如何使用AES將Cisco VPN客戶端配置為PIX

目錄

簡介

此示例配置說明如何使用高級加密標準(AES)進行加密，設定從Cisco VPN客戶端到PIX防火牆的遠端訪問VPN連線。此示例使用Cisco Easy VPN設定安全通道，並將PIX防火牆配置為Easy VPN伺服器。

在Cisco Secure PIX防火牆軟體版本6.3及更高版本中，支援新的國際加密標準AES來保護站點到站點和遠端訪問VPN連線的安全。這是對資料加密標準(DES)和3DES加密演算法的補充。PIX防火牆支援128、192和256位的AES金鑰大小。

從Cisco VPN Client 3.6.1版開始，VPN Client支援AES作為加密演算法。VPN Client僅支援128位和256位的金鑰大小。

必要條件

需求

此示例配置假定PIX完全可操作，並配置必要的命令以便根據組織的安全策略處理流量。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本6.3(1)**注意：**此安裝程式已在PIX軟體版本6.3(1)上測試，預計可以在所有更高版本上運行。

- Cisco VPN使用者端版本4.0.3(A)**注意：**此安裝程式已在VPN客戶端4.0.3(A)版上測試，但可在早期3.6.1版本和最新版本上運行。

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。

背景資訊

遠端訪問VPN滿足移動工作人員安全地連線到組織網路的要求。移動使用者可以使用其PC上安裝的VPN客戶端軟體設定安全連線。VPN客戶端發起與配置為接受這些請求的中央站點裝置的連線。在本示例中，中心站點裝置是配置為Easy VPN伺服器的PIX防火牆，該伺服器使用動態加密對映。

Cisco Easy VPN通過簡化VPN的配置和管理來簡化VPN部署。它包括Cisco Easy VPN Server和Cisco Easy VPN Remote。在Easy VPN Remote上需要最少配置。Easy VPN Remote發起連線。如果身份驗證成功，Easy VPN伺服器會將VPN配置推送到它。有關如何將PIX防火牆配置為Easy VPN伺服器的詳細資訊，請參閱管理VPN遠端訪問。

當設定VPN所需的某些引數無法預先確定時，動態加密對映用於IPsec配置，獲取動態分配的IP地址的移動使用者的情況也是如此。動態加密對映用作模板，丟失的引數在IPsec協商期間確定。有關動態加密對映的詳細資訊，請參閱動態加密對映。

