Ejemplo de Configuración de IKEv2 con etiquetado en línea SGT de TrustSec y firewall basado en zona SGT-Aware

Contenido

Introducción

Este documento describe cómo utilizar Internet Key Exchange Version 2 (IKEv2) y una etiqueta de grupo de seguridad (SGT) para etiquetar paquetes enviados a un túnel VPN. La descripción incluye una implementación típica y un caso práctico. Este documento también explica un firewall basado en zonas (ZBF) que reconoce SGT y presenta dos escenarios:

- Un ZBF basado en etiquetas SGT recibidas desde un túnel IKEv2
- ZBF basado en la asignación del protocolo de intercambio de SGT (SXP)

Todos los ejemplos incluyen depuraciones de nivel de paquete para verificar cómo se transmite la etiqueta SGT.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de los componentes de TrustSec
- Conocimientos básicos sobre la configuración de la interfaz de línea de comandos (CLI) de los switches Cisco Catalyst
- Experiencia en la configuración de Cisco Identity Services Engine (ISE)
- Conocimientos básicos sobre firewall basado en zonas
- Conocimientos básicos de IKEv2

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7 y Microsoft Windows XP
- Software Cisco Catalyst 3750-X versión 15.0 y posterior
- Software Cisco Identity Services Engine versión 1.1.4 y posteriores
- Router de servicios integrados (ISR) Cisco 2901 con versión de software 15.3(2)T o posterior

Nota: IKEv2 solo es compatible con las plataformas ISR Generation 2 (G2).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

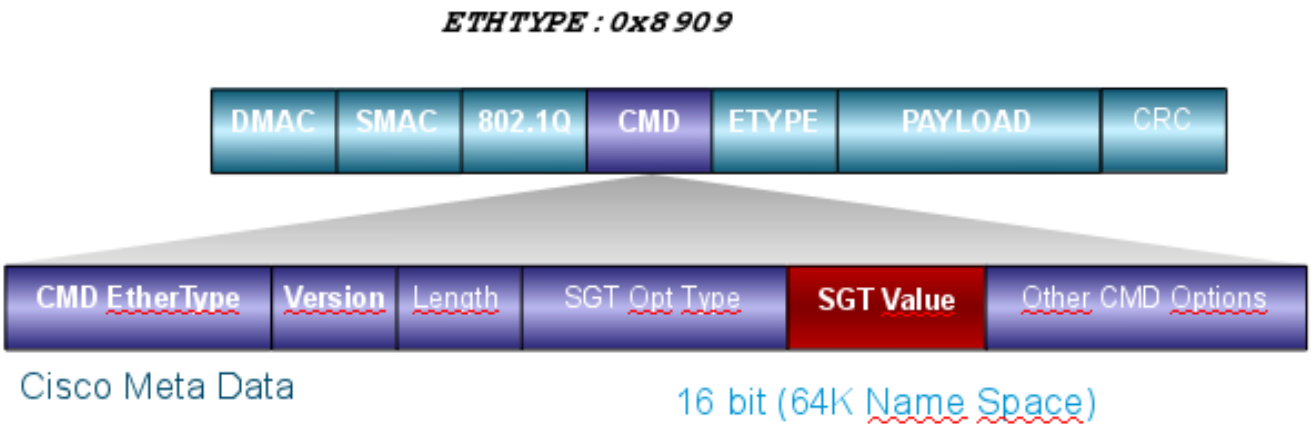
Security Group Tag (SGT)

La SGT forma parte de la arquitectura de la solución Cisco TrustSec, diseñada para utilizar políticas de seguridad flexibles que no se basen en direcciones IP.

El tráfico en la nube de TrustSec se clasifica y marca con una etiqueta SGT. Puede crear políticas de seguridad que filtren el tráfico basándose en esa etiqueta. Todas las políticas se administran de forma centralizada desde ISE y se implementan en todos los dispositivos de la nube TrustSec.

