單臂公共網際網路的路由器和VPN客戶端配置示例

目錄

簡介

本文檔介紹如何設定中心站點路由器以在單臂上執行IPsec流量。此設定適用於以下特定情況：路由器在不啟用分割隧道的情況下，移動使用者（Cisco VPN客戶端）可以通過中央站點路由器訪問網際網路。為此，請在路由器中配置策略對映以將所有VPN流量（Cisco VPN客戶端）指向環回介面。這允許將Internet流量進行埠地址轉換(PATed)到外界。

請參閱PIX/ASA 7.x和VPN Client for Public Internet VPN on a Stick配置示例，以在中心站點PIX防火牆上完成類似的配置。

注意：為了避免網路中IP地址重疊，請將完全不同的IP地址池分配給VPN客戶端（例如，10.x.x.x、172.16.x.x、192.168.x.x）。 此IP編址方案可幫助您排除網路故障。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用Cisco IOS®軟體版本12.4的Cisco路由器3640
- Cisco VPN使用者端4.8

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。

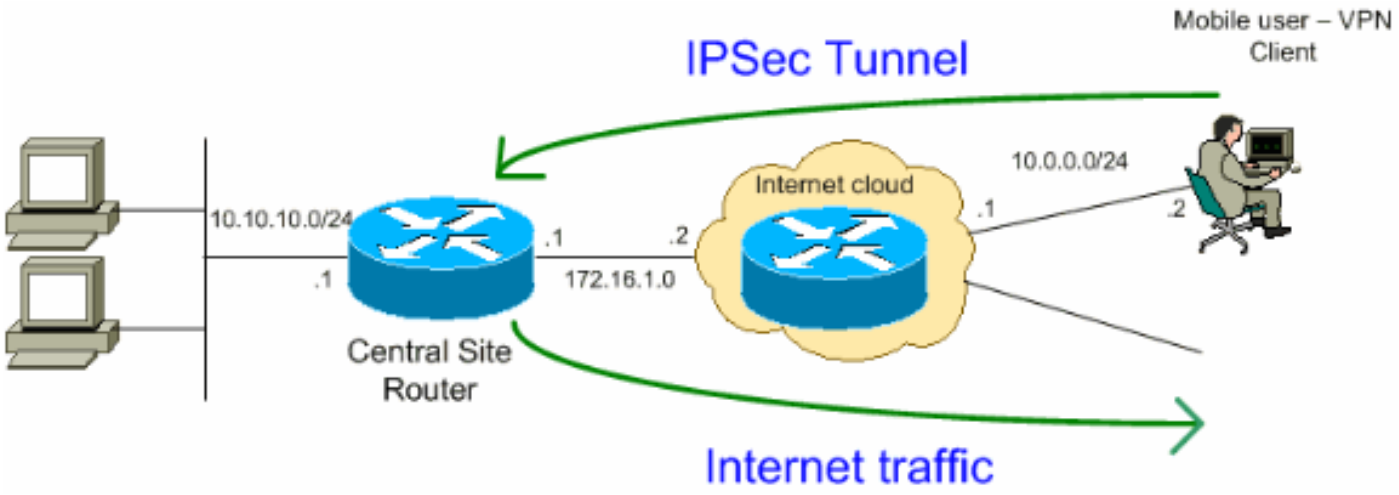
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918 ，已在實驗室環境中使用。

組態

本檔案會使用以下設定：

- 路由器
- Cisco VPN使用者端

路由器

```
 VPN#show run
Building configuration...

Current configuration : 2170 bytes
!
```

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
!
boot-start-marker
boot-end-marker
!
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.


aaa authentication login userauthen local

!--- In order to enable group authorization, enable !---
the aaa authorization commands.

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!--- For local authentication of the IPsec user, !---
create the user with a password. username user password
0 cisco
!
!
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2

!--- Create a group that is used to specify the !---
WINS and DNS server addresses to the VPN Client, !---
along with the pre-shared key for authentication. crypto
isakmp client configuration group vpnclient
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!

!--- Create a dynamic map and apply !--- the transform
set that was created earlier. crypto dynamic-map dynmap
10
 set transform-set myset
 reverse-route
```

```
!

