IKEv2 مع تضمين العلامات داخلي للرقيب TrustSec وتكوين جدار حماية قائم على المنطقة مع مراعاة للرقيب

المحتويات

المقدمة

يصف هذا المستند كيفية إستخدام مفتاح الإنترنت الإصدار 2 (IKEv2) وعلامة مجموعة الأمان (SGT) لوضع علامات على الحزم المرسلة إلى نفق VPN. يتضمن الوصف حالة نشر واستخدام نموذجية. يشرح هذا المستند أيضا جدار حماية قائم على المنطقة قائم على الرقيب (ZBF) ويقدم سيناريوهين:

- إطار ZBF يعتمد على علامات رقيب مستلمة من نفق IKEv2

• بروتوكول ZBF القائم على تخطيط بروتوكول SXP) Sgt Xchange)
تتضمن جميع الأمثلة تصحيح أخطاء مستوى الحزمة للتحقق من كيفية إرسال علامة الرقيب.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بمكونات TrustSec
- معرفة الأساسية من أمر خط قارن (CLI) تشكيل من cisco مادة حفازة مفتاح
- الخبرة في تكوين محرك خدمات الهوية (ISE) من Cisco
- معرفة أساسية بجدار الحماية المستند إلى مناطق
- معرفة أساسية ب IKEv2

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Microsoft Windows 7 و Microsoft Windows XP
- برنامج Cisco Catalyst 3750-X، الإصدار 15.0 والإصدارات الأحدث
- برنامج محرك خدمات الهوية من Cisco، الإصدار 1.1.4 والإصدارات الأحدث
- موجه الخدمات المدمجة الطراز 2901 من ISR) Cisco) مع الإصدار T(2)15.3 من البرنامج أو إصدار أحدث

ملاحظة: يتم دعم IKEv2 فقط على أنظمة ISR Generation 2 (G2) الأساسية.

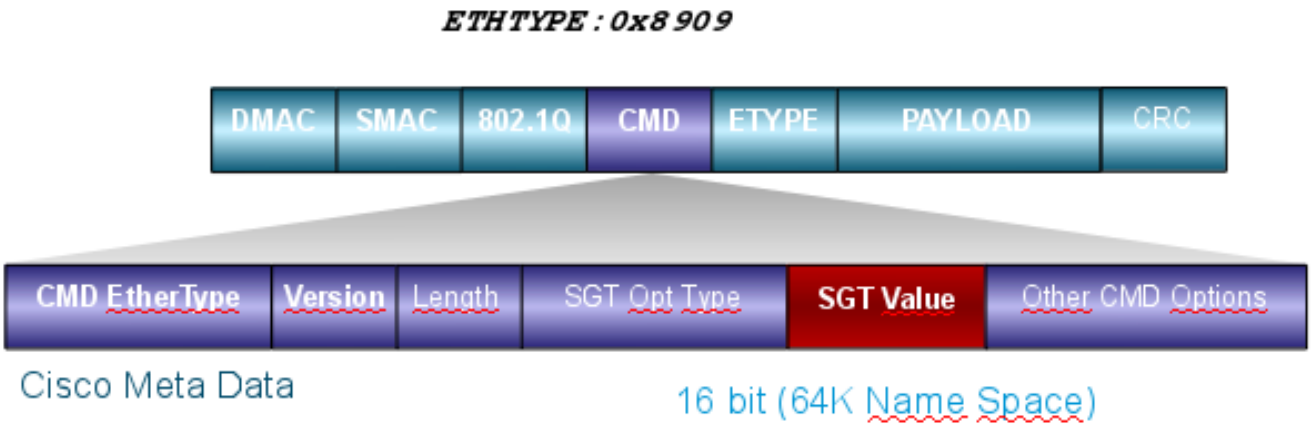
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

علامة مجموعة الأمان (الرقيب)

يعد الرقيب جزءا من بنية حل Cisco TrustSec، التي تم تصميمها لاستخدام سياسات أمان مرنة لا تستند إلى عنوان IP.

يتم تصنيف حركة المرور في سحابة TrustSec ووضع علامة عليها باستخدام علامة SGT. يمكنك إنشاء سياسات تأمين لتصفية حركة مرور البيانات بناء على تلك العلامة. يتم توجيه جميع السياسات مركزيا من ISE ويتم نشرها إلى جميع الأجهزة الموجودة في مجموعة نظراء TrustSec.

من أجل تمرير المعلومات حول علامة الرقيب، قامت Cisco بتعديل إطار الإيثرنت بحيث يماثل طريقة إجراء التعديلات لعلامات 802.1q. لا يمكن فهم إطار الإيثرنت المعدل إلا بواسطة أجهزة Cisco المحددة. هذا هو التنسيق المعدل:



يتم إدخال حقل بيانات التعريف (CMD) من Cisco مباشرة بعد حقل عنوان MAC المصدر (SMAC) أو حقل 802.1q إذا تم إستخدامه (كما في هذا المثال).

