GetVPN مع وضع علامات في السطر للرقيب TrustSec ومثال تكوين جدار الحماية القائم على المنطقة مع مراعاة للرقيب

المحتويات

المقدمة

ستقدم هذه المقالة كيفية تكوين GETVPN لدفع السياسات التي تسمح بإرسال رقم مجموعة الأمان (SGT) واستقباله وإدراجه في الحزم المشفرة. يتضمن المثال وضع علامات على فرعيني يؤديان إلى جميع حركات المرور باستخدام علامات رقيب محددة وتطبيق سياسات جدار حماية قائم على المنطقة (ZBF) استنادا إلى علامات رقيب تم إستالمها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

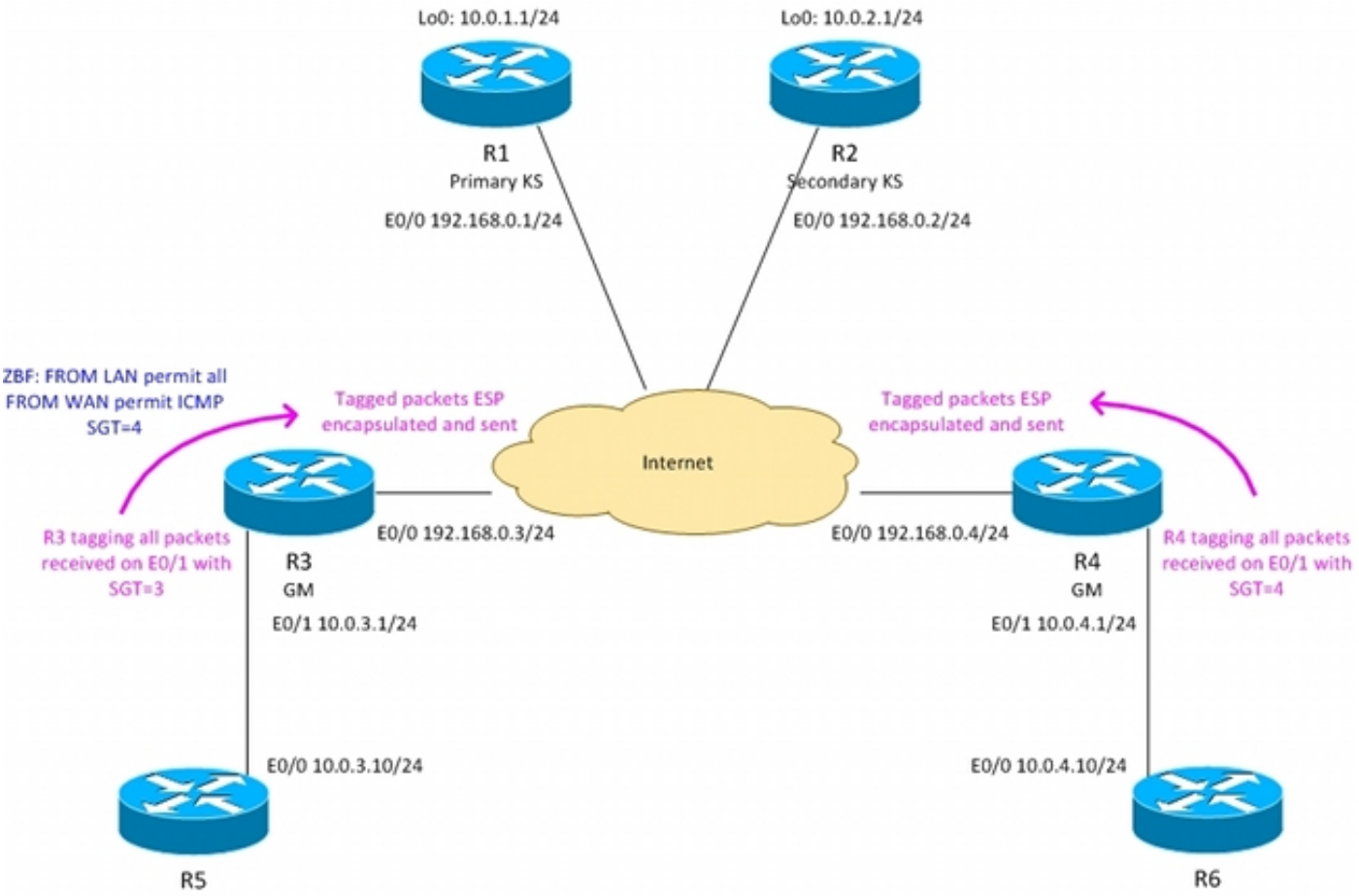
- معرفة أساسية بتكوين واجهة سطر الأوامر (CLI) IOS وتكوين GETVPN
- معرفة أساسية بخدمات TrustSec.
- معرفة أساسية بجدار الحماية المستند إلى مناطق

