# SGT 認識型ゾーン ベース ファイアウォールおよび TrustSec SGT インライン タギングを使用した IKEv2 の設定例

## 内容


概要
前提条件
要件
使用するコンポーネント
セキュリティ グループ タグ ( SGT )
設定
ネットワーク図
Traffic flow
TrustSec クラウドの設定
確認
クライアントの設定
確認
3750X-5 と R1 間の SGT Exchange Protocol
確認
R1 と R2 間の IKEv2 の設定
確認
ESP パケット レベルの確認
IKEv2の落とし穴：GREまたはIPsecモード
IKEv2 からの SGT タグに基づく ZBF
確認
SXP 経由の SGT マッピングに基づく ZBF
確認
ロードマップ
確認
トラブルシュート
関連情報


## 概要

このドキュメントでは、インターネット キー エクスチェンジ バージョン 2 ( IKEv2 ) とセキュリティ グループ タグ ( SGT ) を使用して、VPN トンネルに送信されるパケットにタグを付ける方法について説明します。この説明には一般的な導入と使用例が含まれています。このドキュメントでは、SGT 対応ゾーンベース ファイアウォール ( ZBF ) についても説明し、2 つのシナリオを紹介します。

- IKEv2 トンネルから受信された SGT タグに基づく ZBF
- SGT eXchange Protocol（SXP）マッピングに基づく ZBF

すべての例に、SGT タグの送信方法を検証するためのパケット レベルのデバッグが含まれています。

# 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

- TrustSec コンポーネントの基礎知識
- Cisco Catalyst スイッチのコマンドライン インターフェイス（CLI）設定の基礎知識
- Cisco Identity Services Engine（ISE）の設定経験
- ゾーンベース ファイアウォールの基礎知識
- IKEv2 に関する基礎知識

## 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。

- Microsoft Windows 7 と Microsoft Windows XP
- Cisco Catalyst 3750-X ソフトウェア リリース 15.0 以降
- Cisco Identity Services Engine ソフトウェア リリース 1.1.4 以降
- ソフトウェア リリース 15.3(2)T 以降がインストールされた Cisco 2901 サービス統合型ルータ（ISR）

**注**:IKEv2はISR Generation 2(G2)プラットフォームでのみサポートされています。

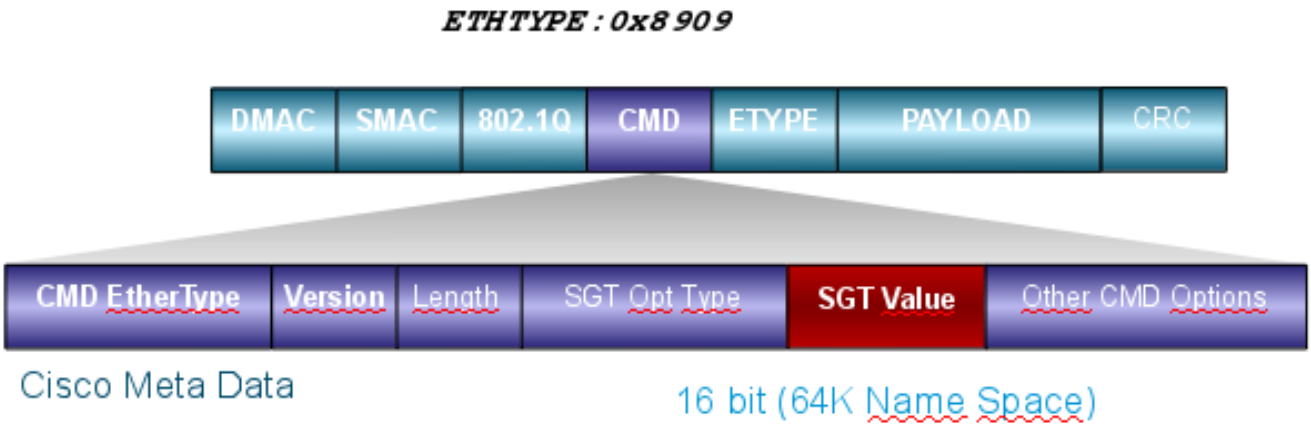
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