لتوصيل سحب TrustSec عبر الشبكة الخاصة الظاهرية (VPN)، تم إنشاء ملحق لبروتوكولات IKE و IPsec. يسمح الملحق، المسمى وضع علامات تمييز سطر IPsec، بإرسال علامات SGT في حزم حمولة أمان التضمين (ESP). يتم تعديل حمولة ESP لحمل حقل CMD مكون من 8 بايت قبل حمولة الحزمة نفسها مباشرة. على سبيل المثال، تحتوي الحزمة المشفرة لبروتوكول رسائل التحكم في الإنترنت (ICMP) التي يتم إرسالها عبر الإنترنت على [[ESP] [IP] ICMP] [IP] [[CMD] [البيانات].

وترد معلومات مفصلة في الجزء الثاني من المادة.

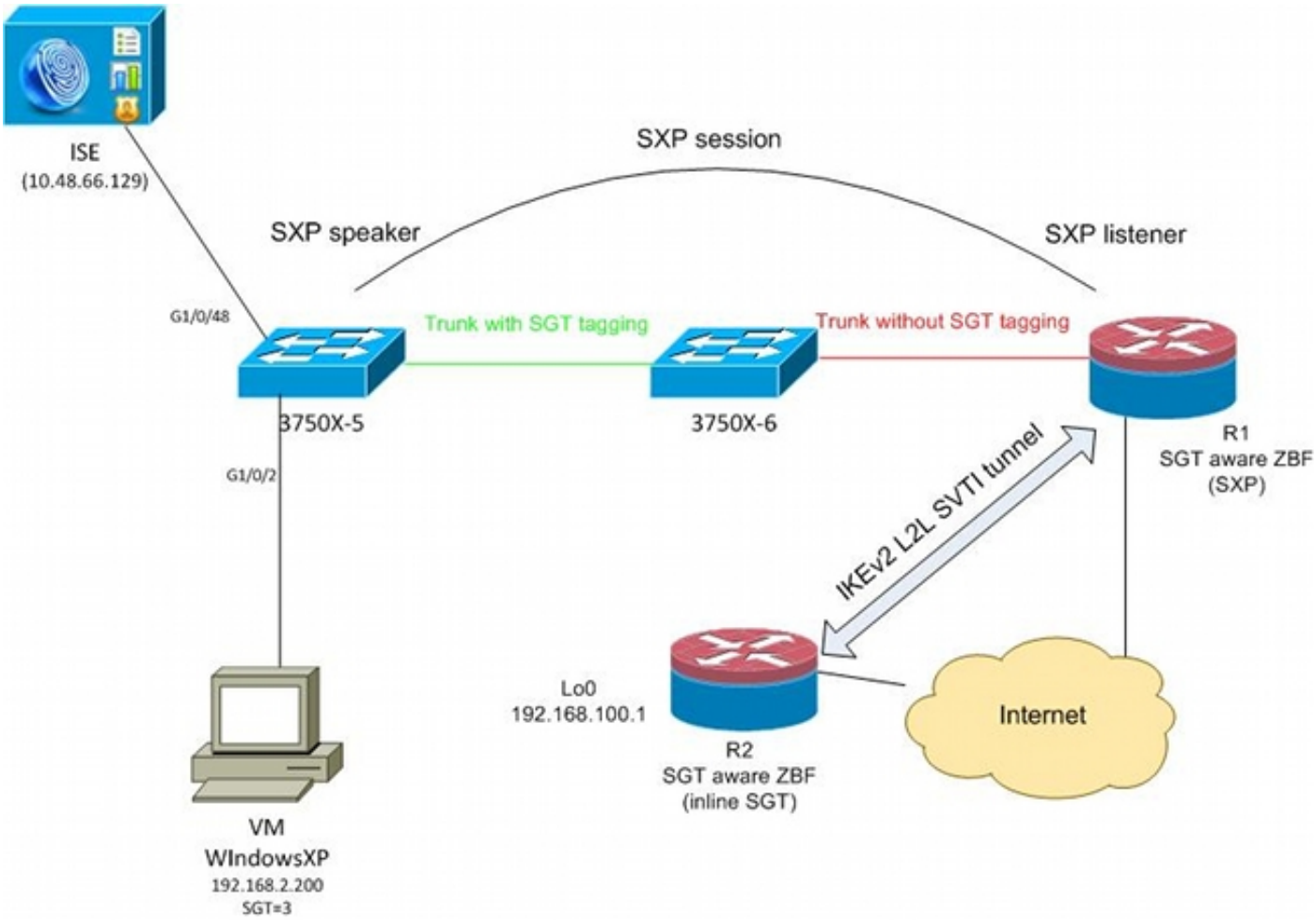
التكوين

ملاحظات:

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

الرسم التخطيطي للشبكة



تدفق حركة المرور

في هذه الشبكة، تعد 3750X-5 و 3750X-6 محولات Catalyst Switches داخل سحابة TrustSec. يستخدم كلا المحولين إمداد مسوغات الوصول المحمي التلقائي (PACs) للانضمام إلى السحابة. تم إستخدام 3750X-5 كبذرة، و 3750X-6 كجهاز غير بذرة. يتم تشفير حركة مرور البيانات بين كلا المحولين باستخدام MACsec ويتم تمييزها بشكل صحيح.

يستخدم WindowsXP 802.1x للوصول إلى الشبكة. وبعد مصادقة ناجحة، ترجع ISE سمة علامة الرقيب التي سيتم تطبيقها في جلسة العمل هذه. يتم وضع علامة على جميع حركات المرور المستمدة من ذلك الكمبيوتر باستخدام SGT=3.

الموجه 1 (R1) والموجه 2 (R2) هما ISRs 2901. نظرا لأن ISR G2 لا يدعم حاليا علامات الرقيب، فإن R1 و R2 خارجان عن سحابة TrustSec ولا يفهمان إطارات الإيثرنت التي تم تعديلها باستخدام حقول CMD من أجل تجاوز علامات المجموعة. وبالتالي، يتم إستخدام SXP لإعادة توجيه المعلومات حول تخطيط IP/SGT من 3750X-5 إلى R1.

يحتوي R1 على نفق IKEv2 تم تكوينه لحماية حركة المرور الموجهة إلى موقع بعيد (192.168.100.1) ويحتوي على علامات مضمن ممكنة. بعد تفاوض IKEv2، يبدأ R1 في تمييز حزم ESP التي يتم إرسالها إلى R2. وضع العلامات يستند إلى بيانات SXP المستلمة من 3750X-5.

يمكن للخادم طراز R2 إستقبال حركة المرور هذه، كما يمكنه، استنادا إلى علامة الرقيب المتلقي، تنفيذ إجراءات محددة محددة وفقا لمعيار ZBF.

ويمكن تنفيذ الأمر نفسه على R1. يسمح تخطيط SXP ل R1 بإسقاط حزمة مستلمة من الشبكة المحلية (LAN) استنادا إلى علامة رقيب، حتى في حالة عدم دعم إطارات الرقيب.

تكوين سحابة TrustSec

تتمثل الخطوة الأولى في التكوين في إنشاء سحابة TrustSec. يحتاج كلا المحولين 3750 إلى:

- الحصول على مسوغ وصول محمي (PAC)، يتم إستخدامه لمصادقة سحابة ISE) TrustSec).
- مصادقة عملية التحكم في الدخول إلى جهاز الشبكة (NDAC) وتمريرها.
- إستخدام بروتوكول اقتران الأمان (SAP) لمفاوضات MacSec على إرتباط ما.

هذه الخطوة ضرورية لحالة الاستخدام هذه، ولكنها ليست ضرورية لبروتوكول SXP ليعمل بشكل صحيح. لا يحتاج R1 إلى الحصول على مسوغ وصول محمي أو بيانات بيئة من ISE لتنفيذ تخطيط SXP ووضع علامات في السطر ل IKEv2.

التحقق

يستخدم الارتباط بين 5-3750X و 6-3750X تشفير MacSec الذي تم التفاوض عليه بواسطة 802. 1x. يعتمد كلا المحولين ويقبلان علامات الرقيب التي يتلقاها النظير:

