入力リフレクタでレイヤ3 CTS を設定して下さい

目次

概要

この資料に入力リフレクタでレイヤ3 Cisco TrustSec （CTS）を設定する方法を記述されています。

前提条件

要件

Cisco は CTS ソリューションの基本的な知識があることを推奨します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- IOS ® リリース 15.0(01)SY の Supervisor Engine 2T が付いている Catalyst 6500 スイッチ
- IXIA トラフィック ジェネレータ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

CTS は高度なネットワーク アクセス制御およびサービス プロバイダー バックボーンおよびデータセンタ ネットワークを渡るエンドツーエンド セキュア接続を提供する識別ソリューションです。

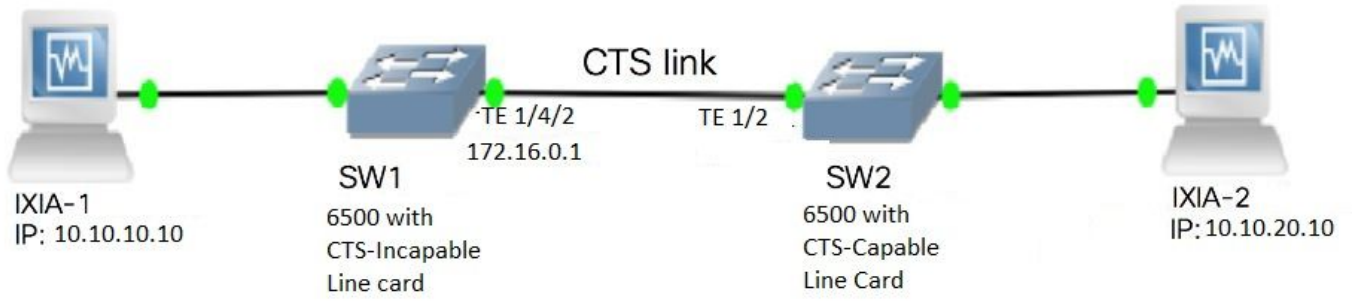
Supervisor Engine 2T および 6900 シリーズ ラインカードが付いている Catalyst 6500 スイッチは CTS が実装されるために完全なハードウェア および ソフトウェア サポートを提供します。 Catalyst 6500 が Supervisor Engine 2T および 6900 シリーズ ラインカードで設定されるとき、システムは CTS 機能を提供する十分にことができます。

顧客が CTS ネットワークに、およびこのような理由で移行する間、既にあっている Catalyst 6500 スイッチをおよびラインカードを使用し続けることを望むので、Supervisor Engine 2T は既にあっているある特定のラインカードと互換性がある必要があります CTS ネットワークで展開されたとき。

セキュリティグループ タグ（SGT）および IEEE 802.1AE MACsec リンク暗号化のような新しい CTS 機能性をサポートするために、Supervisor Engine 2T および新しい 6900 シリーズ ラインカードで使用される専用特定用途向け集積回路（ASIC）があります。 入力リフレクタ モードは CTS を使用しないレガシー ラインカード間の互換性を提供します。 入力リフレクタ モードは Supervisor Engine 2T の PFC に中央集中型転送だけ、パケット転送発生しますサポートします。 6748-GE-TX ラインカードのような 6148 シリーズまたはファブリック対応中央集中型転送カード（CFC）ラインカードだけサポートされます。 入力リフレクタ モードがイネーブルになっているとき Distributed Forwarding Card （DFC）ラインカードおよび 10 ギガビット イーサネット ラインカードはサポートされません。 設定されて入力リフレクタ モードがサポートされていないラインカードは電源投入。 入力リフレクタ モードはグローバル 設定 コマンドの使用とイネーブルになり、システム再ロードを必要とします。

設定

ネットワーク図



ステップ 1. SW1 と SW2 間の出力 インターフェイスの設定 CTS Layer3

-
```
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
```

ステップ 2.グローバルのイネーブル CTS 入力リフレクタ

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

NON CTS サポートされているラインカードから IXIA にインターフェイスを接続して下さい。

```
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
```

SW1 に接続される IXIA 1 から受信されるパケットに SW1 スイッチの静的な SGT を割り当てて下さい。 オーセンティケータの望ましいサブネットのパケットのためのだけ CTS L3 をする設定割り当てポリシー。

```
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
```

確認

このセクションでは、設定が正常に機能していることを確認します。

両方のスイッチで、IFC ステートが OPEN になっていることを確認します。 出力はこのようになる必要があります:

```
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出力を通って確認して下さい

NetFlow を設定するには、次のコマンドを使用します。

```
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
```

示されているように SW2 スイッチ インターフェイスの入力ポートの netflow を加えて下さい:

```
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 1 から IXIA 2.にパケットを送信して下さい。 それはトラフィックポリシーに従って SW2 スイッチに接続される IXIA 2 できちんと受け取る必要があります。 タグ付けされるパケットが SGT であることを確認して下さい。

```
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      10.20.20.10                 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
```

この場合、オーセンティケータ スイッチの特定の IP アドレスにパケットのための CTS L3 をスキップする設定された例外ポリシー。

```
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
```

IXIA 1 から IXIA 2.にパケットを送信して下さい。 それらは例外ポリシーに従って SW2 スイッチに接続される IXIA 2 できちんと受け取る必要があります。

> **注:** タグ付けされる例外ポリシーが優位 **フロー CTS ソース グループ TAG=0 を**奪取 するのでパケットは SGT ではないです。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。