能情報 \(12 ページ\)](#)

IP プレフィックスとセキュリティグループタグ (SGT) ベースのセキュリティ交換プロトコル (SXP) フィルタリングの制約事項

- アクティブデバイスとスタンバイデバイス間のセキュリティ交換プロトコル (SXP) データベースでの、IP セキュリティグループタグ (SGT) バインドのステートフルな同期のハイアベイラビリティのサポートはありません。

- 既存の接続に適用されたフィルタは、エクスポートまたはインポートされた後続のバインドでのみ有効になります。フィルタは、フィルタを適用する前にエクスポートまたはインポートされたバインドには適用されません。
- Virtual Route Forwarding (VRF) 固有のフィルタリングはサポートされておらず、ピア IP に指定されたフィルタはデバイス上のすべての VRF に適用されます。
- フィルタルールの SGT 値は、単一の SGT 番号のリストになります。SGT の範囲はサポートされていません。

IP プレフィックスと SGT ベースの SXP フィルタリングに関する情報

概要

IP プレフィックスと SGT ベースの SXP フィルタリング機能を使用すると、IP と SGT のバインドをエクスポートまたはインポートするときにフィルタリングできます。このフィルタリングは、IP プレフィックス、SGT、またはその両方の組み合わせに基づいて実行できます。

セキュリティグループタグ (SGT) 交換プロトコル (SXP) は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。SXP は、パケットのタグ付け機能がないネットワークデバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。SXP は、ネットワーク上のアップストリームデバイスへの認証ポイントから SGT バインドへの IP を渡します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティサービスは、アクセスデバイスから学習したユーザアイデンティティ情報を伝えることができます。

IP-to-SGT フィルタリングにより、システムは対象のバインドだけを選択的にインポートまたはエクスポートできます。SXP 接続では、バインドのエクスポートまたはインポート中に発生するフィルタリングに基づいて、スピーカーまたはリスナーのどちらかとして機能するデバイスにフィルタを設定できます。

双方向 SXP 接続の場合、スピーカーまたはリスナーのフィルタが設定されているかどうかに基づいて、どちらかの方向にフィルタが適用されます。ピアがスピーカーとリスナーの両方のフィルタグループの一部である場合、フィルタリングは両方向に適用されます。

フィルタは、ピアツーピアベースまたはグローバルに適用できます (すべての SXP 接続に適用可能)。どちらの場合も、フィルタはスピーカーまたはリスナーに適用できます。

フィルタ ルール

デバイスに適用する必要があるフィルタは、一連のフィルタルールを使用して作成されます。各フィルタルールは、特定の SGT 値や IP プレフィックス値を持つバインドに対して実行するアクションを指定します。各バインドは、フィルタルールで指定された値と照合されます。一致が見つかった場合は、フィルタルールで指定された対応するアクションが適用されます。選択したバインドに適用できるアクションは、許可アクションまたは拒否アクションです。IP-SGT

バインドのエクスポートまたはインポート中に、スピーカーまたはリスナーでフィルタが有効になっている場合、バインドはフィルタルールに基づいてフィルタリングされます。

フィルタリストのバインドにルールが指定されていない場合は、フィルタリストに設定されているキャッチオールルールが実行されます。キャッチオールルールがない場合、対応するバインドは暗黙的に拒否されます。

SXP フィルタリングのタイプ

IP-SGT バインドは、次のいずれかの方法でフィルタリングされます。

- SGT ベースのフィルタリング：SGT 値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。
- IP プレフィックスベースのフィルタリング：IP プレフィックス値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。
- SGT および IP プレフィックスベースのフィルタリング：SGT 値と IP プレフィックス値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。

フィルタルールは、各 IP-SGT バインドに適用されます。

IP プレフィックスと SGT ベースの SXP フィルタリングの設定方法

SXP フィルタリストの設定

このステップでは、ルールセットを保持するフィルタリストを作成します。これらのルールは、許可されたバインドを検証し、拒否されたバインドをブロックすることによって、IP-SGT バインドをフィルタリングします。各ルールは、SGT、IP プレフィックス、または SGT と IP プレフィックスの両方の組み合わせに基づいて設定できます。

