# IKEv2 met TrustSec SGT-configuratievoorbeeld voor inline tagging en SGT-Aware Zone-gebaseerde firewalls

## Inhoud



## Inleiding

Dit document beschrijft hoe u Internet Key Exchange Versie 2 (IKEv2) en een beveiligingsgroeptag (SGT) moet gebruiken om pakketten te labelen die naar een VPN-tunnel zijn verzonden. De beschrijving omvat een typische inzet en gebruikscase. Dit document verklaart ook een op SGT-bewuste Zone-Based Firewall (ZBF) en presenteert twee scenario's:

- Een ZBF die is gebaseerd op SGT-tags die zijn ontvangen van IKEv2-tunnel
- Een ZBF die is gebaseerd op SGT eXchange Protocol (SXP)-toewijzing

Alle voorbeelden omvatten pakketniveau debugs om te verifiëren hoe de SGT tag wordt verzonden.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van TrustSec-componenten
- Basiskennis van configuratie van opdrachtregelinterface (CLI) van Cisco Catalyst switches
- Ervaring met de configuratie van een Cisco Identity Services Engine (ISE)
- Basiskennis van Zone-Based Firewall
- Basiskennis van IKEv2

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7 en Microsoft Windows XP
- Cisco Catalyst 3750-X softwarerelease 15.0 en hoger
- Software voor Cisco Identity Services Engine 1.1.4 en hoger
- Cisco 2901 geïntegreerde services router (ISR) met softwarerelease 15.3(2)T of hoger

**Opmerking**: IKEv2 wordt alleen ondersteund op platforms van ISR Generation 2 (G2).

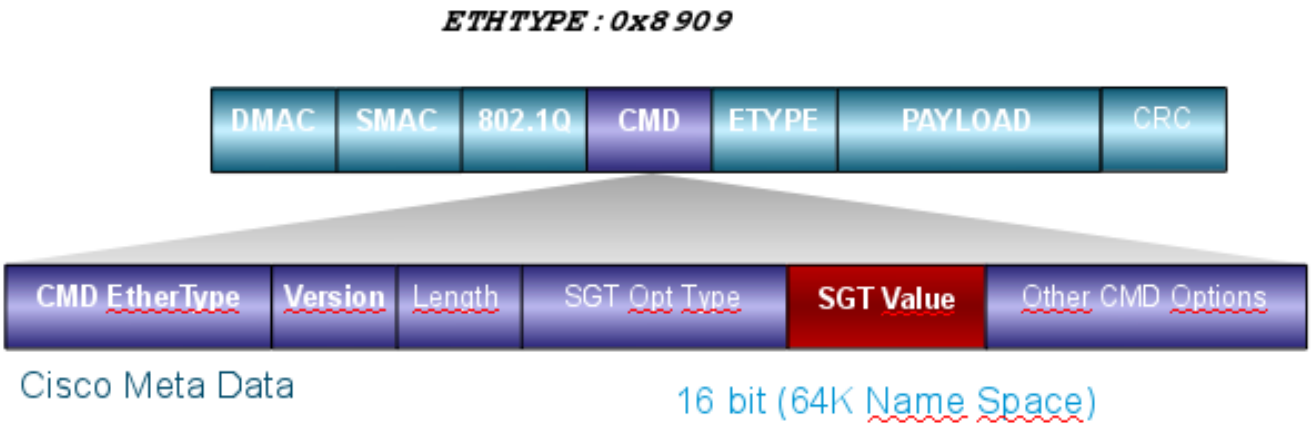
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Security Group Tag (SGT)

SGT maakt deel uit van de Cisco TrustSec-oplossingsarchitectuur, die is ontworpen om flexibel beveiligingsbeleid te gebruiken dat niet op IP-adres is gebaseerd.

Verkeer in de TrustSec-cloud is geclassificeerd en gemarkeerd met een SGT-tag. U kunt beveiligingsbeleid maken om het verkeer te filteren op basis van die tag. Alle beleidsregels worden centraal beheerd vanuit de ISE en worden geïmplementeerd op alle apparaten in de TrustSec-cloud.