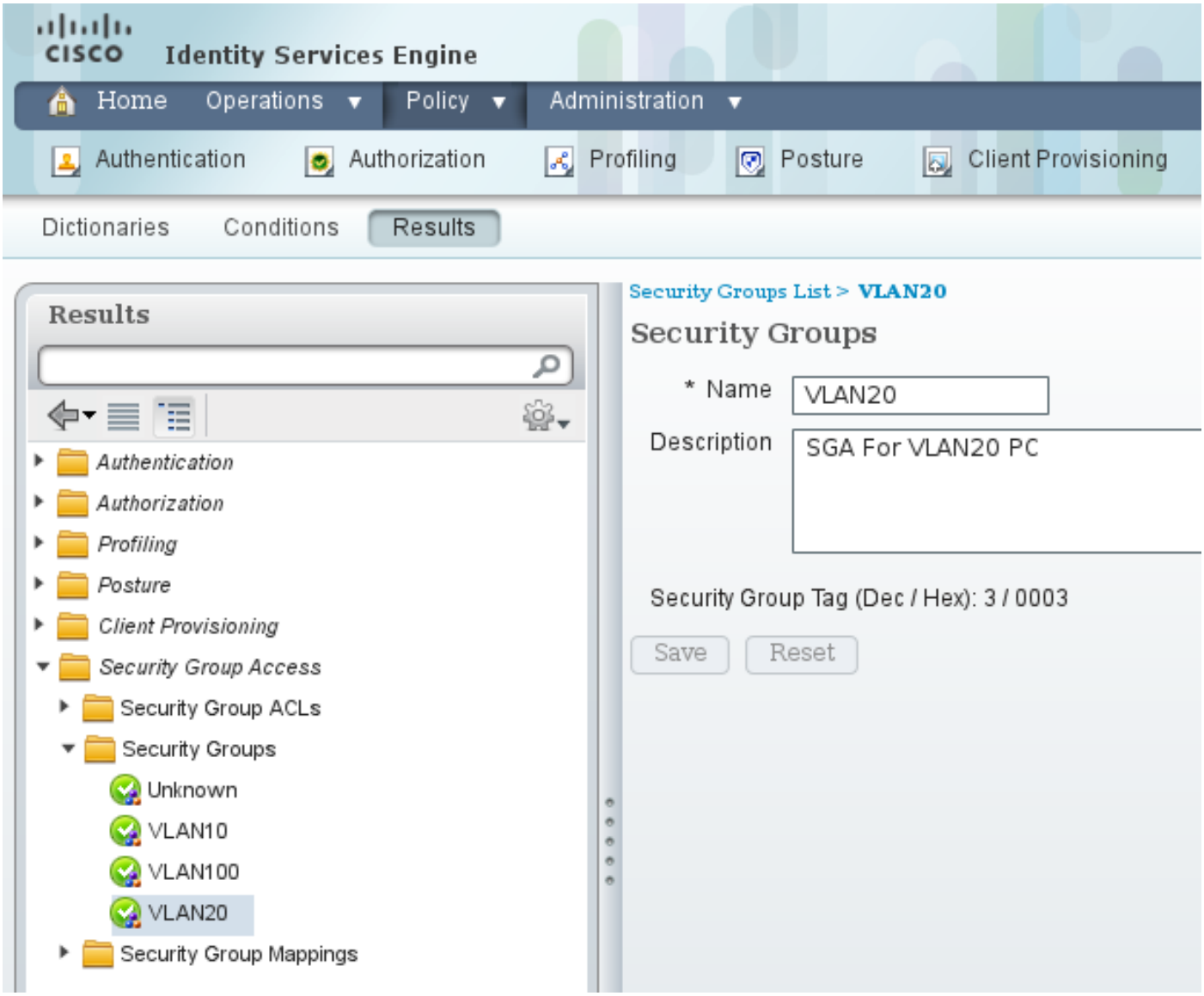
```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
CTS is enabled, mode:    DOT1X
IFC state:               OPEN
Authentication Status:   SUCCEEDED
"Peer identity:       "3750X6
"Peer's advertised capabilities: "sap
802.1X role:         Supplicant
Reauth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

لا يمكن تطبيق قائمة التحكم في الوصول (RBACL) المستندة إلى الأدوار مباشرة على المحولات. ويتم تكوين هذه

السياسات على ISE ويتم تنزيلها تلقائيا على المحولات.

تكوين العميل

يمكن للعميل إستخدام 802.1x أو تجاوز مصادقة MAC (MAB) أو مصادقة ويب. تذكر تكوين ISE حتى يتم إرجاع مجموعة الأمان الصحيحة لقاعدة التخويل:



التحقق

تحقق من تكوين العميل:

```
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
```

من هذه النقطة فصاعدا، يتم تمييز حركة مرور العميل المرسلة من 3750X-5 إلى المحولات الأخرى داخل سحابة TrustSec باستخدام SGT=3.

راجع مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أستكشاف الأخطاء وإصلاحها كمثال على قواعد التخويل.

بروتوكول تبادل الرقيب بين الطرازين 3750x-5 و R1

يتعذر على R1 الانضمام إلى مجموعة النظراء TrustSec لأنه موجه ISR G2 2901 لا يفهم إطارات الإيثرنت بحقول CMD. لذلك، يتم تكوين SXP على 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
```

تم تكوين SXP أيضا على 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
```

التحقق

تأكد من تلقي R1 معلومات تعيين 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
```

يعرف R1 الآن أن كل حركة المرور الواردة من 192.168.2.200 يجب التعامل معها كما لو تم وضع علامة عليها على أنها SGT=3.