Para pasar la información sobre la etiqueta SGT, Cisco ha modificado la trama Ethernet de manera similar a como se hicieron las modificaciones para las etiquetas 802.1q. La trama Ethernet modificada sólo puede ser comprendida por los dispositivos Cisco seleccionados. Este

es el formato modificado:



El campo de metadatos de Cisco (CMD) se inserta directamente después del campo de dirección MAC de origen (SMAC) o del campo 802.1q si se utiliza (como en este ejemplo).

Para conectar nubes TrustSec a través de VPN, se ha creado una extensión para los protocolos IKE e IPsec. La extensión, denominada etiquetado en línea IPSec, permite el envío de etiquetas SGT en los paquetes de carga de seguridad de encapsulación (ESP). La carga útil ESP se modifica para transportar un campo CMD de 8 bytes justo antes de la carga útil del paquete. Por ejemplo, el paquete de protocolo de mensajes de control de Internet (ICMP) cifrado enviado a través de Internet contiene [IP][ESP][CMD][IP][ICMP][DATA].

En la segunda parte del artículo se presenta información detallada.

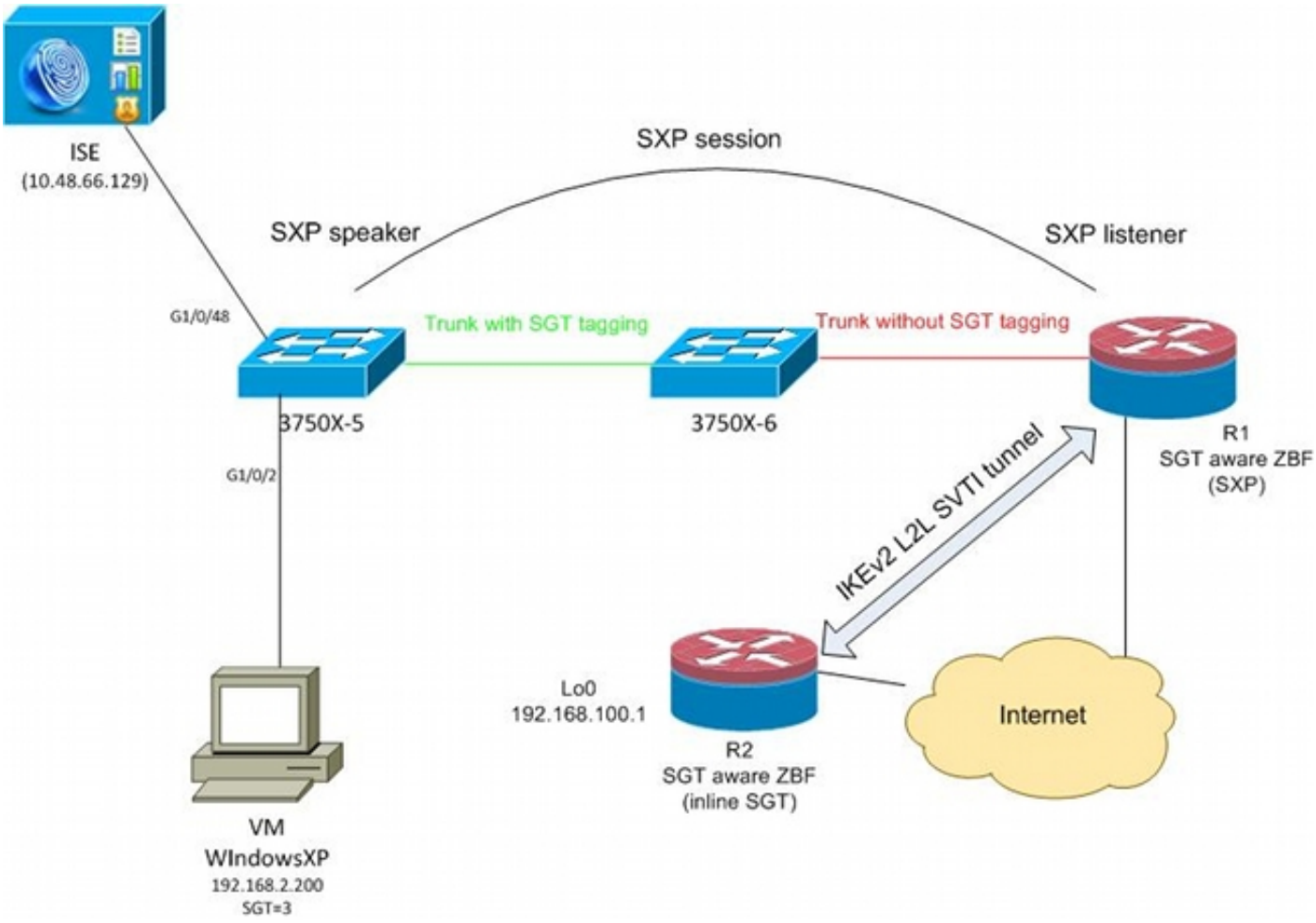
Configurar

Notas:

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Diagrama de la red



Flujo de tráfico

En esta red, 3750X-5 y 3750X-6 son switches Catalyst dentro de la nube TrustSec. Ambos switches utilizan el aprovisionamiento automático de credenciales de acceso protegido (PAC) para unirse a la nube. El 3750X-5 se ha utilizado como semilla y el 3750X-6 como dispositivo no semilla. El tráfico entre ambos switches se cifra con MACsec y se etiqueta correctamente.

Windows XP utiliza 802.1x para acceder a la red. Después de una autenticación correcta, ISE devuelve el atributo de etiqueta SGT que se aplicará para esa sesión. Todo el tráfico originado en ese PC se etiqueta con SGT=3.

