使用CTS手動配置和驗證出口反射器

目錄

簡介

本文說明如何設定和驗證具有輸出反射器的Cisco TrustSec(CTS)。

必要條件

需求

思科建議您瞭解CTS解決方案的基本知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IOS版本15.0(01)SY上搭載Supervisor引擎2T的Catalyst 6500交換器
- IXIA流量產生器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

CTS是一種支援身份的網路訪問架構，可幫助客戶實現安全合作、增強安全性和滿足合規性要求。它還提供可擴展的基於角色的策略實施基礎架構。封包是根據封包來源在網路入口處的群組成員身分來標籤。當這些資料包通過網路時，將應用與組關聯的策略。

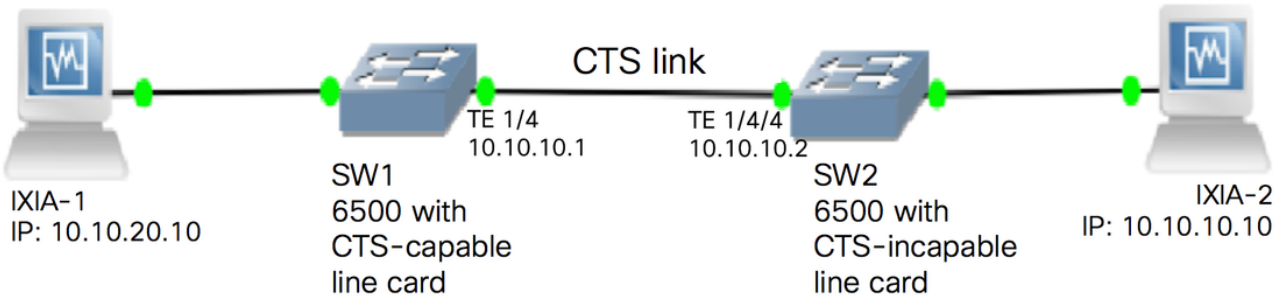
配備管理引擎2T和6900系列線卡的Catalyst 6500系列交換機為實施CTS提供完整的硬體和軟體支援。為了支援CTS功能，新的6900系列線卡上使用了專用應用專用積體電路(ASIC)。傳統線卡沒有這些專用ASIC，因此不支援CTS。

CTS反射器使用Catalyst交換器連線埠分析器(SPAN)將流量從無CTS的交換模組反射到Supervisor引擎，以進行安全群組標籤(SGT)指派和插入。

在具有第3層上行鏈路的分佈交換機上實現CTS出口反射器，其中，不支援CTS的交換模組面向接入交換機。它支援集中轉發卡(CFC)和分散式轉發卡(DFC)。

設定

網路圖表



配置SW1

使用以下命令在通往SW2的上行鏈路上配置CTS手冊：

```
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
```

配置SW2

使用以下命令在交換器上啟用輸出反射器：

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

附註：必須重新載入交換器，才能啟用輸出反射器模式。

使用以下命令在連線到SW1的埠上配置CTS Manual:

```
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
```

在SW2上為來自IXIA的源IP地址10.10.10.10配置靜態SGT。

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

驗證

使用本節內容，確認您的組態是否正常運作。

可以使用以下命令檢視當前CTS模式：

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

使用以下命令可以檢視CTS鏈路狀態：

```
show cts interface summary
```

檢驗兩台交換機上的IFC狀態是否為OPEN。輸出應如下所示：

```
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
```

通過Netflow輸出驗證

可以使用以下命令配置Netflow:

```
SW1(config)#flow record rec2
SW1(config-flow-record)#match ipv4 protocol
SW1(config-flow-record)#match ipv4 source address
SW1(config-flow-record)#match ipv4 destination address
SW1(config-flow-record)#match transport source-port
SW1(config-flow-record)#match transport destination-port
```

```
SW1(config-flow-record)#match flow direction
SW1(config-flow-record)#match flow cts source group-tag
SW1(config-flow-record)#match flow cts destination group-tag
SW1(config-flow-record)#collect routing forwarding-status
SW1(config-flow-record)#collect counter bytes
SW1(config-flow-record)#collect counter packets
SW1(config-flow-record)#exit
SW1(config)#flow monitor mon2
SW1(config-flow-monitor)#record rec2
SW1(config-flow-monitor)#exit
```

將Netflow套用在SW1交換器的輸入介面上：

```
SW1#sh run int t1/4
Building configuration...

Current configuration : 165 bytes
!
interface TenGigabitEthernet1/4
 no switchport
 ip address 10.10.10.1 255.255.255.0
 ip flow monitor mon2 input
 cts manual
  policy static sgt 11 trusted
end
```

驗證傳入資料包是否在SW1交換機上標籤SGT。

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。