具有TrustSec SGT內聯標籤和SGT感知區域型防火牆的IKEv2配置示例

目錄

簡介

本文檔介紹如何使用Internet金鑰交換版本2(IKEv2)和安全組標籤(SGT)來標籤傳送到VPN隧道的資料包。說明包括典型的部署和使用案例。本檔案也說明SGT感知區域型防火牆(ZBF)，並介紹兩種案例：

- 基於從IKEv2隧道接收的SGT標籤的ZBF
- 一種基於SGT交換協定(SXP)對映的ZBF

所有示例都包括資料包級調試，以驗證SGT標籤如何傳輸。

必要條件

需求

思科建議您瞭解以下主題：

- TrustSec元件的基礎知識
- Cisco Catalyst交換器命令列介面(CLI)組態的基本知識
- 配置思科身份服務引擎(ISE)的經驗
- 基於區域的防火牆的基本知識
- IKEv2基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7和Microsoft Windows XP
- Cisco Catalyst 3750-X軟體版本15.0及更新版本
- Cisco Identity Services Engine軟體版本1.1.4及更新版本
- 軟體版本為15.3(2)T或更高版本的Cisco 2901整合服務路由器(ISR)

  註：只有ISR第2代(G2)平台支援IKEv2。

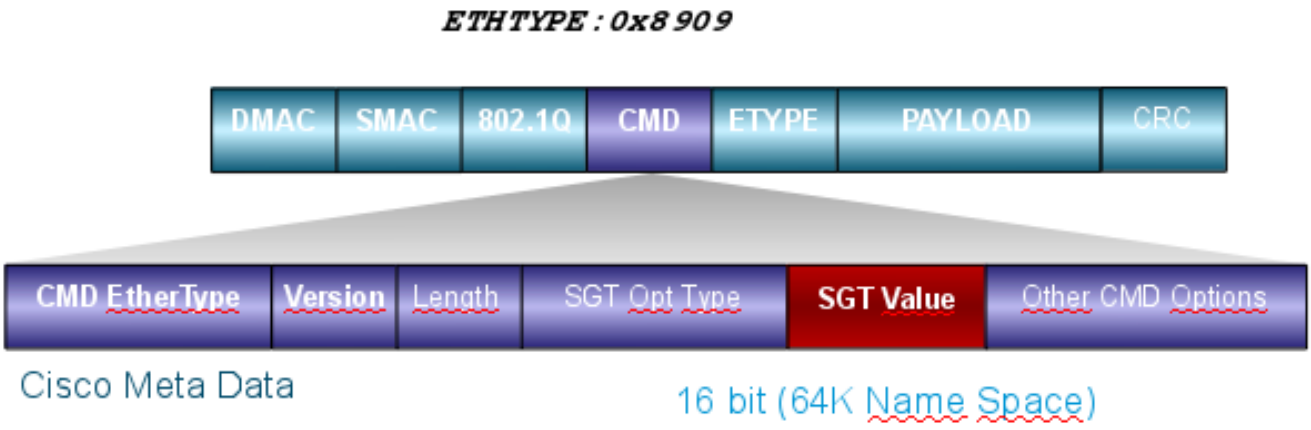
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

安全組標籤(SGT)

SGT是Cisco TrustSec解決方案架構的一部分，旨在使用不基於IP地址的靈活安全策略。

對TrustSec雲中的流量進行分類並使用SGT標籤進行標籤。您可以構建基於該標籤過濾流量的安全策略。從ISE集中管理所有策略，並將其部署到TrustSec雲中的所有裝置。

為了傳遞有關SGT標籤的資訊，思科修改了乙太網幀，類似於對802.1q標籤進行修改的方式。修改後的乙太網幀只能被選定的思科裝置識別。以下是修改後的格式：



思科後設資料(CMD)欄位直接插入源MAC地址欄位(SMAC)或802.1q欄位（如果使用）（如本例所示）。

要通過VPN連線TrustSec雲，已建立IKE和IPsec協定的擴展。稱為IPsec內聯標籤的擴展允許在封裝安全負載(ESP)資料包中傳送SGT標籤。ESP負載經過修改，在資料包本身負載之前攜帶8位元組的CMD欄位。例如，透過網際網路傳送的加密網際網路控制訊息通訊協定(ICMP)封包包含[IP][ESP][CMD][IP][ICMP][DATA]。