Los routers 1 (R1) y 2 (R2) son ISR 2901. Debido a que ISR G2 no admite actualmente el etiquetado SGT, R1 y R2 están fuera de la nube TrustSec y no entienden las tramas Ethernet que se modificaron con los campos CMD para pasar las etiquetas SGT. Por lo tanto, SXP se utiliza para reenviar información sobre el mapeo IP/SGT de 3750X-5 a R1.

R1 tiene un túnel IKEv2 configurado para proteger el tráfico destinado a una ubicación remota (192.168.100.1) y que tiene el etiquetado en línea habilitado. Después de la negociación IKEv2, R1 comienza a etiquetar los paquetes ESP enviados a R2. El etiquetado se basa en los datos SXP recibidos del 3750X-5.

R2 puede recibir ese tráfico y, basándose en la etiqueta SGT recibida, puede realizar acciones específicas definidas por el ZBF.

Lo mismo se puede hacer en R1. La asignación SXP permite que R1 descarte un paquete

recibido de la LAN basado en una etiqueta SGT, incluso si no se soportan las tramas SGT.

Configuración de nube TrustSec

El primer paso de la configuración consiste en crear una nube TrustSec. Ambos switches 3750 necesitan:

- Obtenga una PAC, que se utiliza para la autenticación en la nube de TrustSec (ISE).
- Autentique y pase el proceso de control de admisión de dispositivos a la red (NDAC).
- Utilice el protocolo de asociación de seguridad (SAP) para la negociación MACsec en un enlace.

Este paso es necesario para este caso práctico, pero no es necesario para que el protocolo SXP funcione correctamente. R1 no necesita obtener una PAC o datos de entorno de ISE para realizar la asignación SXP y el etiquetado en línea IKEv2.

Verificación

El enlace entre 3750X-5 y 3750X-6 utiliza cifrado MACsec negociado por 802.1x. Ambos switches confían y aceptan las etiquetas SGT recibidas por el peer:

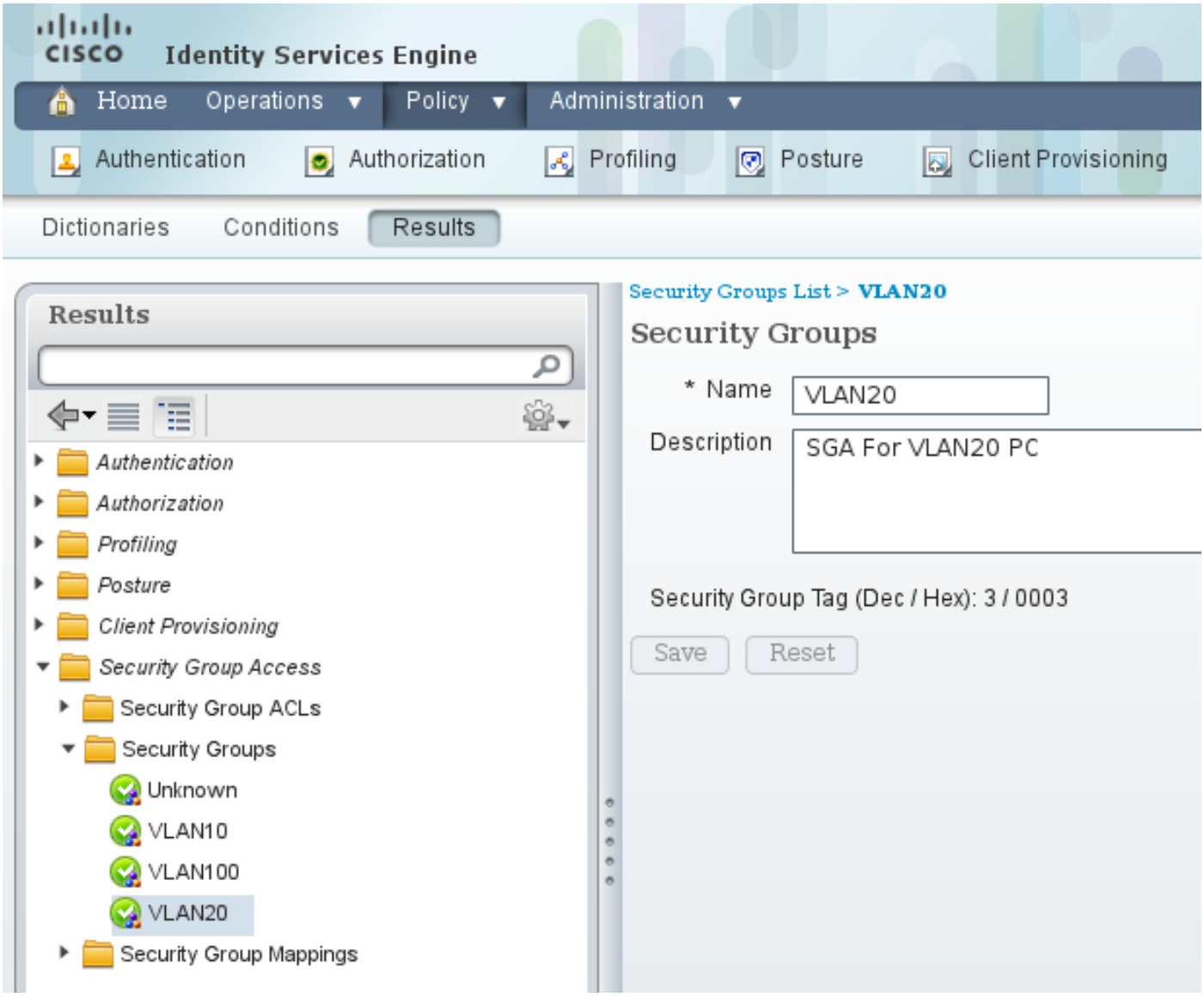
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X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

No es posible aplicar una lista de control de acceso basada en roles (RBACL) directamente en los switches. Estas políticas se configuran en ISE y se descargan automáticamente en los switches.

Configuración del Cliente

El cliente puede utilizar 802.1x, derivación de autenticación MAC (MAB) o autenticación web. Recuerde configurar ISE para que se devuelva el grupo de seguridad correcto para la regla de autorización:



Verificación

Verifique la configuración del 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 de este momento, el tráfico del cliente enviado desde 3750X-5 a otros switches dentro de la nube TrustSec se etiqueta con SGT=3.

Consulte el Ejemplo de Configuración de TrustSec de ASA y Catalyst 3750X Series Switch y la Guía de Troubleshooting para ver un ejemplo de reglas de autorización.

