موقع ديناميكي إلى موقع نفق IKEv2 VPN بين إثنان ASAs تشكيل مثال

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق تبادل مفتاح الإنترنت من موقع إلى موقع الإصدار 2 (IKEv2) VPN بين جهازي الأمان القابل للتكيف (ASAs) حيث يحتوي أحد ASA على عنوان IP ديناميكي في حين يحتوي الآخر على عنوان IP ثابت.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- ASA الإصدار 5505
- ASA الإصدار 9.1(5)

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

هناك طريقتان لإعداد هذا التكوين:

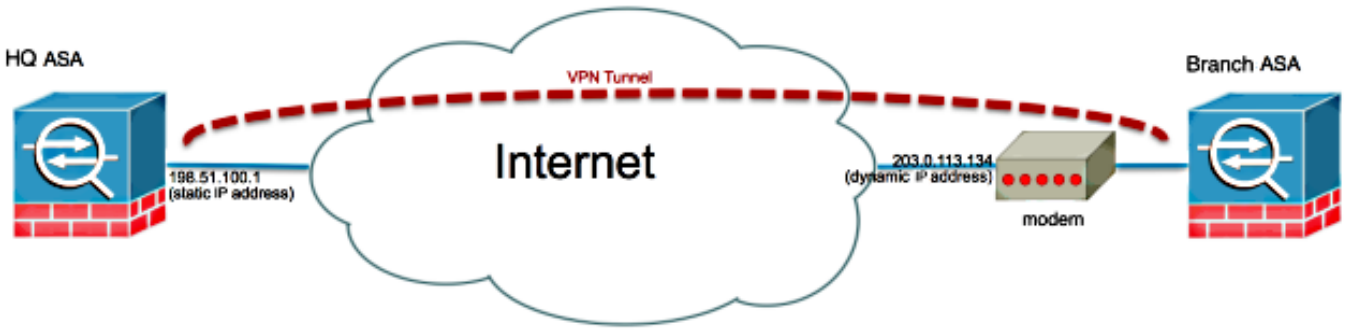
- باستخدام مجموعة النفق DefaultL2LGgroup
- مع مجموعة أنفاق مسماة

أكبر فرق تكوين بين السيناريوهين هو معرف بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) المستخدم من قبل ASA البعيد. عندما يتم إستخدام DefaultL2LGgroup على ASA الثابت، يجب أن يكون معرف ISAKMP الخاص بالنظير هو العنوان. ومع ذلك، إذا تم إستخدام مجموعة نفق مسماة، فيجب أن يكون معرف ISAKMP الخاص بالنظير هو نفس اسم مجموعة النفق باستخدام هذا الأمر:

```
crypto isakmp identity key-id
```

تتمثل ميزة إستخدام مجموعات النفق المسماة على ASA الثابت في أنه عند إستخدام DefaultL2LGgroup، يجب أن يكون التكوين على وحدات ASA الديناميكية البعيدة، والتي تتضمن المفاتيح المشتركة مسبقا، متطابقا ولا يسمح بالكثير من الدقة مع إعداد السياسات.

الرسم التخطيطي للشبكة



التكوين

يصف هذا القسم التكوين على كل ASA وفقا للحل الذي قررت إستخدامه.

الحل 1 - إستخدام DefaultL2LGgroup

هذه هي الطريقة الأبسط لتكوين نفق LAN إلى LAN (L2L) بين نقطتي ASA عندما يحصل أحد ASA على عنوانه بشكل ديناميكي. مجموعة DefaultL2L هي مجموعة نفق تم تكوينها مسبقا على ASA وجميع الاتصالات التي لا تطابق بشكل صريح أي مجموعة نفق معينة تقع على هذا الاتصال. بما أن ASA الديناميكي لا يحتوي على عنوان IP ثابت محدد مسبقا، فهذا يعني أنه لا يمكن للمسؤول تكوين Stats ASA للسماح بالاتصال على مجموعة نفق معينة. في هذه الحالة، يمكن إستخدام مجموعة DefaultL2L للسماح بالاتصالات الديناميكية.

