如何配置Cisco VPN客户端到PIX用AES

目录

简介

此示例配置显示如何使用高级加密标准(AES)加密法，从Cisco VPN客户端设置到PIX防火墙的远程访问虚拟专用网连接。此示例使用 Cisco Easy Vpn 设置安全信道，并将 PIX 防火墙配置为 Easy VPN 服务器。

在 Cisco 安全 PIX 防火墙软件版本 6.3 和更高版本中，支持新的国际加密标准 AES，以确保站点到站点和远程访问 VPN 连接的安全。这是除数据加密标准 (DES) 和 3DES 加密算法之外的算法。PIX 防火墙支持 AES 密钥大小 128、192 和 256 位。

VPN客户端支持AES作为从Cisco VPN客户端版本3.6.1开始的加密算法。VPN客户端仅支持128位和256位的密钥大小。

先决条件

要求

此配置示例假设 PIX 可完全运行并已配置必要命令，以便根据组织的每个安全策略来处理流量。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 软件版本 6.3(1)**注意：**此设置已在PIX软件版本6.3(1)上测试，预期可在所有更高版本上使用。

- Cisco VPN 客户端 4.0.3(A) 版**注意**：此设置已在VPN客户端版本4.0.3(A)上测试，但在早期版本（早于3.6.1版本）和当前版本之前均可使用。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

远程访问 VPN 满足了移动工作者的安全连接组织网络的需要。移动用户可以使用安装在其 PC 机上的 VPN 客户端软件来建立安全连接。VPN 客户端将会向已配置为接受这些请求的中心站点设备发起连接。在本例中，中心站点设备是配置为Easy VPN服务器的PIX防火墙，此服务器使用动态加密映射。

Cisco Easy VPN 通过简化 VPN 的配置和管理简化了 VPN 部署。它包括 Cisco Easy VPN Server 和 Cisco Easy VPN Remote。Easy VPN Remote 中需要进行最低配置。Easy VPN Remote 将启动连接。如果身份验证成功，Easy VPN Server 会为其提供 VPN 配置。管理 VPN 远程访问中提供了有关如何将 PIX 防火墙配置为 Easy VPN 服务器的详细信息。

当设置 VPN 所需的某些参数无法预先确定时，可将动态加密映射用于 IPSec 配置，移动用户获取动态分配的 IP 地址便属于这种情况。动态加密映射用作一个模板，并在 IPsec 协商期间确定缺少的参数。动态加密映射中提供了关于动态加密映射的详细信息。

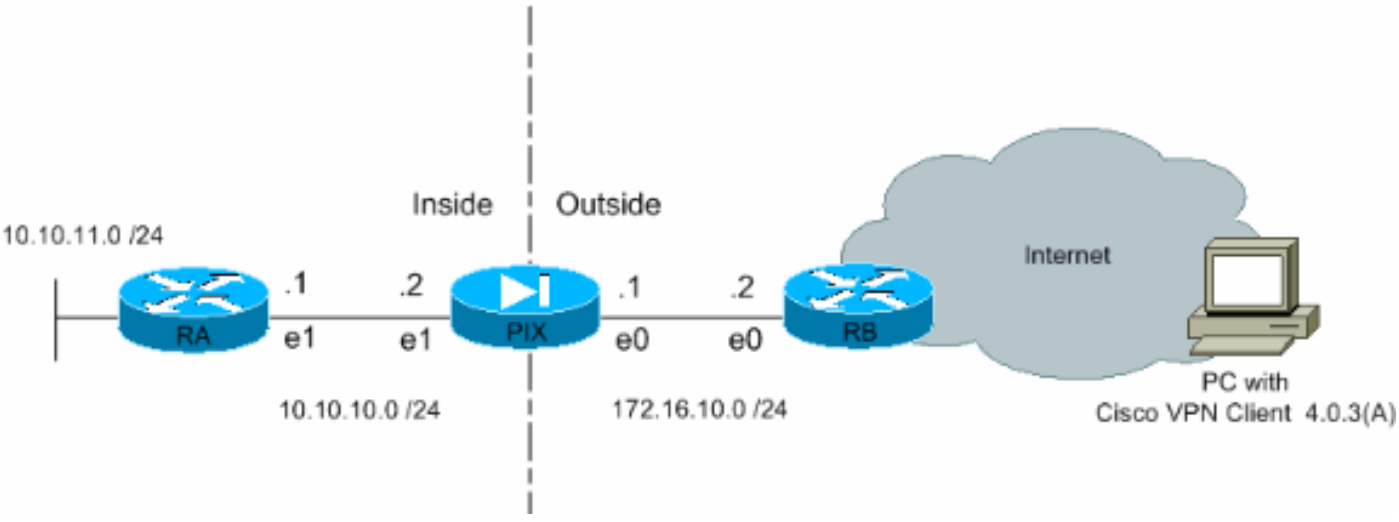
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置 PIX

