Esempio di configurazione del firewall basato su zona compatibile con SGT e tag in linea IKEv2 con TrustSec SGT

Sommario

Introduzione

In questo documento viene descritto come usare Internet Key Exchange versione 2 (IKEv2) e un tag del gruppo di sicurezza (SGT) per assegnare i tag ai pacchetti inviati a un tunnel VPN. La descrizione include un tipico caso di implementazione e utilizzo. Questo documento spiega anche un firewall basato su zone compatibile con SGT (ZBF) e presenta due scenari:

- ZBF basato sui tag SGT ricevuti dal tunnel IKEv2
- Una ZBF basata sul mapping SGT eXchange Protocol (SXP)

Tutti gli esempi includono i debug a livello di pacchetto per verificare come viene trasmesso il tag SGT.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei componenti TrustSec
- Conoscenze base di configurazione dell'interfaccia della riga di comando (CLI) degli switch Cisco Catalyst
- Esperienza nella configurazione di Cisco Identity Services Engine (ISE)
- Conoscenze base di Zone-Based Firewall
- Conoscenze base di IKEv2

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7 e Microsoft Windows XP
- Software Cisco Catalyst 3750-X versione 15.0 e successive
- Software Cisco Identity Services Engine versione 1.1.4 e successive
- Cisco 2901 Integrated Services Router (ISR) con software versione 15.3(2)T o successive

Nota: IKEv2 è supportato solo sulle piattaforme ISR Generation 2 (G2).

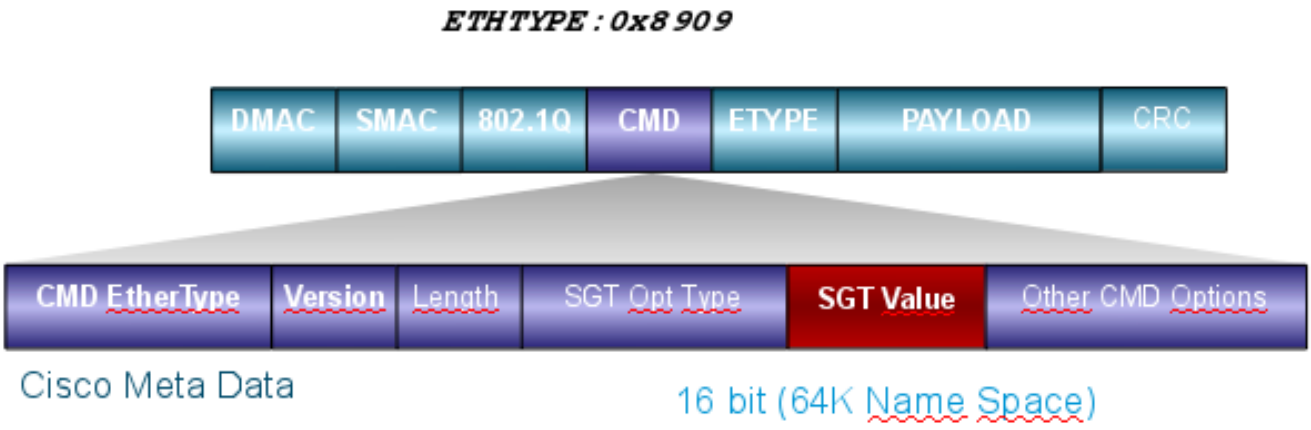
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

SGT (Security Group Tag)

Il SGT fa parte dell'architettura della soluzione Cisco TrustSec, progettata per utilizzare criteri di sicurezza flessibili non basati sull'indirizzo IP.

Il traffico nel cloud TrustSec è classificato e contrassegnato con un tag SGT. È possibile creare criteri di sicurezza che filtrino il traffico in base a tale tag. Tutte le policy vengono gestite centralmente dall'ISE e distribuite a tutti i dispositivi nel cloud TrustSec.

Per trasferire le informazioni sul tag SGT, Cisco ha modificato il frame Ethernet in modo simile alle modifiche apportate ai tag 802.1q. Il frame Ethernet modificato può essere riconosciuto solo da alcuni dispositivi Cisco. Questo è il formato modificato:



Il campo Cisco Meta Data (CMD) viene inserito direttamente dopo il campo indirizzo MAC di origine (SMAC) o il campo 802.1q, se utilizzato (come in questo esempio).

