AES를 사용하여 Cisco VPN Client에서 PIX로 구성하는 방법

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[배경 정보](#)
[구성](#)
[네트워크 다이어그램](#)
[PIX 구성](#)
[VPN 클라이언트 구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 샘플 컨피그레이션에서는 암호화를 위해 Advanced Encryption Standard(AES)를 사용하여 Cisco VPN 클라이언트에서 PIX 방화벽으로 원격 액세스 VPN 연결을 설정하는 방법을 보여줍니다. 이 예에서는 Cisco Easy VPN을 사용하여 보안 채널을 설정하고 PIX 방화벽은 Easy VPN 서버로 구성됩니다.

Cisco Secure PIX Firewall 소프트웨어 릴리스 6.3 이상에서는 사이트 간 및 원격 액세스 VPN 연결을 보호하기 위해 새로운 국제 암호화 표준 AES가 지원됩니다. 이는 DES(Data Encryption Standard) 및 3DES 암호화 알고리즘 외에 추가로 제공됩니다. PIX 방화벽은 128, 192 및 256비트의 AES 키 크기를 지원합니다.

VPN 클라이언트는 Cisco VPN Client 릴리스 3.6.1부터 시작하는 암호화 알고리즘으로 AES를 지원합니다. VPN 클라이언트는 키 크기 128비트 및 256비트만 지원합니다.

사전 요구 사항

요구 사항

이 샘플 컨피그레이션에서는 PIX가 완전히 작동 중이고 조직의 보안 정책에 따라 트래픽을 처리하기 위해 필요한 명령으로 구성된 것으로 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX Software 릴리스 6.3(1)**참고:** 이 설정은 PIX Software Release 6.3(1)에서 테스트되었으며 이후 릴리스에서 모두 작동할 것으로 예상됩니다.
- Cisco VPN Client 버전 4.0.3(A)**참고:** 이 설정은 VPN Client 버전 4.0.3(A)에서 테스트되었지만 이전 릴리스에서 3.6.1 및 최신 릴리스에서 작동합니다.

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 규칙을 참조하십시오.

배경 정보

원격 액세스 VPN은 모바일 인력이 조직의 네트워크에 안전하게 연결해야 하는 요구 사항을 해결합니다. 모바일 사용자는 PC에 설치된 VPN 클라이언트 소프트웨어를 사용하여 보안 연결을 설정할 수 있습니다. VPN 클라이언트는 이러한 요청을 수락하도록 구성된 중앙 사이트 디바이스에 대한 연결을 시작합니다. 이 예에서 중앙 사이트 디바이스는 동적 암호화 맵을 사용하는 Easy VPN 서버로 구성된 PIX 방화벽입니다.

Cisco Easy VPN은 VPN의 구성 및 관리를 쉽게 하여 VPN 구축을 간소화합니다. Cisco Easy VPN Server와 Cisco Easy VPN Remote로 구성됩니다. Easy VPN Remote에서는 최소 컨피그레이션이 필요합니다. Easy VPN Remote에서 연결을 시작합니다. 인증에 성공하면 Easy VPN Server는 VPN 컨피그레이션을 아래로 푸시합니다. PIX 방화벽을 Easy VPN 서버로 구성하는 방법에 대한 자세한 내용은 VPN Remote Access 관리에서 확인할 수 있습니다.

동적 암호화 맵은 VPN을 설정하는 데 필요한 일부 매개변수를 미리 지정할 수 없는 경우 IPsec 컨피그레이션에 사용됩니다. 동적 할당 IP 주소를 가져오는 모바일 사용자의 경우입니다. 동적 암호화 맵은 템플릿 역할을 하며 누락된 매개변수는 IPsec 협상 중에 결정됩니다. 동적 암호화 맵에 대한 자세한 내용은 동적 암호화 맵에서 확인할 수 있습니다.

