IKEv2 com Marcação em linha TrustSec SGT e exemplo de configuração de firewall baseado em zona com reconhecimento de SGT

Contents

Introduction

Este documento descreve como usar o Internet Key Exchange Version 2 (IKEv2) e uma marcação de grupo de segurança (SGT) para marcar os pacotes enviados a um túnel VPN. A descrição inclui uma implantação típica e um caso de uso. Este documento também explica um firewall baseado em zona (ZBF) com reconhecimento de SGT e apresenta dois cenários:

- Um ZBF baseado nas marcas SGT recebidas do túnel IKEv2
- Um ZBF baseado no mapeamento do SGT eXchange Protocol (SXP)

Todos os exemplos incluem depurações em nível de pacote para verificar como a tag SGT é transmitida.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico dos componentes do TrustSec
- Conhecimento básico da configuração da interface de linha de comando (CLI) dos switches Cisco Catalyst
- Experiência na configuração de um Cisco Identity Services Engine (ISE)
- Conhecimento básico de firewall baseado em zona
- Conhecimento básico de IKEv2

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7 e Microsoft Windows XP
- Software Cisco Catalyst 3750-X versão 15.0 e posterior
- Software Cisco Identity Services Engine versão 1.1.4 e posterior
- Cisco 2901 Integrated Services Router (ISR) com Software versão 15.3(2)T ou posterior

Observação: o IKEv2 é suportado somente nas plataformas ISR Geração 2 (G2).

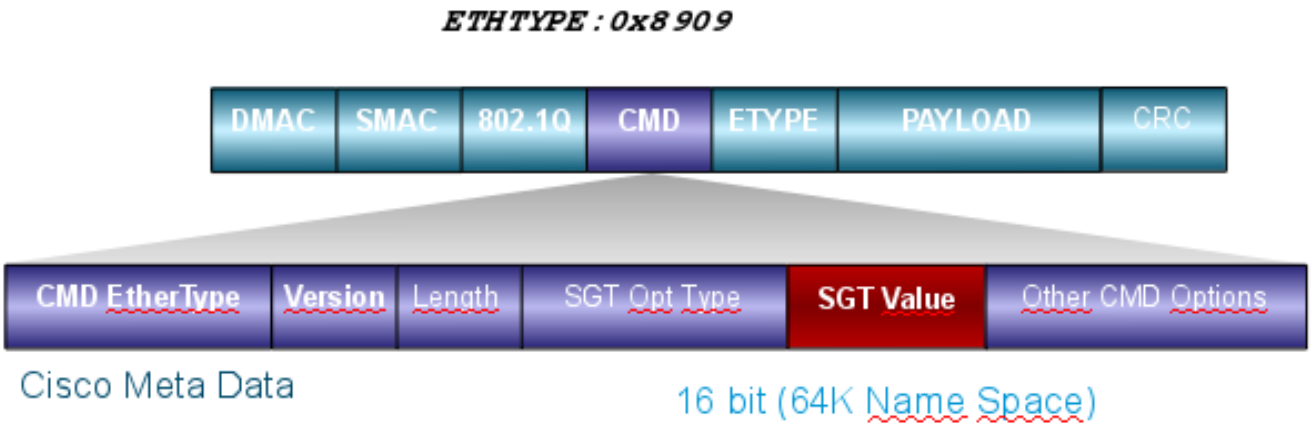
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Tag de grupo de segurança (SGT)

O SGT faz parte da arquitetura da solução Cisco TrustSec, que foi projetada para usar políticas de segurança flexíveis que não se baseiam no endereço IP.

O tráfego na nuvem TrustSec é classificado e marcado com uma marca SGT. Você pode criar políticas de segurança que filtram o tráfego com base nessa marca. Todas as políticas são gerenciadas centralmente pelo ISE e implantadas em todos os dispositivos na nuvem TrustSec.