Per connettere cloud TrustSec tramite VPN, è stata creata un'estensione per i protocolli IKE e IPsec. L'estensione, denominata tagging in linea IPsec, consente l'invio di tag SGT nei pacchetti Encapsulating Security Payload (ESP). Il payload ESP viene modificato in modo da avere un campo CMD di 8 byte immediatamente prima del payload del pacchetto stesso. Ad esempio, il pacchetto ICMP (Internet Control Message Protocol) crittografato inviato tramite Internet contiene [IP][ESP][CMD][IP][ICMP][DATA].

Informazioni dettagliate sono presentate nella seconda parte dell'articolo.

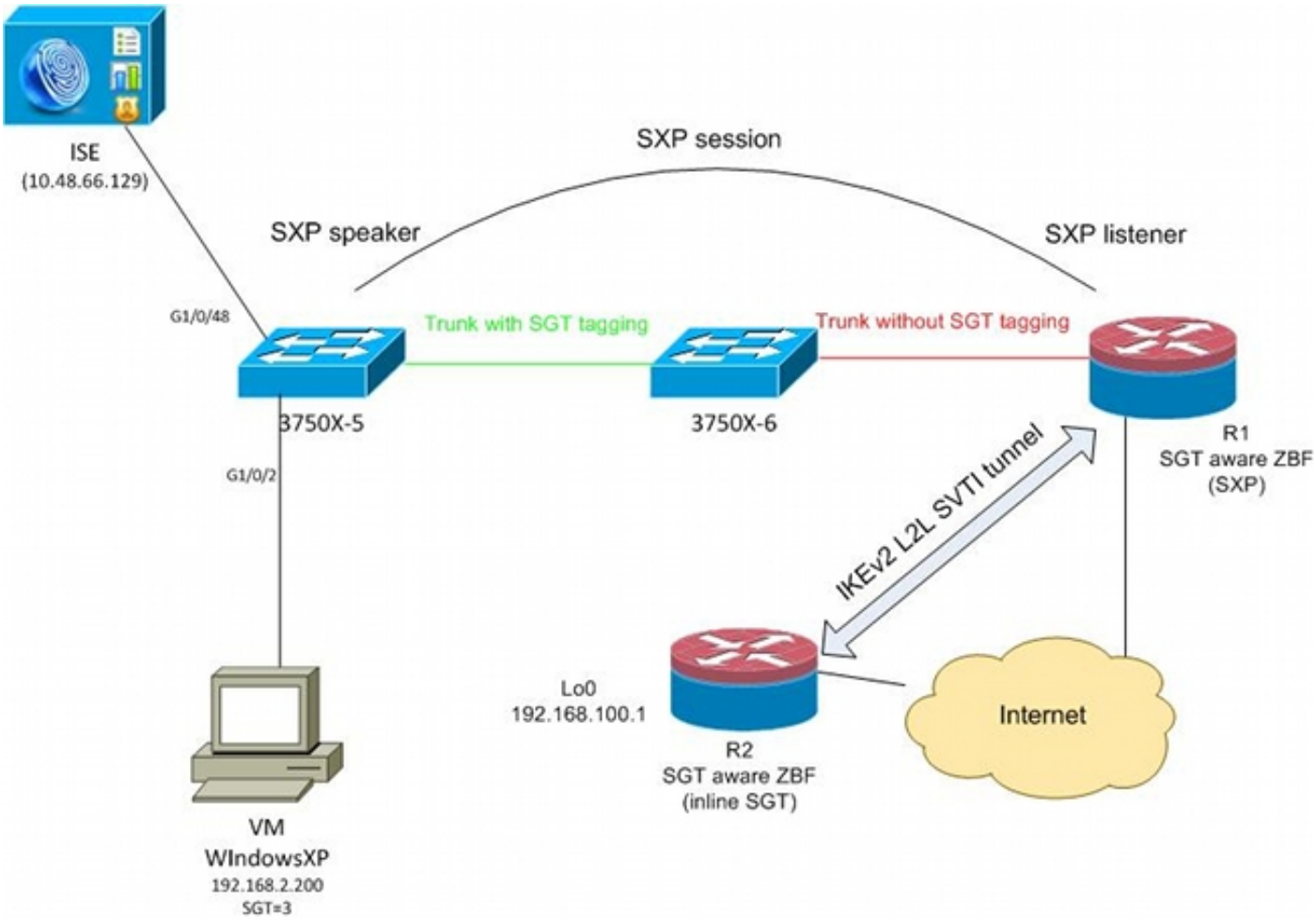
Configurazione

Note:

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Esempio di rete



Flusso traffico

In questa rete, gli switch 3750X-5 e 3750X-6 sono switch Catalyst all'interno del cloud TrustSec. Entrambi gli switch usano il provisioning delle credenziali di accesso protetto (PAC) per collegarsi al cloud. 3750X-5 è stato utilizzato come dispositivo di inizializzazione e 3750X-6 come dispositivo non di inizializzazione. Il traffico tra entrambi gli switch è crittografato con MACsec e viene contrassegnato correttamente.

Per accedere alla rete, Windows XP utilizza 802.1x. Una volta completata l'autenticazione, ISE restituisce l'attributo tag SGT che verrà applicato per quella sessione. Tutto il traffico proveniente da quel PC è contrassegnato con SGT=3.

Il router 1 (R1) e il router 2 (R2) sono 2901 ISR. Poiché ISR G2 non supporta attualmente il tagging SGT, R1 e R2 si trovano all'esterno del cloud TrustSec e non comprendono i frame Ethernet modificati con i campi CMD per passare i tag SGT. Pertanto, SXP viene utilizzato per inoltrare le informazioni sulla mappatura IP/SGT da 3750X-5 a R1.

