Configurar e verificar o refletor de saída com o manual CTS

Contents

Introduction

Este documento descreve como configurar e verificar um Cisco TrustSec (CTS) com refletor de saída.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico da solução CTS.

Componentes Utilizados

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

- Switches Catalyst 6500 com mecanismo de supervisão 2T no IOS versão 15.0(01)SY
- Gerador de tráfego IXIA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O CTS é uma arquitetura de acesso à rede habilitada por identidade que ajuda os clientes a permitir colaboração segura, reforçar a segurança e atender aos requisitos de conformidade. Ele também oferece uma infraestrutura de aplicação de políticas escalável baseada em funções. Os pacotes são marcados com base na associação de grupo da origem do pacote na entrada da

rede. As políticas associadas ao grupo são aplicadas à medida que esses pacotes atravessam a rede.

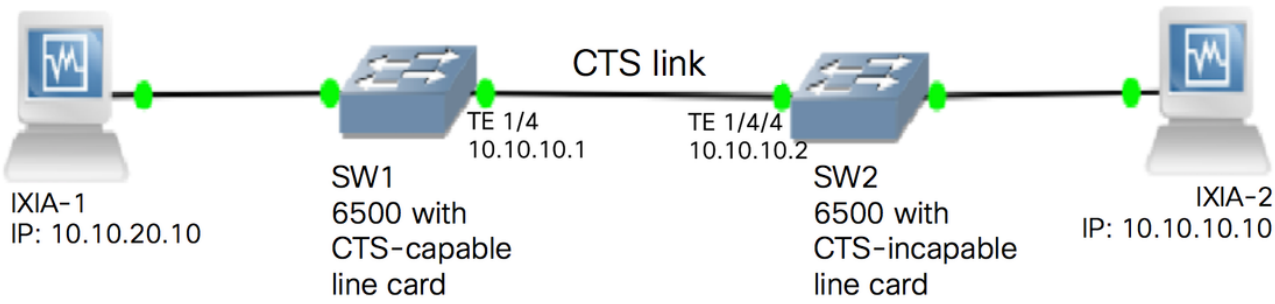
Os switches da série Catalyst 6500 com placas de linha do mecanismo supervisor 2T e 6900 fornecem suporte completo de hardware e software para a implementação do CTS. Para suportar a funcionalidade CTS, existem ASICs (Application Specific Integrated Circuits - Circuitos Integrados Específicos de Aplicações) dedicados usados nas novas placas de linha 6900 Series. As placas de linha antigas não têm esses ASICs dedicados e, portanto, não suportam CTS.

O refletor CTS usa o Catalyst Switch Port Analyzer (SPAN) para refletir o tráfego de um módulo de switching incapaz de CTS para a atribuição e inserção do Supervisor Engine para Security Group Tag (SGT).

Um refletor de saída CTS é implementado em um switch de distribuição com uplinks de Camada 3, onde o módulo de switching incapaz de CTS enfrenta um switch de acesso. Ele suporta placas de encaminhamento centralizado (CFCs - Centralized Forwarding Cards) e placas de encaminhamento distribuído (DFCs - Distributed Forwarding Cards).

Configurar

Diagrama de Rede



Configurar SW1

Configure o manual CTS no uplink para SW2 com estes comandos:

```
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
```

Configurar SW2

Ative o refletor de saída no switch com estes comandos:

```
SW2(config)#platform cts egress
SW2#write memory
```

```
Building configuration...
[OK] SW2#reload
```

Note: O switch precisa ser recarregado para ativar o modo refletor de saída.

Configure o Manual CTS na porta conectada ao SW1 com estes comandos:

```
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
```

Configure um SGT estático no SW2 para o endereço IP origem 10.10.10.10 do IXIA.

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

Verificar

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

O modo CTS atual pode ser visualizado com este comando:

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

O estado do link CTS pode ser visualizado com este comando:

```
show cts interface summary
```

Verifique se o estado IFC está ABERTO em ambos os switches. Os resultados devem ser assim:

```
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
```

Verificar através da saída do Netflow

O Netflow pode ser configurado com estes comandos:

```
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
```

Aplique o Netflow na interface de entrada do switch SW1:

```
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
```

Verifique se os pacotes de entrada estão marcados com SGT no Switch SW1.

```
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
```

Troubleshoot

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