Om de informatie over de SGT-tag door te geven, heeft Cisco het Ethernet-frame aangepast op een manier die lijkt op de manier waarop wijzigingen zijn aangebracht voor 802.1q-tags. Het aangepaste Ethernet-frame kan alleen worden begrepen door geselecteerde Cisco-apparaten. Dit is het aangepaste formaat:




Het veld Cisco Meta Data (CMD) wordt direct na het veld Bron mac address (SMAC) ingevoegd of na het veld 802.1q als het wordt gebruikt (zoals in dit voorbeeld).

Om TrustSec-clouds via VPN te verbinden, is een extensie voor de IKE- en IPsec-protocollen gemaakt. De extensie, genaamd IPsec inline tagging, maakt het mogelijk dat SGT tags worden verzonden in de Encapsulating Security Payload (ESP) pakketten. De ESP payload wordt aangepast om een 8-byte CMD-veld te dragen net voor de payload van het pakket zelf. Het versleutelde ICMP-pakket (Internet Control Message Protocol) dat over het internet wordt verzonden, bevat bijvoorbeeld [IP][ESP][CMD][IP][ICMP][DATA].

In het tweede deel van het artikel wordt een gedetailleerde toelichting gegeven.

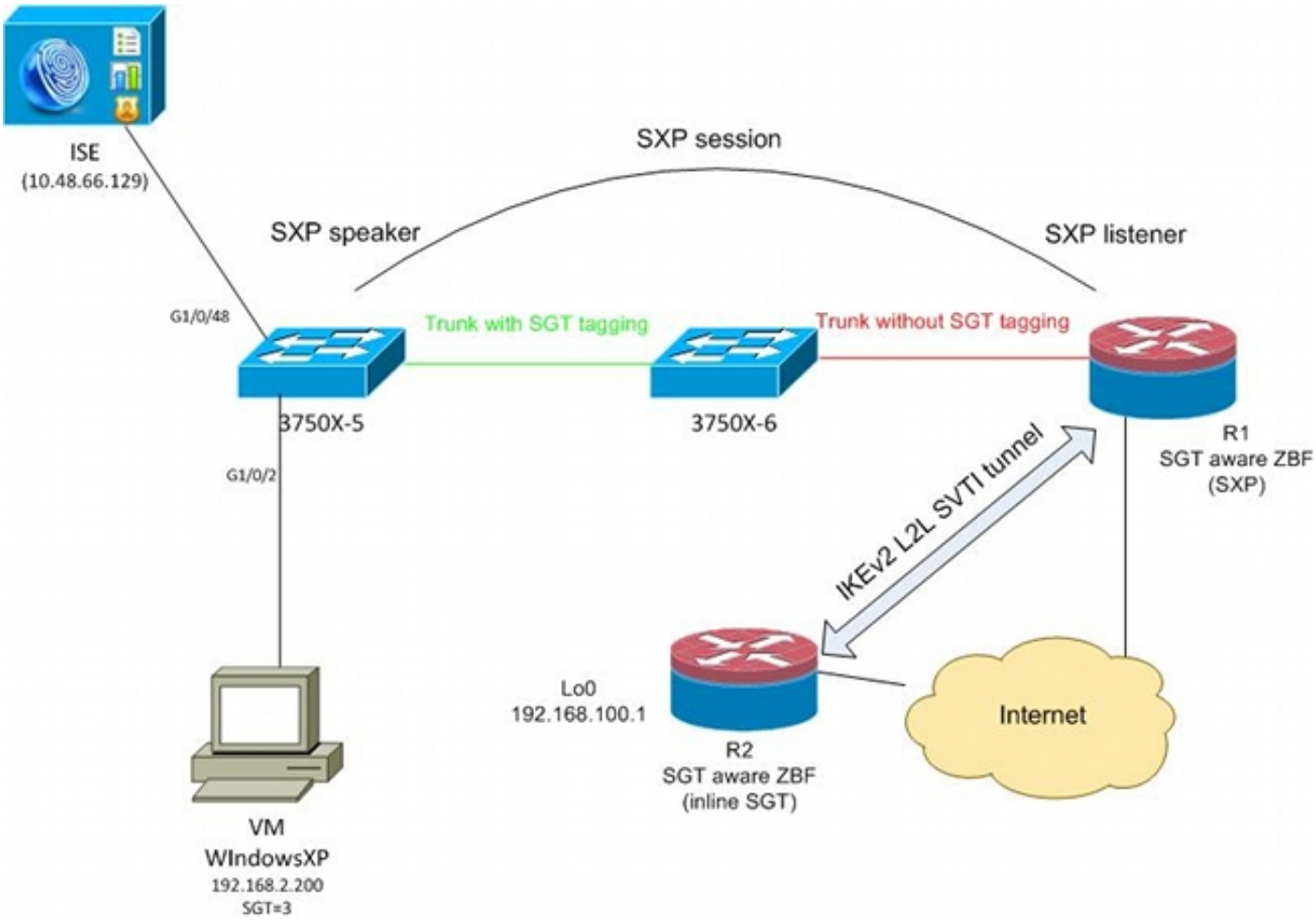
# Configureren

**Opmerkingen:**

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

## Netwerkdiagram




## Traffic Flow

In dit netwerk zijn de 3750X-5 en 3750X-6 Catalyst switches in de TrustSec-cloud. Beide switches maken gebruik van automatische Protected Access Credentials (PAC's) om zich aan te sluiten bij de cloud. 3750X-5 is gebruikt als een zaadje, en 3750X-6 als een niet-zaadapparaat. Het verkeer tussen beide switches is versleuteld met MACsec en is correct gelabeld.

Windows XP gebruikt 802.1x om toegang te krijgen tot het netwerk. Na succesvolle verificatie keert de ISE het SGT-tagkenmerk terug dat voor die sessie zal worden toegepast. Al verkeer dat afkomstig is van die pc is gelabeld met SGT=3.