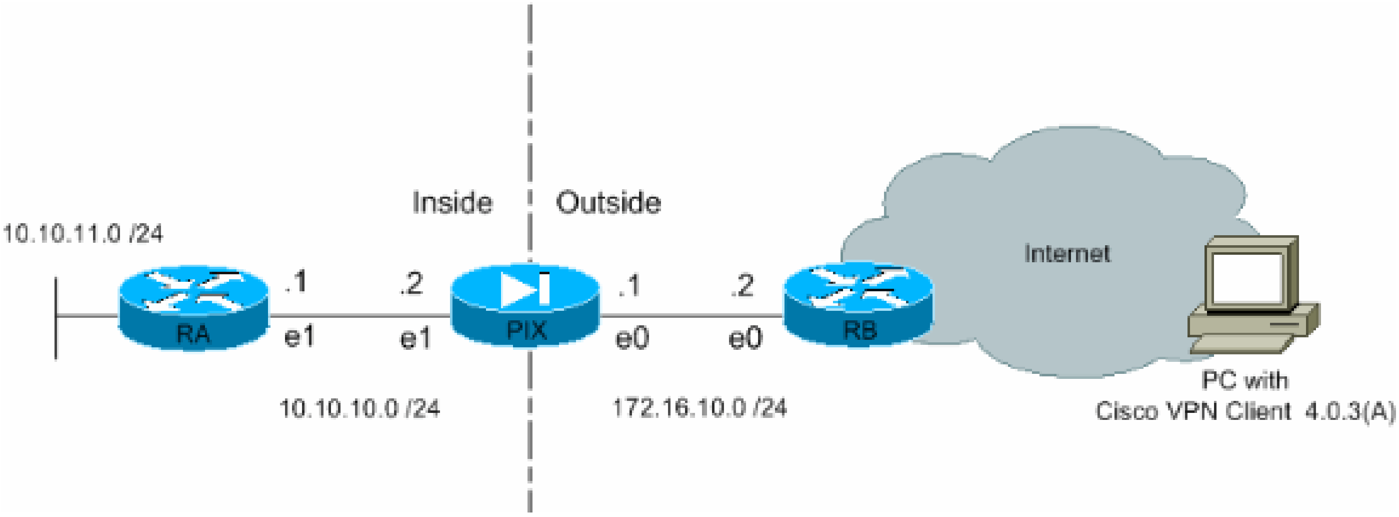
組態

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：



配置PIX

PIX防火牆所需的配置如以下輸出所示。該配置僅用於VPN。

PIX

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names

!--- Define the access list to enable split tunneling.
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
Define the access list to avoid network address !---
translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
255.255.255.0 access-list 102 permit ip 10.10.11.0
255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
Create a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history
enable arp timeout 14400 !--- Disable NAT for IPsec
packets. nat (inside) 0 access-list 102 route outside
0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0
255.255.255.0 10.10.10.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Permit packet that came from an IPsec tunnel
to pass through without !--- checking them against the
configured conduits/access lists. sysopt connection
permit-ipsec !--- Define the transform set to be used
during IPsec !--- security association (SA) negotiation.
Specify AES as the encryption algorithm. crypto ipsec
```