!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
!--- Create the loopback interface for the VPN user
traffic . interface Loopback0
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
 ip nat inside

!--- Apply the crypto map on the interface. interface
FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip policy route-map VPN-Client
 duplex auto
 speed auto
 crypto map clientmap
!
interface Serial2/0
 no ip address
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ! ip local pool ippool 192.168.1.1
192.168.1.2
ip http server
no ip http secure-server
!
ip route 10.0.0.0 255.255.255.0 172.16.1.2
!--- Enables Network Address Translation (NAT) !--- of
the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address. ip
nat inside source list 101 interface FastEthernet1/0
overload
!
!--- The access list is used to specify which traffic is
to be translated for the !--- outside Internet. access-
```

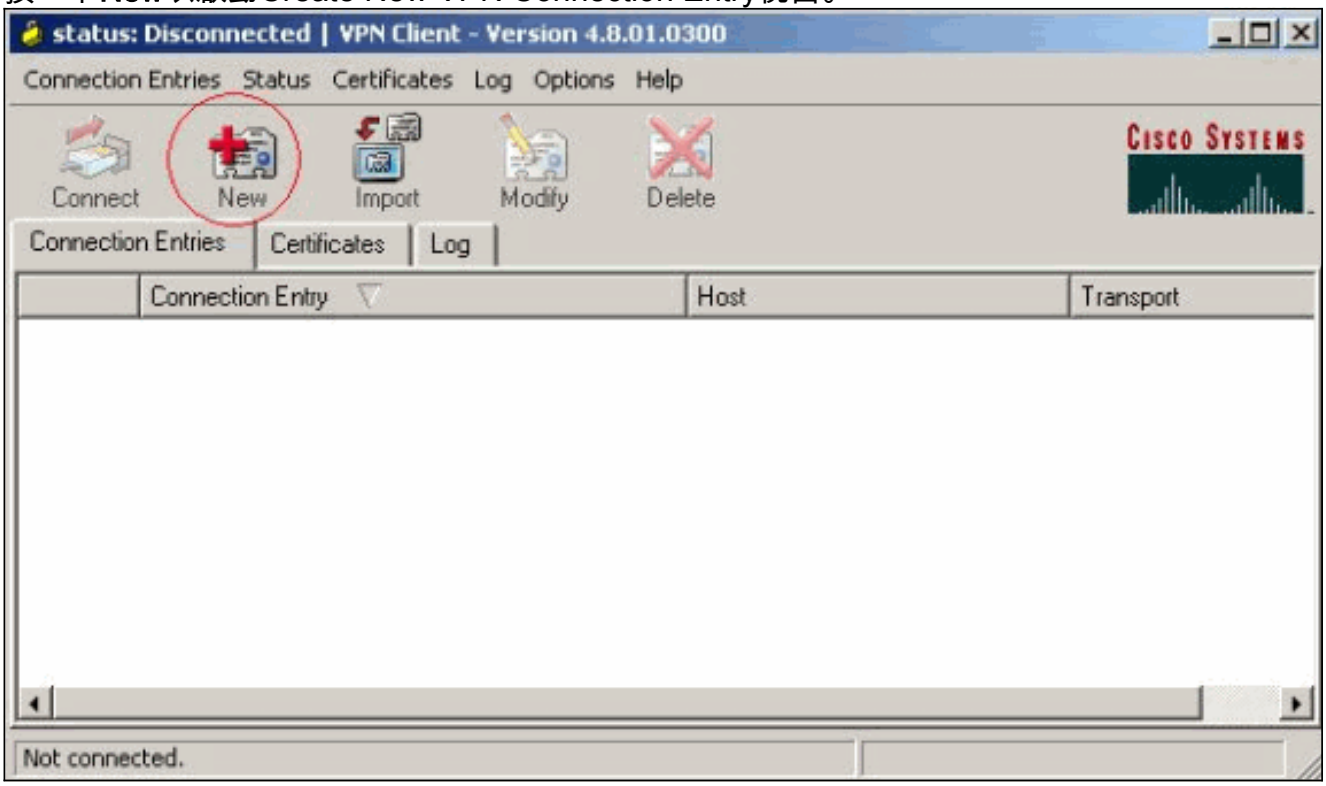
```
list 101 permit ip any any