Para passar as informações sobre a marca SGT, a Cisco modificou o quadro Ethernet de forma semelhante à forma como as modificações foram feitas para as marcas 802.1q. O quadro Ethernet modificado pode ser compreendido apenas por dispositivos Cisco selecionados. Este é o formato modificado:



O campo Cisco Meta Data (CMD) é inserido diretamente após o campo de endereço MAC de origem (SMAC) ou o campo 802.1q, se for usado (como neste exemplo).

Para conectar nuvens TrustSec via VPN, foi criada uma extensão para os protocolos IKE e IPsec. A extensão, chamada de marcação inline IPsec, permite que as marcas SGT sejam enviadas nos pacotes ESP (Encapsulating Security Payload). O payload ESP é modificado para transportar um campo CMD de 8 bytes logo antes do payload do próprio pacote. Por exemplo, o pacote criptografado do Internet Control Message Protocol (ICMP) enviado pela Internet contém [IP][ESP][CMD][IP][ICMP][DATA].

Informações detalhadas são apresentadas na segunda parte do artigo.

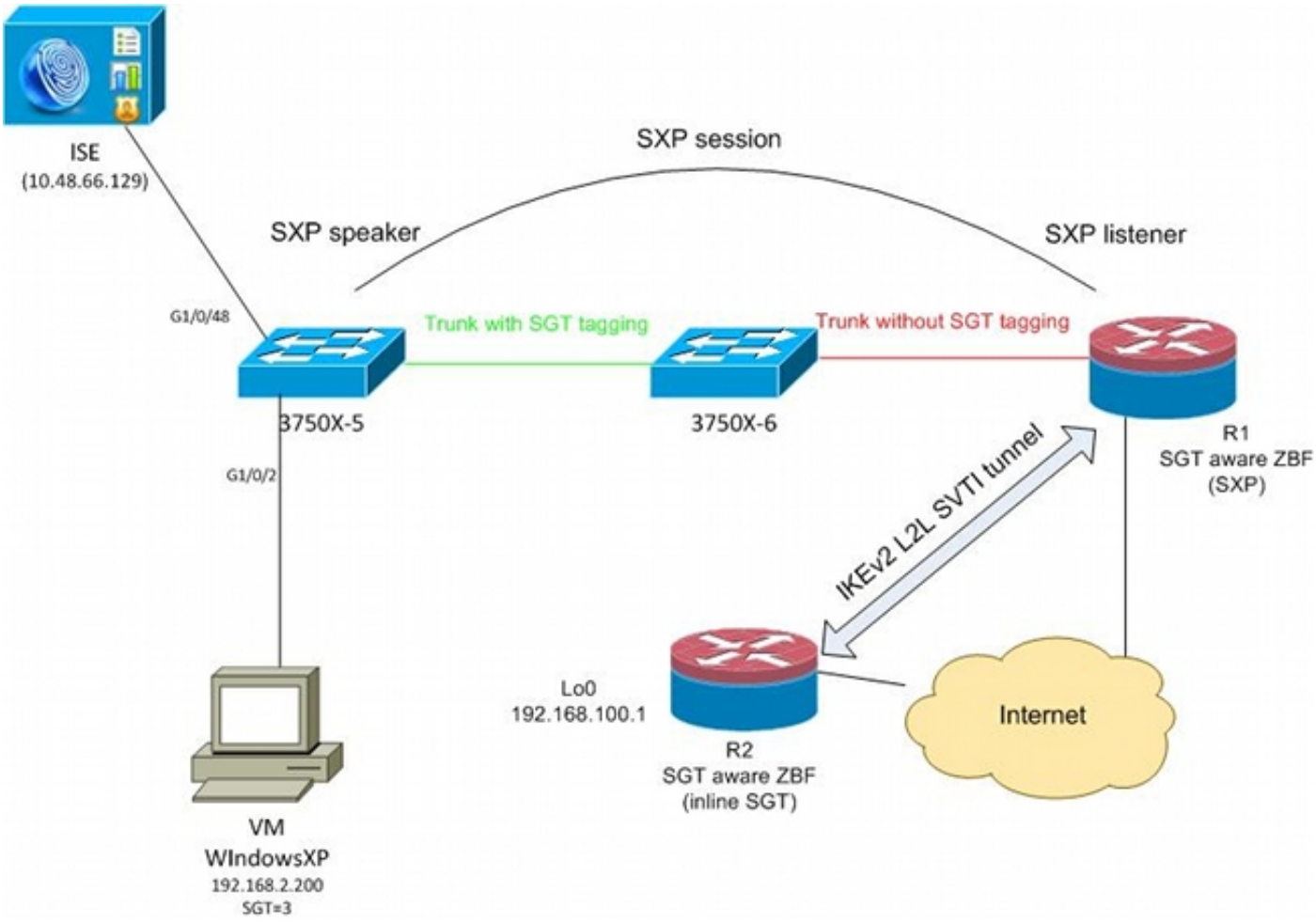
Configurar

Notas:

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Diagrama de Rede



Fluxo de tráfico

Nessa rede, 3750X-5 e 3750X-6 são switches Catalyst dentro da nuvem TrustSec. Ambos os switches usam o provisionamento automático de PACs (Protected Access Credentials) para ingressar na nuvem. O 3750X-5 foi usado como uma semente e o 3750X-6 como um dispositivo não semente. O tráfego entre os dois switches é criptografado com MACsec e é marcado corretamente.

O Windows XP usa 802.1x para acessar a rede. Após a autenticação bem-sucedida, o ISE retorna o atributo de tag SGT que será aplicado a essa sessão. Todo o tráfego originado nesse PC é marcado com SGT=3.