```
transform-set trmset1 esp-aes-256 esp-sha-hmac !---
Create a dynamic crypto map entry !--- and add it to a
static crypto map. crypto dynamic-map map2 10 set
transform-set trmset1 crypto map map1 10 ipsec-isakmp
dynamic map2 !--- Bind the crypto map to the outside
interface. crypto map map1 interface outside !--- Enable
Internet Security Association and Key Management !---
Protocol (ISAKMP) negotiation on the interface on which
the IPsec !--- peer communicates with the PIX Firewall.
isakmp enable outside isakmp identity address !---
Define an ISAKMP policy to be used while !---
negotiating the ISAKMP SA. Specify !--- AES as the
encryption algorithm. The configurable AES !--- options
are aes, aes-192 and aes-256. !--- Note: AES 192 is not
supported by the VPN Client.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- Create a VPN group and configure the policy
attributes which are !--- downloaded to the Easy VPN
Clients. vpngroup groupmarketing address-pool vpnpool1
vpngroup groupmarketing dns-server 10.10.11.5 vpngroup
groupmarketing wins-server 10.10.11.5 vpngroup
groupmarketing default-domain org1.com vpngroup
groupmarketing split-tunnel 101 vpngroup groupmarketing
idle-time 1800 vpngroup groupmarketing password ********
telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421ee1c3 : end
```

注意：在此設定中，建議在配置轉換集或ISAKMP策略時不要指定aes-192。VPN客戶端不支援加密aes-192。

注意：在早期版本中，需要使用IKE模式配置命令**isakmp client configuration address-pool**和**crypto map client-configuration address**。但是，對於較新版本（3.x及更高版本），這些命令不再必要。現在可以使用**vpngroup address-pool**命令指定多個地址池。

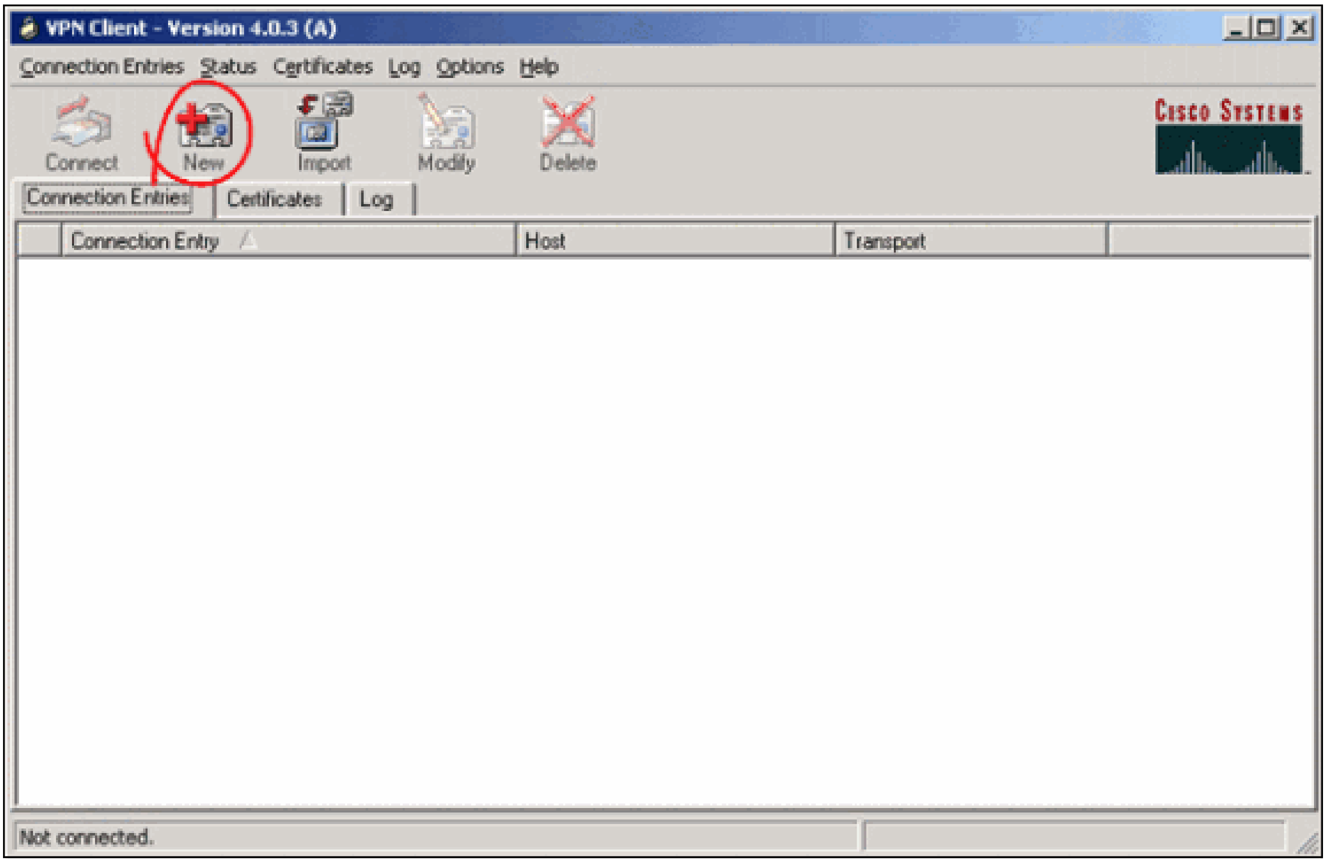
注意：VPN組名稱區分大小寫。這意味著，如果PIX中指定的組名稱和VPN客戶端上的組名稱在字母大小寫方面不同（大寫或小寫），則使用者身份驗證失敗。