詳細的資料載於文章第二部分。

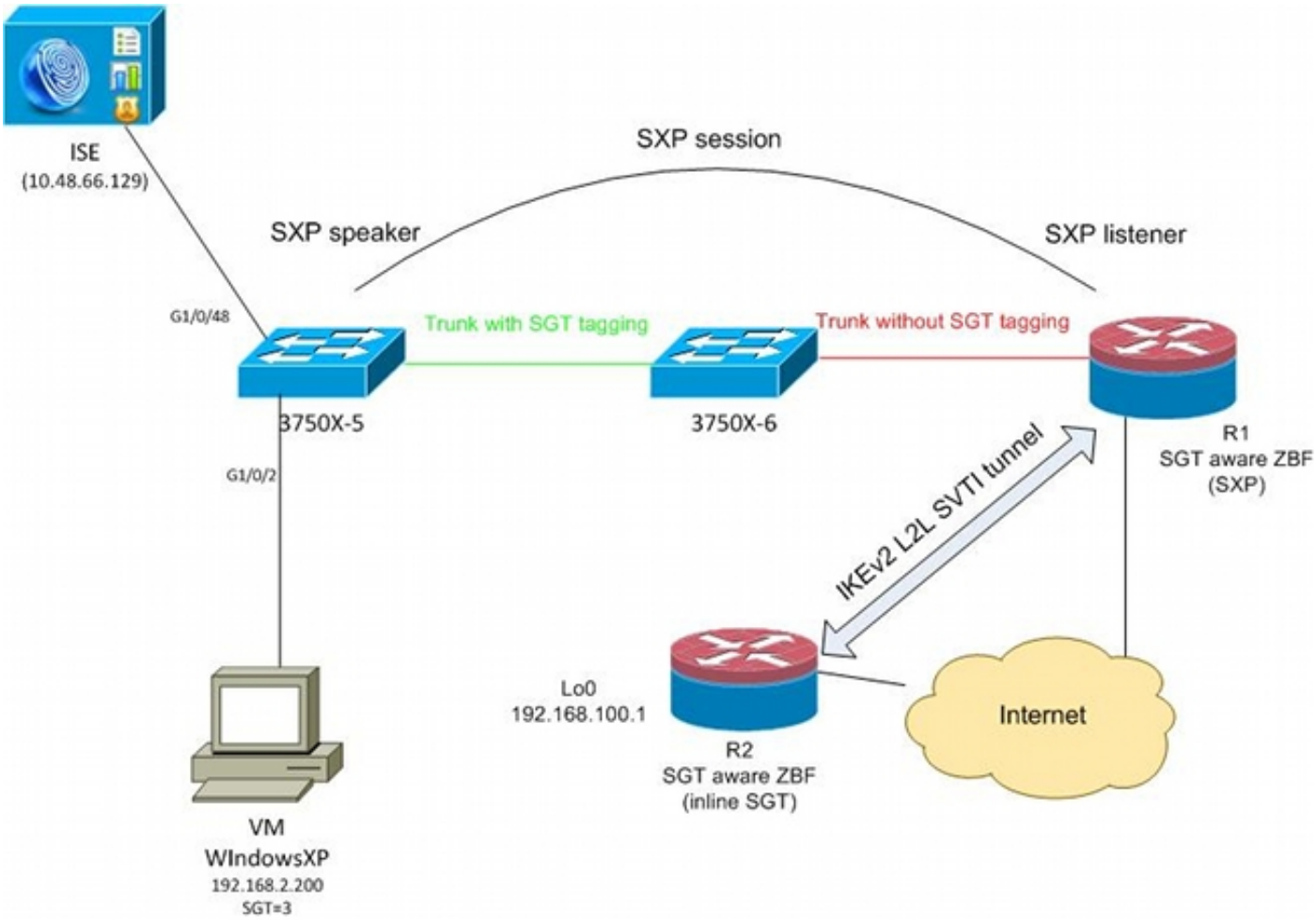
設定

附註：

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。

使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

網路圖表



流量

在此網路中，3750X-5和3750X-6是TrustSec雲中的Catalyst交換機。兩台交換機均使用自動保護訪問憑證(PAC)調配來加入雲。3750X-5已被用作種子，而3750X-6則被用作非種子裝置。兩台交換器之間的流量是使用MACsec加密的，且已正確標籤。

WindowsXP使用802.1x訪問網路。身份驗證成功後，ISE返回將應用於該會話的SGT標籤屬性。源自PC的所有流量都使用SGT=3標籤。

路由器1(R1)和路由器2(R2)是2901 ISR。由於ISR G2當前不支援SGT標籤，因此R1和R2位於TrustSec雲之外，無法理解使用CMD欄位修改以傳遞SGT標籤的乙太網幀。因此，使用SXP將有關IP/SGT對映的資訊從3750X-5轉發到R1。

R1有一個IKEv2隧道，該隧道配置為保護髮往遠端位置(192.168.100.1)的流量，並且已啟用內聯標籤。在IKEv2協商之後，R1開始標籤傳送到R2的ESP資料包。標籤基於從3750X-5接收的SXP資料。