O roteador 1 (R1) e o roteador 2 (R2) são ISRs 2901. Como o ISR G2 atualmente não suporta marcação SGT, R1 e R2 estão fora da nuvem TrustSec e não entendem os quadros Ethernet que foram modificados com campos CMD para passar as marcas SGT. Assim, o SXP é usado para encaminhar informações sobre o mapeamento IP/SGT do 3750X-5 para o R1.

R1 tem um túnel IKEv2 configurado para proteger o tráfego destinado a um local remoto (192.168.100.1) e que tem a marcação em linha habilitada. Após a negociação de IKEv2, R1 começa a marcar pacotes ESP enviados a R2. A marcação é baseada nos dados do SXP recebidos do 3750X-5.

R2 pode receber esse tráfego e, com base na marca SGT recebida, pode executar ações específicas definidas pela ZBF.

O mesmo pode ser feito em R1. O mapeamento SXP permite que R1 descarte um pacote recebido da LAN com base em uma marca SGT, mesmo que os quadros SGT não sejam suportados.

Configuração de nuvem do TrustSec

A primeira etapa na configuração é criar uma nuvem TrustSec. Ambos os switches 3750 precisam:

- Obtenha uma PAC, que é usada para autenticação na nuvem do TrustSec (ISE).
- Autentique e passe o processo Network Device Admission Control (NDAC).
- Usar o protocolo SAP para negociação MACsec em um link.

Esta etapa é necessária para este caso de uso, mas não é necessária para que o protocolo SXP funcione corretamente. R1 não precisa obter uma PAC ou dados de ambiente do ISE para executar o mapeamento SXP e a marcação inline IKEv2.

Verificação

O link entre 3750X-5 e 3750X-6 usa criptografia MACsec negociada por 802.1x. Ambos os switches confiam e aceitam as marcas SGT recebidas pelo peer:

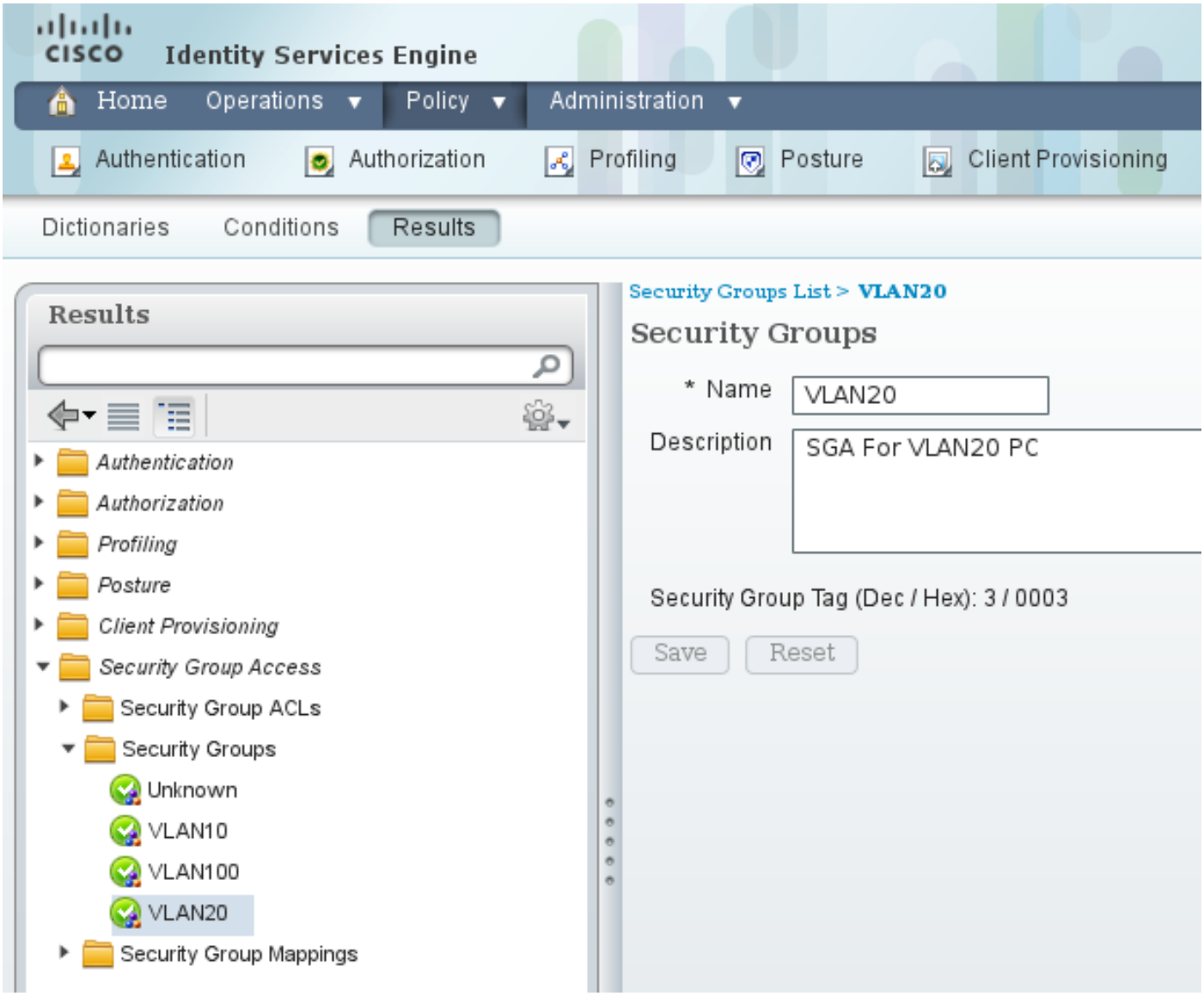
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X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

Não é possível aplicar uma lista de controle de acesso baseada em função (RBACL) diretamente nos switches. Essas políticas são configuradas no ISE e o download é feito automaticamente nos switches.

Configuração do Cliente

O cliente pode usar 802.1x, desvio de autenticação MAC (MAB) ou autenticação da Web. Lembre-se de configurar o ISE para que o grupo de segurança correto para a regra de autorização seja retornado:



Verificação

Verifique a configuração do cliente:

```
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
```

A partir desse ponto, o tráfego do cliente enviado do 3750X-5 para outros switches dentro da nuvem TrustSec é marcado com SGT=3.

Consulte Exemplo de Configuração e Troubleshooting do ASA e do Catalyst 3750X Series Switch TrustSec para obter um exemplo de regras de autorização.

