CTS Manual로 이그레스 리플렉터 구성

목차

소개

이 문서에서는 이그레스 리플렉터를 사용하여 Cisco CTS(TrustSec)를 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 고객이 안전한 협업을 지원하고 보안을 강화하며 규정 준수 요구 사항을 해결할 수 있도록 지원하는 ID 기반 네트워크 액세스 아키텍처입니다.또한 확장 가능한 역할 기반 정책 시행 인프라를 제공합니다.패킷은 네트워크의 인그레스(ingress)에 있는 패킷 소스의 그룹 멤버십에 따라 태그가 지정됩니다.이러한 패킷이 네트워크를 통과할 때 그룹과 연결된 정책이 적용됩니다.

수퍼바이저 엔진 2T 및 6900 시리즈 라인 카드가 장착된 Catalyst 6500 시리즈 스위치는 CTS 구현

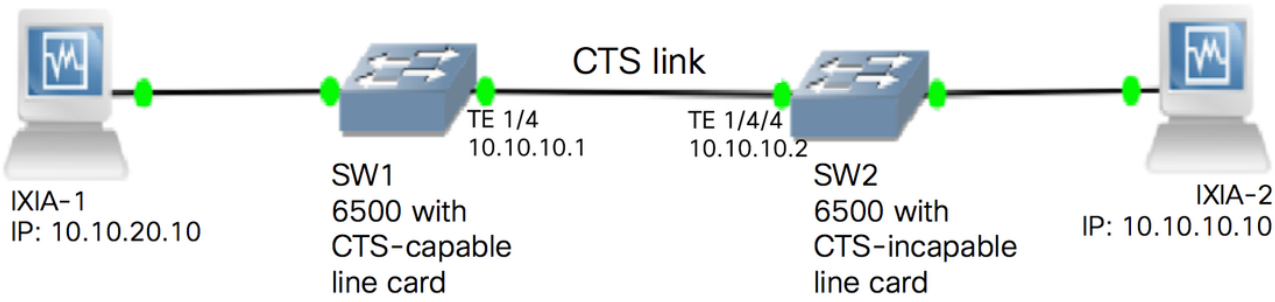
을 위한 완전한 하드웨어 및 소프트웨어 지원을 제공합니다.CTS 기능을 지원하기 위해 새로운 6900 Series 라인 카드에 전용 ASIC(Application Specific Integrated Circuit)가 사용됩니다.레거시 라인 카드에는 이러한 전용 ASIC가 없으므로 CTS를 지원하지 않습니다.

CTS 리플렉터는 CTS 무능력 스위칭 모듈의 트래픽을 SGT(Security Group Tag) 할당 및 삽입을 위해 수퍼바이저 엔진으로 반영하기 위해 Catalyst SPAN(Switch Port Analyzer)을 사용합니다.

CTS 이그레스 리플렉터는 CTS 무능력 스위칭 모듈이 액세스 스위치에 연결되는 레이어 3 업링크가 있는 디스트리뷰션 스위치에 구현됩니다.CFC(Centralized Forwarding Card) 및 DFC(Distributed Forwarding Card)를 지원합니다.

구성

네트워크 다이어그램



SW1 구성

다음 명령을 사용하여 SW2에 대한 업링크에서 CTS 설명서를 구성합니다.

```
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 구성

다음 명령을 사용하여 스위치에서 이그레스 리플렉터를 활성화합니다.

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

참고:이그레스 리플렉터 모드를 활성화하려면 스위치를 다시 로드해야 합니다.

다음 명령을 사용하여 SW1에 연결된 포트에서 CTS Manual을 구성합니다.

```
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
```

IXIA의 소스 IP 주소 10.10.10.10에 대해 SW2에서 고정 SGT를 구성합니다.

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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

다음 명령을 사용하여 현재 CTS 모드를 볼 수 있습니다.

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

CTS 링크 상태는 다음 명령으로 볼 수 있습니다.

```
show cts interface summary
```

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

```
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
```

Netflow 출력을 통해 확인

Netflow는 다음 명령으로 구성할 수 있습니다.

```
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
```

SW1 스위치의 인그레스 인터페이스에 Netflow 적용:

```
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
```

수신 패킷이 SW1 스위치에서 태그가 지정된 SGT인지 확인합니다.

```
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
```

문제 해결

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