IPSec - PIX에서 Cisco VPN 클라이언트 와일드카드, 사전 공유, 확장 인증을 통한 모드 구성

목차

소개

이 컨피그레이션 예에서는 와일드카드, mode-config, sysopt **connection permit-ipsec** 명령 및 확장 인증(Xauth)을 사용하여 VPN 클라이언트를 PIX 방화벽에 연결하는 방법을 보여 줍니다.

PIX 6.3 이상에 대한 TACACS+ 및 RADIUS 컨피그레이션을 보려면 PIX 6.3 및 PIX/ASA 7.x 컨피그레이션의 TACACS+ 및 RADIUS 예를 참조하십시오.

VPN 클라이언트는 Cisco VPN Client 릴리스 3.6.1 이상과 PIX Firewall 6.3에서 암호화 알고리즘으로 AES(Advanced Encryption Standard)를 지원합니다. VPN 클라이언트는 128비트 및 256비트의 키 크기만 지원합니다. AES를 구성하는 방법에 대한 자세한 내용은 How to Configure the Cisco VPN Client to PIX with AES(Cisco VPN 클라이언트를 PIX with AES로 구성하는 방법)를 참조하십시오.

Microsoft Windows 2003 Internet Service를 사용하여 Cisco VPN 클라이언트(4.x for Windows)와 PIX 500 Series Security Appliance 7.x 간의 원격 액세스 VPN 연결을 설정하려면 Microsoft Windows 2003 IAS 203 IAS RADIUS 인증 구성 예를 참조하십시오. IAS) RADIUS 서버.

사용자 인증 및 계정 관리를 위해 RADIUS를 사용하는 Windows용 VPN 3000 Concentrator와 VPN Client 4.x 간의 IPsec을 참조하십시오. 사용자 인증 및 계정 관리를 위해 RADIUS를 사용하는 Windows용 Cisco VPN 3000 Concentrator와 Cisco VPN Client 4.x 간의 IPsec를 참조하십시오.

사용자 인증을 위해 RADIUS를 사용하여 라우터와 Cisco VPN 클라이언트 4.x 간의 연결을 구성하려면 Cisco IOS 라우터와 Cisco VPN Client 4.x 간 IPsec 구성 사용자 인증을 위해 RADIUS를 사용하여 Cisco VPN Client 4.x를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco VPN Client 4.x. 이 제품에는 Cisco Secure VPN Client 1.x와 달리 고급 VPN 기능이 있습니다.
- PIX Firewall 515E 버전 6.3(3).

참고: 암호화 기술은 내보내기 제어의 대상이 됩니다. 암호화 기술 수출에 관한 법률을 아는 것은 여러분의 책임입니다. 자세한 내용은 수출 관리 부서 웹 사이트를 참조하십시오 . 수출 통제와 관련하여 궁금한 점이 있으시면 export@cisco.com으로 이메일을 보내주십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

sysopt **connection permit-ipsec** 명령은 IPsec 터널에서 오는 모든 패킷이 IPsec 연결에 대해 연결된 **access-list**, **도관** 또는 **access-group** 명령의 검사를 우회하도록 암시적으로 허용합니다. Xauth는 외부 TACACS+ 또는 RADIUS 서버에 대한 IPsec 사용자를 인증합니다. 와일드카드 사전 공유 키 외에 사용자 이름/비밀번호를 제공해야 합니다.

VPN 클라이언트가 있는 사용자는 ISP에서 IP 주소를 수신합니다. 이는 PIX의 IP 주소 풀에서 IP 주소로 대체됩니다. 사용자는 네트워크를 포함하여 방화벽 내부의 모든 것에 액세스할 수 있습니다. VPN 클라이언트를 실행하지 않는 사용자는 정적 할당에서 제공하는 외부 주소를 사용하여 웹 서버에만 연결할 수 있습니다.

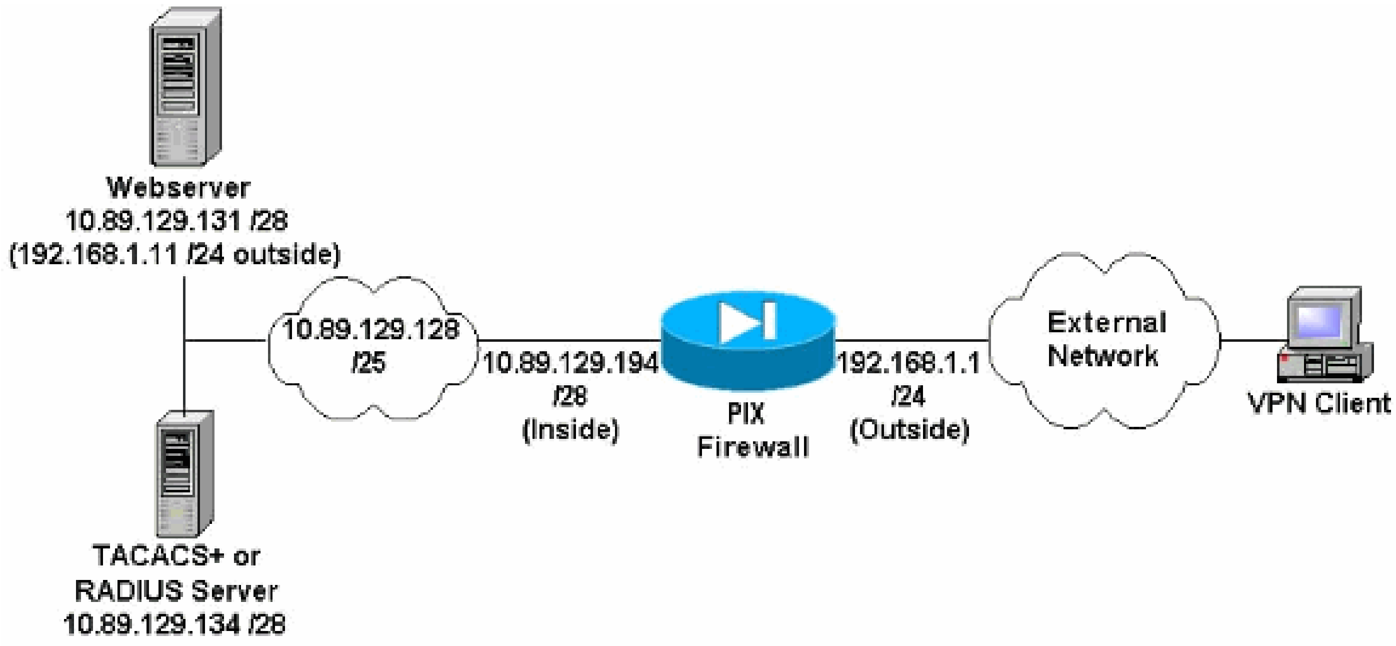
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