!--- Interesting traffic used for policy route. access-
list 144 permit ip 192.168.1.0 0.0.0.255 any
!--- Configures the route map to match the interesting
traffic (access list 144) !--- and routes the traffic to
next hop address 10.11.0.2. ! route-map VPN-Client
permit 10
 match ip address 144
 set ip next-hop 10.11.0.2
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end
```

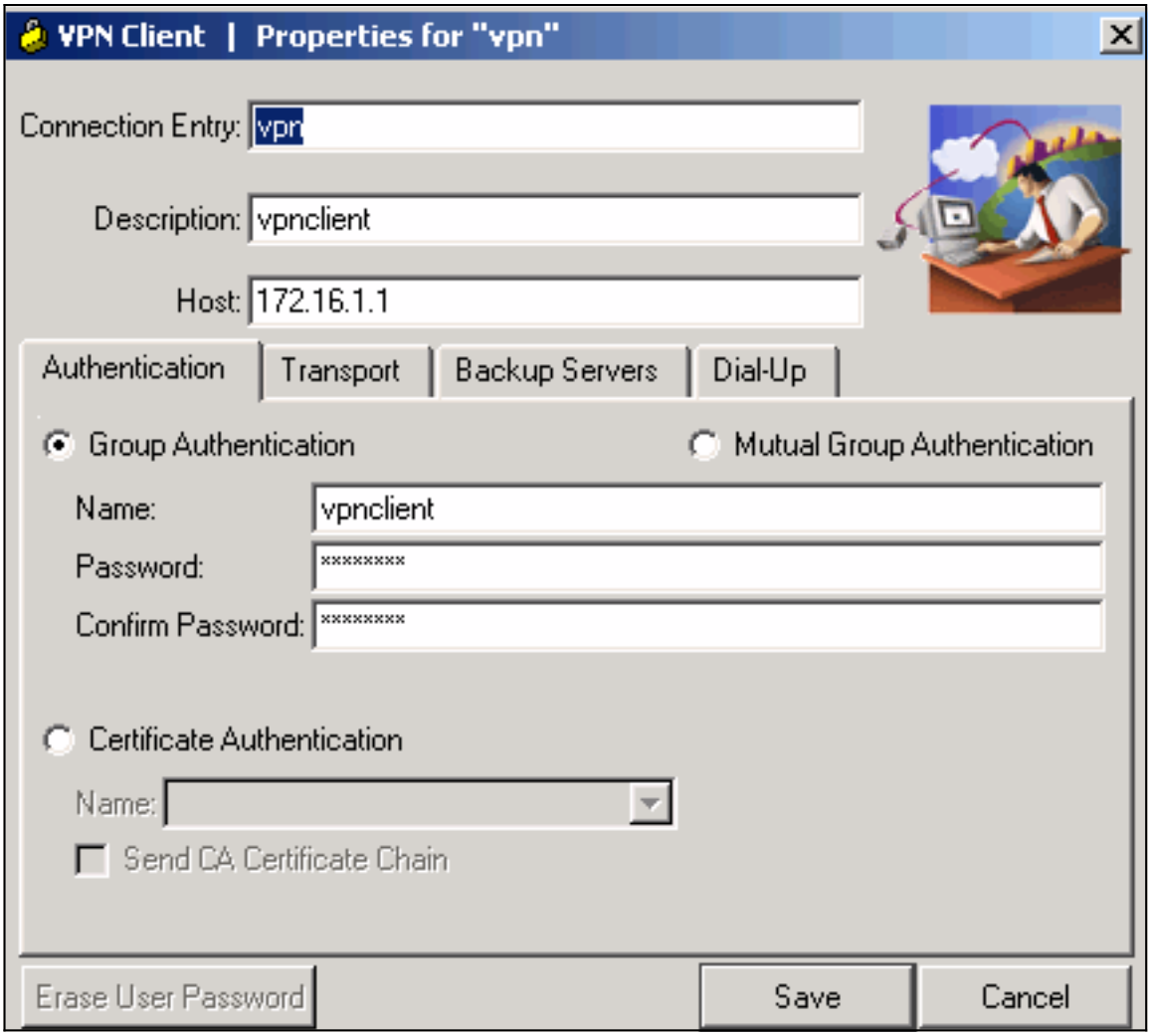
VPN客戶端4.8配置

完成以下步驟以配置VPN客戶端4.8。

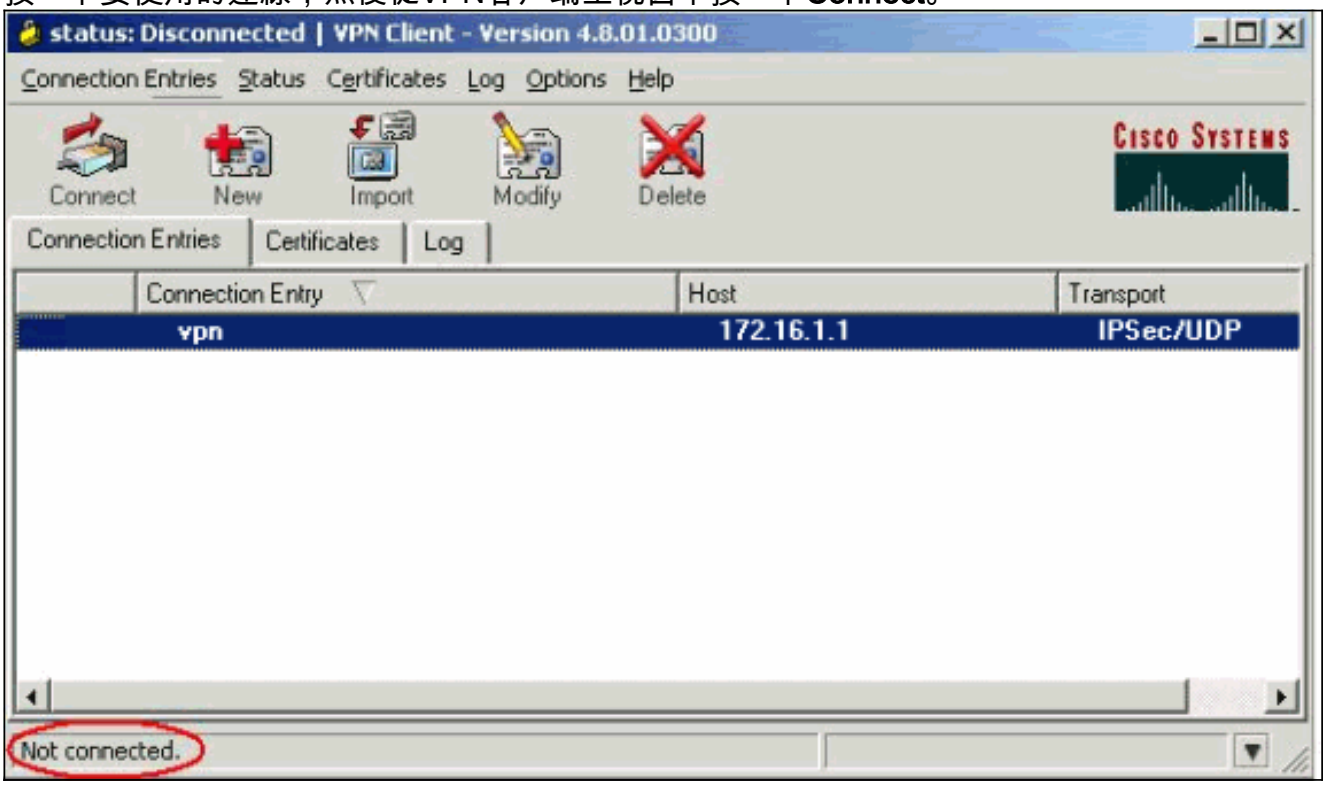
1. 選擇**Start > Programs > Cisco Systems VPN Client > VPN Client**。
2. 按一下**New**以啟動Create New VPN Connection Entry視窗。



