Konfigurieren des Ausgangs-Reflektors mithilfe des CTS-Handbuchs

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Konfigurieren von SW1](#)
[Konfigurieren von SW2](#)
[Überprüfen](#)
[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco TrustSec (CTS) mit Egress-Reflektor konfigurieren.

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 identitätsbasierte Netzwerkzugriffsarchitektur, mit der Kunden eine sichere Zusammenarbeit ermöglichen, die Sicherheit erhöhen und Compliance-Anforderungen erfüllen

können. Sie bietet außerdem eine skalierbare, rollenbasierte Infrastruktur zur Richtliniendurchsetzung. Pakete werden abhängig von der Gruppenmitgliedschaft der Paketquelle am Netzwerkeingang getaggt. Die der Gruppe zugeordneten Richtlinien werden angewendet, wenn diese Pakete das Netzwerk durchlaufen.

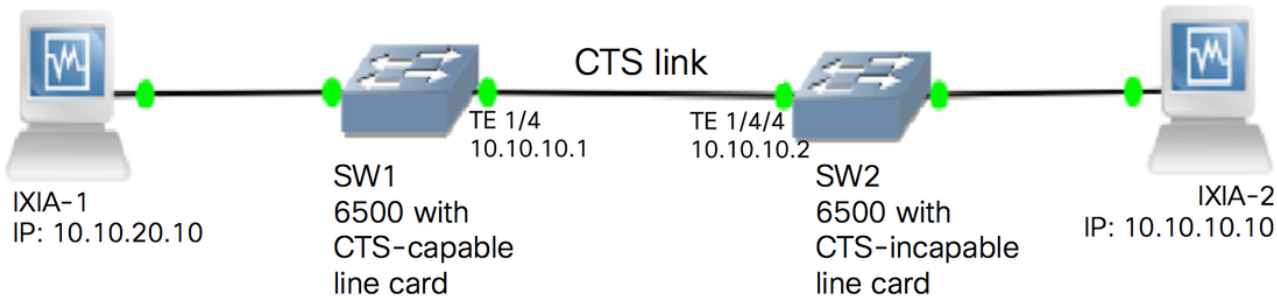
Die Catalyst Switches der Serie 6500 mit Supervisor Engine 2T und Line Cards der Serie 6900 bieten vollständigen Hardware- und Software-Support für die Implementierung von CTS. Zur Unterstützung der CTS-Funktionalität kommen auf den neuen Linecards der Serie 6900 dedizierte ASICs (Application Specific Integrated Circuits) zum Einsatz. Ältere Line Cards verfügen nicht über dedizierte ASICs und unterstützen daher CTS nicht.

Der CTS-Reflektor verwendet den Catalyst Switch Port Analyzer (SPAN), um den Datenverkehr von einem CTS-nicht-fähigen Switching-Modul zur Supervisor Engine für die Zuweisung und Einfügung der Security Group Tag (SGT) wiederzugeben.

Ein CTS-Egress-Reflektor wird auf einem Distribution Switch mit Layer-3-Uplinks implementiert, wo das CTS-nicht-fähige Switching-Modul an einen Access Switch angeschlossen ist. Sie unterstützt zentrale Weiterleitungskarten (CFCs) und verteilte Weiterleitungskarten (DFCs).

Konfigurieren

Netzwerkdiagramm



Konfigurieren von SW1

Konfigurieren Sie das CTS-Handbuch für den Uplink zu SW2 mithilfe der folgenden Befehle:

```
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
```

Konfigurieren von SW2

Aktivieren Sie mit den folgenden Befehlen den Ausgangs-Reflektor am Switch:

```
SW2(config)#platform cts egress
SW2#write memory
Building configuration...
[OK] SW2#reload
```

> **Hinweis**: Der Switch muss neu geladen werden, um den Egress-Reflektor-Modus zu aktivieren.

Konfigurieren Sie das CTS-Handbuch für den mit SW1 verbundenen Port mithilfe der folgenden Befehle:

```
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
```

Konfigurieren Sie ein statisches SGT auf SW2 für die Quell-IP-Adresse 10.10.10.10 von IXIA.

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

Überprüfen

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

Der aktuelle CTS-Modus kann mit dem folgenden Befehl angezeigt werden:

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

Der CTS-Verbindungsstatus kann mit dem folgenden Befehl angezeigt werden:

```
show cts interface summary
```

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

```
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
```

Überprüfung durch NetFlow-Ausgabe

NetFlow kann mit den folgenden Befehlen konfiguriert werden:

```
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 auf die Eingangs-Schnittstelle des SW1-Switches anwenden:

```
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
```

Überprüfen Sie, ob die eingehenden Pakete auf dem SW1-Switch mit einem SGT markiert sind.

```
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
```

Fehlerbehebung

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