

Ipsec-PIX到Cisco VPN客户端的通配符，密钥共享，有扩展认证的模式配置

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[PIX 调试示例](#)

[使用VPN客户端4.x的调试](#)

[调试 VPN Client 1.1](#)

[相关信息](#)

简介

此配置示例演示如何使用通配符、模式配置、`sysopt connection permit-ipsec`命令和扩展身份验证(Xauth)将VPN客户端连接到PIX防火墙。

要查看PIX 6.3及更高版本的TACACS+和RADIUS配置，请参阅[PIX 6.3和PIX/ASA 7.x的TACACS+和RADIUS配置示例](#)。

VPN客户端支持高级加密标准(AES)作为Cisco VPN客户端版本3.6.1及更高版本以及PIX防火墙6.3中的加密算法。VPN客户端仅支持128位和256位的密钥大小。有关如何配置AES的详细信息，请参阅[如何使用AES配置Cisco VPN客户端到PIX](#)。

请参阅[PIX/ASA 7.x和Cisco VPN Client 4.x for Windows with Microsoft Windows 2003 IAS RADIUS身份验证配置示例](#)，以在Cisco VPN客户端(4.x for Windows)和PIX 500系列安全设备之间设置远程访问VPN连接7.x。

请参阅[使用 RADIUS 作为用户身份验证和记账方式在 VPN 3000 集中器和 VPN 客户端 4.x for Windows 之间建立 IPsec 的配置示例](#)，以了解如何使用 RADIUS 作为用户身份验证和记账方式在 Cisco VPN 3000 集中器和 Cisco VPN 客户端 4.x for Windows 之间建立 IPsec 隧道。

请参阅[使用 RADIUS 作为用户身份验证方式在 Cisco IOS 路由器和 Cisco VPN 客户端 4.x for](#)

[Windows 之间配置 IPsec，以了解如何使用 RADIUS 作为用户身份验证方式在路由器和 Cisco VPN 客户端 4.x for Windows 之间配置连接。](#)

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- 思科VPN客户端4.x.此产品具有高级VPN功能，与思科安全VPN客户端1.x不同。
- PIX防火墙515E版本6.3(3)。

注：加密技术受出口控制。您有责任了解与加密技术导出有关的法律。有关详情，请参阅[出口管理局网站](#)。如果您对导出控制有任何疑问，请发送电子邮件至 export@cisco.com。

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](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[背景信息](#)

`sysopt connection permit-ipsec` 命令隐式允许来自IPsec隧道的任何数据包绕过对IPsec连接的关联访问列表、`conduit`或`access-group` 命令的检查。Xauth向外部TACACS+或RADIUS服务器验证IPsec用户。除通配符预共享密钥外，用户还必须提供用户名/密码。

具有VPN客户端的用户从其ISP接收IP地址。这被来自PIX上IP地址池的IP地址替换。用户有权访问防火墙里面的一切，包括网络。不运行VPN客户端的用户只能使用静态分配提供的外部地址连接到Web服务器。

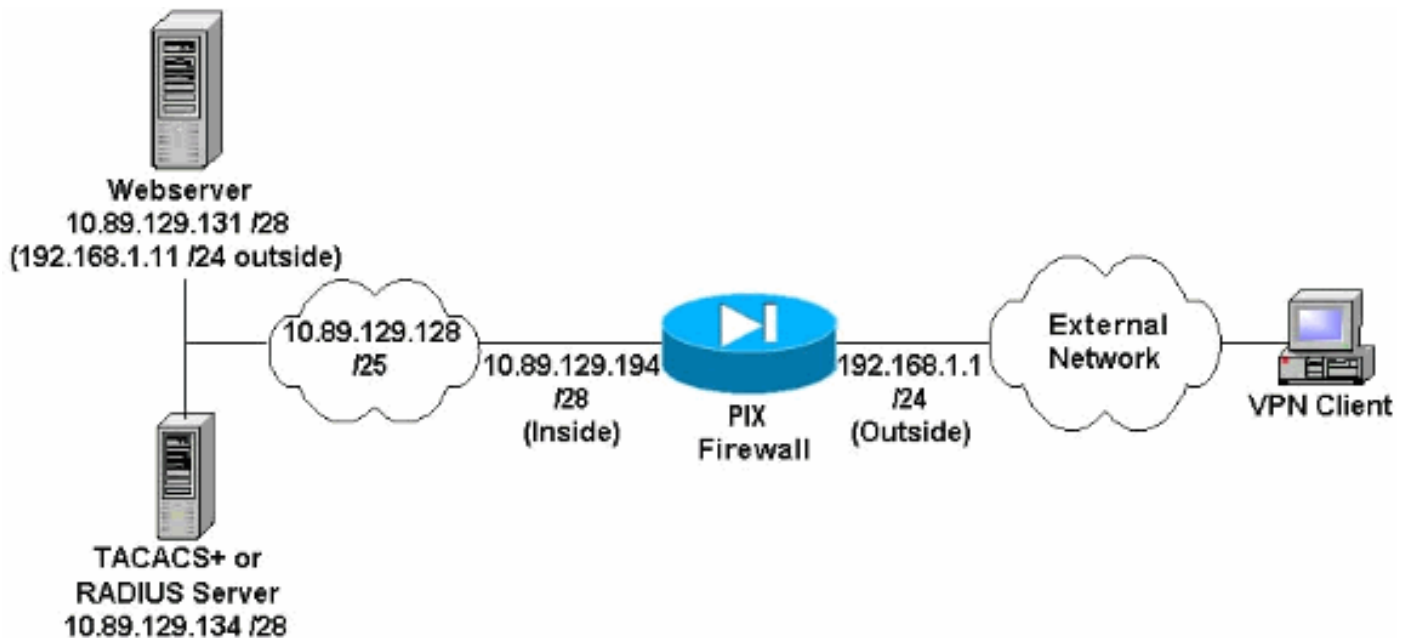
[配置](#)

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)可查找有关本文档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：



网络图说明

- 使用全局IP地址192.168.1.1访问Web服务器的Internet主机将进行身份验证，即使未建立VPN连接。此流量未加密。
- VPN客户端建立IPsec隧道后，即可访问内部网络(10.89.129.128 /25)上的所有主机。从VPN客户端到PIX防火墙的所有流量都已加密。如果没有IPsec隧道，则它们只能通过其全局IP地址访问Web服务器，但仍需要进行身份验证。
- VPN客户端来自Internet，其IP地址不是预先知道的。

配置

本文档使用以下配置。

- [PIX配置6.3\(3\)](#)
- [VPN客户端4.0.5配置](#)
- [VPN客户端3.5配置](#)
- [VPN客户端1.1配置](#)