# セキュリティ グループ タグ（SGT）

SGT は、IP アドレスに基づかない柔軟なセキュリティ ポリシーを使用するように設計された Cisco TrustSec ソリューション アーキテクチャの一部です。

TrustSec クラウド内のトラフィックは SGT タグを使って分類され、マーキングされます。このタグに基づいてトラフィックをフィルタリングするセキュリティ ポリシーを作成できます。すべてのポリシーは、ISE から一元的に管理され、TrustSec クラウド内のすべてのデバイスに展開されます。

SGT タグに関する情報を渡すために、802.1q タグに対する変更と同様の方法でイーサネット フレームが変更されています。変更されたイーサネット フレームは、選択されたシスコ デバイスでなければ認識できません。変更された形式を以下に示します。




Cisco メタデータ（CMD）フィールドは、この例のように、使用されている送信元 MAC アドレス フィールド（SMAC）または 802.1q フィールドの直後に挿入されます。

VPN 経由で TrustSec クラウドに接続するために、IKE プロトコルと IPsec プロトコルが拡張されました。IPsec インライン タギングと呼ばれるこの拡張を使用すれば、SGT タグを Encapsulating Security Payload（ESP）パケットで送信することができます。ESP ペイロードは、パケット自体のペイロードの直前の 8 バイトの CMD フィールドを伝送するように変更されます。たとえば、インターネット経由で送信される暗号化された Internet Control Message Protocol（ICMP）パケットには [IP][ESP][CMD][IP][ICMP][DATA] が含まれています。

