Configure Layer 3 CTS with Ingress Reflector

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Network Diagram
Step 1. Setup CTS Layer3 on Egress Interface between SW1 and SW2
Step 2. Enable CTS Ingress Reflector Globally
Verify
 Troubleshoot

Introduction

This document describes how to configure the Layer 3 Cisco TrustSec (CTS) with Ingress Reflector.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of CTS solution.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 6500 Switches with Supervisor Engine 2T on IOS® Release 15.0(01)SY
- IXIA Traffic Generator

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

CTS is an advanced network access control and identity solution to provide end-to-end secure connectivity across Service Providers backbone and Data Center networks.

The Catalyst 6500 switches with Supervisor Engine 2T and 6900 Series line cards provide complete hardware and software support in order to implement CTS. When a Catalyst 6500 is configured with the Supervisor Engine 2T and 6900 Series line cards, the system is fully capable
of providing CTS features.

Since customers would like to continue to use their Catalyst 6500 switches and line cards that already exist while they migrate to a CTS network, and for this reason, Supervisor Engine 2T needs to be compatible with certain line cards that already exist when deployed in a CTS network.

In order to support new CTS functionality such as Security Group Tag (SGT) and IEEE 802.1AE MACsec link encryption, there are dedicated application-specific integrated circuits (ASICs) used on the Supervisor Engine 2T and the new 6900 Series line cards. Ingress reflector mode provides compatibility between legacy line cards that do not use CTS. Ingress reflector mode supports only centralized forwarding, packet forwarding will occur on the PFC of Supervisor Engine 2T. Only 6148 Series or fabric-enabled Centralized Forwarding Card (CFC) line cards such as the 6748-GE-TX line cards are supported. The Distributed Forwarding Card (DFC) Line cards and 10 Gigabit Ethernet line cards are not supported when ingress reflector mode is enabled. With ingress reflector mode configured, non-supported line cards do not power up. Ingress reflector mode is enabled with the use of a global configuration command and requires a system reload.

Configure

Network Diagram

Step 1. Setup CTS Layer3 on Egress Interface between SW1 and SW2

```
SW1(config)#int t1/4/2
SW1(config-if)#ip address 172.16.0.1 255.255.255.0
SW1(config-if)# cts layer3 ipv4 trustsec forwarding
SW1(config-if)# cts layer3 ipv4 policy
SW1(config-if)#no shutdown
SW1(config-if)#exit

SW2(config)#int t1/2
SW2(config-if)#ip address 172.16.0.2 255.255.255.0
SW2(config-if)# cts layer3 ipv4 trustsec forwarding
SW2(config-if)# cts layer3 ipv4 policy
SW2(config-if)#no shutdown
SW2(config-if)#exit
```

Step 2. Enable CTS Ingress Reflector Globally

```
SW1(config)#platform cts ingress
SW1#sh platform  cts
```
CTS Ingress mode enabled

Connect an interface from a NON CTS supported line card to IXIA.

```
SW1#sh run int gi2/4/1
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet2/4/1
no switchport
ip address 10.10.10.1 255.255.255.0
end
```

Assign static SGT in SW1 switch for packets received from the IXIA 1 connected to SW1. Setup permit policy to do CTS L3 only for packets in the desired subnet on authenticator.

```
SW1(config)#cts role-based sgt-map 10.10.10.10 sgt 15
SW1(config)#ip access-list extended traffic_list
SW1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
SW1(config)#cts policy layer3 ipv4 traffic traffic_list
```

**Verify**

Use this section in order to confirm that your configuration works properly.

Verify that the IFC-state is OPEN on both switches. The outputs must look like this:

```
SW1#sh cts int summary

Global Dot1x feature is Enabled
CTS Layer2 Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>IFC-state</th>
<th>dot1x-role</th>
<th>peer-id</th>
<th>IFC-cache</th>
<th>Critical Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/4/1</td>
<td>DOT1X</td>
<td>OPEN</td>
<td>Supplic</td>
<td>SW2</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
<tr>
<td>Te1/4/4</td>
<td>MANUAL</td>
<td>OPEN</td>
<td>unknown</td>
<td>unknown</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
<tr>
<td>Te1/4/5</td>
<td>DOT1X</td>
<td>OPEN</td>
<td>Authent</td>
<td>SW2</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
<tr>
<td>Te1/4/6</td>
<td>DOT1X</td>
<td>OPEN</td>
<td>Supplic</td>
<td>SW2</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
<tr>
<td>Te2/3/9</td>
<td>DOT1X</td>
<td>OPEN</td>
<td>Supplic</td>
<td>SW2</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
</tbody>
</table>

CTS Layer3 Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv4 encap</th>
<th>IPv6 encap</th>
<th>IPv4 policy</th>
<th>IPv6 policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/4/2</td>
<td>OPEN</td>
<td>OPEN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SW2#sh cts int summary

Global Dot1x feature is Enabled
CTS Layer2 Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>IFC-state</th>
<th>dot1x-role</th>
<th>peer-id</th>
<th>IFC-cache</th>
<th>Critical-Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/1</td>
<td>DOT1X</td>
<td>OPEN</td>
<td>Authent</td>
<td>SW1</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
<tr>
<td>Te1/4</td>
<td>MANUAL</td>
<td>OPEN</td>
<td>unknown</td>
<td>unknown</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
<tr>
<td>Te1/5</td>
<td>DOT1X</td>
<td>OPEN</td>
<td>Supplic</td>
<td>SW1</td>
<td>invalid</td>
<td>Invalid</td>
</tr>
</tbody>
</table>
```
CTS Layer3 Interfaces
---------------------
<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv4 encap</th>
<th>IPv6 encap</th>
<th>IPv4 policy</th>
<th>IPv6 policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/2</td>
<td>OPEN</td>
<td>----------</td>
<td>OPEN</td>
<td>------------</td>
</tr>
</tbody>
</table>