네트워크 다이어그램 참고 사항

- 전역 IP 주소 192.168.1.1을 사용하여 웹 서버에 액세스하는 인터넷 호스트는 VPN 연결이 설정되지 않은 경우에도 인증됩니다. 이 트래픽은 암호화되지 *않습니다*.
- VPN 클라이언트는 IPsec 터널이 설정되면 내부 네트워크(10.89.129.128/25)의 모든 호스트에 액세스할 수 있습니다. VPN 클라이언트에서 PIX 방화벽으로의 모든 트래픽이 암호화됩니다. IPsec 터널이 없으면 전역 IP 주소를 통해서만 웹 서버에 액세스할 수 있지만 여전히 인증해야 합니다.
- VPN 클라이언트는 인터넷에서 가져오고 해당 IP 주소는 미리 알려지지 않습니다.

구성

이 문서에서는 이러한 구성을 사용합니다.

- PIX 구성 6.3(3)
- VPN 클라이언트 4.0.5 구성
- VPN 클라이언트 3.5 구성
- VPN 클라이언트 1.1 구성

PIX 구성 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
```

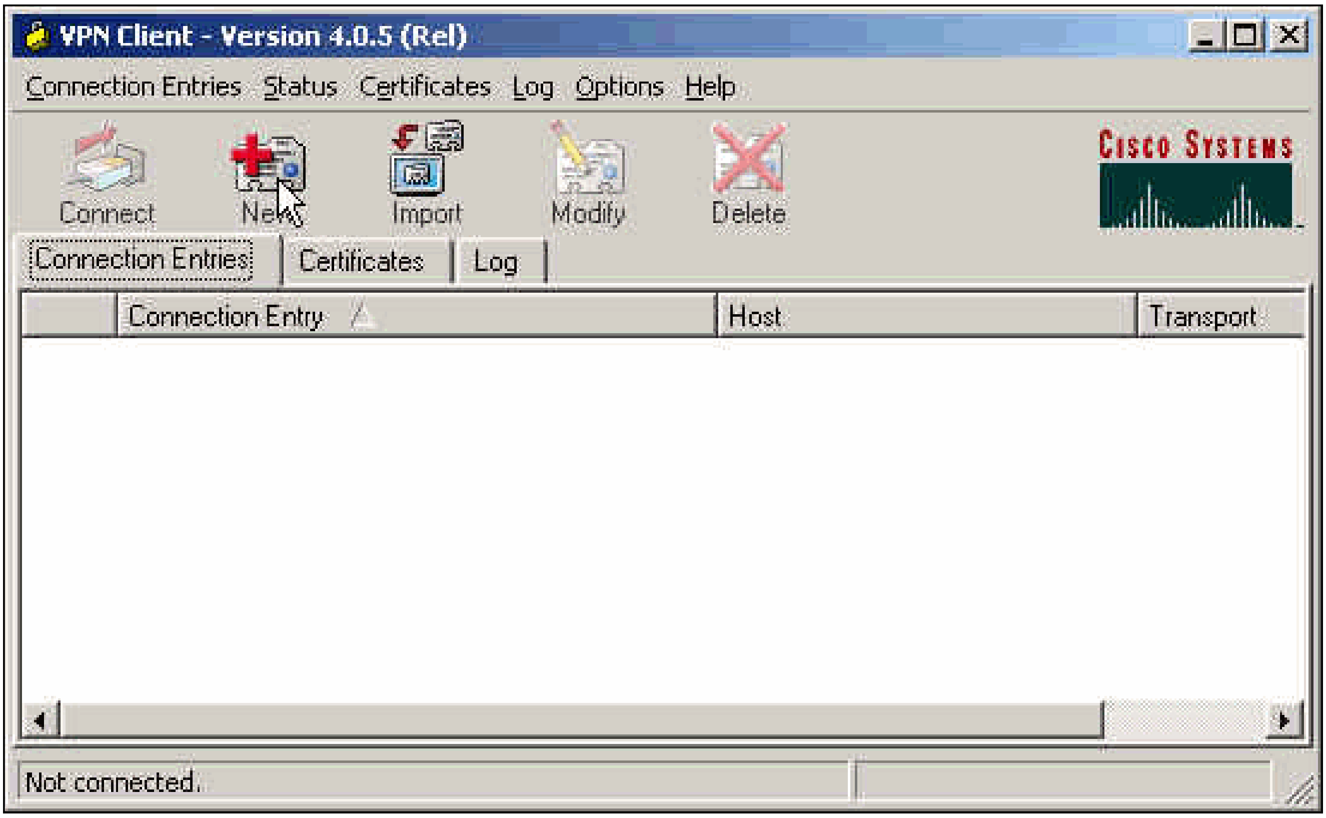
```
secretkey timeout 10 !--- Authenticate HTTP, FTP, and
Telnet traffic to the web server. aaa authentication
include http outside 10.89.129.131 255.255.255.255
0.0.0.0 0.0.0.0 AuthInbound aaa authentication include
ftp outside 10.89.129.131 255.255.255.255 0.0.0.0
0.0.0.0 AuthInbound aaa authentication 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 클라이언트 4.0.5 구성