Router 1 (R1) en router 2 (R2) zijn 2901 ISRs. Omdat ISR G2 op dit moment SGT-tagging niet ondersteunt, zijn R1 en R2 buiten de TrustSec-cloud en begrijpen ze de Ethernet-frames niet die met CMD-velden zijn aangepast om de SGT-tags te kunnen doorgeven. SXP wordt dus gebruikt om informatie over IP/SGT-mapping van 3750X-5 naar R1 te doorsturen.

R1 heeft een IKEv2-tunnel die is geconfigureerd om verkeer op een externe locatie te beveiligen (192.168.100.1) en die inline codering heeft ingeschakeld. Na IKEv2-onderhandeling begint R1 ESP-pakketten te labelen die naar R2 zijn verzonden. Tagging is gebaseerd op de SXP-gegevens ontvangen van 3750X-5.

R2 kan dat verkeer ontvangen en kan, op basis van de ontvangen SGT-tag, specifieke acties uitvoeren die door de ZBF zijn gedefinieerd.

Hetzelfde kan worden gedaan op R1. SXP-toewijzing maakt het mogelijk dat R1 een pakket laat

vallen dat van het LAN wordt ontvangen op basis van een SGT-tag, zelfs als SGT-frames niet worden ondersteund.

## Configuratie van TrustSec Cloud

De eerste stap in de configuratie is het bouwen van een TrustSec-cloud. Beide 3750 switches moeten:

- Verkrijg een PAC, die wordt gebruikt voor authenticatie naar de TrustSec cloud (ISE).
- Verifiëren en doorlopen van het NDAC-proces (Network Device Admission Control).
- Gebruik het Security Association Protocol (SAP) voor MACsec-onderhandeling over een link.

Deze stap is noodzakelijk voor dit gebruiksgeval, maar is niet noodzakelijk voor het SXP-protocol om correct te werken. R1 hoeft geen PAC- of omgevingsgegevens van ISE te verkrijgen om SXP-mapping en IKEv2 inline tagging uit te voeren.

### Verificatie

De koppeling tussen 3750X-5 en 3750X-6 maakt gebruik van MACsec-encryptie die tot stand is gebracht door 802.1x. Beide switches vertrouwen en accepteren de SGT-tags die door de peer worden ontvangen:

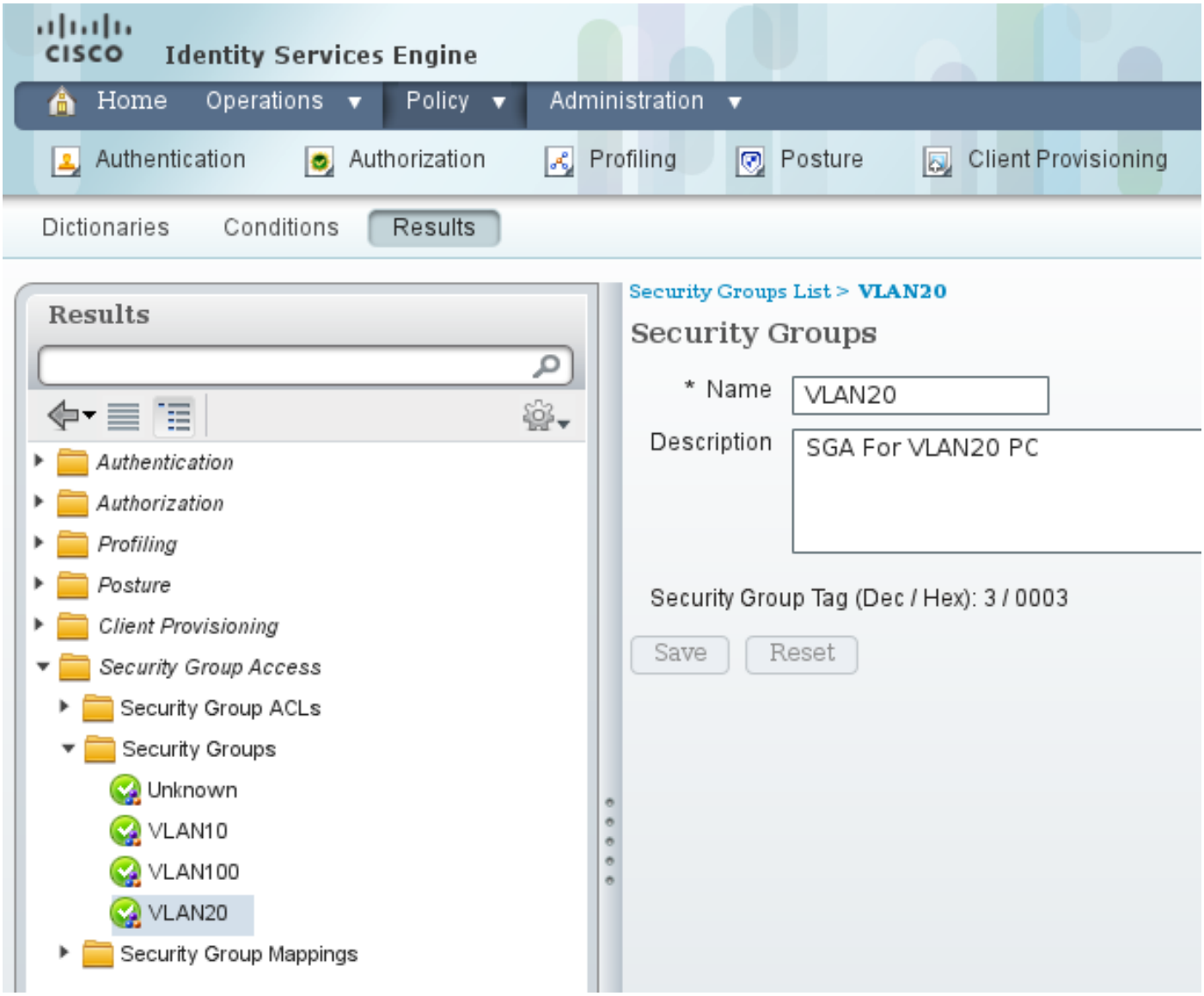
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X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

Het is niet mogelijk om een op rollen gebaseerde toegangscontrolelijst (RBACL) direct op switches toe te passen. Dit beleid is ingesteld op ISE en wordt automatisch gedownload op de switches.

## Clientconfiguratie

De client kan 802.1x, MAC-verificatie-omzeiling (MAB) of webverificatie gebruiken. Vergeet niet om ISE te configureren zodat de juiste beveiligingsgroep voor de autorisatieregel wordt geretourneerd:




### Verificatie

Controleer de clientconfiguratie:

```
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
```

Vanaf dit punt, client verkeer verzonden van 3750X-5 naar andere switches binnen de TrustSec cloud wordt gelabeld met SGT=3.

Zie ASA en Catalyst 3750X Series Switch TrustSec Configuration Voorbeeld en de Handleiding voor probleemoplossing voor een voorbeeld van autorisatieregels.

