使用CTS手册配置和验证出口反射器

目录

简介

本文档介绍如何配置和验证具有出口反射器的思科TrustSec(CTS)。

先决条件

要求

思科建议您具备CTS解决方案的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 在IOS版本15.0(01)SY上具有管理引擎2T的Catalyst 6500交换机
- IXIA流量生成器

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是一种支持身份的网络访问架构，可帮助客户实现安全协作、增强安全性并满足合规性要求。它还提供基于角色的可扩展策略实施基础设施。根据网络入口处数据包源的组成员身份标记数据包。当这些数据包通过网络时，会应用与组关联的策略。

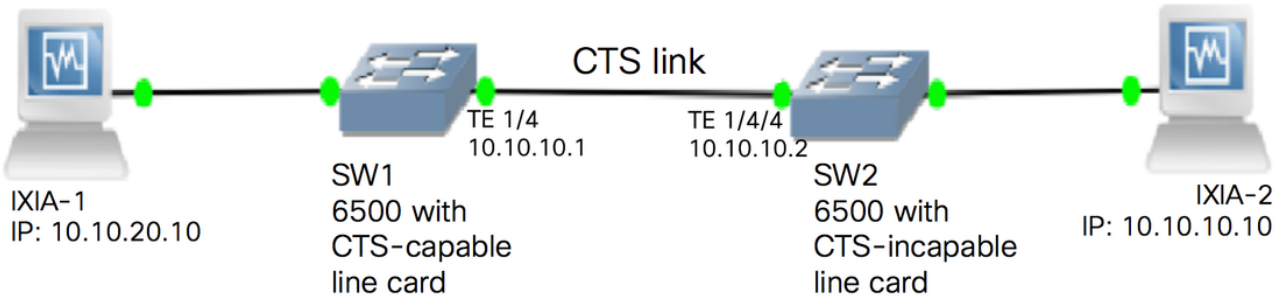
Catalyst 6500系列交换机配备管理引擎2T和6900系列线卡，为实施CTS提供完整的硬件和软件支持。为了支持CTS功能，新的6900系列线卡上使用专用专用专用集成电路(ASIC)。传统线卡没有这些专用ASIC，因此不支持CTS。

CTS反射器使用Catalyst交换机端口分析器(SPAN)将流量从不支持CTS的交换模块反射到管理引擎，以进行安全组标记(SGT)分配和插入。

CTS出口反射器在具有第3层上行链路的分布层交换机上实施，其中不支持CTS的交换模块面对接入交换机。它支持集中转发卡(CFC)和分布式转发卡(DFC)。

配置

网络图



配置SW1

使用以下命令在通往SW2的上行链路上配置CTS手动：

```
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

使用以下命令在交换机上启用出口反射器：

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

注意：必须重新加载交换机才能启用出口反射器模式。

使用以下命令在连接到SW1的端口上配置CTS手册：

```
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上为来自IXIA的源IP地址10.10.10.10配置静态SGT。

```
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。

可使用以下命令查看当前CTS模式：

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

可使用以下命令查看CTS链路状态：

```
show cts interface summary
```

验证两台交换机上的IFC状态都为OPEN。输出应如下所示：

```
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

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
```

在SW1交换机的入口接口上应用Netflow:

```
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
```

验证SW1交换机上的传入数据包是否已标记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
```

故障排除

目前没有针对此配置的故障排除信息。