PIX配置6.3(3)

```

pixfirewall#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 100full
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719

```

```

fixup protocol http 80
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
fixup protocol tftp 69
names
!--- Do not use Network Address Translation (NAT) for
inside-to-pool !--- traffic. This should not go through
NAT. access-list 101 permit ip 10.89.129.128
255.255.255.240 10.89.129.192 255.255.255.240 !---
Permits Internet Control Message Protocol (ICMP) !---
Transmission Control Protocol (TCP) and User Datagram
Protocol (UDP) !--- traffic from any host on the
Internet (non-VPN) to the web server. access-list 120
permit icmp any host 10.89.129.131 access-list 120
permit tcp any host 10.89.129.131 access-list 120 permit
udp any host 10.89.129.131 pager lines 24 mtu outside
1500 mtu inside 1500 ip address outside 192.168.1.1
255.255.255.0 ip address inside 10.89.129.194
255.255.255.240 ip audit info action alarm ip audit
attack action alarm !--- Specifies the inside IP address
range to be assigned !--- to the VPN Clients. ip local
pool VPNpool 10.89.129.200-10.89.129.204 no failover
failover timeout 0:00:00 failover poll 15 no failover ip
address outside no failover ip address inside pdm
history enable arp timeout 14400 !--- Defines a pool of
global addresses to be used by NAT. global (outside) 1
192.168.1.6-192.168.1.10 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--- Specifies which
outside IP address to apply to the web server. static
(inside,outside) 192.168.1.11 10.89.129.131 netmask
255.255.255.255 0 0 !--- Apply ACL 120 to the outside
interface in the inbound direction. access-group 120 in
interface outside !--- Defines a default route for the
PIX. route outside 0.0.0.0 0.0.0.0 192.168.1.3 1 !---
Defines a route for traffic within the PIX's !--- subnet
to reach other inside hosts. route inside 10.89.129.128
255.255.255.128 10.89.129.193 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
!--- Authentication, authorization, and accounting (AAA)
statements !--- for authentication. !--- Use either of
these statements to define the protocol of the group
AuthInbound. !--- You cannot use both.
aaa-server AuthInbound protocol tacacs+

!--- OR aaa-server AuthInbound protocol radius !---
After you define the protocol of the group AuthInbound,
define !--- a server of the same type. !--- In this case
we specify the TACACS+ server and key of "secretkey".
aaa-server AuthInbound (inside) host 10.89.129.134
secretkey timeout 10 !--- Authenticate HTTP, FTP, and
Telnet traffic to the web server. aaa authentication
include http outside 10.89.129.131 255.255.255.255
0.0.0.0 0.0.0.0 AuthInbound aaa authentication include
ftp outside 10.89.129.131 255.255.255.255 0.0.0.0
0.0.0.0 AuthInbound aaa authentication include telnet

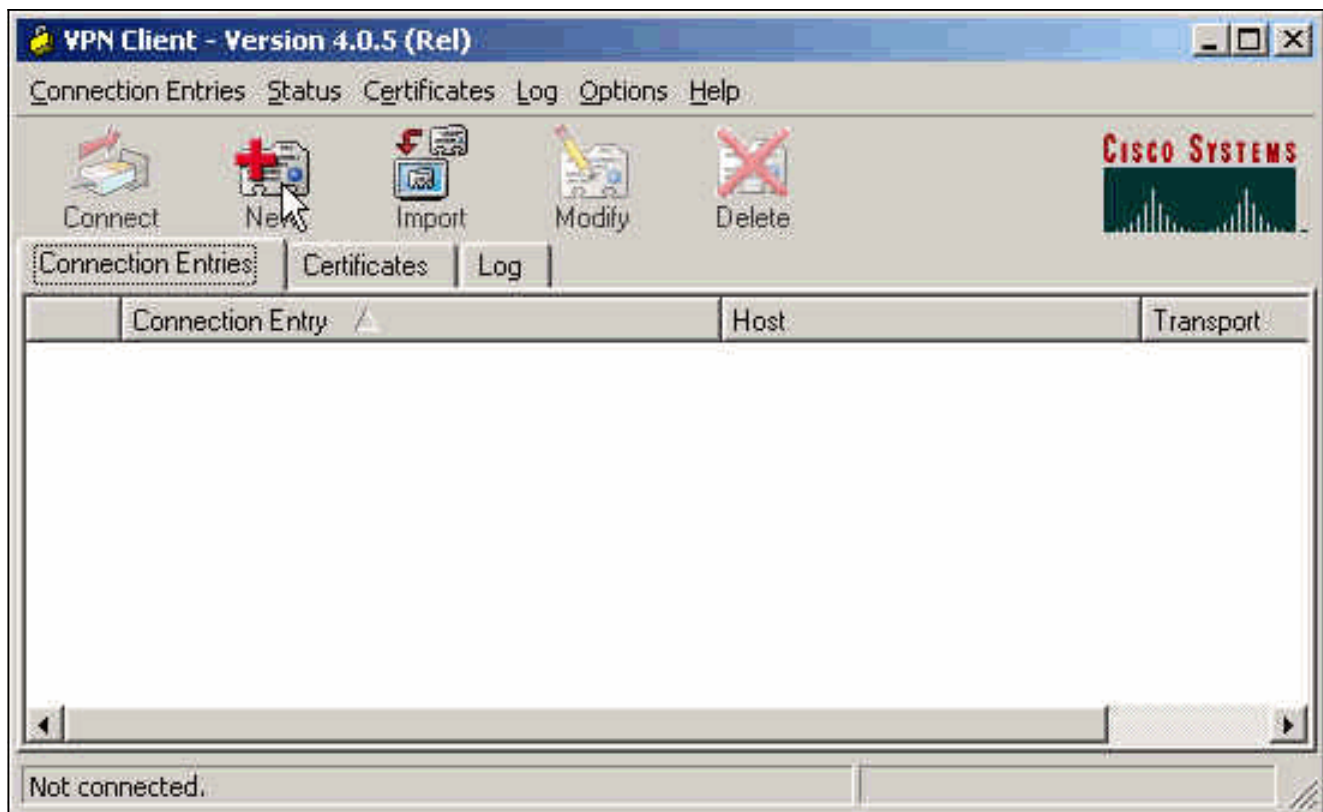
```

```
outside 10.89.129.131 255.255.255.255 0.0.0.0 0.0.0.0
AuthInbound no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- Trust IPsec traffic
and avoid going through ACLs/NAT. sysopt connection
permit-ipsec !--- IPsec and dynamic map configuration.
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap !---
Assign IP address for VPN 1.1 Clients. crypto map mymap
client configuration address initiate crypto map mymap
client configuration address respond !--- Use the AAA
server for authentication (AuthInbound). crypto map
mymap client authentication AuthInbound !--- Apply the
IPsec/AAA/ISAKMP configuration to the outside interface.
crypto map mymap interface outside isakmp enable outside
!--- Pre-shared key for VPN 1.1 Clients. isakmp key
***** address 0.0.0.0 netmask 0.0.0.0 isakmp identity
address !--- Assign address from "VPNpool" pool for VPN
1.1 Clients. isakmp client configuration address-pool
local VPNpool outside !--- ISAKMP configuration for VPN
Client 3.x/4.x. isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 2 isakmp policy 10
lifetime 86400 !--- ISAKMP configuration for VPN Client
1.x. isakmp policy 20 authentication pre-share isakmp
policy 20 encryption des isakmp policy 20 hash md5
isakmp policy 20 group 1 isakmp policy 20 lifetime 86400
!--- Assign addresses from "VPNpool" for VPN Client
3.x/4.x. vpngroup vpn3000 address-pool VPNpool vpngroup
vpn3000 idle-time 1800 !--- Group password for VPN
Client 3.x/4.x (not shown in configuration). vpngroup
vpn3000 password ***** telnet timeout 5 ssh timeout 5
console timeout 0 terminal width 80
Cryptochecksum:ba54c063d94989cbd79076955dbfeefc : end
pixfirewall#
```