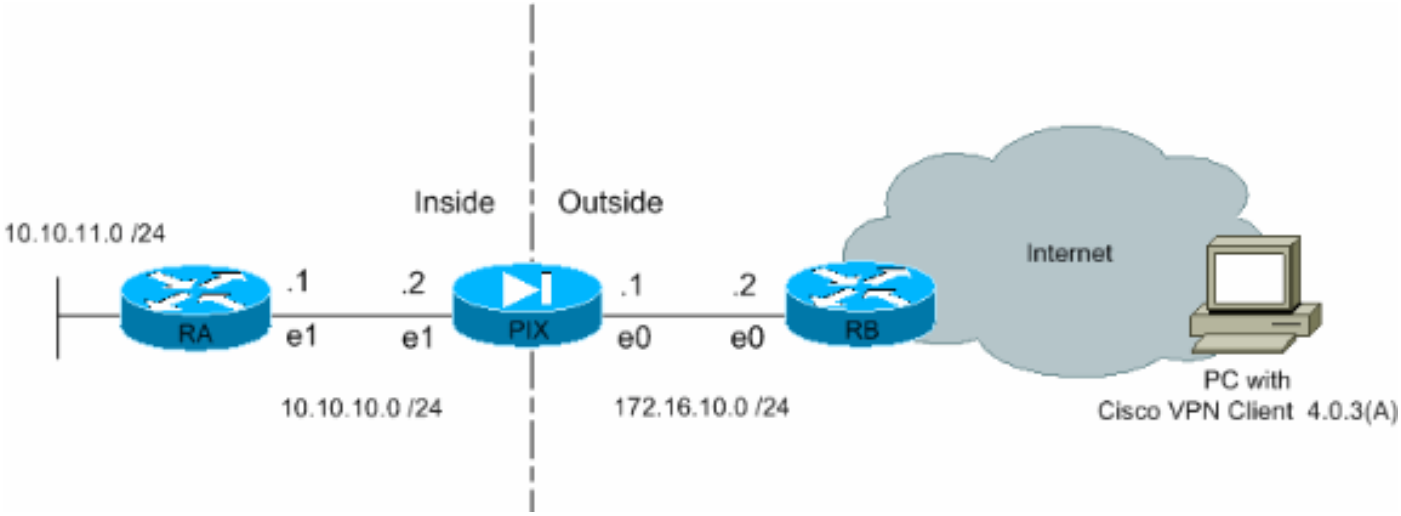
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



PIX 구성

PIX 방화벽에 필요한 컨피그레이션이 이 출력에 표시됩니다. 컨피그레이션은 VPN에만 적용됩니다 .