R1 dispone di un tunnel IKEv2 configurato per proteggere il traffico destinato a una postazione remota (192.168.100.1) e per il quale è abilitata l'assegnazione di tag in linea. Dopo la negoziazione IKEv2, R1 inizia a contrassegnare i pacchetti ESP inviati a R2. Il tagging si basa sui dati SXP ricevuti da 3750X-5.

R2 può ricevere quel traffico e, in base al tag SGT ricevuto, può eseguire azioni specifiche definite dallo ZBF.

Lo stesso può essere fatto con R1. La mappatura SXP consente a R1 di rilasciare un pacchetto ricevuto dalla LAN in base a un tag SGT, anche se i frame SGT non sono supportati.

Configurazione cloud TrustSec

Il primo passaggio della configurazione consiste nella generazione di un cloud TrustSec. Entrambi gli switch 3750 devono:

- Ottenere una PAC, utilizzata per l'autenticazione nel cloud TrustSec (ISE).
- Consente di autenticare e superare il processo NDAC (Network Device Admission Control).
- Utilizzare il protocollo SAP (Security Association Protocol) per la negoziazione MACsec su un collegamento.

Questo passaggio è necessario per questo scenario, ma non è necessario per il corretto funzionamento del protocollo SXP. R1 non ha bisogno di ottenere una PAC o dati di ambiente da ISE per eseguire il mapping SXP e l'etichettatura in linea IKEv2.

Verifica

Il collegamento tra 3750X-5 e 3750X-6 utilizza la crittografia MACsec negoziata da 802.1x. Entrambi gli switch considerano attendibili e accettano i tag SGT ricevuti dal peer:

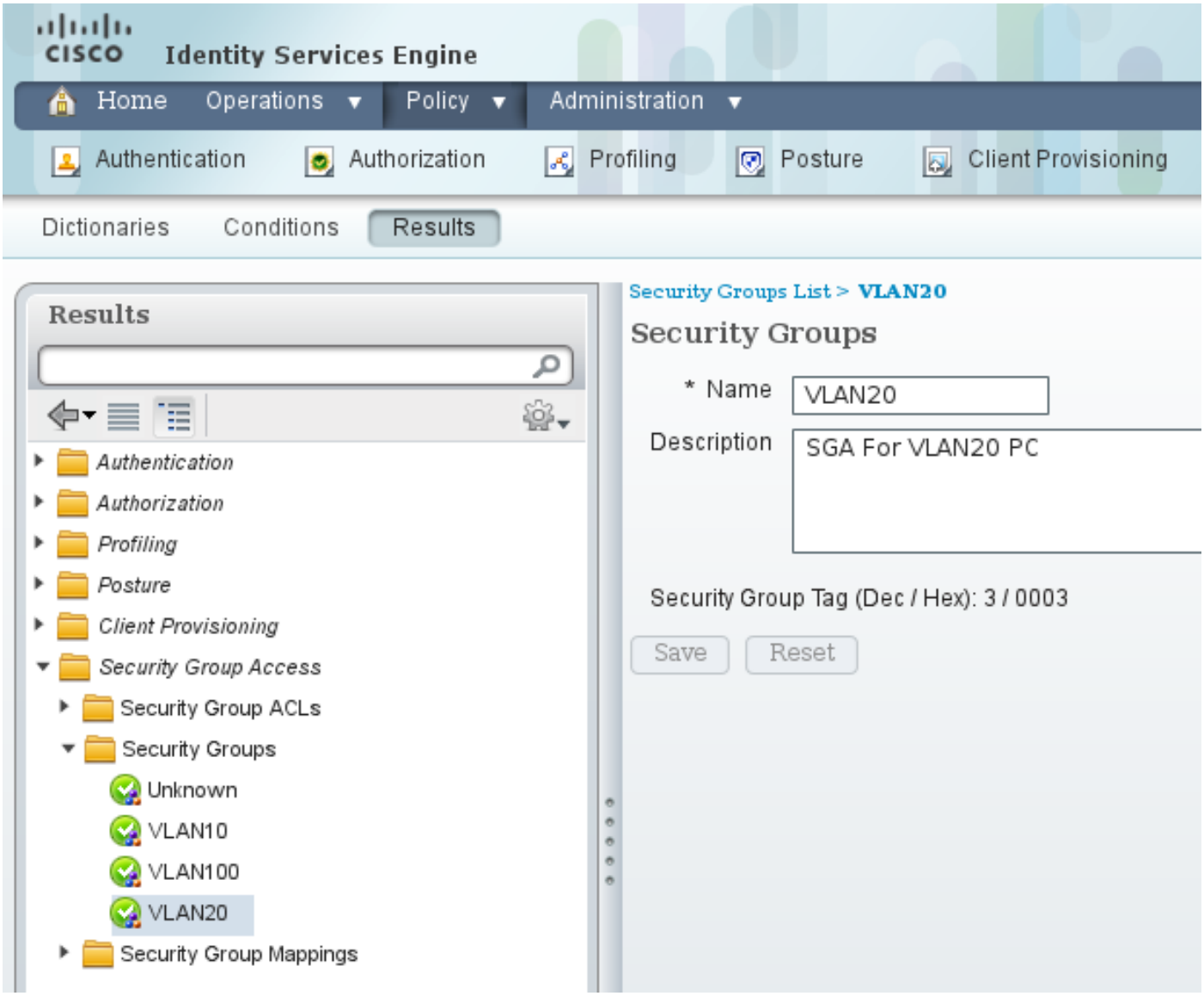
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X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

Non è possibile applicare un elenco di controllo di accesso basato sui ruoli (RBACL) direttamente sugli switch. Queste policy vengono configurate su ISE e scaricate automaticamente sugli switch.

Configurazione client

Il client può utilizzare l'autenticazione 802.1x, MAC Authentication Bypass (MAB) o Web. Ricordare di configurare ISE in modo che venga restituito il gruppo di sicurezza corretto per la regola di autorizzazione:



Verifica

Verificare la configurazione del client:

```
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
```

Da questo momento in poi, il traffico client inviato da 3750X-5 ad altri switch nel cloud TrustSec viene contrassegnato con SGT=3.

Per un esempio di regole di autorizzazione, vedere Esempio di configurazione e guida alla risoluzione dei problemi degli switch ASA e Catalyst serie 3750X.

Protocollo SGT Exchange tra 3750X-5 e R1

Impossibile aggiungere R1 al cloud TrustSec perché è un router 2901 ISR G2 che non riconosce i frame Ethernet con campi CMD. Pertanto, SXP è configurato sullo switch 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 è configurato anche su 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
```

Verifica

Verificare che R1 riceva le informazioni di mapping 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 ora sa che tutto il traffico ricevuto da 192.168.2.200 deve essere trattato come se fosse contrassegnato come SGT=3.

Configurazione IKEv2 tra R1 e R2

Si tratta di uno scenario semplice basato su SVTI (Static Virtual Tunnel Interfaces) con impostazioni predefinite intelligenti IKEv2. Le chiavi già condivise vengono utilizzate per l'autenticazione, mentre la crittografia null viene utilizzata per semplificare l'analisi dei pacchetti ESP. Tutto il traffico diretto a 192.168.100.0/24 viene inviato tramite l'interfaccia Tunnel1.

Questa è la configurazione su 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
```

Su R2, tutto il traffico di ritorno alla rete 192.168.2.0/24 viene inviato tramite l'interfaccia Tunnel1:

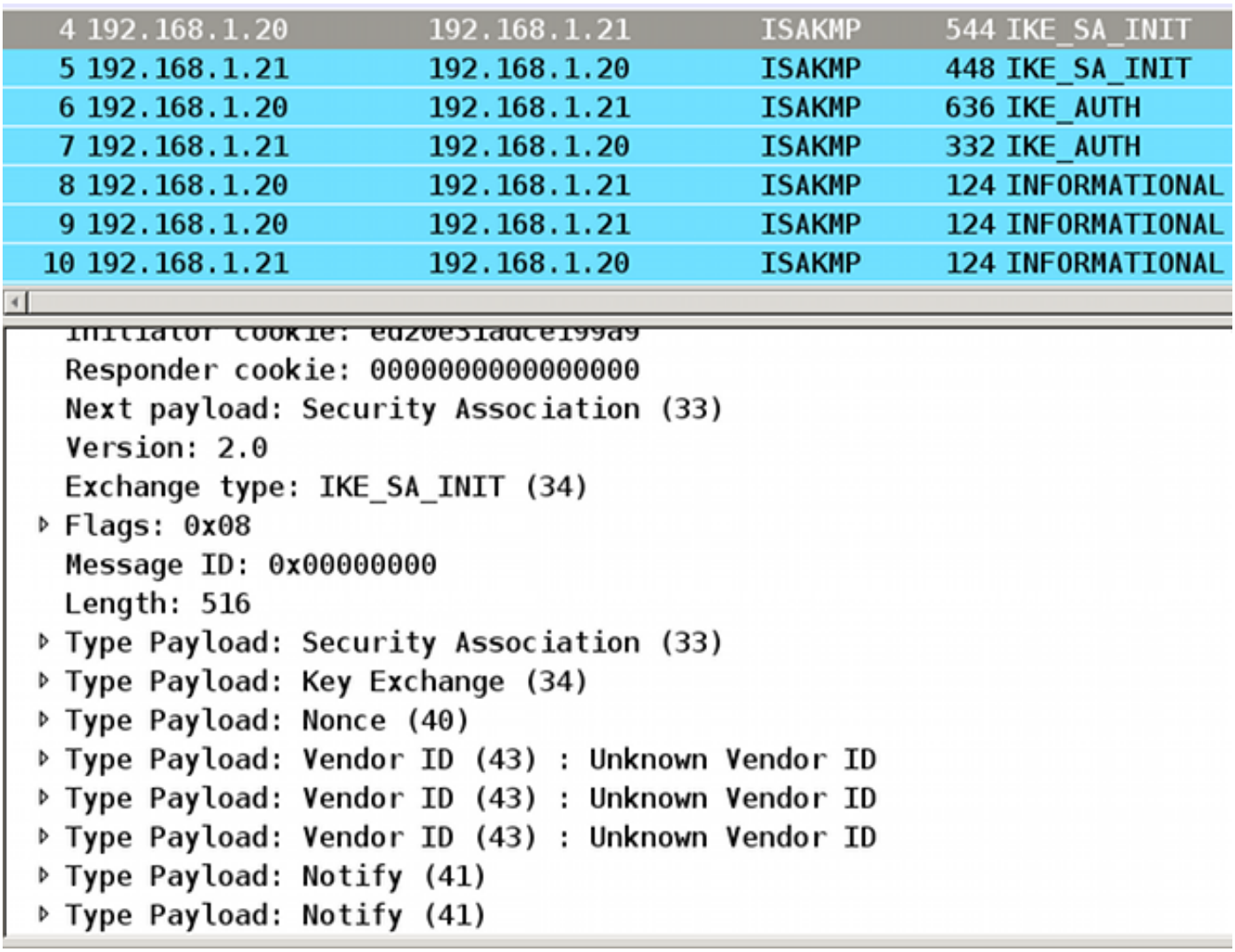
```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.20
 address 192.168.1.20
```

```
 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
```

Per abilitare il tagging inline, su entrambi i router è richiesto un solo comando: il comando **crypto ikev2 ct sgt**.

Verifica

Il tagging in linea deve essere negoziato. Nel primo e nel secondo pacchetto IKEv2, viene inviato un ID fornitore specifico:



Wireshark non conosce tre ID fornitore (VID). Sono correlati a:

- DELETE-REASON, supportato da Cisco
- FlexVPN, supportata da Cisco
- Tagging in linea SGT

I debug verificano questa condizione. R1, un iniziatore IKEv2, invia:

```
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 riceve un secondo pacchetto IKEv2 e lo stesso 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
```

Pertanto, entrambe le parti concordano di inserire i dati CMD all'inizio del payload ESP.

Per verificare il presente accordo, controllare l'associazione di protezione IKEv2:

```
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
```

Dopo l'invio del traffico dal client Windows alla versione 192.168.100.1, in R1 viene visualizzato quanto segue:

```
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#
```

Notare che i pacchetti con tag sono stati inviati.

Per il traffico di transito, quando R1 deve contrassegnare il traffico inviato dal client Windows a R2, confermare che il pacchetto ESP sia stato contrassegnato correttamente con SGT=3:

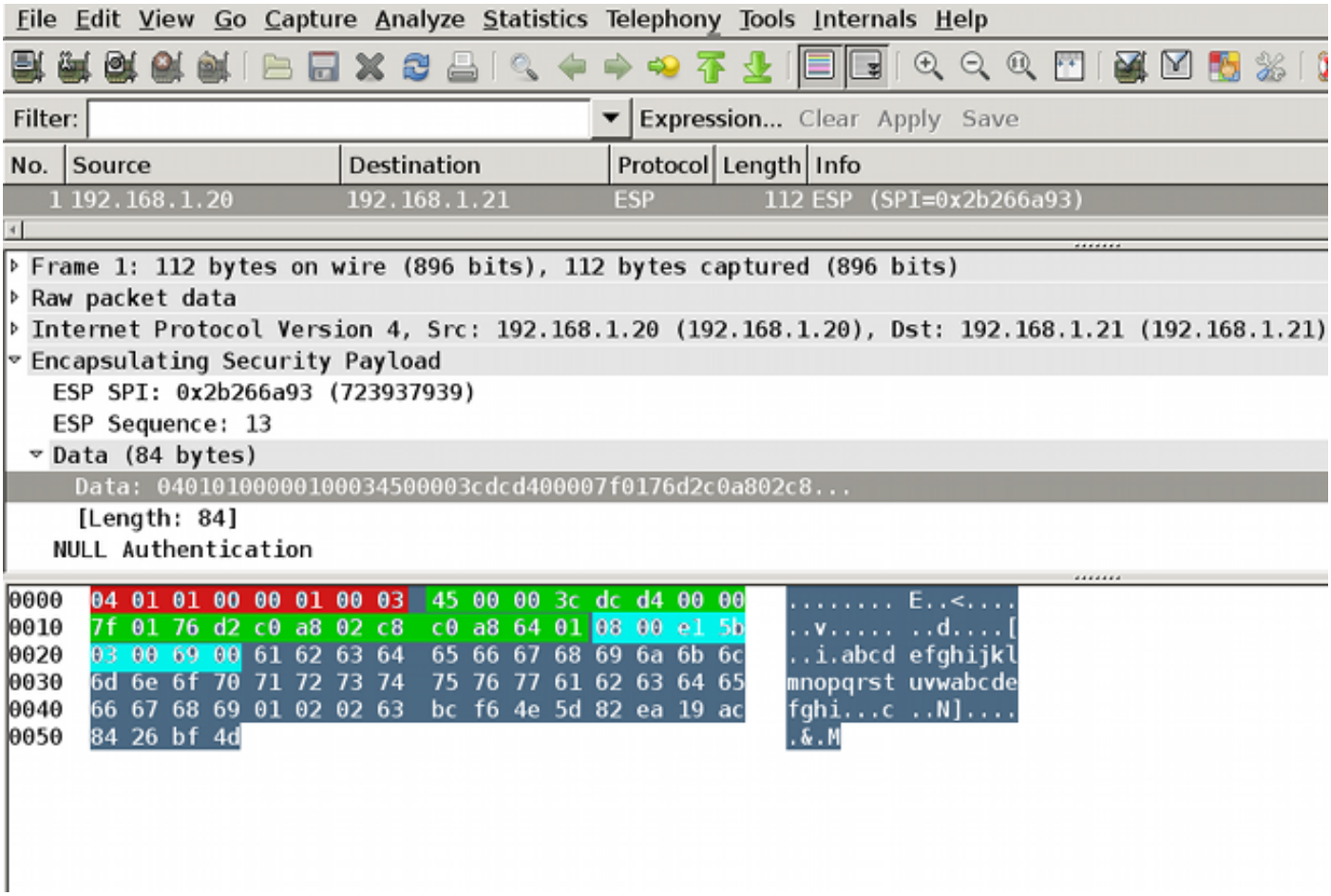
```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

Per il resto del traffico proveniente dalla stessa VLAN e proveniente dallo switch, il valore predefinito è SGT=0:

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

Verifica a livello di pacchetto ESP

Utilizzare Embedded Packet Capture (EPC) per esaminare il traffico ESP da R1 a R2, come mostrato nella seguente figura:



Wireshark è stato utilizzato per decodificare la crittografia Null per l'indice dei parametri di sicurezza (SPI, Security Parameter Index). Nell'intestazione IPv4, l'indirizzo IP di origine e di destinazione sono gli indirizzi IP Internet dei router (usati come origine e destinazione del tunnel).