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- الموجه 2921 من Cisco مع البرنامج 15.3(2)T والإصدارات الأحدث

طوبولوجيا



R3 - موجه الحدود في الفرع 1، عضو مجموعة GETVPN

R4 - موجه حدود في الفرع 2، عضو مجموعة GETVPN

R1،R2 - خوادم GETVPN الأساسية في الموقع المركزي

تشغيل OSPF على جميع الموجهات

تم دفع قائمة التحكم في الوصول من KS التي تفرض التشفير لحركة المرور بين 10.0.0.0/16 <-> 10.0.0.0/16

يقوم الموجه R3 بوضع علامات على جميع حركات المرور المرسلة من الفرع 1 باستخدام علامة الرقيب = 3

يقوم الموجه R4 بوضع علامات على جميع حركات المرور المرسلة من الفرع 2 باستخدام علامة الرقيب = 4

يقوم R3 بإزالة علامات SGT عند إرسال حركة مرور البيانات باتجاه الشبكة المحلية (مع افتراض أن R5 لا يدعم وضع العلامات داخل السطر)

يقوم R4 بإزالة علامات SGT عند إرسال حركة مرور البيانات باتجاه الشبكة المحلية (مع افتراض أن R6 لا يدعم وضع علامات في السطر)

لا يحتوي R4 على جدار حماية (قبول جميع الحزم)

تم تكوين R3 باستخدام ZBF بالسياسات التالية:

- قبول جميع حركات المرور من شبكة LAN إلى شبكة WAN

- قبول ICMP فقط الذي تم وضع علامة عليه بالرقيب=4 من شبكة الاتصال واسعة النطاق (WAN) تجاه الشبكة المحلية

التكوين

R1 (الخادم الرئيسي في الموقع المركزي)

للإسال السياسات التي تسمح بإرسال واستقبال الحزم المميزة يجب أن يكون الأمر "TAC CTS Sgt" موجود:

```
interface Loopback0
 ip address 10.0.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile prof1
 set transform-set TS
!
crypto gdoi group group1
 identity number 1
 server local
 rekey authentication mypubkey rsa GETKEY
 rekey transport unicast
 sa ipsec 1
  profile prof1
  match address ipv4 GET-IPV4
  replay counter window-size 64
   tag cts sgt
 address ipv4 192.168.0.1
 redundancy
  local priority 100
  peer address ipv4 192.168.0.2

router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.0.255 area 0

ip access-list extended GET-IPV4
 permit icmp 10.0.0.0 0.0.255.255 10.0.0.0 0.0.255.255
```

تكوين R2 مماثل جدا.

