IOS VPN（路由器）：向現有L2L VPN新增新的L2L隧道或遠端訪問

目錄

簡介

本文檔提供向IOS路由器中已存在的L2L VPN配置中新增新的L2L VPN隧道或遠端訪問VPN所需的步驟。

必要條件

需求

嘗試此配置之前，請確保正確配置當前可運行的L2L IPSec VPN隧道。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 兩台運行軟體版本12.4和12.2的IOS路由器
- 一台思科自適應安全裝置(ASA)，運行軟體版本8.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

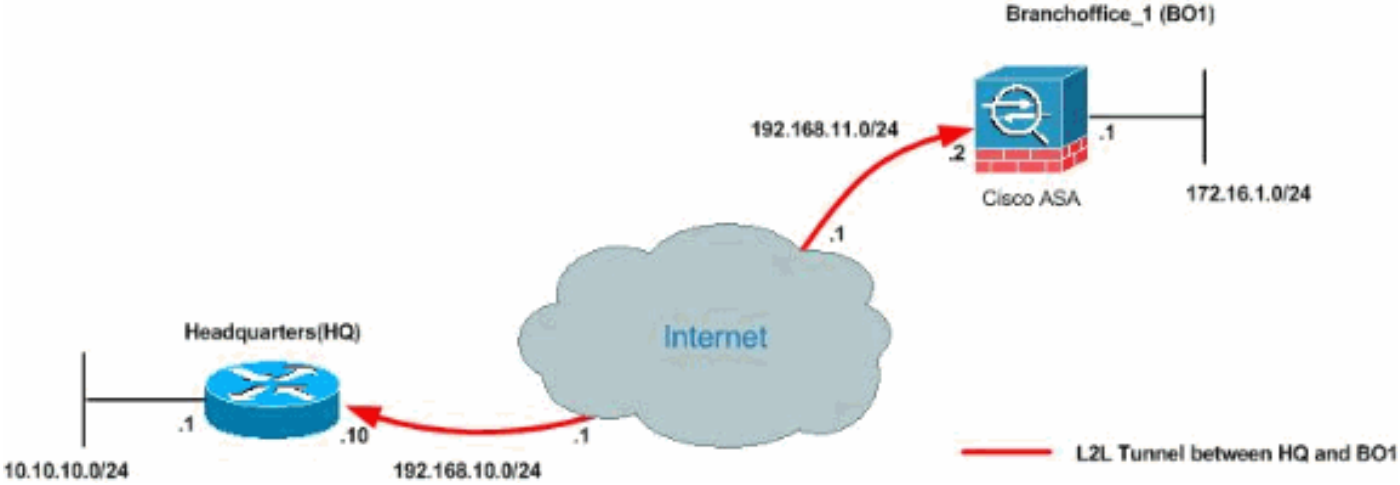
）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

網路圖表

此文件使用以下網路設定：



這些輸出是HQ(HUB)路由器和分支辦公室1(BO1)ASA的當前運行配置。在此配置中，在HQ和BO1 ASA之間配置了IPSec L2L隧道。

當前HQ(HUB)路由器配置
<#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#
```

BO1 ASA配置

<#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
```

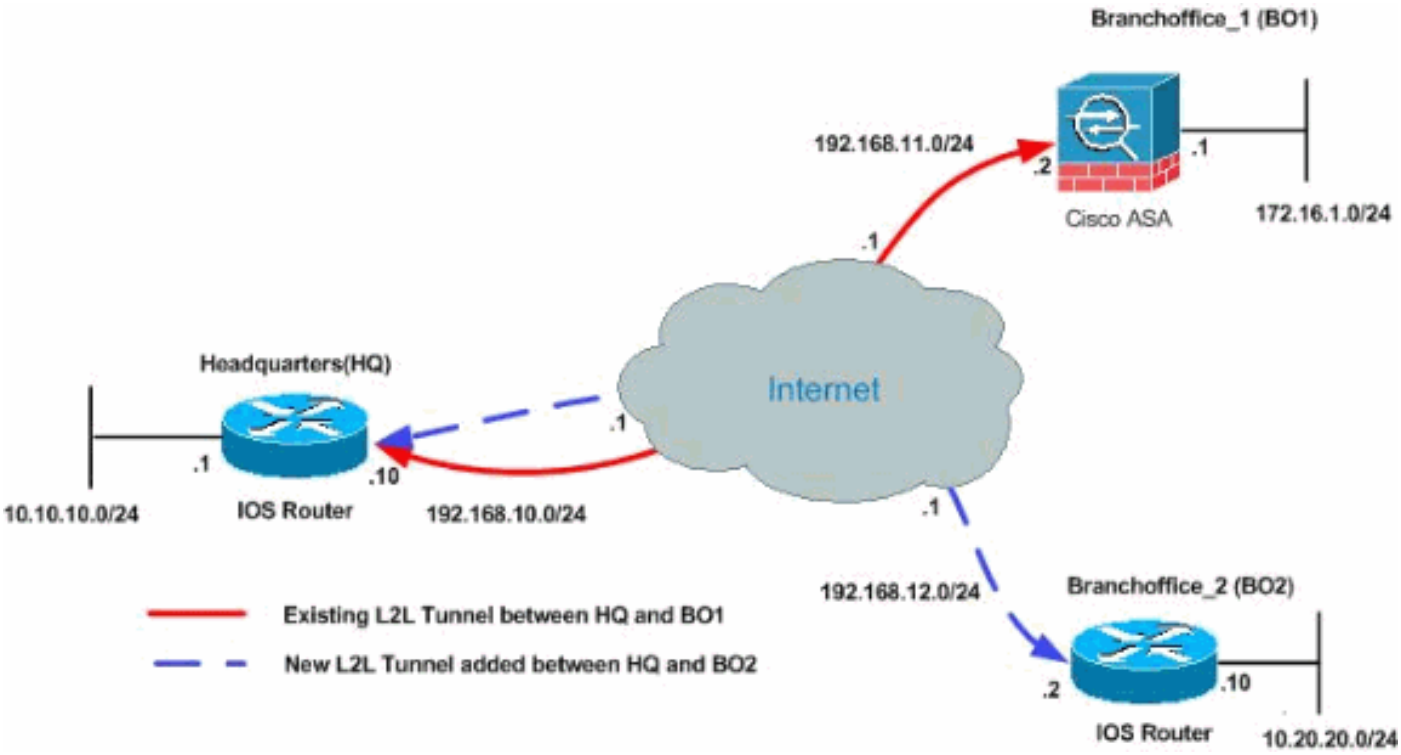
```
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

背景資訊

目前，在HQ辦公室和BO1辦公室之間已經建立了一個L2L隧道。您的公司最近開設了一個新的分支機構(BO2)。這個新辦公室需要連線到總部辦公室內的本地資源。此外，還額外要求允許員工有機會在家工作，並安全地遠端訪問內部網路上的資源。在本示例中，配置了新的VPN隧道以及位於HQ辦公室的遠端訪問VPN伺服器。

將額外的L2L隧道新增到配置

以下是此組態的網路圖：



逐步說明

本節提供了必須在HUB HQ路由器上執行的過程。

請完成以下步驟：

1. 請建立此新的存取清單，以供密碼編譯對應用來定義相關流量：

```
<#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
```

警告：若要發生通訊，通道的另一端必須擁有與該特定網路的存取控制清單(ACL)專案相反的專案。

2. 將這些條目新增到no nat語句中，以免除在這些網路之間的命名：

```
<#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
```

將以下ACL新增到現有路由對映nonat:

```
<#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
```

警告：為了進行通訊，通道的另一端必須擁有與該特定網路的此ACL專案相反的專案。

3. 在階段1配置中指定對等體地址，如下所示：

