IOS VPN(الموجه): إضافة نفق L2L جديد أو وصول عن بعد إلى شبكة VPN موجودة L2L

المحتويات

المقدمة

يقدم هذا المستند الخطوات المطلوبة لإضافة نفق L2L VPN جديد أو شبكة VPN للوصول عن بعد إلى تكوين L2L VPN موجود بالفعل في موجه IOS.

المتطلبات الأساسية

المتطلبات

تأكد من تكوين نفق VPN L2L IPSec الذي يكون قيد التشغيل حاليا قبل أن تحاول إجراء هذا التكوين بشكل صحيح.

المكونات المستخدمة

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

- موجهات IOS التي تشغل الإصدارات 12.2 و 12.4 من البرنامج
- جهاز واحد من أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA) التي تشغل الإصدار 8.0 من البرنامج

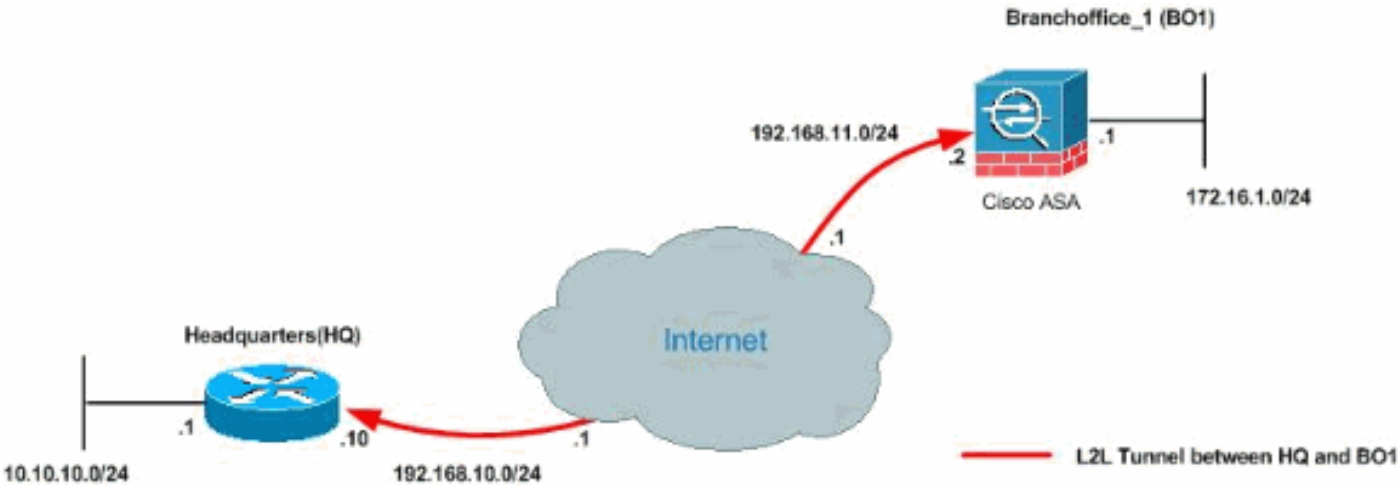
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



هذه المخرجات هي التكوينات الجاري تشغيلها حاليا من الموجه HQ (HUB) والمكتب الفرعي 1 ASA (BO1). في هذا التكوين، هناك نفق IPSec L2L تم تكوينه بين HQ و BO1 ASA.

تكوين موجه (HUB) HQ الحالي
<#root> HQ_HUB# **show running-config** Building configuration... Current configuration : 1680 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname HQ_HUB ! boot-start-marker boot-end-marker ! ! no aaa new-model

```
!
resource policy
!

!--- Output is suppressed.

!
ip cef
!
!

crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
set peer 192.168.11.2
set transform-set newset
match address VPN_BO1

!
!
!
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
ip nat inside



interface Serial2/0
ip address 192.168.10.10 255.255.255.0
ip nat outside
ip virtual-reassembly
clock rate 64000
crypto map map1

!
interface Serial2/1
no ip address
shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!

ip nat inside source route-map nonat interface Serial2/0 overload

!

ip access-list extended NAT_Exempt
deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255

!
```

```
route-map nonat permit 10
match ip address NAT_Exempt

!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

تكوين BO1 ASA

```
<#root>

CiscoASA#

show running-config

: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif inside
security-level 100
ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
nameif outside
security-level 0
ip address 192.168.11.2 255.255.255.0
!

!--- Output is suppressed.