詳細については、記事の第 2 部で説明します。

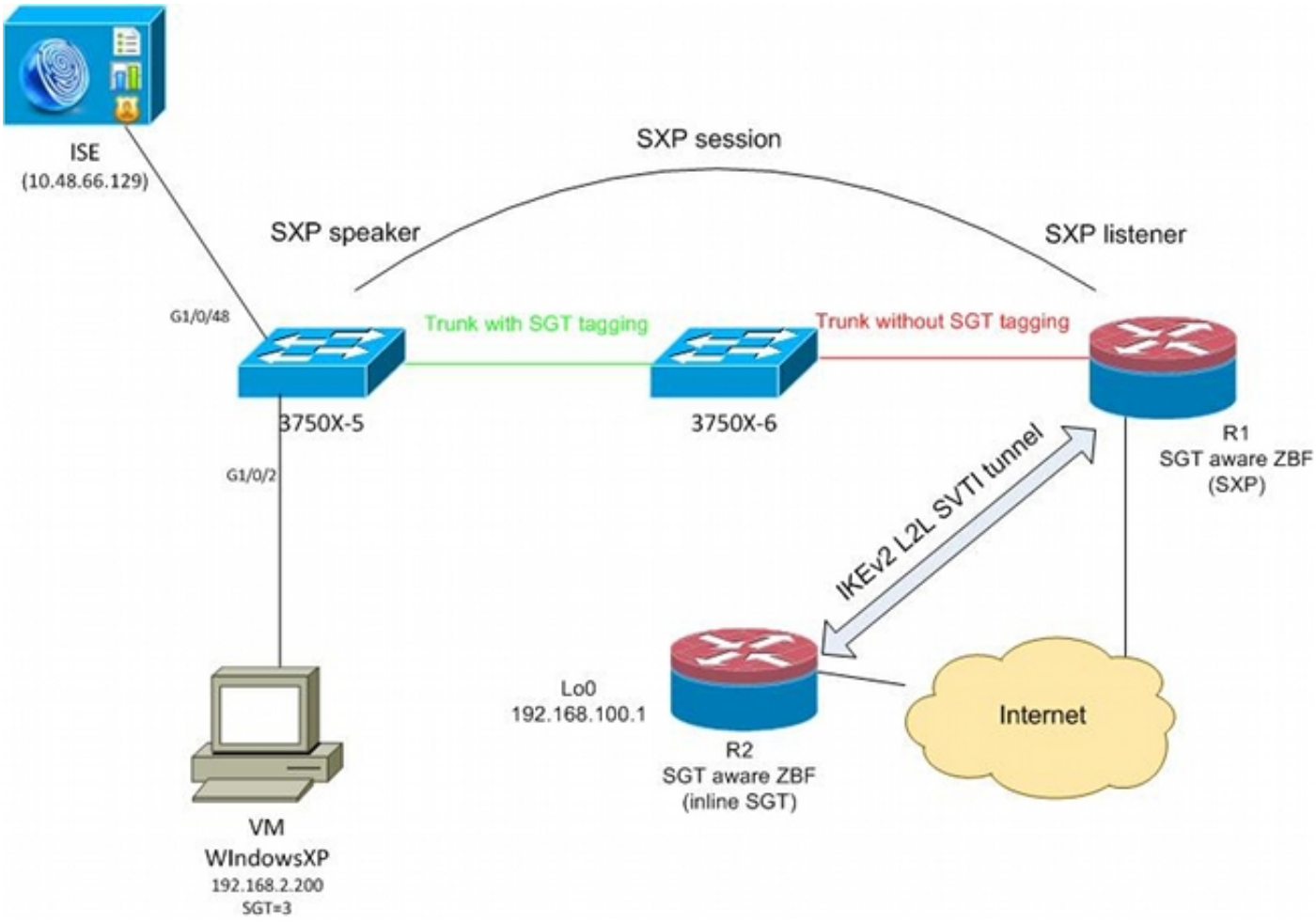
# 設定

**注：**

アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

**debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。**

## ネットワーク図




## Traffic flow

このネットワークでは、3750X-5 と 3750X-6 が TrustSec クラウド内部の Catalyst スイッチです。両方のスイッチでクラウドに参加するために自動 Protected Access Credential ( PAC ) プロビジョニングが使用されます。3750X-5 はシードとして、3750X-6 は非シード デバイスとして使用されます。両方のスイッチ間のトラフィックは、MACsec で暗号化され、正しくタグ付けされます。

Windows XP では、ネットワークにアクセスするために 802.1x が使用されます。認証に成功すると、ISE はそのセッションに適用する SGT タグ属性を返します。その PC から発信されたすべてのトラフィックに SGT=3 を使用したタグが付けられます。

ルータ 1 ( R1 ) とルータ 2 ( R2 ) は 2901 ISR です。ISR G2 は、現在、SGT タギングをサポートしていないため、R1 と R2 は TrustSec クラウドの外部に配置され、SGT タグを渡すように CMD フィールドが変更されたイーサネット フレームを認識しません。そのため、3750X-5 から R1 への IP/SGT マッピングに関する情報を転送するために SXP が使用されます。

R1 には、リモート ロケーション ( 192.168.100.1 ) 宛てのトラフィックを保護するように設定され、インライン タギングが有効になっている IKEv2 トンネルが設置されています。IKEv2 ネゴシエーション後に、R1 が R2 に送信される ESP パケットへのタグ付けを開始します。タギングは 3750X-5 から受信した SXP データに基づきます。

R2 は、そのトラフィックを受信して、受信した SGT タグに基づいて、ZBF で定義された特定のアクションを実行することができます。

R1 上でも同じアクションを実行できます。SXP マッピングを使用すれば、R1 は、SGT フレームがサポートされていない場合でも、SGT タグに基づいて LAN から受信したパケットをドロップすることができます。

## TrustSec クラウドの設定

設定の最初のステップは、TrustSec クラウドを構築することです。両方の 3750 スイッチで以下を実行する必要があります。

- TrustSec クラウド（ISE）に対する認証に使用される PAC を取得します。
- ネットワーク デバイス アドミッション コントロール（NDAC）プロセスを認証して通過させます。
- リンク上での MACsec ネゴシエーションに Security Association Protocol（SAP）を使用します。

このステップは、この使用例には必要ですが、SXP プロトコルが正しく機能するために必要なわけではありません。R1 は、SXP マッピングと IKEv2 インライン タギングを実行するために ISE から PAC または環境データを取得する必要はありません。

### 確認

3750X-5 と 3750X-6 間のリンクでは、802.1x によってネゴシエートされた MACsec 暗号化が使用されます。両方のスイッチが、ピアによって受信された SGT タグを信頼して受け入れます。