```
<#root>
HQ_HUB(config)#
```

```
crypto isakmp key cisco123 address 192.168.12.2
```

注意：預先共用金鑰在通道的兩端必須完全相符。

4. 為新的VPN隧道建立加密對映配置。使用在第一個VPN配置中使用的相同轉換集，因為所有階段2設定都相同。

```
<#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. 現在您已設定新通道，您必須透過通道傳送相關流量才能將其啟用。若要執行此操作，請發出擴展ping命令，對遠端隧道內部網路上的主機執行ping。

   在本例中，對位於隧道另一端、地址為10.20.20.16的工作站執行ping操作。這樣就會在HQ和BO2之間開啟隧道。現在，有兩條隧道連線到HQ辦公室。如果您無法訪問通道後面的系統，請參閱最常見的L2L和遠端訪問IPSec VPN故障排除解決方案，以使用management-access查詢替代解決方案。

組態範例

HUB_HQ — 新增了新的L2L VPN隧道配置
<#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#
```

BO2 L2L VPN隧道配置

```
<#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
!
!
!
!
!
```

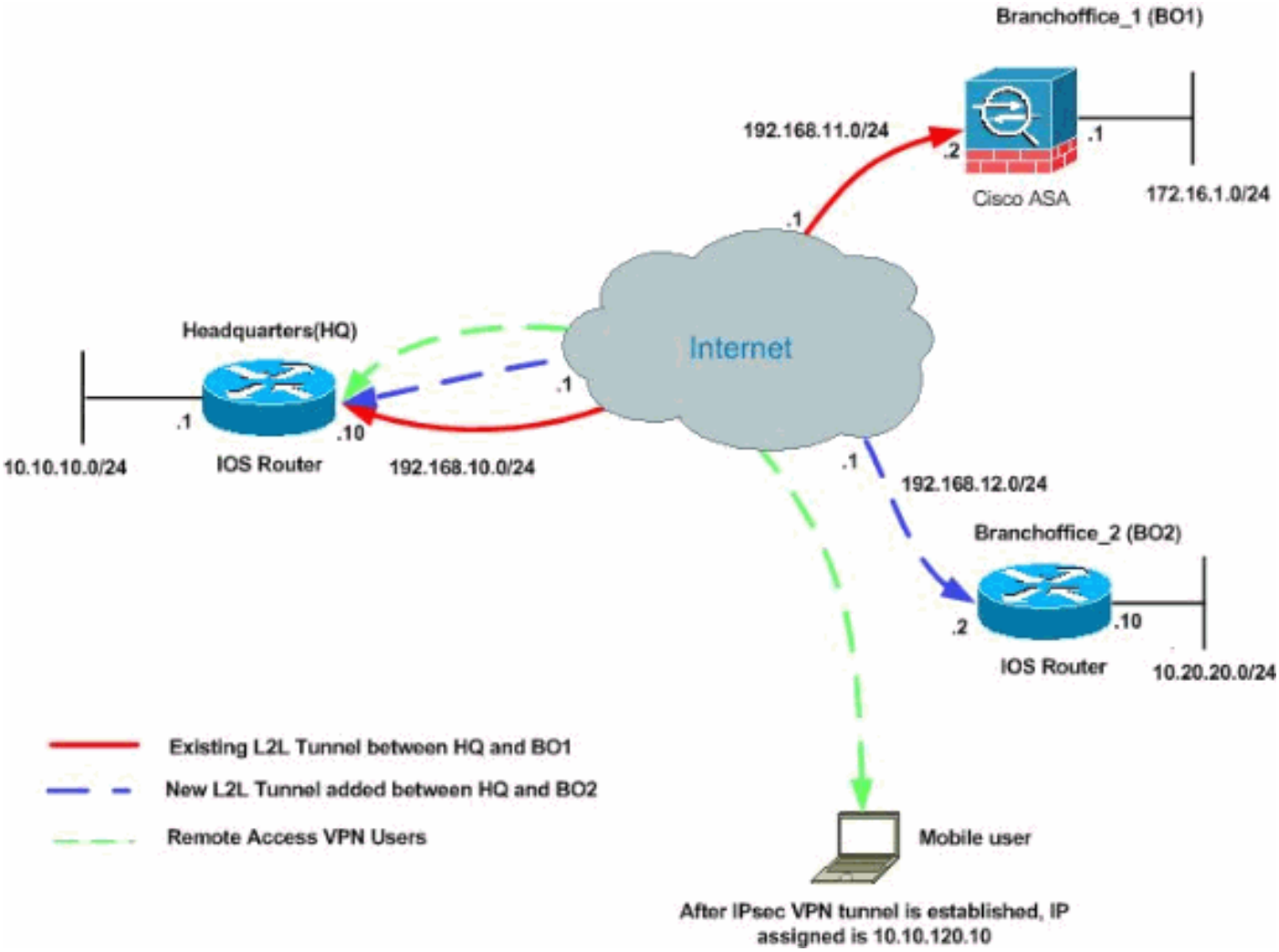
```
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match 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#
```

將遠端訪問VPN新增到配置

以下是此組態的網路圖：



在本示例中，使用名為split-tunneling的功能。此功能允許遠端訪問IPSec客戶端有條件地將資料包以加密形式通過IPSec隧道轉發，或者以明文形式轉發到網路介面。啟用分割隧道後，未繫結到IPSec隧道另一側上的目標的資料包不必經過加密、通過隧道傳送、解密，然後路由到最終目標。此概念將分割隧道策略應用於指定網路。預設為透過通道傳輸所有流量。若要設定分割通道原則，請指定可提到代表Internet的流量的ACL。

逐步說明

本節提供新增遠端訪問功能和允許遠端使用者訪問所有站點所需的過程。

請完成以下步驟：

1. 建立用於通過VPN隧道連線的客戶端的IP地址池。此外，建立基本使用者，以便在配置完成後訪問VPN。
    -

<#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. 免除特定流量的NAT。

<#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

將以下ACL新增到現有路由對映nonat:

<#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

請注意，在此示例中，VPN隧道之間的nat通訊被免除。

3. 允許現有L2L隧道和遠端訪問VPN使用者之間的通訊。