R3 (عضو المجموعة في الفرع 1)

تكوين GETvpn هو نفسه للسيناريو بدون علامات SGT. تم تكوين واجهة LAN باستخدام TRUSTsec اليدوي:

- "النهج الثابت للرقيب 3 موثوق" - يضع علامات على جميع الحزم المستلمة من

الشبكة المحلية (LAN) باستخدام الرقيب=3

- "ال مساعد نشر" - يزيل جميع عالمات الرقيب عند نقل الحزم باتجاه الشبكة المحلية (LAN)

```
crypto gdoi group group1
 identity number 1
 server address ipv4 192.168.0.1
 server address ipv4 192.168.0.2
!
!
crypto map cmap 10 gdoi
 set group group1

interface Ethernet0/0
 ip address 192.168.0.3 255.255.255.0
 crypto map cmap
!
interface Ethernet0/1
 ip address 10.0.3.1 255.255.255.0
cts manual
   no propagate sgt
   policy static sgt 3 trusted

router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
```

تكوين ZBF على R3:

سيتم قبول جميع الحزم من LAN. من شبكة الاتصال واسعة النطاق (WAN)، سيتم قبول فقط حزم ICMP التي تم وضع العالمة عليها بالرقيب=4:

```
class-map type inspect match-all TAG_4_ICMP
match security-group source tag 4
 match protocol icmp
!
policy-map type inspect FROM_LAN
 class class-default
 pass log
policy-map type inspect FROM_WAN
 class type inspect TAG_4_ICMP
 pass log
 class class-default
 drop log
!
zone security lan
zone security wan
zone-pair security WAN-LAN source wan destination lan
 service-policy type inspect FROM_WAN
zone-pair security LAN-WAN source lan destination wan
 service-policy type inspect FROM_LAN

interface Ethernet0/0
 zone-member security wan
!
interface Ethernet0/1
 zone-member security lan
```

R4 في تكوين Branch2 مماثل جدا باستثناء ZBF الذي لم يتم تكوينه هناك.

تكوين R5 و R6

يقوم R5 و R6 بمحاكاة شبكة LAN المحلية في كل الفرعين. مثال على تكوين R5:

```
interface Ethernet0/0
 ip address 10.0.3.10 255.255.255.0
router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
```

التحقق

تحقق من تكوين GETVPN

التحقق من دعم علامات الرقيب على عضو المجموعة في الفرع 1 (R3):

```
R3#show crypto gdoi feature cts-sgt
      Version    Feature Supported
       1.0.8           Yes
```

التحقق مما إذا كانت سياسات TEK التي تم دفعها إلى عضو المجموعة في الفرع 1 (R3) تستخدم الرقيب:

```
R3#show crypto gdoi
GROUP INFORMATION

<...some output ommited for clarity...>

TEK POLICY for the current KS-Policy ACEs Downloaded:
 Ethernet0/0:
   IPsec SA:
       spi: 0xD100D58E(3506492814)
       transform: esp-aes esp-sha256-hmac
       sa timing:remaining key lifetime (sec): expired
       Anti-Replay(Counter Based) : 64
        tag method : cts sgt
       alg key size: 16 (bytes)
       sig key size: 32 (bytes)
       encaps: ENCAPS_TUNNEL

   IPsec SA:
       spi: 0x52B3CA86(1387514502)
       transform: esp-aes esp-sha256-hmac
       sa timing:remaining key lifetime (sec): (1537)
       Anti-Replay(Counter Based) : 64
        tag method : cts sgt
       alg key size: 16 (bytes)
       sig key size: 32 (bytes)
       encaps: ENCAPS_TUNNEL
```

إرسال حركة مرور ICMP من R6 إلى R5:

```
R6#ping 10.0.3.10 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.0.3.10, timeout is 2 seconds:
```

```
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/6 ms
```

التحقق مما إذا كان R3 يقوم بإرفاق علامة الرقيب بالحزم المشفرة:

```
R3#show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: cmap, local addr 192.168.0.3

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.0.0.0/255.255.0.0/1/0)
  remote ident (addr/mask/prot/port): (10.0.0.0/255.255.0.0/1/0)
  Group: group1
  current_peer 0.0.0.0 port 848
    PERMIT, flags={}
   #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
   #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
   #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): 39, #pkts untagged (rcv): 39

<...some output ommited for clarity...>
```

