Exemple de configuration d'IKEv2 avec étiquetage en ligne TrustSec SGT et pare-feu basé sur les zones et reconnaissant les balises SGT

Table des matières

Introduction

Ce document décrit comment utiliser Internet Key Exchange Version 2 (IKEv2) et une balise de groupe de sécurité (SGT) afin de marquer les paquets envoyés à un tunnel VPN. La description inclut un exemple de déploiement et d'utilisation type. Ce document explique également un pare-

feu ZBF (Zone-Based Firewall) compatible SGT et présente deux scénarios :

- ZBF basé sur les balises SGT reçues du tunnel IKEv2
- ZBF basé sur le mappage SXP (SGT eXchange Protocol)

Tous les exemples incluent des débogages au niveau paquet afin de vérifier comment la balise SGT est transmise.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base des composants TrustSec
- Connaissance de base de la configuration de l'interface de ligne de commande (CLI) des commutateurs Cisco Catalyst
- Expérience de la configuration d'un moteur Cisco Identity Services Engine (ISE)
- Connaissances de base du pare-feu basé sur les zones
- Connaissances de base de IKEv2

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7 et Microsoft Windows XP
- Logiciel Cisco Catalyst 3750-X versions 15.0 et ultérieures
- Logiciel Cisco Identity Services Engine version 1.1.4 et ultérieure
- Routeur à services intégrés (ISR) Cisco 2901 avec version logicielle 15.3(2)T ou ultérieure

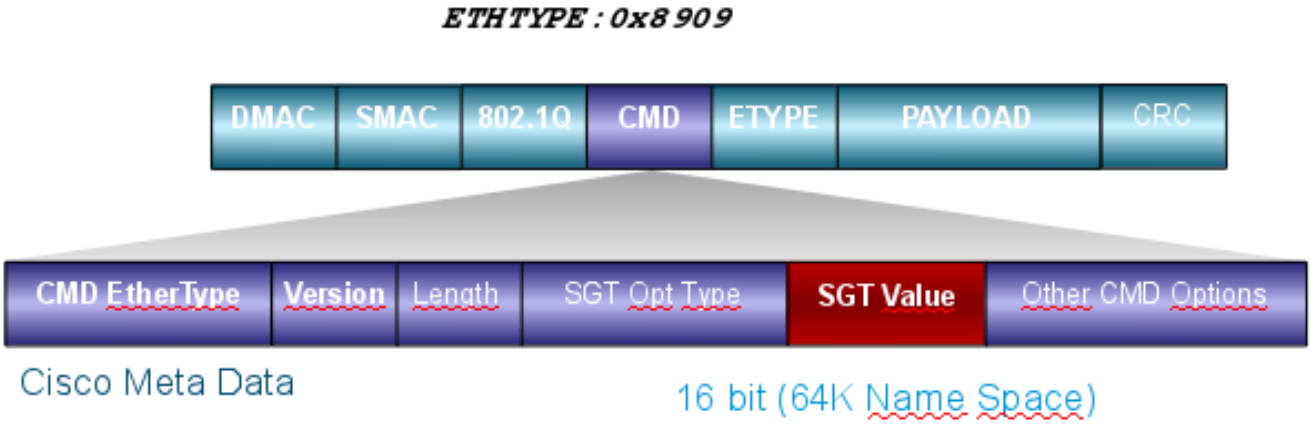
  Remarque : IKEv2 est uniquement pris en charge sur les plates-formes ISR de 2e génération (G2).

Balise de groupe de sécurité (SGT)

Le SGT fait partie de l'architecture de la solution Cisco TrustSec, qui est conçue pour utiliser des politiques de sécurité flexibles qui ne sont pas basées sur l'adresse IP.

Le trafic dans le cloud TrustSec est classifié et marqué avec une balise SGT. Vous pouvez créer des stratégies de sécurité qui filtrent le trafic en fonction de cette balise. Toutes les politiques sont gérées de manière centralisée depuis ISE et sont déployées sur tous les périphériques du cloud TrustSec.