Il payload ESP include il campo CMD a 8 byte, evidenziato in rosso:

- 0x04 - Intestazione successiva, ovvero IP
- 0x01 - Lunghezza (4 byte dopo l'intestazione, 8 byte con l'intestazione)
- 0x01 - Versione 01
- 0x00 - Riservato
- 0x00 - Lunghezza SGT (4 byte totali)
- 0x01 - Tipo SGT
- 0x0003 - Tag SGT (gli ultimi due ottetti, ovvero 00.03; SGT viene utilizzato per il client Windows)

Poiché per l'interfaccia del tunnel è stata usata la modalità IPsec IPv4, l'intestazione successiva è IP, che viene evidenziata in verde. L'IP di origine è c0 a8 02 c8 (192.168.2.200), e l'IP di destinazione è c0 a8 64 01 (192.168.100.1). Il numero di protocollo è 1, ossia ICMP.

L'ultima intestazione è ICMP, evidenziata in blu, con tipo 08 e codice 8 (richiesta echo).

Il payload ICMP è il successivo e ha una lunghezza di 32 byte (lettere dalla a alla i). Il payload illustrato nella figura è tipico di un client Windows.

Le altre intestazioni ESP seguono il payload ICMP:

- 0x01 0x02 - Spaziatura interna.
- 0x02 - Lunghezza spaziatura interna.
- 0x63 - Intestazione successiva che punta al protocollo 0x63, che è 'Qualsiasi schema di crittografia privato'. Ciò indica che il campo successivo (il primo campo nei dati ESP) è il tag SGT.
- 12 byte di Valore controllo integrità.

Il campo CMD si trova all'interno del payload ESP, in genere crittografato.

insidie di IKEv2: modalità GRE o IPsec

Finora questi esempi hanno utilizzato la modalità tunnel IPsec IPv4. Cosa succede se si utilizza la modalità GRE (Generic Routing Encapsulation)?

Quando il router incapsula un pacchetto IP di transito nel GRE, TrustSec visualizza il pacchetto come originato localmente, ossia l'origine del pacchetto GRE è il router, non il client Windows. Quando viene aggiunto il campo CMD, viene sempre utilizzato il tag predefinito (SGT=0) anziché un tag specifico.

Quando il traffico viene inviato dal client Windows (192.168.2.200) in modalità IPsec IPv4, viene visualizzato 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
```