تكوين IKEv2 بين R1 و R2

هذا سيناريو ثابت بسيط يستند إلى واجهات النفق الظاهرية (SVTI) مع إعدادات افتراضية ذكية ل IKEv2. يتم إستخدام المفاتيح المشتركة مسبقا للمصادقة، ويتم إستخدام التشفير الفارغ لتسهيل تحليل حزمة ESP. يتم إرسال جميع حركات المرور إلى 24/192.168.100.0 من خلال واجهة Tunnel1.

هذا هو التكوين على 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
```

في R2، يتم إرسال جميع حركة مرور البيانات العائدة إلى الشبكة 24/192.168.2.0 من خلال واجهة Tunnel1:

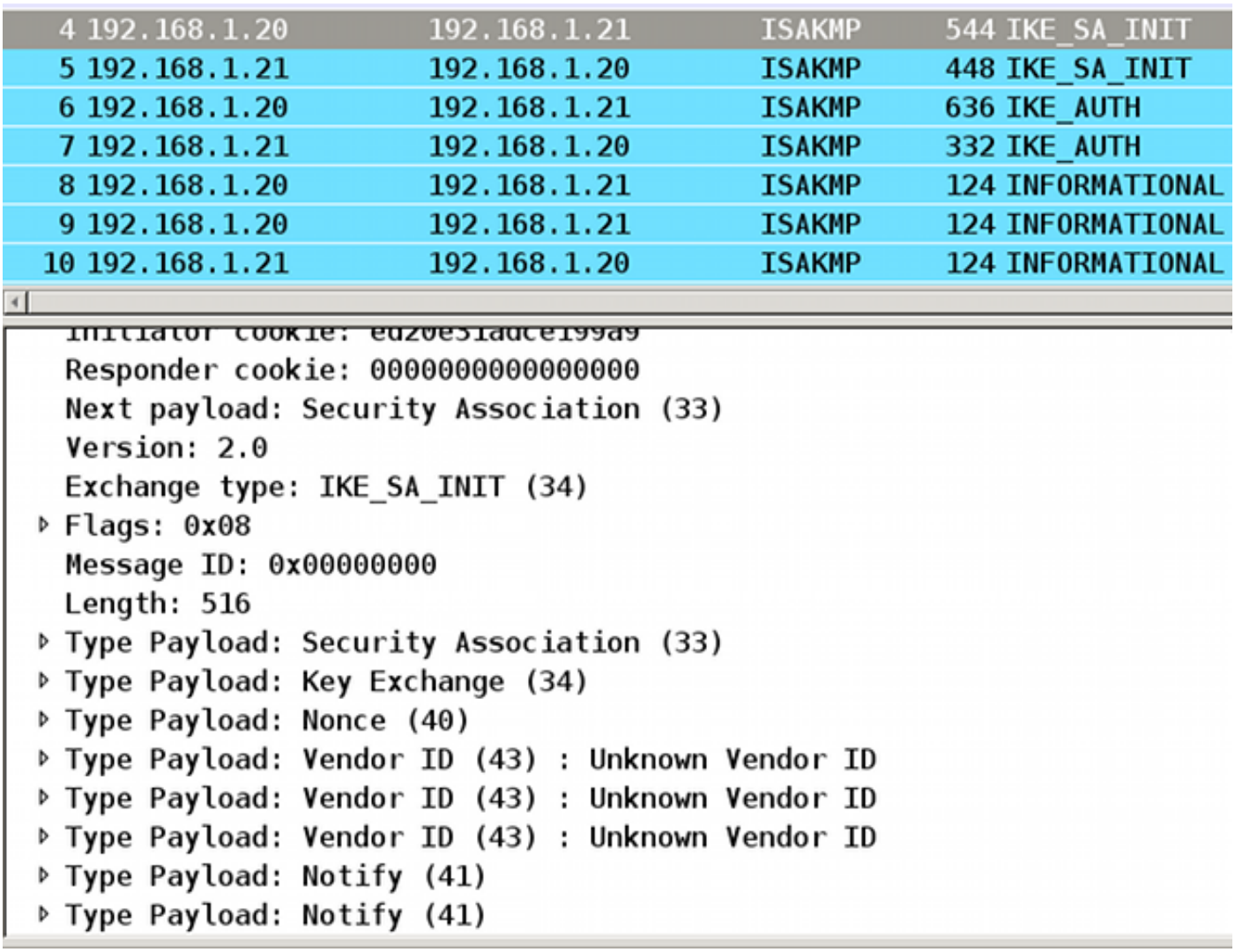
```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.20
  address 192.168.1.20
  pre-shared-key cisco