Protocolo de intercambio SGT entre 3750X-5 y R1

R1 no puede unirse a la nube de TrustSec porque es un router ISR G2 2901 que no entiende las tramas Ethernet con campos CMD. Por lo tanto, SXP está configurado en el 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
```

SXP también está configurado en 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
```

Verificación

Asegúrese de que R1 esté recibiendo la información de asignación 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 ahora sabe que todo el tráfico recibido desde 192.168.2.200 debe tratarse como si estuviera etiquetado como SGT=3.

Configuración IKEv2 entre R1 y R2

Se trata de un escenario basado en interfaces de túnel virtual estáticas (SVTI) simple con valores predeterminados inteligentes IKEv2. Las claves previamente compartidas se utilizan para la autenticación y el cifrado nulo para facilitar el análisis de paquetes ESP. Todo el tráfico a 192.168.100.0/24 se envía a través de la interfaz Tunnel1.

Esta es la configuración en 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
```

En R2, todo el tráfico de retorno a la red 192.168.2.0/24 se envía a través de la interfaz Tunnel1:

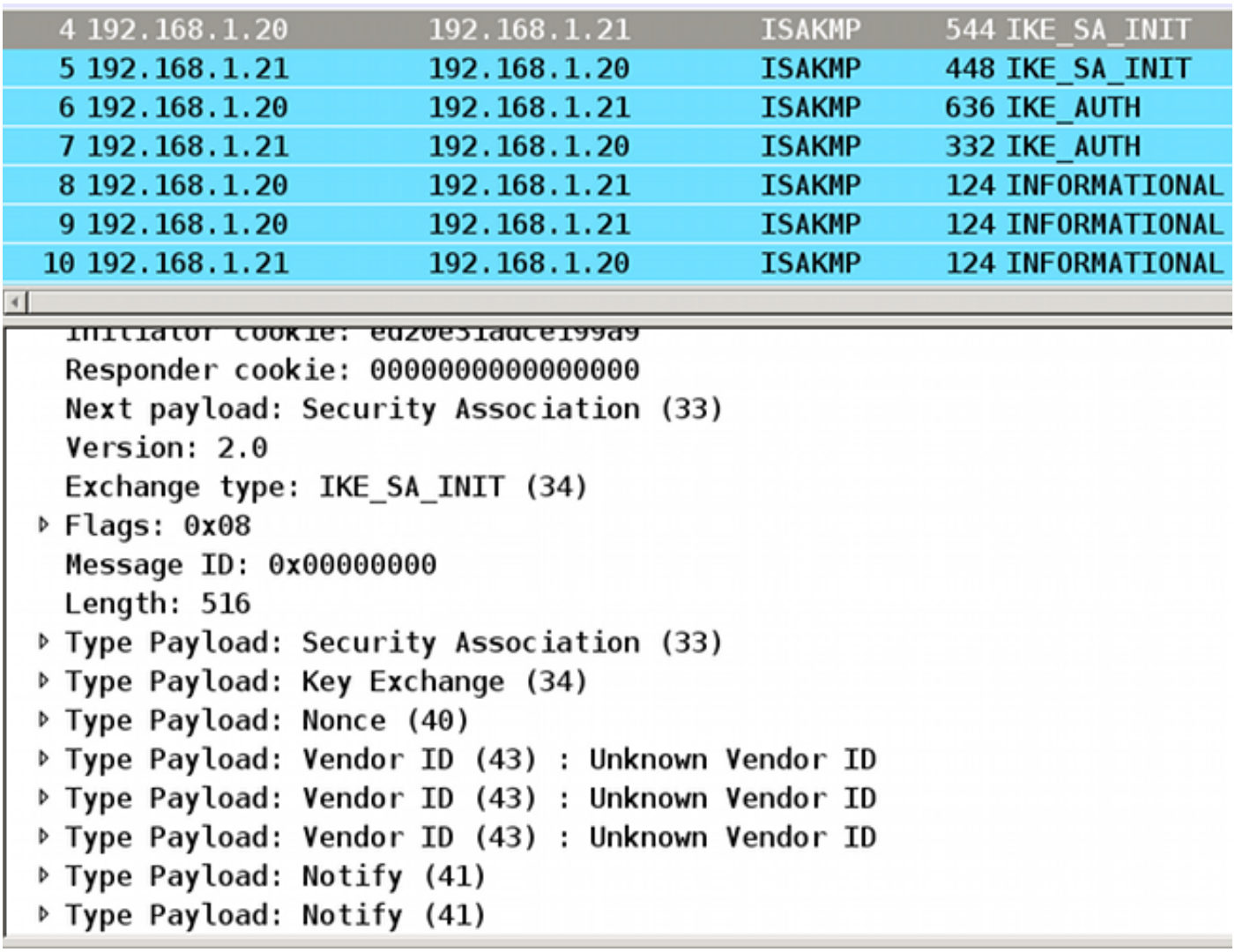
```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.20
 address 192.168.1.20
 pre-shared-key cisco
```