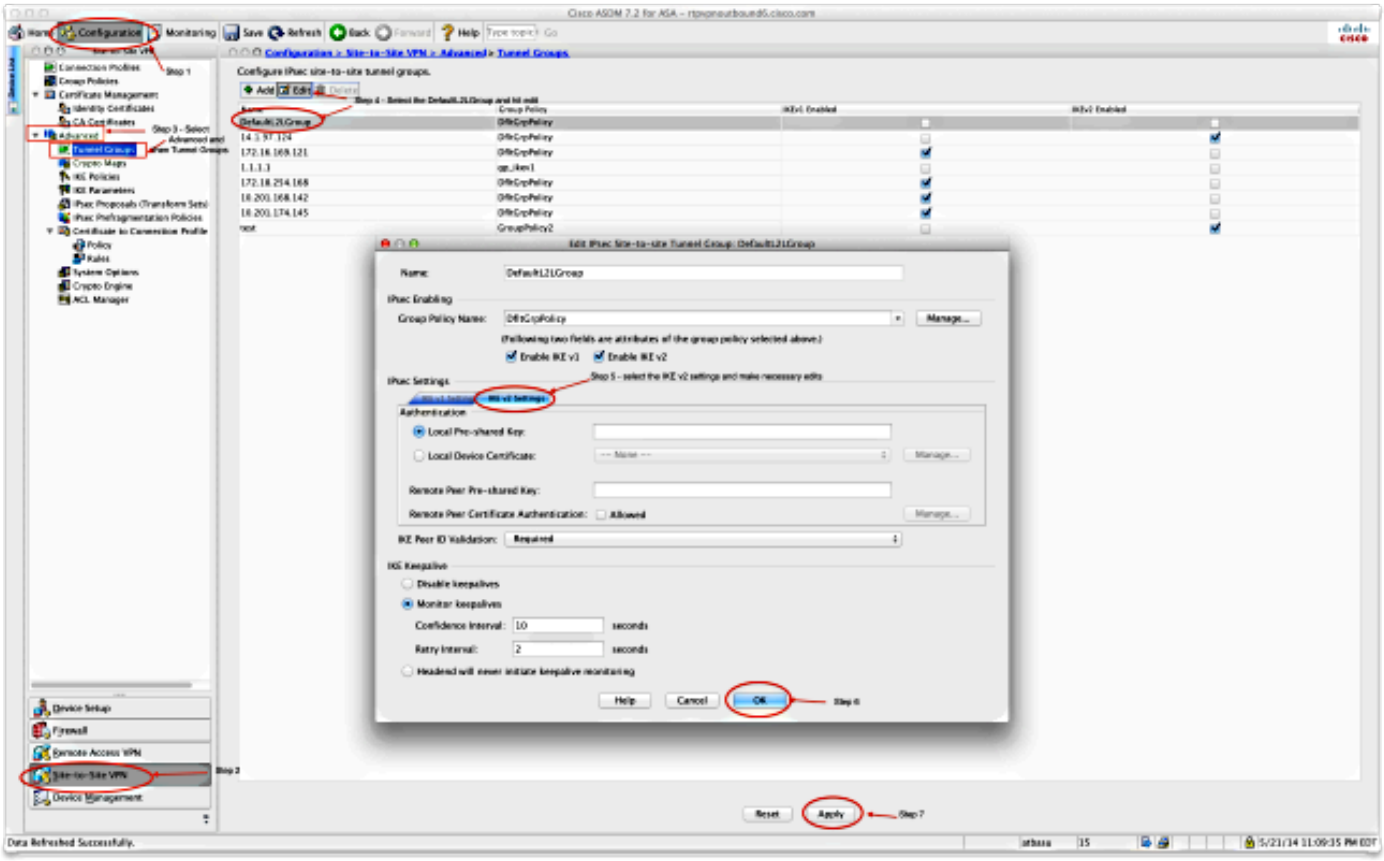
تلميح: باستخدام هذه الطريقة، يتمثل الجانب السلبي في أن جميع النظراء سيكون لديهم نفس المفتاح المشترك مسبقا نظرا لأنه يمكن تحديد مفتاح مشترك مسبقا واحد فقط لكل مجموعة نفق وسيتصل جميع النظراء بنفس مجموعة النفق DefaultL2LGgroup.