此输出中显示了 PIX 防火墙所需要的配置。该配置仅用于 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：在此设置中，建议在配置转换集或ISAKMP策略时不要指定aes-192。VPN 客户端不支持 aes-192 加密。

注意：对于早期版本，IKE模式配置命令isakmp client configuration address-pool和**crypto map client-configuration地址是必**需的。但是，在较新版本（3.x 和更高版本）中，不必再使用这些命令。现在，可以使用 **vpngroup address-pool 命令指定多个地址池。**

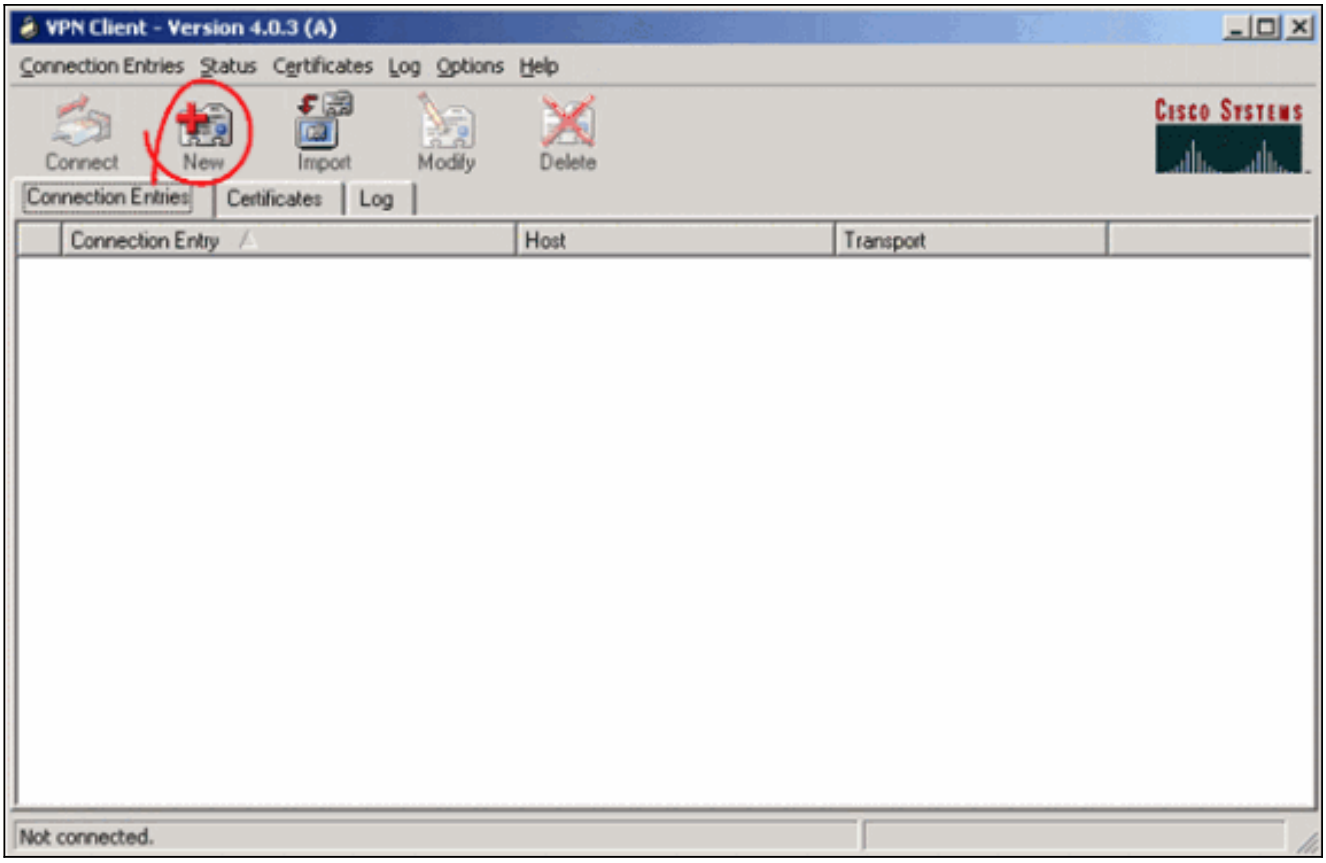
注意：VPN组名称区分大小写。这意味着，如果在 PIX 中指定的组名称与 VPN 客户端上的组名称的大小写形式不同（大写或小写），用户身份验证将失败。

