SXP IP-Prefix and SGT based Filtering

The Security Group Tag (SGT) Exchange Protocol (SXP) is one of several protocols that supports CTS and is referred to in this document as SXP. SXP is a control protocol for propagating IP to SGT binding information across network devices that do not have the capability to tag packets. SXP passes IP-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn user identity information from access devices.

The SXP IP-Prefix and SGT based Filtering feature allows IP-SGT bindings to be filtered when they are exported or imported. The filtering can be done based on IP prefix, SGT or a combination of both.

Restrictions for SXP IP-Prefix and SGT-based Filtering

- High Availability (HA) is not supported for stateful synchronization of IP-SGT bindings in SXP database between active and standby devices. This is as per the existing behavior on routers and some switches.
- The applied filters to an existing connection takes effect only on the subsequent bindings that are exported/imported. Any bindings that have been imported/exported prior to applying the filters remains untouched.
- There is no VRF-specific filtering, and a filter specified for a peer IP is applicable across all VRFs on the device
- The SGT values taken in the filter rules will be a list of single SGT numbers. SGT ranges are not currently supported.

Information about SXP IP-Prefix and SGT based Filtering

Filtering IP-SGT bindings allows systems to selectively import or export only bindings of interest. In an SXP connection, a filter can be configured on a device that acts either as a speaker or a listener based on the filtering that happens during the export or import of bindings

In case of bi-directional SXP connections, the filters are applied in either of the directions based on whether a speaker or listener filter is configured. If a peer is a part of both the speaker and the listener filter groups, then filtering is applied in both directions.

The filters can be applied either on a peer-to-peer basis or globally (applicable to all SXP connections). In both the cases, the filter can be applied on the speaker or the listener.

How does SXP IP-Prefix and SGT based Filtering Work

A filter that needs to be applied on a device is created with a set of filter rules. Each filter rule specifies the action or actions to be taken for bindings with specific SGT values and/or IP-prefix values. Each binding is matched against the values specified in the filter rules; if a match is found, the corresponding action specified in the filter rule is taken. An action that can be executed on a selected binding is either a permit or a deny .

When a filter is enabled on the speaker or listener during the export or import of IP-SGT bindings, IP-SGT bindings are filtered based on the filter rules. If a rule is not specified for a binding in a filter list, the catch-all rule that is configured in the filter-list is executed. In the absence of a catch-all rule, the corresponding binding is implicitly denied.

Feature Information for SXP IP-Prefix and SGT Based Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Information for SXP IP-Prefix and SGT Based Filtering

Feature Name	Releases	Feature Information
SXP IP-Prefix and SGT Based Filtering	Cisco IOS XE Everest 16.6.1	The SXP IP-Prefix and SGT based Filtering feature allows IP-SGT bindings to be filtered when they are exported or imported. The filtering can be done based on IP prefix, SGT or a combination of both. The following commands were introduced: **cts sxp filter-enable**, **cts sxp filter-group**, **cts sxp filter-list**, **debug cts sxp filter events**, **show cts sxp filter-group**, **show cts sxp filter-list**.

Types of SXP Filtering

IP-SGT bindings are filtered in one of the following ways:

- SGT-based filtering: Filter IP-SGT bindings in an SXP connection based on the SGT value.
- IP-prefix based filtering: Filter IP-SGT bindings in an SXP connection based on the IP-prefix value.
- SGT and IP-prefix based filtering: Filter IP-SGT bindings in an SXP connection based on the SGT value and IP-prefix value.

A filter rule is applied on each of the IP-SGT binding.

How to Configure an SXP Filter

1. **Configure an SXP filter list with filter rules:** In this step, a filter list is created to hold a set of rules. These rules filter the IP-SGT bindings by allowing bindings that are permitted and blocking bindings that are denied. Each rule can be based on SGT, IP prefix or a combination of both.

   If a filter list does not have a rule that matches a specific IP-SGT binding, the binding is implicitly denied unless a default or catch-all ruled is defined.

2. **Configure an SXP filter group:** In this step, a set of peers are grouped and a filter list is applied to the group. A filter-group can be either be defined as a speaker group or listener group. To apply the same filter list to all the speakers or all the listeners, you can create a global speaker filter group or a global listener filter group.

Note Only one filter list can be attached to a filter group.

3. **Enable SXP filtering:** The configured SXP filter list and filter group takes effect only after you enable filtering. Hence, you can configure all the required filters before executing them. You can also temporarily disable filters.

Configuring an SXP Filter List

The **cts sxp filter-list** command is used to create an SXP filter list.

cts sxp filter-list *filter_name*

When you issue this command, the filter lists is created and the device is placed in the filter list configuration mode. In this mode, you can define the filter rules.

A filter rule can be based on SGT or IP Prefix or a combination of both SGT and IP prefix. The command format to add rules to the filter list is a follows:

sequence-number **action(permit/deny) filter-type(ipv4/ipv6/sgt)** *value/values*

Given below is an example for creating a filter list and adding a filter rule:

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# 10 deny ipv4 1.1.1.0/24 permit sgt 100
```

Note that the sequence number is optional. If a sequence number is not mentioned, it is generated by the system. Sequence numbers are automatically incremented by a value of 10 from the last used/configured sequence number. A new rule can be inserted by specifying a sequence number in between two existing rules.

The range of valid SGT values is between 2 and 65519. To provide multiple SGT values in a rule, seperate the values using a space. A maximum of 8 SGT values are allowed in a rule.

In a SGT and IP prefix combination rule, if there is a match for the binding in both the parts of the rule, then the action specified in the second part of the rule takes precedence. For example, in the following rule, if the SGT value of the IP prefix 10.0.0.1 is 20, the corresponding binding will be denied even if the first part of the rule permits the binding.

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

Similarly, in the rule below the binding with the sgt value 20 will be permitted even if the sgt of the IP prefix 10.0.0.1 is 20, and the first action does not permit the binding.

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

Configuring an SXP Filter Group

The **cts sxp filter-group** command is used to create a filter group for grouping a set of devices and applying a filter list to them.

cts sxp filter-group {**listener** | **speaker**} [**global**] {*filter-group-name*]

When you issue this command, the filter group is created and the device is placed in a filter group configuration mode.

From this mode, you can do the following:

- Specify the peers to be grouped.
- Apply a filter list to the filter group.

The command format to add devices or peers to the group is a follows:

peer ipv4 *peer-IP*

In a single command, you can add a maximum a set of eight peers. To add more peers, repeat the command as many times as required.

The command format to apply a filter list to the group is as follows:

filter *filter-list-name*

The following example shows how to create a listener group called group_1 and assign peers to this group:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

The following example shows how to create a global listener group called group_2:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

There won't be a peer list option for the global listener and global speaker filter-group options because in this case the filter is applied for all SXP connections across the box that are either in the listener or speaker mode.

When both the global filter group and peer-based filter groups are applied, the global filter takes priority. If only a global listener or global speaker filter group is configured, then the global filtering takes precendence only in that specific direction. For the other direction, the peer-based filter group is implemented.

Enabling SXP Filtering

The configured SXP filter list and filter groups will take effect only after enabling filtering. The **cts sxp filter-enable** command is used to enable filtering.

cts sxp filter-enable

```
Device(config)# cts sxp filter-enable
```

Configuring the Default or Catch-All Rule

The default or catch-all rule is applied on IP-SGT bindings for which there was no match with any of the rules in the filter list. If a default rule is not specified, these IP-SGT bindings are denied.

Define the default or catch-all rule in the filter-list configuration mode of the corresponding filter list.

The following example shows how to create a default prefix rule that permits bindings corresponding to all IPv4 and IPv6 addresses:

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

```
Device(config-filter-list)# permit ipv4 0.0.0.0/0
Device(config-filter-list)# deny ipv6 00::/0
```

The following example shows how to create a default SGT rule that permits bindings corresponding to all SGTs :

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

Show Commands

show cts sxp filter-list

The **show cts sxp filter-list** command displays the filter lists configured on the box along with the filter rules in each of the filter list. When this command is executed with a filter-list name, only the rules specific to that filter list is displayed.

cts sxp filter-list *filter-list-name*

The following example shows how to display the rules in a filter list:

```
Device# show cts sxp filter-list filter_1
   Filter-name: filter_1
   10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
```

Note The number within round barackets against each rule is the count of the number of times that rule has matched.

The following example shows how to display all the filter lists and their corresponding rules:

```
Device# show cts sxp filter-list
   Filter-name: filter_1 (0)
        10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Filter-name: filter_2 (0)
        10 permit sgt all (0)
        20 deny ipv4 5.5.5.0/24 (0)
        30 deny ipv6 ::/0 (0)
        40 permit ipv6 66:99::88/128 (0)
        50 permit sgt 100 200 300 (0)
        60 deny sgt 99 (0)
        90 permit ipv4 8.8.8.8/32 deny sgt 89 (0)
        100 deny ipv6 1::1/128 permit sgt 90 70 (0)
```

show cts sxp filter-group

The **sxp filter-group** command is used to display information about the configured filter groups along with their corresponding filter list name and peer list.

show cts sxp filter-group [**listener** | **speaker** | {**listener** | **speaker**} *filter-group-name*]
show cts sxp filter-group [**global**] [**detailed**]

The following example shows how to display the details of a specific speaker filter group:

```
Device# show cts sxp filter-group speaker group_1
   Filter-group: group_1
    Filter-name: filter_1
    peer 1.1.1.1
    peer 1.1.1.2
```

Note The number within round barackets against each rule is the count of the number of times that rule has matched.

The following example shows how to display the complete details of all the listener filter groups:

```
Device# show cts sxp filter-group listener detailed
    Global Listener Filter Name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0

    Global Speaker Filter Name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0

    Listener Groups:

    Filter-group: group_1
    Filter-name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0
    peer 1.1.1.1

    Speaker Groups:

    Filter-group: group_3
    peer 1.1.1.1
```

The following example shows how to display the brief details of the global filter group:

```
Device# show cts sxp filter-group global
   Global Listener Filter Name: filter_1
   Global Speaker Filter Name: filter_2
```

Troubleshooting

debug cts sxp filter events

The **debug cts sxp filter events** command is used to log events related to the creation, deletion, update of filter-lists and filter-groups. This command is also used to capture events related to the matching actions in a filtering process.

Syslog Messages for SXP Filtering

Syslog messages for SXP filtering are generated to indicate the various events related to filtering.

Syslog Messages for Filter Rules

The maximum number of rules that can be configured in a single filter is 128. The following message is generated everytime the number of filter rules that is configured in a single filter increases by 20% of this limit:

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

The following message is generated when the number of rules configured in a single filter reaches 95% of the maximum number of rules allowed for a filter list:

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

The following message is generated when the number of rules configured in a single filter reaches the maximum number of allowed rules, and no more rules can be added.

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

Syslog Messages for Filter Lists

The maximum number of filter lists that can be configured is 256. The following message is generated everytime the number of filter lists that is configured increases by 20% of this limit:

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

The following message is generated when the number of filter lists that is configured reaches 95% of the maximum number of allowed filter lists:

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

The following message is generated when the number of filter lists that is configured reaches the maximum number of allowed filter lists, and no more filter lists can be added:

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