!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list 100 extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list nonat extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0

access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
```

```
arp timeout 14400

global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0

access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup linkdown coldstart

crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp policy 65535
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global

tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
```

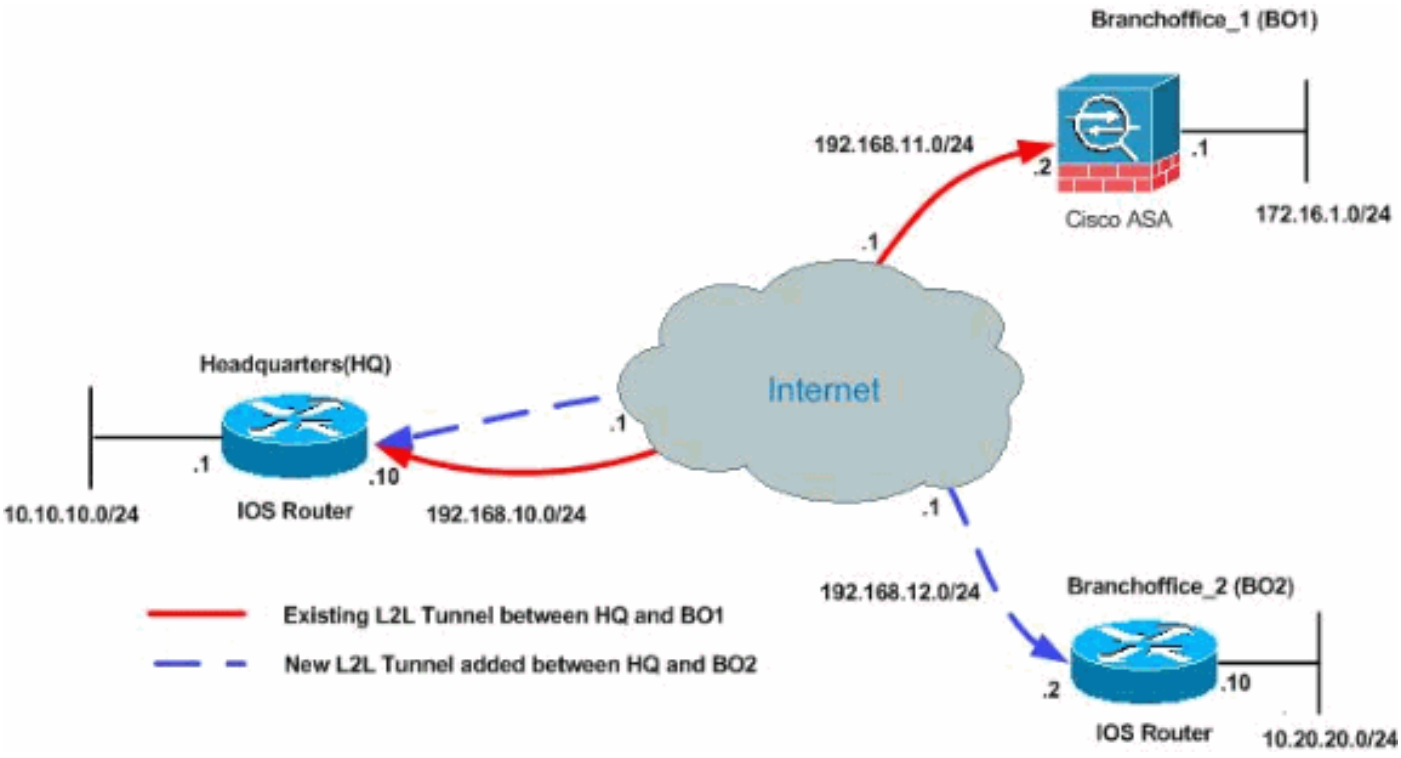
```
                                                                pre-shared-key *

                                                                prompt hostname context
                                                Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
                                                                        : end
                                                                CiscoASA#
```

معلومات أساسية

حالياً، هناك نفق L2L موجود تم إعداده بين مكتب المقر الرئيسي ومكتب BO1. قامت شركتك مؤخرا بفتح مكتب فرع جديد (BO2). يتطلب هذا المكتب الجديد الاتصال بالموارد المحلية الموجودة في مكتب المقر الرئيسي. بالإضافة إلى ذلك، هناك حاجة إضافية للسماح للموظفين بفرصة العمل من المنزل والوصول الآمن إلى الموارد الموجودة على الشبكة الداخلية عن بعد. في هذا المثال، تم تكوين نفق VPN جديد بالإضافة إلى خادم VPN للوصول عن بعد موجود في مكتب المقر (HQ).

إضافة نفق L2L إضافي إلى التكوين

هذا هو الرسم التخطيطي للشبكة لهذا التكوين:



التعليمات بالتفصيل

يوفر هذا القسم الإجراءات المطلوبة التي يجب تنفيذها على موجه HUB HQ.

أكمل الخطوات التالية:

1. قم بإنشاء قائمة الوصول الجديدة هذه التي سيتم إستخدامها من قبل خريطة

التشفير لتحديد حركة المرور المفيدة:

```
<#root>

HQ_HUB(config)#

ip access-list extended VPN_BO2

HQ_HUB(config-ext-nacl)#

permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

exit
```

تحذير: لكي يحدث الاتصال، يجب أن يكون للجانب الآخر من النفق عكس إدخال قائمة التحكم في الوصول (ACL) هذا الخاص بتلك الشبكة المحددة.

2. قم بإضافة هذه الإدخالات إلى جملة NAT بدون إستثناء الحد الفاصل بين هذه الشبكات:

```
<#root>

HQ_HUB(config)#

ip access-list extended NAT_Exempt

HQ_HUB(config-ext-nacl)#

deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

permit ip 10.10.10.0 0.0.0.255 any
```

إضافة قوائم التحكم في الوصول (ACL) هذه إلى غير الموجود في خريطة المسار:

```
<#root>

HQ_HUB(config)#

route-map nonat permit 10

HQ_HUB(config-route-map)#

match ip address NAT_Exempt

HQ_HUB(config)#

ip nat inside source route-map nonat interface Serial2/0 overload
```

تحذير: لكي يحدث الاتصال، يجب أن يكون للجانب الآخر من النفق عكس إدخال قائمة

التحكم في الوصول هذا للشبكة المحددة.

3. حدد عنوان النظير في تكوين المرحلة 1 كما هو موضح:

```
<#root>

HQ_HUB(config)#

crypto isakmp key cisco123 address 192.168.12.2
```

ملاحظة: يجب أن يتطابق المفتاح المشترك مسبقا تماما على كلا جانبي النفق.

4. قم بإنشاء تكوين خريطة التشفير لنفق VPN الجديد. استعملت ال نفسه توجيل إعداد ال مرحلة 2 عملية أن all the أمر، أن كان استعملت في أول VPN تشكيل مجموعة نفس.

```
<#root>

HQ_HUB(config)#

crypto map map1 10 ipsec-isakmp

HQ_HUB(config-crypto-map)#

set peer 192.168.12.2

HQ_HUB(config-crypto-map)#

set transform-set newset

HQ_HUB(config-crypto-map)#

match address VPN_BO2
```

5. والآن بعد ان انتهيت من تكوين النفق الجديد، يجب ان ترسل حركة مرور مثيرة للاهتمام عبر النفق لكي ترفعه. ولتنفيذ هذا الإجراء، قم بإصدار الأمر ping الموسع للاتصال بمضيف على الشبكة الداخلية للنفق البعيد.

في هذا المثال، يتم سحب محطة عمل على الجانب الآخر من النفق بعنوان 10.20.20.16. الآن، هناك نفقين متصلان. 2 وبو وهذا يجعل النفق يصل بين المقر الرئيسي والمقر الرئيسي. إذا لم يكن لديك حق الوصول إلى نظام خلف النفق، فارجع إلى حلول استكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) الخاصة بـ L2L و Remote Access للوصول عن بعد للعثور على حل بديل باستخدام management-access.

مثال التكوين

HUB_HQ - تمت إضافة تكوين نفق L2L VPN جديد
<#root>

```
HQ_HUB#
show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
crypto isakmp policy 10
authentication pre-share
encryption 3des
group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2

!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
set peer 192.168.11.2
set transform-set newset
match address VPN_BO1
crypto map map1 10 ipsec-isakmp
set peer 192.168.12.2
set transform-set newset
match address VPN_BO2

!
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly
!

interface Serial2/0
ip address 192.168.10.10 255.255.255.0
ip nat outside
ip virtual-reassembly
clock rate 64000
```

```
                                                    crypto map map1

                                                                  !
                                                                  !
                                                        ip http server
                                                 no ip http secure-server
                                                                  !
                                       ip route 0.0.0.0 0.0.0.0 192.168.10.1
                                                                  !
ip nat inside source route-map nonat interface Serial2/0 overload
                                                                  !


