مثال على تكوين نفق Dynamic to Dynamic IPsec Tunnel

المحتويات

المقدمة

يصف هذا المستند كيفية إنشاء نفق IPsec للشبكة المحلية إلى الشبكة المحلية بين موجّهات Cisco عندما يكون للطرفين عناوين IP ديناميكية ولكن يتم تكوين نظام اسم المجال الديناميكي (DDNS).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة VPN من موقع إلى موقع باستخدام نفق IPSec وتضمين التوجيه العام (GRE)
- واجهة النفق الظاهري (VTI) ل IPsec
- دعم DNS الديناميكي لبرنامج Cisco IOS

تلميح: راجع قسم تكوين شبكة VPN من مقالة تكوين البرنامج من السلسلة Cisco 3900 Series و 2900

Series و 1900 Series Software وتكوين واجهة نفق ظاهري باستخدام أمان IP للحصول على مزيد من المعلومات.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى موجه الخدمات المدمجة الطراز 2911 من Cisco الذي يشغل الإصدار M6a(4)15.2.

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.

معلومات أساسية

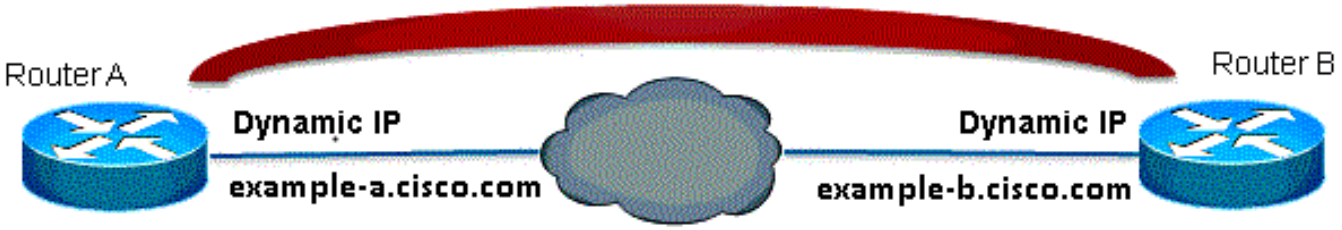
عندما يلزم إنشاء نفق من شبكة LAN إلى شبكة LAN، يجب أن يكون عنوان IP لكل من نظاري IPSec معروفا. إذا لم يكن أحد عناوين IP معروفا لأنه ديناميكي، مثل أحد العناوين التي تم الحصول عليها عبر DHCP، فحينئذ يكون البديل هو إستخدام خريطة تشفير ديناميكية. وهذا يعمل، ولكن يمكن فقط إظهار النفق بواسطة النظير الذي لديه عنوان IP الديناميكي نظرا لأن النظير الآخر لا يعرف مكان العثور على النظير الخاص به.

أحلت ل كثير معلومة حول حركي إلى ساكن إستاتيكي، بشكل مسحاج تخديد إلى مسحاج تخديد حركي إلى ساكن إستاتيكي IPSec مع NAT.

التكوين

دقة في الوقت الفعلي لنظير نفق IPsec

قدم Cisco IOS® ميزة جديدة في الإصدار T(4)12.3 تتيح تحديد اسم المجال المؤهل بالكامل (FQDN) لنظير IPSec. عندما تكون هناك حركة مرور تطابق قائمة الوصول إلى التشفير، يقوم Cisco IOS بعد ذلك بحل FQDN ويحصل على عنوان IP الخاص بالنظير. ثم يحاول ان يجلب النفق.



ملاحظة: هناك تقييد لهذه الميزة: سيعمل تحليل أسماء DNS لنظراء IPsec عن بعد فقط إذا تم إستخدامهم كبادئ. ستقوم الحزمة الأولى التي سيتم تشفيرها بتشغيل بحث DNS؛ بعد اكتمال البحث عن DNS، ستقوم الحزم التالية بتشغيل تبادل مفتاح الإنترنت (IKE). لن يعمل الحل في الوقت الفعلي على الاستجابة.

من أجل معالجة التحديد والقدرة على بدء تشغيل النفق من كل موقع، سيكون لديك إدخال خريطة تشفير ديناميكي على كلا الموجهين حتى يمكنك تعيين إتصالات IKE الواردة إلى التشفير الديناميكي. هذا ضروري لأن الإدخال الثابت مع ميزة حل الوقت الفعلي لا يعمل عندما يعمل كمستجيب.

الموجه A

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-b.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

الموجه B

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
```

```
!
crypto dynamic-map dyn 10
  set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
                match address 140
set peer example-a.cisco.com dynamic
                set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
          ip address dhcp
       crypto map secure_b
```

ملاحظة: نظرا لأنك لا تعرف عنوان IP الذي سيستخدمه FQDN، فأنت بحاجة إلى إستخدام مفتاح مشترك مسبقا لبطاقة البدل: 0.0.0.0.0.0

تحديث وجهة النفق باستخدام مدير الحدث المضمن (EEM)

أنت يستطيع أيضا VTI in order to أنجزت هذا. يتم عرض التكوين الأساسي هنا:

الموجه A

```
crypto isakmp policy 10
          encryption aes
authentication pre-share
                group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
     set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.0
       tunnel source fastethernet0/0
tunnel destination example-b.cisco.com
          tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