تشكيل ASA الثابت

```
interface Ethernet0/0
nameif inside
security-level 100
IP address 172.30.2.6 255.255.255.0
!
interface Ethernet0/3
nameif Outside
security-level 0
IP address 207.30.43.15 255.255.255.128
!
boot system disk0:/asa915-k8.bin
crypto ipsec IKEv2 ipsec-proposal Site2Site
protocol esp encryption aes-256
protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
protocol esp encryption 3des
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 10 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set
-ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES
256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map Outside_map interface Outside
crypto IKEv2 policy 2
encryption aes-256
integrity sha512
group 24
prf sha512
```

```
 lifetime seconds 86400
  crypto IKEv2 policy 3
    encryption aes-256
integrity sha group 5 2
                 prf sha
 lifetime seconds 86400
  crypto IKEv2 policy 10
     encryption aes-192
          integrity sha
              group 5 2
                prf sha
 lifetime seconds 86400
  crypto IKEv2 policy 20
         encryption aes
          integrity sha
              group 5 2
                prf sha
 lifetime seconds 86400
  crypto IKEv2 policy 30
        encryption 3des
          integrity sha
              group 5 2
                prf sha
 lifetime seconds 86400
  crypto IKEv2 policy 40
         encryption des
          integrity sha
              group 5 2
                prf sha
 lifetime seconds 86400
crypto IKEv2 enable inside client-services port 443
crypto IKEv2 enable Outside client-services port 443
                group-policy Site2Site internal
            group-policy Site2Site attributes
                      vpn-idle-timeout none
                   vpn-session-timeout none
                           vpn-filter none
                 vpn-tunnel-protocol IKEv2
      tunnel-group DefaultL2LGroup general-attributes
                   default-group-policy Site2Site
     tunnel-group DefaultL2LGroup ipsec-attributes
 ***** IKEv2 remote-authentication pre-shared-key
 ***** IKEv2 local-authentication pre-shared-key
```

في مدير أجهزة الأمان المعدلة (ASDM)، يمكنك تكوين DefaultL2LGgroup كما هو موضح هنا:



ASA الديناميكي

```
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
IP address 172.16.1.1 255.255.255.224
!
interface Vlan2
nameif outside
security-level 0
IP address dhcp setroute
!
ftp mode passive
object network NETWORK_OBJ_172.16.1.0_24
subnet 172.16.1.0 255.255.255.0
```

```
object-group network DM_INLINE_NETWORK_1
 network-object object 10.0.0.0
 network-object object 172.0.0.0
access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
 object-group DM_INLINE_NETWORK_1
_nat (inside,outside) source static NETWORK_OBJ_172.16.1.0_24 NETWORK_OBJ
 destination static DM_INLINE_NETWORK_1 DM_INLINE_NETWORK_1 24_172.16.1.0
nat (inside,outside) source dynamic any interface
crypto ipsec IKEv2 ipsec-proposal Site2Site
 protocol esp encryption aes-256
 protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs group5
crypto map outside_map 1 set peer 198.51.100.1
crypto map outside_map 1 set ikev1 phase1-mode aggressive group5
crypto map outside_map 1 set IKEv2 ipsec-proposal Site2Site
crypto map outside_map interface outside
crypto IKEv2 policy 2
 encryption aes-256
 integrity sha512
 group 24
 prf sha512
lifetime seconds 86400
crypto IKEv2 policy 3
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
lifetime seconds 86400
crypto IKEv2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
lifetime seconds 86400
crypto IKEv2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
lifetime seconds 86400
crypto IKEv2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
lifetime seconds 86400
crypto IKEv2 policy 40
```

```
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 enable outside
management-access inside
group-policy GroupPolicy_198.51.100.1 internal
group-policy GroupPolicy_198.51.100.1 attributes
vpn-tunnel-protocol IKEv2
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 general-attributes
default-group-policy GroupPolicy_198.51.100.1
tunnel-group 198.51.100.1 ipsec-attributes
***** ikev1 pre-shared-key
***** IKEv2 remote-authentication pre-shared-key
***** IKEv2 local-authentication pre-shared-key
```

في ASDM، يمكنك إستخدام المعالج القياسي لإعداد ملف تعريف التوصيل المناسب أو يمكنك ببساطة إضافة توصيل جديد واتباع الإجراء القياسي.

الحل 2 - إنشاء مجموعة نفق معرفة من قبل المستخدم

تتطلب هذه الطريقة تكوين أكثر بقليل، ولكنها تسمح بمزيد من القابلية للتعديل. يمكن أن يكون لكل نظير سياسة منفصلة ومفتاح مشترك مسبقا. ومع ذلك، من المهم هنا تغيير معرف ISAKMP على النظير الديناميكي حتى يستخدم اسما بدلا من عنوان IP. وهذا يسمح ل ASA الثابت بمطابقة طلب تهيئة ISAKMP الوارد إلى مجموعة النفق الأيمن واستخدام السياسات الصحيحة.

تشكيل ASA الثابت

```
interface Ethernet0/0
nameif inside
security-level 100
IP address 172.16.0.1 255.255.255.0
!
interface Ethernet0/3
nameif Outside
security-level 0
IP address 198.51.100.1 255.255.255.128
!
boot system disk0:/asa915-k8.bin
object-group network DM_INLINE_NETWORK_1
network-object object 10.0.0.0
network-object object 172.0.0.0

_access-list Outside_cryptomap_1 extended permit IP object-group DM_INLINE_NETWORK
255.255.255.0 1 172.16.1.0

crypto ipsec IKEv2 ipsec-proposal Site2Site
protocol esp encryption aes-256
protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
```

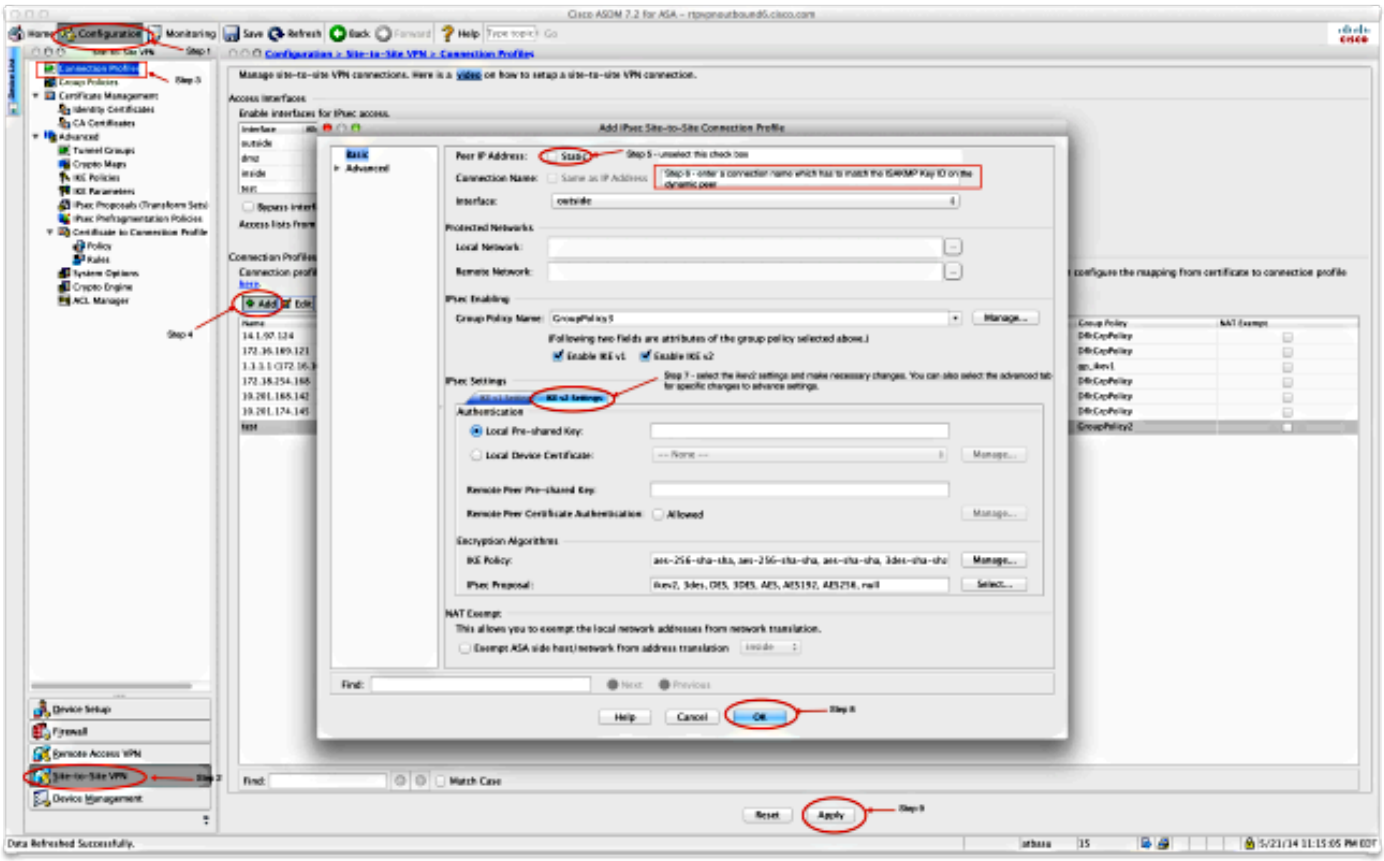
```
                                                    protocol esp encryption aes
                                                protocol esp integrity sha-1 md5
                                            crypto ipsec IKEv2 ipsec-proposal 3DES
                                                    protocol esp encryption 3des
                                                protocol esp integrity sha-1 md5
                                             crypto ipsec IKEv2 ipsec-proposal DES
                                                    protocol esp encryption des
                                                protocol esp integrity sha-1 md5
                                                    crypto engine large-mod-accel
                                    crypto ipsec security-association pmtu-aging infinite
                  crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-
                       SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
                 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set IKEv2 ipsec-proposal
                                                    AES256 AES192 AES 3DES DES
                    crypto dynamic-map DynamicSite2Site1 4 match address Outside_cryptomap_1
                  crypto dynamic-map DynamicSite2Site1 4 set IKEv2 ipsec-proposal Site2Site
                        crypto map Outside_map 65534 ipsec-isakmp dynamic DynamicSite2Site1
                 crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
                                                crypto map Outside_map interface Outside

                                                      crypto IKEv2 policy 2
                                                        encryption aes-256
                                                          integrity sha512
                                                                  group 24
                                                                prf sha512
                                                    lifetime seconds 86400
                                                      crypto IKEv2 policy 3
                                                        encryption aes-256
                                                             integrity sha
                                                                 group 5 2
                                                                   prf sha
                                                    lifetime seconds 86400
                                                     crypto IKEv2 policy 10
                                                        encryption aes-192
                                                             integrity sha
                                                                 group 5 2
                                                                   prf sha
                                                    lifetime seconds 86400
                                                     crypto IKEv2 policy 20
                                                            encryption aes
                                                             integrity sha
                                                                 group 5 2
                                                                   prf sha
                                                    lifetime seconds 86400
                                                     crypto IKEv2 policy 30
                                                           encryption 3des
                                                             integrity sha
                                                                 group 5 2
                                                                   prf sha
                                                    lifetime seconds 86400
                                                     crypto IKEv2 policy 40
                                                            encryption des
                                                             integrity sha
                                                                 group 5 2
                                                                   prf sha
                                                    lifetime seconds 86400
                                    crypto IKEv2 enable Outside client-services port 443
                                                        management-access inside

                                                  group-policy GroupPolicy4 internal
                                                group-policy GroupPolicy4 attributes
                                                        vpn-tunnel-protocol IKEv2
```

```
tunnel-group DynamicSite2Site1 type ipsec-l2l
tunnel-group DynamicSite2Site1 general-attributes
default-group-policy GroupPolicy4
tunnel-group DynamicSite2Site1 ipsec-attributes
***** IKEv2 remote-authentication pre-shared-key
***** IKEv2 local-authentication pre-shared-key
```

في ASDM، يكون اسم ملف تعريف الاتصال عنوان IP بشكل افتراضي. لذلك عندما تقوم بإنشائه، يجب أن تقوم بتغييره لإعطائه اسما كما هو موضح في لقطة الشاشة هنا:



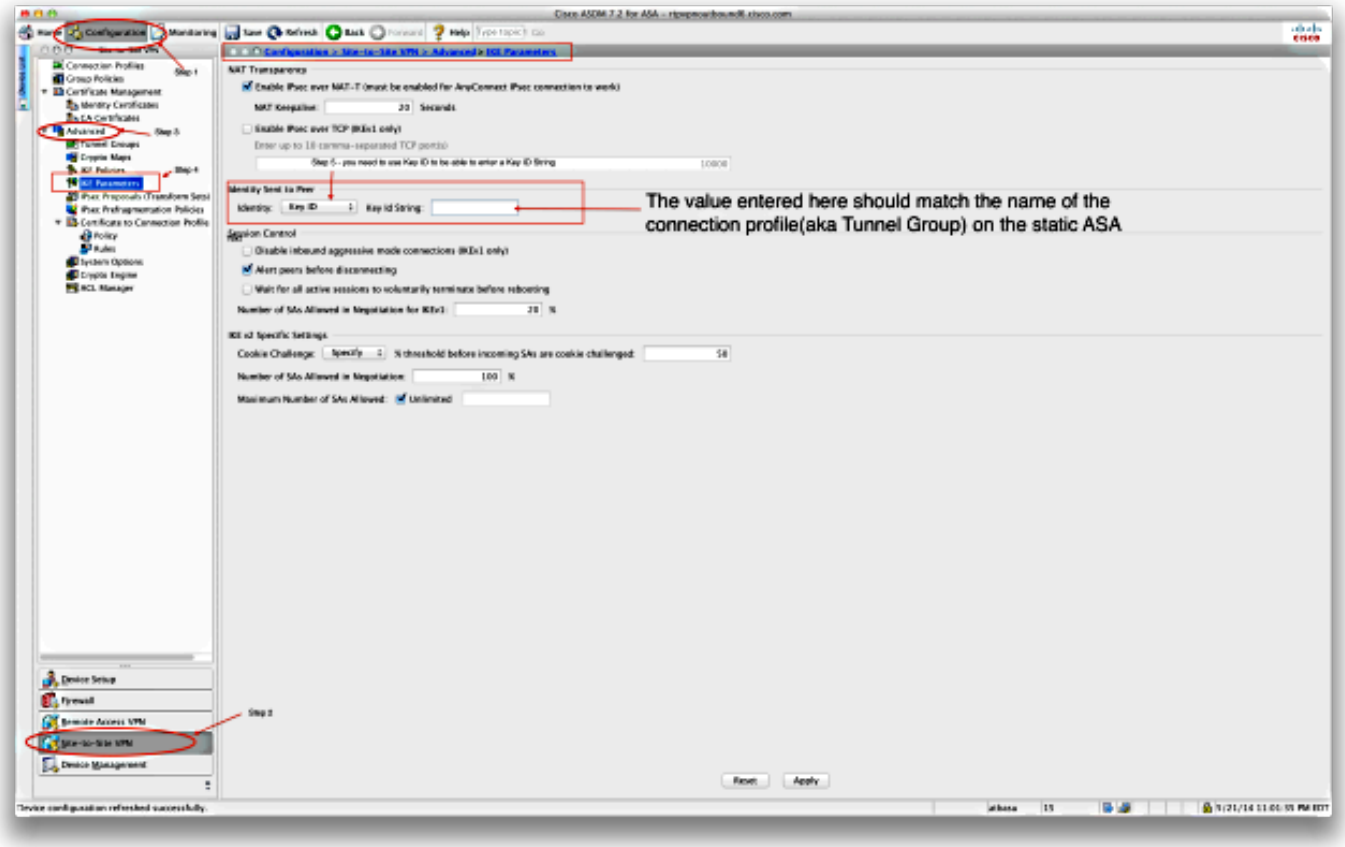
تكوين ASA الديناميكي

يتم تكوين ASA الديناميكي بنفس الطريقة تقريبا في كلا الحلين مع إضافة أمر واحد كما هو موضح هنا:

```
crypto isakmp identity key-id DynamicSite2Site1
```

وكما هو موضح مسبقا، يستخدم ASA افتراضيا عنوان IP الخاص بالواجهة التي يتم تعيين نفق VPN عليها كمعرف مفتاح ISAKMP. ومع ذلك في هذه الحالة، يكون معرف المفتاح على ASA الديناميكي هو نفسه اسم مجموعة النفق على ASA الثابت. لذلك في كل نظير حركي، سيكون معرف المفتاح مختلف ويجب إنشاء مجموعة نفق مقابلة على ASA ساكن إستاتيكي بالاسم الصحيح.

في ASDM، يمكن تكوين هذا كما هو موضح في لقطة الشاشة هذه:



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

على ال ASA الثابت

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

```
:IKEv2 SAs

                Session-id:132, Status:UP-ACTIVE, IKE count:1, CHILD count:1

 Tunnel-id                 Local                 Remote      Status          Role
READY     RESPONDER      203.0.113.134/4500    198.51.100.1/4500      1574208993
    ,Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK
                                                          Auth verify: PSK
                                          Life/Active Time: 86400/352 sec
                                                   Session-id: 132
                                  Status Description: Negotiation done
          Local spi: 4FDFF215BDEC73EC       Remote spi: 2414BEA1E10E3F70
                                                 Local id: 198.51.100.1
                                               Remote id: DynamicSite2Site1
                  Local req mess id: 13             Remote req mess id: 17
                 Local next mess id: 13            Remote next mess id: 17
                   Local req queued: 13              Remote req queued: 17
                        Local window: 1                   Remote window: 1
                                    DPD configured for 10 seconds, retry 2
                                                NAT-T is detected  outside
```

```
Child sa: local selector  172.0.0.0/0 - 172.255.255.255/65535
   remote selector 172.16.1.0/0 - 172.16.1.255/65535
               ESP spi in/out: 0x9fd5c736/0x6c5b3cc9
                        AH spi in/out: 0x0/0x0
                          CPI in/out: 0x0/0x0
        Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
    ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

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

```
                                                interface: Outside
  Crypto map tag: DynamicSite2Site1, seq num: 4, local addr: 198.51.100.1

  access-list Outside_cryptomap_1 extended permit IP 172.0.0.0 255.0.0.0
                                                  255.255.255.0 172.16.1.0
          (local ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0
     (remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0
                                       current_peer: 203.0.113.134

                     pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1#
                   pkts decaps: 12, #pkts decrypt: 12, #pkts verify: 12#
                              pkts compressed: 0, #pkts decompressed: 0#
   pkts not compressed: 1, #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.: 198.51.100.1/4500, remote crypto endpt
                                                  203.0.113.134/4500
                 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: 6C5B3CC9
                                    current inbound spi : 9FD5C736