                                          ip access-list extended NAT_Exempt
                          deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255


                          deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255



                                          permit ip 10.10.10.0 0.0.0.255 any

                                             ip access-list extended VPN_BO1
                          permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255

                                          ip access-list extended VPN_BO2
                          permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255




                                                                  !
                                                  route-map nonat permit 10
                                                match ip address NAT_Exempt
                                                                  !
                                                                  !
                                                        control-plane
                                                                  !
                                                                  !
                                                                  !
                                                          line con 0
                                                          line aux 0
                                                        line vty 0 4
                                                                  !
                                                                  !
                                                               end
                                                            HQ_HUB#
```

تكوين نفق BO2 L2L VPN

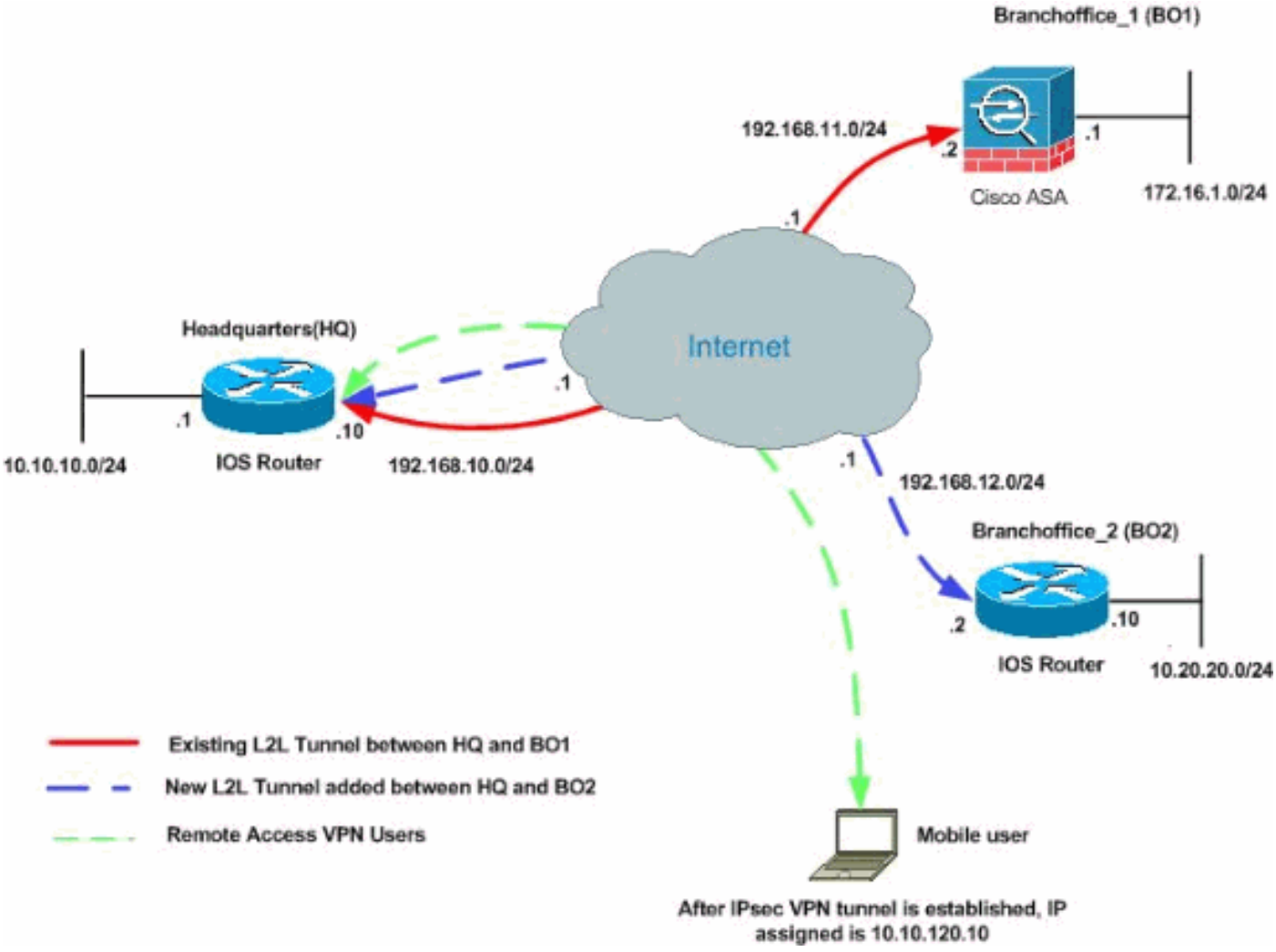
```
                                                            <#root>

                                                             BO2#

                                                    show running-config

                                                 Building configuration...

                3w3d: %SYS-5-CONFIG_I: Configured from console by console
                                          Current configuration : 1212 bytes
```

```
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
authentication pre-share
encryption 3des
group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
set peer 192.168.10.10
set transform-set newset
match address 100
!
!
!
!
interface Ethernet0
ip address 10.20.20.10 255.255.255.0
ip nat inside
!

!
interface Ethernet1
ip address 192.168.12.2 255.255.255.0
ip nat outside
crypto map map1
!
interface Serial0
no ip address
no fair-queue
!
interface Serial1
no ip address
shutdown
!
ip nat inside source route-map nonat interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
```

```
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

إضافة شبكة VPN للوصول عن بعد إلى التكوين

هذا هو الرسم التخطيطي للشبكة لهذا التكوين:



في هذا مثال، استعملت السمة يدعو split-tunneling. تتيح هذه الميزة لعميل IPSec للوصول عن بعد توجيه الحزم بشروط عبر نفق IPSec في شكل مشفر، وأ إلى واجهة شبكة في شكل نص واضح. مع تمكين تقسيم النفق، ال يجب تشفير الحزم غير المرتبطة باالوجهات على الجانب الآخر من نفق IPSec، وإرسالها عبر النفق، وفك تشفيرها، ثم توجيهها إلى وجهة

.ةيئانه .يطبق هذا المفهوم سياسة تقسيم الاتصال النفقي على شبكة محددة
التقصير أن ينفق لك حركة مرور .لتعييني سياسة تقسيم الاتصال النفقي، حدد قائمة
.تحكم في الوصول (ACL) حيث يمكن ذكر حركة المرور المخصصة للإنترنت

التعليمات بالتفصيل

يوفر هذا القسم الإجراءات المطلوبة لإضافة إمكانية الوصول عن بعد والسماح
.للمستخدمين عن بعد بالوصول إلى كافة المواقع

:أكمل الخطوات التالية

1. خلقت .ق VPN نفق. خلقت عنوان بركة أن يكون استعملت لزبون أن يربط عن طريق الـ VPN
   .أيضا، مستعمل أساسي in order to نفذت الـ VPN ام إن التشكيل أتمت

- ```
  <#root>

  HQ_HUB(config)#

  ip local pool ippool 10.10.120.10 10.10.120.50
  ```

- ```
  <#root>

  HQ_HUB(config)#

  username vpnuser password 0 vpnuser123
  ```

2. إستثناء حركة مرور معينة من كونها غير محددة.

```
<#root>

HQ_HUB(config)#

ip access-list extended NAT_Exempt

HQ_HUB(config-ext-nacl)#

deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

permit ip host 10.10.10.0 any

HQ_HUB(config-ext-nacl)#

exit
```

إضافة قوائم التحكم في الوصول (ACL) هذه إلى غير الموجود في خريطة المسار:

```
<#root>

HQ_HUB(config)#

route-map nonat permit 10

HQ_HUB(config-route-map)#

match ip address NAT_Exempt

HQ_HUB(config)#

ip nat inside source route-map nonat interface Serial2/0 overload
```

لاحظ أن اتصال NAT بين أنفاق الشبكة الخاصة الظاهرية (VPN) معفى في هذا المثال.

3. السماح بالاتصال بين أنفاق L2L الموجودة ومستخدمي شبكة VPN للوصول عن بعد.

```
<#root>

HQ_HUB(config)#

ip access-list extended VPN_BO1

HQ_HUB(config-ext-nacl)#

permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

exit

HQ_HUB(config)#

ip access-list extended VPN_BO2

HQ_HUB(config-ext-nacl)#

permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

exit
```

وهذا يتيح لمستخدمي الوصول عن بعد إمكانية الاتصال بالشبكات خلف الأنفاق المحددة.

تحذير: لكي يحدث الاتصال، يجب أن يكون للجانب الآخر من النفق عكس إدخال قائمة التحكم في الوصول هذا للشبكة المحددة.