```
<#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
```

這樣，遠端訪問使用者就能夠與指定隧道後的網路通訊。

警告：為了進行通訊，通道的另一端必須擁有與該特定網路的此ACL專案相反的專案。

4. 配置分割隧道

若要為VPN連線啟用分割通道，請確保在路由器上配置ACL。在本例中，access-list split_tunnel命令與用於分割隧道的組相關聯，並且隧道形成到10.10.10.0 /24和10.20.20.0/24以及172.16.1.0/24網路。未加密的流量流向不在ACL分割通道中的裝置（例如Internet）。

```
<#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. 為VPN客戶端配置本地身份驗證、授權和客戶端配置資訊，例如wins、dns、相關流量acl和ip池。

```
<#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. 配置建立VPN隧道所需的動態對映和加密對映資訊。

```
<#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
```

組態範例

示例配置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#
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- ping — 此命令可讓您啟動L2L VPN通道，如圖所示。

延伸Ping
<#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#
```

疑難排解

請參閱這些檔案瞭解可用於對組態進行疑難排解的資訊：

- 最常見的L2L和遠端訪問IPSec VPN故障排除解決方案
- IP安全性疑難排解 — 瞭解和使用debug命令

提示：清除安全關聯時，不會解決IPsec VPN問題，然後刪除並重新應用相關加密對映以解決各種問題。

警告：如果從介面刪除加密對映，則會關閉與該加密對映關聯的所有IPSec隧道。請謹慎遵循這些步驟，並在繼續操作之前考慮組織的變更控制策略。

範例

<#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
```

相關資訊

- IP安全(IPSec)加密簡介
- IPSec協商/IKE通訊協定支援頁面
- 配置IPsec路由器動態LAN到LAN對等路由器和VPN客戶端
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。