Druk richting uitgang instellen met CTS-handleiding

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco TrustSec (CTS) met de reflector van het Estricht moet configureren.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van CTS-oplossing te hebben.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 6500 switches met Supervisor Engine 2T op IOS 15.0(10)SY
- IXIA verkeersgenerator

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

CTS is een op identiteit gebaseerde netwerktoegangsarchitectuur die klanten helpt om veilige samenwerking mogelijk te maken, veiligheid te versterken en aan conformiteitseisen te voldoen. Het biedt ook een schaalbare, op beleidshandhaving gebaseerde infrastructuur. Packets zijn

gelabeld op basis van het groepslidmaatschap van de pakketbron bij de ingang van het netwerk. Het beleid dat met de groep wordt geassocieerd wordt toegepast aangezien deze pakketten het netwerk oversteken.

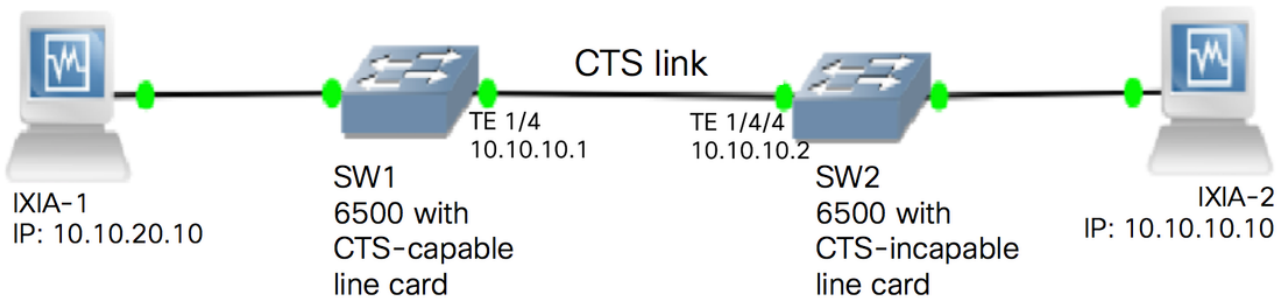
De Catalyst 6500 Series-switches met Supervisor Engine 2T en 6900 Series lijnkaarten bieden volledige hardware- en softwareondersteuning voor de implementatie van CTS. Om de CTS-functionaliteit te ondersteunen, zijn er speciale Application Specific Integrated Circuits (ASIC's) gebruikt op de nieuwe 6900 Series lijnkaarten. Verouderde lijnkaarten hebben deze specifieke ASIC's niet en ondersteunen daarom geen CTS.

CTS-reflector gebruikt Catalyst Switch Port Analyzer (SPAN) om verkeer weer te geven van een CTS-ongeschikt switchmodule naar de Supervisor Engine voor Security Group Tag (SGT) toewijzing en invoeging.

Een CTS drukreflector wordt op een distributieschakelaar met Layer 3 uplinks geïmplementeerd, waar de CTS-ongeschikte switchmodule met een toegangsschakelaar wordt geconfronteerd. Zij ondersteunt Centralized Forwarding Cards (CFC's) en Distributed Forwarding Cards (DFC's).

Configureren

Netwerkdiagram



SW1 configureren

Configureer de CTS handleiding in de uplink naar SW2 met deze opdrachten:

```
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
```

SW2 configureren

Druk op reflector op de schakelaar met deze opdrachten om:

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

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

> Opmerking: De schakelaar moet opnieuw worden geladen om de omgevingsreflectiemodus in te schakelen.

Configureer de CTS handleiding op de poort die is aangesloten op SW1 met deze opdrachten:

```
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
```

Configureer een statische SGT op SW2 voor het IP-bronadres 10.10.10.10 vanaf IXIA.

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

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De huidige CTS-modus kan met deze opdracht worden bekeken:

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

De CTS verbindingsstaat kan met deze opdracht worden bekeken:

```
show cts interface summary
```

Controleer dat de IFC-status op beide switches is OPEN. De output zou er als volgt moeten uitzien:

```
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
```

Controleer door NetFlow-uitvoer

NetFlow kan met deze opdrachten worden ingesteld:

```
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
```

NetFlow toepassen op de ingangsinterface van de SW1-schakelaar:

```
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
```

Controleer dat de inkomende pakketten SGT zijn gelabeld op SW1-switch.

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.