Protocolo de troca SGT entre 3750X-5 e R1

R1 não pode se unir à nuvem TrustSec porque é um roteador 2901 ISR G2 que não entende os quadros Ethernet com campos CMD. Assim, o SXP é configurado no 3750X-5:

```
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
```

O SXP também é configurado em R1:

```
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
```

Verificação

Verifique se R1 está recebendo as informações de mapeamento de IP/SGT:

```
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 agora sabe que todo o tráfego recebido de 192.168.2.200 deve ser tratado como se estivesse marcado como SGT=3.

Configuração de IKEv2 entre R1 e R2

Este é um cenário simples baseado em Interfaces de túnel estático virtual (SVTI - Static Virtual Tunnel Interfaces) com padrões inteligentes IKEv2. As chaves pré-compartilhadas são usadas para autenticação e a criptografia nula é usada para facilitar a análise de pacotes ESP. Todo o tráfego para 192.168.100.0/24 é enviado através da interface Tunnel1.

Esta é a configuração no R1:

```
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
```

Em R2, todo o tráfego de retorno para a rede 192.168.2.0/24 é enviado através da interface Tunnel1:

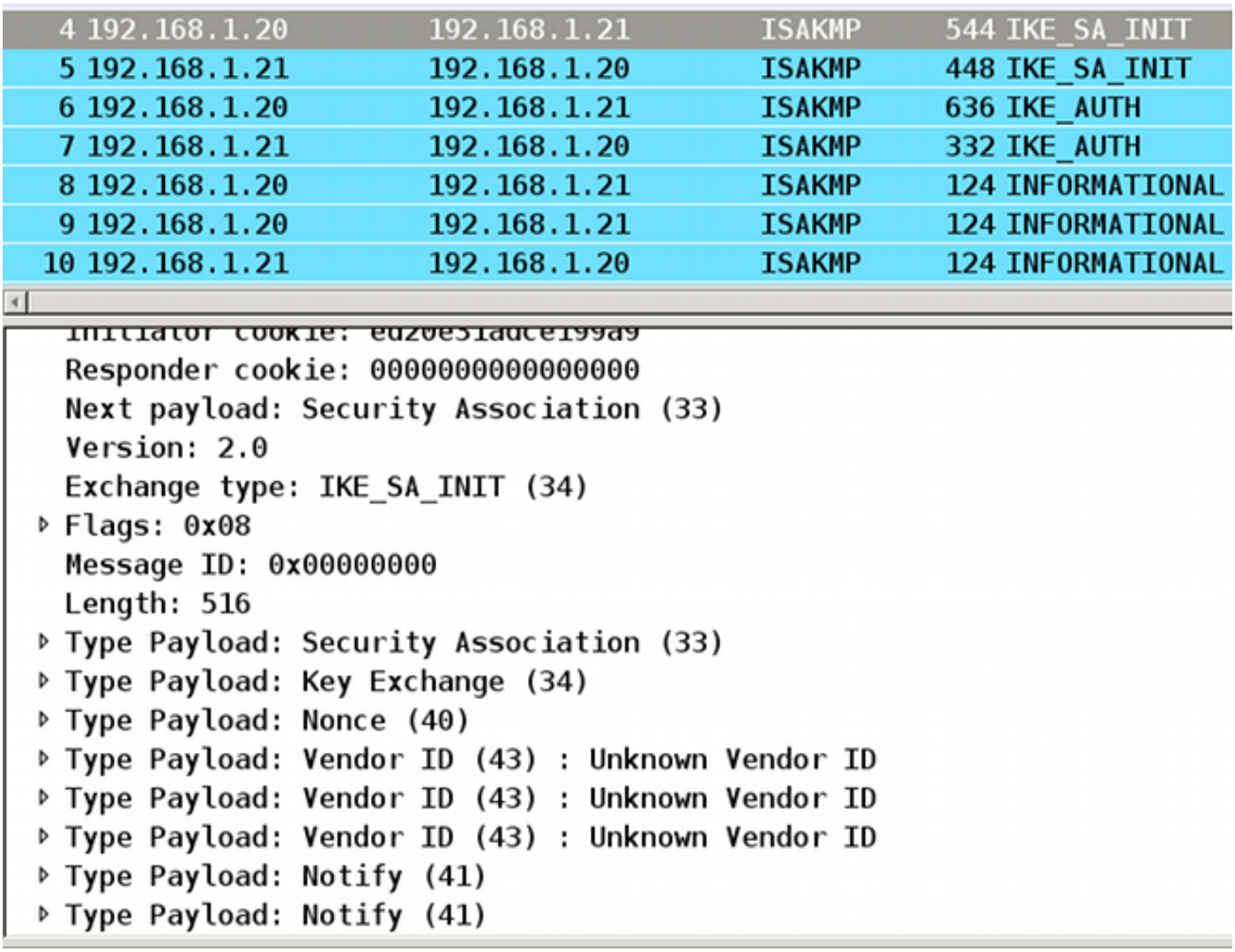
```
crypto ikev2 keyring ikev2-keyring
```