注：**例**如，在一台设备中输入组名称**为**GroupMarketing，在另**一台**设备中输入组营销时，设备不工作。

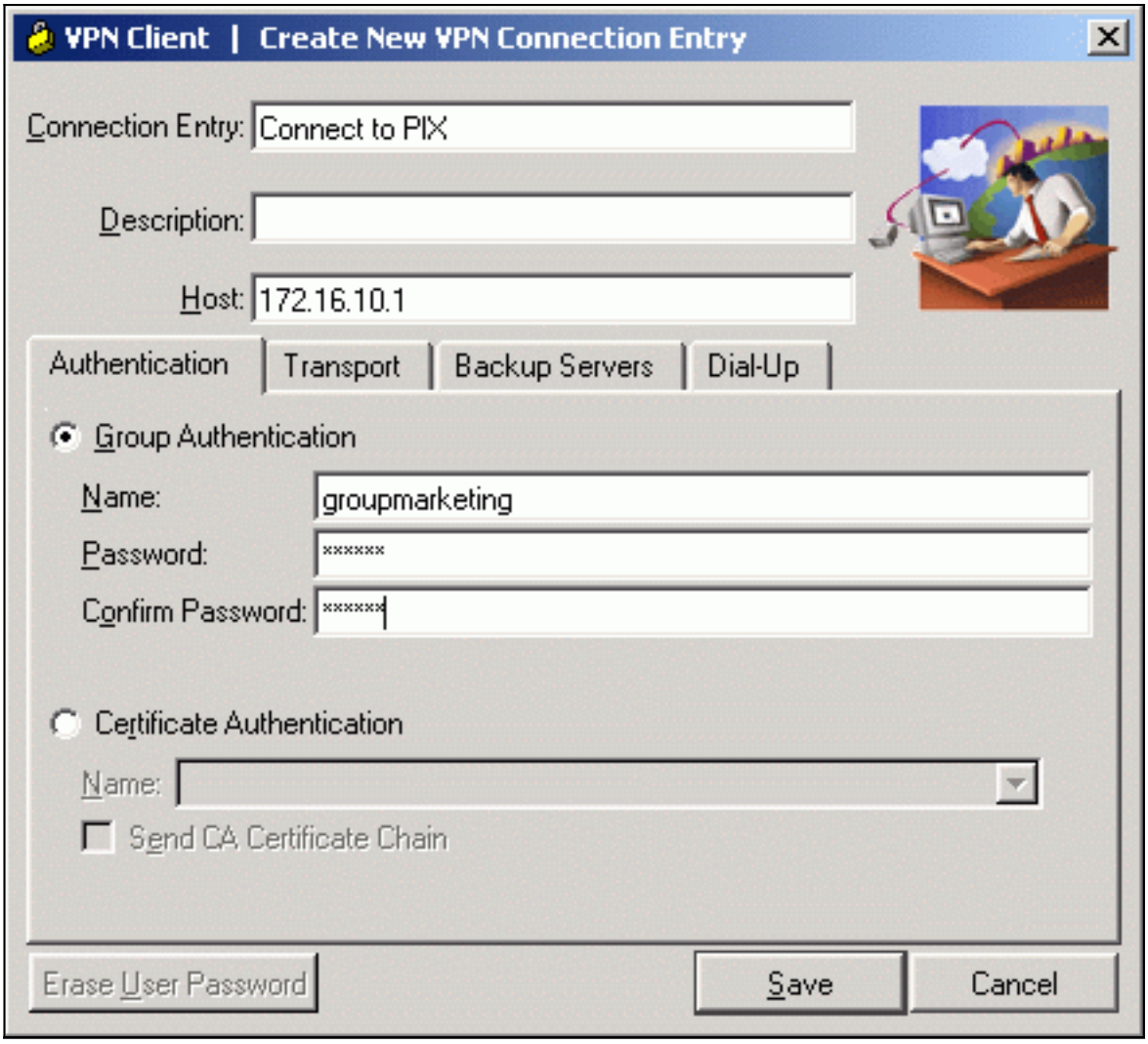
配置 VPN 客户端

在 PC 上安装 VPN 客户端后，请如以下步骤所示创建新连接：

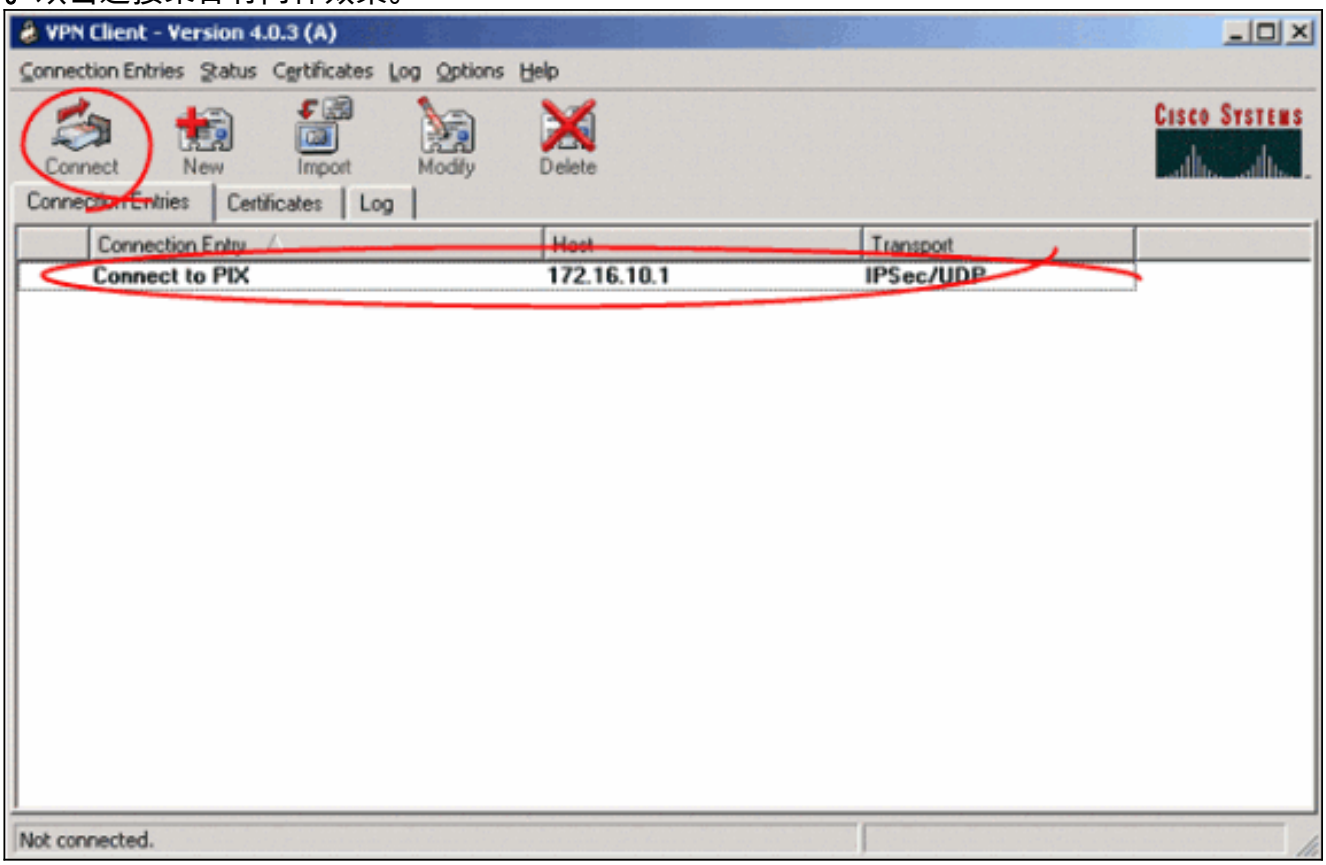