## SGT-uitwisselingsprotocol tussen 3750X-5 en R1

R1 kan zich niet bij de TrustSec-cloud aansluiten omdat het een 2901 ISR G2-router is die Ethernet-frames met CMD-velden niet begrijpt. SXP is dus geconfigureerd op de 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 is ook geconfigureerd op 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
```

### Verificatie

Zorg ervoor dat R1 de IP/SGT-mapping-informatie ontvangt:

```
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 weet nu dat al het verkeer ontvangen van 192.168.2.200 moet worden behandeld alsof het als SGT=3 wordt geëtiketteerd.

## Configuratie IKEv2 tussen R1 en R2

Dit is een eenvoudig op Static Virtual Tunnel Interfaces (SVTI) gebaseerd scenario met IKEv2 slimme standaardwaarden. De pre-gedeelde sleutels worden gebruikt voor authentificatie, en de ongeldige encryptie wordt gebruikt voor gemak van ESP pakketanalyse. Al verkeer naar 192.168.100.0/24 wordt verzonden door de Tunnel1 interface.

Dit is de configuratie van 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
```

Op R2, wordt al terugkeerverkeer naar netwerk 192.168.2.0/24 verzonden door de Tunnel1 interface:

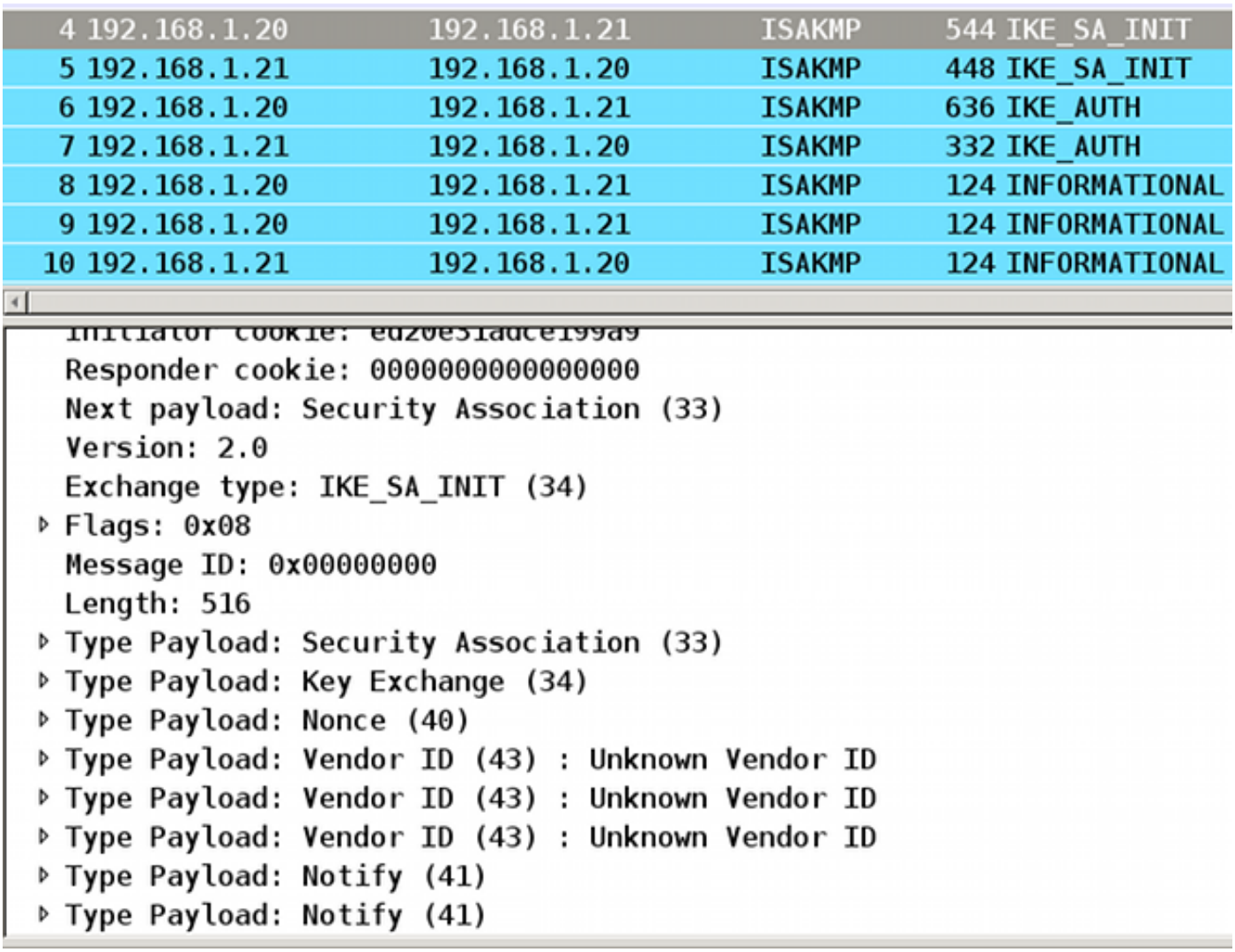
```
crypto ikev2 keyring ikev2-keyring
```