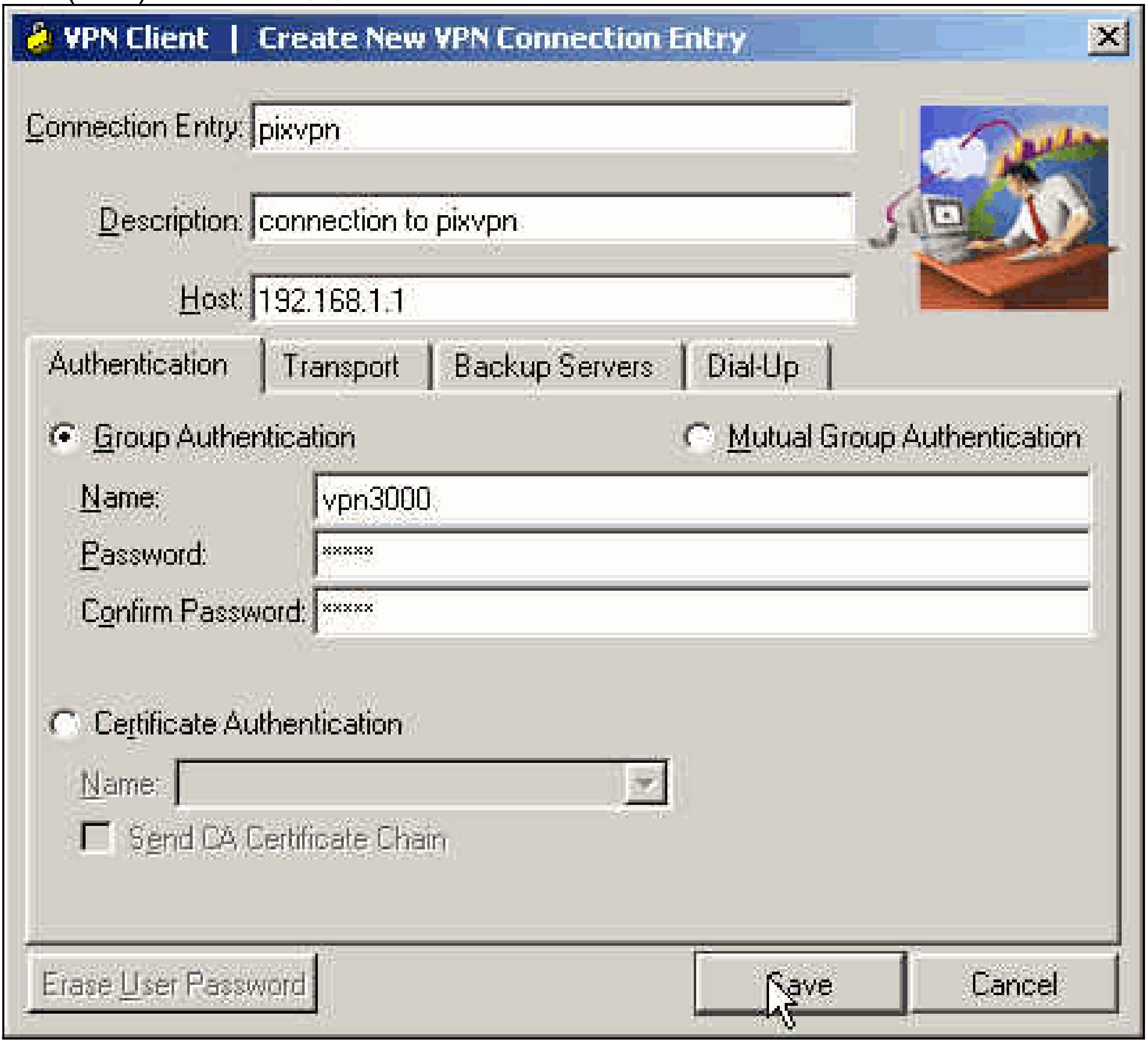
VPN 클라이언트 4.0.5을 구성하려면 다음 단계를 완료합니다.

1. Start(**시작) > Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > VPN Client(VPN 클라이언트)를 선택합니다**.
2. New(**새로 만들기)**를 클릭하여 Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창을 시작합니다

   .



3. 설명과 함께 연결 항목의 이름을 입력합니다. Host(호스트) 상자에 PIX Firewall의 외부 IP 주소를 입력합니다. 그런 다음 VPN Group name(VPN 그룹 이름)과 비밀번호를 입력하고 Save(저장)를 **클릭합니다**