R2可以接收該流量，並根據收到的SGT標籤，可以執行由ZBF定義的特定操作。

R1上也可以執行同樣的操作。SXP對映允許R1根據SGT標籤丟棄從LAN接收的資料包，即使不支援SGT幀。

TrustSec雲配置

配置的第一步是構建TrustSec雲。兩台3750交換機都需要：

- 獲取用於對TrustSec雲(ISE)進行身份驗證的PAC。
- 驗證並通過網路裝置認可控制(NDAC)程式。
- 在連結上使用安全關聯通訊協定(SAP)for MACsec交涉。

此步驟對於此使用情形是必需的，但對於使SXP協定正常工作不是必需的。R1不需要從ISE獲取PAC或環境資料即可執行SXP對映和IKEv2內聯標籤。

驗證

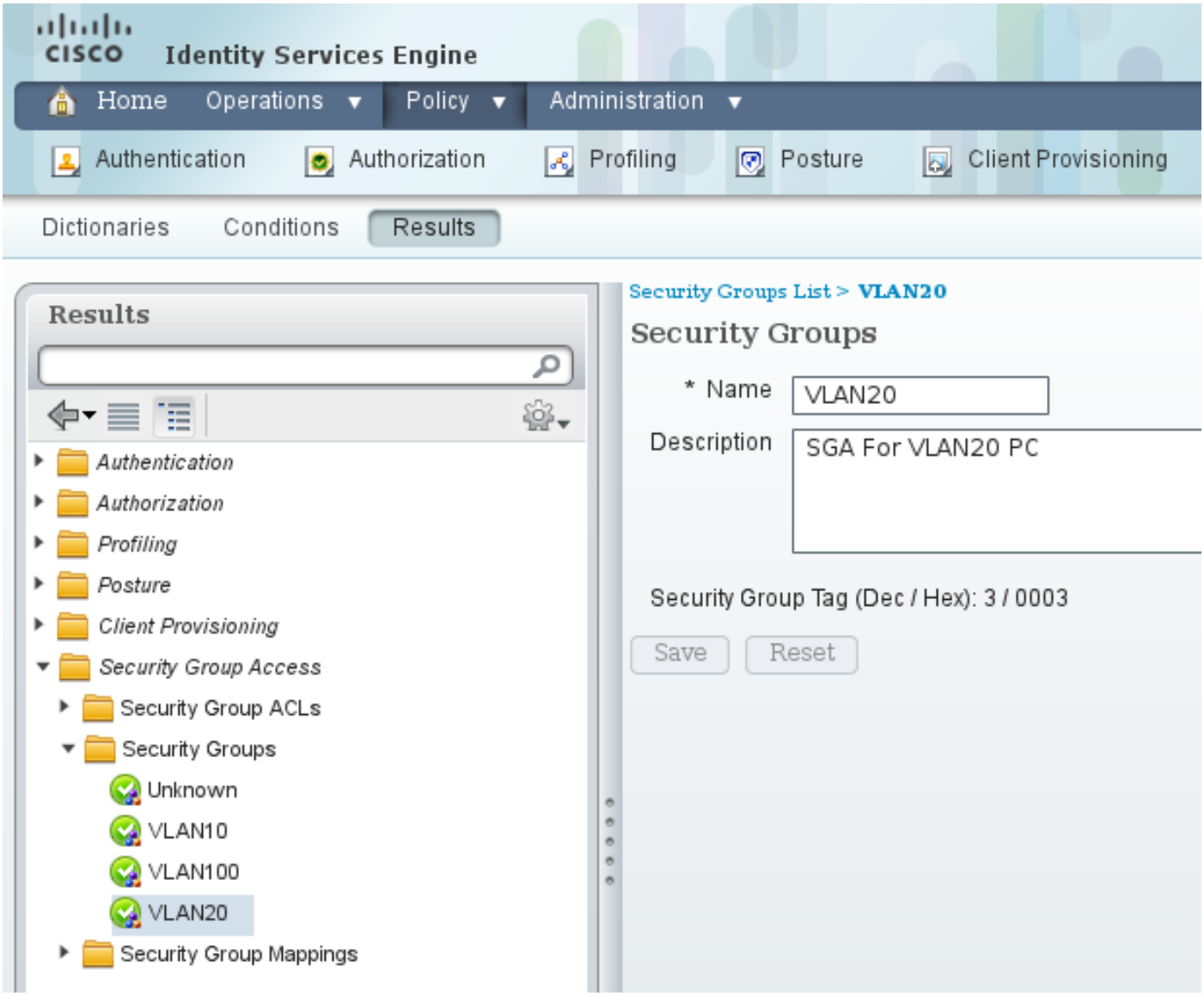
3750X-5和3750X-6之間的鏈路使用802.1x協商的MACsec加密。兩台交換機都信任並接受對等體接收的SGT標籤：

```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

       Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
       authc success:              32
       authc reject:               1543
       authc failure:              0
       authc no response:          0
       authc logoff:               2
       sap success:                32
       sap fail:                   0
       authz success:              50
       authz fail:                 0
       port auth fail:             0
```