```
 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
```

Slechts één opdracht is op beide routers vereist om inline tagging in te schakelen: de opdracht **crypto ikev2 cts sgt**.

## Verificatie

Er moet worden onderhandeld over inline-tagging. In het eerste en tweede IKEv2-pakket wordt een specifieke leveranciersidentificatie verzonden:




Er zijn drie Vendor ID's (VID's) die onbekend zijn bij Wireshark. Zij houden verband met:

- DELETE-REDEN, ondersteund door Cisco
- FlexVPN, ondersteund door Cisco
- SGT-inline tagging

De debugs verifiëren dit. R1, die een IKEv2 initiator is, verstuurt:

```
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 ontvangt een tweede IKEv2-pakket en hetzelfde 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
```

Beide partijen zijn het er dus over eens dat CMD-gegevens aan het begin van de ESP-payload moeten worden geplaatst.

Controleer de IKEv2 security associatie (SA) om deze overeenkomst te verifiëren:

```
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
```

Nadat het verkeer van Windows-client naar 192.168.100.1 verstuurt, toont R1:

```
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#
```

Merk op dat geëtiketteerde pakketten zijn verzonden.

Voor transitverkeer, wanneer R1 verkeer moet taggen dat van de Windows-client naar R2 wordt verzonden, bevestig dat het ESP-pakket correct met SGT=3 is gelabeld:

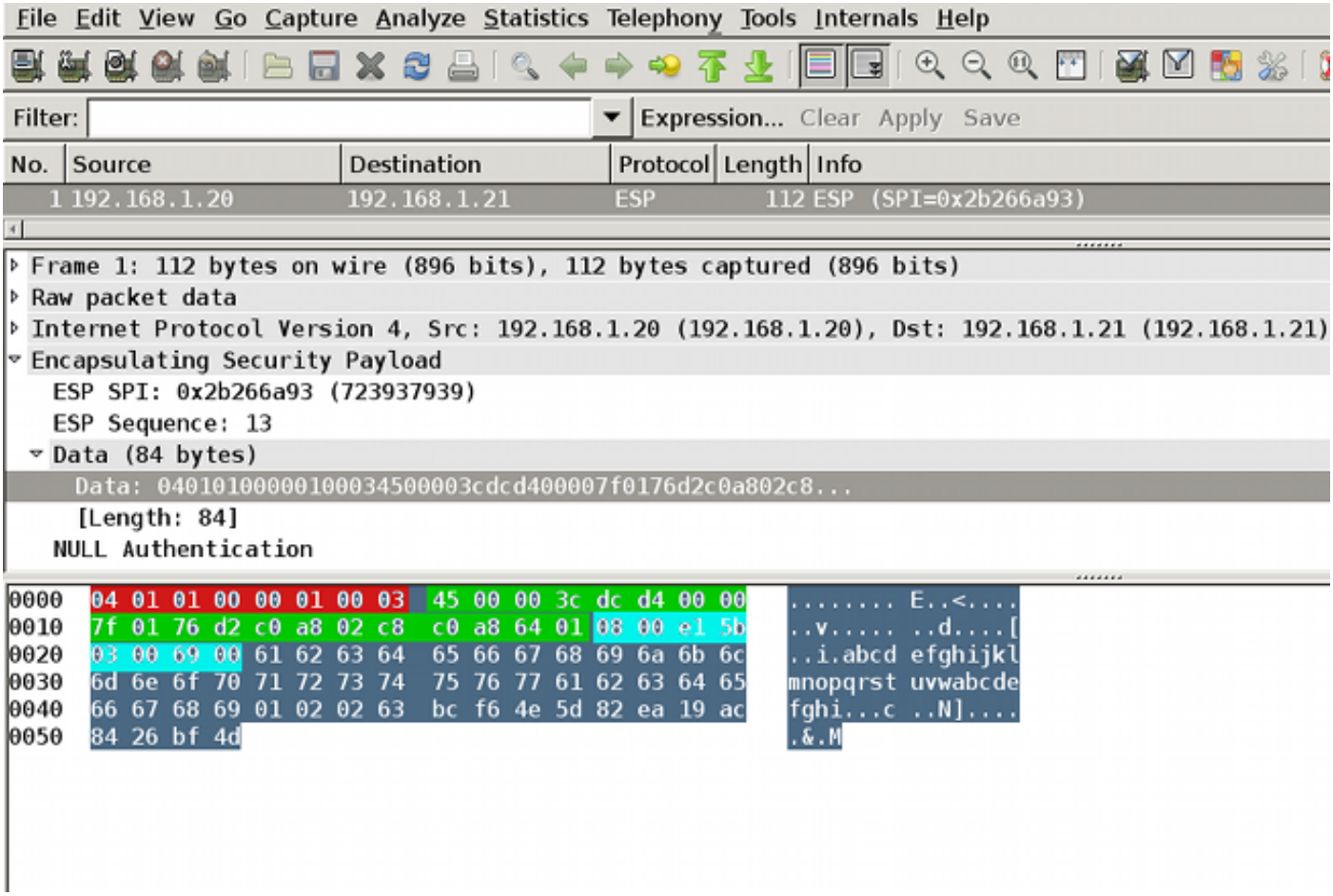
```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