Tuttavia, quando la modalità tunnel viene modificata in GRE per lo stesso traffico, il valore SGT viene visualizzato come 0. Nell'esempio, 192.168.1.20 è l'IP di origine del tunnel:

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

> **Nota**: è molto importante **non utilizzare il GRE**.

Vedere l'ID bug Cisco CSCuj25890, IOS IPSec Inline tagging per la modalità GRE: inserimento del router SGT. Questo bug è stato creato per consentire la corretta propagazione SGT quando si usa il GRE. SGT over DMVPN è supportato da Cisco IOS® XE 3.13S

ZBF basato sui tag SGT di IKEv2

Questa è una configurazione di esempio di ZBF su R2. È possibile identificare il traffico VPN con

SGT=3 perché tutti i pacchetti ricevuti dal tunnel IKEv2 sono contrassegnati (ossia contengono il campo CMD). In questo modo, il traffico VPN può essere interrotto e registrato:

```
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
```

Verifica

Quando si esegue il ping da un client Windows a 192.168.100.1 (SGT=3), i debug mostrano quanto segue:

```
*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
```

Per un ping originato da uno switch (SGT=0), i debug mostrano quanto segue:

```
*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
```

Le statistiche del firewall di R2 sono:

```
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
```

Sono disponibili quattro rilasci (il numero predefinito di Echo ICMP inviati da Windows) e cinque accettazioni (il numero predefinito per lo switch).

ZBF basato su mappatura SGT tramite SXP

Èpossibile eseguire ZBF con riconoscimento SGT su R1 e filtrare il traffico ricevuto dalla LAN. Sebbene tale traffico non sia contrassegnato da SGT, R1 dispone di informazioni di mappatura SXP e può trattare tale traffico come contrassegnato.

Nell'esempio, viene usata una policy tra le zone LAN e 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
```

Verifica

Quando si invia l'eco ICMP dal client Windows, è possibile visualizzare le perdite:

```
*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
```

Poiché la sessione SXP è basata su TCP, è possibile creare una sessione SXP tramite un tunnel IKEv2 tra 3750X-5 e R2 e applicare i criteri ZBF basati sui tag di R2 senza tag inline.

Roadmap

GET VPN inline tagging è supportato anche sui router ISR G2 e Cisco ASR serie 1000 Aggregation Services. Il pacchetto ESP ha 8 byte aggiuntivi per il campo CMD.

Èinoltre previsto il supporto per la VPN dinamica multipunto (DMVPN).

Per ulteriori informazioni, vedere la roadmap dell'infrastruttura abilitata per Cisco TrustSec.

Verifica

Le procedure di verifica sono incluse negli esempi di configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guida alla configurazione dello switch Cisco TrustSec: informazioni su Cisco TrustSec
- Libro 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1: Configuring the ASA to Integration with Cisco TrustSec
- Note di rilascio per Cisco TrustSec Disponibilità generale Release: Note di rilascio per Cisco TrustSec 3.0 General Deployability 2013 Release
- Configurazione della codifica in linea IPsec per TrustSec
- Guida alla configurazione di Cisco Group Encrypted Transport VPN, Cisco IOS XE release 3S: GET VPN Support of IPsec Inline Tagging for Cisco TrustSec
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).