基於角色的訪問控制清單(RBACL)無法直接應用於交換機。這些策略在ISE上配置並自動下載到交換機上。

客戶端配置

使用者端可以使用802.1x、MAC驗證略過(MAB)或Web驗證。請記得配置ISE，以便返回授權規則的正確安全組：



驗證

驗證使用者端組態：

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.2.200
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
```

```
                SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000006367BE96D54
     Acct Session ID:  0x00000998
              Handle:  0x8B000637

Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

從此以後，從3750X-5傳送到TrustSec雲中其他交換機的客戶端流量將使用SGT=3標籤。

有關授權規則的示例，請參閱ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南。

3750X-5和R1之間的SGT交換協定

R1無法加入TrustSec雲，因為它是一台2901 ISR G2路由器，它無法識別具有CMD欄位的乙太網幀。因此，在3750X-5上配置了SXP:

```
bsns-3750-5#show run | i sxp
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.20 password default mode local
```

R1上也配置了SXP:

```
BSNS-2901-1#show run | i sxp
cts sxp enable
cts sxp default source-ip 192.168.1.20
cts sxp default password cisco
cts sxp connection peer 192.168.1.10 password default mode local listener
hold-time 0 0
```

驗證

確保R1正在接收IP/SGT對映資訊：

```
BSNS-2901-1#show cts sxp sgt-map
SXP Node ID(generated):0xC0A80214(192.168.2.20)
IP-SGT Mappings as follows:
IPv4,SGT: <192.168.2.200 , 3>
source  : SXP;
Peer IP : 192.168.1.10;
Ins Num : 1;
Status  : Active;
Seq Num : 1
Peer Seq: 0
```

R1現在知道，從192.168.2.200接收的所有流量都應被視為標籤為SGT=3。

R1和R2之間的IKEv2配置

這是一個基於SVTI（靜態虛擬通道介面）的簡單方案，具有IKEv2智慧預設值。預共用金鑰用於身份驗證，空加密用於簡化ESP資料包分析。到192.168.100.0/24的所有流量都通過Tunnel1介面傳送。

這是R1上的配置：

```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.21
 address 192.168.1.21
 pre-shared-key cisco
 !
crypto ikev2 profile ikev2-profile
 match identity remote address 192.168.1.21 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local ikev2-keyring

crypto ipsec transform-set tset esp-null esp-sha-hmac
 mode tunnel
!
crypto ipsec profile ipsec-profile
 set transform-set tset
 set ikev2-profile ikev2-profile

interface Tunnel1
 ip address 172.16.1.1 255.255.255.0
 tunnel source GigabitEthernet0/1.10
 tunnel mode ipsec ipv4
 tunnel destination 192.168.1.21
 tunnel protection ipsec profile ipsec-profile

interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.20 255.255.255.0

ip route 192.168.100.0 255.255.255.0 172.16.1.2
```