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
```

참고: 이 설정에서는 변환 세트 또는 ISAKMP 정책을 구성하는 동안 aes-192를 지정하지 않는 것이 좋습니다. VPN 클라이언트는 암호화를 위해 aes-192를 지원하지 않습니다.

참고: 이전 버전에서는 IKE Mode Configuration 명령**이 isakmp 클라이언트 컨피그레이션 주소 풀** 및 **암호화 맵 클라이언트 컨피그레이션 주소가** 필요합니다. 그러나 최신 버전(3.x 이상)에서는 이러한 명령이 더 이상 필요하지 않습니다. 이제 vpngroup address-**pool** 명령을 사용하여 여러 주소 풀을 지정할 수 있습니다.

참고: VPN 그룹 이름은 대/소문자를 구분합니다. 이는 PIX에 지정된 그룹 이름과 VPN 클라이언트의 그룹 이름이 문자 대/소문자(대문자 또는 소문자)와 다른 경우 사용자 인증이 실패함을 의미합니다.

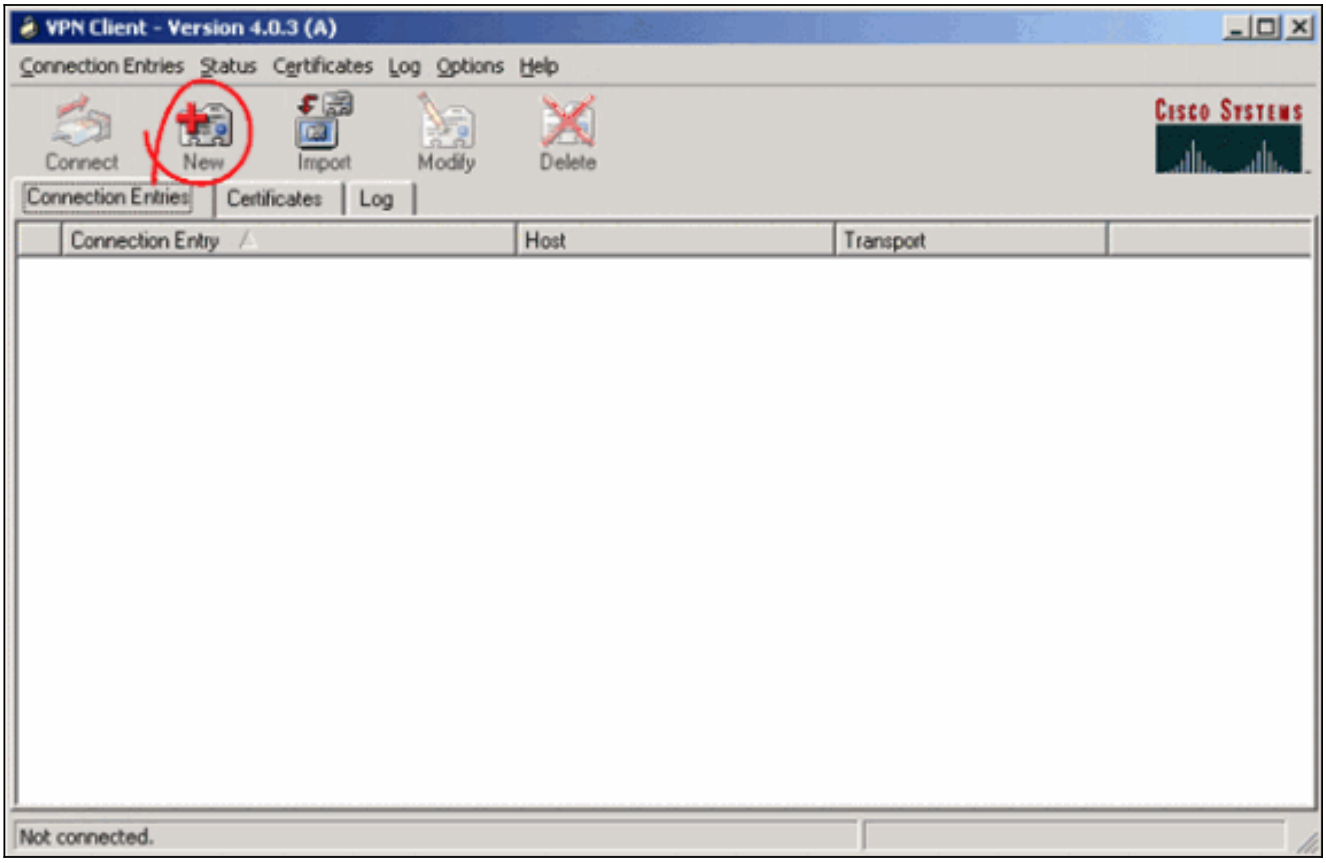
참고: 예를 들어 한 장치에서 그룹 이름을 **GroupMarketing**으로 입력하고 다른 장치에서 그룹 **마케팅**을 입력하면 디바이스가 작동하지 않습니다.

VPN 클라이언트 구성

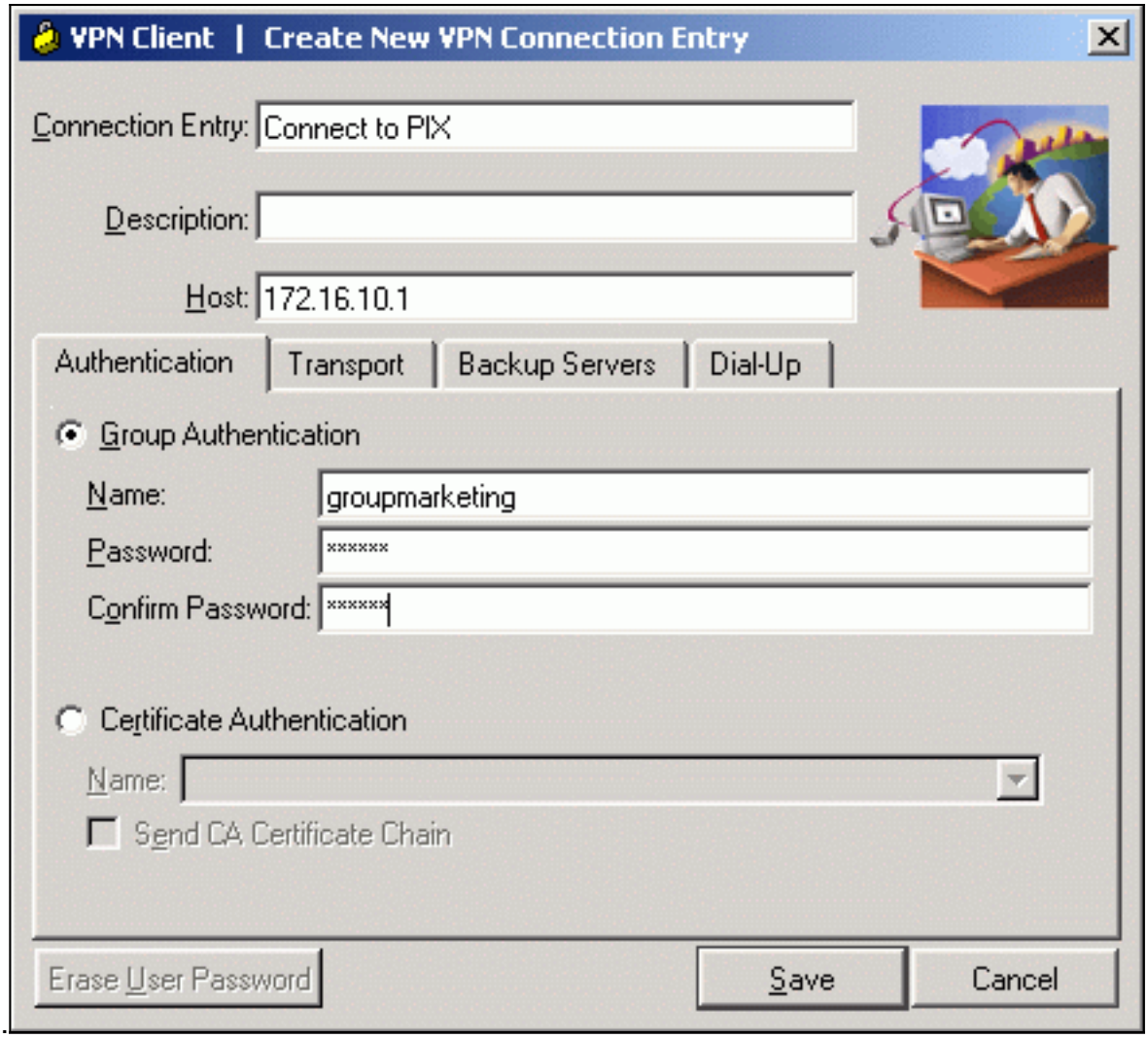
PC에 VPN Client를 설치한 후 다음 단계와 같이 새 연결을 생성합니다.

1. VPN Client 애플리케이션을 시작하고 New(**새로 만들기**)를 클릭하여 새 연결 항목을 생성합니다

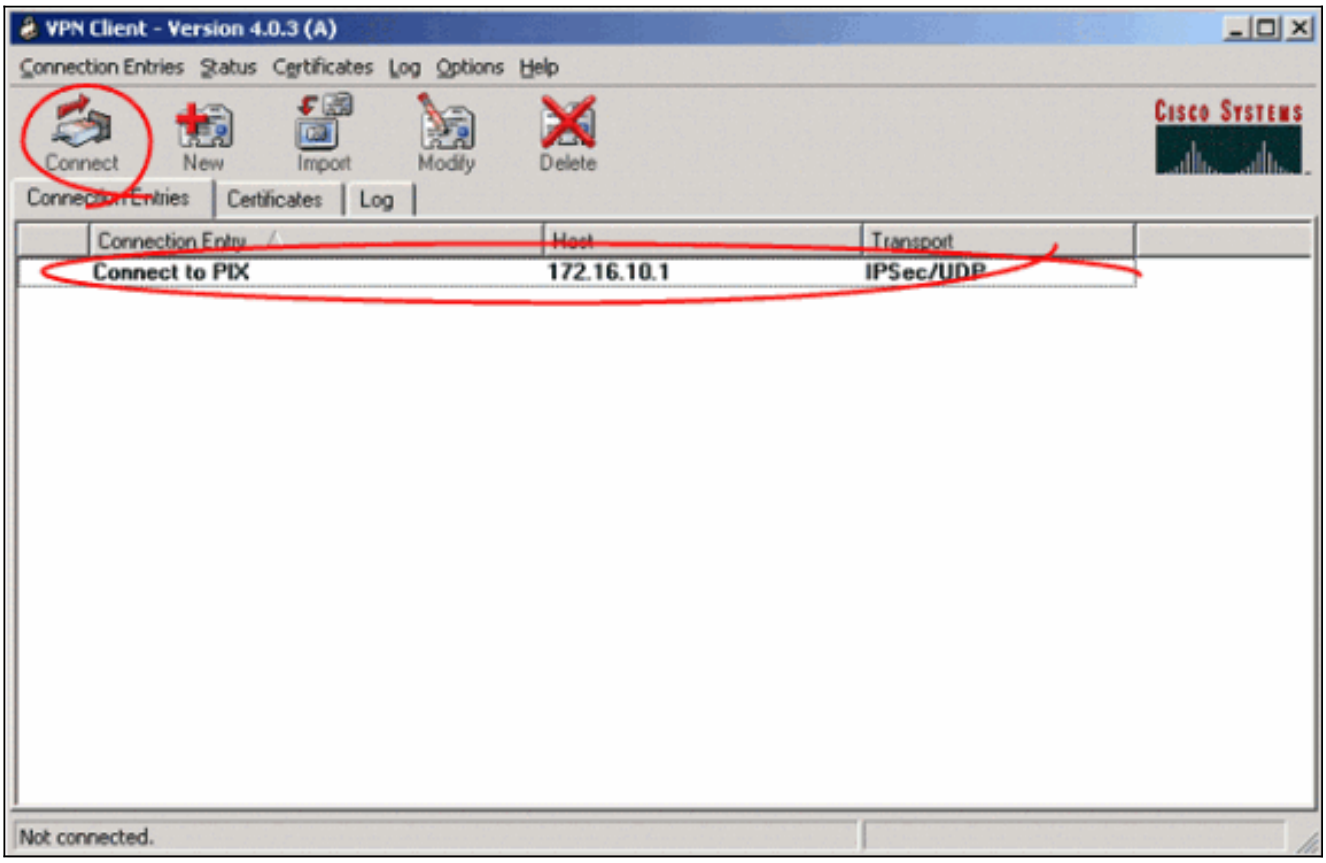
.



2. VPN Client라는 이름의 새 대화 상자 | Create New VPN Connection Entry가 나타납니다. 새 연결에 대한 구성 정보를 입력합니다.Connection Entry(연결 항목) 필드에서 생성된 새 항목에 이름을 할당합니다.Host 필드에 PIX의 공용 