Afin de transmettre les informations relatives à l'étiquette SGT, Cisco a modifié la trame Ethernet de la même manière que les modifications ont été apportées pour les étiquettes 802.1q. La trame Ethernet modifiée ne peut être comprise que par les périphériques Cisco sélectionnés. Il s'agit du format modifié :



Le champ de métadonnées Cisco (CMD) est inséré directement après le champ d'adresse MAC source (SMAC) ou le champ 802.1q s'il est utilisé (comme dans cet exemple).

Pour connecter des clouds TrustSec via le VPN, une extension pour les protocoles IKE et IPsec a été créée. L'extension, appelée marquage IPsec en ligne, permet l'envoi de balises SGT dans les paquets ESP (Encapsulating Security Payload). La charge utile ESP est modifiée pour transporter un champ CMD de 8 octets juste avant la charge utile du paquet lui-même. Par exemple, le paquet ICMP (Internet Control Message Protocol) crypté envoyé sur Internet contient [IP][ESP][CMD][IP][ICMP][DATA].

Des informations détaillées sont présentées dans la deuxième partie de l'article.

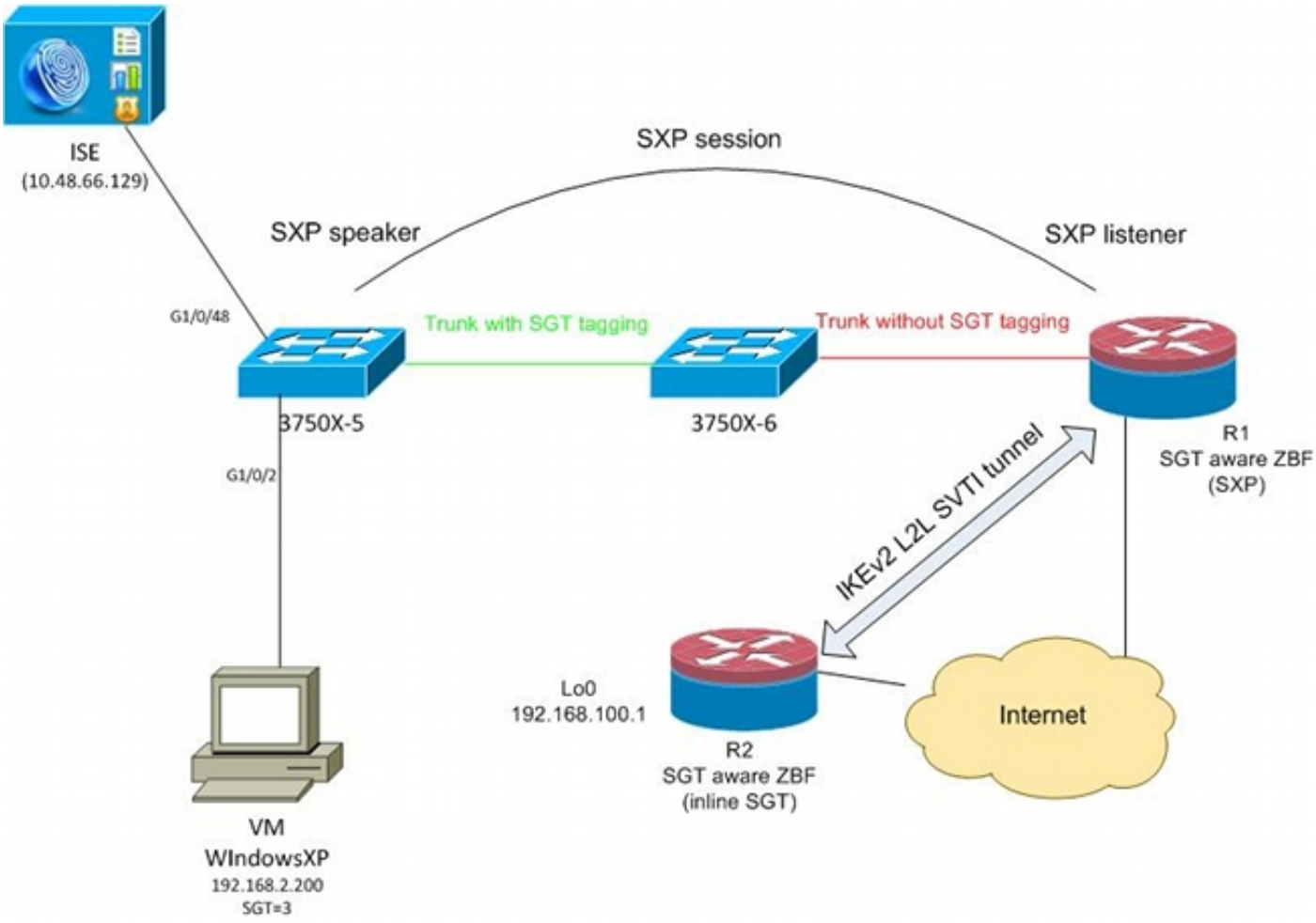
Configurer

Remarques :

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Diagramme du réseau



Flux de trafic

Dans ce réseau, 3750X-5 et 3750X-6 sont des commutateurs Catalyst situés dans le cloud TrustSec. Les deux commutateurs utilisent le provisionnement automatique des PAC (Protected Access Credentials) pour rejoindre le cloud. 3750X-5 a été utilisé comme amorce et 3750X-6 comme périphérique non amorce. Le trafic entre les deux commutateurs est chiffré avec MACsec et est correctement étiqueté.

WindowsXP utilise 802.1x pour accéder au réseau. Une fois l'authentification réussie, l'ISE renvoie l'attribut de balise SGT qui sera appliqué à cette session. Tout le trafic provenant de ce PC est étiqueté avec SGT=3.