在R2上，所有返回網路192.168.2.0/24的流量都通過Tunnel1介面傳送：

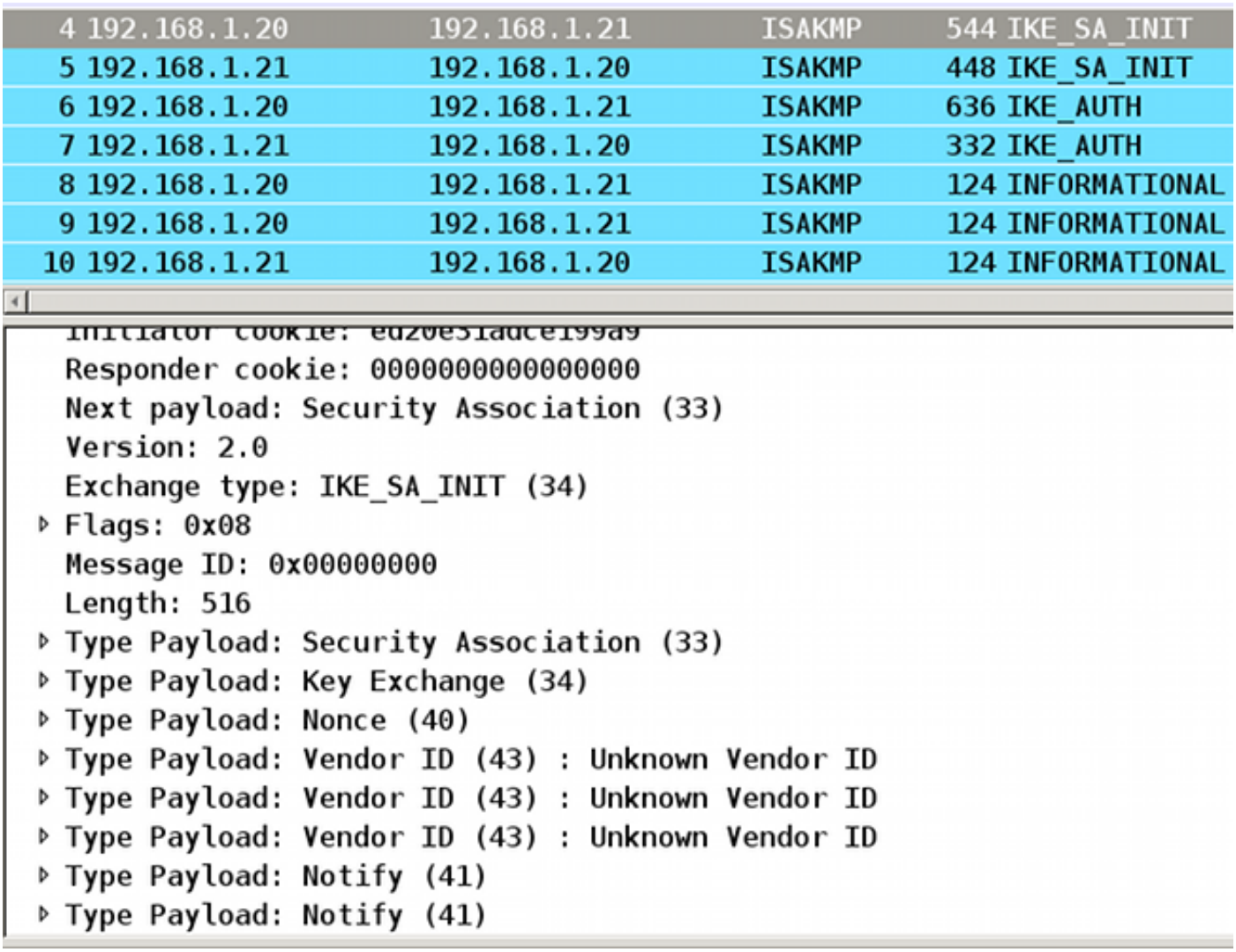
```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.20
 address 192.168.1.20
 pre-shared-key cisco

crypto ikev2 profile ikev2-profile
 match identity remote address 192.168.1.20 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local ikev2-keyring

crypto ipsec transform-set tset esp-null esp-sha-hmac
 mode tunnel

crypto ipsec profile ipsec-profile
 set transform-set tset
 set ikev2-profile ikev2-profile

interface Loopback0
description Protected Network
 ip address 192.168.100.1 255.255.255.0
```

```
interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 tunnel source GigabitEthernet0/1.10
 tunnel mode ipsec ipv4
 tunnel destination 192.168.1.20
 tunnel protection ipsec profile ipsec-profile

interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.21 255.255.255.0

ip route 192.168.2.0 255.255.255.0 172.16.1.1
```

兩台路由器上只需要一個命令即可啟用內嵌標籤：**crypto ikev2 cts sgt**命令。

驗證

需要協商內聯標籤。在第一和第二IKEv2資料包中，正在傳送特定供應商ID:



Wireshark未知的供應商ID(VID)有三種。它們與：

- DELETE-REASON，思科支援
- FlexVPN，由Cisco支援
- SGT內嵌標籤

調試驗證這一點。R1（是IKEv2啟動器）傳送：

```
debug crypto ikev2 internal

*Jul 25 07:58:10.633: IKEv2:Construct Vendor Specific Payload: DELETE-REASON
*Jul 25 07:58:10.633: IKEv2:(1): Sending custom vendor id : CISCO-CTS-SGT

*Jul 25 07:58:10.633: IKEv2:Construct Vendor Specific Payload: (CUSTOM)
*Jul 25 07:58:10.633: IKEv2:Construct Vendor Specific Payload: (CUSTOM)
```

R1收到第二個IKEv2資料包和相同的VID:

```
*Jul 25 07:58:10.721: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID
*Jul 25 07:58:10.721: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID
*Jul 25 07:58:10.721: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID
*Jul 25 07:58:10.721: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP)
*Jul 25 07:58:10.725: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP)

*Jul 25 07:58:10.725: IKEv2:(1): Received custom vendor id : CISCO-CTS-SGT
```

