شبكة LAN من موقع إلى شبكة LAN IPSec بين vEdge و Cisco IOS®

المحتويات

المقدمة

يصف هذه المستند شبكة VPN من موقع إلى موقع IPSec مع تكوين مفاتيح مشتركة مسبقا في transport-vpn على vEdge بين جهاز Cisco IOS® باستخدام التوجيه الظاهري وإعادة التوجيه (VRF) الذي تم تكوينه. كما يمكن إستخدامها كمرجع لتكوين IPSec بين موجه vEdge وقناة المنفذ الظاهري (vPC) من Amazon (بوابة العملاء).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- IKEv1
- بروتوكولات IPSec

المكونات المستخدمة

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

- موجه vEdge مع برنامج 18.2 أو أحدث
- الموجه Cisco IOS®-XE

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

التكوين

موجه vEdge

```
vpn 0
 !
 interface ge0/1
  ip address 192.168.103.7/24
  !
  no shutdown
 !
 interface ipsec1
  ip address 10.0.0.2/30
  tunnel-source-interface ge0/1
  tunnel-destination      192.168.103.130
  ike
   version      1
   mode         main
   rekey        14400
   cipher-suite aes128-cbc-sha1
   group        2
   authentication-type
    pre-shared-key
     pre-shared-secret $8$qzBthmnUSTMs54lxyHYZXVcnyCwENxJGcxRQT09X6SI=
     local-id          192.168.103.7
     remote-id         192.168.103.130
    !
   !
  !
  ipsec
   rekey                   3600
   replay-window           512
   cipher-suite            aes256-cbc-sha1
   perfect-forward-secrecy group-2
  !
  no shutdown
 !
vpn 1
 ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1
```

IOS®-XE من Cisco

```
crypto keyring KR vrf vedge2_vrf
  pre-shared-key address 0.0.0.0 0.0.0.0 key test
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp profile IKE_PROFILE
   keyring KR
   self-identity address
   match identity address 0.0.0.0 vedge2_vrf
crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec profile IPSEC_PROFILE
 set transform-set TSET
 set pfs group2
 set isakmp-profile IKE_PROFILE
!
```

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.252
 description "*** IPSec tunnel ***"
 tunnel source 192.168.103.130
 tunnel mode ipsec ipv4
 tunnel destination 192.168.103.7
 tunnel vrf vedge2_vrf
 tunnel protection ipsec profile IPSEC_PROFILE isakmp-profile IKE_PROFILE
!
interface GigabitEthernet4
 description "*** vEdge2 ***"
 ip vrf forwarding vedge2_vrf
 ip address 192.168.103.130 255.255.255.0 secondary
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. تأكد من إمكانية الوصول إلى عنوان النظير البعيد:

```
csr1000v2#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
```

2. تحقق مما إذا تم إنشاء تبادل مفتاح الإنترنت (IKE) للمرحلة الأولى من IPSec على موجه Cisco IOS®-XE. يجب أن تكون الحالة "QM_IDLE":

```
csr1000v2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.103.130 192.168.103.7   QM_IDLE           1004 ACTIVE

IPv6 Crypto ISAKMP SA
```

3. تأكد من إنشاء المرحلة 2 من IPSec على موجه Cisco IOS®-XE وتأكد من زيادة عدادات "pkts encaps" و"kts decaps" على كلا النظيرين:

```
csr1000v2#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.103.130

   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 192.168.103.7 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
     local crypto endpt.: 192.168.103.130, remote crypto endpt.: 192.168.103.7
     plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet4
     current outbound spi: 0xFFB55(1047381)
     PFS (Y/N): Y, DH group: group2

     inbound esp sas:
      spi: 0x2658A80C(643344396)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2023, flow_id: CSR:23, sibling_flags FFFFFFFF80004048, crypto map: Tunnel1-
head-0
        sa timing: remaining key lifetime (k/sec): (4608000/1811)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xFFB55(1047381)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2024, flow_id: CSR:24, sibling_flags FFFFFFFF80004048, crypto map: Tunnel1-
head-0
        sa timing: remaining key lifetime (k/sec): (4608000/1811)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

4. أكد أمم إذا كانت المرحلة الأولى والجلسة الثانية من IPSec قد تم إنشاؤها على vEdge أيضا. يجب أن تكون الحالة "IKE_UP_IPSec_UP".

```
vedge4# show ipsec ike sessions
ipsec ike sessions 0 ipsec1
 version       1
 source-ip     192.168.103.7
 source-port   4500
 dest-ip       192.168.103.130
 dest-port     4500
 initiator-spi 8012038bc7cf1e09
 responder-spi 29db204a8784ff02
 cipher-suite  aes128-cbc-sha1
 dh-group      "2 (MODP-1024)"
 state         IKE_UP_IPSEC_UP
 uptime        0:01:55:30

vedge4# show ipsec ike outbound-connections SOURCE SOURCE DEST DEST CIPHER EXT IP PORT IP PORT
SPI SUITE KEY HASH TUNNEL MTU SEQ ----------------------------------------------------------------
--------------------------------------------------------------------------------------
192.168.103.7 4500 192.168.103.130 4500 643344396 aes256-cbc-sha1 ****ba9b 1418 no
```

5. تحقق إذا كانت عدادات tx-and rx- تزايدت في الكل الاتجاهين مع العدادات المطابقة التي تم توفيرها على موجه Cisco IOS®-XE.

```
vedge4# show tunnel statistics dest-ip 192.168.103.130
```

```
TCP
TUNNEL                                    SOURCE  DEST  SYSTEM  LOCAL  REMOTE  TUNNEL
MSS
PROTOCOL  SOURCE IP      DEST IP          PORT    PORT  IP      COLOR  COLOR   MTU     tx-pkts
tx-octets  rx-pkts  rx-octets  ADJUST
-------------------------------------------------------------------------------------------
-------------------------------------
ipsec     192.168.103.7  192.168.103.130  4500    4500  -       -      -       1418    10
1900       11       2038       1334
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

للحصول على دليل أستكشاف أخطاء IPSec وإصلاحها على Cisco IOS®/IOS®-XE، ارجع إلى ما يلي:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

معلومات ذات صلة

- مزيد من المعلومات حول Amazon VPC "بوابة العملاء": https://docs.aws.amazon.com/en_us/vpc/latest/adminguide/Introduction.html
- 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).