Configurazione e verifica del riflettore di avanzamento con il manuale CTS

Sommario

Introduzione

In questo documento viene descritto come configurare e verificare un Cisco TrustSec (CTS) con reflector di uscita.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base delle soluzioni CTS.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Catalyst 6500 con supervisor engine 2T su IOS release 15.0(10)SY
- IXIA Traffic Generator

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

CTS è un'architettura di accesso alla rete basata sull'identità che consente ai clienti di abilitare la collaborazione sicura, rafforzare la sicurezza e soddisfare i requisiti di conformità. Offre inoltre

un'infrastruttura di applicazione delle policy scalabile e basata su ruoli. I pacchetti vengono contrassegnati in base all'appartenenza a gruppi dell'origine del pacchetto in entrata nella rete. I criteri associati al gruppo vengono applicati quando questi pacchetti attraversano la rete.

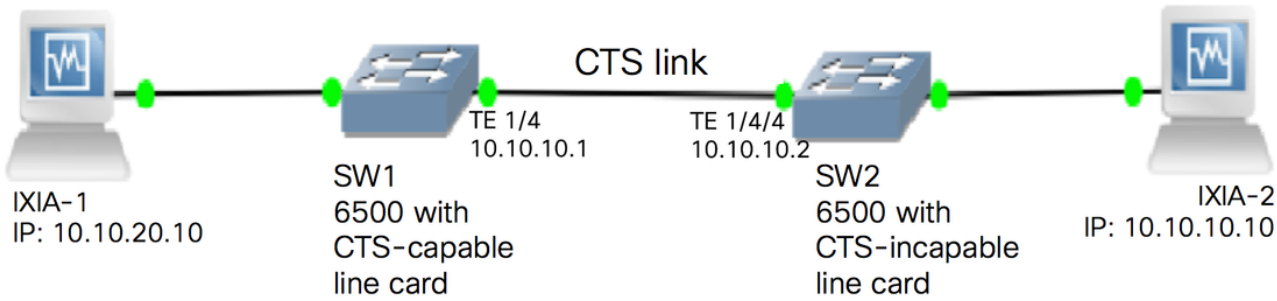
Gli switch Catalyst serie 6500 con schede di linea supervisor engine serie 2T e 6900 offrono supporto hardware e software completo per l'implementazione di CTS. Per supportare la funzionalità CTS, sono disponibili circuiti integrati specifici dell'applicazione (ASIC, Application Specific Integrated Circuits) dedicati utilizzati sulle nuove schede di linea serie 6900. Le schede di linea legacy non dispongono di questi ASIC dedicati e pertanto non supportano CTS.

Il reflector CTS utilizza Catalyst Switch Port Analyzer (SPAN) per riflettere il traffico da un modulo di switching non compatibile con CTS al supervisor engine per l'assegnazione e l'inserimento del tag Security Group Tag (SGT).

Un riflettore di uscita CTS viene implementato su uno switch di distribuzione con uplink di layer 3, dove il modulo di switching non compatibile CTS è rivolto a uno switch di accesso. Supporta le schede di inoltro centralizzate (CFC, Centralized Forwarding Card) e le DFC (Distributed Forwarding Card).

Configurazione

Esempio di rete



Configurazione SW1

Configurare il manuale CTS sull'uplink al SW2 con questi comandi:

```
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
```

Configurazione SW2

Abilitare il riflettore in uscita sullo switch con questi comandi:

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

Nota: Per attivare la modalità del riflettore in uscita, è necessario ricaricare lo switch.

Configurare CTS Manual sulla porta collegata a SW1 con questi comandi:

```
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
```

Configurare un SGT statico su SW2 per l'indirizzo IP di origine 10.10.10.10 da IXIA.

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

La modalità CTS corrente può essere visualizzata con questo comando:

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

Lo stato del collegamento CTS può essere visualizzato con questo comando:

```
show cts interface summary
```

Verificare che lo stato IFC sia OPEN su entrambi gli switch. I risultati dovrebbero avere il seguente aspetto:

```
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
```

Verifica tramite output NetFlow

Netflow può essere configurato con questi comandi:

```
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
```

Applicare Netflow sull'interfaccia in entrata dello switch SW1:

```
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
```

Verificare che i pacchetti in arrivo siano contrassegnati con SGT sullo switch SW1.

```
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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.