인터페이스의 IP 주소를 입력합니다 .Authentication(인증) 탭을 선택한 다음 그룹 이름 및 비밀번호(확인을 위해 두 번)를 입력합니다. vpngroup password 명령을 사용하여 PIX에 입력한 정보와 일치해야 **합니다**.Save(**저장**)를 클릭하여 입력한 정보를 저장합니다. 이제 새 연결이 생성됩니다



3. 새 연결 항목을 사용하여 게이트웨이에 연결하려면 연결 항목을 한 번 클릭하여 선택한 다음 **연결** 아이콘을 클릭합니다. 연결 항목을 두 번 클릭하면 동일한 효과가 나타납니다

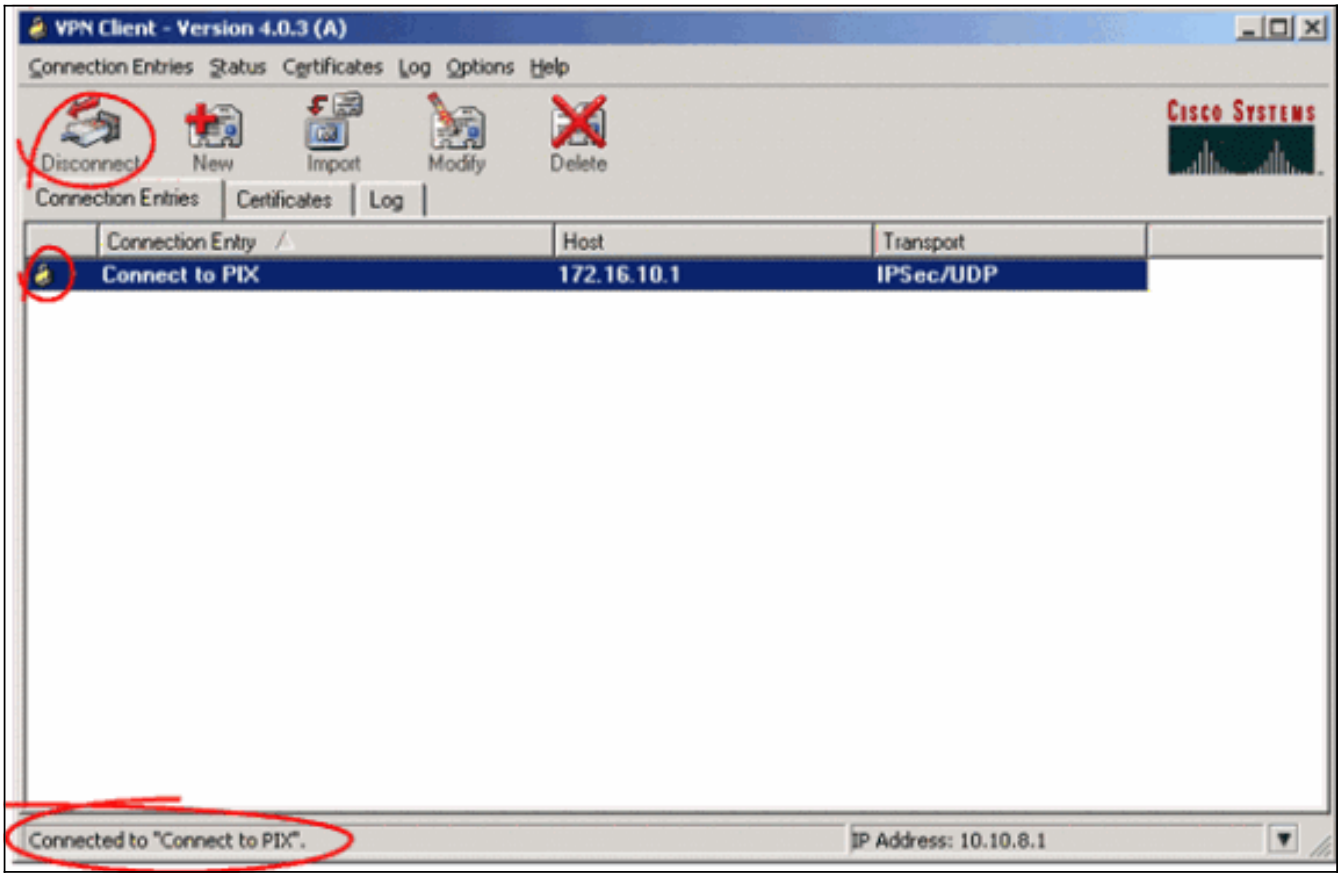


다음을 확인합니다.

VPN 클라이언트에서 원격 게이트웨이에 성공적으로 설정된 연결은 다음 항목으로 표시됩니다.

- 활성 연결 항목에 대해 노란색 닫힌 잠금 아이콘이 나타납니다.
- Connection Entries(연결 항목) 탭 옆에 있는 도구 모음의 Connect(연결) 아이콘이 Disconnect(연결 끊기)로 변경됩니다.
- 창 끝에 있는 상태 줄은 상태를 "연결 대상"으로 표시하고 연결 항목 이름을 표시합니다

.



참고: 기본적으로 연결이 설정되면 VPN 클라이언트는 Windows 작업 표시줄의 오른쪽 아래 모서리에 있는 시스템 트레이에서 잠금 아이콘이 최소화됩니다. VPN Client(VPN 클라이언트) 창을 다시 표시하려면 닫힌 잠금 아이콘을 두 번 클릭합니다.

PIX 방화벽에서 이 **show** 명령을 사용하여 설정된 연결의 상태를 확인할 수 있습니다.

참고: 특정 **show** 명령은 Output Interpreter Tool(등록된 고객만 해당)에서 지원되므로 **show** 명령 출력의 분석을 볼 수 있습니다.

- **show crypto ipsec sa** - PIX의 현재 IPsec SA를 모두 표시합니다. 또한 출력에 원격 피어의 실제 IP 주소, 할당된 IP 주소, 로컬 IP 주소 및 인터페이스, 적용된 암호화 맵이 표시됩니다.