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
```

يتطلب الأمر أمر واحد فقط على كلا الموجهين لتمكين التمييز داخل السطر: الأمر **crypto ikev2 cts sgt**.

التحقق

يجب التفاوض على وضع العلامات في الخانة. في الحزمة الأولى والثانية IKEv2، يتم إرسال معرف مورد محدد:



هناك ثلاثة معرفات لمورد (VIDs) غير معروفة بواسطة Wireshark. وهي تتعلق بما يلي:

- سبب الحذف، مدعوم من قبل Cisco
- FlexVPN، مدعوم من قبل Cisco
- وضع علامات الرقيب في السطر

يتحقق تصحيح الأخطاء من ذلك. يرسل R1، وهو مهيئ IKEv2، ما يلي:

```
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*
```

يتلقى R1 حزمة IKEv2 ثانية ونفس 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*
```
وبالتالي فإن كلا الجانبين يتفقان على وضع بيانات الدفاع الصاروخي الباليستي في بداية حمولة بروتوكول الإنترنت (ESP).

تحقق من اقتران أمان SA) IKEv2) للتحقق من هذه الاتفاقية:

```
BSNS-2901-1#show crypto ikev2 sa detailed
                                 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
 none/none            READY      192.168.1.21/500      192.168.1.20/500         1
   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
```
بعد أن يقوم بإرسال حركة مرور البيانات من عميل Windows إلى الإصدار 192.168.100.1، يظهر 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#
```

لاحظ أنه قد تم إرسال الحزم المميزة.

بالنسبة لحركة مرور النقل، عندما يحتاج R1 إلى تمييز حركة مرور البيانات المرسلة من عميل Windows إلى R2، تأكد من وضع علامة بشكل صحيح على حزمة ESP باستخدام SGT=3:

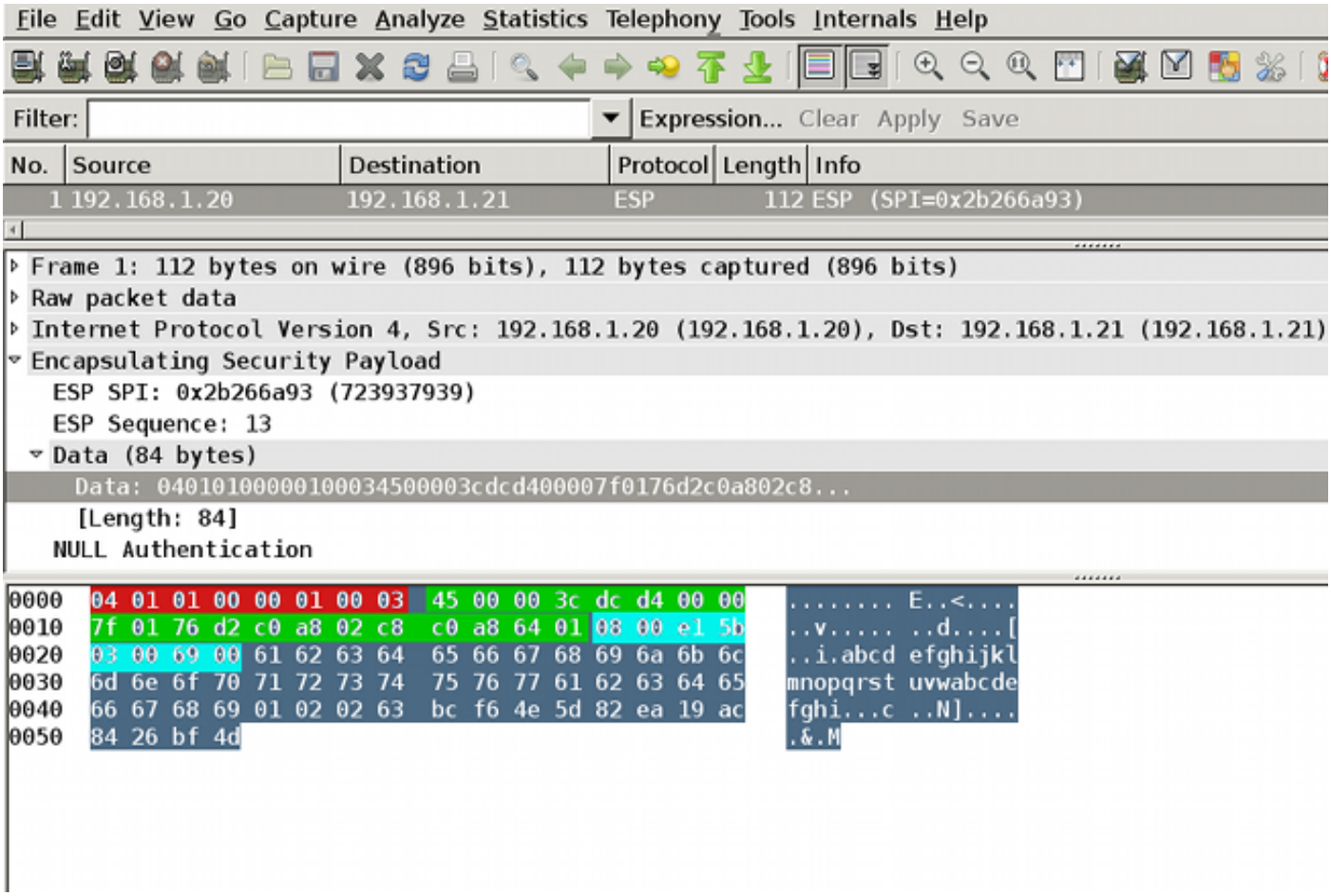
```
debug crypto ipsc metadata sgt
Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200*
```

آخر حركة مرور من ال نفسه VLAN، أي يكون مصدر من المفتاح، تقصير إلى رقيب=0:

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

التحقق من مستوى حزمة ESP

أستخدم التقاط الحزمة المضمنة (EPC) لمراجعة حركة مرور ESP من R1 إلى R2، كما هو موضح في هذا الشكل:



تم إستخدام Wireshark لفك ترميز التشفير الفارغ لفهرس معلمات الأمان (SPI). في رأس IPv4، يمثل المصدر والوجهة عنوان IP للإنترنت الخاص بالموجهات (يستخدم كمصدر نفق ووجهة).

تتضمن حمولة بروتوكول ESP حقل CMD مكون من 8 بايت، والذي يتم إبرازه بالأحمر:

- 0x04 - العنوان التالي، وهو IP