Verify through Netflow Output

Netflow can be configured with these commands:

```
SW2(config)#flow record rec2
SW2(config-flow-record)#match ipv4 protocol
SW2(config-flow-record)#match ipv4 source address
SW2(config-flow-record)#match ipv4 destination address
SW2(config-flow-record)#match transport source-port
SW2(config-flow-record)#match transport destination-port
SW2(config-flow-record)#match flow direction
SW2(config-flow-record)#match flow cts source group-tag
SW2(config-flow-record)#match flow cts destination group-tag
SW2(config-flow-record)#collect routing forwarding-status
SW2(config-flow-record)#collect counter bytes
SW2(config-flow-record)#collect counter packets
SW2(config-flow-record)#exit
```

```
SW2(config)#flow monitor mon2
SW2(config-flow-monitor)#record rec2
SW2(config-flow-monitor)#exit
```

Apply netflow on the ingress port of SW2 switch interface as shown:

```
SW2#  sh run int t1/2
Building configuration...
Current configuration : 166 bytes
!
interface TenGigabitEthernet1/2
 ip address 172.16.0.2 255.255.255.0
 ip flow monitor mon2 input
 cts layer3 ipv4 trustsec forwarding
 cts layer3 ipv4 policy
end
```

Send packets from IXIA 1 to IXIA 2. It must be received properly on IXIA 2 connected to the SW2 switch according to the traffic policy. Ensure that the packets are SGT tagged.
There are no cache entries to display.

Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 4:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 2:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 1:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 4

IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  FLOW DIRN  FLOW CTS SRC GROUP
TAG  FLOW CTS DST GROUP TAG  IPPROT  ip fwd status                  bytes        pkts
===============  ===============  =============  =============  =========  =========  ===========  =========  =========  =========  =========  ===========  =========  =========  =========
---
1.1.1.10         2.2.2.10                     0              0  Input
10                       0      255  Unknown                       148121702     3220037
10.10.10.10      10.10.20.10                  0              0  Input
15                       0      255  Unknown                       23726754      515799
10.10.10.1       224.0.0.5                    0              0  Input
2                       0       89  Unknown                       9536          119
172.16.0.1       224.0.0.5                    0              0  Input
0                       0       89  Unknown                       400           5

Now, setup exception policy to skip CTS L3 for packets to a specific IP address in Authenticator switch.

SW2#sh flow monitor mon2 cache format  table
Cache type: Normal
Cache size: 4096
Current entries: 0
High Watermark: 0
Flows added: 0
Flows aged: 0
- Active timeout ( 1800 secs) 0
- Inactive timeout ( 15 secs) 0
- Event aged 0
- Watermark aged 0
- Emergency aged 0

There are no cache entries to display.

Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 4:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 2:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 1:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 4

<table>
<thead>
<tr>
<th>IPV4 SRC ADDR</th>
<th>IPV4 DST ADDR</th>
<th>TRNS SRC PORT</th>
<th>TRNS DST PORT</th>
<th>FLOW DIRN</th>
<th>FLOW CTS SRC GROUP</th>
<th>TAG</th>
<th>FLOW CTS DST GROUP</th>
<th>TAG</th>
<th>IPPROT</th>
<th>ip fwd status</th>
<th>bytes</th>
<th>pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.10</td>
<td>2.2.2.10</td>
<td>0</td>
<td>0</td>
<td>Input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>148121702</td>
<td>3220037</td>
</tr>
</tbody>
</table>

10.10.10.10  10.10.20.10  0  0  Input
15  0  255  Unknown  23726754  515799
10.10.10.1  224.0.0.5  0  0  Input
2  0  89  Unknown  9536  119
172.16.0.1  224.0.0.5  0  0  Input
0  0  89  Unknown  400  5

SW2#sh flow monitor mon2 cache format table
Cache type: Normal
Cache size: 4096
Current entries: 0
High Watermark: 0

Flows added: 0
Flows aged:
- Active timeout (1800 secs) 0
- Inactive timeout (15 secs) 0
- Event aged 0
- Watermark aged 0
- Emergency aged 0

There are no cache entries to display.

Module 4:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.
Current entries: 0

There are no cache entries to display.

Module 2:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

There are no cache entries to display.

Module 1:
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 3

IPV4 SRC ADDR IPV4 DST ADDR TRNS SRC PORT TRNS DST PORT FLOW DIRN FLOW CTS SRC GROUP TAG FLOW CTS DST GROUP TAG IP PROT ip fwd status bytes pkts
===============  ===============  =============  =============  =========  =========  =========  =========  =========  =========  =========  =========  =========  =========  =========
1.1.1.10         2.2.2.10                     0              0  Input   10 255 Unknown                        1807478       39293
10.10.10.10      10.10.20.10                  0              0  Input   0       0 255 Unknown                        1807478       39293
10.10.10.1       224.0.0.5                    0              0  Input   2 0 89 Unknown                        1807478       39293

Send packets from IXIA 1 to IXIA 2. They must be received properly on IXIA 2 connected to the SW2 switch according to the exception policy.

**Note:** The packets are not SGT tagged because the exception policy takes precedence FLOW CTS SRC GROUP TAG=0.

**Troubleshoot**

There is currently no specific troubleshooting information available for this configuration.