入力リフレクタによるレイヤ 3 Cisco TrustSec の設定と確認

目次

概要

この資料は入力 リフレクタ 設定および確認を用いるレイヤ3 Cisco TrustSec （ CTS ）を記述したものです。

前提条件

要件

Cisco TrustSec ソリューションの基礎知識があることが推奨されます。

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 ベースの Supervisor Engine 2T を搭載した Catalyst 6500 スイッチ
- IXIA トラフィック ジェネレータ

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

CTS は高度なネットワーク アクセスコントロール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。

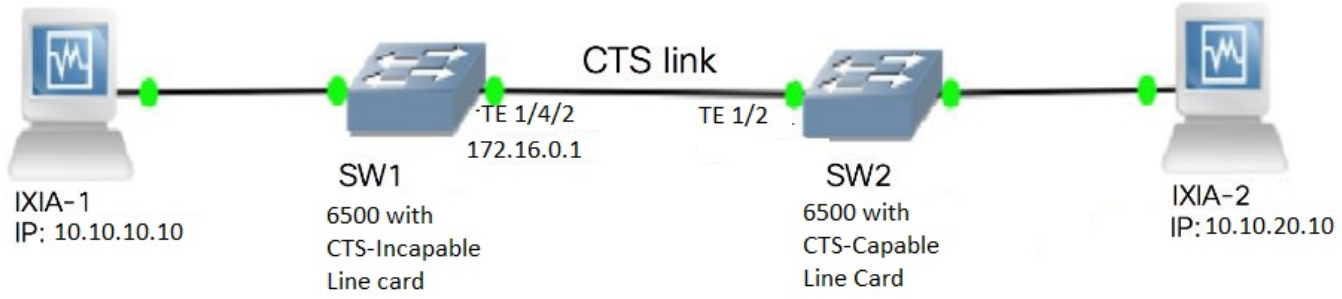
Supervisor Engine 2T が付いている Catalyst 6500 スイッチおよび 6900 シリーズ ラインカードは CTS を設定するために完全なハードウェア および ソフトウェア サポートを提供します。 Catalyst 6500 が Supervisor Engine 2T および 6900 シリーズ ラインカードで設定されるとき、システムは CTS 機能を提供する十分にことができます。

CTS CTS ネットワークで展開されたときネットワークおよびこのような理由で顧客が既存の Catalyst 6500 スイッチ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 に移行している間ある特定の既存のラインカードと互換性がある必要があります。

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 を使用することができないレガシー 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 に中央集中型フォワーディングだけ、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 CFC （中央集中型フォワーディング カード）ラインカードだけサポートされます。 入力 リフレクタ モードが有効に なるとき DFC （Distributed Forwarding Card）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 コマンドを使用して有効に 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 CTS Layer3 を設定して下さい

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
   ```
   ```

ステップ 2.グローバルに 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 スイッチのスタティック 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 をするセットアップ割り当てポリシー。

```
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 の出力による検証

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 であることに注目して下さい。

```
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      10.10.20.10                 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
```

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 をスキップするために例外 ポリシーを設定して下さい。

```
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      10.10.20.10                 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:** 以下の事項に注意して下さい:タグ付けされる例外 ポリシーが precedence.FLOW CTS SRC 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。