Layer 3 CTS configureren met inbraakreflector

Inhoud

Inleiding

Dit document beschrijft hoe u Layer 3 Cisco TrustSec (CTS) met Ingress Reflector kunt 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 geavanceerde oplossing voor de controle van de netwerktoegang en de identiteit om veilige verbindingen van begin tot eind over de backbone en de netwerken van datacenters van serviceproviders te bieden.

De Catalyst 6500-switches met Supervisor Engine 2T en 6900 Series lijnkaarten bieden volledige

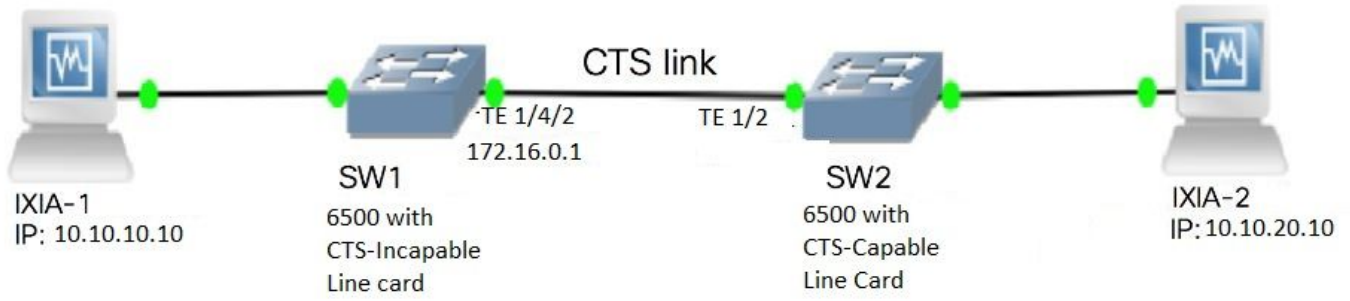
hardware- en softwareondersteuning om CTS te implementeren. Wanneer een Catalyst 6500 met de Supervisor Engine 2T en 6900 Series lijnkaarten wordt geconfigureerd, is het systeem volledig in staat om CTS-functies te leveren.

Aangezien klanten hun Catalyst 6500 switches en lijnkaarten willen blijven gebruiken die al bestaan terwijl ze naar een CTS-netwerk migreren, en om deze reden moet Supervisor Engine 2T compatibel zijn met bepaalde lijnkaarten die al bestaan wanneer ze in een CTS-netwerk worden ingezet.

Om nieuwe CTS-functies zoals Security Group Tag (SGT) en IEEE 802.1AE MACsec-encryptie te ondersteunen zijn er speciale applicatie-specifieke geïntegreerde circuits (ASIC's) gebruikt op de Supervisor Engine 2T en de nieuwe 6900 Series lijnkaarten. De reflectormodus Ingress biedt compatibiliteit tussen de legacy-lijnkaarten die geen CTS gebruiken. Ingreress reflector-modus ondersteunt alleen het gecentraliseerde verzenden, pakkettransport zal plaatsvinden op de PFC van Supervisor Engine 2T. Slechts 6148 Series of fabric-enabled-lijnkaarten voor gecentraliseerd doorsturen (CFC), zoals de 6748-GE-TX lijnkaarten, worden ondersteund. De lijnkaarten voor gedistribueerd doorsturen (DFC) en de 10 Gigabit Ethernet-lijnkaarten worden niet ondersteund wanneer de reflectiemodus ingeschakeld is. Als de reflectormodus is ingesteld, worden de niet-ondersteunde lijnkaarten niet uitgezet. De reflectiemodus van het Ingress wordt ingeschakeld met het gebruik van een wereldwijde configuratieopdracht en moet opnieuw worden geladen.

Configureren

Netwerkdiagram



Stap 1. Setup CTS Layer 3 op IP-interface tussen SW1 en 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
```

Stap 2. Schakel CTS-reflector mondiaal in

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

Sluit een interface van een door NON CTS ondersteunde lijnkaart aan op 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
```

Pas statische SGT in SW1 schakelaar aan voor pakketten die van IXIA 1 worden ontvangen die op SW1 worden aangesloten. De opstelling laat beleid CTS L3 slechts voor pakketten in gewenste netto op authentiek toe.

```
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
```

Verifiëren

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

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

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

Controleer door NetFlow-uitvoer

NetFlow kan met deze opdrachten worden ingesteld:

```
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
```

Pas netflow op de ingangspoort van SW2 switch interface toe zoals wordt getoond:

```
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
```

Verstuur pakketten van IXIA 1 naar IXIA 2. Deze moeten correct worden ontvangen op IXIA 2, aangesloten op de SW2-schakelaar volgens het verkeersbeleid. Zorg ervoor dat de pakketten voorzien zijn van een SGT-label.

```
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
```

Stel nu een uitzondering beleid in om CTS L3 te overslaan voor pakketten naar een specifiek IP-adres in de Authenticator-schakelaar.

```
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
```

Verstuur pakketten van IXIA 1 naar IXIA 2. Ze moeten correct worden ontvangen op IXIA 2 dat is aangesloten op de SW2-schakelaar volgens het afwijkingsbeleid.

> Opmerking: De pakketten worden niet getagd SGT omdat het uitzonderingsbeleid voorrang heeft op **FLOW CTS SRC GROUP TAG=0.**

Problemen oplossen

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