الموجه B

```
crypto isakmp policy 10
          encryption aes
authentication pre-share
                group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
```

```
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-a.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

بمجرد أن يكون التكوين السابق في موضعه مع FQDN كوجهة النفق، يعرض الأمر **show run** عنوان IP بدلا من الاسم. ده علشان القرار بيحصل مرة واحدة بس:

```
RouterA(config)#do show run int tunn 1
...Building configuration

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.201.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end

RouterB(config)#do show run int tunn 1
...Building configuration

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.200.225
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

workaround ل هذا أن يشكل برمجية in order to حللت النفق غاية كل دقيقة:

الموجه A

```
event manager applet change-tunnel-dest
"* * * * *" event timer cron name TAC cron-entry
"action 1.0 cli command "enable
"action 1.1 cli command "configure terminal
"action 1.2 cli command "interface tunnel1
"action 1.3 cli command "tunnel destination example-b.cisco.com
```

الموجه B

```
event manager applet change-tunnel-dest
"* * * * *" event timer cron name TAC cron-entry
"action 1.0 cli command "enable
"action 1.1 cli command "configure terminal
"action 1.2 cli command "interface tunnel1
"action 1.3 cli command "tunnel destination example-a.cisco.com
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

```
RouterA(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.200.225 YES NVRAM up up
FastEthernet0/1 192.168.10.1 YES NVRAM up up
Tunnel1 172.16.12.1 YES manual up up


RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.201.1 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up

RouterA(config)#do show cry isa sa
dst src state conn-id slot status
QM_IDLE 2 0 ACTIVE 209.165.201.1 209.165.200.225

RouterB(config)#do show cry isa sa
dst src state conn-id slot status
QM_IDLE 1002 0 ACTIVE 209.165.201.1 209.165.200.225

RouterA(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.200.225

(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 209.165.201.1 port 500
{,PERMIT, flags={origin_is_acl
pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10#
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.: 209.165.200.225, remote crypto endpt.: 209.165.201.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
(current outbound spi: 0x8F1592D2(2400555730

:inbound esp sas
(spi: 0xF7B373C0(4155732928
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
conn id: 2002, flow_id: AIM-VPN/BPII-PLUS:2, crypto map: Tunnel1-head-0
(sa timing: remaining key lifetime (k/sec): (4501866/3033
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

:inbound ah sas

:inbound pcp sas
```

```
                                                                :outbound esp sas
                                                        (spi: 0x8F1592D2(2400555730
                                                , transform: esp-3des esp-sha-hmac
                                                        { ,in use settings ={Tunnel
            conn id: 2001, flow_id: AIM-VPN/BPII-PLUS:1, crypto map: Tunnel1-head-0
                                (sa timing: remaining key lifetime (k/sec): (4501866/3032
                                                                IV size: 8 bytes
                                                        replay detection support: Y
                                                                  Status: ACTIVE

                                                                :outbound ah sas

                                                               :outbound pcp sas




                                                    RouterB(config)#do show cry ipsec sa

                                                              interface: Tunnel1
                                        Crypto map tag: Tunnel1-head-0, local addr 209.165.201.1

                                                           (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 209.165.200.225 port 500
                                                          {,PERMIT, flags={origin_is_acl
                                          pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10#
                                          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.: 209.165.201.1, remote crypto endpt.: 209.165.200.225
                                               path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
                                                    (current outbound spi: 0xF7B373C0(4155732928
                                                       PFS (Y/N): N, DH group: none

                                                                :inbound esp sas
                                                        (spi: 0x8F1592D2(2400555730
                                                , transform: esp-3des esp-sha-hmac
                                                        { ,in use settings ={Tunnel
        conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: Tunnel1-head-0
                                (sa timing: remaining key lifetime (k/sec): (4424128/3016
                                                                IV size: 8 bytes
                                                        replay detection support: Y
                                                                  Status: ACTIVE

                                                                 :inbound ah sas

                                                                :inbound pcp sas

                                                                :outbound esp sas
                                                        (spi: 0xF7B373C0(4155732928
                                                , transform: esp-3des esp-sha-hmac
                                                        { ,in use settings ={Tunnel
        conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: Tunnel1-head-0
                                (sa timing: remaining key lifetime (k/sec): (4424128/3016
                                                                IV size: 8 bytes
                                                        replay detection support: Y
                                                                  Status: ACTIVE

                                                                :outbound ah sas
```

```
:outbound pcp sas
```

بعد تغيير سجل DNS ل b.cisco.com على خادم DNS من 209.165.201.1 إلى 209.165.202.129، سيتسبب IM في تحقيق الموجه A وسيعاد إنشاء النفق باستخدام عنوان IP الجديد الصحيح.

```
RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.202.129 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up
```

```
RouterA(config-if)#do show run int tunn1
...Building configuration

Current configuration : 192 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.252
tunnel source fastethernet0/0
tunnel destination 209.165.202.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

```
Router1841A#show cry isa sa
dst src state conn-id slot status
QM_IDLE 3 0 ACTIVE 209.165.202.129 209.165.200.225
```

استكشاف الأخطاء وإصلاحها

يمكنك الرجوع إلى تصحيح أخطاء وضع IPSec و IKE - أستكشاف أخطاء وضع IKEv1 الرئيسي وإصلاحها فيما يتعلق باستكشاف أخطاء IKE/IPsec المشتركة وإصلاحها.

معلومات ذات صلة

- دقة في الوقت الفعلي لنظير نفق IPsec
- 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).