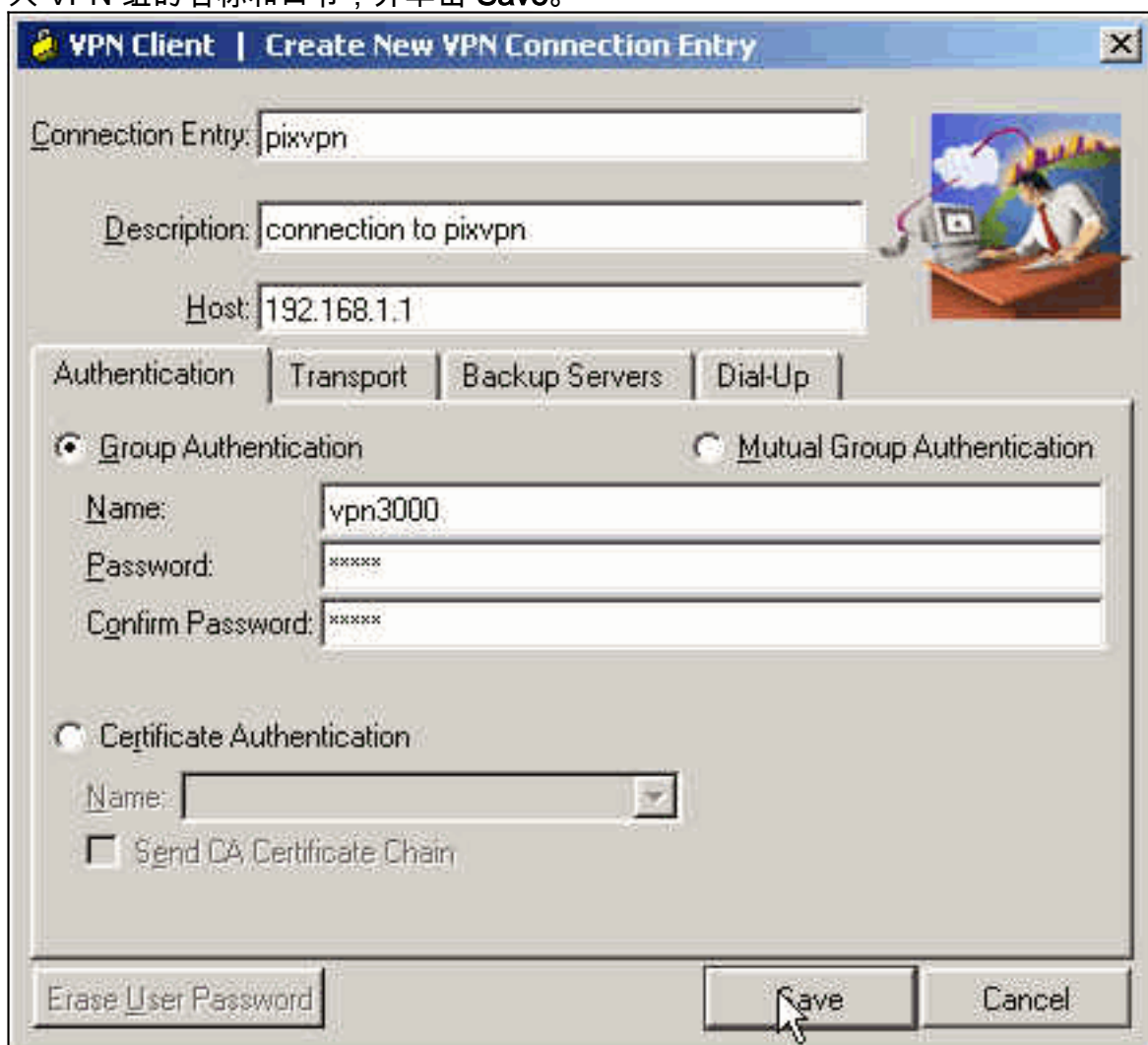
VPN客户端4.0.5配置

完成以下步骤以配置VPN客户端4.0.5。

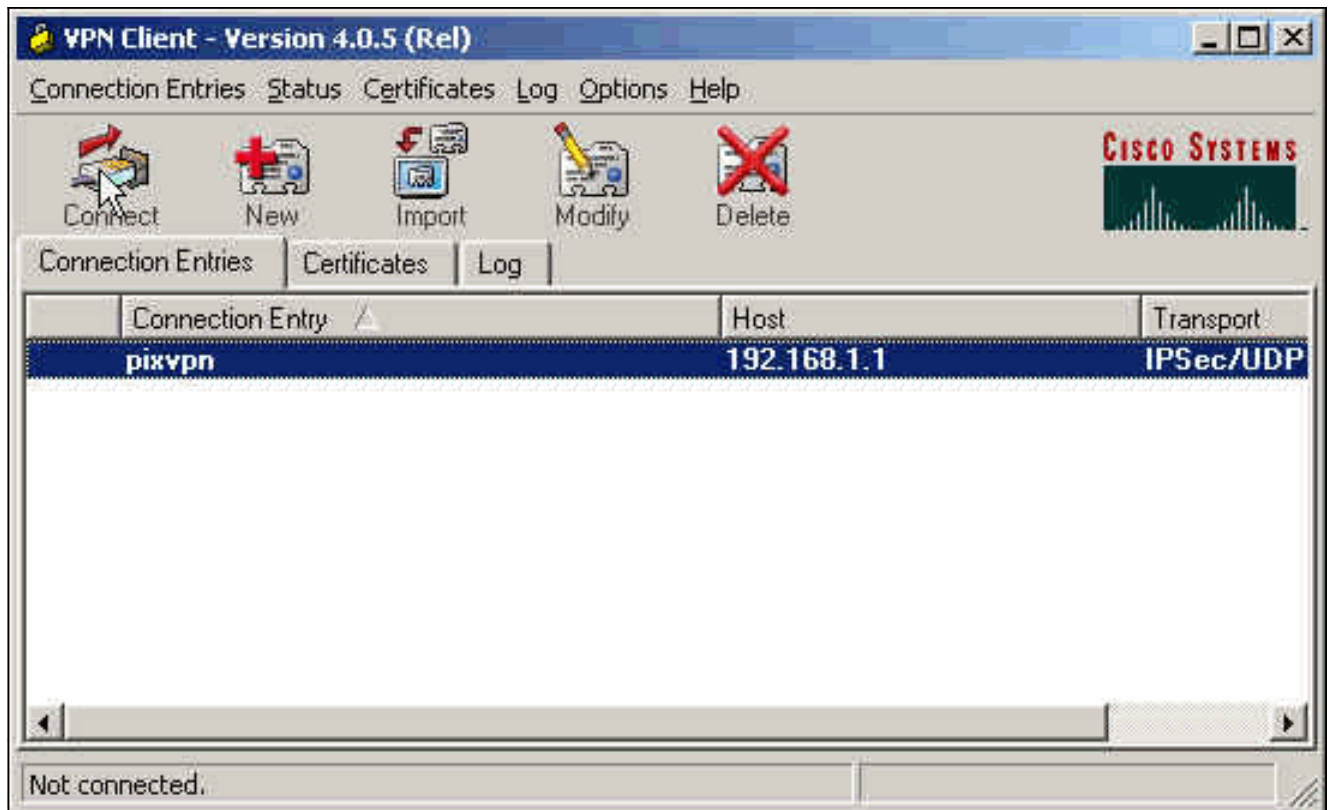
1. 选择 **Start > Programs > Cisco Systems VPN Client > VPN Client**。