Les routeurs 1 (R1) et 2 (R2) sont des routeurs ISR 2901. Étant donné que le routeur ISR G2 ne prend actuellement pas en charge l'étiquetage SGT, R1 et R2 se trouvent en dehors du nuage TrustSec et ne comprennent pas les trames Ethernet qui ont été modifiées avec des champs CMD afin de passer les étiquettes SGT. Ainsi, SXP est utilisé afin de transférer des informations sur le mappage IP/SGT de 3750X-5 à R1.

R1 dispose d'un tunnel IKEv2 configuré pour protéger le trafic destiné à un emplacement distant (192.168.100.1) et dont l'étiquetage en ligne est activé. Après la négociation IKEv2, R1 commence à marquer les paquets ESP envoyés à R2. L'étiquetage est basé sur les données SXP reçues de 3750X-5.

R2 peut recevoir ce trafic et, en fonction de la balise SGT reçue, effectuer des actions spécifiques définies par le ZBF.

La même opération peut être effectuée sur R1. Le mappage SXP permet à R1 d'abandonner un paquet reçu du LAN en fonction d'une balise SGT, même si les trames SGT ne sont pas prises en charge.

Configuration du cloud TrustSec

La première étape de la configuration consiste à créer un cloud TrustSec. Les deux commutateurs 3750 doivent :

- Obtenez un PAC, qui est utilisé pour l'authentification au cloud TrustSec (ISE).
- Authentifiez et passez le processus NDAC (Network Device Admission Control).
- Utilisez le protocole SAP (Security Association Protocol) pour la négociation MACsec sur une liaison.

Cette étape est nécessaire pour ce cas d'utilisation, mais pas pour que le protocole SXP fonctionne correctement. R1 n'a pas besoin d'obtenir de données PAC ou d'environnement d'ISE pour effectuer le mappage SXP et le balisage en ligne IKEv2.

Vérification

La liaison entre 3750X-5 et 3750X-6 utilise le chiffrement MACsec négocié par 802.1x. Les deux commutateurs approuvent et acceptent les balises SGT reçues par l'homologue :