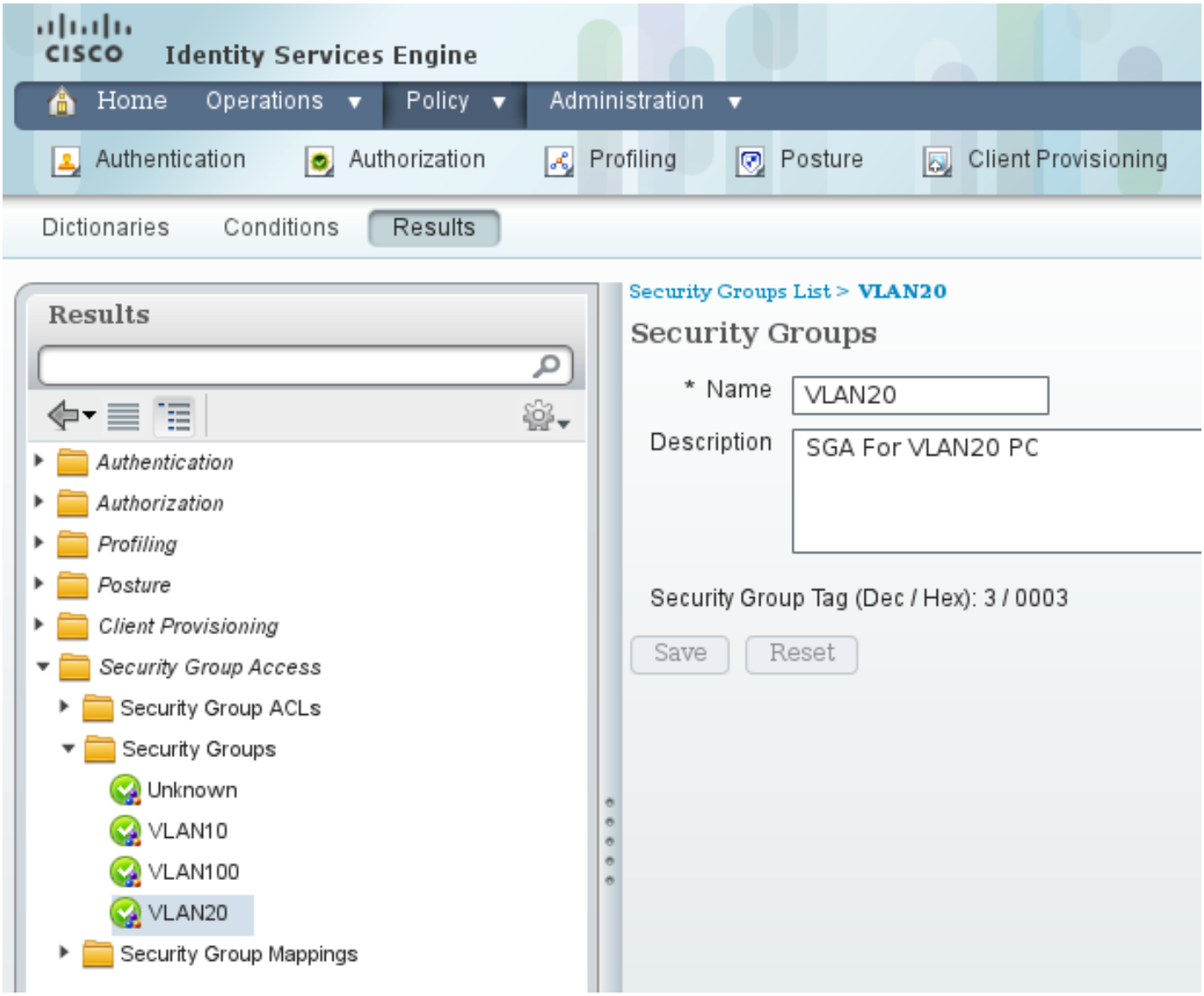
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X 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
```

スイッチ上で直接ロールベース アクセス コントロール リスト（RBACL）を適用することはできません。これらのポリシーは、ISE 上で設定され、自動的にスイッチにダウンロードされます。

## クライアントの設定

クライアントは、802.1x、MAC 認証バイパス（MAB）、または Web 認証を使用できます。正しい認可ルールのセキュリティ グループが返されるように ISE を設定してください。




### 確認

クライアントの設定を検証します。