2. 单击 **New** 以启动 **Create New VPN Connection Entry** 窗口。



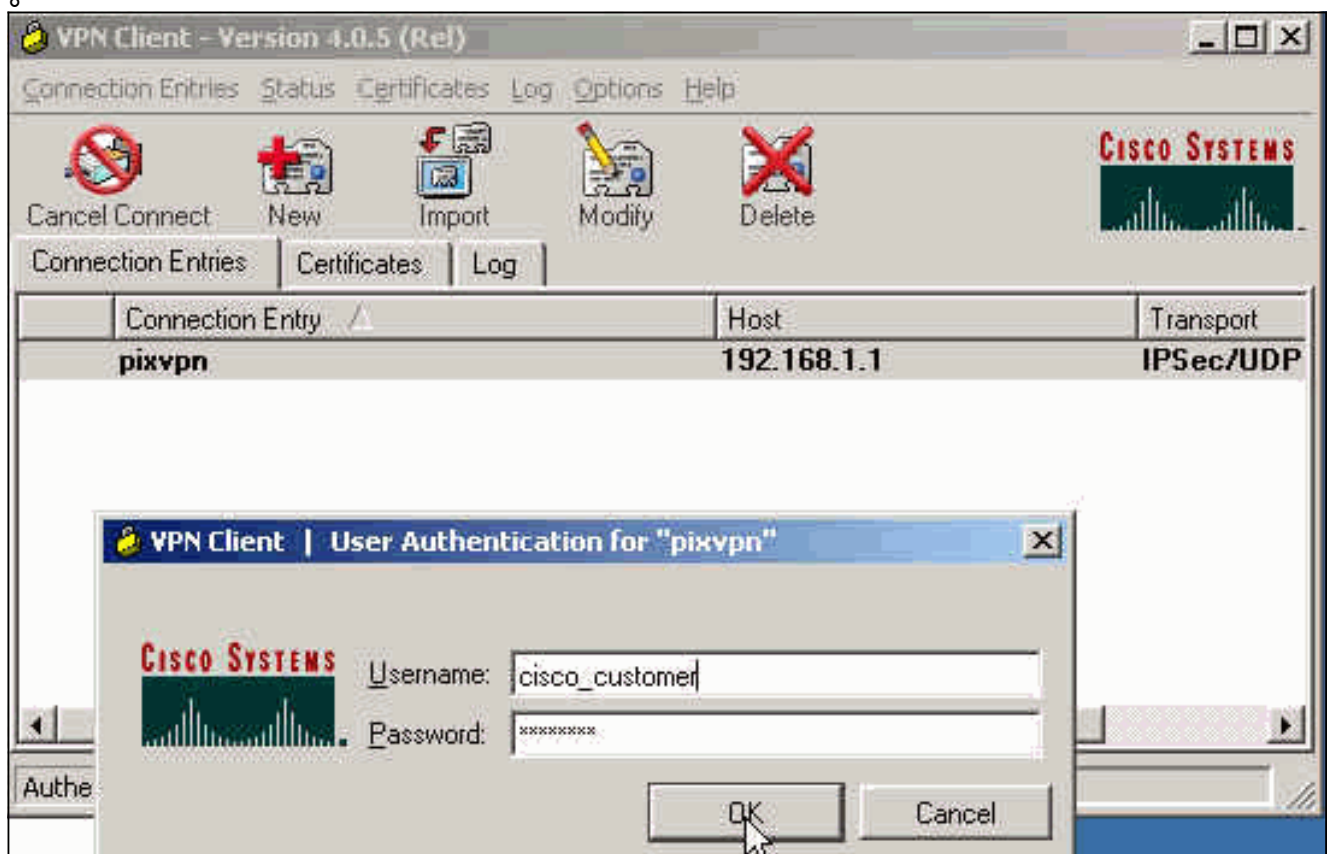
3. 输入 Connection Entry 的名称与说明。在 Host 框中输入 PIX 防火墙的外部 IP 地址。然后输入 VPN 组的名称和口令，并单击 **Save**。