Connection Entry: pixvpn

Description: connection to pixvpn

Host: 192.168.1.1

● Group Authentication ○ Mutual Group Authentication

Name: vpn3000

Password: *****

Confirm Password: *****

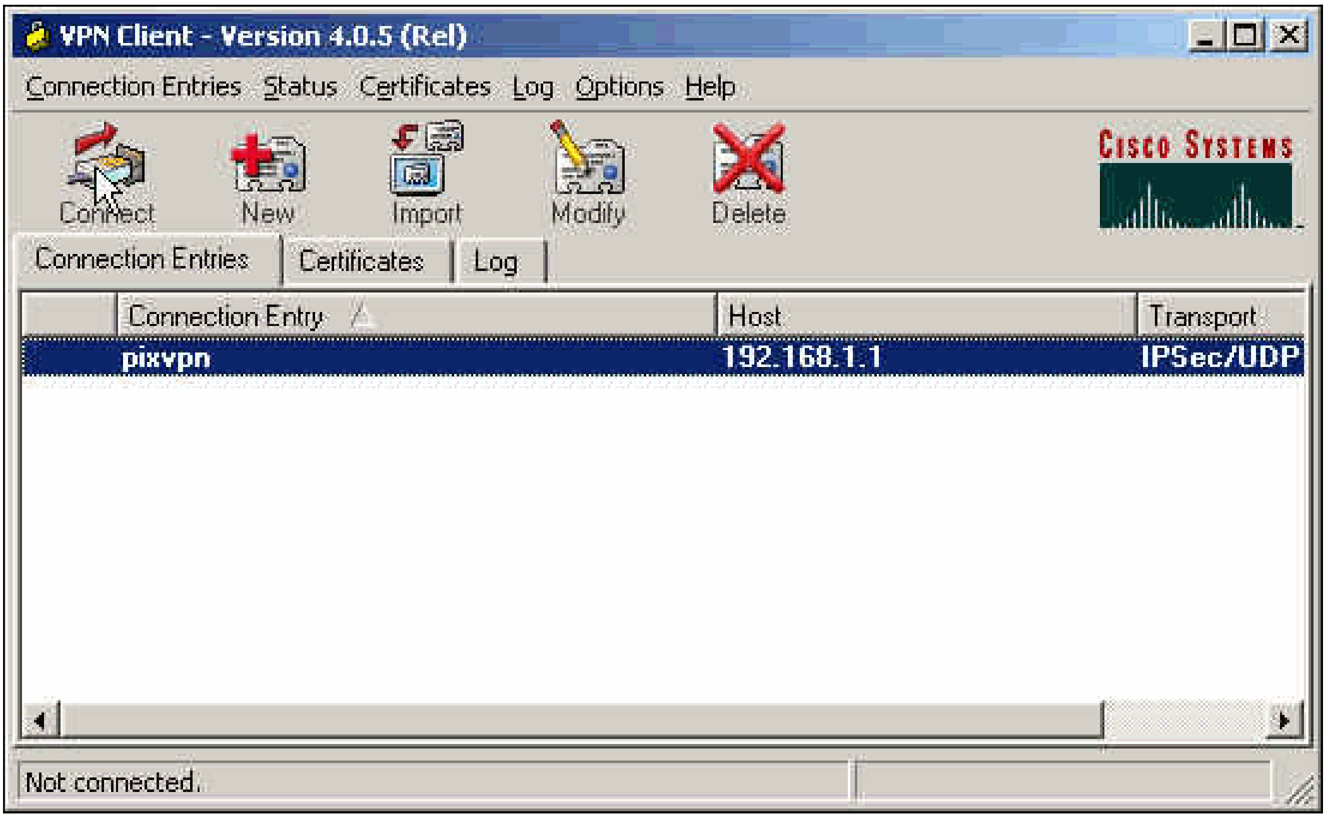
○ Certificate Authentication

Name:

□ Send CA Certificate Chain

4. VPN Client 주 창에서 사용할 연결을 클릭하고 **Connect** 버튼을 클릭합니다

.

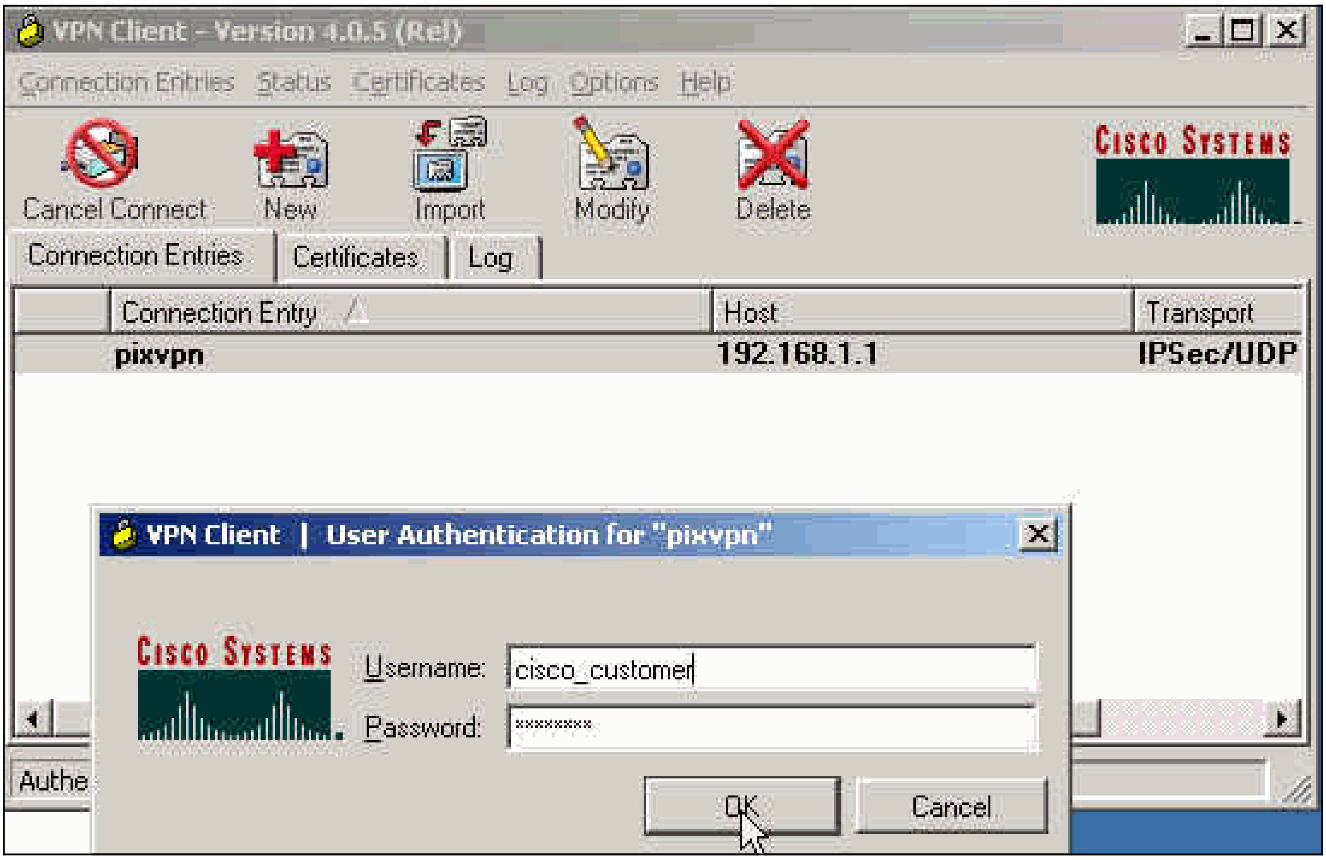

VPN Client - Version 4.0.5 (Rel)
Connection Entries Status Certificates Log Options Help
Connect
New
Import
Modify
Delete
Cisco Systems
Connection Entries
Certificates
Log

Connection Entry	Host	Transport
pixvpn	192.168.1.1	IPSec/UDP

Not connected.

5. 프롬프트가 표시되면 Xauth에 대한 사용자 이름 및 비밀번호 정보를 입력하고 **OK**를 클릭하여 원격 네트워크에 연결합니다

.