Ander verkeer van hetzelfde VLAN dat afkomstig is van de switch, blijft standaard over op SGT=0:

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

### Verificatie op ESP-pakketniveau

Gebruik Embedded Packet Capture (EPC) om het ESP-verkeer van R1 naar R2 te bekijken, zoals in deze afbeelding:




Wireshark is gebruikt om de null-encryptie voor de security parameter index (SPI) te decoderen. In de IPv4-header zijn de IP-bron en -bestemming de IP-adressen van de routers (gebruikt als tunnelbron en als doelmap).

De ESP-lading bevat het 8-byte CMD-veld, dat in rood wordt gemarkeerd:

- 0x04 - Volgende header, die IP is
- 0x01 - Lengte (4 bytes na de header, 8 bytes met de header)
- 0x01 - versie 10
- 0x00 - gereserveerd
- 0x00 - SGT-lengte (4 bytes in totaal)
- 0x01 - SGT-type
- 0x0003 - SGT-tag (de laatste twee octetten zijn 00 03; SGT wordt gebruikt voor de Windows-client)

Aangezien IPsec IPv4-modus is gebruikt voor de tunnelinterface, is de volgende header IP, die

groen wordt gemarkeerd. De bron IP is c0 a8 02 c8 (192.168.2.200), en de bestemming IP is c0 a8 64 01 (192.168.100.1). Het protocolnummer is 1, wat ICMP is.

De laatste header is ICMP, gemarkeerd in blauw, met Type 08 en Code 8 (Echo-aanvraag).

De ICMP-payload volgt hierna en is 32 bytes lang (dat wil zeggen, letters van a tot i). De payload in de afbeelding is typisch voor een Windows-client.

De rest van ESP kopballen volgt de nuttige lading ICMP:

- 0x01 0x02 - Opvulling.
- 0x02 - Opvullengte.
- 0x63 - Volgende header die verwijst naar protocol 0x63, wat 'Elke privé-encryptie schema' is. Dit geeft aan dat het volgende veld (het eerste veld in de ESP-gegevens) de SGT-tag is.
- 12 bytes integriteitscontrole waarde.

Het CMD-veld bevindt zich in de ESP-payload, die doorgaans wordt versleuteld.

## IKEv2-valkuilen: GRE of IPsec-modus

Tot nu toe hebben deze voorbeelden de tunnelmodus IPsec IPv4 gebruikt. Wat gebeurt er als de Generic Routing Encapsulation (GRE)-modus wordt gebruikt?