```
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
```

Solo se requiere un comando en ambos routers para habilitar el etiquetado en línea: el comando **crypto ikev2 cts sgt**.

Verificación

El etiquetado en línea debe negociarse. En el primer y segundo paquete IKEv2, se envía una ID de proveedor específica:



Wireshark desconoce tres ID de proveedor (VID). Están relacionados con:

- DELETE-REASON, compatible con Cisco
- FlexVPN, compatible con Cisco
- Etiquetado en línea SGT

Las depuraciones lo comprueban. R1, que es un iniciador IKEv2, envía:

```
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 recibe un segundo paquete IKEv2 y el mismo 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
```

Por lo tanto, ambas partes acuerdan poner los datos de CMD al inicio de la carga útil de ESP.

Verifique la asociación de seguridad (SA) IKEv2 para verificar este acuerdo:

```
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
```

Después de enviar tráfico desde el cliente Windows hacia 192.168.100.1, R1 muestra:

```
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#
```

Tenga en cuenta que se han enviado paquetes etiquetados.

Para el tráfico de tránsito, cuando R1 necesita etiquetar el tráfico enviado desde el cliente Windows a R2, confirme que el paquete ESP se ha etiquetado correctamente con SGT=3:

```
debug crypto ipsc metadata sgt
```

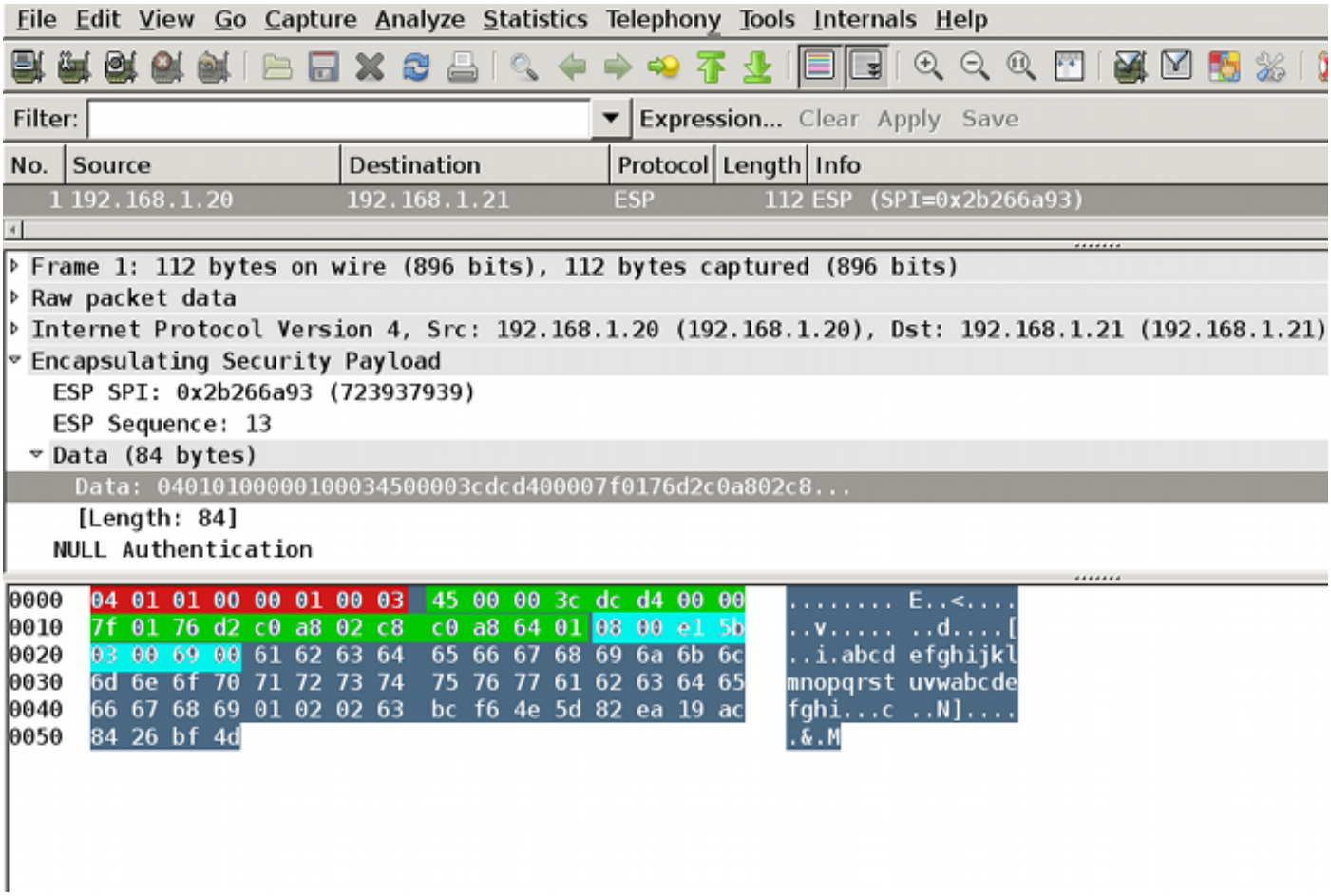
```
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

El resto del tráfico de la misma VLAN, que se origina en el switch, se establece de forma predeterminada en SGT=0:

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

Verificación de nivel de paquete ESP