註：例如，當您在一個裝置上將組名稱輸入為**GroupMarketing**，而在另一個設**備中**將組名稱輸入為**GroupMarketing**時，裝置無法工作。

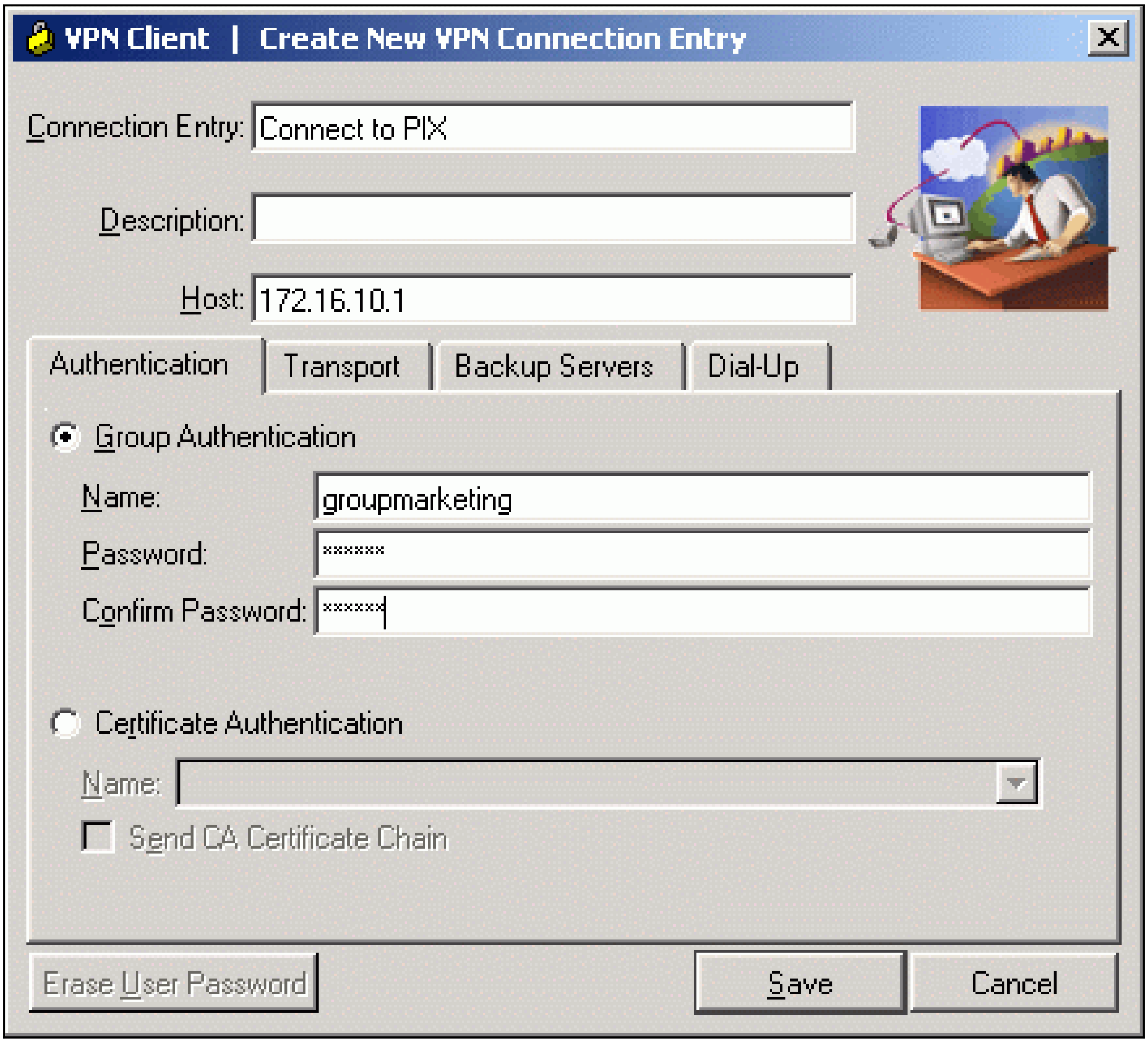
配置VPN客戶端

在PC上安裝VPN客戶端後，按以下步驟建立新連線：

1. 啟動VPN客戶端應用程式，然後按一下**New**以建立新的連線條目。



2. 標題為VPN客戶端的新對話方塊 |建立新VPN連線條目。輸入新連線的配置資訊。在Connection Entry欄位中，為建立的新條目分配名稱。在Host欄位中，鍵入PIX公共介面的IP地址。選擇Authentication頁籤，然後鍵入組名稱和密碼（兩次 — 用於確認）。 這需要與使用**vpngroup password**命令在PIX上輸入的資訊相匹配。按一下**Save**以儲存輸入的資訊。現在已建立新連線。



VPN Client | Create New VPN Connection Entry

Connection Entry: Connect to PIX

Description:

Host: 172.16.10.1

● Group Authentication

Name: groupmarketing

Password: ******

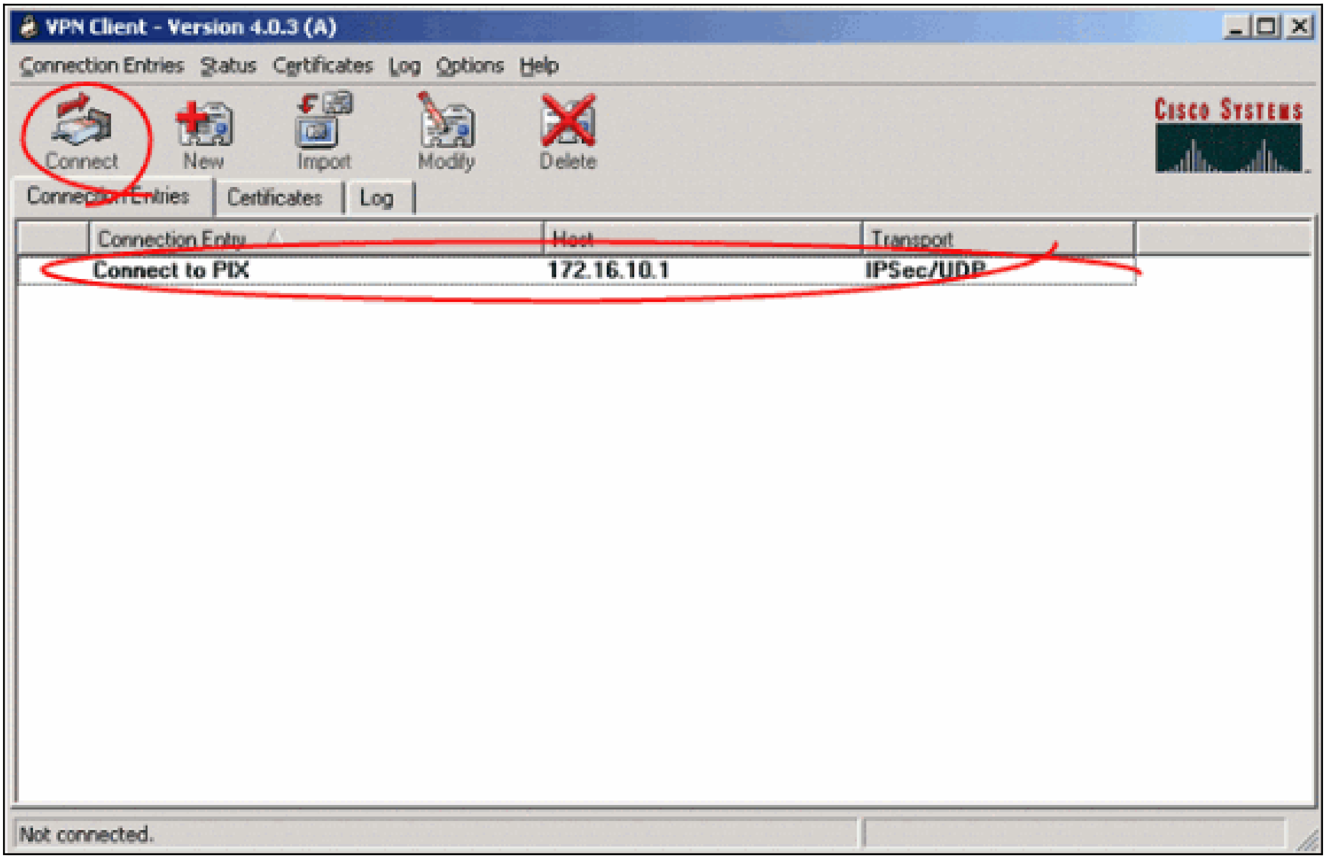
Confirm Password: ******

○ Certificate Authentication

Name:

□ Send CA Certificate Chain

3. 若要使用新的連線條目連線到網關，請通過按一下連線條目一次選擇該連線條目，然後按一下**連線**圖示。按兩下連線條目具有相同的效果。



VPN Client - Version 4.0.3 (A)