التحقق من عدادات مستوى البيانات لـ GETVPN على عضو المجموعة في Branch2 (R3):

```
R3#show crypto gdoi gm dataplane counters

Data-plane statistics for group group1:
   #pkts encrypt            : 53       #pkts decrypt            : 53
   #pkts tagged (send)      : 53       #pkts untagged (rcv)     : 53
   #pkts no sa (send)       : 0        #pkts invalid sa (rcv)   : 0
   #pkts encaps fail (send) : 0        #pkts decap fail (rcv)   : 0
   #pkts invalid prot (rcv) : 0        #pkts verify fail (rcv)  : 0
   #pkts not tagged (send)  : 0        #pkts not untagged (rcv) : 0
   #pkts internal err (send): 0        #pkts internal err (rcv) : 0
```

حسب النظام الأساسي يمكن كشف المزيد من التفاصيل باستخدام تصحيح الأخطاء. على سبيل المثال في R3:

```
R3#debug cts platform l2-sgt rx
R3#debug cts platform l2-sgt tx
```

يجب أن تكون الحزم التي يتم استقبالها بواسطة R3 من الشبكة المحلية (LAN) ذات علامة SGT:

```
01:48:08: cts-l2sgt_rx:l2cts-policysgt:[in=Ethernet0/1 src=0100.5e00.0005 dst=aabb.cc00.6800]
Policy SGT Assign [pak=F1B00E00:flag=0x1:psgt=3]
```

كما سيتم تمييز الحزم المشفرة التي يتم إرسالها عبر النفق:

```
01:49:28: cts_ether_cmd_handle_post_encap_feature:pak[36BF868]:size=106 in=Ethernet0/1
out=Ethernet0/0 enctype=1 encsize=0 sgt_offset=18 [adj]:idb=Ethernet0/0 is_dot1q=0 linktype=7
```

```
mac_length=22 SGT=3
```

Test Sgt Aware ZBF

لن يقبل R3 إلا حزم ICMP التي تم وضع علامة عليها بالرقيب=4 القادمة من شبكة WAN. عند إرسال حزم ICMP من R6 إلى R5:

```
R6#ping 10.0.3.10 repeat 11
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.0.3.10, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/6 ms
```

يتلقى R3 حزمة ESP ذات علامات تمييز، ويفك تشفيرها. بعد ذلك سيقبل ZBF حركة المرور:

```
*Mar 17 12:45:28.039: %FW-6-PASS_PKT: (target:class)-(WAN-LAN:TAG_4_ICMP) Passing icmp pkt
10.0.4.10:0 => 10.0.3.10:0 with ip ident 57
```

كما ستقدم خريطة السياسة العدادات بأرقام الحزم التي تم قبولها:

```
R3#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 WAN-LAN
 Zone-pair: WAN-LAN

 Service-policy inspect : FROM_WAN

   Class-map: TAG_4_ICMP (match-all)
      Match: security-group source tag 4
      Match: protocol icmp
     Pass
        18 packets, 1440 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
       3 packets, 72 bytes

policy exists on zp LAN-WAN
 Zone-pair: LAN-WAN

 Service-policy inspect : FROM_LAN

   Class-map: class-default (match-any)
     Match: any
     Pass
       18 packets, 1440 bytes
```

عند محاولة إستخدام برنامج Telnet من R6 إلى R5 - سيتم إسقاط هذا البرنامج من قبل R3 لأنه غير مسموح ببرنامج Telnet:

```
*Mar 17 12:49:30.475: %FW-6-DROP_PKT: Dropping tcp session 10.0.4.10:37500 10.0.3.10:23 on zone-
pair WAN-LAN class class-default due to  DROP action found in policy-map with ip ident 36123
```

المراجع

- دليل تكوين محول Cisco TrustSec: فهم Cisco TrustSec
- تكوين خادم خارجي لتفويض مستخدم جهاز الأمان
- دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN، الإصدار 9.1
- دليل مستخدم محرك خدمات الهوية من Cisco، إصدار 1.2
- 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).