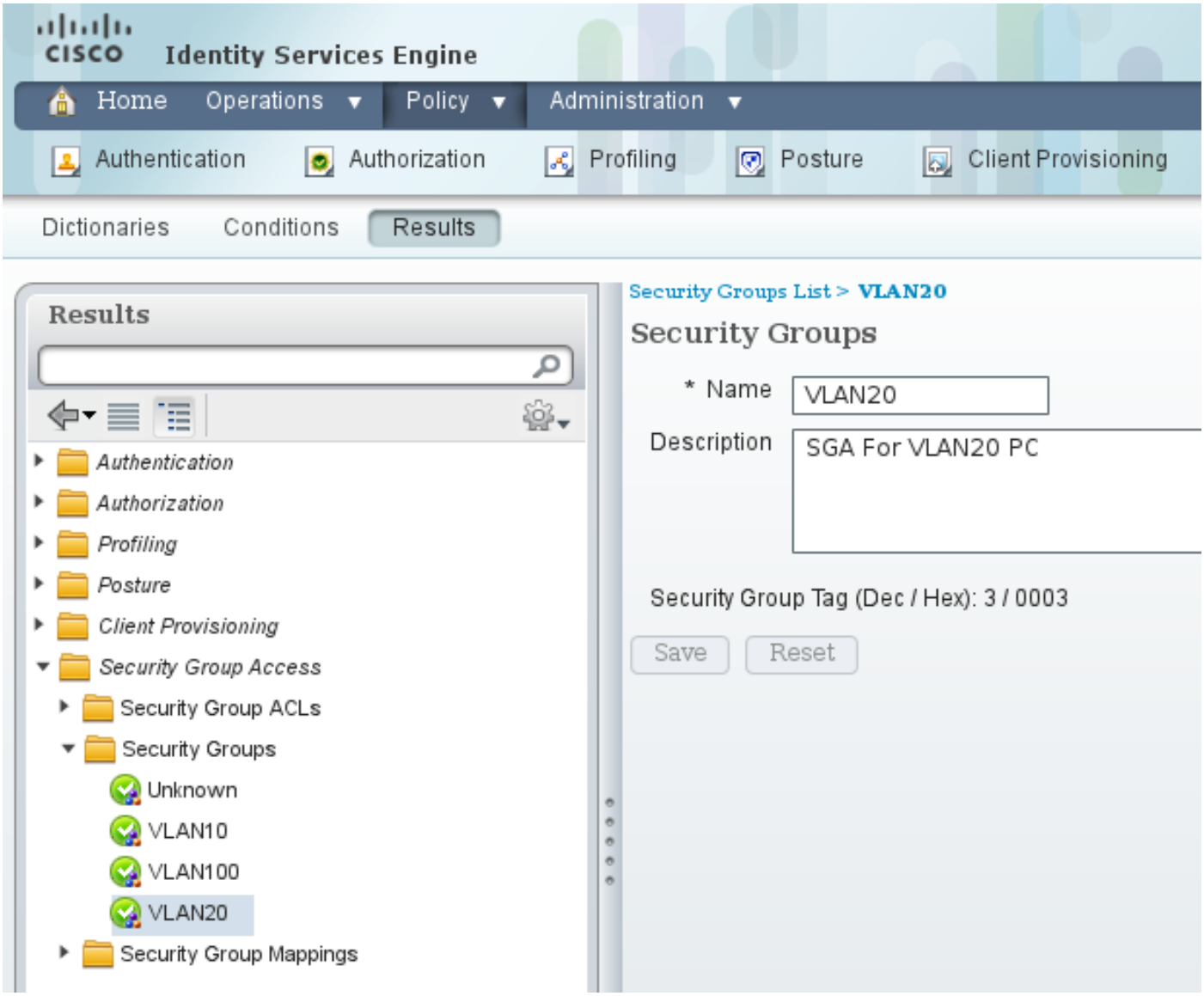
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X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

Il n'est pas possible d'appliquer une liste de contrôle d'accès basée sur les rôles (RBACL) directement sur les commutateurs. Ces stratégies sont configurées sur ISE et sont téléchargées automatiquement sur les commutateurs.

Configuration du client

Le client peut utiliser la norme 802.1x, le contournement d'authentification MAC (MAB) ou l'authentification Web. N'oubliez pas de configurer ISE afin que le groupe de sécurité correct pour la règle d'autorisation soit renvoyé :



Vérification

Vérifiez la configuration du 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
```

Àpartir de ce moment, le trafic client envoyé de 3750X-5 vers d'autres commutateurs dans le cloud TrustSec est étiqueté avec SGT=3.

Consultez Exemple de configuration et guide de dépannage TrustSec des commutateurs ASA et Catalyst 3750X pour un exemple de règles d'autorisation.

Protocole SGT Exchange entre 3750X-5 et R1

R1 ne peut pas rejoindre le cloud TrustSec, car il s'agit d'un routeur ISR G2 2901 qui ne comprend pas les trames Ethernet avec champs CMD. Ainsi, SXP est configuré sur le 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 est également configuré sur 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
```

Vérification

Assurez-vous que R1 reçoit les informations de mappage 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 sait maintenant que tout le trafic reçu de 192.168.2.200 doit être traité comme s'il était étiqueté comme SGT=3.

