使用入口反射器配置第3层CTS

目录

简介

本文档介绍如何使用入口反射器配置第3层思科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：

- IOS®版本15.0(01)SY上带管理引擎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是一种高级网络访问控制和身份解决方案，可跨服务提供商主干和数据中心网络提供端到端安全连接。

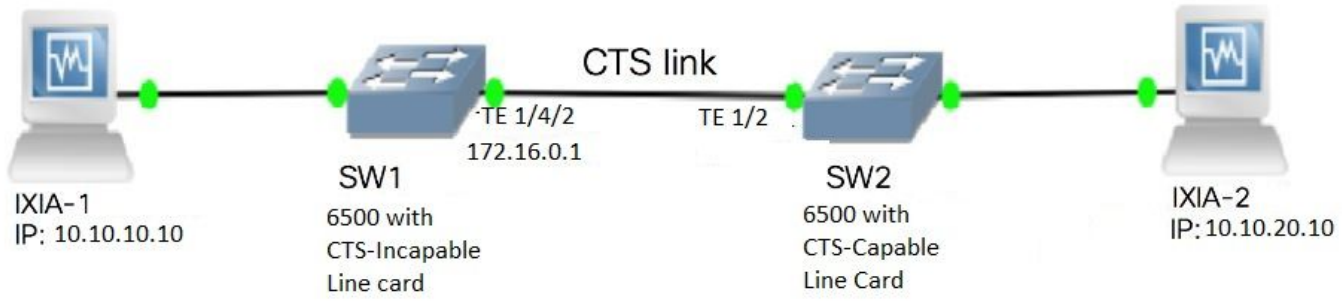
配备管理引擎2T和6900系列线卡的Catalyst 6500交换机提供完整的硬件和软件支持，以实施CTS。当Catalyst 6500配置了Supervisor引擎2T和6900系列线卡时，系统完全能够提供CTS功能。

由于客户希望继续使用其Catalyst 6500交换机和迁移到CTS网络时已存在的线卡，因此，Supervisor引擎2T需要与部署在CTS网络中时已存在的某些线卡兼容。

为了支持新的CTS功能，如安全组标记(SGT)和IEEE 802.1AE MACsec链路加密，Supervisor引擎2T和新的6900系列线卡上使用专用专用专用集成电路(ASIC)。入口反射器模式提供不使用CTS的传统线卡之间的兼容性。入口反射器模式仅支持集中转发，数据包转发将在Supervisor引擎2T的PFC上进行。仅支持6148系列或交换矩阵型集中转发卡(CFC)线卡，例如6748-GE-TX线卡。启用入口反射器模式时，不支持分布式转发卡(DFC)线卡和万兆以太网线卡。配置入口反射器模式后，不支持的线卡不会通电。入口反射器模式使用全局配置命令启用，需要系统重新加载。

配置

网络图



步骤1.在SW1和SW2之间的出口接口上设置CTS第3层

-

```
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.全局启用CTS入口反射器

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

将接口从NON CTS支持的线卡连接到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
```

为从连接到SW1的IXIA 1接收的数据包在SW1交换机中分配静态SGT。设置允许策略仅对身份验证器上所需子网中的数据包执行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
```

验证

使用本部分可确认配置能否正常运行。

验证两台交换机上的IFC状态都为OPEN。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

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
```

在SW2交换机接口的入口端口上应用netflow，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
```

从IXIA 1向IXIA 2发送数据包。必须根据流量策略在连接到SW2交换机的IXIA 2上正确接收数据包。确保数据包已标记为SGT。

```
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，设置异常策略以跳过CTS L3，将数据包发送到身份验证器交换机中的特定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
```

将数据包从IXIA 1发送到IXIA 2。必须根据例外策略在连接到SW2交换机的IXIA 2上正确接收数据包。

> **注意**：由于异常策略优先于FLOW CTS SRC GROUP TAG=0，因**此未对数据包进行SGT标记。**

故障排除

目前没有针对此配置的故障排除信息。