フィルタリストに特定の IP-SGT バインドと一致するルールがない場合、デフォルトまたはキャッチオールルールが定義されていない限り、バインドは暗黙的に拒否されます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • 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	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 3	<code>cts sxp filter-list filter-name</code>	Cisco TrustSec フィルタリストを設定し、フィルタリストコンフィギュレーションモードを開始します。
ステップ 4	<code>sequence-number permit ipv4 ip-address/prefix deny sgt sgt-value</code>	フィルタリストのルールを設定します。
ステップ 5	<code>exit</code>	フィルタリストコンフィギュレーションモードを終了して、グローバルコンフィギュレーションモードに戻ります。
ステップ 6	<code>cts sxp filter-list filter-name</code>	Cisco TrustSec フィルタリストを設定し、フィルタリストコンフィギュレーションモードを開始します。
ステップ 7	<code>[sequence-number] deny sgt sgt-value permit ipv6 ipv6-address/prefix</code>	フィルタリストのルールを設定します。
ステップ 8	<code>exit</code>	フィルタリストコンフィギュレーションモードを終了して、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	<code>cts sxp filter-list filter-name</code>	Cisco TrustSec フィルタリストを設定し、フィルタリストコンフィギュレーションモードを開始します。
ステップ 10	<code>[sequence-number] permit ipv6 ipv6-address/prefix permit sgt-value permit</code>	フィルタリストのルールを設定します。
ステップ 11	<code>end</code>	フィルタリストコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

SXP フィルタグループの設定

このステップでは、ピアセットを1つのグループにまとめ、そのグループにフィルタリストを適用します。フィルタグループは、スピーカーグループまたはリスナーグループとして定義できます。すべてのスピーカーまたはすべてのリスナーに同じフィルタリストを適用するには、グローバルスピーカーのフィルタグループまたはグローバルリスナーのフィルタグループを作成します。



(注) フィルタグループに適用できるフィルタリストは1つだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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	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 filter-group listener <i>listener-name</i>	SXP フィルタグループのリスナーを設定し、フィルタグループコンフィギュレーションモードを開始します。
ステップ 4	filter <i>filter-list-name</i>	フィルタリストのルールを設定します。
ステップ 5	peer <i>ipv4-address</i>	ピアの IP アドレスを設定します。
ステップ 6	exit	フィルタグループ コンフィギュレーションモードを終了して、グローバル コンフィギュレーションモードに戻ります。
ステップ 7	cts sxp filter-group speaker <i>speaker-name</i>	複数の VLAN アクセス ポートで音声 VLAN を設定します。
ステップ 8	filter <i>filter-list-name</i>	フィルタリスト名を設定します。
ステップ 9	peer <i>ipv4-address</i>	ピアの IP アドレスを設定します。
ステップ 10	end	フィルタグループ コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

グローバルリスナーまたはグローバルスピーカーのフィルタグループの設定

グローバルリスナーとグローバルスピーカーのフィルタグループを設定すると、リスナーモードまたはスピーカーモードのすべての SXP 接続のボックス全体にフィルタが適用されます。

フィルタグループにフィルタリストを追加すると、ボックスに現在設定されているフィルタリストのセットがヘルプストリングとして表示されます。



(注) **peer** コマンドは、グローバルリスナーとグローバルスピーカーのフィルタグループでは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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	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 filter-group listener global <i>filter-list-name</i>	グローバルリスナーのフィルタグループを設定します。
ステップ 4	cts sxp filter-group speaker global <i>filter-list-name</i>	グローバルスピーカーのフィルタグループを設定します。
ステップ 5	end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SXP フィルタリングの有効化