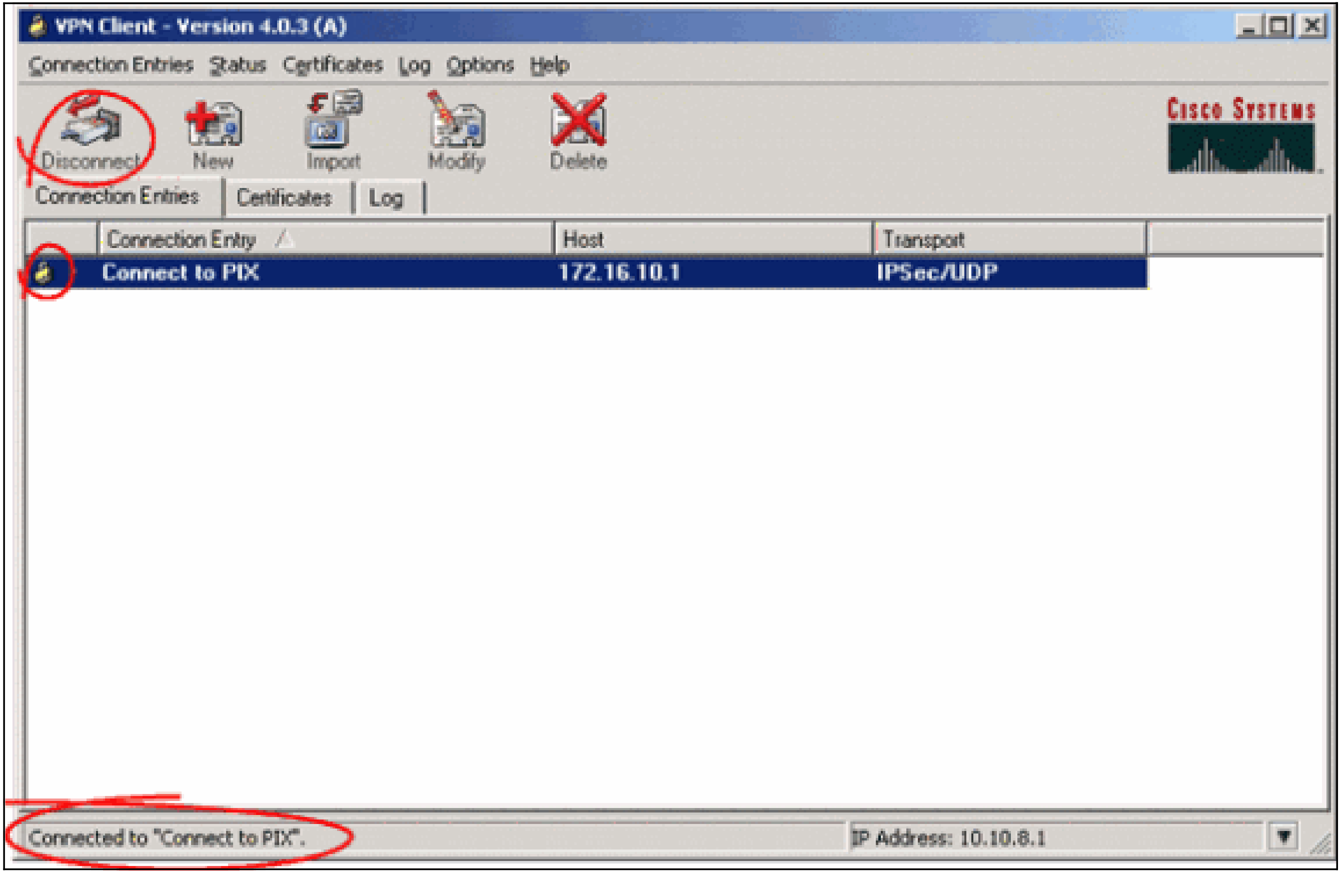
Connection Entry	Host	Transport
Connect to PIX	172.16.10.1	IPSec/UDP

Not connected.

驗證

在VPN客戶端上，以下專案指示已成功建立到遠端網關的連線：

- 活動連線條目上會顯示一個黃色的閉鎖圖示。
- 工具欄上的「連線」圖示（「連線條目」頁籤旁邊）更改為「斷開連線」。
- 視窗結束處的狀態行顯示為「Connected to」，後跟連線條目名稱。


VPN Client - Version 4.0.3 (A)
Connection Entries Status Certificates Log Options Help
Disconnect
New
Import
Modify
Delete
Cisco Systems
Connection Entries
Certificates
Log

	Connection Entry	Host	Transport
🔒	Connect to PIX	172.16.10.1	IPSec/UDP

Connected to "Connect to PIX".
IP Address: 10.10.8.1

注意：預設情況下，一旦建立連線，VPN客戶端將最小化至Windows工作列右下角的系統托盤中的閉鎖圖示。按兩下closed-lock圖示以使VPN客戶端視窗再次可見。

在PIX防火牆上，這些**show**命令可用於驗證已建立連線的狀態。

注意： Output Interpreter Tool(**僅供**註冊客戶使用)支援某些**show**命令，這允許您檢視**show**命令輸出的分析。

- **show crypto ipsec sa** — 顯示PIX上的所有當前IPsec SA。此外，輸出還顯示遠端對等裝置的實際IP地址、分配的IP地址、本地IP地址和介面以及應用的加密對映。