Wanneer de router een IP-transitpakket in GRE inkapselt, ziet TrustSec het pakket als lokaal gegenereerd - dat wil zeggen, de bron van het GRE-pakket is de router, niet de Windows-client. Wanneer het CMD-veld wordt toegevoegd, wordt de standaardtag (SGT=0) altijd gebruikt in plaats van een specifieke tag.

Wanneer er verkeer wordt verzonden vanaf de Windows-client (192.168.2.200) in modus IPsec IPv4, ziet u 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
```

Maar nadat de tunnelmodus is veranderd in GRE voor hetzelfde verkeer, ziet u dat SGT=0. In dit voorbeeld is 192.168.1.20 de tunnelbron IP:

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

> **Opmerking**: Het is dus erg belangrijk **om geen GRE te gebruiken**.

Zie Cisco bug-id CSCuj25890, IOS IPSec inline tagging voor GRE-modus: router SGT invoegen. Deze bug is gemaakt om goede SGT-voortplanting toe te staan wanneer u GRE gebruikt. SGT over DMVPN wordt ondersteund door Cisco IOS® XE 3.13S

## ZBF gebaseerd op SGT Tags van IKEv2

Dit is een voorbeeld van ZBF op R2. Het VPN-verkeer met SGT=3 kan worden geïdentificeerd omdat alle pakketten die van de IKEv2-tunnel worden ontvangen, zijn gelabeld (dat wil zeggen, ze bevatten het CMD-veld). Zodoende kan het VPN-verkeer worden gedropt en vastgelegd:

```
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
```

## Verificatie

Wanneer een ping naar 192.168.100.1 afkomstig is van de Windows-client (SGT=3), tonen de debugs dit:

```
*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
```

Voor pingelen dat uit een switch (SGT=0) afkomstig is, tonen de debugs dit:

```
*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
```

De firewallstatistieken van R2 zijn:

```
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
```

Er zijn vier druppels (standaardnummer van ICMP Echo verzonden door Windows) en vijf accepteert (standaardnummer voor switch).

## ZBF gebaseerd op SGT-toewijzing via SXP

Het is mogelijk om SGT-bewuste ZBF op R1 uit te voeren en om verkeer te filteren dat van het LAN wordt ontvangen. Hoewel dat verkeer niet SGT is gelabeld, heeft R1 SXP-mapping informatie en kan dat verkeer behandelen als gelabeld.

In dit voorbeeld wordt een beleid gebruikt tussen de LAN- en de VPN-zones:

```
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
```

### Verificatie

Wanneer ICMP Echo wordt verzonden vanaf de Windows-client, ziet u de druppels:

```
*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
```

Omdat de SXP-sessie is gebaseerd op TCP, kunt u ook een SXP-sessie bouwen via een IKEv2-tunnel tussen 3750X-5 en R2 en ZBF-beleid toepassen dat is gebaseerd op de tags op R2 zonder inline tagging.

## Routekaart

GET VPN inline tagging wordt ook ondersteund op de ISR G2 en Cisco ASR 1000 Series aggregatieservices routers. Het ESP-pakket heeft nog eens 8 bytes voor het CMD-veld.

Ondersteuning voor Dynamic Multipoint VPN (DMVPN) is ook gepland.

Zie de Cisco TrustSec-Enabled Infrastructure roadmap voor meer informatie.

## Verifiëren

Verificatieprocedures zijn opgenomen in de configuratievoorbeelden.

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## Gerelateerde informatie

- Cisco TrustSec Switch-configuratiehandleiding: begrip van Cisco TrustSec
- Boek 1: Configuratiehandleiding voor Cisco ASA Series General Operations CLI, 9.1: De ASA configureren voor integratie met Cisco TrustSec
- Releaseopmerkingen voor Cisco TrustSec Algemene beschikbaarheidsreleases: Releaseopmerkingen voor Cisco TrustSec 3.0 Algemene implementeerbaarheid 2013 release
- IPsec inline tagging voor TrustSec configureren
- Configuratiehandleiding voor Cisco Group Encrypted Transport VPN, Cisco IOS XE release 3S: GET VPN-ondersteuning van IPsec inline tagging voor Cisco TrustSec
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.