Configurar e verifique o refletor da saída com manual CTS

Índice

Introdução

Este documento descreve como configurar e verifiy Cisco TrustSec (CTS) com refletor da saída.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico da solução de Cisco TrustSec.

Componentes Utilizados

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

- Catalyst 6500 Switch com Supervisor Engine 2T na versão do IOS 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

Cisco TrustSec é uma arquitetura identidade-permitida do acesso de rede que ajude clientes a permitir a Colaboração segura, a reforçar a Segurança, e a endereçar exigências da conformidade. Igualmente fornece papel escalável uma infraestrutura baseada do reforço de

política. Os pacotes são etiquetados basearam na membrasia do clube do origem do pacote no ingresso da rede. As políticas associadas com o grupo são aplicadas enquanto estes pacotes atravessam a rede.

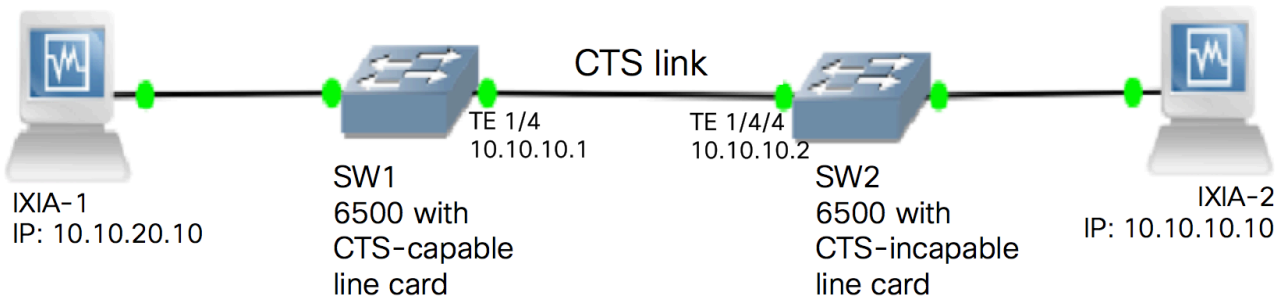
Os Catalyst 6500 Series Switch com as placas de linha do 2T e 6900 Series do Supervisor Engine fornecem o suporte de hardware e software completo executando o CTS. A fim apoiar a funcionalidade CTS, há os circuitos integrados característicos da aplicação dedicados (ASIC) usados nas placas de linha novas do 6900 Series. As placas de linha do legado não têm estes ASIC dedicados e consequentemente, não apoie o CTS.

Analisador da porta de Catalyst switch dos usos do refletor de Cisco TrustSec (PERÍODO) para refletir o tráfego de um módulo de switching CTS-incapaz ao Supervisor Engine para a atribuição e a inserção da etiqueta do grupo de segurança (SGT).

Um refletor da saída de Cisco TrustSec é executado em um switch de distribuição com uplinks da camada 3, onde o módulo de switching CTS-incapaz enfrenta um switch de acesso. Apoia centralizado enviando os cartões (CFC) e distribuído enviando os cartões (DFC).

Configurar

Diagrama de Rede



Configuração SW1

Configurar o manual CTS no uplink ao 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
```

Configuração SW2

Permita o refletor da saída no interruptor com estes comandos:

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

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

Note: O interruptor tem que ser recarregado a fim permitir o modo refletor da saída.

Configurar 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
```

Configurar um SGT estático no SW2 para o endereço IP de 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 atual CTS pode ser visto com este comando:

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

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

```
show cts interface summary
```

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

```
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
```

Verificação 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 ingresso do interruptor 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 que os pacotes recebidos são SGT etiquetados no interruptor 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
```

Troubleshooting

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