4. تكوين تقسيم الاتصال النفقي

تأكد in order to مكنت انقسام tunneling ل الـ VPN توصيل، لذلك تشكل ACL على مجموعة access-list split_tunnel المسماة. في هذا المثال، يتم إقران الأمر ip access-list extended split_tunnel بالشبكات 10.10.10.0 /24 و 10.10.120.0 /24 لإنشاء قنوات منفصلة، ويتم تكوين النفق لشبكات غير موجودة في النفق المقسم (على سبيل المثال، الإنترنت). تدفق حركة المرور غير المشفرة إلى الأجهزة 172.16.1.0/24 و 10.20.20.0/24 لتحكم في الوصول القائمة التحكم في الوصول (ACL) لحركة المرور المفيدة وتجميع IP، على سبيل المثال، WINS و DNS.

```
<#root>

HQ_HUB(config)#

ip access-list extended split_tunnel

HQ_HUB(config-ext-nacl)#

permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255

HQ_HUB(config-ext-nacl)#

exit
```

5. قم بتكوين معلومات المصادقة والتفويض وتكوين العميل المحلية، مثل WINS و DNS. قائمة التحكم في الوصول (ACL) لحركة المرور المفيدة وتجميع IP، على سبيل المثال، شبكة العملاء VPN.

```
<#root>

HQ_HUB(config)#

aaa new-model

HQ_HUB(config)#

aaa authentication login userauthen local

HQ_HUB(config)#

aaa authorization network groupauthor local

HQ_HUB(config)#

crypto isakmp client configuration group vpngroup

HQ_HUB(config-isakmp-group)#

key cisco123

HQ_HUB(config-isakmp-group)#

dns 10.10.10.10

HQ_HUB(config-isakmp-group)#
```

```
wins 10.10.10.20
HQ_HUB(config-isakmp-group)#
domain cisco.com
HQ_HUB(config-isakmp-group)#
pool ippool
HQ_HUB(config-isakmp-group)#
acl split_tunnel
HQ_HUB(config-isakmp-group)#
exit
```

6. قم بتكوين معلومات الخريطة الديناميكية والخريطة المتبلورة المطلوبة لإنشاء نفق VPN.

```
<#root>
HQ_HUB(config)#
crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#
match identity group vpngroup
HQ_HUB(config-isakmp-group)#
client authentication list userauthen
HQ_HUB(config-isakmp-group)#
isakmp authorization list groupauthor
HQ_HUB(config-isakmp-group)#
client configuration address respond
HQ_HUB(config-isakmp-group)#
exit
HQ_HUB(config)#
crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#
set transform-set newset
HQ_HUB(config-crypto-map)#
set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#
reverse-route
HQ_HUB(config-crypto-map)#
```

```
exit
HQ_HUB(config)#
crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#
interface serial 2/0
HQ_HUB(config-if)#
crypto map map1
```

مثال التكوين

مثال تشكيل 2

```
<#root>
HQ_HUB#
show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!

aaa new-model

!
!

aaa authentication login userauthen local
aaa authorization network groupauthor local

!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!

!--- Output is suppressed
```

```
!
username vpnuser password 0 vpnuser123
!
!
!
crypto isakmp policy 10
authentication pre-share
encryption 3des
group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!

crypto isakmp client configuration group vpngroup
key cisco123
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
acl split_tunnel
crypto isakmp profile vpnclient
match identity group vpngroup
client authentication list userauthen
isakmp authorization list groupauthor
client configuration address respond

!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac

crypto ipsec transform-set remote-set esp-3des esp-md5-hmac

!

crypto dynamic-map dynmap 10
set transform-set remote-set
set isakmp-profile vpnclient
reverse-route

!
!
crypto map map1 5 ipsec-isakmp
set peer 192.168.11.2
set transform-set newset
match address VPN_BO1
crypto map map1 10 ipsec-isakmp
set peer 192.168.12.2
set transform-set newset
match address VPN_BO2

crypto map map1 65535 ipsec-isakmp dynamic dynmap

!
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly
!

interface Serial2/0
ip address 192.168.10.10 255.255.255.0
ip nat outside
```

```
 ip virtual-reassembly
 clock rate 64000


 crypto map map1

 !
 !

ip local pool ippool 10.10.120.10 10.10.120.50

 ip http server
 no ip http secure-server
 !
ip route 0.0.0.0 0.0.0.0 192.168.10.1
 !

ip nat inside source route-map nonat interface Serial2/0 overload

 !
 ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255


 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any

 ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255


 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255

 ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255


 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255

 ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255




 !

 route-map nonat permit 10
 match ip address NAT_Exempt

 !
 !
 control-plane
 !
 line con 0
 line aux 0
 line vty 0 4
 !
 !
 end
```

```
HQ_HUB#
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

- ping— يسمح لك هذا الأمر ببدء نفق L2L VPN كما هو موضح.

إختبار الاتصال الموسع

```
<#root>

HQ_HUB#

ping



!--- In order to make the L2L VPN tunnel with

BO1

!--- to be established.

