نفق VPN الخاص بالموقع الديناميكي إلى الموقع بين ASA ومثال تكوين موجه IOS

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق تبادل مفتاح الإنترنت من موقع إلى موقع الإصدار 2 (IKEv2) VPN بين جهاز الأمان القابل للتكيف (ASA) وموجه Cisco حيث يحتوي الموجه على عنوان IP ديناميكي ويمتلك ASA عنوان IP ثابت على الواجهات العامة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- Cisco IOS® الإصدار 15.1(1)T أو إصدار أحدث
- Cisco ASA، الإصدار 8.4(1) أو إصدار أحدث

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

معلومات أساسية

يناقش هذا المستند السيناريوهات التالية:

- السيناريو 1: يتم تكوين ASA باستخدام عنوان IP ثابت يستخدم مجموعة نفق مسماة ويتم تكوين الموجه باستخدام عنوان IP ديناميكي.

- السيناريو 2: يتم تكوين ASA باستخدام عنوان IP ديناميكي ويتم تكوين الموجه باستخدام عنوان IP ديناميكي.

- السيناريو 3: لا يناقش هذا السيناريو هنا. في هذا السيناريو، يتم تكوين ASA باستخدام عنوان IP ثابت ولكن يستخدم مجموعة نفق DefaultL2LGgroup. ويكون التكوين الخاص بهذا مماثلا لما يتم وصفه في الموقع الديناميكي إلى نفق IKEv2 VPN الخاص بالموقع بين مقالة مثال تكوين ASAs.

أكبر فرق تكوين بين السيناريوهين 1 و 3 هو معرف بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) المستخدم بواسطة الموجه عن بعد. عندما يتم إستخدام DefaultL2LGgroup على ASA الثابت، يجب أن يكون معرف ISAKMP الخاص بالنظير على الموجه هو عنوان ASA. ومع ذلك، إذا تم إستخدام مجموعة أنفاق مسماة، فيجب أن يكون معرف ISAKMP الخاص بالنظير على الموجه هو نفسه اسم مجموعة النفق الذي تم تكوينه على ASA. يتم تحقيق ذلك باستخدام هذا الأمر على الموجه:

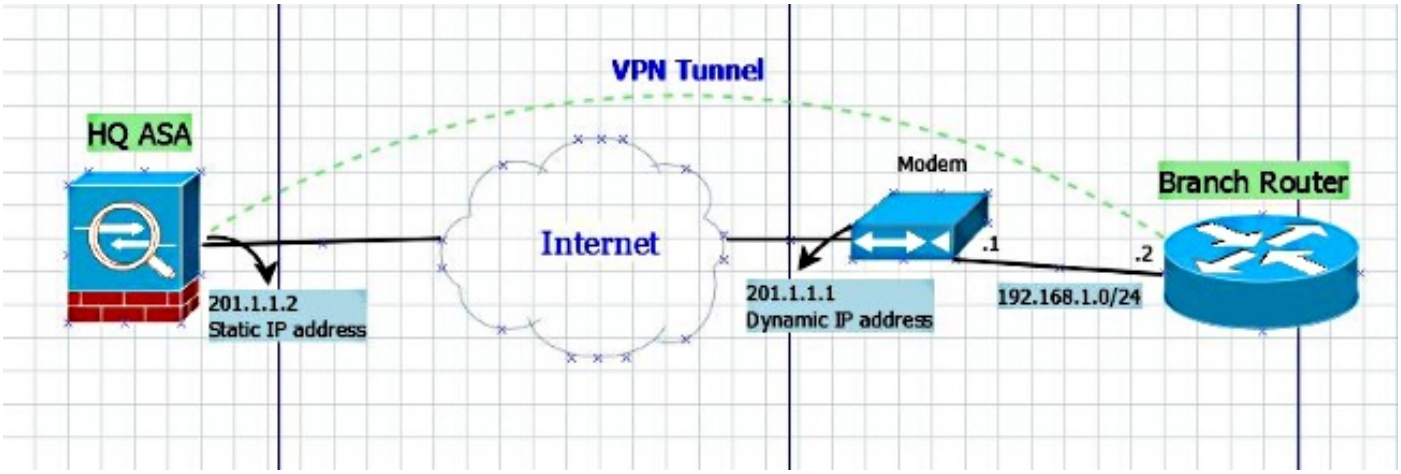
```
identity local key-id
```

تتمثل ميزة إستخدام مجموعات النفق المسماة على ASA الثابت في أنه عند إستخدام DefaultL2LGgroup، يجب أن يكون التكوين الموجود على موجهات/ASAs الديناميكية البعيدة، والذي يتضمن المفاتيح المشتركة مسبقا، متطابقا ولا يسمح بالكثير من الدقة مع إعداد السياسات.