```
 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
```

Apenas um comando é necessário em ambos os roteadores para habilitar a marcação em linha: o comando **crypto ikev2 cts sgt**.

Verificação

A marcação embutida precisa ser negociada. No primeiro e segundo pacotes IKEv2, uma ID de fornecedor específica está sendo enviada:



Há três VIDs (Vendor IDs, IDs de fornecedor) desconhecidas pelo Wireshark. Eles estão relacionados a:

- DELETE-REASON, com suporte da Cisco
- FlexVPN, suportado pela Cisco
- SGT inline taggging

As depurações verificam isso. R1, que é um iniciador IKEv2, envia:

```
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 recebe um segundo pacote IKEv2 e o mesmo 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
```

Assim, ambos os lados concordam em colocar os dados CMD no início da carga ESP.

Verifique a associação de segurança (SA) IKEv2 para verificar este contrato:

```
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
```

Depois de enviar o tráfego do cliente Windows para 192.168.100.1, R1 mostra:

```
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#
```

Observe que os pacotes marcados foram enviados.

Para tráfego de trânsito, quando R1 precisa marcar o tráfego enviado do cliente Windows para R2, confirme se o pacote ESP foi marcado corretamente com SGT=3:

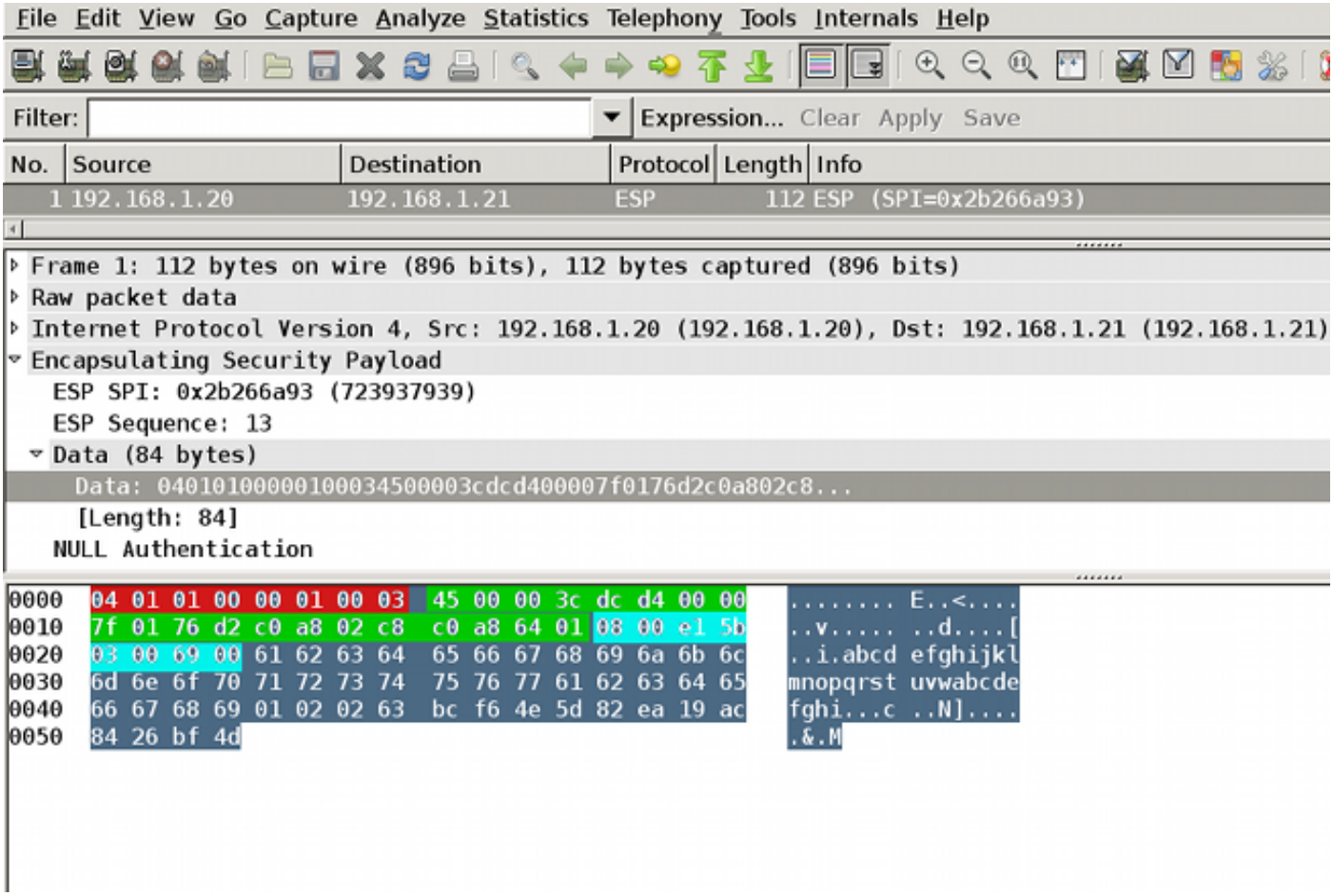
```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

