인그레스 리플렉터로 레이어 3 CTS 구성

목차

소개

이 문서에서는 인그레스 리플렉터로 레이어 3 Cisco TrustSec(CTS)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 CTS 솔루션에 대한 기본적인 지식을 습득할 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 6500 Switch with Supervisor Engine 2T on IOS® Release 15.0(01)SY
- IXIA 트래픽 생성기

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

CTS는 서비스 공급자 백본 및 데이터 센터 네트워크 전체에서 엔드 투 엔드 보안 연결을 제공하는 고급 네트워크 액세스 제어 및 ID 솔루션입니다.

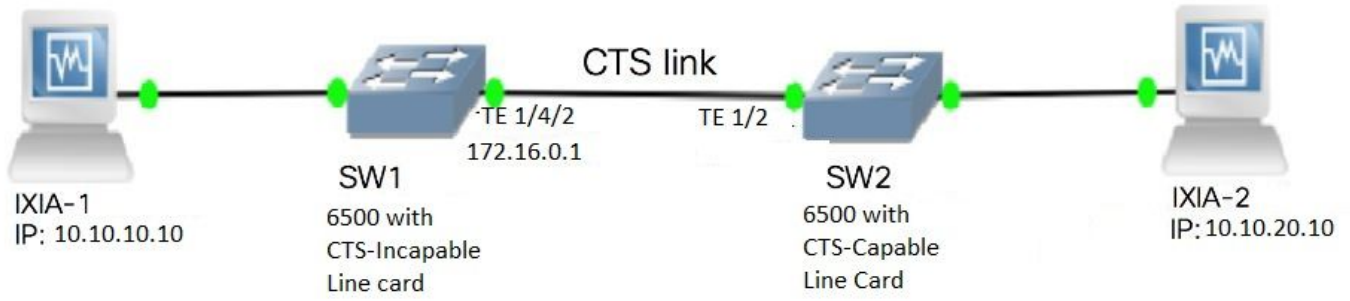
Supervisor Engine 2T 및 6900 Series 라인 카드가 장착된 Catalyst 6500 스위치는 CTS를 구현하기 위해 완전한 하드웨어 및 소프트웨어 지원을 제공합니다.Catalyst 6500이 Supervisor Engine 2T 및 6900 Series 라인 카드로 구성된 경우 시스템은 CTS 기능을 완벽하게 제공할 수 있습니다.

고객은 CTS 네트워크로 마이그레이션하는 동안 이미 존재하는 Catalyst 6500 스위치와 라인 카드를 계속 사용하고 싶어하기 때문에 Supervisor Engine 2T는 CTS 네트워크에 구축할 때 이미 존재하는 특정 라인 카드와 호환되어야 합니다.

SGT(Security Group Tag) 및 IEEE 802.1AE MACsec 링크 암호화와 같은 새로운 CTS 기능을 지원하기 위해 Supervisor Engine 2T 및 새로운 6900 Series 라인 카드에 전용 ASIC가 사용됩니다.인그레스 리플렉터 모드는 CTS를 사용하지 않는 레거시 라인 카드 간의 호환성을 제공합니다.인그레스 리플렉터 모드는 중앙 집중식 포워딩만 지원하며, 패킷 포워딩은 Supervisor Engine 2T의 PFC에서 발생합니다.6748-GE-TX 라인 카드와 같은 6148 Series 또는 CFC(Fabric-Enabled Centralized Forwarding Card) 라인 카드만 지원됩니다.인그레스 리플렉터 모드가 활성화된 경우 DFC(Distributed Forwarding Card) 라인 카드와 10기가비트 이더넷 라인 카드는 지원되지 않습니다.인그레스 리플렉터 모드가 구성된 경우 지원되지 않는 라인 카드의 전원이 켜지지 않습니다.인그레스 리플렉터 모드는 전역 컨피그레이션 명령을 사용하여 활성화되며 시스템을 다시 로드해야 합니다.

구성

네트워크 다이어그램



1단계. SW1과 SW2 간의 이그레스 인터페이스에서 CTS Layer3 설정

-

```
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
```

2단계. CTS 인그레스 리플렉터를 전역적으로 활성화합니다.

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

NON CTS 지원 라인 카드에서 IXIA에 인터페이스를 연결합니다.

```
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
```

SW1에 연결된 IXIA 1에서 수신한 패킷에 대해 SW1 스위치에서 고정 SGT를 할당합니다. 인증자의 원하는 서브넷에 있는 패킷에 대해서만 CTS L3을 수행하도록 정책을 허용합니다.

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

두 스위치 모두에서 IFC-state가 OPEN인지 확인합니다.출력은 다음과 같아야 합니다.

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

Netflow 출력을 통해 확인

Netflow는 다음 명령으로 구성할 수 있습니다.

```
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
```

다음과 같이 SW2 스위치 인터페이스의 인그레스 포트에 netflow를 적용합니다.

```
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
```

IXIA 1에서 IXIA 2로 패킷을 전송합니다. 트래픽 정책에 따라 SW2 스위치에 연결된 IXIA 2에서 패킷을 올바르게 수신해야 합니다.패킷이 SGT 태그되었는지 확인합니다.

```
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
```

이제 Authenticator 스위치의 특정 IP 주소로 전달되는 패킷에 대해 CTS L3을 건너뛰도록 예외 정책을 설정합니다.

```
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
```

IXIA 1에서 IXIA 2로 패킷을 전송합니다. 예외 정책에 따라 SW2 스위치에 연결된 IXIA 2에서 패킷을 올바르게 수신해야 합니다.

> **참고:**예외 정책이 FLOW CTS SRC **GROUP TAG=0**보다 우선하므로 패킷은 SGT **태그가 지정되지 않습니다.**

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.