SGT Inline Tagging and SXPv4

Introduction to SGT Inline Tagging on AP and SXPv4

The Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Scalable Group Tag (SGT) Exchange Protocol (SXP) is one of the several protocols that support CTS. CTS SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection mechanism to prevent stale binding in the network. In addition, Cisco TrustSec supports SGT inline tagging which allows propagation of SGT embedded in clear-text (unencrypted) ethernet packets.

When a wireless client is connected and is authenticated by ISE, the IP-SGT binding is generated on the controller . The same SGT is pushed to the AP along with the other client details.

For more details on SGT inline tagging on the AP and SXPv4, see the **Cisco TrustSec Configuration Guide** at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/sec-usr-cts-xe-3s-book/sec-cts-sxpv4.html

Creating an SXP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless cts-sxp profile** *profile-name* **Example:** `Device(config)# wireless cts-sxp profile rr-profile`	Configures a wireless CTS profile and enters cts-sxp profile configuration mode.
Step 3	**cts sxp enable** **Example:** `Device(config-cts-sxp-profile)# cts sxp enable`	Enables SXP for Cisco TrustSec.

Configuring SGT Inline Tagging on Access Points

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

Before you begin

- 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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a wireless flex profile and enters the wireless flex profile configuration mode.
Step 3	**cts inline-tagging** **Example:** `Device(config-wireless-flex-profile)# cts inline-tagging`	Enables inline-tagging on the AP.

Configuring an SXP Connection (GUI)

Perform the following steps to set SXP global configuration.

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.

Configuring an SXP Connection

Follow the procedure given below to configure an SXP connection:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**cts sxp enable** **Example:** `Device(config)# cts sxp enable`	Enables CTS SXP support.
Step 3	**cts sxp connection peer** *ipv4-address* **password none mode local speaker** **Example:** `Device(config)# cts sxp connection peer 1.1.1.1 password none mode local 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
```

Verifying SGT Push to Access Points

When a wireless client is connected and authenticated by ISE, the IP-SGT binding is generated on the controller . This can be verified using the following 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 the following 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          : 40.1.1.1
Source IP        : 40.1.1.2
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 the following 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 the following 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                               : 16.6.230.41
HwVer                               : 1.0.0.0
MwarApMgrIp                         : 9.3.72.38
MwarName                            : mohit-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
```