SGT Inline Tagging and SXPv4

SGT inline tagging on AP and SXPv4

SGT inline tagging on AP and SXPv4 is a set of Cisco TrustSec enhancements that

- enables secure propagation of scalable group tag (SGT) information across network devices using the SXP protocol
- introduces loop detection in SXP version 4 to prevent stale binding in the network, and
- supports embedding SGTs in clear-text Ethernet packets with inline tagging.

When a wireless client is authenticated by Cisco Identity Services Engine (ISE), the IP-SGT binding is generated on the controller and pushed to the access point along with other client details.

Additional information

Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. CTS uses SGTs and the SXP protocol to securely exchange group information and enhance network segmentation.

For details on SGT inline tagging on the AP and SXP version 4, see the Cisco TrustSec Configuration Guide.

Create an SXP profile

Configuring an SXP profile is essential for enabling Cisco TrustSec features in a wireless environment.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a wireless CTS profile and enter cts-sxp profile configuration mode.

Example:

```
Device(config)# wireless cts-sxp profile profile-name
```

The *profile-name* is the name of the SXP profile being created.

Step 3 Enable SXP for Cisco TrustSec.

Example:

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

The SXP profile is now created and SXP is enabled for Cisco TrustSec.

Configure SGT inline tagging on APs

Enable SGT inline tagging on APs to support dynamic SGT allocation through ISE authentication.

Follow the procedure given below to configure SGT inline tagging on APs.

Before you begin

Ensure that the SGTs pushed to the AP for inline tagging will only be from dynamic SGT allocation through ISE authentication. It is not supported for static bindings configured on the controller . SGTs will be pushed to an AP only when it is operating in flex mode. To know the list of Cisco APs that support SGT inline tagging, see the release notes: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Enters the global configuration mode.

Step 2 Configure a wireless flex profile and enter the wireless flex profile configuration mode.

Example:

```
Device(config)# wireless profile flex flex-profile
```

The *flex-profile* is the name of the wireless flex profile being configured.

Step 3 Enable inline-tagging on the AP.

Example:

```
Device(config-wireless-flex-profile)# cts inline-tagging
```

Enables inline-tagging on the AP.

SGT inline tagging is now configured on the access points, allowing for dynamic SGT allocation.

Configure an SXP connection (GUI)

Configure an SXP (Security Group Tag Exchange Protocol) connection using the graphical user interface (GUI) to enable secure policy exchange between network devices.

Procedure

Step 1 In the **Global** section, select the **SXP Enabled** check box to enable SXP.

Step 2 Enter an IP address in the **Default Source IP** field.

Step 3 Enter a value in the **Reconciliation Period (sec)** field.

Step 4 Enter a value in the **Retry Period (sec)** field.

Step 5 Select the **Set New Default Password** check box. Selecting this check box displays the **Password Type** and **Enter Password** fields.

Step 6 Choose any one of the available types from the **Password Type** drop-down list.

Step 7 Enter a value in the **Enter Password** field.

Step 8 Click the **Apply** button.

Step 9 In the **Peer** section, click the **Add** button.

Step 10 Enter an IP address in the **Peer IP** field.

Step 11 Enter an IP address in the **Source IP** field.

Step 12 Choose any one of the available types from the **Password** drop-down list.

Step 13 Choose any one of the available types from the **Mode of Local Device** drop-down list.

Step 14 Click the **Save & Apply to Device** button.

Step 15 In the **AP** tab, click the **Add** button. The **Add SXP AP** dialog box appears.

Step 16 Enter a name for the profile in the **Profile Name** field.

Step 17 Set the **Status** field to **Enabled** to enable AP.

Step 18 Enter a value in the **Default Password** field.

Step 19 Enter a value (in seconds) for the **CTS Speaker Seconds, CTS Recon Period, CTS Retry Period, CTS Listener Maximum** , and **CTS Listener Minimum**

Step 20 In the **CTS SXP Profile Connections** section, click **Add** .

Step 21 Enter an IP address in the **Peer IP** field.

Step 22 Choose any one of the modes from the **Connection Mode** drop-down list. The available modes are **Both** , **Listener** , and **Speaker** .

Step 23 From the **Password Type** drop-down list, choose either **None** or **Default** .

Step 24 Click the **Add** button.

Step 25 Click the **Save & Apply to Device** button.

You have a fully configured SXP connection, including global settings, peer devices, and AP (Access Point) profiles, ready for secure operation in your network.

Configure an SXP connection

Follow the procedure given below to configure an SXP connection:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 2 Enable CTS SXP support.

Example:

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

Enables CTS SXP support.

Step 3 Configure the CTS-SXP peer address connection.

Example:

```
Device(config)# cts sxp connection peer ipv4-address password password-value mode mode-value
 speaker
```

Configures the CTS-SXP peer address connection.

Note
The password need not be *none* always and the mode can either be Speaker or Listener, or Both.

What to do next

Use the following command to verify the configuration:

```
Device# show running-config | inc sxp
```

Verify SGT push to APs

When a wireless client is connected and authenticated by ISE, the IP-SGT binding is generated on the controller . This can be verified using these commands:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Use this command to verify the SXP connections status:

```
Device# show cts sxp connections

 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 198.51.100.1
Source IP        : 198.51.100.2
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: none
Hold timer is running
Duration since last state change: 0:00:00:06 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

Use this command to see the bindings learnt over SXP connection:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Use these commands on the AP to check the status of inline tagging on the AP and its IP-SGT bindings:

```
AP# show capwap client rcb

AdminState                          : ADMIN_ENABLED
OperationState                      : UP
Name                                : AP2C33.1185.C4D0
SwVer                               : 192.6.230.41
HwVer                               : 1.0.0.0
MwarApMgrIp                         : 192.0.2.38
MwarName                            : test-ewlc
MwarHwVer                           : 0.0.0.0
Location                            : default location
ApMode                              : FlexConnect
ApSubMode                           : Not Configured
CAPWAP Path MTU                     : 1485
CAPWAP UDP-Lite                     : Enabled
IP Prefer-mode                      : IPv4
AP Link DTLS Encryption             : OFF
AP TCP MSS Adjust                   : Disabled
```

```
LinkAuditing                         : disabled
Efficient Upgrade State              : Disabled
Flex Group Name                      : anrt-flex
AP Group Name                        : default-group
Cisco Trustsec Config
      AP Inline Tagging Mode                : Enabled
! The status can be Enabled or Disabled and is based on the tag that is pushed to the AP.
      AP Sgacl Enforcement                  : Disabled
      AP Override Status                    : Disabled


AP# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information
        IP SGT SOURCE
9.3.74.101  17  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1

Active IPv6-SGT Bindings Information
                        IP SGT SOURCE
fe80::c1d5:3da2:dc96:757d  17  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1
```