Configuration IKEv2 entre R1 et R2

Il s'agit d'un scénario simple basé sur des interfaces SVTI (Static Virtual Tunnel Interfaces) avec des valeurs par défaut intelligentes IKEv2. Les clés pré-partagées sont utilisées pour l'authentification, et le chiffrement nul est utilisé pour faciliter l'analyse des paquets ESP. Tout le trafic vers 192.168.100.0/24 est envoyé via l'interface de Tunnel1.

Voici la configuration du 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
```

Sur R2, tout le trafic de retour vers le réseau 192.168.2.0/24 est envoyé via l'interface Tunnel1 :

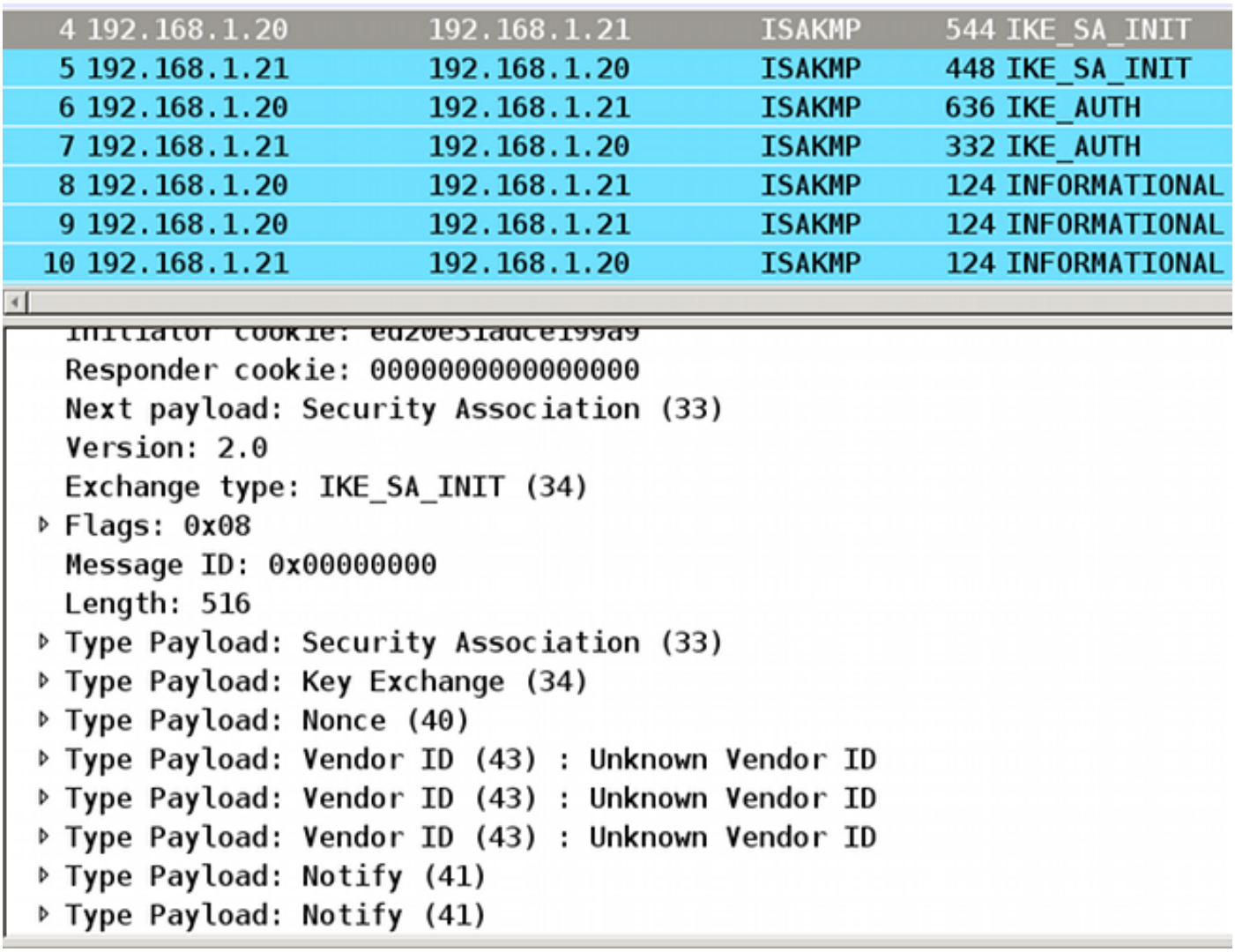
```
crypto ikev2 keyring ikev2-keyring
```