```
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
```

これ以降、3750X-5 から TrustSec クラウド内の他のスイッチに送信されるクライアント トラフィックは SGT=3 を使用してタグ付けされます。

認可ルールの例については、「ASA および Catalyst 3750X シリーズ スイッチ TrustSec の設定例およびトラブルシューティング ガイド」を参照してください。

## 3750X-5 と R1 間の SGT Exchange Protocol

R1 は、CMD フィールドを含むイーサネット フレームを認識しない 2901 ISR G2 ルータのため、TrustSec クラウドに参加できません。したがって、SXP は 3750X-5 上で設定されます。

```
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
```

SXP は R1 上でも設定されます。

```
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
```

### 確認

R1 が IP/SGT マッピング情報を受信していることを確認します。

```
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
```

この時点で、R1 は、192.168.2.200 から受信したすべてのトラフィックを SGT=3 としてタグ付けされているかのように処理する必要があることを認識しています。

## R1 と R2 間の IKEv2 の設定

これは、IKEv2 スマート デフォルトを使用した単純な Static Virtual Tunnel Interface ( SVTI ) ベースのシナリオです。事前共有キーが認証に使用され、null 暗号化が ESP パケット分析を容易にするために使用されます。192.168.100.0/24 へのすべてのトラフィックが、Tunnel1 インターフェイス経由で送信されます。

これは R1 の設定です。

```
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
```

R2 では、ネットワーク 192.168.2.0/24 宛てのすべてのリターン トラフィックが Tunnel1 インターフェイス経由で送信されます。

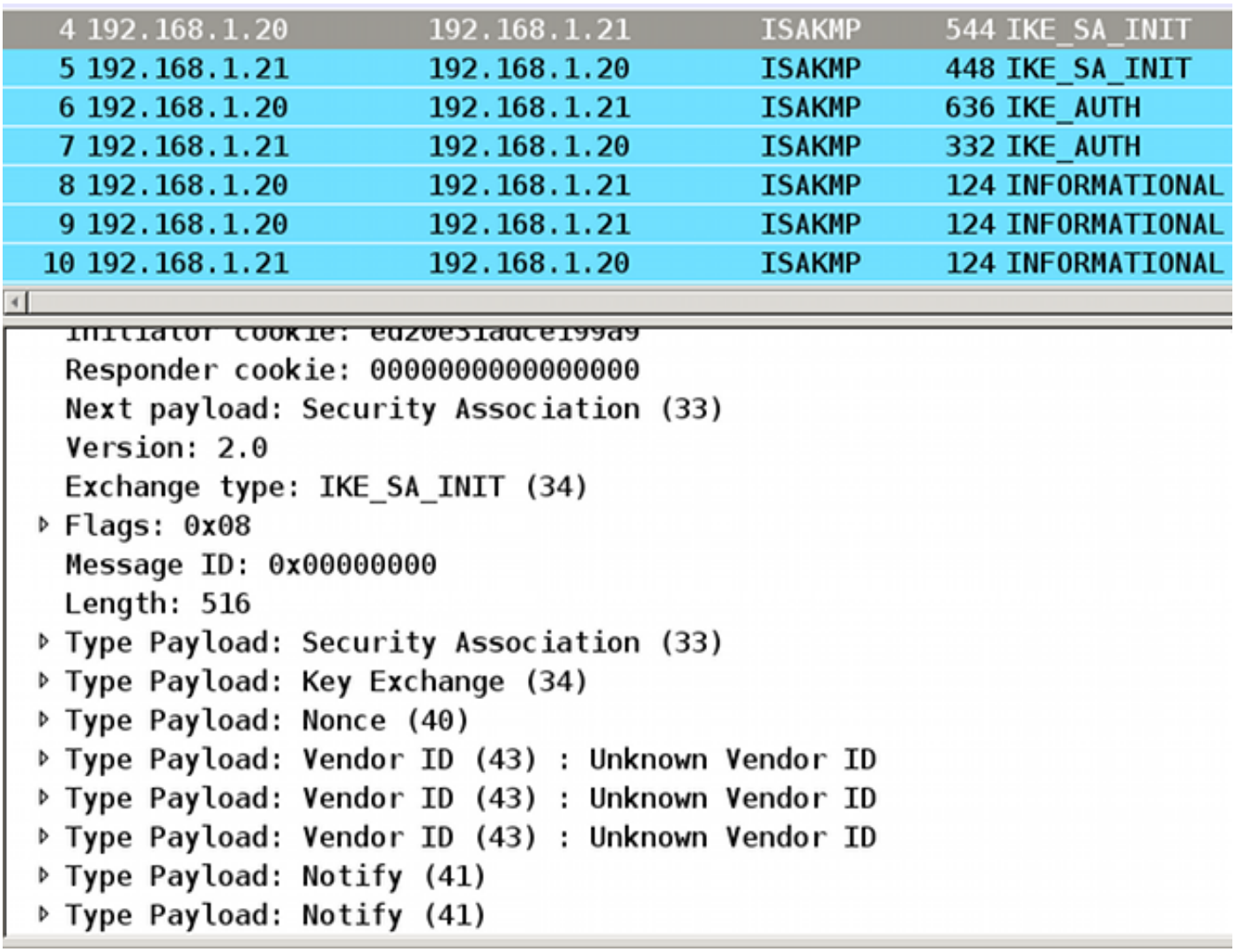
```
crypto ikev2 keyring ikev2-keyring
```

```
 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
```

両方のルータでインラインタギングを有効にするために必要なコマンドは、crypto ikev2 cts sgtコマンドだけです。

## 確認

インライン タギングをネゴシエートする必要があります。1 つ目と 2 つ目の IKEv2 パケットで、特定のベンダー ID が送信されています。




Wireshark で認識されない 3 つのベンダー ID ( VID ) があります。それらは以下に関係します。

- シスコでサポートされる DELETE-REASON
- シスコでサポートされる FlexVPN
- SGT インライン タギング

これをデバッグで検証します。IKEv2 イニシエータである R1 が以下を送信します。

```
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 が 2 つ目の IKEv2 パケットと同じ VID を受信します。

```
*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
```

そのため、両側で ESP ペイロードの先頭への CMD データの挿入に同意します。

IKEv2 セキュリティ アソシエーション（SA）をチェックして、この同意を検証します。

```
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
```

Windows クライアントから 192.168.100.1 にトラフィックが送信されたら、R1 が以下を表示します。

```
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#
```

タグ付きのパケットが送信されていることに注意してください。

中継トラフィックでは、R1 が Windows クライアントから R2 に送信されるトラフィックにタグ付けする必要がある場合に、ESP パケットが SGT=3 を使用して正しくタグ付けされていることを確認します。

