Настройте и проверьте уровень 3 Cisco TrustSec с входным отражателем

Содержание

Введение

Этот документ описывает Уровень 3 Cisco TrustSec (CTS) с Входной конфигурацией Отражателя и проверкой.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания о решении Cisco TrustSec.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутаторы Catalyst 6500 с Supervisor Engine 2T на IOS Release 15.0 (01) SY
- Генератор трафика IXIA

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

CTS является управлением доступом сложной сети и идентификационным решением

предоставить от начала до конца безопасное подключение через магистраль Поставщиков услуг и сети Data Center.

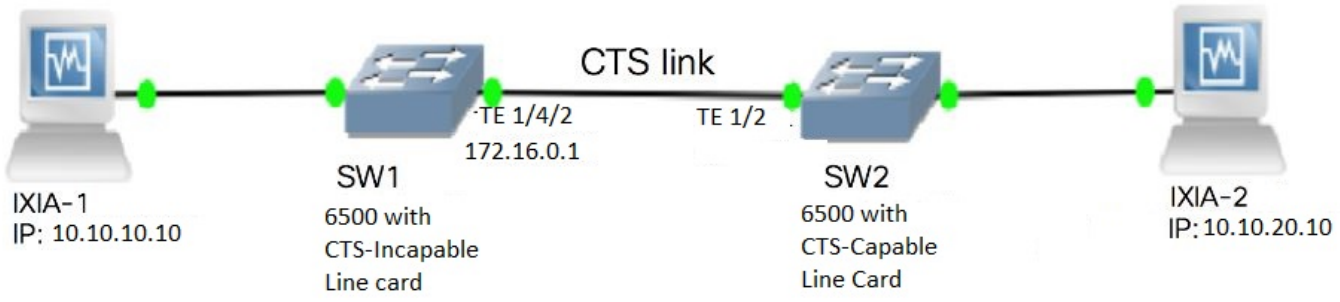
Коммутаторы Catalyst 6500 с Supervisor Engine 2T и линейные карты серии 6900 предоставляют завершенную поддержку программного и аппаратного обеспечения для реализации CTS. Когда Catalyst 6500 настроен с Supervisor Engine 2T и линейные карты серии 6900, система полностью способна к обеспечению функций CTS.

Так как клиенты хотели бы продолжить использовать их существующие Коммутаторы Catalyst 6500 и линейные карты при миграции на сеть CTS, и поэтому Supervisor Engine 2T должен быть совместим с определенными существующими линейными картами, когда развернуто в сети CTS.

Для поддержки новой функциональности CTS, такой как тег группы безопасности (SGT) и IEEE 802.1AE шифрование ссылки MACsec существуют выделенные специализированные интегральные схемы (ASIC-схемы), используемые на Supervisor Engine 2T и новые линейные карты серии 6900. Входной режим отражателя предоставляет совместимость между устаревшими линейными картами, не способными к использованию CTS. Входной режим отражателя поддерживает только централизованную передачу, пересылка пакетов произойдет на PFC Supervisor Engine 2T. Поддерживаются только 6148 Серий или CFC с возможностью использования матрицы (Централизованная передающая карта) линейные карты, такие как линейные карты с 6748 TX GE. DFC (Distributed Forwarding Card), Линейные карты и линейные карты 10 Gigabit Ethernet не поддерживаются, когда включен входной режим отражателя. С входным режимом отражателя не включатся настроенные, неподдерживаемые линейные карты. Входной режим отражателя включен с помощью команды глобальной кофигурации и требует перезагрузки системы.

Настройка

Схема сети



Шаг 1. CTS Layer3 настройки на исходящем интерфейсе между SW1 и SW2

1. ```
   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
```

Шаг 2. Включите Входной отражатель CTS глобально.

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

Соединитесь интерфейс от CTS NON поддержал линейную карту к 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
```

Назначьте статический SGT в коммутаторе SW1 для пакетов, полученных от IXIA 1, связанного с SW1. Политика разрешения на настройку, чтобы сделать L3 CTS только для пакетов в желаемой подсети на средстве проверки подлинности.

```
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
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Проверьте, что IFC-состояние ОТКРЫТО на обоих коммутаторах. Выходные данные должны быть похожими на это:

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

Проверка через netflow выведена

Netflow может быть настроен с этими командами:

```
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
```

Примените netflow на входной порт интерфейса коммутатора SW2 как показано:

```
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
```

Передайте пакеты от IXIA 1 до IXIA 2. Это должно быть полученный должным образом на IXIA 2, связанном с коммутатором SW2 согласно политике трафика. Обратите внимание на то, что пакетами является теговый SGT.

```
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
```

Теперь политика исключения Настройки для пропуска L3 CTS для пакетов к определенному IP-адресу в коммутаторе Средства проверки подлинности.

```
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
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
```

Передайте пакеты от IXIA 1 до IXIA 2. Они должны быть получены должным образом на IXIA 2, связанном с коммутатором SW2 согласно политике исключения.

> **Примечание:** Обратите внимание на то, что пакетами не является SGT, помеченный, потому что политика исключения имеет приоритет. FLOW CTS SRC GROUP TAG=0

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.