Konfigurieren von Layer-3-CTS mit Ingress Reflector

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Cisco TrustSec (CTS) für Layer 3 mit Ingress Reflector konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse der CTS-Lösung zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst Switches der Serie 6500 mit Supervisor Engine 2T auf IOS® Version 15.0(01)SY
- IXIA Traffic Generator

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

CTS ist eine erweiterte Lösung für die Netzwerkzugriffskontrolle und -identität, die eine sichere End-to-End-Anbindung zwischen Backbone- und Rechenzentrumsnetzwerken von Service

Providern ermöglicht.

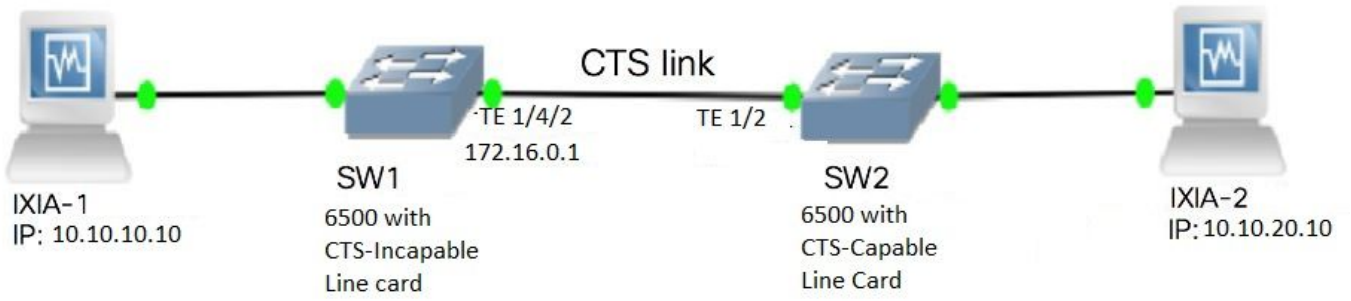
Die Catalyst Switches der Serie 6500 mit den Line Cards Supervisor Engine 2T und 6900 bieten vollständigen Hardware- und Software-Support für die Implementierung von CTS. Wenn ein Catalyst 6500 mit den Line Cards der Supervisor Engines 2T und 6900 konfiguriert ist, ist das System in der Lage, CTS-Funktionen bereitzustellen.

Da Kunden ihre Catalyst 6500-Switches und Line Cards weiter verwenden möchten, die bereits bei der Migration zu einem CTS-Netzwerk vorhanden sind, muss die Supervisor Engine 2T aus diesem Grund mit bestimmten Linecards kompatibel sein, die bereits in einem CTS-Netzwerk vorhanden sind.

Zur Unterstützung neuer CTS-Funktionen wie Security Group Tag (SGT) und IEEE 802.1AE MACsec-Link-Verschlüsselung werden auf der Supervisor Engine 2T dedizierte anwendungsspezifische integrierte Schaltungen (ASICs) und die neuen Line Cards der Serie 6900 verwendet. Der Eingangs-Reflektormodus bietet Kompatibilität zwischen älteren Line Cards, die kein CTS verwenden. Der Eingangs-Reflektormodus unterstützt nur die zentrale Weiterleitung, die Paketweiterleitung erfolgt auf der PFC der Supervisor Engine 2T. Es werden nur Linecards der Serie 6148 oder Fabric-fähige Centralized Forwarding Card (CFC)-Linecards wie die Linecards 6748-GE-TX unterstützt. Die DFC-Linecards (Distributed Forwarding Card) und 10-Gigabit-Ethernet-Linecards werden bei aktiviertem Eingangs-Reflektormodus nicht unterstützt. Wenn der Eingangsreflektormodus konfiguriert ist, werden nicht unterstützte Linecards nicht hochgefahren. Der Eingangs-Reflektormodus wird mithilfe eines globalen Konfigurationsbefehls aktiviert und erfordert ein erneutes Laden des Systems.

Konfigurieren

Netzwerkdiagramm



Schritt 1: Einrichtung von CTS Layer3 an der Ausgangsschnittstelle zwischen SW1 und 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
```

Schritt 2: CTS-Eingangs-Reflektor global aktivieren

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

Verbinden Sie eine Schnittstelle von einer nicht von CTS unterstützten Line Card mit 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
```

Weisen Sie dem SW1-Switch ein statisches SGT für Pakete zu, die von der mit SW1 verbundenen IXIA 1 empfangen wurden. Einrichtung einer Genehmigungsrichtlinie, die CTS-L3 nur für Pakete im gewünschten Subnetz auf dem Authentifizierer vorsieht.

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Stellen Sie sicher, dass der IFC-Status auf beiden Switches OPEN ist. Die Ergebnisse müssen wie folgt aussehen:

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

Überprüfung durch NetFlow-Ausgabe

NetFlow kann mit den folgenden Befehlen konfiguriert werden:

```
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
```

Wenden Sie NetFlow auf den Eingangsport der SW2-Switch-Schnittstelle an, wie gezeigt:

```
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
```

Senden Sie Pakete von IXIA 1 an IXIA 2. Sie muss korrekt auf IXIA 2 empfangen werden, die

entsprechend der Datenverkehrsrichtlinie mit dem SW2-Switch verbunden ist. Stellen Sie sicher, dass die Pakete mit SGT gekennzeichnet sind.

```
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
```

Legen Sie jetzt eine Ausnahmerichtlinie fest, um CTS L3 für Pakete an eine bestimmte IP-Adresse im Authenticator-Switch zu überspringen.

```
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
```

Senden Sie Pakete von IXIA 1 an IXIA 2. Sie müssen korrekt auf IXIA 2 empfangen werden, die an den SW2-Switch angeschlossen ist, entsprechend der Ausnahmerichtlinie.

Hinweis: Die Pakete werden nicht mit einem SGT versehen, da die Ausnahmerichtlinie

Vorrang vor **FLOW CTS SRC GROUP TAG=0** hat.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.