                                                  :inbound esp sas
                                     (spi: 0x9FD5C736 (2681587510
                 transform: esp-aes-256 esp-sha-hmac no compression
            { ,in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2
       slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
(sa timing: remaining key lifetime (kB/sec): (4193279/28441
                                          IV size: 16 bytes
                                    replay detection support: Y
                                            :Anti replay bitmap
                                       0x00000000 0x00001FFF
                                                 :outbound esp sas
                                     (spi: 0x6C5B3CC9 (1817918665
                 transform: esp-aes-256 esp-sha-hmac no compression
            { ,in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2
       slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
(sa timing: remaining key lifetime (kB/sec): (3962879/28441
                                          IV size: 16 bytes
                                    replay detection support: Y
                                            :Anti replay bitmap
                                       0x00000000 0x00000001
```

حول جهاز التنفس المتكامل (ASA) الديناميكي

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

```
                                                                :IKEv2 SAs

                        Session-id:11, Status:UP-ACTIVE, IKE count:1, CHILD count:1

 Tunnel-id                 Local                 Remote     Status         Role
READY    INITIATOR      198.51.100.1/4500     192.168.50.155/4500   1132933595
    ,Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK
                                                                Auth verify: PSK
                                             Life/Active Time: 86400/267 sec
                                                               Session-id: 11
                                         Status Description: Negotiation done
          Local spi: 2414BEA1E10E3F70       Remote spi: 4FDFF215BDEC73EC
                                            Local id: DynamicSite2Site1
                                                Remote id: 198.51.100.1
                  Local req mess id: 13             Remote req mess id: 9
                 Local next mess id: 13            Remote next mess id: 9
                   Local req queued: 13              Remote req queued: 9
                       Local window: 1                   Remote window: 1
                                    DPD configured for 10 seconds, retry 2
                                                  NAT-T is detected inside
                   Child sa: local selector  172.16.1.0/0 - 172.16.1.255/65535
                  remote selector 172.0.0.0/0 - 172.255.255.255/65535
                                ESP spi in/out: 0x6c5b3cc9/0x9fd5c736
                                               AH spi in/out: 0x0/0x0
                                                  CPI in/out: 0x0/0x0
                        Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
                       ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

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

```
                                                        interface: outside
       Crypto map tag: outside_map, seq num: 1, local addr: 192.168.50.155

access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
                                                      255.0.0.0 172.0.0.0
        (local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0
            (remote ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0
                                               current_peer: 198.51.100.1

                     pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12#
                        pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1#
                                pkts compressed: 0, #pkts decompressed: 0#
   pkts not compressed: 12, #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.: 192.168.50.155/4500, remote crypto endpt
                                                        198.51.100.1/4500
                      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: 9FD5C736
                                         current inbound spi : 6C5B3CC9

                                                        :inbound esp sas
                                       (spi: 0x6C5B3CC9 (1817918665
                    transform: esp-aes-256 esp-sha-hmac no compression
  { ,in use settings ={L2L, Tunnel,  NAT-T-Encaps, PFS Group 5, IKEv2
                      slot: 0, conn_id: 77824, crypto-map: outside_map
```

```
(sa timing: remaining key lifetime (kB/sec): (4008959/28527
                                                IV size: 16 bytes
                                      replay detection support: Y
                                              :Anti replay bitmap
                                          0x00000000 0x00000003
                                                    :outbound esp sas
                                        (spi: 0x9FD5C736 (2681587510
                              transform: esp-aes-256 esp-sha-hmac no compression
                  { ,in use settings ={L2L, Tunnel,  NAT-T-Encaps, PFS Group 5, IKEv2
                                 slot: 0, conn_id: 77824, crypto-map: outside_map
                  (sa timing: remaining key lifetime (kB/sec): (4147199/28527
                                                IV size: 16 bytes
                                      replay detection support: Y
                                              :Anti replay bitmap
                                          0x00000000 0x00000001
```

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

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**.

- **حزمة IKEv2 المشفرة**
- **تشفير IKEv2 داخلي**

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).