```
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** - 피어 간에 구축된 ISAKMP SA의 상태를 표시합니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

이러한 디버그 명령은 VPN 설정 문제를 해결하는 데 도움이 될 수 있습니다.

참고: 디버그 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto isakmp** - 빌드된 ISAKMP SA와 협상된 IPsec 특성을 표시합니다. ISAKMP SA 협상 중에 PIX는 여러 제안을 수락하기 전에 "수락 불가"로 폐기할 수 있습니다. ISAKMP SA가 합의되면 IPsec 특성이 협상됩니다. 이 디버그 출력에 나와 있는 것처럼 여러 제안서가 승인되기

전에 거부될 수 있습니다.

```
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** - IPsec SA 협상에 대한 정보를 표시합니다.

```
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
```

이 문서에 표시된 컨피그레이션을 통해 VPN 클라이언트는 AES를 사용하여 중앙 사이트 PIX에 성공적으로 연결할 수 있습니다. VPN 터널이 성공적으로 설정되었지만 사용자가 네트워크 리소스 ping, 도메인에 로그온 또는 네트워크 환경 찾아보기 등의 일반적인 작업을 수행할 수 없는 경우가 있습니다. 이러한 문제를 해결하는 방법에 대한 자세한 내용은 Cisco VPN 클라이언트를 사용하여 VPN 터널을 설정한 후 Microsoft 네트워크 환경 문제 해결을 참조하십시오.

관련 정보

- 고급 암호화 표준(AES)
- IPSec(IP Security) 암호화 소개
- IP 보안 문제 해결 - 디버그 명령 이해 및 사용
- IPsec 협상/IKE 프로토콜 지원 페이지
- PIX 지원 페이지
- Cisco VPN 클라이언트 지원 페이지
- PIX 명령 참조
- 기술 지원 및 문서 – Cisco Systems