SXP フィルタリストとフィルタグループを設定したら、フィルタリングを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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	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 3	cts sxp filter enable	インターフェイスにソース テンプレートを設定します。
ステップ 4	exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	show cts sxp filter-list <i>filter_name</i>	デバイスに設定されているフィルタリストを、各フィルタリストのフィルタルールとともに表示します。

デフォルトルールまたはキャッチオールルールの設定

デフォルトまたはキャッチオールルールは、フィルタリスト内のどのルールとも一致しない IP-SGT バインドに適用されます。デフォルトルールが指定されていない場合、これらの IP-SGT バインドは拒否されます。

対応するフィルタリストのフィルタリスト コンフィギュレーション モードで、デフォルトまたはキャッチオールルールを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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	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 filter-list <i>filter-name</i>	Cisco TrustSec フィルタリストを設定し、フィルタリスト コンフィギュレーション モードを開始します。
ステップ 4	permit ipv4 <i>ip-address/prefix</i>	条件が一致した場合にアクセスを許可します。
ステップ 5	deny ipv6 <i>ipv6-address/prefix</i>	条件に一致する場合、アクセスを拒否します。
ステップ 6	permit sgt all	すべての SGT に対応するバインドを許可します。

	コマンドまたはアクション	目的
ステップ7	<code>end</code>	フィルタリスト コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

IP プレフィックスと SGT ベースの SXP フィルタリングの設定例

例：SXP フィルタリストの設定

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.1.1.0/24 deny sgt 3 4
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter2
Device(config-filter-list)# permit sgt all
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter3
Device(config-filter-list)# deny ipv6 2001:db8::1/64 permit sgt 67
Device(config-filter-list)# end
```

例：SXP フィルタグループの設定

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-group listener group1
Device(config-filter-group)# filter filter1
Device(config-filter-group)# peer 172.16.0.1 192.168.0.1
Device(config-filter-group)# exit
Device(config)# cts sxp filter-group listener global group2
Device(config)# end
```

例：SXP フィルタリングの有効化

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-enable
Device(config)# end
```


例：デフォルトルールまたはキャッチオールルールの設定

次に、すべての IPv4 および IPv6 アドレスに対応するバインドを許可するデフォルトのプレフィックスルールを作成する例を示します。

```
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.0.0.0/0
Device(config-filter-list)# deny ipv6 2001:db8::1/0
```

次に、すべての SGT に対応するバインドを許可するデフォルトの SGT ルールを作成する例を示します。

```
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# permit sgt all
```

IP プレフィックスと SGT ベースの SXP フィルタリングの確認

設定を確認するには、次のコマンドを使用します。

debug cts sxp filter events コマンドは、フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録するために使用されます。このコマンドは、フィルタリングプロセスの一致アクションに関連するイベントをキャプチャするためにも使用されます。

```
Device# debug cts sxp filter events
```

次に、SXP スピーカーのフィルタグループを表示する **show cts sxp filter-group speaker** コマンドの出力例を示します。

```
Device# show cts sxp filter-group speaker group1
  Filter-group: group1
  Filter-name: filter1
  Peer-list: 172.16.0.1 192.168.0.1
```

次に、SXP スピーカーのリスナーグループを表示する **show cts sxp filter-group listener** コマンドの出力例を示します。

```
Device# show cts sxp filter-group listener

Global Listener Filter: Not configured
  Filter-group: group1
  Filter-name: filter1
  Peer-list: 172.16.0.1 192.168.0.1
  Filter-group: group2
  Filter-name: filter1
  Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

次に、SXP スピーカーのフィルタグループに関する詳細情報を表示する **show cts sxp filter-group speaker detailed** コマンドの出力例を示します。

```
Device# show cts sxp filter-group speaker group1 detailed

Filter-group: group1
Filter-name: filter1
Filter-rules:
  10 deny sgt 30
  20 deny prefix 10.1.0.0/16
  30 permit sgt 60-100
Peer-list: 172.16.0.1 192.168.0.1
```