التكوين

السيناريو 1

الرسم التخطيطي للشبكة



التكوين

يصف هذا القسم التكوين على ASA والموجه القائم على تكوين مجموعة النفق المسماة.

تشكيل ASA الثابت

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

تكوين الموجه الديناميكي

يتم تكوين الموجه الديناميكي بنفس الطريقة تقريبا التي تقوم بتكوينها عادة في الحالات التي يكون فيها الموجه موقعا ديناميكيا لنفق IKEv2 L2L مع إضافة أمر واحد كما هو موضح هنا:

```
ip access-list extended vpn
permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
encryption 3des
integrity sha1
group 2 5
!
crypto ikev2 policy L2L-Pol
proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
peer vpn
address 201.1.1.2
pre-shared-key local cisco321
pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
match identity remote address 201.1.1.2 255.255.255.255
identity local key-id S2S-IKEv2
authentication remote pre-share
authentication local pre-share
keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
!
crypto map vpn 10 ipsec-isakmp
set peer 201.1.1.2
set transform-set ESP-AES-SHA
set ikev2-profile L2L-Prof
match address vpn
!
interface GigabitEthernet0/0
ip address 192.168.1.2 255.255.255.0
duplex auto
speed auto
crypto map vpn
```

لذلك في كل نظير ديناميكي، يكون معرف المفتاح مختلف ويجب إنشاء مجموعة نفق مقابلة على ASA ساكن إستاتيكي بالاسم الصحيح، مما يزيد أيضا من دقة السياسات التي يتم تنفيذها على ASA.

السيناريو 2

ملاحظة: لا يكون هذا التكوين ممكنا إلا عندما يكون جانب واحد على الأقل هو الموجه. إذا كان كلا الطرفين ASA، فإن هذا الإعداد لا يعمل في هذا الوقت. في الإصدار 8.4، لا يمكن أن يستخدم ASA اسم المجال المؤهل بالكامل (FQDN) باستخدام أمر **set peer**، ولكن تم طلب تحسين CSCus37350 للإصدارات المستقبلية.

إذا كان عنوان IP الخاص ب ASA البعيد ديناميكيا كذلك، يحتوي على اسم مجال مؤهل بالكامل تم تعيينه لواجهة VPN الخاصة به، بدلا من تحديد عنوان IP الخاص ب ASA البعيد، فأنت تقوم الآن بتعريف FQDN الخاص ب ASA البعيد باستخدام هذا الأمر على الموجه:

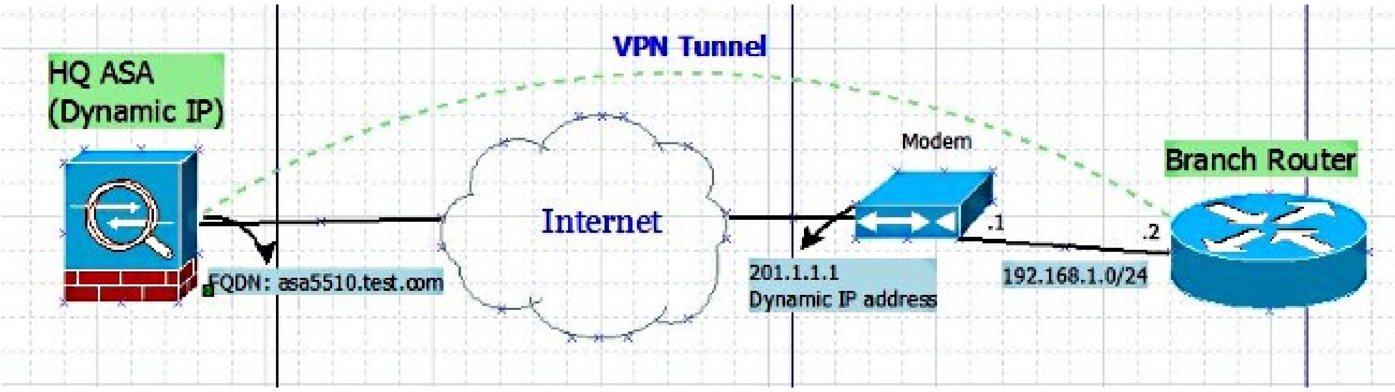
```
C1941(config)#do show run | sec crypto map

crypto map vpn 10 ipsec-isakmp
```

```
set peer <FQDN> dynamic
```

تلميح: تكون الكلمة الأساسية **الديناميكية** إختيارية. عند تحديد اسم المضيف لنظير IPsec بعيد عبر أمر **set** peer، يمكنك أيضا إصدار الكلمة الأساسية الديناميكية، والتي تؤجل تحليل خادم اسم المجال (DNS) لاسم المضيف حتى قبل إنشاء نفق IPsec مباشرة.