```
 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
```

Une seule commande est requise sur les deux routeurs afin d'activer l'étiquetage en ligne : la commande **crypto ikev2 cts sgt**.

Vérification

L'étiquetage en ligne doit être négocié. Dans le premier et le deuxième paquet IKEv2, un ID de fournisseur spécifique est envoyé :



Il existe trois ID de fournisseur (VID) inconnus par Wireshark. Ils sont liés à :

- DELETE-REASON, prise en charge par Cisco
- FlexVPN, pris en charge par Cisco
- Balisage en ligne SGT

Les débogages le vérifient. R1, qui est un initiateur IKEv2, envoie :

```
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 reçoit un deuxième paquet IKEv2 et le même 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
```

Les deux parties conviennent donc de placer les données CMD au début de la charge utile ESP.

Vérifiez l'association de sécurité (SA) IKEv2 afin de vérifier cet accord :

```
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
```

Après avoir envoyé le trafic du client Windows vers 192.168.100.1, R1 affiche :

```
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#
```

Notez que des paquets balisés ont été envoyés.

Pour le trafic de transit, lorsque R1 doit étiqueter le trafic envoyé du client Windows à R2, vérifiez que le paquet ESP a été correctement étiqueté avec SGT=3 :

```
debug crypto ipsc metadata sgt
```

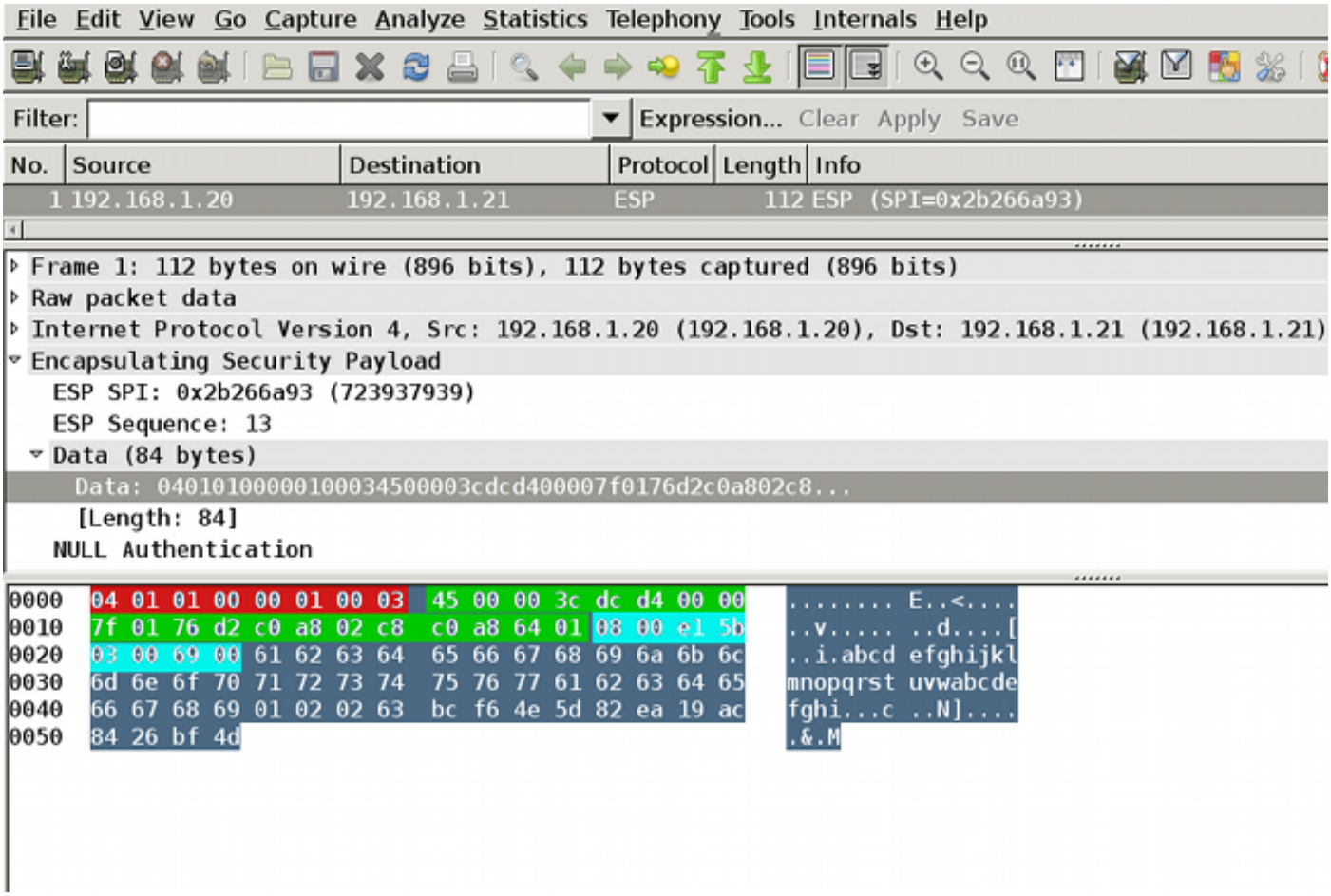
```
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