4. 在 VPN Client 主窗口中，单击要使用的连接，然后单击 **Connect** 按钮。



5. 出现提示时，输入用于 xauth 的 Username 和 Password 信息，然后单击 OK 以连接远程网络。



VPN 客户端 3.5 配置

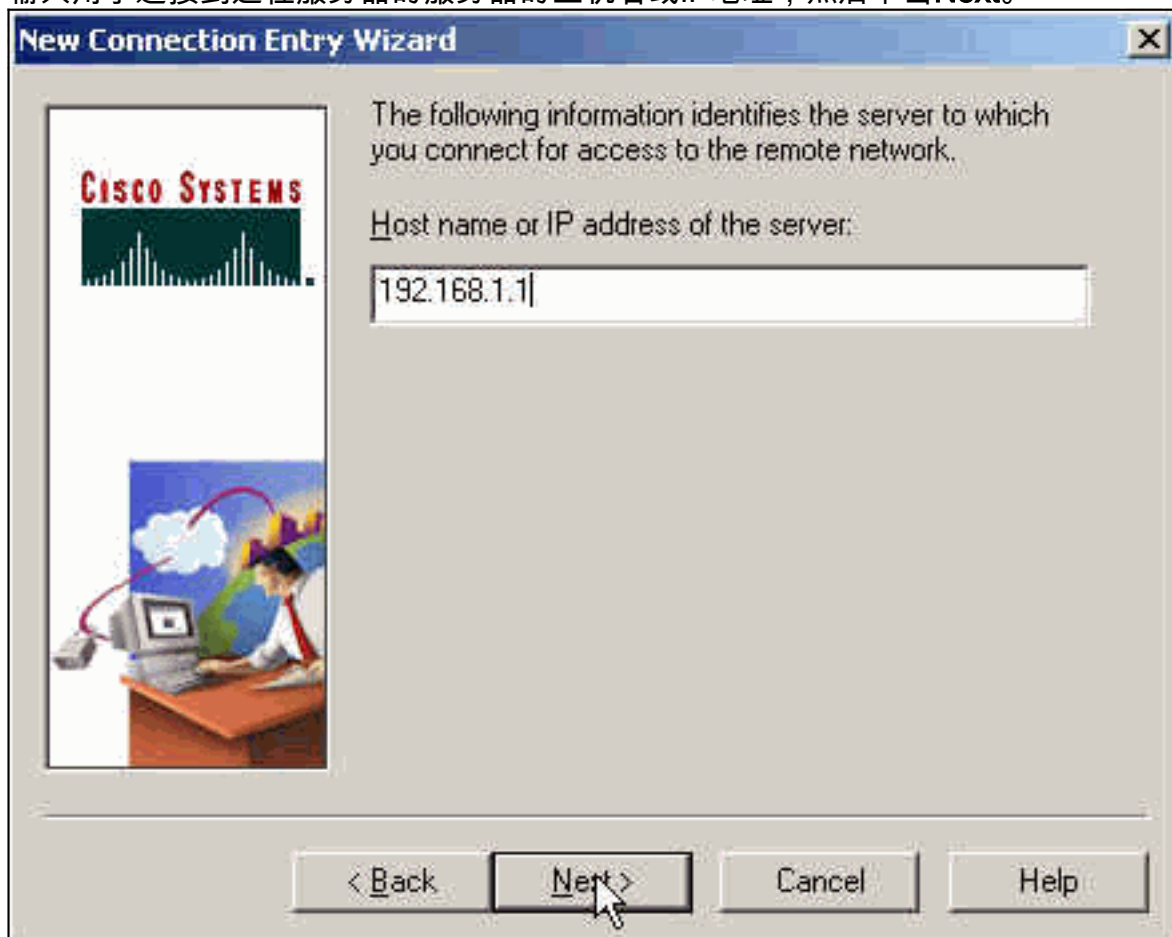
完成以下步骤以配置VPN Client 3.5配置。

1. 选择开始>程序> Cisco Systems VPN Client > VPN Dialer。
2. 单击New以启动“New Connection Entry Wizard”。