3. 輸入連線條目的名稱和說明，在主機框中輸入路由器的外部IP地址，然後輸入VPN組的名稱和密碼。按一下「**Save**」。

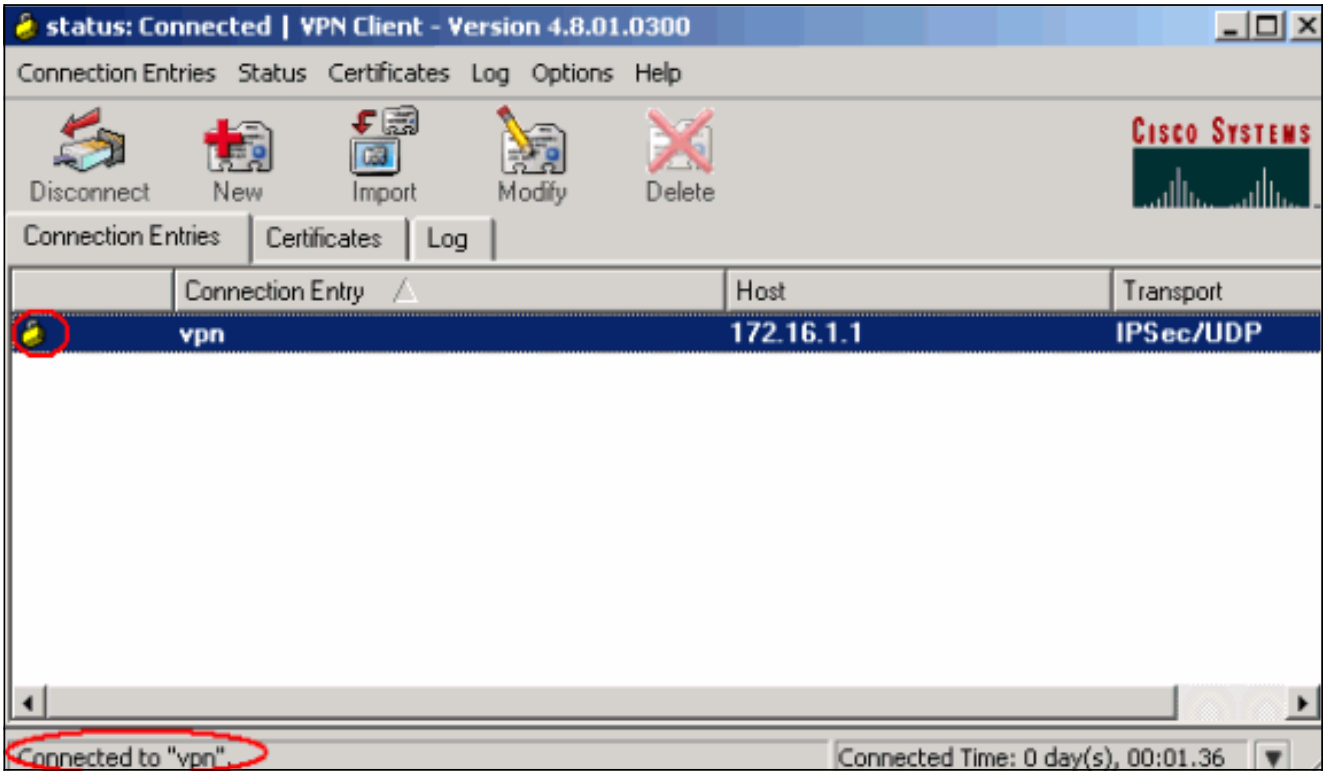


4. 按一下要使用的連線，然後從VPN客戶端主視窗中按一下**Connect**。

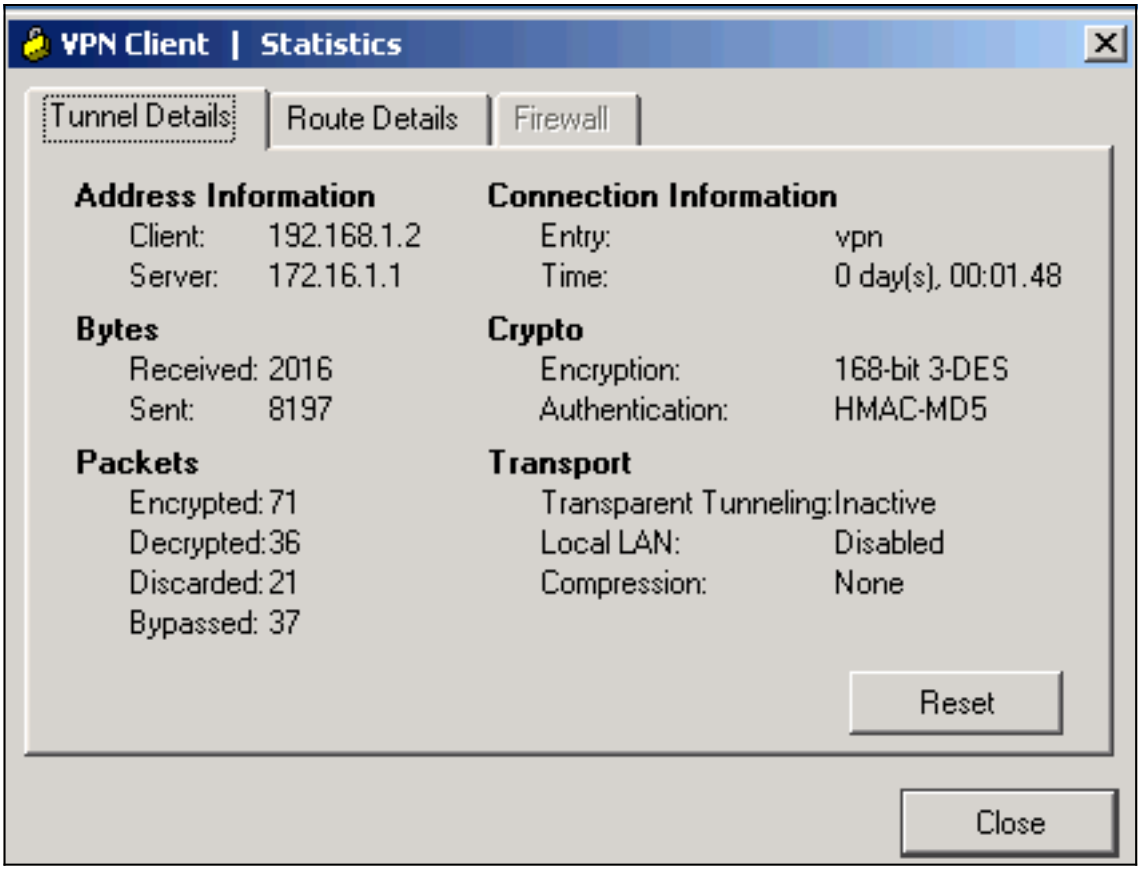


5. 出現提示時，輸入Xauth的使用者名稱和密碼資訊，然後按一下**OK**以連線到遠端網路。

6. VPN客戶端與中心站點的路由器連線。



7. 選擇**Status > Statistics**以檢查VPN客戶端的隧道統計資訊。



驗證

本節提供的資訊可用於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。

- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE安全關聯(SA)。

```
VPN#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: clientmap, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={}
    #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270
    #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270
    #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.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0xEF7C20EA(4017889514)

     inbound esp sas:
      spi: 0x17E0CBEC(400608236)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
```

```
    conn id: 2001, flow_id: SW:1, crypto map: clientmap
    sa timing: remaining key lifetime (k/sec): (4530341/3288)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xEF7C20EA(4017889514)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: SW:2, crypto map: clientmap
    sa timing: remaining key lifetime (k/sec): (4530354/3287)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

  outbound ah sas:

  outbound pcp sas:
```

- **show crypto ipsec sa** — 顯示當前SA使用的設定。

```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        QM_IDLE              15    0 ACTIVE
```

疑難排解

疑難排解指令

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。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug crypto ipsec** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。

相關資訊

- IPSec 協商/IKE 通訊協定
- Cisco VPN使用者端 — 產品支援
- 思科路由器 — 產品支援
- 技術支援與文件 - Cisco Systems