

配置第3层CTS用入口反射器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[步骤1. 设置在出口接口的CTS第3层SW1和SW2之间](#)

[步骤2. Enable \(event\) CTS全局入口反射器](#)

[验证](#)

[故障排除](#)

简介

本文描述如何配置第3层思科TrustSec (CTS)用入口反射器。

先决条件

要求

思科建议您有CTS解决方案基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 6500交换机用在IOS®版本15.0(01)SY的Supervisor引擎2T
- 鸢尾属数据流生成器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

CTS是提供在间服务提供商骨干网和数据中心网络的端到端安全连接的高级网络访问控制和标识解决方案。

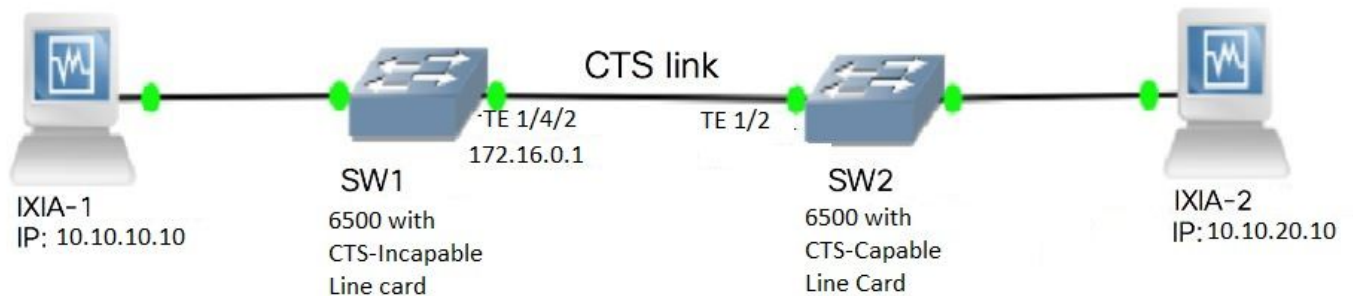
Catalyst 6500交换机用Supervisor引擎2T和6900系列线卡提供完整硬件和软件支持为了实现CTS。当Catalyst 6500配置与Supervisor引擎2T和6900系列线卡时，系统充分地能够提供CTS功能。

因为客户希望继续使用已经存在的他们的Catalyst 6500交换机和线卡，当他们移植到CTS网络，和为此时，Supervisor引擎2T需要是与在CTS网络已经存在，当部署的某些线卡兼容。

为了支持新建的CTS功能例如安全组标记(SGT)和IEEE 802.1AE MACsec链路加密，有在Supervisor引擎2T和新的6900系列线卡(ASIC)使用的投入的专用集成电路。入口反射器模式提供在不使用CTS的传统线卡之间的兼容性。入口反射器模式在Supervisor引擎2T PFC支持仅集中化转发，信息包转发将发生。例如6748-GE-TX线卡支持只6148系列或支持结构的集中化转发卡(CFC)线卡。不支持分布式转发卡(DFC)线卡和万兆以太网线卡，当入口反射器模式启用时。当入口反射器模式配置，不支持的线卡不启动。入口反射器模式启用与使用全局配置命令并且要求系统重新加载。

配置

网络图



步骤1.设置在出口接口的CTS第3层SW1和SW2之间

- ```

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

```

### 步骤2. Enable (event) CTS全局入口反射器

```

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

```

连接从NON CTS支持的线路卡的一个接口到鸢尾属。

```

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

```

为从鸢尾属接收的数据包分配在SW1交换机的静态SGT 1连接到SW1。设置要执行数据包的仅CTS的permit策略L3在验证器的希望的子网。

```

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

```

## 验证

使用本部分可确认配置能否正常运行。

验证Ifc状态是开放的在两交换机。输出必须如下所示:

```
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 -----

```

## 通过NetFlow输出验证

Netflow可以用这些命令配置：

```
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
```

应用在SW2交换机接口入站端口的Netflow如显示：

```
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
```

发送从鸢尾属1的数据包对鸢尾属2。在根据数据流策略2必须适当地接收它连接的对SW2交换机鸢尾属。保证是SGT被标记的数据包。

```
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 TAG           | SRC ADDR FLOW CTS | IPV4 DST ADDR DST GROUP | TRNS SRC PORT IP     | TRNS DST PORT | FLOW DIRN       | FLOW CTS     | SRC GROUP     |
|--------------------|-------------------|-------------------------|----------------------|---------------|-----------------|--------------|---------------|
|                    |                   |                         | IPPROT ip fwd status |               | bytes           |              | pkts          |
| 1.1.1.10           |                   | 2.2.2.10                |                      | 0             | 0               | Input        |               |
| 10                 |                   | 0                       | 255 Unknown          |               | 148121702       |              | 3220037       |
| <b>10.10.10.10</b> |                   | <b>10.10.20.10</b>      |                      | <b>0</b>      | <b>0</b>        | <b>Input</b> |               |
| <b>15</b>          |                   | <b>0</b>                | <b>255 Unknown</b>   |               | <b>23726754</b> |              | <b>515799</b> |
| 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             |

现在，跳过数据包的CTS的设置的例外策略L3对在验证器交换机的一个特定IP地址。

```
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 TAG  | IPV4 DST ADDR CTS DST GROUP | TRNS SRC PORT IPPROT | TRNS DST PORT ip fwd status | FLOW DIRN bytes | FLOW CTS SRC GROUP pkts |
|--------------------|-----------------------------|----------------------|-----------------------------|-----------------|-------------------------|
| 1.1.1.10           | 2.2.2.10                    |                      | 0                           | 0 Input         |                         |
| 10                 | 0                           | 255                  | Unknown                     | 148121702       | 3220037                 |
| <b>10.10.10.10</b> | <b>10.10.20.10</b>          | <b>0</b>             | <b>255 Unknown</b>          | <b>0 Input</b>  |                         |
| <b>15</b>          | <b>0</b>                    | <b>255</b>           | <b>Unknown</b>              | <b>23726754</b> | <b>515799</b>           |
| 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: 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 TAG           | SRC ADDR FLOW CTS | IPV4 DST ADDR DST GROUP TAG | TRNS SRC PORT IP PROT | TRNS DST PORT ip fwd status | FLOW DIRN bytes | FLOW CTS SRC GROUP pkts |
|--------------------|-------------------|-----------------------------|-----------------------|-----------------------------|-----------------|-------------------------|
| 1.1.1.10           |                   | 2.2.2.10                    |                       | 0                           | 0               | Input                   |
| 10                 |                   | 0                           | 255                   | Unknown                     |                 | 1807478 39293           |
| <b>10.10.10.10</b> |                   | <b>10.10.20.10</b>          |                       | <b>0</b>                    | <b>0</b>        | <b>Input</b>            |
| <b>0</b>           |                   | <b>0</b>                    | <b>255</b>            | <b>Unknown</b>              |                 | <b>1807478 39293</b>    |
| 10.10.10.1         |                   | 224.0.0.5                   |                       | 0                           | 0               | Input                   |
| 2                  |                   | 0                           | 89                    | Unknown                     |                 | 164 2                   |

发送从鸢尾属1的数据包对鸢尾属2。在根据例外策略2必须适当地接收他们连接的对SW2交换机鸢尾属。

**Note:**因为例外策略采取优先流CTS SRC组TAG=0，不是SGT被标记的数据包。

## 故障排除

目前没有针对此配置的故障排除信息。