L'autre trafic provenant du même VLAN, qui provient du commutateur, prend par défaut la valeur SGT=0 :

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

Vérification du niveau de paquet ESP

Utilisez Embedded Packet Capture (EPC) afin d'examiner le trafic ESP de R1 à R2, comme le montre cette figure :



Wireshark a été utilisé pour décoder le cryptage Null pour l'index des paramètres de sécurité (SPI). Dans l'en-tête IPv4, les adresses IP source et de destination sont les adresses IP Internet des routeurs (utilisées comme source et destination du tunnel).

La charge utile ESP inclut le champ CMD de 8 octets, mis en surbrillance en rouge :

- 0x04 - En-tête suivant, qui est IP
- 0x01 - Longueur (4 octets après l'en-tête, 8 octets avec l'en-tête)
- 0x01 - Version 01
- 0x00 - Réservé
- 0x00 - Longueur SGT (4 octets au total)
- 0x01 - Type SGT
- 0x0003 - SGT tag (les deux derniers octets, 00 03 ; SGT est utilisé pour le client Windows)

Le mode IPsec IPv4 ayant été utilisé pour l'interface du tunnel, l'en-tête suivant est IP, mis en surbrillance en vert. L'adresse IP source est c0 a8 02 c8 (192.168.2.200) et l'adresse IP de

destination est c0 a8 64 01 (192.168.100.1). Le numéro de protocole est 1, c'est-à-dire ICMP.

Le dernier en-tête est ICMP, surligné en bleu, avec le type 08 et le code 8 (requête d'écho).

La charge utile ICMP est la suivante et elle a une longueur de 32 octets (c'est-à-dire les lettres de a à i). La charge utile de la figure est typique d'un client Windows.

Les autres en-têtes ESP suivent la charge utile ICMP :

- 0x01 0x02 - Remplissage.
- 0x02 - Longueur du remplissage.
- 0x63 - En-tête suivant qui pointe vers le protocole 0x63, qui est « Tout schéma de chiffrement privé ». Cela indique que le champ suivant (le premier champ des données ESP) est l'étiquette SGT.
- 12 octets de valeur de contrôle d'intégrité.

Le champ CMD se trouve à l'intérieur de la charge utile ESP, qui est généralement chiffrée.