Outro tráfego da mesma VLAN, originado do switch, é padronizado como SGT=0:

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

Verificação de nível de pacote ESP

Use o Embedded Packet Capture (EPC) para revisar o tráfego ESP de R1 para R2, como mostrado na figura:



O Wireshark foi usado para decodificar a criptografia nula para o índice de parâmetro de segurança (SPI). No cabeçalho IPv4, o IP origem e destino são os endereços IP de Internet dos roteadores (usados como origem e destino do túnel).

O payload ESP inclui o campo CMD de 8 bytes, que é destacado em vermelho:

- 0x04 - Próximo cabeçalho, que é IP
- 0x01 - Comprimento (4 bytes após o cabeçalho, 8 bytes com o cabeçalho)
- 0x01 - Versão 01
- 0x00 - Reservado
- 0x00 - tamanho de SGT (total de 4 bytes)
- 0x01 - tipo SGT
- 0x0003 - tag SGT (os dois últimos octetos, que são 00 03; SGT é usado para o cliente Windows)

Como o modo IPv4 do IPsec foi usado para a interface de túnel, o próximo cabeçalho é IP, que

está realçado em verde. O IP origem é c0 a8 02 c8 (192.168.2.200) e o IP destino é c0 a8 64 01 (192.168.100.1). O número do protocolo é 1, que é ICMP.

O último cabeçalho é ICMP, destacado em azul, com Tipo 08 e Código 8 (Solicitação de Eco).

O payload ICMP é o próximo e tem 32 bytes de comprimento (ou seja, letras de a a i). O payload na figura é típico para um cliente Windows.

O restante dos cabeçalhos ESP seguem a carga útil do ICMP:

- 0x01 0x02 - Enchimento.
- 0x02 - Comprimento do preenchimento.
- 0x63 - Próximo cabeçalho que aponta para o protocolo 0x63, que é 'Qualquer esquema de criptografia particular'. Isso indica que o próximo campo (o primeiro campo nos dados ESP) é a tag SGT.
- 12 bytes de valor de verificação de integridade.