次に、設定されたすべてのフィルタグループに関する情報を表示する **show cts sxp filter-group** コマンドの出力例を示します。

```
Device# show cts sxp filter-group

Global Listener Filter: Not configured
Global Speaker Filter: Not configured

Listener Group:
  Filter-group: group1
  Filter-name: filter1
  Peer-list: 172.16.0.1 192.168.0.1
  Filter-group: group2
  Filter-name: filter1
  Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group:
  Filter-group: group3
  Filter-name: filter1
  Peer-list: 172.16.0.1 192.168.0.13
  Filter-group: group2
  Filter-name: filter1
  Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

次に、設定されたすべての SXP フィルタグループに関する詳細情報を表示する **show cts sxp filter-group detailed** コマンドの出力例を示します。

```
Device# show cts sxp filter-group detailed

Global Listener Filter: Configured
  Filter-name: global1
  Filter-rules:
    10 deny 192.168.0.13/32
    20 deny sgt 100-200

Global Speaker Filter: Configured
  Filter-name: global2
  Filter-rules:
    10 deny 192.168.0.13/32
    20 deny sgt 100-200

Listener Group:
  Filter-group: group1
  Filter-name: filter1
  Filter-rules:
```

```
10 deny sgt 30
20 deny prefix 172.16.0.0/16
30 permit sgt 60-100
Peer-list: 172.16.0.1, 192.168.0.13

Filter-group: group2
Filter-name: filter1
Filter-rules:
10 deny sgt 30
20 deny prefix 172.16.0.0/16
30 permit sgt 60-100
Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group
Filter-group: group3
Filter-name: filter1
Filter-rules:
10 deny sgt 30
20 deny prefix 172.16.0.0/16
30 permit sgt 60-100
Peer-list: 10.10.10.1, 172.16.0.1, 192.168.0.13

Filter-group: group2
Filter-name: filter1
Filter-rules:
10 deny sgt 30
20 deny prefix 172.16.0.0/16
30 permit sgt 60-100
Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

SXP フィルタリングの syslog メッセージ

SXP フィルタリングの syslog メッセージは、フィルタリングに関連するさまざまなイベントを示すために生成されます。

フィルタルールの syslog メッセージ

単一のフィルタに設定できるルールの最大数は 128 です。単一のフィルタに設定されているフィルタルールの数が制限の 20% 増加するたびに、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in filter [filter-name].
```

単一のフィルタに設定されているルールの数が、フィルタリストに許可されているルールの最大数の 95% に達すると、次のメッセージが生成されます。

```
CTS SXP filter rules exceed [ ] threshold. Reached count of [count] out of [max] in filter [filter-name].
```

次のメッセージは、単一のフィルタで設定されたルールの数が許可されたルールの最大数に達し、それ以上ルールを追加できない場合に生成されます。

```
Reached maximum filter rules. Could not add new rule in filter [filter-name]
```

フィルタリストの syslog メッセージ

設定できるフィルタリストの最大数は256です。設定されているフィルタリストの数がこの制限の 20% 増加するたびに、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in filter [filter-name].
```

設定されているフィルタリストの数が、許可されたフィルタリストの最大数の 95% に達すると、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max]
```

次のメッセージは、設定されているフィルタリストの数が許可されたフィルタリストの最大数に達し、それ以上フィルタリストを追加できない場合に生成されます。

```
Reached maximum filter count. Could not add new filter
```

IP プレフィックスと SGT ベースの SXP フィルタリングの機能情報

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: IP プレフィックスと SGT ベースの SXP フィルタリングの機能情報

機能名	リリース	機能情報
IP プレフィックスと SGT ベースの SXP フィルタリング	Cisco IOS XE Denali 16.1.1	IP プレフィックスと SGT ベースの SXP フィルタリング機能は、高い IP-SGT バイン드의拡張性の問題を解決するためのフィルタリングメカニズムを提供します。 次のコマンドが導入されました： debug cts sxp filter events 、 cts sxp filter-list 、 cts sxp filter-group 、 cts sxp filter-enable 、 show cts sxp filter-group 、 show cts sxp filter-list