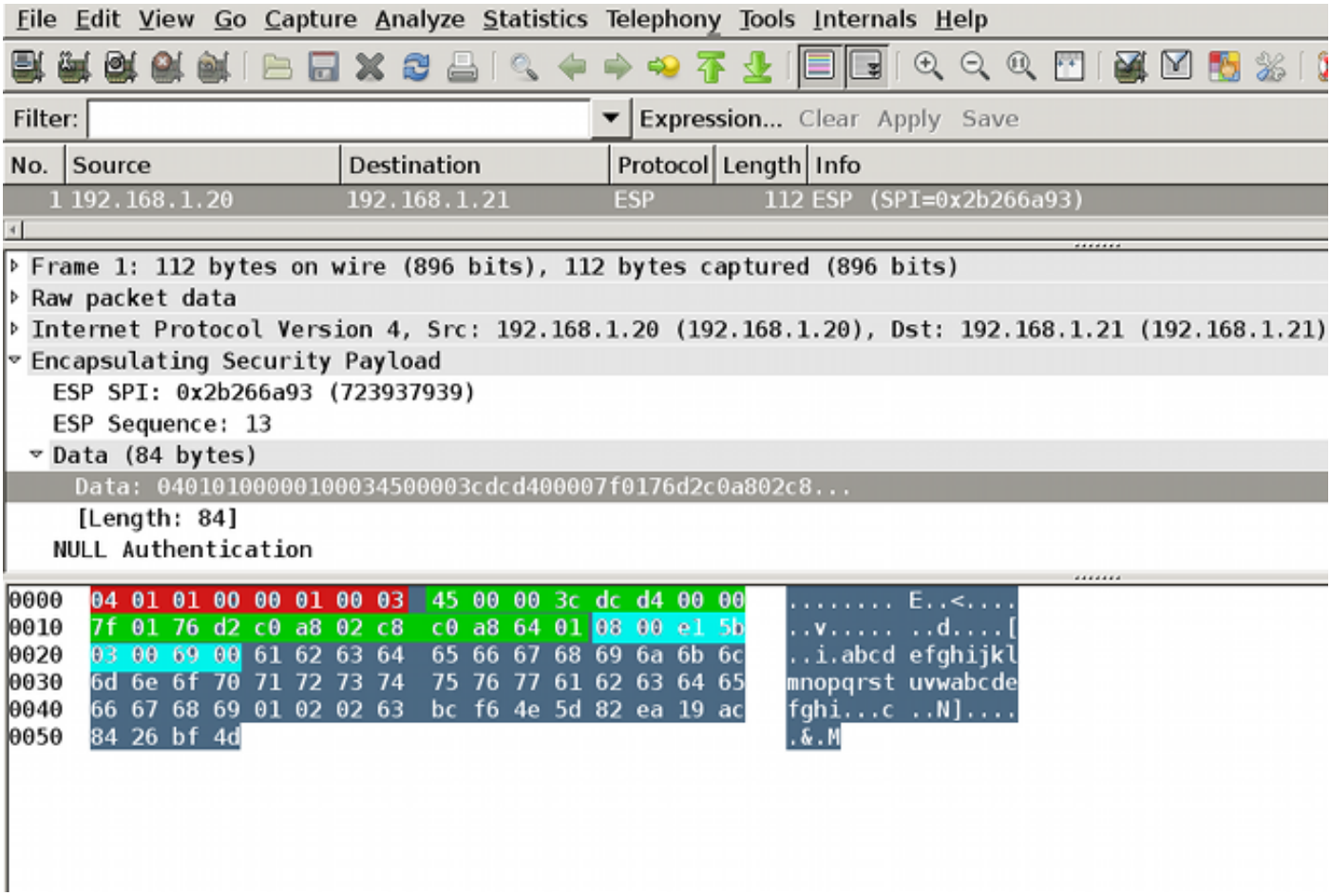
```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

スイッチから発信された同じ VLAN からの他のトラフィックはデフォルトで SGT=0 に設定されます。

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

## ESP パケット レベルの確認

次の図に示すように、Embedded Packet Capture（EPC）を使用して R1 から R2 への ESP トラフィックを確認します。




Wireshark は、セキュリティ パラメータ インデックス（SPI）の null 暗号化をデコードするために使用されます。IPv4 ヘッダー内の送信元 IP と宛先 IP はルータのインターネット IP アドレスです（トンネルの送信元と宛先として使用されます）。

ESP ペイロードには、赤色で強調表示された 8 バイトの CMD フィールドが含まれています。

- 0x04：IP である次のヘッダー
- 0x01：長さ（ヘッダーの後ろの 4 バイト、ヘッダーを含めて 8 バイト）
- 0x01：バージョン 01
- 0x00：予約済み
- 0x00：SGT 長（全部で 4 バイト）
- 0x01：SGT タイプ
- 0x0003:SGTタグ（最後の2オクテットは00 03。SGTはWindowsクライアントに使用される

）
IPsec IPv4 モードがトンネル インターフェイスに使用されているため、緑色で強調表示された次のヘッダーが IP です。送信元 IP は c0 a8 02 c8（192.168.2.200）で、宛先 IP は c0 a8 64 01（192.168.100.1）です。プロトコル番号は ICMP を表す 1 です。

最後のヘッダーは、タイプ 08 とコード 8（エコー要求）の青色で強調表示された ICMP です。

次が ICMP ペイロードで、32 バイト長（つまり、a から i までの文字）です。図のペイロードは Windows クライアントに典型的なものです。

残りの ESP ヘッダーが ICMP ペイロードに続きます。

- 0x01 0x02：パディング。
- 0x02：パディング長。
- 0x63：「任意のプライベート暗号化方式」のプロトコル 0x63 を指す次のヘッダー。 これは、次のフィールド（ESP データ内の最初のフィールド）が SGT タグであることを示します。
- 12 バイトの整合性チェック値。

CMD フィールドは、通常は暗号化される ESP ペイロード内にあります。

## IKEv2の落とし穴：GREまたはIPsecモード

ここまでは、これらの例でトンネル モード IPsec IPv4 を使用してきました。総称ルーティングカプセル化(GRE)モードを使用するとどうなりますか。

ルータが中継 IP パケットを GRE 内にカプセル化すると、TrustSec がローカルに発信されたものとしてそのパケットを表示します。つまり、GRE パケットの送信元が Windows クライアントではなく、ルータになります。CMD フィールドが追加された場合は、常に、特定のタグの代わりにデフォルト タグ（SGT=0）が使用されます。

トラフィックが IPsec IPv4 モードの Windows クライアント（192.168.2.200）から送信された場合は、SGT=3 が表示されます。

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

ただし、同じトラフィックのトンネル モードが GRE に変更されたら、SGT=0 が表示されます。この例では、192.168.1.20 がトンネル送信元 IP です。

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

**注**：したがって、GREを使用しないことは非常に重要です。

Cisco Bug ID CSCuj25890、「GREモードのIOS IPSecインラインタギング：ルータSGTの挿入」を参照してください。このバグは、GRE を使用するときに適切な SGT 伝搬を可能にするために作成されました。DMVPN上のSGTは、Cisco IOS® XE 3.13Sからサポートされます。

## IKEv2 からの SGT タグに基づく ZBF

これは R2 上での ZBF の設定例です。SGT=3 の VPN トラフィックは、IKEv2 トンネルから受信されたすべてのパケットがタグ付けされている ( つまり、CMD フィールドが含まれている ) ことから識別できます。したがって、VPN トラフィックをドロップして、ログに記録することができます。