Utilice Embedded Packet Capture (EPC) para revisar el tráfico ESP de R1 a R2, como se muestra en esta figura:



Wireshark se ha utilizado para descodificar el cifrado nulo del índice de parámetros de seguridad (SPI). En el encabezado IPv4, la IP de origen y de destino son las direcciones IP de Internet de los routers (utilizadas como origen y destino del túnel).

La carga útil de ESP incluye el campo CMD de 8 bytes, que está resaltado en rojo:

- 0x04 - Siguiente encabezado, que es IP
- 0x01 - Longitud (4 bytes después del encabezado, 8 bytes con el encabezado)
- 0x01 - Versión 01
- 0x00 - Reservado
- 0x00 - Longitud de SGT (4 bytes en total)
- 0x01 - Tipo SGT
- 0x0003 - Etiqueta SGT (los dos últimos octetos, que son 00 03; SGT se utiliza para el cliente Windows)

Dado que el modo IPv4 de IPsec se ha utilizado para la interfaz de túnel, el siguiente encabezado es IP, que se resalta en verde. La IP de origen es c0 a8 02 c8 (192.168.2.200) y la IP de destino es c0 a8 64 01 (192.168.100.1). El número de protocolo es 1, que es ICMP.

El último encabezado es ICMP, resaltado en azul, con Tipo 08 y Código 8 (Solicitud de eco).

La carga útil de ICMP es la siguiente y tiene una longitud de 32 bytes (es decir, letras de a a i). La carga útil de la figura es típica de un cliente de Windows.

El resto de los encabezados ESP siguen la carga útil ICMP:

- 0x01 0x02 - Relleno
- 0x02 - Longitud de relleno.
- 0x63 - Siguiente encabezado que señala al protocolo 0x63, que es 'Cualquier esquema de cifrado privado'. Esto indica que el siguiente campo (el primer campo de los datos ESP) es la etiqueta SGT.
- 12 bytes de valor de comprobación de integridad.

