Configurar a camada 3 CTS com refletor do ingresso

Índice

Introdução

Este documento descreve como configurar a camada 3 Cisco TrustSec (CTS) com refletor do ingresso.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico da solução CTS.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Os Catalyst 6500 Switch com Supervisor Engine 2T no IOS® liberam 15.0(01)SY
- Gerador de tráfego IXIA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O CTS é uma solução do controle de acesso e da identidade da rede avançada para fornecer a conectividade segura fim-a-fim através do backbone dos provedores de serviços e das redes do centro de dados.

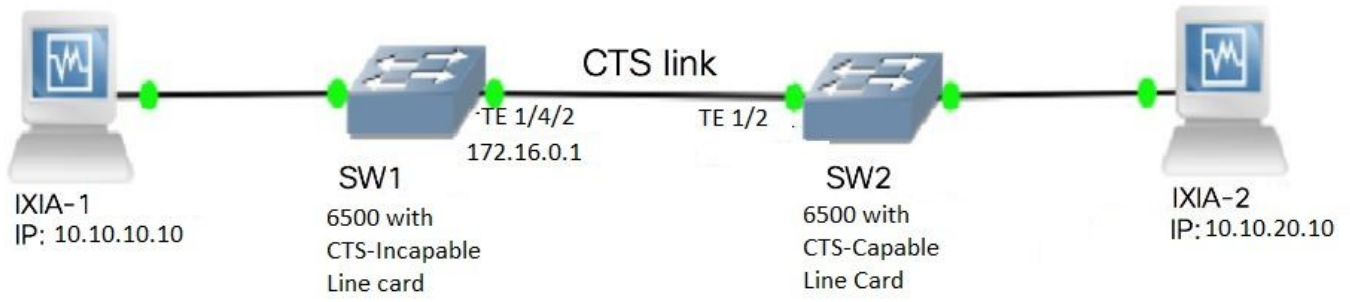
Os Catalyst 6500 Switch com as placas de linha do 2T e 6900 Series do Supervisor Engine fornecem o suporte de hardware e software completo a fim executar o CTS. Quando um Catalyst 6500 é configurado com as placas de linha do 2T e 6900 Series do Supervisor Engine, o sistema é inteiramente capaz de fornecer características CTS.

Desde que os clientes gostariam de continuar a usar seus Catalyst 6500 Switch e placas de linha que já existem quando migrarem a uma rede CTS, e por este motivo, o Supervisor Engine 2T precisa de ser compatível com determinadas placas de linha que já existem quando distribuídas em uma rede CTS.

A fim apoiar a funcionalidade nova CTS tal como a criptografia de link da etiqueta (SGT) e da IEEE 802.1AE MACsec do grupo de segurança, há os circuitos integrados do aplicativo específicos dedicados (ASIC) usados no Supervisor Engine 2T e nas placas de linha novas do 6900 Series. O modo refletor do ingresso fornece a compatibilidade entre as placas de linha do legado que não usam o CTS. O modo refletor do ingresso apoia somente a transmissão centralizada, encaminhamento de pacote ocorrerá no PFC do Supervisor Engine 2T. Somente o 6148 Series ou as placas de linha de transmissão centralizadas ativados por tecla do cartão (CFC) tais como as placas de linha 6748-GE-TX são apoiados. As placas de linha do Distributed Forwarding Card (DFC) e as placas de linha dos Ethernet de 10 Gigabit não são apoiadas quando o modo refletor do ingresso é permitido. Com o modo refletor do ingresso configurado, as placas de linha NON-apoiadas não põem acima. O modo refletor do ingresso é permitido com o uso de um comando global configuration e exige um recarregamento do sistema.

Configurar

Diagrama de Rede



Etapa 1. Instalação CTS Layer3 na interface de saída entre o SW1 e o SW2

-

```
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
```

Etapa 2. Permita o refletor do ingresso CTS globalmente

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

Conecte uma relação de uma placa de linha apoiada CTS NON ao 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
```

Atribua SGT estático no interruptor SW1 para os pacotes recebidos do IXIA 1 conectado ao SW1. Política da licença da instalação para fazer CTS L3 somente para pacotes na sub-rede desejada no autenticador.

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique que o IFC-estado está ABERTO em ambo o Switches. As saídas devem olhar como esta:

```
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             -----------
```

Verifique através da saída do Netflow

O Netflow pode ser configurado com estes comandos:

```
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
```

Aplique o Netflow na porta de ingresso da interface de switch SW2 como mostrado:

```
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
```

Envie pacotes de IXIA 1 a IXIA 2. Deve ser recebido corretamente em IXIA 2 conectado ao interruptor SW2 de acordo com a política de tráfego. Assegure-se de que os pacotes sejam SGT etiquetados.

```
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      10.20.20.10                 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
```

Agora, política setup da exceção para saltar CTS L3 para pacotes a um endereço IP de Um ou Mais Servidores Cisco ICM NT específico no interruptor do autenticador.

```
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
```

Envie pacotes de IXIA 1 a IXIA 2. Devem ser recebidos corretamente em IXIA 2 conectado ao interruptor SW2 de acordo com a política da exceção.

> **Note**: Os pacotes não são SGT etiquetados porque a política da exceção toma o **GRUPO TAG=0 do FLUXO CTS SRC da** precedência.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.