1. 启动 VPN 客户端应用程序并单击 **New 创建新连接条目。**



2. 标题为 VPN 客户端的新对话框 |将显示Create New VPN Connection Entry。输入新连接的配置信息。在 Connection Entry 字段，为创建的新条目分配名称。在 Host 字段中，键入 PIX 的公共接口的 IP 地址。选择 Authentication 选项卡，然后键入组名称和密码（两次，以供确认）。 此信息需要与使用 **vpngroup password 命令在 PIX 中输入的信息匹配。**点击 **Save 保存输入的信息。**现在已创建新连接。



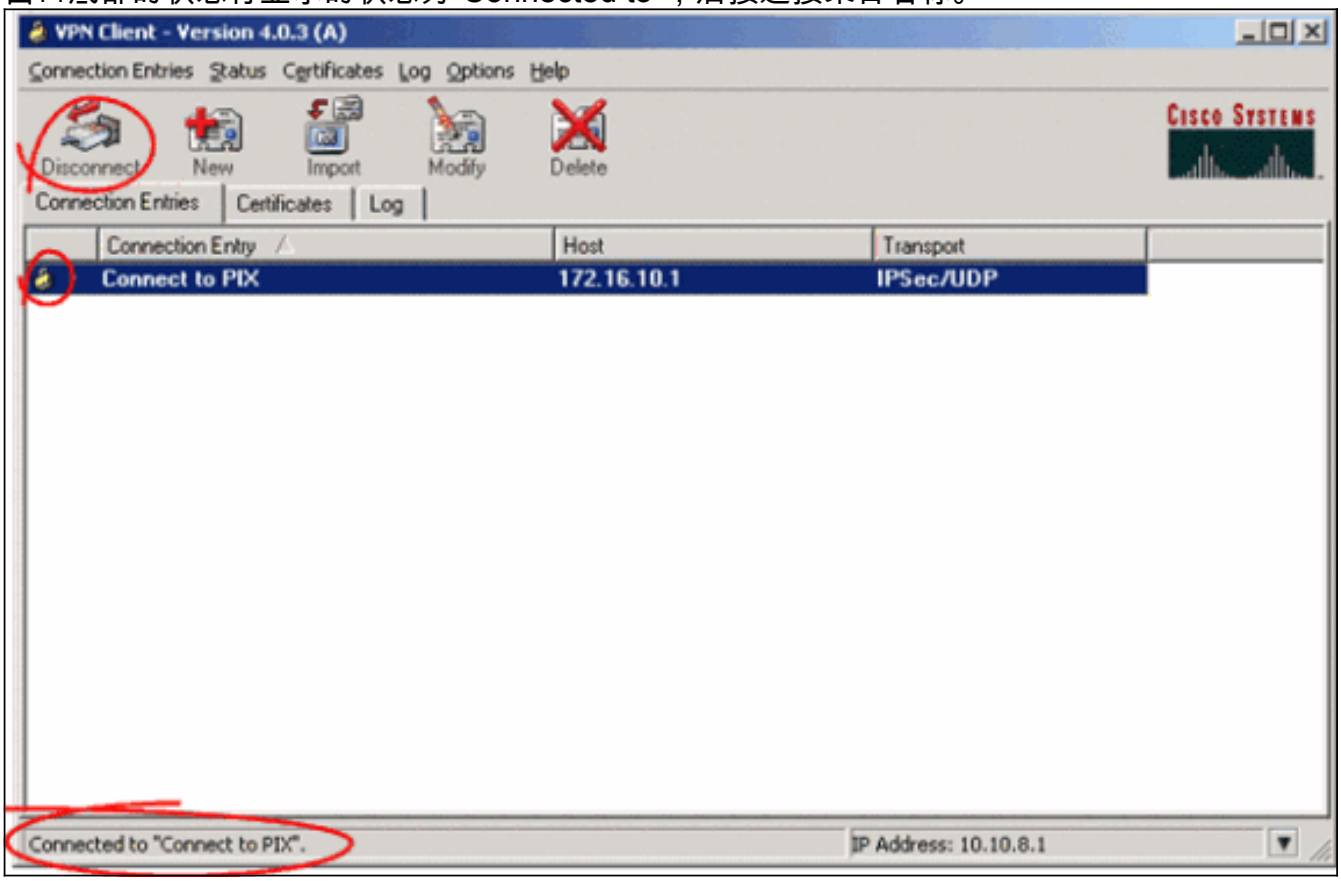
3. 为了使用新连接条目连接网关，请通过单击一次选择该连接条目，然后再单击 **Connect 图标**。双击连接条目有同样效果。