VPN Client - Version 4.0.5 (Rel)
Connection Entries Status Certificates Log Options Help
Cancel Connect
New
Import
Modify
Delete
Cisco Systems
Connection Entries
Certificates
Log
Authe
VPN Client | User Authentication for "pixvpn"
Cisco Systems
OK
Cancel

Connection Entry	Host	Transport
pixvpn	192.168.1.1	IPSec/UDP

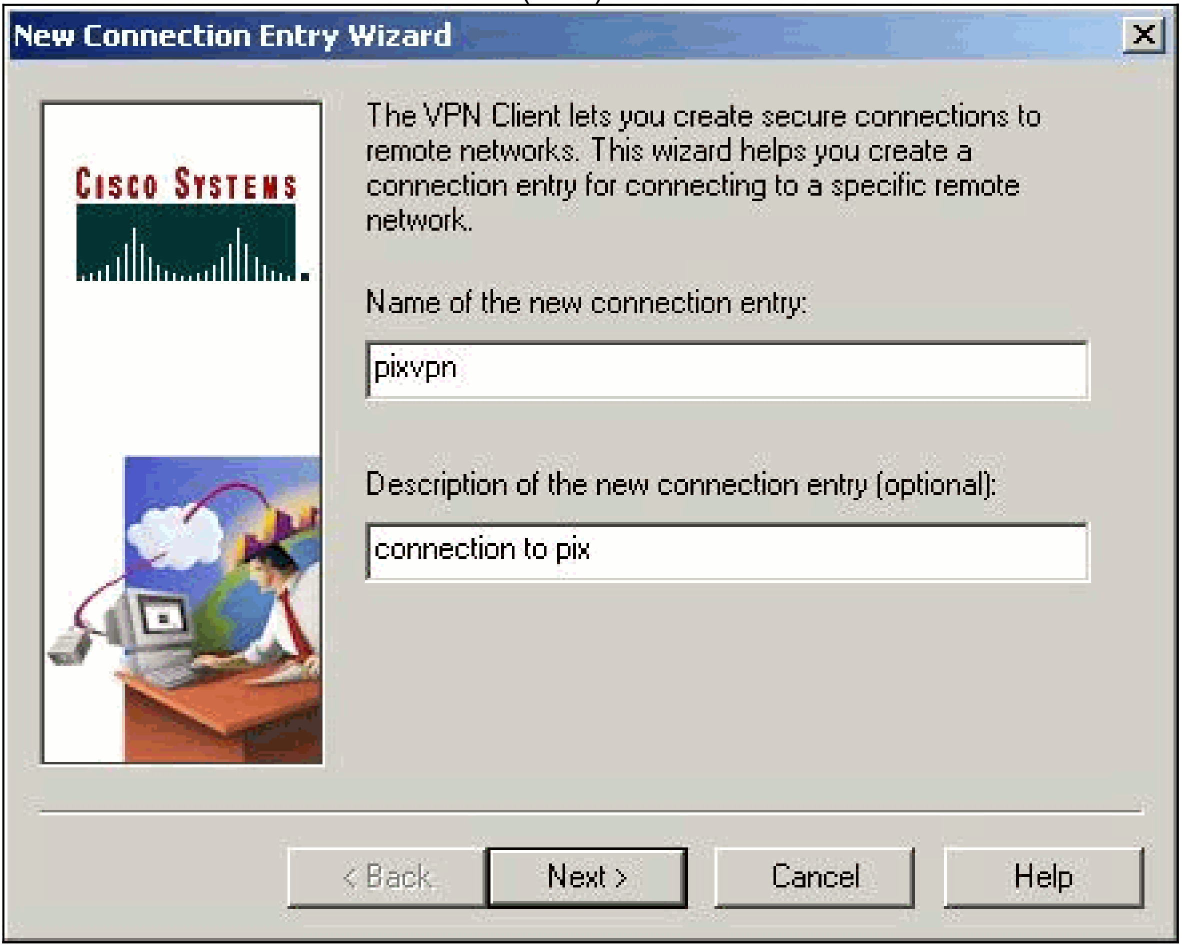
Username: cisco_customer

Password: ********

VPN 클라이언트 3.5 구성

VPN Client 3.5 컨피그레이션을 구성하려면 다음 단계를 완료합니다.

1. Start(**시작) > Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > VPN Dialer(VPN 다이얼러)를 선택합니다**.
2. New(**새로** 만들기)를 클릭하여 새 연결 항목 마법사를 시작합니다.
3. 새 연결 항목의 이름을 입력하고 Next(**다음**)를 클릭합니다