El campo CMD se encuentra dentro de la carga útil de ESP, que suele cifrarse.

Obstáculos de IKEv2: modo GRE o IPsec

Hasta ahora, estos ejemplos han utilizado IPv4 IPsec en modo túnel. ¿Qué ocurre si se utiliza el modo de encapsulación de enrutamiento genérico (GRE)?

Cuando el router encapsula un paquete IP de tránsito en GRE, TrustSec ve el paquete como originado localmente, es decir, el origen del paquete GRE es el router, no el cliente de Windows. Cuando se agrega el campo CMD, siempre se utiliza la etiqueta predeterminada (SGT=0) en lugar de una etiqueta específica.

Cuando el tráfico se envía desde el cliente Windows (192.168.2.200) en el modo IPsec IPv4, verá 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
```

Sin embargo, después de cambiar el modo de túnel a GRE para el mismo tráfico, verá que SGT=0. En este ejemplo, 192.168.1.20 es la IP de origen del túnel:

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

> **Nota**: Por lo tanto, es muy importante **no utilizar GRE**.

Consulte Cisco bug ID CSCuj25890, IOS IPSec Inline tagging for GRE mode: insert router SGT. Este bug fue creado para permitir la propagación adecuada de SGT cuando usted utiliza GRE. SGT sobre DMVPN es compatible con Cisco IOS® XE 3.13S

ZBF basado en etiquetas SGT de IKEv2

Este es un ejemplo de configuración de ZBF en R2. El tráfico VPN con SGT=3 se puede

identificar porque todos los paquetes recibidos del túnel IKEv2 están etiquetados (es decir, contienen el campo CMD). Por lo tanto, el tráfico VPN se puede descartar y registrar:

```
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
```

Verificación

Cuando un ping a 192.168.100.1 se obtiene del cliente Windows (SGT=3), las depuraciones muestran lo siguiente:

```
*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 un ping que se origina en un switch (SGT=0), las depuraciones muestran lo siguiente:

```
*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
```

Las estadísticas del firewall de R2 son:

```
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
```

Existen cuatro descartes (número predeterminado de eco ICMP enviado por Windows) y cinco aceptaciones (número predeterminado para el switch).

ZBF basado en asignación de SGT mediante SXP

Es posible ejecutar ZBF con detección de SGT en R1 y filtrar el tráfico recibido de la LAN. Aunque ese tráfico no está etiquetado por SGT, R1 tiene información de mapeo de SXP y puede tratar ese tráfico como etiquetado.

En este ejemplo, se utiliza una política entre las zonas LAN y 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
```

Verificación

Cuando se envía el eco ICMP desde el cliente de Windows, puede ver las caídas:

```
*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
```

Dado que la sesión SXP se basa en TCP, también puede crear una sesión SXP a través de un túnel IKEv2 entre 3750X-5 y R2 y aplicar políticas ZBF basadas en las etiquetas de R2 sin etiquetado en línea.

Hoja de ruta

El etiquetado en línea GET VPN también es compatible con ISR G2 y los routers de servicios de agregación Cisco ASR 1000 Series. El paquete ESP tiene 8 bytes adicionales para el campo CMD.

También está prevista la compatibilidad con la VPN multipunto dinámica (DMVPN).

Consulte la guía de infraestructura habilitada para Cisco TrustSec para obtener más información.

Verificación

Los procedimientos de verificación se incluyen en los ejemplos de configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración del switch Cisco TrustSec: Descripción de Cisco TrustSec
- Libro 1: Guía de configuración CLI de operaciones generales de la serie Cisco ASA, 9.1: Configuración de ASA para su integración con Cisco TrustSec
- Notas de la versión de Cisco TrustSec: versiones de notas de la versión de Cisco TrustSec 3.0 General Deployability 2013
- Configuración de IPsec Inline Tagging for TrustSec
- Guía de configuración de VPN de transporte cifrado de grupo de Cisco, Cisco IOS XE versión 3S: GET VPN Support of IPsec Inline Tagging for Cisco TrustSec
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).