Protocol [ip]:
Target IP address:

172.16.1.2

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:

y

Source address or interface:

10.10.10.1

Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 132/160/172 ms
```

```
                                                                HQ_HUB#
                                                                ping


                                        !--- In order to make the L2L VPN tunnel with
                                                                BO2
                                                !--- to be established.
                                                          Protocol [ip]:
                                                Target IP address: 10.20.20.10
                                                     Repeat count [5]:
                                                   Datagram size [100]:
                                                  Timeout in seconds [2]:
                                                   Extended commands [n]:
                                                                y
                                                  Source address or interface:
                                                                10.10.10.1
                                                      Type of service [0]:
                                                 Set DF bit in IP header? [no]:
                                                     Validate reply data? [no]:
                                                         Data pattern [0xABCD]:
                                 Loose, Strict, Record, Timestamp, Verbose[none]:
                                                     Sweep range of sizes [n]:
                                                 Type escape sequence to abort.
                   Sending 5, 100-byte ICMP Echos to 10.20.20.10, timeout is 2 seconds:
                                 Packet sent with a source address of 10.10.10.1
                                                                ....!

Success rate is 20 percent (1/5), round-trip min/avg/max = 64/64/64 ms
```

show crypto isakmp sa

```
                                                                <#root>

                                                                HQ_HUB#
                                                      show crypto isakmp sa

dst             src             state          conn-id slot status

192.168.12.2    192.168.10.10   QM_IDLE              2    0 ACTIVE
192.168.11.2    192.168.10.10   QM_IDLE              1    0 ACTIVE
```

show crypto ipsec sa

```
                                                                <#root>
```

```
HQ_HUB#
show crypto ipsec sa

interface: Serial2/0
Crypto map tag: map1, local addr
192.168.10.10

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.10.120.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer 192.168.11.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#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.:
192.168.10.10
, remote crypto endpt.:
192.168.11.2

2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

local crypto endpt.:
192.168.10.10
, remote crypto endpt.:
192.168.12.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:
```

```
                                                    outbound esp sas:

                                                     outbound ah sas:

                                                    outbound pcp sas:

                                                  protected vrf: (none)
      local  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
                                      current_peer 192.168.12.2 port 500
                                          PERMIT, flags={origin_is_acl,}
                     #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
                     #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
                             #pkts compressed: 0, #pkts decompressed: 0
                        #pkts not compressed: 0, #pkts compr. failed: 0
                  #pkts not decompressed: 0, #pkts decompress failed: 0
                                      #send errors 4, #recv errors 0

  local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
                       path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                                  current outbound spi: 0xF1328(987944)

                                                    inbound esp sas:
                                               spi: 0xAD07C262(2902966882)
                                      transform: esp-3des esp-md5-hmac ,
                                               in use settings ={Tunnel, }
                           conn id: 2004, flow_id: SW:4, crypto map: map1
               sa timing: remaining key lifetime (k/sec): (4601612/3292)
                                                    IV size: 8 bytes
                                               replay detection support: Y
                                                      Status: ACTIVE

                                                     inbound ah sas:

                                                    inbound pcp sas:

                                                   outbound esp sas:
                                                 spi: 0xF1328(987944)
                                      transform: esp-3des esp-md5-hmac ,
                                               in use settings ={Tunnel, }
                           conn id: 2003, flow_id: SW:3, crypto map: map1
               sa timing: remaining key lifetime (k/sec): (4601612/3291)
                                                    IV size: 8 bytes
                                               replay detection support: Y
                                                      Status: ACTIVE

                                                    outbound ah sas:

                                                   outbound pcp sas:

                                                  protected vrf: (none)
     local  ident (addr/mask/prot/port): (10.10.120.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
                                      current_peer 192.168.12.2 port 500
                                          PERMIT, flags={origin_is_acl,}
                     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
                     #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
                             #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.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
                      path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                                          current outbound spi: 0x0(0)

                                                        inbound esp sas:

                                                         inbound ah sas:

                                                        inbound pcp sas:

                                                       outbound esp sas:

                                                        outbound ah sas:

                                                       outbound pcp sas:

                                                    protected vrf: (none)
      local  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
                                      current_peer 192.168.11.2 port 500
                                          PERMIT, flags={origin_is_acl,}
                    #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: 0, #pkts compr. failed: 0
                #pkts not decompressed: 0, #pkts decompress failed: 0
                                      #send errors 11, #recv errors 0

  local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.11.2
                      path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                          current outbound spi: 0x978B3F93(2542485395)

                                                        inbound esp sas:
                                                  spi: 0x2884F32(42487602)
                                      transform: esp-3des esp-md5-hmac ,
                                             in use settings ={Tunnel, }
                        conn id: 2002, flow_id: SW:2, crypto map: map1
              sa timing: remaining key lifetime (k/sec): (4421529/3261)
                                                    IV size: 8 bytes
                                             replay detection support: Y
                                                      Status: ACTIVE

                                                         inbound ah sas:

                                                        inbound pcp sas:

                                                       outbound esp sas:
                                                  spi: 0x978B3F93(2542485395)
                                      transform: esp-3des esp-md5-hmac ,
                                             in use settings ={Tunnel, }
                        conn id: 2001, flow_id: SW:1, crypto map: map1
              sa timing: remaining key lifetime (k/sec): (4421529/3261)
                                                    IV size: 8 bytes
                                             replay detection support: Y
                                                      Status: ACTIVE

                                                        outbound ah sas:
```

```
                                                    outbound pcp sas:

    local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
                          path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                                              current outbound spi: 0x0(0)

                                                     inbound esp sas:

                                                      inbound ah sas:

                                                     inbound pcp sas:

                                                    outbound esp sas:

                                                     outbound ah sas:

                                                    outbound pcp sas:

                                                  protected vrf: (none)
        local  ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
        remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
                                        current_peer 192.168.12.2 port 500
                                            PERMIT, flags={origin_is_acl,}
                       #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
                       #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
                               #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.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
                          path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                                              current outbound spi: 0x0(0)

                                                     inbound esp sas:

                                                      inbound ah sas:

                                                     inbound pcp sas:

                                                    outbound esp sas:

                                                     outbound ah sas:

                                                    outbound pcp sas:

                                                  protected vrf: (none)
        local  ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
        remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
                                        current_peer 192.168.11.2 port 500
                                            PERMIT, flags={origin_is_acl,}
                       #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
                       #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
                               #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.: 192.168.10.10, remote crypto endpt.: 192.168.11.2
```

```
                                    path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                                          current outbound spi: 0x0(0)

                                                    inbound esp sas:

                                                     inbound ah sas:

                                                    inbound pcp sas:

                                                   outbound esp sas:

                                                    outbound ah sas:

                                                   outbound pcp sas:

        local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
                                    path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
                                          current outbound spi: 0x0(0)

                                                    inbound esp sas:

                                                     inbound ah sas:

                                                    inbound pcp sas:

                                                   outbound esp sas:

                                                    outbound ah sas:

                                                   outbound pcp sas:
                                                             HQ_HUB#
```

استكشاف الأخطاء وإصلاحها

ارجع إلى هذه المستندات للحصول على معلومات يمكن إستخدامها لاستكشاف أخطاء التكوين وإصلاحها:

- [حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPSec للوصول عن بعد و L2L الأكثر شيوعا](#)
- [استخدام أوامر التصحيح و أستكشاف أخطاء أمان IP وإصلاحها - فهم](#)

تلميح: عند [مسح اقترانات الأمان](#)، وقم بعد ذلك بإزالة مشكلة IPsec VPN، والي يوقوم بحل مشكلة خريطة التشفير ذات الصلة وإعادة تطبيقها لحل مجموعة كبيرة من المشاكل.

تحذير: إذا قمت بإزالة خريطة تشفير من واجهة، فإنها تسقط أي أنفاق IPSec مرتبطة بخريطة التشفير هذه. اتبع هذه الخطوات بحذر وتفكر في سياسة التحكم في التغيير الخاصة بمؤسستك قبل المتابعة.

لمثال

<#root>

```
HQ_HUB(config)#

interface s2/0

HQ_HUB(config-if)#

no crypto map map1

*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#

crypto map map1

*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

معلومات ذات صلة

- [مقدمة عن تشفير أمان IP (IPSec)]
- [صفحة دعم مواضيع IPSec/بروتوكولات IKE]
- [تكوين نظير شبكة LAN إلى شبكة LAN الديناميكية لموجه IPsec وعملاء شبكة VPN الديناميكية]
- [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).