يقوم تأجيل الحل بتمكين برنامج Cisco IOS software من اكتشاف ما إذا تم تغيير عنوان IP الخاص بنظير IPsec البعيد أم لا. وبالتالي، يمكن للبرنامج الاتصال بالنظير على عنوان IP الجديد. إذا لم يتم إصدار الكلمة الأساسية الديناميكية، فسيتم حل اسم المضيف مباشرة بعد تحديدها. لذلك، لا يمكن لبرنامج Cisco IOS اكتشاف تغيير عنوان IP، وبالتالي، يحاول الاتصال بعنوان IP الذي قام بحله مسبقا.

الرسم التخطيطي للشبكة



التكوين

تكوين ASA الديناميكي

التشكيل على ال ASA ال نفسه بما أن السّاكن إستاتيكي ASA تشكيل مع فقط واحد إستثناء، أي أن عنوان ال ip على القارن طبيعي لم يعين بشكل ثابت.

تكوين الموجّه

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
  hostname asa5510.test.com
  pre-shared-key local cisco321
  pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel

crypto map vpn 10 ipsec-isakmp
```

```
set peer asa5510.test.com dynamic
set transform-set ESP-AES-SHA
set ikev2-profile L2L-Prof
match address vpn
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ASA الثابت

- فيما يلي نتيجة الأمر **show crypto IKEv2 sa det**:

```
:IKEv2 SAs

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                Remote     Status         Role
READY    RESPONDER      201.1.1.1/4500        201.1.1.2/4500        120434199
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
                                    Life/Active Time: 86400/915 sec
                                                     Session-id: 23
                               Status Description: Negotiation done
          Local spi: 97272A4B4DED4A5C       Remote spi: 67E01CB8E8619AF1
                                                Local id: 201.1.1.2
                                               Remote id: S2S-IKEv2
                 Local req mess id: 43          Remote req mess id: 2
                Local next mess id: 43         Remote next mess id: 2
                  Local req queued: 43           Remote req queued: 2
                      Local window: 1               Remote window: 5
                             DPD configured for 10 seconds, retry 2
                                         NAT-T is detected  outside
                 Child sa: local selector  201.1.1.2/0 - 201.1.1.2/65535
                remote selector 10.10.10.1/0 - 10.10.10.1/65535
                            ESP spi in/out: 0x853c02/0x41aa84f4
                                        AH spi in/out: 0x0/0x0
                                           CPI in/out: 0x0/0x0
                  Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
                 ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

- فيما يلي نتيجة الأمر **show crypto ipSec**:

```
interface: outside
Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2

(local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0
(remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0
current_peer: 201.1.1.1


pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4#
pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0#
```

```
    pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                        TFC rcvd: 0, #TFC sent: 0#
                Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0#
                                    send errors: 0, #recv errors: 0#

local crypto endpt.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
                    path mtu 1500, ipsec overhead 82(52), media mtu 1500
                        PMTU time remaining (sec): 0, DF policy: copy-df
                ICMP error validation: disabled, TFC packets: disabled
                                    current outbound spi: 41AA84F4
                                    current inbound spi : 00853C02

                                                    :inbound esp sas
                                            (spi: 0x00853C02 (8731650
                        transform: esp-aes esp-sha-hmac no compression
            { ,in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2
                        slot: 0, conn_id: 94208, crypto-map: dmap
(sa timing: remaining key lifetime (kB/sec): (4101119/27843
                                                IV size: 16 bytes
                                    replay detection support: Y
                                            :Anti replay bitmap
                                         0x00000000 0x0000001F
                                                   :outbound esp sas
                                      (spi: 0x41AA84F4 (1101694196
                        transform: esp-aes esp-sha-hmac no compression
            { ,in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2
                        slot: 0, conn_id: 94208, crypto-map: dmap
(sa timing: remaining key lifetime (kB/sec): (4055039/27843
                                                IV size: 16 bytes
                                    replay detection support: Y
                                            :Anti replay bitmap
                                         0x00000000 0x00000001
```

موجه ديناميكي

- وفيما يلي نتيجة الأمر **show crypto IKEv2 sa detail**:

```
                                                IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
 none/none            READY        201.1.1.2/4500      192.168.1.2/4500         1
        Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
                                    Life/Active Time: 86400/1013 sec
                                         CE id: 1023, Session-id: 23
                                Status Description: Negotiation done
            Local spi: 67E01CB8E8619AF1       Remote spi: 97272A4B4DED4A5C
                                                  Local id: S2S-IKEv2
                                                  Remote id: 201.1.1.2
                  Local req msg id:  2              Remote req msg id:  48
                  Local next msg id: 2              Remote next msg id: 48
                  Local req queued:  2              Remote req queued:  48
                   Local window:      5               Remote window:      1
                                DPD configured for 0 seconds, retry 0
                                        .Fragmentation not configured
                               .Extended Authentication not configured
                                            NAT-T is detected inside
                                Cisco Trust Security SGT is disabled
                                                Initiator of SA : Yes

                                                IPv6 Crypto IKEv2  SA
```

- فيما يلي نتيجة الأمر **show crypto ipSec**:

```
                                                interface: GigabitEthernet0/0
                                    Crypto map tag: vpn, local addr 192.168.1.2

                                                          (protected vrf: (none
                                 (local  ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0
                                  (remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0
                                                       current_peer 201.1.1.2 port 4500
                                                       {,PERMIT, flags={origin_is_acl
                                          pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6#
                                          pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6#
                                                  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.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
                        plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
                                                  (current outbound spi: 0x853C02(8731650
                                                    PFS (Y/N): N, DH group: none

                                                                       :inbound esp sas
                                                                  (spi: 0x41AA84F4(1101694196
                                                        , transform: esp-aes esp-sha-hmac
                                                    { ,in use settings ={Tunnel UDP-Encaps
conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
                                 (sa timing: remaining key lifetime (k/sec): (4263591/2510
                                                                  IV size: 16 bytes
                                                       replay detection support: Y
                                                            (Status: ACTIVE(ACTIVE

                                                                       :inbound ah sas

                                                                       :inbound pcp sas

                                                                      :outbound esp sas
                                                                 (spi: 0x853C02(8731650
                                                        , transform: esp-aes esp-sha-hmac
                                                    { ,in use settings ={Tunnel UDP-Encaps
conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
                                 (sa timing: remaining key lifetime (k/sec): (4263591/2510
                                                                  IV size: 16 bytes
                                                       replay detection support: Y
                                                            (Status: ACTIVE(ACTIVE

                                                                       :outbound ah sas

                                                                      :outbound pcp sas
```

الموجه الديناميكي (مع ASA الديناميكي البعيد)

- وفيما يلي نتيجة الأمر **show crypto IKEv2 sa detail**:

```
C1941#show cry ikev2 sa detailed
IPv4 Crypto IKEv2  SA
```

```
Tunnel-id Local                 Remote                fvrf/ivrf              Status
 none/none            READY        201.1.1.2/4500      192.168.1.2/4500         1
        Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
                                           Life/Active Time: 86400/1516 sec
                                                CE id: 1034, Session-id: 24
                                      Status Description: Negotiation done
            Local spi: 98322AED6163EE83       Remote spi: 092A1E5620F6AA9C
                                                     Local id: S2S-IKEv2
                                                    Remote id: asa5510.test.com
                  Local req msg id:  2              Remote req msg id:  73
                  Local next msg id: 2              Remote next msg id: 73
                  Local req queued:  2              Remote req queued:  73
                   Local window:      5               Remote window:      1
                                      DPD configured for 0 seconds, retry 0
                                              .Fragmentation not configured
                                    .Extended Authentication not configured
                                                  NAT-T is detected inside
                                    Cisco Trust Security SGT is disabled
                                                  Initiator of SA : Yes

                                                      IPv6 Crypto IKEv2  SA
```

ملاحظة: المعرف البعيد والمحلي في هذا الإخراج هو **مجموعة النفق المسماة** التي قمت بتعريفها على ASA للتحقق مما إذا قمت بالسقوط على مجموعة النفق اليمنى. كما يمكن التحقق من هذا الإجراء إذا قمت بتصحيح أخطاء IKEv2 على أي من الطرفين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

على موجه Cisco IOS، أستخدم:

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

على ASA، أستخدم:

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```

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).