

配置并且验证有Cts manual的出口反射器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置SW1](#)

[配置SW2](#)

[验证](#)

[故障排除](#)

简介

本文描述如何配置和验证思科TrustSec (CTS)用出口反射器。

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是帮助客户启用安全协作，加强安全和解决标准需求的标识启用的网络访问体系结构。它也提供一个可扩展角色基于策略执行基础设施。根据信息包来源的组成员是标记为的数据包在网络的入口。当这些数据包穿程网络，策略关联与组应用。

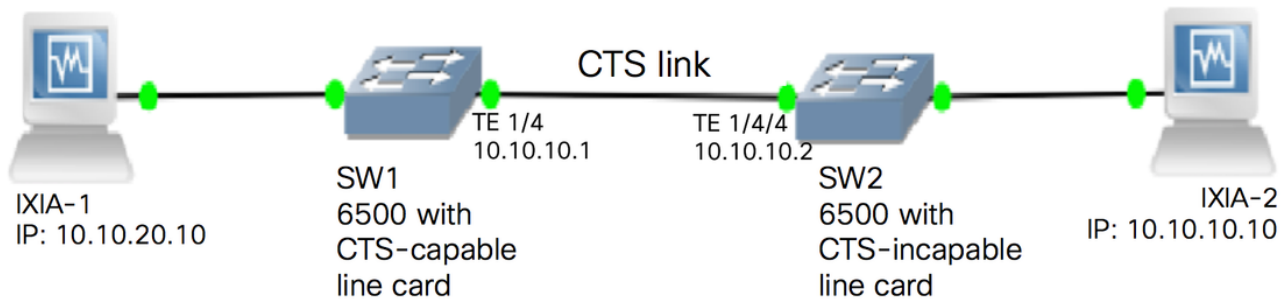
Catalyst 6500系列交换机用Supervisor引擎2T和6900系列线卡为实现CTS提供完整硬件和软件支持。为了支持CTS功能，有在新的6900系列线卡(ASIC)使用的投入的特殊用途的集成电路。传统线卡没有这些专用的ASIC并且，请勿支持CTS。

CTS反射器用途反射从一个CTS不能胜任的交换模块的流量的Catalyst交换机端口分析器(SPAN)到安全组标记(SGT)分配和插入的Supervisor引擎。

CTS出口反射器在有第3层uplink端口的一台分布式交换机实现，CTS不能胜任的交换模块面对接入交换机。它支持集中化转发卡(CFCs)和分布式转发卡(DFCs)。

配置

网络图



配置SW1

配置在上行链路的Cts manual对SW2用这些命令：

```
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

启用在交换机的出口反射器用这些命令：

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

Note:交换机必须重新加载为了启动出口反射器模式。

配置在端口的Cts manual连接对SW1用这些命令：

```
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
```

配置在SW2的一静态SGT从鸢尾属的源IP地址的10.10.10.10。

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

验证

使用本部分可确认配置能否正常运行。

当前CTS模式可以用此命令查看：

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

CTS链路状态可以用此命令查看：

```
show cts interface summary
```

验证Ifc状态是开放的在两交换机。输出如下所示：

```
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 |

通过NetFlow输出验证

Netflow可以用这些命令配置：

```
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 |

应用在SW1交换机入口接口的Netflow :

```
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 |

验证在SW1交换机是SGT标记的流入数据包。

```
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

故障排除

目前没有针对此配置的故障排除信息。