CTS Manual を使用した出力リフレクタの設定と確認

内容

概要

このドキュメントでは、出力リフレクタを使用してCisco TrustSec(CTS)を設定および確認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 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ID対応のネットワークアクセスアーキテクチャで、セキュアなコラボレーションの実現、セキュリティの強化、コンプライアンス要件への対応を支援します。さらに、スケーラブルなロールベースのポリシー適用インフラストラクチャでもあります。ネットワークに入ってくるパケ

ットには、パケット ソールのグループ メンバーシップに基づいてタグが付けられます。パネットがネットワークを経由する間、そのグループに関連付けられたポリシーがパケットに適用されます。

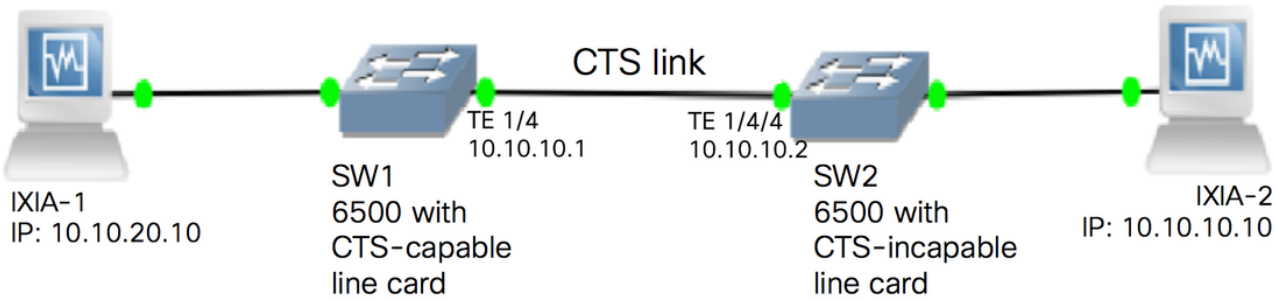
CTS を実装する際は、Supervisor Engine 2T を搭載した Catalyst 6500 シリーズ スイッチと 6900 シリーズ ライン カードが完全なハードウェアおよびソフトウェア サポートを提供します。CTS の機能をサポートするために、新しい 6900 シリーズ ラインカードでは専用の Application Specific Integrated Circuit（ASIC）が使用されています。これらの専用 ASIC を使用していないレガシー ライン カードでは、CTS はサポートされません。

CTSリフレクタは、Catalyst Switch Port Analyzer(SPAN)を使用して、CTS非対応スイッチングモジュールからセキュリティグループタグ(SGT)の割り当てと挿入のためのスーパーバイザエンジンへのトラフィックを反映します。

CTS出力リフレクタは、レイヤ3アップリンクを備えたディストリビューションスイッチに実装され、CTS非対応スイッチングモジュールがアクセススイッチに面しています。Cisco TrustSec では、集中型フォワーディング カード（CFC）および分散型フォワーディング カード（DFC）の両方がサポートされます。

設定

ネットワーク図



SW1の設定

SW2 へのアップリンクに手動で CTS を設定するには、次のコマンドを使用します。:

```
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の設定

スイッチ上で出力リフレクタを有効にするには、次のコマンドを使用します。

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

注：出力リフレクタ モードを有効にするには、スイッチをリロードする必要があります。

SW1 に接続するポートに手動で CTS を設定するには、次のコマンドを使用します。

```
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
```

SW2 に、IXIA の送信元 IP アドレス 10.10.10.10 に対する静的 SGT を設定します。

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

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。

現在の CTS モードを表示するには、次のコマンドを使用します。

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

CTS リンク ステートを表示するには、次のコマンドを使用します。

```
show cts interface summary
```

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#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。

```
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 スイッチの入力インターフェイスに NetFlow を適用します。

```
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
```

SW1 スイッチで着信パケットに SGT タグが付けられていることを確認します。

```
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

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。