配置并且验证第3层思科TrustSec用入口反射器

目录

简介

本文描述第3层与入口反射器配置和验证的思科TrustSec (CTS)。

先决条件

要求

思科建议您有思科TrustSec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系列线卡为实现CTS提供完整硬件和软件支持。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。

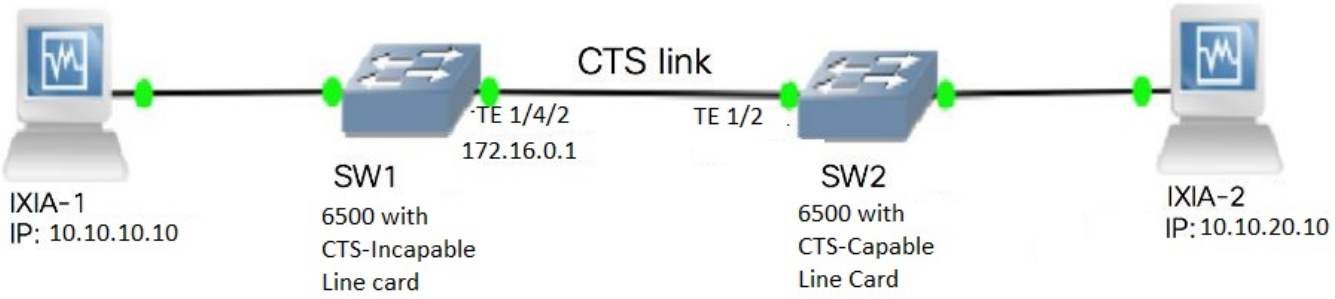
因为客户希望继续使用他们的现有Catalyst 6500交换机和线卡，当转移到CTS网络和为此时

Supervisor引擎2T在CTS网络需要是与某些现有的线路卡兼容，当部署。

要支持新建的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传统线卡之间的兼容性不能够使用CTS。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CFC (集中化转发卡)线卡。不支持DFC (分布式转发卡)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，不支持的线卡不会启动。入口反射器模式启用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

1. ```
   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             -----------
```

验证通过NetFlow输出

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。注意是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 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
```

现在请设置例外策略跳过数据包的CTS L3到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    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
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
```

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。

注意：请注意:，因为例外策略采取precedence.FLOW 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。