验证

在 VPN 客户端上，成功建立的与远程网关的连接由以下各项来指示：

- 黄色闭合锁定图标表示活动连接条目。
- 工具栏上的 Connect 图标（在 Connection Entries 选项卡旁边）更改为 Disconnect。
- 窗口底部的状态行显示的状态为“Connected to”，后接连接条目名称。



注意：默认情况下，一旦建立连接，VPN客户端将最小化为Windows任务栏右下角系统托盘中的关闭锁定图标。双击闭合锁定图标，以便再次显示 VPN Client 窗口。

在 PIX 防火墙上，可以使用以下 **show 命令来验证已建立连接的状态。**

注意：某些**show**命令受Output Interpreter Tool（仅注册客户）支持（仅限注册客户），它允许您查看对show命令输出的分**析。**

- **show crypto ipsec sa — 显示 PIX 上所有当前的 IPsec SA。**此外，输出显示远端对等体的实际IP地址、分配的IP 地址、本地IP地址和接口及应用的加密映射等。

```
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 — 显示在对等体之间构建的 ISAKMP SA 的状态。**

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

这些调试指令能协助解决 VPN 设置存在的问题。

注意：在发出debug命令之前，请参阅有关Debug命**令的**重要信息。

- **debug crypto isakmp — 显示构建的 ISAKMP SA 和协商的 IPSec 属性。**在 ISAKMP SA 协商过程中，PIX 在接受某个建议之前，可能会将若干个建议视为“不可接受”而丢弃。一旦同意 ISAKMP SA，就协商了 IPSec 属性。同样，在接受一个建议之前，可能会拒绝若干个建议，如此**调试输出中所示。**

```
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 — 显示有关 IPSec SA 协商的信息。**

```
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
```

使用本文档中显示的配置，VPN 客户端能够使用 AES 成功连接到中心站点 PIX。我们发现，有时候虽然已成功建立 VPN 隧道，但用户无法执行常见任务，如 ping 网络资源、登录到域或浏览网络邻居。在与 Cisco VPN 客户端建立 VPN 信道后解决 Microsoft 网络邻居的问题中提供了有关解决此类问题的详细信息。

相关信息

- 高级加密标准 (AES)
- IP 安全 (IPsec) 加密简介
- IP安全故障排除-了解和使用debug命令
- IPsec 协商/IKE 协议支持页
- PIX 支持页
- Cisco VPN 客户端支持页
- PIX 命令参考
- 技术支持和文档 - Cisco Systems