因此，兩端都同意在ESP負載開始時放置CMD資料。

檢查IKEv2安全關聯(SA)以驗證此協定：

```
BSNS-2901-1#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.20/500      192.168.1.21/500      none/none            READY
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/225 sec
     CE id: 1019, Session-id: 13
     Status Description: Negotiation done
     Local spi: 1A4E0F7D5093D2B8       Remote spi: 08756042603C42F9
     Local id: 192.168.1.20
     Remote id: 192.168.1.21
     Local req msg id:  2              Remote req msg id:  0
     Local next msg id: 2              Remote next msg id: 0
     Local req queued:  2              Remote req queued:  0
     Local window:      5              Remote window:      5
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is not detected
     Cisco Trust Security SGT is enabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2 SA
```

從Windows客戶端向192.168.100.1傳送流量後，R1顯示：

```
BSNS-2901-1#sh crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel1
```

```
Uptime: 00:01:17
Session status: UP-ACTIVE
Peer: 192.168.1.21 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 192.168.1.21
     Desc: (none)
 IKEv2 SA: local 192.168.1.20/500 remote 192.168.1.21/500 Active
         Capabilities:(none) connid:1 lifetime:23:58:43
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4227036/3522
       Outbound: #pkts enc'ed 9 drop 0 life (KB/Sec) 4227035/3522


BSNS-2901-1#show crypto ipsec sa detail

interface: Tunnel1
   Crypto map tag: Tunnel1-head-0, local addr 192.168.1.20

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 192.168.1.21 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
   #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
   #pkts invalid prot (recv) 0, #pkts verify failed: 0
   #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
   #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
   ##pkts replay failed (rcv): 0
   #pkts tagged (send): 9, #pkts untagged (rcv): 4
    #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0
   #send dummy packets 9, #recv dummy packets 0

    local crypto endpt.: 192.168.1.20, remote crypto endpt.: 192.168.1.21
    plaintext mtu 1454, path mtu 1500, ip mtu 1500, ip mtu idb
GigabitEthernet0/1.10
    current outbound spi: 0x9D788FE1(2641924065)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xDE3D2D21(3728551201)
       transform: esp-null esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2020, flow_id: Onboard VPN:20, sibling_flags 80000040,
crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4227036/3515)
       IV size: 0 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x9D788FE1(2641924065)
       transform: esp-null esp-sha-hmac ,
       in use settings ={Tunnel, }
```

```
        conn id: 2019, flow_id: Onboard VPN:19, sibling_flags 80000040,
crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4227035/3515)
        IV size: 0 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
BSNS-2901-1#
```

請注意，已傳送標籤的資料包。

對於傳輸流量，當R1需要標籤從Windows客戶端傳送到R2的流量時，請確認ESP資料包已正確標籤了SGT=3:

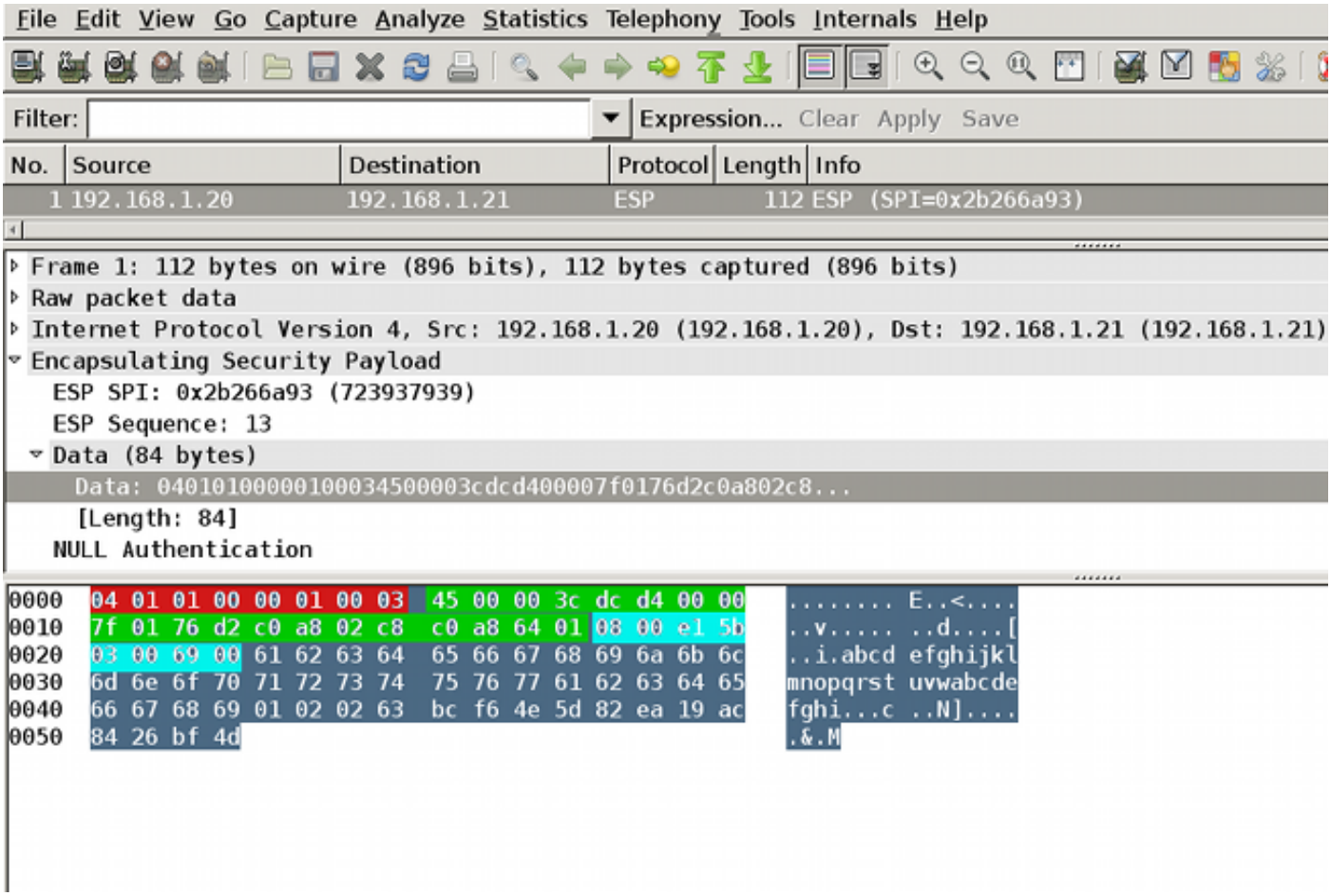
```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

來自同一VLAN（源自交換器）的其他流量預設為SGT=0:

```
*Jul 23 19:43:08.590: IPsec SGT:: inserted SGT = 0 for src ip 192.168.2.10
```

ESP封包層級驗證

使用嵌入式資料包捕獲(EPC)檢視從R1到R2的ESP流量，如下圖所示：



Wireshark已被用於解碼安全引數索引(SPI)的空加密。在IPv4標頭中，來源和目的地IP是路由器

（用作通道來源和目的地）的Internet IP地址。

ESP負載包括8位元組的CMD欄位，該欄位以紅色突出顯示：

- 0x04 — 下一個報頭，即IP
- 0x01 — 長度（標頭後4個位元組，標頭後8個位元組）
- 0x01 — 版本01
- 0x00 — 保留
- 0x00 - SGT長度（共4個位元組）
- 0x01 - SGT型別
- 0x0003 - SGT標籤（最後兩個二進位制八位數，即00 03;SGT用於Windows客戶端）

由於通道介面已使用IPsec IPv4模式，因此下一個報頭是IP，以綠色突出顯示。源IP是c0 a8 02 c8(192.168.2.200)，目的IP是c0 a8 64 01(192.168.100.1)。通訊協定編號為1，即ICMP。

最後一個標頭是ICMP，以藍色突出顯示，具有型別08和代碼8（回應請求）。

接下來是ICMP負載，長度為32個位元組（即從a到i的字母）。圖中的負載是Windows客戶端的典型負載。

ESP報頭的其餘部分會跟隨ICMP負載：

- 0x01 0x02 — 填充。
- 0x02 — 填充長度。
- 0x63 — 下一報頭指向協定0x63，該協定是「任何私有加密方案」。 這表示下一個欄位（ESP資料中的第一個欄位）是SGT標籤。
- 12位元組的完整性檢查值。

CMD欄位位於通常加密的ESP負載內。

IKEv2缺陷：GRE或IPsec模式

到目前為止，這些示例都使用隧道模式IPsec IPv4。如果採用通用路由封裝(GRE)模式，會發生什麼情況？

路由器將傳輸IP封包封裝到GRE中時，TrustSec會將封包視為本地產生的，即GRE封包的來源是路由器，而不是Windows使用者端。新增CMD欄位時，始終使用預設標籤(SGT=0)而不是特定標籤。

在IPsec IPv4模式下從Windows使用者端(192.168.2.200)傳送流量時，您會看到SGT=3:

```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

但是，將相同流量的通道模式更改為GRE後，您會看到SGT=0。在本例中，192.168.1.20是通道來源IP:

```
*Jul 25 20:34:08.577: IPsec SGT:: inserted SGT = 0 for src ip 192.168.1.20
```