- 0x01 - الطول (4 بايت بعد الرأس و 8 بايت مع الرأس)
- 0x01 - الإصدار 01
- 0x00 - محجوز
- 0x00 - طول الرقيب (إجمالي 4 بايت)
- 0x01 - نوع الرقيب
- 0x0003 - علامة الرقيب (آخر نظامان ثمانيان، وهما 0003، يتم إستخدام العلامة الرقيب لعميل Windows)

ونظرا لاستخدام وضع IPsec IPv4 لواجهة النفق، فإن الرأس التالي هو IP، والذي يتم إبرازه بالأخضر. المصدر هو (192.168.2.200 c0 a8 02 c8)، والوجهة (192.168.100.1 IP c0 a8 64 01). رقم البروتوكول هو 1، وهو ICMP.

الرأس الأخير هو ICMP، مبرزة بالأزرق، مع نوع 08 ورمز 8 (طلب صدى).

تكون حمولة ICMP التالية ويبلغ طولها 32 بايت (أي، الحروف من a إلى i). الحمولة الموجودة في الشكل نموذجية لعميل Windows.

وتتبع باقي رؤوس ESP حمولة ICMP:

- 0x02 0x01 - التوسيع.
- 0x02 - طول الحشو.
- 0x63 - يشير العنوان التالي إلى البروتوكول 0x63، وهو "أي مخطط تشفير خاص". وهذا يشير إلى أن الحقل التالي (أول حقل في بيانات ESP) هو علامة الرقيب.
- 12 بايت من قيمة التحقق من التكامل.

يوجد حقل CMD داخل حمولة ESP، والتي يتم تشفيرها بشكل شائع.

ثقوب IKEv2: وضع GRE أو IPsec

حتى الآن، كانت هذه الأمثلة تستخدم IPv4 لوضع النفق. ماذا يحدث إذا تم إستخدام وضع تضمين التوجيه العام (GRE)؟

عندما يقوم الموجه بتضمين حزمة IP للنقل في GRE، يعرض TrustSec الحزمة كما تم إنشاؤها محليا - أي، أن مصدر حزمة GRE هو الموجه، وليس عميل Windows. عند إضافة حقل CMD، يتم دائما إستخدام العلامة الافتراضية (SGT=0) بدلا من علامة تمييز معينة.

عند إرسال حركة مرور البيانات من عميل (192.168.2.200 Windows) في الوضع IPsec IPv4، يمكنك الاطلاع على الرقيب=3:

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

ولكن بعد تغيير وضع النفق إلى GRE لنفس حركة المرور، ترى أن الرقيب=0. في هذا المثال، 192.168.1.20 هو مصدر النفق IP:

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

ملاحظة: من المهم جدا **عدم إستخدام تقنية GRE**.

راجع معرف تصحيح الأخطاء من CSCuj25890 Cisco، وضع علامة الخط المضمنة IOS IPSec لوضع GRE: إدخال موجه الرقيب. تم إنشاء هذا الخطأ للسماح بانتشار الرقيب بشكل مناسب عند إستخدام GRE. يتم دعم الرقيب عبر DMVPN من برنامج Cisco IOS® XE 3.13S

معيار ZBF قائم على علامات رقيب من IKEv2

هذا مثال لتكوين ZBF على R2. يمكن تحديد حركة مرور VPN مع SGT=3 لأن جميع الحزم المستلمة من نفق IKEv2 تم تمييزها (أي أنها تحتوي على حقل CMD). وبالتالي، يمكن إسقاط حركة مرور شبكة VPN وتسجيلها:

```
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
```

التحقق

عندما يتم الحصول على إختبار اتصال من عميل Windows (SGT=3) من 192.168.100.1، تظهر الأخطاء ما يلي:

```
Jul 23 20:05:18.822: %FW-6-DROP_PKT: Dropping icmp session*
on zone-pair ZP class TAG_3 due to 192.168.100.1:0 192.168.2.200:0
DROP action found in policy-map with ip ident 0
```

بالنسبة لعملية إختبار الاتصال التي يتم الحصول عليها من محول (SGT=0)، تظهر عمليات تصحيح الأخطاء ما يلي:

```
(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
```

إحصائيات جدار الحماية من R2 هي:

```
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
   packets, 160 bytes 4

  (Class-map: TAG_ANY (match-all
  Match: security-group source tag 0
   Pass
   packets, 400 bytes 5
```

```
(Class-map: class-default (match-any
Match: any
Drop
packets, 0 bytes 0
```

هناك أربع حالات إسقاط (الرقم الافتراضي لصدى ICMP الذي تم إرساله بواسطة Windows) وخمس حالات قبول (الرقم الافتراضي للمحول).

ZBF استنادا إلى تخطيط الرقيب من خلال SXP

من الممكن تشغيل ZBF التابع للرقيب-aware على R1 وتصفية حركة المرور المستلمة من الشبكة المحلية. على الرغم من أن حركة المرور ليست SGT tagged، فإن R1 له معلومات تخطيط SXP ويمكن أن يتعامل مع حركة المرور تلك على أنها مميزة.

في هذا المثال، يتم إستخدام سياسة بين مناطق LAN و 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
```

التحقق

عند إرسال "صدى ICMP" من عميل Windows، يمكنك مشاهدة عمليات السقوط:

```
Jul 25 09:22:07.380: %FW-6-DROP_PKT: Dropping icmp session 192.168.2.200:0*
on zone-pair ZP class TAG_3 due to DROP action found in 192.168.100.1:0
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
          packets, 160 bytes 4

  (Class-map: TAG_ANY (match-all
Match: security-group source tag 0
                              Pass
          packets, 400 bytes 5

(Class-map: class-default (match-any
                    Match: any
                      Drop
        packets, 0 bytes 0
```

لأن جلسة SXP تستند إلى TCP، يمكنك أيضا إنشاء جلسة SXP عبر نفق IKEv2 بين 3750X-5 و R2 وتطبيق سياسات ZBF استنادا إلى علامات التمييز على R2 بدون وضع علامات في السطر.

خارطة الطريق

كما يتم دعم وضع علامة VPN المضمنة على موجهات خدمات التجميع من السلسلة ISR G2 و Cisco ASR 1000 Series. تحتوي حزمة ESP على 8 بايت إضافية لحقل CMD.

كما تم تخطيط دعم شبكة VPN متعددة النقاط الديناميكية (DMVPN).

راجع مخطط البنية الأساسية التي تم تمكين Cisco TrustSec لها للحصول على مزيد من المعلومات.

التحقق من الصحة

يتم تضمين إجراءات التحقق من الصحة ضمن أمثلة التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- دليل تكوين محول Cisco TrustSec: فهم Cisco TrustSec
- الدليل 1: دليل تكوين واجهة سطر الأوامر (CLI) للعمليات العامة Cisco ASA Series، الإصدار 9.1: تكوين ASA للتكامل مع Cisco TrustSec
- ملاحظات الإصدار الخاصة بإصدارات التوفر العام من Cisco TrustSec: ملاحظات الإصدار الخاصة بإصدار Cisco TrustSec 3.0 General Deployment 2013

- تكوين علامات IPsec المضمنة لـ TrustSec
- دليل تكوين Cisco IOS XE، Cisco Group Encrypted Transport VPN، الإصدار 3S: الحصول على دعم VPN لتضمين علامات سطر IPsec لـ Cisco TrustSec
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).