使用輸入反射器設定第3層CTS

目錄

簡介

本檔案介紹如何使用輸入反射器設定第3層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：

- 採用Supervisor Engine 2T的Catalyst 6500交換器(IOS®版本15.0(01)SY)
- 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是一種高級網路訪問控制和身份解決方案，可在服務提供商骨幹網和資料中心網路之間提供端到端安全連線。

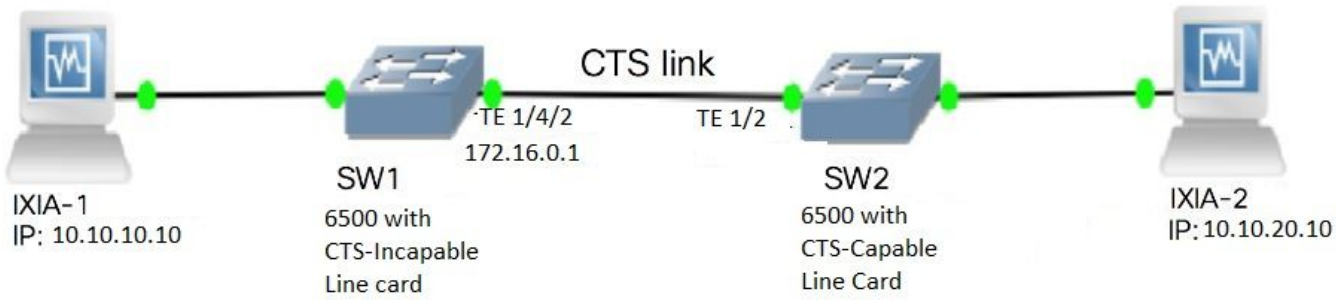
搭載Supervisor Engine 2T和6900系列線路卡的Catalyst 6500交換器提供完整的硬體和軟體支援，以實作CTS。當Catalyst 6500配置管理引擎2T和6900系列線卡時，系統完全能夠提供CTS功能。

由於客戶希望繼續使用遷移到CTS網路時已經存在的Catalyst 6500交換機和線卡，因此，Supervisor Engine 2T需要與部署在CTS網路中時已經存在的特定線卡相容。

為了支援新的CTS功能，例如安全群組標籤(SGT)和IEEE 802.1AE MACsec連結加密，Supervisor Engine 2T和新的6900系列線路卡上使用專用應用程式專屬積體電路(ASIC)。輸入反射器模式在不使用CTS的舊版線卡之間提供相容性。入口反射器模式僅支援集中轉發，資料包轉發將在Supervisor引擎2T的PFC上發生。僅支援6148系列或支援交換矩陣的集中轉發卡(CFC)線卡，如6748-GE-TX線卡。啟用輸入反射器模式時，不支援分散式轉送卡(DFC)線路卡和10 Gigabit乙太網路線路卡。配置了輸入反射器模式後，不支援的線卡不能通電。輸入反射器模式是透過使用全域組態命令來啟用，且需要重新載入系統。

設定

網路圖表



步驟1.在SW1和SW2之間的出口介面上設定CTS第3層

- ```
  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
  ```

步驟2.全域性啟用CTS輸入反射器

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

將介面從非CTS支援的線卡連線到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
```

在SW1交換機中為從連線到SW1的IXIA 1收到的資料包分配靜態SGT。設定允許策略僅對身份驗證器上所需子網中的資料包執行CTS L3。

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

檢驗兩台交換機上的IFC狀態是否為OPEN。輸出必須如下所示：

```
SW1#sh cts int summary

Global Dot1x feature is Enabled
CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical Authentication
-------------------------------------------------------------------------------
Te1/4/1    DOT1X   OPEN      Supplic    SW2        invalid  Invalid
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/4/5    DOT1X   OPEN      Authent    SW2        invalid  Invalid
Te1/4/6    DOT1X   OPEN      Supplic    SW2        invalid  Invalid
Te2/3/9    DOT1X   OPEN      Supplic    SW2        invalid  Invalid

CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
Te1/4/2     OPEN             ----------       OPEN             -----------

SW2#sh cts int summary
Global Dot1x feature is Enabled
CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
-------------------------------------------------------------------------------
Te1/1      DOT1X   OPEN      Authent    SW1         invalid     Invalid
Te1/4      MANUAL  OPEN      unknown    unknown     invalid     Invalid
Te1/5      DOT1X   OPEN      Supplic    SW1         invalid     Invalid
Te1/6      DOT1X   OPEN      Authent    SW1         invalid     Invalid
Te4/5      DOT1X   OPEN      Authent    SW1         invalid     Invalid

CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
-------------------------------------------------------------------------------
Te1/2       OPEN             ----------       OPEN             -----------
```

通過Netflow輸出驗證

可以使用以下命令配置Netflow:

```
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
```

將netflow應用於SW2交換機介面的輸入埠，如下所示：

```
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
```

將資料包從IXIA 1傳送到IXIA 2。根據流量策略，必須在連線到SW2交換機的IXIA 2上正確接收該資料包。確保資料包帶有SGT標籤。

```
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

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
```

現在，設定例外策略以跳過CTS L3，將資料包跳至身份驗證器交換機中的特定IP地址。

```
SW1(config)#ip access-list extended exception_list
SW1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
SW1(config)#cts policy layer3 ipv4 exception exception_list
```

```
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:                               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                       0      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                          164           2
```

將資料包從IXIA 1傳送到IXIA 2。根據異常策略，必須在連線到SW2交換機的IXIA 2上正確接收這些資料包。

> **附註**：由於異常策略優先使用FLOW CTS SRC GROUP TAG=0，因此未對資料包進行SGT標籤。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。