入力リフレクタを使用したレイヤ3 CTSの設定

内容

概要

このドキュメントでは、レイヤ3 Cisco TrustSec(CTS)を入力リフレクタで設定する方法について説明します。

前提条件

要件

CTSソリューションに関する基本的な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いています。

- IOS®リリース15.0(01)SY上の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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

CTSは、サービスプロバイダーのバックボーンおよびデータセンターネットワーク全体にエンドツーエンドのセキュアな接続を提供する、高度なネットワークアクセスコントロールおよびアイデンティティ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を搭載したCatalyst 6500スイッチは、

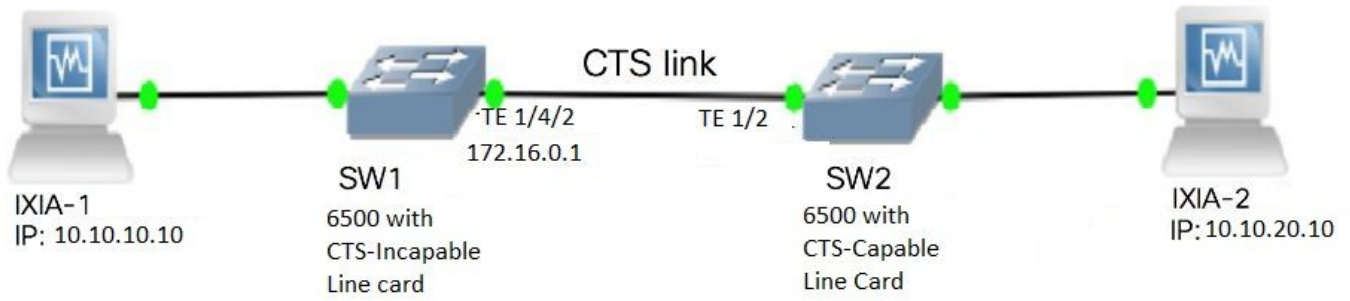
CTSを実装するためのハードウェアおよびソフトウェアの完全なサポートを提供します。Catalyst 6500にSupervisor Engine 2Tおよび6900シリーズのラインカードを設定すると、システムはCTS機能を完全に提供できます。

お客様は、CTSネットワークへの移行時に既存のCatalyst 6500スイッチとラインカードを引き続き使用したいと考えており、そのため、Supervisor Engine 2Tは、CTSネットワークに導入した際に既存のラインカードと互換性がある必要があります。

Security Group Tag(SGT)やIEEE 802.1AE MACsecリンク暗号化などの新しいCTS機能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の特定集積回路(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中央集中型フォワーディングのみをサポートし、Supervisor Engine 2TのPFCでパケット転送が行われます。6748-GE-TXラインカードなど、6148シリーズまたはファブリック対応の中央集中型フォワーディングカード(CFC)ラインカードだけがサポートされています。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、入力リフレクタモードが有効な場合はサポートされません。入力リフレクタモードが設定されている場合、サポートされていないラインカードの電源はオンになりません。入力リフレクタモードは、グローバルコンフィギュレーションコマンドを使用してイネーブルにされており、システムのリロードが必要です。

設定

ネットワーク図



手順1:SW1とSW2の間の出力インターフェイスにCTSレイヤ3を設定する

-

```
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:CTS入力リフレクタをグローバルに有効にする

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

非CTSで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ます。

```
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に接続されたIXIA 1から受信したパケットに対して、SW1スイッチのスタティックSGTを割り当てます。CTS L3をオーセンティケータの目的のサブネットのパケットに対してのみ実行するように設定します。

```
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

ここでは、設定が正常に機能しているかどうかを確認します。

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。出力は次のようになります。

```
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出力による確認

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
```

次に示すように、SW2スイッチインターフェイスの入力ポートにnetflowを適用します。

```
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ます。トラフィックポリシーに従って、SW2スイッチに接続されたIXIA 2で正しく受信する必要があります。パケットにSGTタグが付いていることを確認します。

```
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
```

次に、オーセンティケータスイッチの特定のIPアドレスへのパケットに対するCTS L3をスキップするように、例外ポリシーを設定します。

```
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 1からIXIA 2にパケットを送信します。例外ポリシーに従って、SW2スイッチに接続されたIXIA 2でパケットを正しく受信する必要があります。

> **注：**例外ポリシーが優先されるため、パケットにはSGTタグが付けられ**ません。FLOW CTS SRC GROUP TAG=0。**

トラブルシュート

現在、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。