3. 输入新连接条目的名称，然后单击“下一步”。

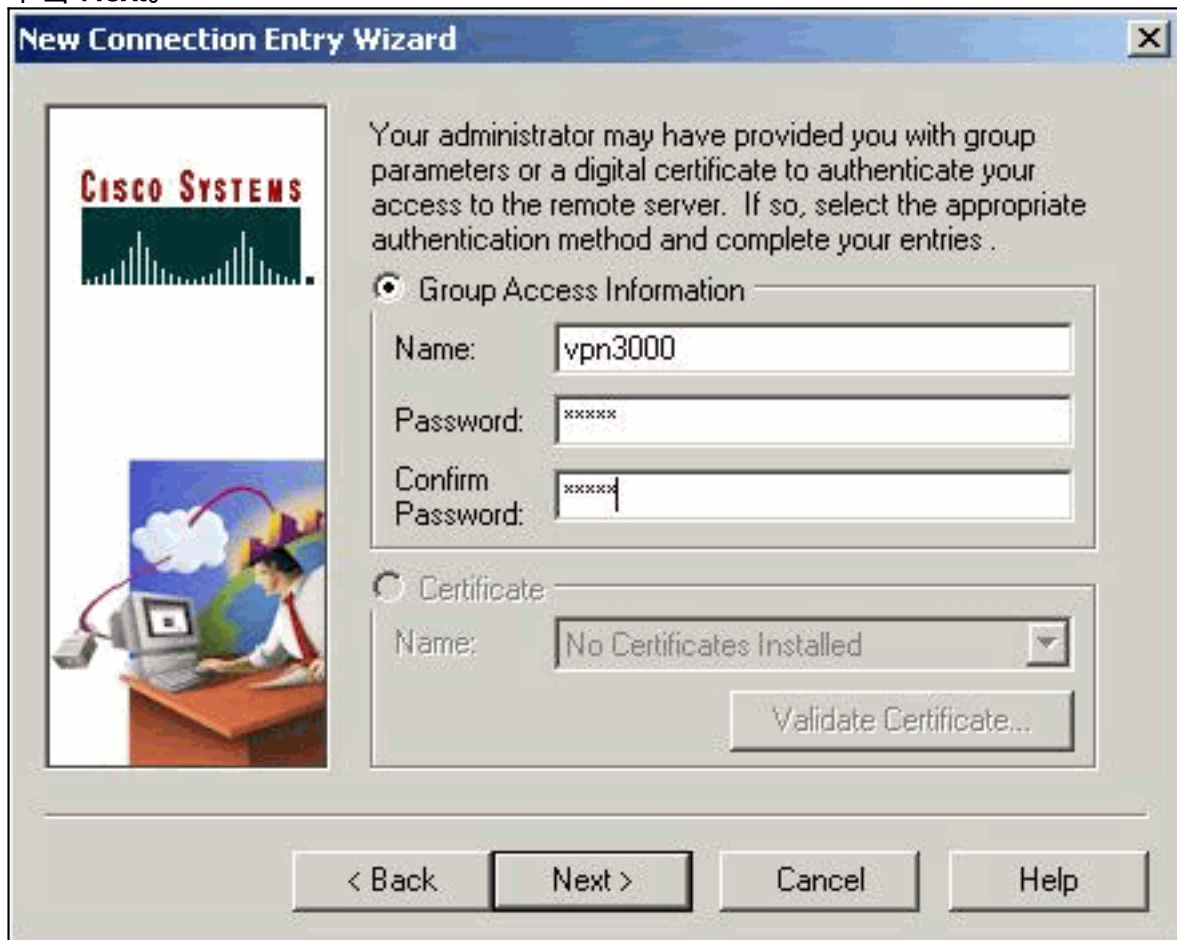


4. 输入用于连接到远程服务器的服务器的主机名或IP地址，然后单击Next。

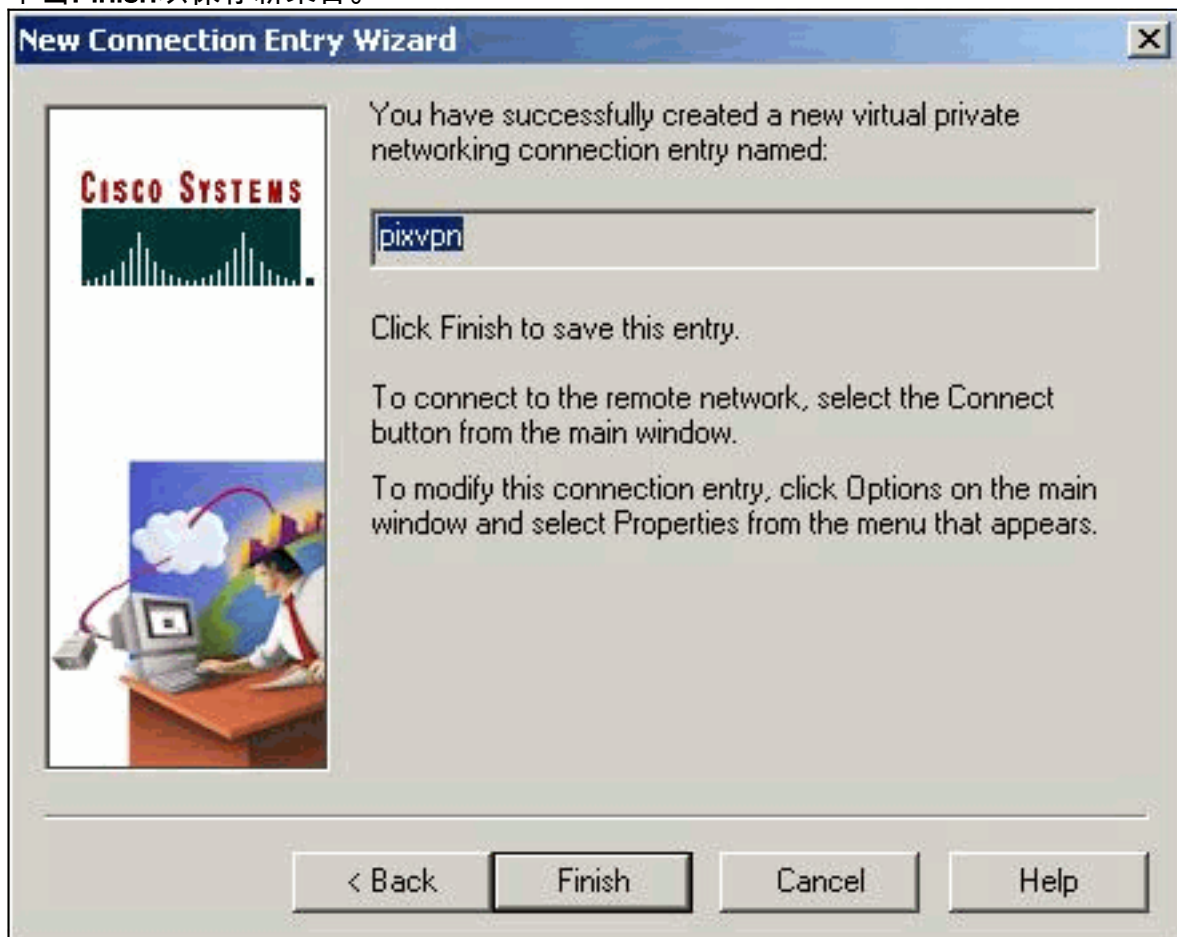


5. 选择Group Access Information并输入用于验证您对远程服务器的访问的Name和Password。

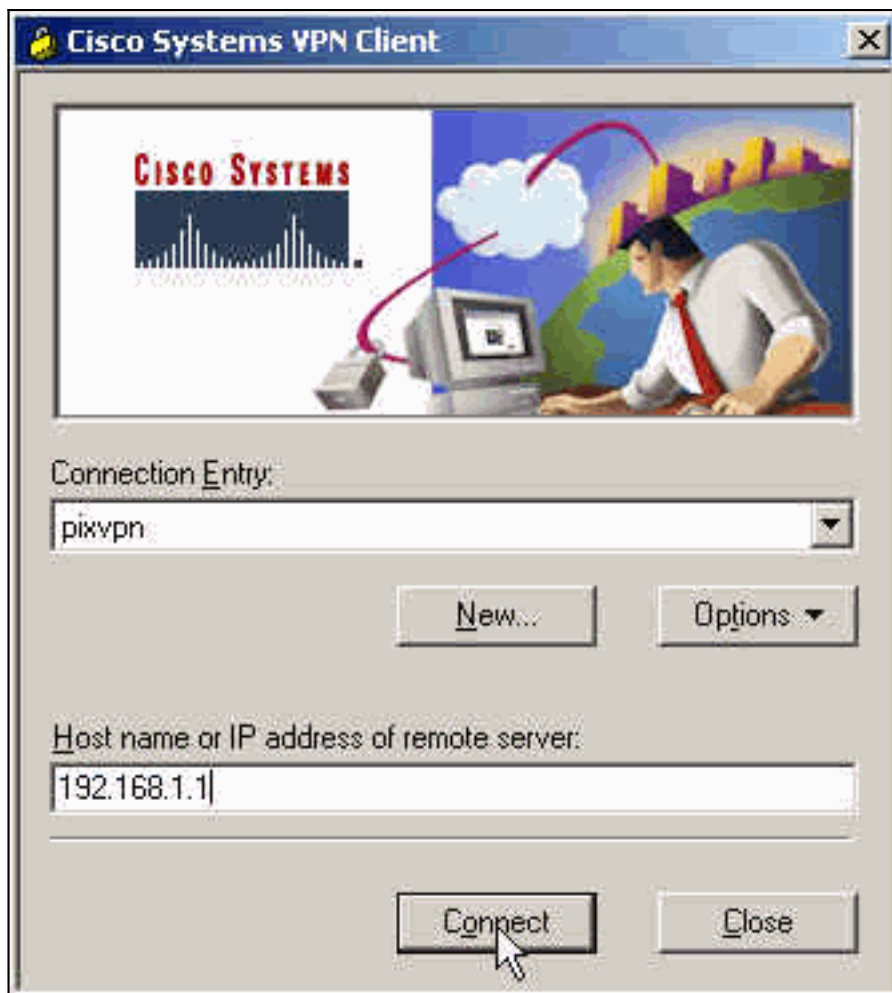
单击 **Next**。



6. 单击 **Finish** 以保存新条目。



7. 在拨号器中选择 **Connection Entry**，然后单击 **Connect**。



8. 出现提示时，输入用于 xauth 的 Username 和 Password 信息，然后单击 OK 以连接远程网络



VPN 客户端 1.1 配置

Network Security policy:

1- TACconn

My Identity

Connection security: Secure
Remote Party Identity and addressing
ID Type: IP subnet
10.89.129.128
255.255.255.128
Port all Protocol all

Connect using secure tunnel

ID Type: IP address
192.168.1.1

Pre-shared Key=cisco1234

Authentication (Phase 1)

Proposal 1

Authentication method: pre-shared key
Encrypt Alg: DES
Hash Alg: MD5
SA life: Unspecified
Key Group: DH 1

Key exchange (Phase 2)

Proposal 1

Encapsulation ESP
Encrypt Alg: DES
Hash Alg: MD5
Encap: tunnel
SA life: Unspecified
no AH

2- Other Connections

Connection security: Non-secure
Local Network Interface
Name: Any
IP Addr: Any
Port: All

添加记帐

用于添加记帐的命令语法为：

```
aaa accounting include acctg_service inbound|outbound l_ip l_mask [f_ip f_mask] server_tag
```

例如，在PIX配置中，添加了以下命令：

```
aaa accounting include any inbound
```

注意：使用 `sysopt connection permit-ipsec` 命令(而非 `sysopt ipsec pl-compatible` 命令)是 Xauth 记帐工作所必需的。Xauth 记帐不仅与 `sysopt ipsec pl-compatible` 命令一起使用。Xauth 记帐对 TCP 连接有效，对 ICMP 或 UDP 无效。

以下输出是 TACACS+ 记帐记录的示例：

```
07/27/2004 15:17:54 cisco_customer Default Group 10.89.129.200 stop 15 .. 99 1879 .. ..
    0x5 .. PIX 10.89.129.194 telnet
07/27/2004 15:17:39 cisco_customer Default Group 10.89.129.200 start .. .. .. .. ..
    0x5 .. PIX 10.89.129.194 telnet
```

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意：在使用 [debug 命令之前](#)，请参阅有关 Debug 命令的重要信息。

启用 Cisco 安全日志查看器以查看客户端调试。

- `debug crypto ipsec` — 用于查看第2阶段的IPsec协商。
- `debug crypto isakmp` — 用于查看第1阶段的ISAKMP协商。

故障排除

本部分提供的信息可用于对配置进行故障排除。此外本部分还提供了 debug 输出示例。

故障排除命令

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意：在使用 [debug 命令之前](#)，请参阅有关 Debug 命令的重要信息。

- `debug crypto engine` — 用于调试加密引擎进程。

PIX 调试示例

```
pixfirewall#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
    tx      Off
    rx      Off
    open    Off
    cable   Off
```

```
txdmp    Off
rxdmp    Off
ifc      Off
rxip     Off
txip     Off
get      Off
put      Off
verify   Off
switch   Off
fail     Off
fmsg     Off
```

使用VPN客户端4.x的调试

```
pixfirewall#
crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1
VPN Peer: ISAKMP: Added new peer: ip:192.168.1.2
Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:192.168.1.2 Ref cnt incremented
to:1 Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:    encryption 3DES-CBC
ISAKMP:    hash SHA
ISAKMP:    default group 2
ISAKMP:    extended auth pre-share
ISAKMP:    life type in seconds
ISAKMP:    life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:    encryption 3DES-CBC
ISAKMP:    hash MD5
ISAKMP:    default group 2
ISAKMP:    extended auth pre-share
ISAKMP:    life type in seconds
ISAKMP:    life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:    encryption 3DES-CBC
ISAKMP:    hash SHA
ISAKMP:    default group 2
ISAKMP:    auth pre-shared
ISAKMP:    life type in seconds