New Connection Entry Wizard

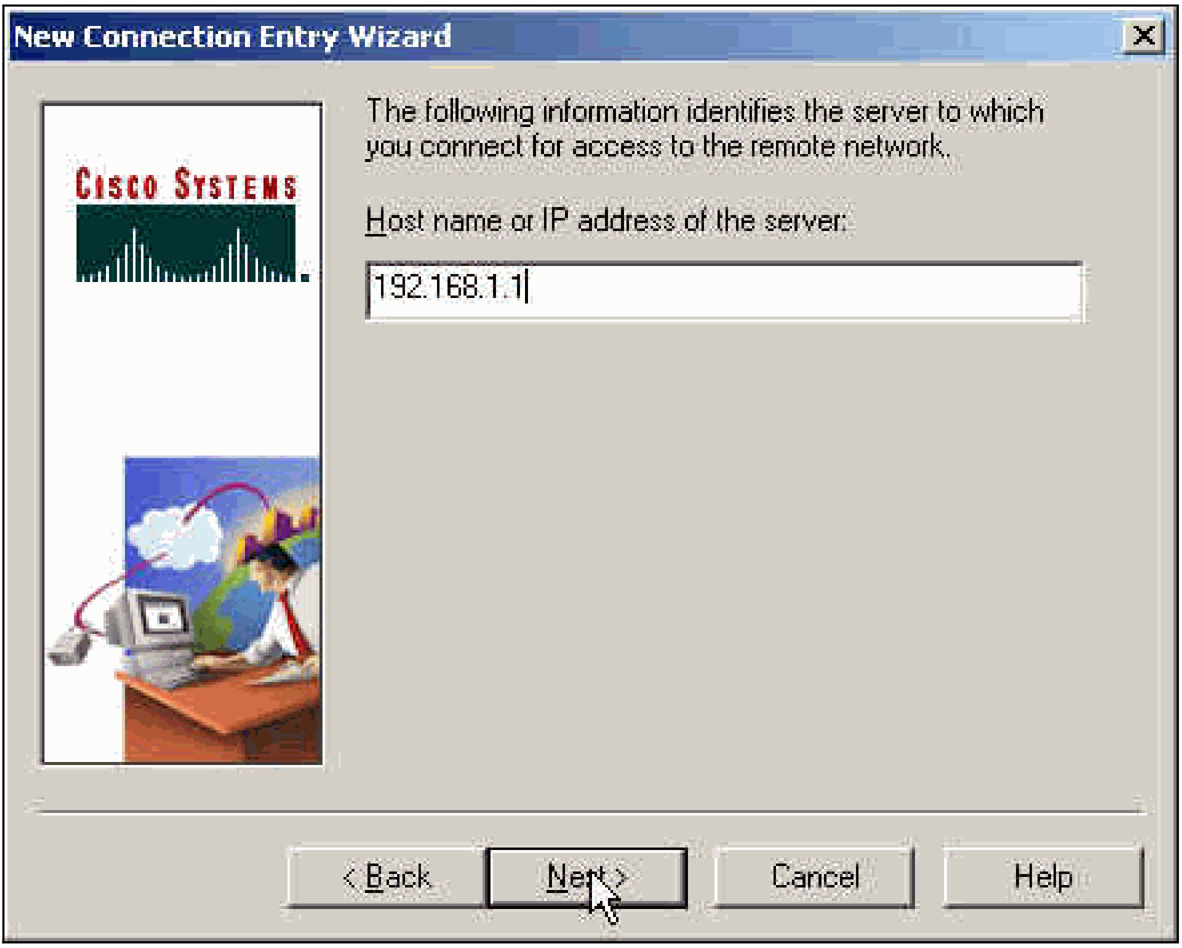
The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.

Name of the new connection entry: pixvpn

Description of the new connection entry (optional): connection to pix

.

4. 원격 서버에 연결하는 데 사용되는 서버의 호스트 이름 또는 IP 주소를 입력하고 **Next**를 클릭



New Connection Entry Wizard

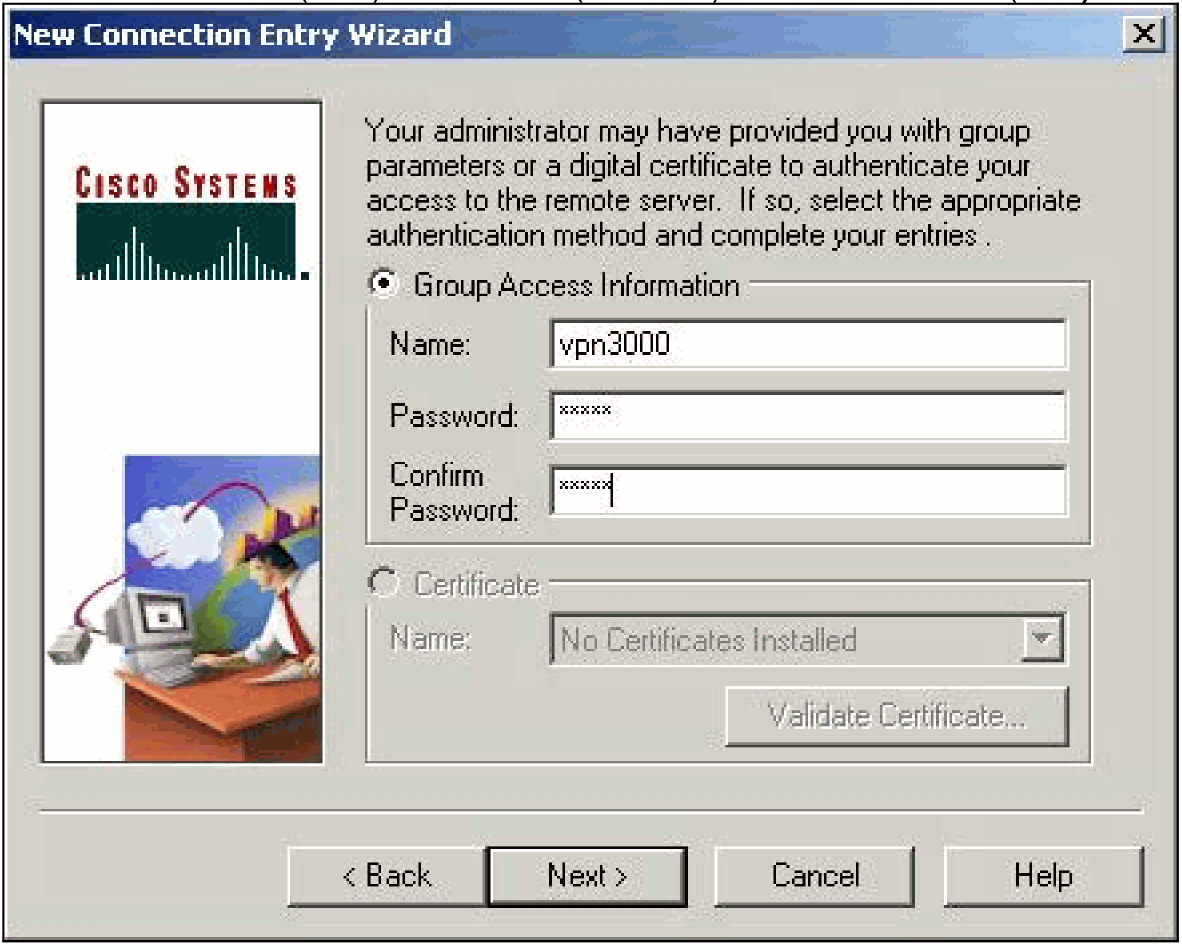
The following information identifies the server to which you connect for access to the remote network.

Host name or IP address of the server:

192.168.1.1

합니다.