O campo CMD está dentro do payload ESP, que geralmente é criptografado.

Desvantagens de IKEv2: modo GRE ou IPsec

Até agora, esses exemplos têm usado o IPv4 IPsec de modo de túnel. O que acontece se o modo Generic Routing Encapsulation (GRE) for usado?

Quando o roteador encapsula um pacote IP de trânsito no GRE, o TrustSec vê o pacote como originado localmente - isto é, a origem do pacote GRE é o roteador, não o cliente Windows. Quando o campo CMD é adicionado, a tag padrão (SGT=0) é sempre usada em vez de uma tag específica.

Quando o tráfego é enviado do cliente Windows (192.168.2.200) no modo IPv4 IPsec, você vê 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
```

Mas, depois que o modo de túnel for alterado para GRE para o mesmo tráfego, você verá que SGT=0. Neste exemplo, 192.168.1.20 é o IP origem do túnel:

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

Observação: portanto, é muito importante **não usar o GRE**.

Consulte o bug da Cisco ID CSCuj25890, IOS IPSec Inline tagging para o modo GRE: inserção do roteador SGT. Esse bug foi criado para permitir a propagação adequada de SGT quando você usa o GRE. SGT sobre DMVPN é suportado pelo Cisco IOS® XE 3.13S

ZBF com base em tags SGT de IKEv2

Este é um exemplo de configuração de ZBF em R2. O tráfego de VPN com SGT=3 pode ser identificado porque todos os pacotes recebidos do túnel IKEv2 são marcados (ou seja, eles

contêm o campo CMD). Assim, o tráfego VPN pode ser descartado e registrado:

```
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
```

Verificação

Quando um ping para 192.168.100.1 é originado do cliente Windows (SGT=3), as depurações mostram isso:

```
*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
```

Para um ping originado de um switch (SGT=0), as depurações mostram isso:

```
*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
```

As estatísticas de firewall de R2 são:

```
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
```

Há quatro descartes (número padrão de eco ICMP enviado pelo Windows) e cinco aceitações (número padrão para o switch).

ZBF com base no mapeamento SGT via SXP

Épossível executar o ZBF com reconhecimento de SGT em R1 e filtrar o tráfego recebido da LAN. Embora esse tráfego não esteja marcado como SGT, R1 tem informações de mapeamento SXP e pode tratá-lo como marcado.

Neste exemplo, uma política é usada entre a LAN e as zonas VPN:

```
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
```

Verificação

Quando o eco ICMP é enviado do cliente Windows, você pode ver as quedas:

```
*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
```

Como a sessão SXP é baseada no TCP, você também pode criar uma sessão SXP através de um túnel IKEv2 entre 3750X-5 e R2 e aplicar políticas ZBF com base nas marcas em R2 sem marcação embutida.

Roteiro

A marcação inline GET VPN também é suportada no ISR G2 e nos Cisco ASR 1000 Series Aggregation Services Routers. O pacote ESP tem 8 bytes adicionais para o campo CMD.

O suporte para Dynamic Multipoint VPN (DMVPN) também está planejado.

Consulte o roteiro da infraestrutura habilitada para Cisco TrustSec para obter mais informações.

Verificar

Os procedimentos de verificação estão incluídos nos exemplos de configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração do switch Cisco TrustSec: noções básicas sobre o Cisco TrustSec
- Livro 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1: Configuring the ASA to Integrate with Cisco TrustSec (Guia de configuração da CLI de operações gerais do Cisco ASA Series, 9.1: Configurando o ASA para integração com o Cisco TrustSec)
- Notas de versão para as versões de disponibilidade geral do Cisco TrustSec: Notas de versão para a versão de implantação geral do Cisco TrustSec 3.0 de 2013
- Configurando marcação em linha IPsec para TrustSec
- Guia de configuração de VPN de transporte criptografado de grupo da Cisco, Cisco IOS XE versão 3S: suporte de VPN GET de marcação em linha IPsec para Cisco TrustSec
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.