ISAKMP:    life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:    encryption 3DES-CBC
ISAKMP:    hash MD5
ISAKMP:    default group 2
ISAKMP:    auth pre-share
ISAKMP:    life type in seconds
ISAKMP:    life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:    encryption DES-CBC
ISAKMP:    hash SHA
ISAKMP:    default group 2
ISAKMP:    extended auth pre-share
ISAKMP:    life type in seconds
ISAKMP:    life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
```

ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy

ISAKMP: encryption DES-CBC

ISAKMP: hash MD5

ISAKMP: default group 2

ISAKMP: extended auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are acceptable. Next payload is 3

!--- Attributes offered by the VPN Client are accepted by the PIX. ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to a Unity client ISAKMP (0): ID payload next-payload: 10 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0) : Total payload length: 12 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 OAK_AG exchange ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1 spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL_CONTACT IPSEC(key_engine): got a queue event... IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.1.2 ISAKMP (0): SA has been authenticated return status is IKMP_NO_ERROR ISAKMP/xauth: request attribute XAUTH_TYPE ISAKMP/xauth: request attribute XAUTH_USER_NAME ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD ISAKMP (0:0): initiating peer config to 192.168.1.2. ID = 1623347510 (0x60c25136) crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 84 ISAKMP: Config payload CFG_REPLY return status is IKMP_ERR_NO_RETRANS ISAKMP (0:0): initiating peer config to 192.168.1.2. ID = 2620656926 (0x9c340d1e) crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 60 ISAKMP: Config payload CFG_ACK return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 0 ISAKMP: Config payload CFG_REQUEST ISAKMP (0:0): checking request: ISAKMP: attribute IP4_ADDRESS (1) ISAKMP: attribute IP4_NETMASK (2) ISAKMP: attribute IP4_DNS (3) ISAKMP: attribute IP4_NBNS (4) ISAKMP: attribute ADDRESS_EXPIRY (5) Unsupported Attr: 5 ISAKMP: attribute APPLICATION_VERSION (7) Unsupported Attr: 7 ISAKMP: attribute UNKNOWN (28672) Unsupported Attr: 28672 ISAKMP: attribute UNKNOWN (28673) Unsupported Attr: 28673 ISAKMP: attribute UNKNOWN (28674) ISAKMP: attribute UNKNOWN (28676) ISAKMP: attribute UNKNOWN (28679) Unsupported Attr: 28679 ISAKMP: attribute UNKNOWN (28680) Unsupported Attr: 28680 ISAKMP: attribute UNKNOWN (28677) Unsupported Attr: 28677 ISAKMP (0:0): responding to peer config from 192.168.1.2. ID = 177917346 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 942875080 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported 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_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDed proposal (2) ISAKMP: Checking IPsec proposal 3 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP: Checking IPsec proposal 4 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 5 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP: Checking IPsec proposal 6 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 2, hmac_alg 2) not

supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (6) ISAKMP : Checking IPsec proposal 7 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 192.168.1.1, src= 192.168.1.2, dest_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1), src_proxy= 10.89.129.200/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 942875080 ISAKMP (0): processing ID payload. message ID = 942875080 ISAKMP (0): ID_IPV4_ADDR src 10.89.129.200 prot 0 port 0 ISAKMP (0): processing ID payload. message ID = 942875080 ISAKMP (0): ID_IPV4_ADDR dst 192.168.1.1 prot 0 port 0IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0x64d7a518(1691854104) for SA from 192.168.1.2 to 192.168.1.1 for prot 3 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 3008609960 ISAKMP: Checking IPsec proposal 1 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 2 map_alloc_entry: allocating entry 1 ISAKMP (0): Creating IPsec SAs inbound SA from 192.168.1.2 to 192.168.1.1 (proxy 10.89.129.200 to 192.168.1.1) has spi 1691854104 and conn_id 2 and flags 4 lifetime of 2147483 seconds outbound SA from 192.168.1.1 to 192.168.1.2 (proxy 192.168.1.1 to 10.89.129.200) has spi 1025193431 and conn_id 1 and flags 4 lifetime of 2147483 seconds IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 192.168.1.1, src= 192.168.1.2, dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), src_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x64d7a518(1691854104),conn_id= 2, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 192.168.1.1, dest=192.168.1.2, src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), dest_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x3d1b35d7(1025193431),conn_id= 1, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 4 map_alloc_entry: allocating entry 3 ISAKMP (0): Creating IPsec SAs inbound SA from 192.168.1.2 to 192.168.1.1 (proxy 10.89.129.200 to 0.0.0.0) has spi 3415657865 and conn_id 4 and flags 4 lifetime of 2147483 seconds outbound SA from 192.168.1.1 to 192.168.1.2 (proxy 0.0.0.0 to 10.89.129.200) has spi 2383969893 and conn_id 3 and flags 4 lifetime of 2147483 secondsIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 192.168.1.1, src=192.168.1.2, dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), src_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0xcb96cd89(3415657865),conn_id= 4, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 192.168.1.1, dest=192.168.1.2, src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), dest_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x8e187e65(2383969893),conn_id= 3, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:4 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:5 Total VPN Peers:1 return status is IKMP_NO_ERROR pixfirewall#**show uauth**

Current Most Seen

Authenticated Users

1 1

Authen In Progress

0 1

ipsec user 'cisco_customer' at 10.89.129.200, authenticated

pixfirewall#

[调试 VPN Client 1.1](#)

crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1

VPN Peer: ISAKMP: Added new peer: ip:192.168.1.3

Total VPN Peers:1

VPN Peer: ISAKMP: Peer ip:192.168.1.3 Ref cnt incremented to:1

Total VPN Peers:1

OAK_MM exchange

```
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
    encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
    spi 0, message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): ID payload
    next-payload : 8
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
ISAKMP: Created a peer node for 192.168.1.3
OAK_QM exchange
ISAKMP (0:0): Need XAUTH
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 192.168.1.3.
ID = 3196940891 (0xbe8d725b)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload
from 192.168.1.3. message ID = 84
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 192.168.1.3.
ID = 3196940891 (0xbe8d725b)
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
ISAKMP_TRANSACTION exchange
```



```
ISAKMP (0:0): processing transaction payload
from 192.168.1.3. message ID = 60
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): initiating peer config to 192.168.1.3.
ID = 1647424595 (0x6231b453)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload
from 192.168.1.3. message ID = 60
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 802013669

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request)
:proposal part #1,
  (key eng. msg.) dest= 192.168.1.1, src = 192.168.1.3,
  dest_proxy= 10.89.129.128/255.255.255.128/0/0 (type=4),
  src_proxy= 10.89.129.200/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform=esp-des esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize=0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 802013669

ISAKMP (0): processing ID payload. message ID = 802013669
ISAKMP (0): ID_IPV4_ADDR src 10.89.129.200 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 802013669
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.89.129.128/255.255.255.128
prot 0 port 0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd7cef5ba(3620664762) for SA
  from 192.168.1.3 to 192.168.1.1 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 192.168.1.3, dest 192.168.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2

ISAKMP (0): Creating IPsec SAs
  inbound SA from 192.168.1.3 to 192.168.1.1
  (proxy 10.89.129.200 to 10.89.129.128)
  has spi 3620664762 and conn_id 1 and flags 4
  outbound SA from 192.168.1.1 to 192.168.1.3
  (proxy 10.89.129.128 to 10.89.129.200)
  has spi 541375266 and conn_id 2 and flags 4
IPSEC(key_engine): got a queue event...

IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 192.168.1.1, src=192.168.1.3,
  dest_proxy= 10.89.129.128/255.255.255.128/0/0 (type=4),
  src_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1),
```

```
protocol= ESP, transform=esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xd7cef5ba(3620664762),conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 192.168.1.1, dest=192.168.1.3,
src_proxy= 10.89.129.128/255.255.255.128/0/0 (type=4),
dest_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1),
protocol= ESP, transform=esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x2044bb22(541375266),conn_id= 2, keysize= 0, flags= 0x4
```

```
VPN Peer: IPSEC: Peer ip:192.168.1.3 Ref cnt incremented
to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:192.168.1.3 Ref cnt incremented
to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

[相关信息](#)

- [PIX 500 系列安全设备](#)
- [PIX 命令参考](#)
- [IPsec 协商/IKE 协议](#)
- [IPSec 简介](#)
- [建立通过 Cisco PIX 防火墙的连接](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)