Pièges liés à IKEv2 : mode GRE ou IPsec

Jusqu'à présent, ces exemples ont utilisé le mode tunnel IPsec IPv4. Que se passe-t-il si le mode Generic Routing Encapsulation (GRE) est utilisé ?

Lorsque le routeur encapsule un paquet IP de transit dans GRE, TrustSec considère le paquet comme provenant localement, c'est-à-dire que la source du paquet GRE est le routeur et non le client Windows. Lorsque le champ CMD est ajouté, la balise par défaut (SGT=0) est toujours utilisée à la place d'une balise spécifique.

Lorsque le trafic est envoyé à partir du client Windows (192.168.2.200) en mode IPsec IPv4, vous voyez 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
```

Mais, une fois que le mode tunnel est changé en GRE pour le même trafic, vous voyez que SGT=0. Dans cet exemple, 192.168.1.20 est l'adresse IP source du tunnel :

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

> **Remarque** : il est donc très important de **ne pas utiliser GRE**.

Voir ID de bogue Cisco CSCuj25890, IOS IPSec Inline tagging for GRE mode : insert router SGT. Ce bogue a été créé afin de permettre une propagation SGT correcte lorsque vous utilisez GRE. SGT sur DMVPN est pris en charge par Cisco IOS® XE 3.13S

ZBF basé sur les balises SGT d'IKEv2

Ceci est un exemple de configuration de ZBF sur R2. Le trafic VPN avec SGT=3 peut être identifié parce que tous les paquets reçus du tunnel IKEv2 sont étiquetés (c'est-à-dire qu'ils contiennent le champ CMD). Ainsi, le trafic VPN peut être abandonné et consigné :

```
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
```

Vérification

Lorsqu'une requête ping vers 192.168.100.1 provient du client Windows (SGT=3), les débogages affichent ceci :

```
*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
```

Pour une requête ping qui provient d'un commutateur (SGT=0), les débogages montrent ceci :

```
*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
```

Les statistiques de pare-feu de R2 sont les suivantes :

```
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
```

Il y a quatre abandons (nombre par défaut d'écho ICMP envoyé par Windows) et cinq acceptations (nombre par défaut pour le commutateur).

ZBF basé sur le mappage SGT via SXP

Il est possible d'exécuter ZBF compatible SGT sur R1 et de filtrer le trafic reçu du LAN. Bien que ce trafic ne soit pas étiqueté SGT, R1 dispose d'informations de mappage SXP et peut traiter ce trafic comme étiqueté.

Dans cet exemple, une politique est utilisée entre les zones LAN et 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
```

Vérification

Lorsque ICMP Echo est envoyé à partir du client Windows, vous pouvez voir les abandons :

```
*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
```

La session SXP étant basée sur TCP, vous pouvez également créer une session SXP via un tunnel IKEv2 entre 3750X-5 et R2 et appliquer des stratégies ZBF basées sur les balises de R2 sans marquage en ligne.

Feuille De Route

L'étiquetage en ligne GET VPN est également pris en charge sur les routeurs ISR G2 et les routeurs à services d'agrégation Cisco ASR 1000. Le paquet ESP comporte un champ CMD supplémentaire de 8 octets.

La prise en charge de DMVPN (Dynamic Multipoint VPN) est également prévue.

Pour plus d'informations, consultez la feuille de route Cisco TrustSec-Enabled Infrastructure.

Vérifier

Les procédures de vérification sont incluses dans les exemples de configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration du commutateur Cisco TrustSec : Présentation de Cisco TrustSec
- Livre 1 : Cisco ASA Series General Operations CLI Configuration Guide, 9.1 : Configuration de l'ASA pour l'intégration à Cisco TrustSec
- Notes de version pour les versions de disponibilité générale de Cisco TrustSec : Notes de version pour la version 2013 de Cisco TrustSec 3.0 General Deployability
- Configuration du balisage IPsec en ligne pour TrustSec
- Guide de configuration VPN de transport crypté de groupe Cisco, Cisco IOS XE version 3S : prise en charge GET VPN du marquage IPsec en ligne pour Cisco TrustSec
- Technical Support & Documentation - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.