Configure and Verify Egress Reflector with CTS Manual

Contents

Introduction

This document describes how to configure and verify a Cisco TrustSec (CTS) with Egress 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 identity-enabled network access architecture that helps customers to enable secure collaboration, strengthen security, and address compliance requirements. It also provides a scalable role based policy enforcement infrastructure. Packets are tagged based on the group membership of the packet source at the ingress of the network. Policies associated with the group

are applied as these packets traverse the network.

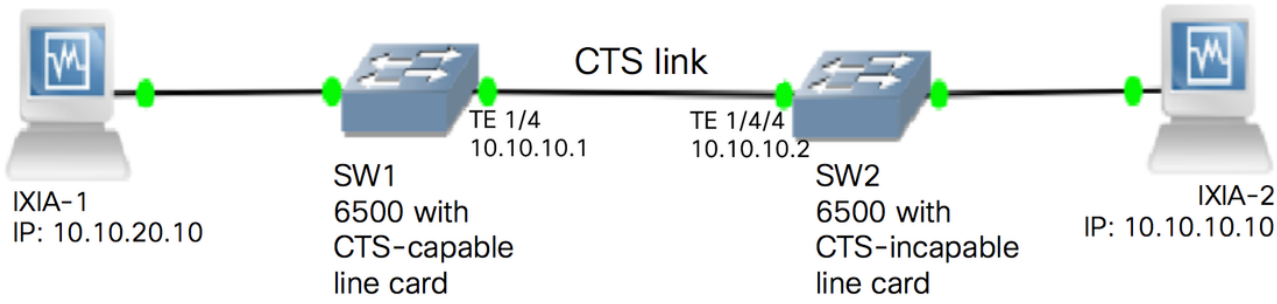
The Catalyst 6500 series switches with supervisor engine 2T and 6900 series line cards provide complete hardware and software support for implementing CTS. In order to support the CTS functionality, there are dedicated Application Specific Integrated Circuits (ASICs) used on the new 6900 Series line cards. Legacy line cards do not have these dedicated ASICs and therefore, do not support CTS.

CTS reflector uses Catalyst Switch Port Analyzer (SPAN) to reflect traffic from a CTS-incapable switching module to the supervisor engine for Security Group Tag (SGT) assignment and insertion.

A CTS egress reflector is implemented on a distribution switch with Layer 3 uplinks, where the CTS-incapable switching module faces an access switch. It supports Centralized Forwarding Cards (CFCs) and Distributed Forwarding Cards (DFCs).

Configure

Network Diagram



Configure SW1

Configure CTS manual on the uplink to SW2 with these commands:

```
SW1(config)#int t1/4
SW1(config-if)#ip address 10.10.10.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#cts manual
SW1(config-if-cts-manual)#propagate sgt
SW1(config-if-cts-manual)#policy static sgt 11 trusted
SW1(config-if-cts-manual)#exit
SW1(config-if)#exit
```

Configure SW2

Enable egress reflector on the switch with these commands:

```
SW2(config)#platform cts egress
SW2#write memory
Building configuration...
[OK] SW2#reload
```

Note: The switch has to be reloaded in order to enable the egress reflector mode.

Configure CTS Manual on the port connected to SW1 with these commands:

```
SW2(config)#int t1/4/4
SW2(config-if)#ip address 10.10.10.2 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#cts manual
SW2(config-if-cts-manual)#propagate sgt
SW2(config-if-cts-manual)#policy  static sgt 10 trusted
SW2(config-if-cts-manual)#exit
SW2(config-if)#exit
```

Configure a static SGT on SW2 for the source IP address 10.10.10.10 from IXIA.

```
SW2(config)#cts role-based sgt-map 10.10.10.10 sgt 11
```

Verify

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

The current CTS mode can be viewed with this command:

```
SW2#show platform cts
 CTS Egress mode enabled
```

The CTS link state can be viewed with this command:

```
show cts interface summary
```

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

```
SW1#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
------------------------------------------------------------------------------
Te1/4      MANUAL  OPEN      unknown    unknown    invalid      Invalid

SW2#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
------------------------------------------------------------------------------
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid      Invalid
```

Verify through Netflow Output

Netflow can be configured with these commands:

```
SW2#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
-------------------------------------------------------------------------------
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid      Invalid
```

Apply Netflow on the ingress interface of SW1 switch:

```
SW2#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
-------------------------------------------------------------------------------
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid      Invalid
```

Verify that the incoming packets are SGT tagged on SW1 Switch.

```
SW1#show 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 35:
  Cache type:                               Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                               0

There are no cache entries to display.

Module 34:
```

```
  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 33:
  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 20:
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               2

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
===============  ===============  =============  =============  =========
====================  ====================  =======  =============  ==========  ==========
10.10.10.10      10.10.20.10                   0              0  Input
11                       0      255  Unknown        375483970     8162695
10.10.10.2       224.0.0.5                     0              0  Input
4                        0       89  Unknown         6800          85

Module 19: Cache type: Normal (Platform cache) Cache size: Unknown Current entries: 0 There are
no cache entries to display. Module 18: 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
```

Troubleshoot

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