```
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
```

## 確認

192.168.100.1 への ping が Windows クライアント ( SGT=3 ) から送信された場合は、デバッグに次のように表示されます。

```
*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
```

ping がスイッチ ( SGT=0 ) から送信された場合は、デバッグに次のように表示されます。

```
*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
```

R2 からのファイアウォール統計情報を以下に示します。

```
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
```

4 つのドロップ ( Windows によって送信された ICMP エコーのデフォルト数 ) と 5 つの承認 ( スイッチのデフォルト数 ) が確認できます。

## SXP 経由の SGT マッピングに基づく ZBF

R1 上で SGT 対応 ZBF を実行して、LAN から受信されたトラフィックをフィルタリングすることができます。このトラフィックは SGT タグが付けられていませんが、R1 は SXP マッピング情報を入手して、そのトラフィックをタグ付きとして処理できます。

この例では、LAN ゾーンと VPN ゾーンの間でポリシーが使用されます。

```
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
```

### 確認

ICMP エコーが Windows クライアントから送信された場合は、ドロップを確認できます。

```
*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
```

SXP セッションは TCP に基づいているため、3750X-5 と R2 間の IKEv2 トンネル経由で SXP セッションを構築し、インライン タギングを使用せずに、R2 上のタグに基づいて ZBF ポリシーを適用することもできます。

# ロードマップ

GET VPN インライン タギングは、ISR G2 と Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上でもサポートされます。ESP パケットには CMD フィールド用の追加の 8 バイトが含まれています。

Dynamic Multipoint VPN（DMVPN）のサポートも予定されています。

詳細については、「シスコ TrustSec 対応インフラストラクチャ」ロードマップを参照してください。

# 確認

設定例には検証手順も記載されています。

# 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。

## 関連情報

- Cisco TrustSecスイッチ設定ガイド：Cisco TrustSecについて
- ブック1: Cisco ASAシリーズの一般的な操作CLIコンフィギュレーションガイド、9.1:Cisco TrustSecと統合するためのASAの設定
- Cisco TrustSec General Availabilityリリースのリリースノート：Cisco TrustSec 3.0 General Deployability 2013リリースのリリースノート
- TrustSec 用の IPSec インライン タギングの設定
- Cisco Group Encrypted Transport VPNコンフィギュレーションガイド、Cisco IOS XEリリース3S:Cisco TrustSecのIPsecインラインタギングのGET VPNサポート
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。