5. Group **Access Information(그룹 액세스 정보**)을 선택하고 원격 서버에 대한 액세스를 인증하는 데 사용되는 Name(이름) 및 Password(비밀번호)를 입력합니다. Next(**다음)를 클릭합니다**



New Connection Entry Wizard

Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .

● Group Access Information

Name: vpn3000

Password: *****

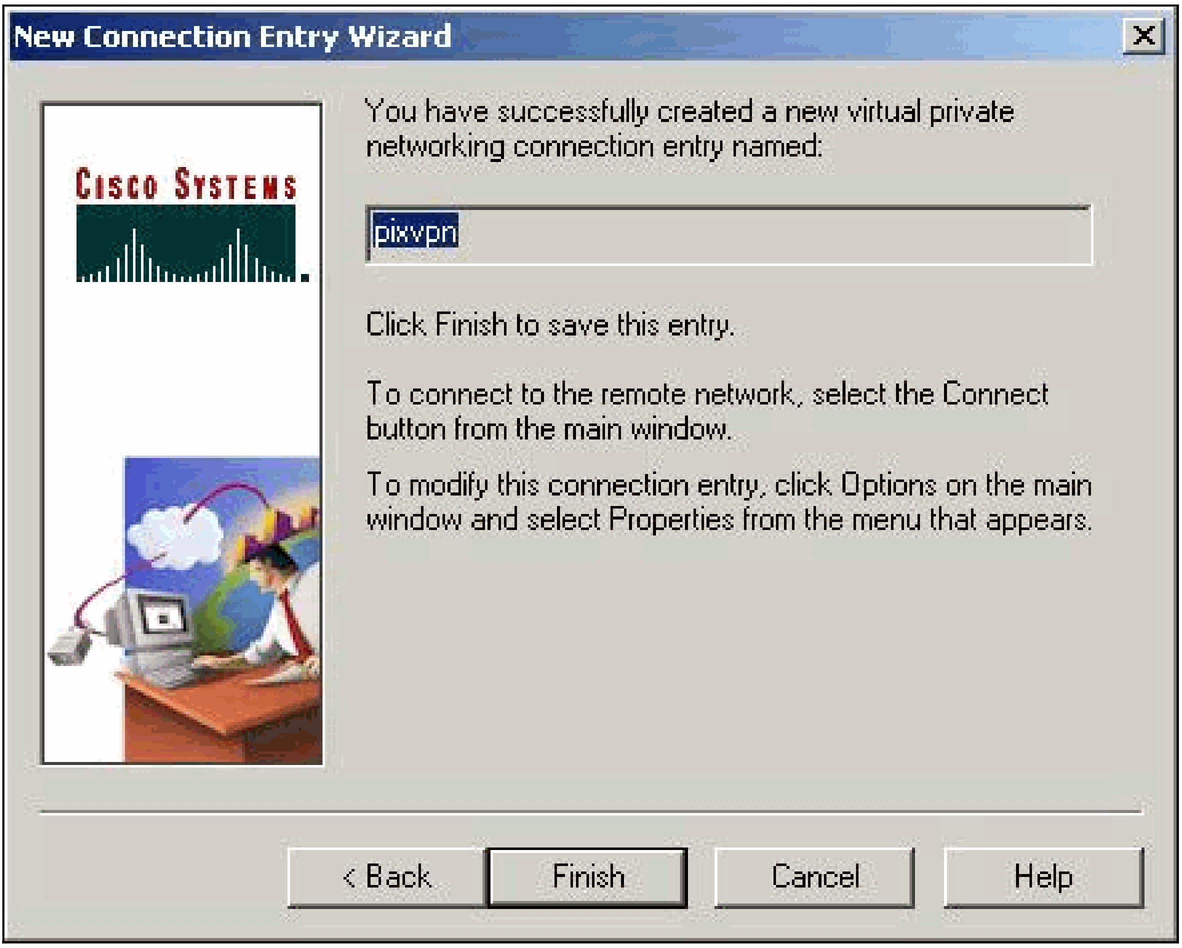
Confirm Password: *****

○ Certificate

Name: No Certificates Installed

.

6. **마침**을 클릭하여 새 항목을 저장합니다



New Connection Entry Wizard

You have successfully created a new virtual private networking connection entry named:

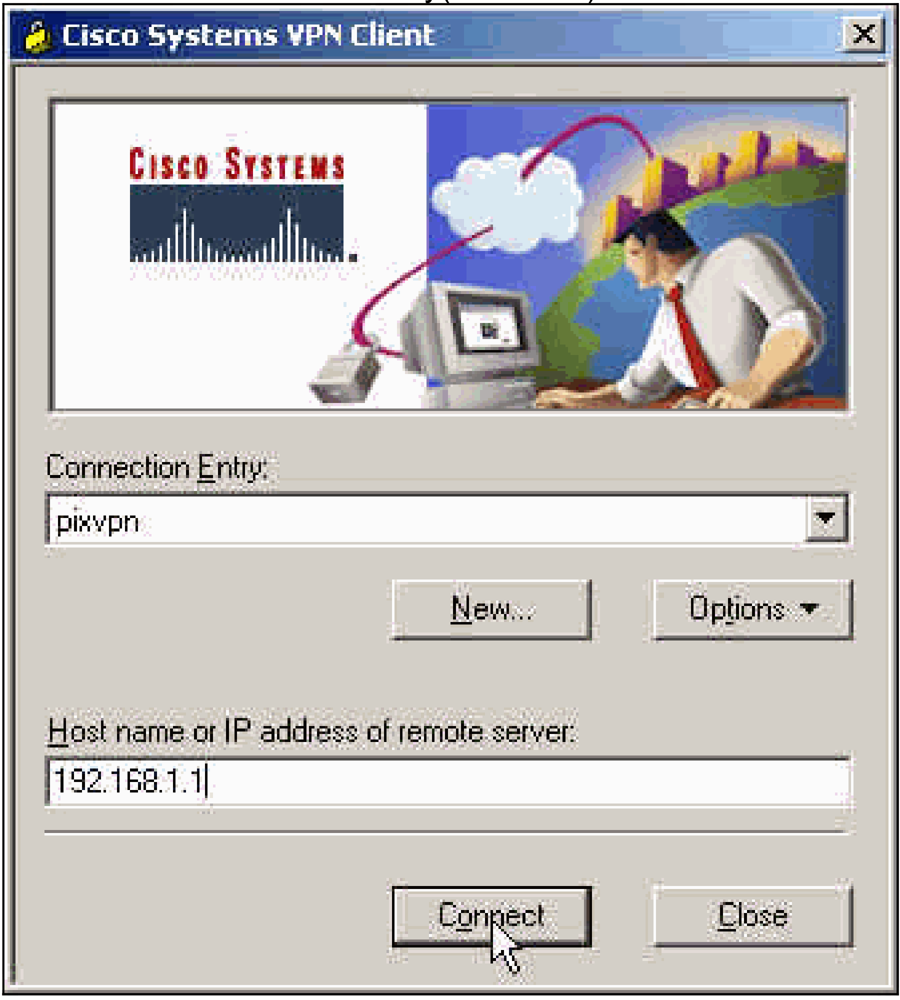
pixvpn

Click Finish to save this entry.

To connect to the remote network, select the Connect button from the main window.

To modify this connection entry, click Options on the main window and select Properties from the menu that appears.

7. 다이얼러에서 Connection Entry(연결 항목)를 선택하고 **Connect(연결)**를 클릭합니다

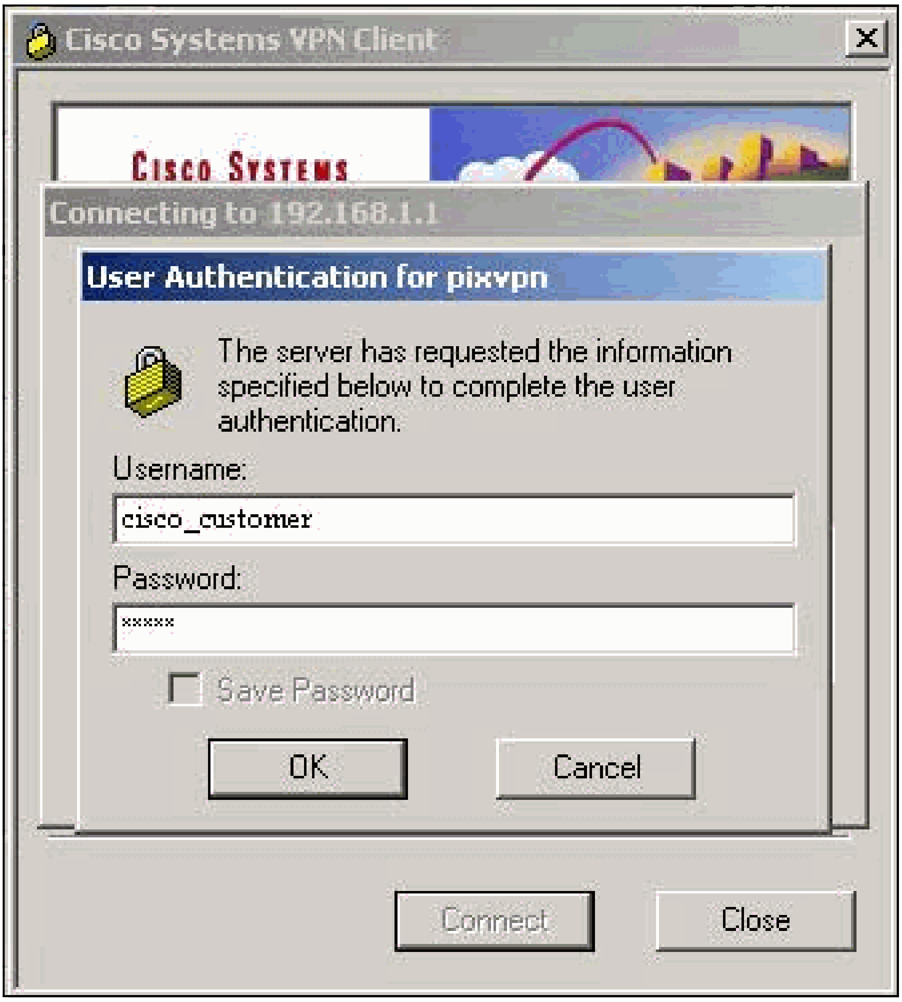


Cisco Systems VPN Client

Connection Entry: pixvpn

Host name or IP address of remote server: 192.168.1.1

8. 프롬프트가 표시되면 Xauth에 대한 사용자 이름 및 비밀번호 정보를 입력하고 **OK**를 클릭하여



The server has requested the information specified below to complete the user authentication.

Username: cisco_customer

Password: *****

원격 네트워크에 연결합니다.

VPN 클라이언트 1.1 구성

```
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
         Encryp 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
```

계정 추가

어카운팅을 추가하는 명령의 구문은 다음과 같습니다.

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

예를 들어, PIX 컨피그레이션에서 다음 명령이 추가됩니다.

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

참고: Xauth 어카운팅이 작동하려면 sysopt ipsec **pl-compatible** 명령이 아닌 sysopt connection permit-ipsec 명령이 필요합니다. Xauth 어카운팅은 sysopt ipsec p**l-compatible** 명령에서만 작동하지 않습니다. Xauth 어카운팅은 ICMP 또는 UDP가 아닌 TCP 연결에 유효합니다.

이 출력은 TACACS+ 계정 레코드의 예입니다.

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

클라이언트측 디버그를 보려면 Cisco Secure Log Viewer를 활성화합니다.

- **debug crypto ipsec** - 2단계의 IPsec 협상을 확인하는 데 사용됩니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 확인하는 데 사용됩니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. 샘플 디버그 출력도 표시됩니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto engine** - 암호화 엔진 프로세스를 디버깅하는 데 사용됩니다.

PIX 디버그 샘플

```
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
```

VPN Client 4.x로 디버깅

```
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#
```

VPN Client 1.1을 사용하여 디버깅

```
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
```

관련 정보

- PIX 500 Series 보안 어플라이언스
- PIX 명령 참조
- IPSec 협상/IKE 프로토콜
- IPSec 소개
- Cisco PIX 방화벽을 통한 연결 설정
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems