具有TrustSec SGT内联标记和SGT感知区域防火墙的IKEv2配置示例

目录

简介

本文档介绍如何使用Internet密钥交换版本2(IKEv2)和安全组标记(SGT)来标记发送到VPN隧道的数据包。说明包括典型的部署和使用案例。本文档还介绍了SGT感知区域防火墙(ZBF)，并提供了两种场景：

- 基于从IKEv2隧道接收的SGT标记的ZBF
- 基于SGT交换协议(SXP)映射的ZBF

所有示例都包括数据包级别调试，以验证SGT标记如何传输。

先决条件

要求

Cisco 建议您了解以下主题：

- TrustSec组件的基础知识
- Cisco Catalyst交换机命令行界面(CLI)配置的基本知识
- 配置思科身份服务引擎(ISE)的经验
- 基于区域的防火墙的基本知识
- IKEv2基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7和Microsoft Windows XP
- Cisco Catalyst 3750-X软件版本15.0及更高版本
- 思科身份服务引擎软件1.1.4版及更高版本
- 软件版本为15.3(2)T或更高版本的Cisco 2901集成多业务路由器(ISR)

  注：仅ISR第2代(G2)平台支持IKEv2。

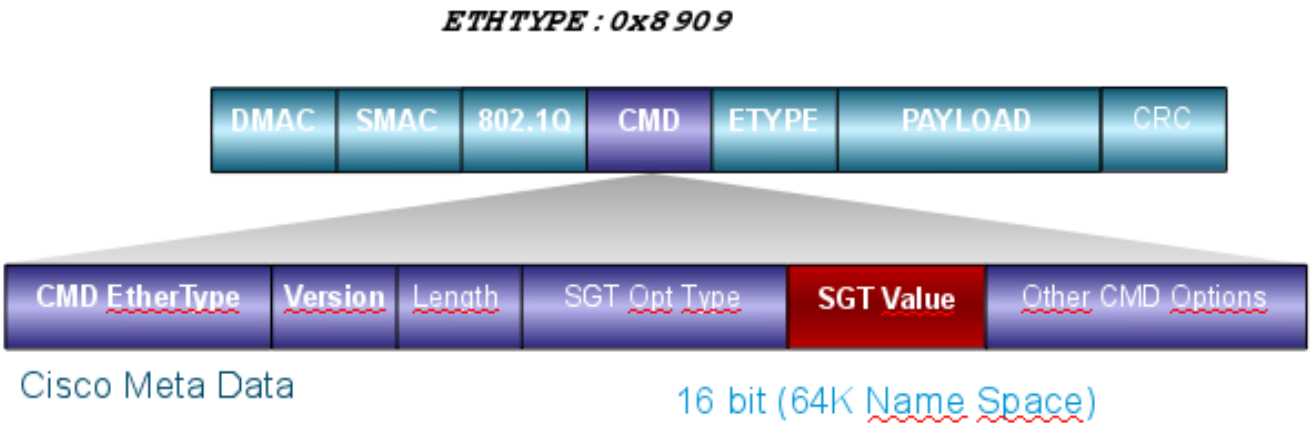
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

安全组标记(SGT)

SGT是Cisco TrustSec解决方案架构的一部分，旨在使用不基于IP地址的灵活安全策略。

对TrustSec云中的流量进行分类并使用SGT标记进行标记。您可以构建基于该标记过滤流量的安全策略。所有策略都从ISE集中管理，并部署到TrustSec云中的所有设备。

为了传递有关SGT标记的信息，思科修改了以太网帧，类似于对802.1q标记进行修改的方式。只有选定的Cisco设备才能理解修改的以太网帧。这是修改的格式：



思科元数据(CMD)字段直接插入源MAC地址字段(SMAC)或802.1q字段（如本例所示）之后。

要通过VPN连接TrustSec云，已创建IKE和IPsec协议的扩展。称为IPsec内联标记的扩展允许在封装安全负载(ESP)数据包中发送SGT标记。ESP负载经过修改，在数据包本身负载之前携带8字节的CMD字段。例如，通过Internet发送的加密互联网控制消息协议(ICMP)数据包包含[IP][ESP][CMD][IP][ICMP][DATA]。

本文第二部分介绍了详细资料。

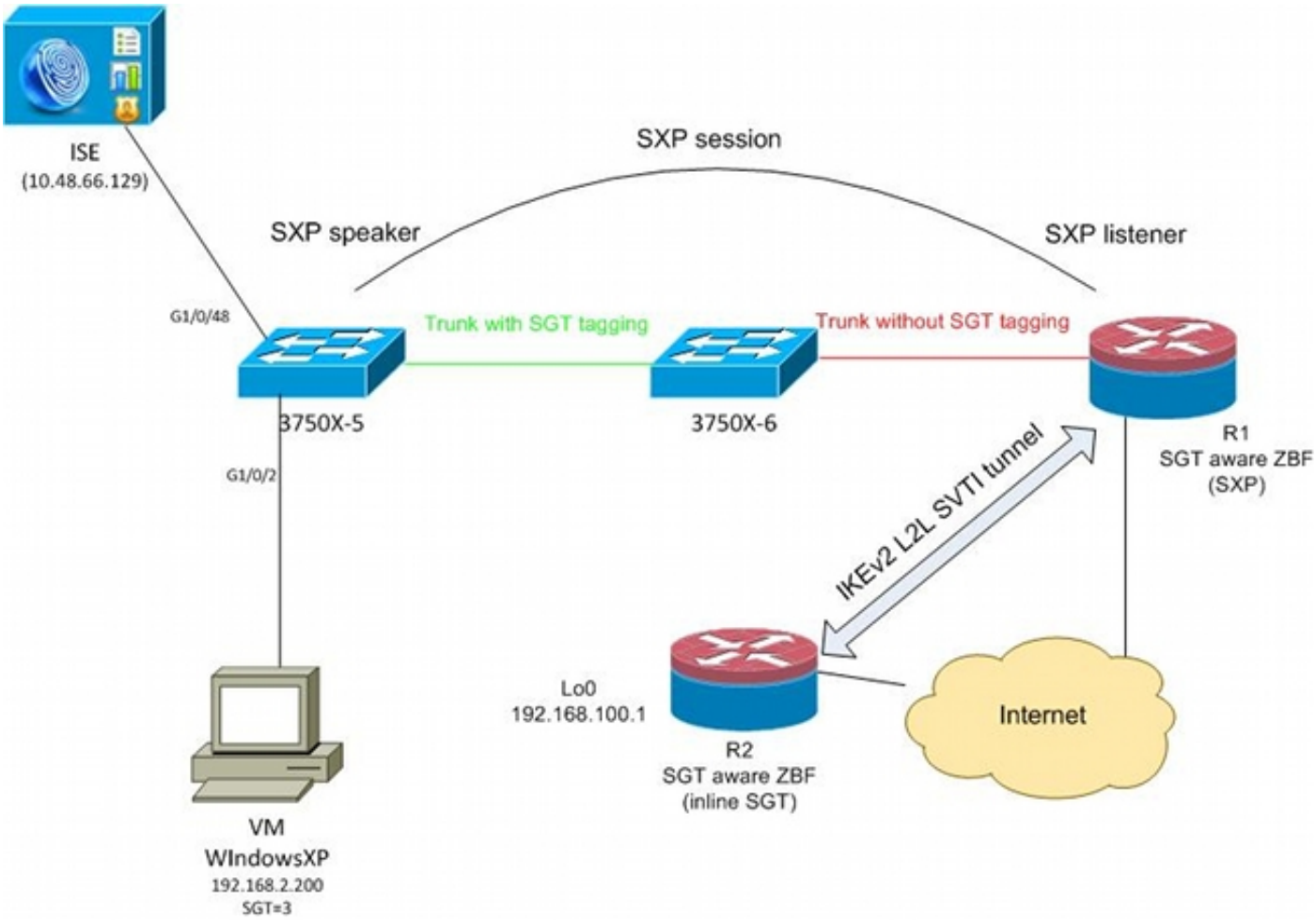
配置

注意：

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

网络图



流量传输

在此网络中，3750X-5和3750X-6是TrustSec云中的Catalyst交换机。两台交换机都使用自动保护访问凭证(PAC)调配来加入云。3750X-5已用作种子，3750X-6已用作非种子设备。两台交换机之间的流量使用MACsec进行加密并正确标记。

Windows XP使用802.1x来访问网络。身份验证成功后，ISE返回将应用于该会话的SGT标记属性。源自该PC的所有流量都使用SGT=3标记。

Router 1(R1)和Router 2(R2)是2901 ISR。由于ISR G2当前不支持SGT标记，因此R1和R2位于TrustSec云之外，不了解通过CMD字段修改以传递SGT标记的以太网帧。因此，使用SXP将有关IP/SGT映射的信息从3750X-5转发到R1。

R1有一个IKEv2隧道，该隧道配置为保护发往远程位置(192.168.100.1)的流量，并且已启用内联标记。在IKEv2协商后，R1开始标记发送到R2的ESP数据包。标记基于从3750X-5接收的SXP数据。

R2可以接收该流量，并根据收到的SGT标记执行ZBF定义的特定操作。

R1上也可以执行相同操作。SXP映射允许R1根据SGT标记丢弃从LAN接收的数据包，即使不支持SGT帧也是如此。

TrustSec云配置

配置的第一步是构建TrustSec云。两台3750交换机都需要：

- 获取用于对TrustSec云(ISE)进行身份验证的PAC。
- 验证并通过网络设备准入控制(NDAC)进程。
- 在链路上使用安全关联协议(SAP)进行MACsec协商。

此步骤对于此用例是必需的，但对于SXP协议正常工作不是必需的。R1不需要从ISE获取PAC或环境数据以执行SXP映射和IKEv2内联标记。

确认

3750X-5和3750X-6之间的链路使用802.1x协商的MACsec加密。两台交换机都信任并接受对等体收到的SGT标记：

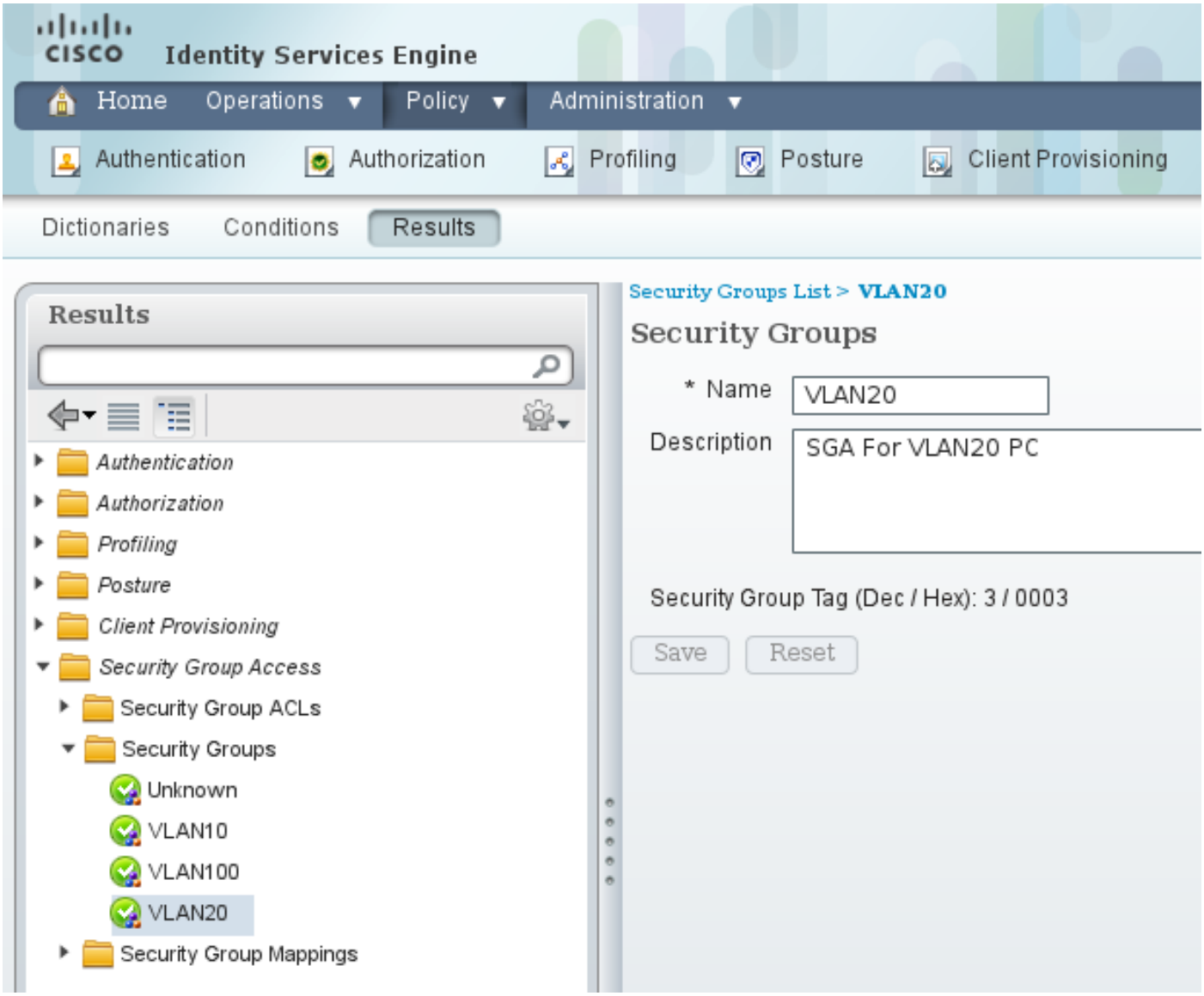
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X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

无法直接在交换机上应用基于角色的访问控制列表(RBACL)。这些策略在ISE上配置并自动下载到交换机上。

客户端配置

客户端可以使用802.1x、MAC身份验证绕行(MAB)或Web身份验证。请记住配置ISE，以便返回授

权规则的正确安全组：



确认

验证客户端配置：

```
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
```

从此以后，从3750X-5发送到TrustSec云内其他交换机的客户端流量标记为SGT=3。

有关授权规则的示例，请参阅ASA和Catalyst 3750X系列交换机TrustSec配置示例和故障排除指南。

3750X-5和R1之间的SGT交换协议

R1无法加入TrustSec云，因为它是一台2901 ISR G2路由器，无法识别带有CMD字段的以太网帧。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
```

确认

确保R1正在接收IP/SGT映射信息：

```
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现在知道，从192.168.2.200接收的所有流量都应被视为标记为SGT=3。

R1和R2之间的IKEv2配置

这是一个基于SVTI的简单静态虚拟隧道接口(SVTI)场景，具有IKEv2智能默认值。预共享密钥用于身份验证，而空加密用于简化ESP数据包分析。到192.168.100.0/24的所有流量都通过Tunnel1接口发送。

这是 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，所有返回网络192.168.2.0/24的流量都通过Tunnel1接口发送：

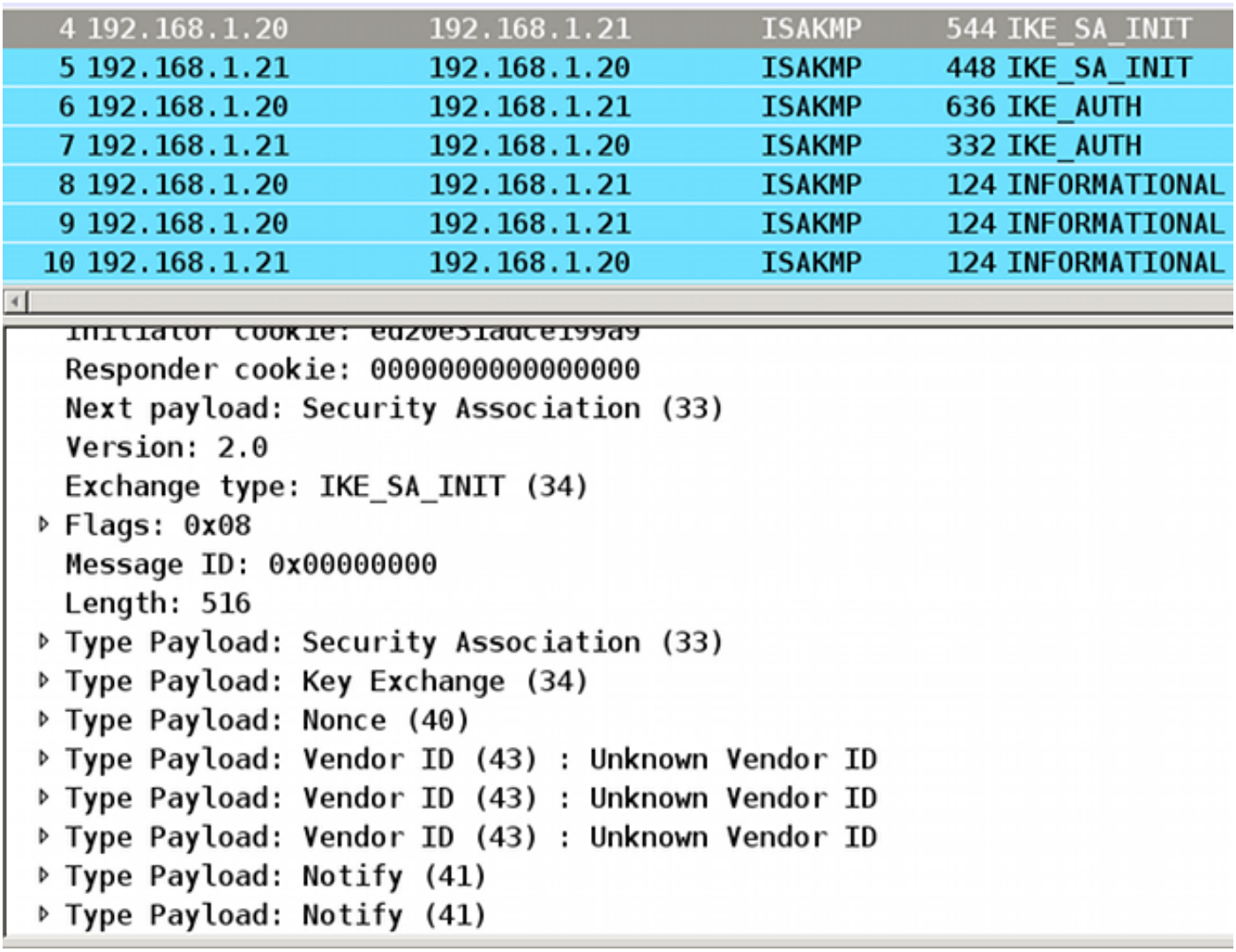
```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.20
 address 192.168.1.20
 pre-shared-key cisco

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
```

两台路由器上只需一个命令即可启用内联标记：**crypto ikev2 cts sgt**命令。

确认

需要协商内联标记。在第一和第二个IKEv2数据包中，正在发送特定供应商ID:



有三个供应商ID(VID)是Wireshark未知的。它们与：

- DELETE-REASON，思科支持
- 思科支持的FlexVPN
- SGT内联标记

调试会验证这一点。R1是IKEv2发起方，它发送：

```
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收到第二个IKEv2数据包和相同的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，两端都同意在ESP负载的开始处放置CMD数据。

检查IKEv2安全关联(SA)以验证此协议：

```
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
```

从Windows客户端向192.168.100.1发送流量后，R1显示：

```
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#
```

请注意，已发送标记的数据包。

对于中转流量，当R1需要标记从Windows客户端发送到R2的流量时，请确认ESP数据包已正确标记为SGT=3:

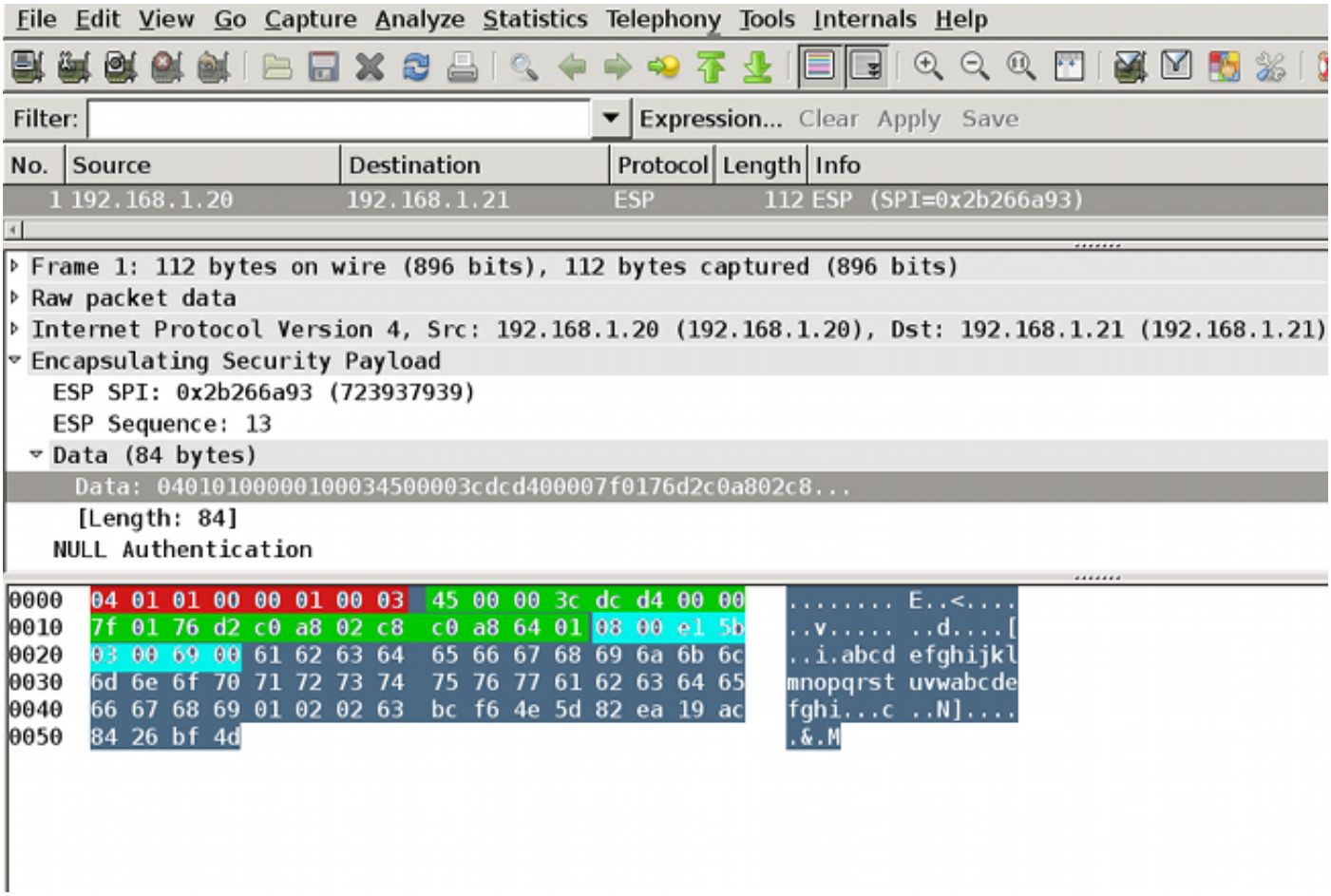
```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

来自同一VLAN（源自交换机）的其他流量默认为SGT=0:

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

ESP数据包级别验证

使用嵌入式数据包捕获(EPC)查看从R1到R2的ESP流量，如下图所示：



Wireshark已用于解码安全参数索引(SPI)的空加密。在IPv4报头中，源和目的IP是路由器的Internet

IP地址（用作隧道源和目的）。

ESP负载包括8字节的CMD字段，该字段以红色突出显示：

- 0x04 — 下一个报头，即IP
- 0x01 — 长度（报头后4个字节，报头后8个字节）
- 0x01 — 版本01
- 0x00 — 保留
- 0x00 - SGT长度（共4个字节）
- 0x01 - SGT类型
- 0x0003 - SGT标记（最后两个二进制八位数，即00 03;SGT用于Windows客户端）

由于隧道接口已使用IPsec IPv4模式，因此下一报头是IP，以绿色突出显示。源IP是c0 a8 02 c8(192.168.2.200)，目的IP是c0 a8 64 01(192.168.100.1)。协议编号为1，即ICMP。

最后一个报头是ICMP，以蓝色突出显示，带有类型08和代码8（回应请求）。

接下来是ICMP负载，长度为32个字节（即从a到i的字母）。图中的负载是Windows客户端的典型负载。

ESP报头的其余部分遵循ICMP负载：

- 0x01 0x02 — 填充。
- 0x02 — 填充长度。
- 0x63 — 指向协议0x63的下一个报头，该协议是“任何私有加密方案”。 这表示下一个字段（ESP数据中的第一个字段）是SGT标记。
- 完整性检查值的12个字节。

CMD字段位于ESP负载（通常加密）内部。

IKEv2缺陷：GRE或IPsec模式

到目前为止，这些示例都使用隧道模式IPsec IPv4。如果使用通用路由封装(GRE)模式，会发生什么情况？

当路由器将中转IP数据包封装到GRE中时，TrustSec会将数据包视为本地数据包，即GRE数据包的来源是路由器，而不是Windows客户端。添加CMD字段时，始终使用默认标记(SGT=0)而不是特定标记。

当流量从IPsec IPv4模式下的Windows客户端(192.168.2.200)发送时，您将看到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，将相同流量的隧道模式更改为GRE后，您会看到SGT=0。在本示例中，192.168.1.20是隧道源IP:

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

注意：因此，不使用**GRE非常重要**。

请参阅Cisco Bug ID CSCuj25890,GRE模式的IOS IPSec内联标记：插入路由器SGT。创建此Bug是为了在您使用GRE时允许正确的SGT传播。Cisco IOS® XE 3.13S支持基于DMVPN的SGT

基于IKEv2的SGT标记的ZBF

这是R2上ZBF的配置示例。可以识别SGT=3的VPN流量，因为从IKEv2隧道接收的所有数据包都已标记（即，它们包含CMD字段）。因此，可以丢弃并记录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
```

确认

当从Windows客户端(SGT=3)对192.168.100.1执行ping操作时，调试显示如下：

```
*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
```

对于从交换机(SGT=0)发出的ping，调试显示如下：

```
*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
```

来自R2的防火墙统计信息如下：

```
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
```

有四个丢弃（Windows发送的ICMP回应的默认数量）和五个接受（交换机的默认数量）。

基于SGT映射的ZBF通过SXP实现

可以在R1上运行SGT感知ZBF并过滤从LAN接收的流量。虽然该流量没有SGT标记，但R1具有SXP映射信息，可以将该流量视为已标记。

在本示例中，在LAN和VPN区域之间使用策略：

```
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
```

确认

从Windows客户端发送ICMP回应时，您可以看到丢包：

```
*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
```

由于SXP会话基于TCP，因此您还可以通过IKEv2隧道在3750X-5和R2之间构建SXP会话，并基于R2上的标记应用ZBF策略，而无需内联标记。

路线图

ISR G2和Cisco ASR 1000系列聚合服务路由器也支持GET VPN内联标记。ESP数据包的CMD字段另外有8个字节。

还计划支持动态多点VPN(DMVPN)。

有关详细信息，请参阅支持Cisco TrustSec的基础设施路线图。

验证

验证过程包含在配置示例中。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco TrustSec交换机配置指南：了解Cisco TrustSec
- 第1册：Cisco ASA系列常规操作CLI配置指南，9.1：配置ASA以与Cisco TrustSec集成
- Cisco TrustSec通用可用性版本说明：Cisco TrustSec 3.0通用可部署性2013版版本说明
- 为TrustSec配置IPsec内联标记
- Cisco Group Encrypted Transport VPN配置指南，Cisco IOS XE版本3S:Cisco TrustSec的IPsec内联标记的GET VPN支持
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。