```
Pixfirewall#show crypto ipsec sa

interface: outside
    Crypto map tag: map1, local addr. 172.16.10.1

   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0)
   current_peer: 172.16.12.3:500
   dynamic allocated peer ip: 10.10.8.1

     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.12.3
     path mtu 1500, ipsec overhead 64, media mtu 1500
     current outbound spi: cbabd0ce

     inbound esp sas:
      spi: 0x4d8a971d(1300928285)
        transform: esp-aes-256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: map1
        sa timing: remaining key lifetime (k/sec): (4607996/28685)
        IV size: 16 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0xcbabd0ce(3417034958)
        transform: esp-aes-256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: map1
        sa timing: remaining key lifetime (k/sec): (4608000/28676)
        IV size: 16 bytes
        replay detection support: Y


     outbound ah sas:


     outbound pcp sas:
```

- **show crypto isakmp sa** — 顯示對等體之間構建的ISAKMP SA的狀態。

```
Pixfirewall#show crypto isakmp sa
Total      : 1
Embryonic : 0
        dst               src        state      pending     created
     172.16.10.1      172.16.12.3    QM_IDLE          0           1
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

這些debug命令有助於排除VPN設定問題。

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

- **debug crypto isakmp** — 顯示已構建的ISAKMP SA和已協商的IPsec屬性。在ISAKMP SA協商期間，PIX可能會在接受ISAKMP SA協商之前將多個建議作為「不可接受」丟棄。一旦同意ISAKMP SA，就會協商IPsec屬性。同樣，在某個建議被接受之前，可能會拒絕該多個建議，如**debug**輸出所示。

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- Proposal is rejected since extended auth is not configured. ISAKMP (0): atts are not
acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- Proposal is rejected since MD5 is not specified as the hash algorithm. ISAKMP (0): atts
are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- This proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are
acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
!--- Output is suppressed. OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3348522173

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      key length is 256
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
!--- This proposal is not accepted since transform-set !--- trmset1 does not use MD5. ISAKMP
(0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      key length is 256
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
!--- This proposal is accepted since it matches !--- transform-set trmset1. ISAKMP (0): atts
are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 3
!--- Output is suppressed.
```

- **debug crypto ipsec** — 顯示有關IPsec SA協商的資訊。

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with     172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
        from     172.16.12.3 to     172.16.10.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4
```

使用本文檔中顯示的配置，VPN客戶端能夠使用AES成功連線到中心站點PIX。有時會觀察到，雖然VPN隧道已成功建立，但使用者無法執行常見任務，例如ping網路資源、登入到域或瀏覽網路鄰居。有關排除此類問題的詳細資訊，請參閱使用Cisco VPN客戶端建立VPN隧道後Microsoft網路鄰居故障排除。

相關資訊

- **進階加密標準(AES)**
- **IP安全(IPSec)加密簡介**
- **IP安全性疑難排解 — 瞭解和使用debug命令**
- **IPsec協商/IKE通訊協定支援頁面**
- **PIX支援頁**
- **Cisco VPN使用者端支援頁面**
- **PIX命令參考**
- **技術支援與文件 - Cisco Systems**