註：因此，不使用**GRE非常重要**。

請參閱Cisco錯誤ID CSCuj25890,GRE模式的IOS IPSec內聯標籤：插入路由器SGT。建立此錯誤

是為了在使用GRE時允許正確的SGT傳播。Cisco IOS® XE 3.13S支持SGT over DMVPN

基於IKEv2的SGT標籤的ZBF

以下是R2上ZBF的配置示例。可以識別SGT=3的VPN流量，因為從IKEv2隧道接收的所有資料包都已標籤（即，它們包含CMD欄位）。因此，可以丟棄並記錄VPN流量：

```
class-map type inspect match-all TAG_3
 match security-group source tag 3
class-map type inspect match-all TAG_ANY
 match security-group source tag 0
!
policy-map type inspect FROM_VPN
 class type inspect TAG_3
 drop log
 class type inspect TAG_ANY
 pass log
 class class-default
 drop
!
zone security vpn
zone security inside
zone-pair security ZP source vpn destination self
 service-policy type inspect FROM_VPN

interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 zone-member security vpn
```

驗證

從Windows客戶端(SGT=3)發出對192.168.100.1的ping命令時，調試會顯示以下情況：

```
*Jul 23 20:05:18.822: %FW-6-DROP_PKT: Dropping icmp session
192.168.2.200:0 192.168.100.1:0 on zone-pair ZP class TAG_3 due to
DROP action found in policy-map with ip ident 0
```

對於來自交換器(SGT=0)的ping，debug顯示如下：

```
*Jul 23 20:05:39.486: %FW-6-PASS_PKT: (target:class)-(ZP:TAG_ANY)
Passing icmp pkt 192.168.2.10:0 => 192.168.100.1:0 with ip ident 0
```

來自R2的防火牆統計資訊為：

```
BSNS-2901-2#show policy-firewall stats all
Global Stats:
       Session creations since subsystem startup or last reset 0
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [0:0:0]
       Last session created never
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 0
       Last half-open session total 0
```

```
policy exists on zp ZP
 Zone-pair: ZP

 Service-policy inspect : FROM_VPN

   Class-map: TAG_3 (match-all)
     Match: security-group source tag 3
     Drop
        4 packets, 160 bytes

   Class-map: TAG_ANY (match-all)
     Match: security-group source tag 0
      Pass
        5 packets, 400 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
```

有四個捨棄（Windows傳送的ICMP回應的預設數量）和五個接受（交換器的預設數量）。

基於SXP的SGT對映的ZBF

可以在R1上運行SGT感知ZBF並過濾從LAN接收的流量。雖然該流量沒有SGT標籤，但R1具有SXP對映資訊，可以將該流量視為已標籤。

在本示例中，在LAN和VPN區域之間使用策略：

```
class-map type inspect match-all TAG_3
 match security-group source tag 3
class-map type inspect match-all TAG_ANY
 match security-group source tag 0
!
policy-map type inspect FROM_LAN
 class type inspect TAG_3
  drop log
 class type inspect TAG_ANY
  pass log
 class class-default
 drop
!
zone security lan
zone security vpn
zone-pair security ZP source lan destination vpn
 service-policy type inspect FROM_LAN

interface Tunnel1
 zone-member security vpn

interface GigabitEthernet0/1.20
 zone-member security lan
```

驗證

從Windows客戶端傳送ICMP回應時，您可以看到丟棄：

```
*Jul 25 09:22:07.380: %FW-6-DROP_PKT: Dropping icmp session 192.168.2.200:0
192.168.100.1:0 on zone-pair ZP class TAG_3 due to  DROP action found in
policy-map with ip ident 0

BSNS-2901-1#show policy-firewall stats all
Global Stats:
       Session creations since subsystem startup or last reset 0
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [0:0:0]
       Last session created never
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 0
       Last half-open session total 0

policy exists on zp ZP
 Zone-pair: ZP

 Service-policy inspect : FROM_LAN

   Class-map: TAG_3 (match-all)
     Match: security-group source tag 3
      Drop
        4 packets, 160 bytes

   Class-map: TAG_ANY (match-all)
     Match: security-group source tag 0
      Pass
        5 packets, 400 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
```

由於SXP會話基於TCP，因此還可以通過IKEv2隧道在3750X-5和R2之間構建SXP會話，並基於標籤在R2上應用ZBF策略，而無需內聯標籤。

路線圖

ISR G2和Cisco ASR 1000系列聚合服務路由器也支援GET VPN內聯標籤。ESP資料包的CMD欄位還有一個8位元組。

還計畫支援動態多點VPN(DMVPN)。

有關詳細資訊，請參閱支援Cisco TrustSec的基礎架構路線圖。

驗證

驗證程式包括在配置示例中。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco TrustSec交換機配置指南：瞭解Cisco TrustSec
- 第1冊：Cisco ASA系列常規操作CLI配置指南，9.1：配置ASA以與Cisco TrustSec整合
- Cisco TrustSec通用可用性版本說明：Cisco TrustSec 3.0通用部署性2013版本說明
- 為TrustSec配置IPsec內聯標籤
- Cisco Group Encrypted Transport VPN配置指南，Cisco IOS XE版本3S:為Cisco TrustSec獲取IPSec內嵌標籤的VPN支援
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。