Stick 컨피그레이션의 공용 인터넷용 라우터 및 VPN 클라이언트 예

목차

소개

이 문서에서는 스틱에서 IPsec 트래픽을 수행하도록 중앙 사이트 라우터를 설정하는 방법에 대해 설명합니다.이 설정은 라우터가 스플릿 터널링을 활성화하지 않고 모바일 사용자(Cisco VPN Client)가 중앙 사이트 라우터를 통해 인터넷에 액세스할 수 있는 특정 경우에 적용됩니다.이를 위해 라우터에서 모든 VPN 트래픽(Cisco VPN Client)을 루프백 인터페이스에 가리키도록 정책 맵을 구성합니다.이를 통해 인터넷 트래픽이 PATed(port address translated)를 외부 세상으로 변환할 수 있습니다.

중앙 사이트 PIX 방화벽에서 유사한 컨피그레이션을 완료하려면 Stick 컨피그레이션 예에서 PIX/ASA 7.x 및 VPN Client for Public Internet VPN(공용 인터넷 VPN용 PIX/ASA 7.x 및 VPN 클라이언트)을 참조하십시오.

참고: 네트워크에서 IP 주소가 중복되지 않도록 하려면 완전히 다른 IP 주소 풀을 VPN 클라이언트에 할당합니다(예: 10.x.x.x, 172.16.x.x, 192.168.x.x). 이 IP 주소 지정 체계는 네트워크 문제를 해결하는 데 도움이 됩니다.

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 IOS® 소프트웨어 릴리스 12.4가 포함된 Cisco Router 3640
- Cisco VPN Client 4.8

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.

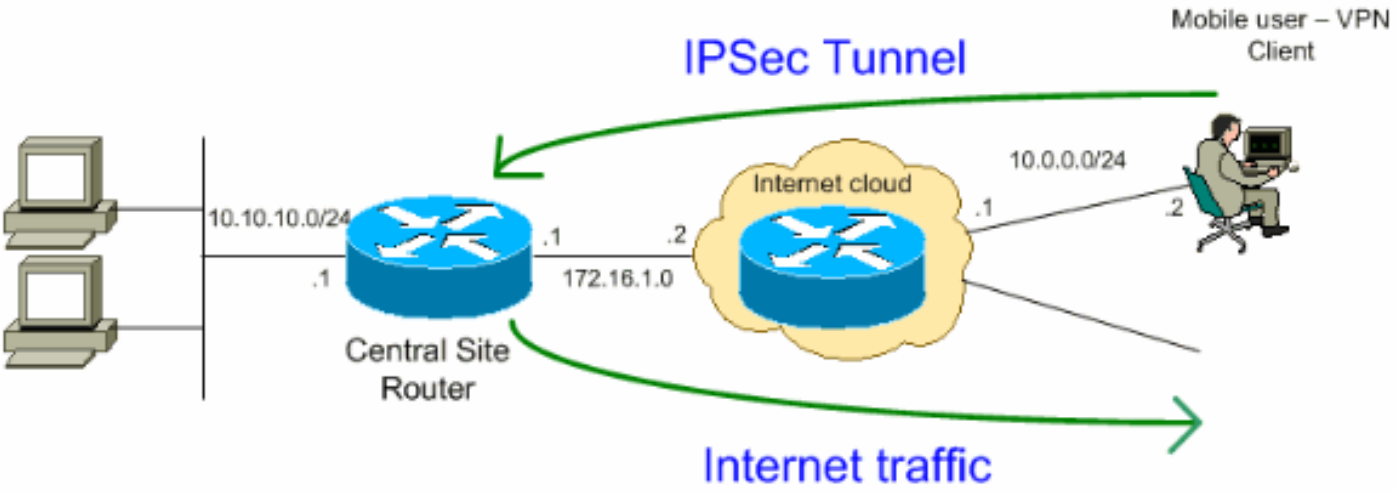
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- 라우터
- Cisco VPN 클라이언트

라우터

```
 VPN#show run
Building configuration...

Current configuration : 2170 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
!
boot-start-marker
boot-end-marker
!
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.


aaa authentication login userauthen local

!--- In order to enable group authorization, enable !---
the aaa authorization commands.

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!--- For local authentication of the IPsec user, !---
create the user with a password. username user password
0 cisco
!
!
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2

!--- Create a group that is used to specify the !---
WINS and DNS server addresses to the VPN Client, !---
along with the pre-shared key for authentication. crypto
isakmp client configuration group vpnclient
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
```

```
esp-md5-hmac
!

!--- Create a dynamic map and apply !--- the transform
set that was created earlier. crypto dynamic-map dynmap
10
 set transform-set myset
 reverse-route
!

!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
!--- Create the loopback interface for the VPN user
traffic . interface Loopback0
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
 ip nat inside

!--- Apply the crypto map on the interface. interface
FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip policy route-map VPN-Client
 duplex auto
 speed auto
 crypto map clientmap
!
interface Serial2/0
 no ip address
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ! ip local pool ippool 192.168.1.1
192.168.1.2
ip http server
no ip http secure-server
!
ip route 10.0.0.0 255.255.255.0 172.16.1.2
```

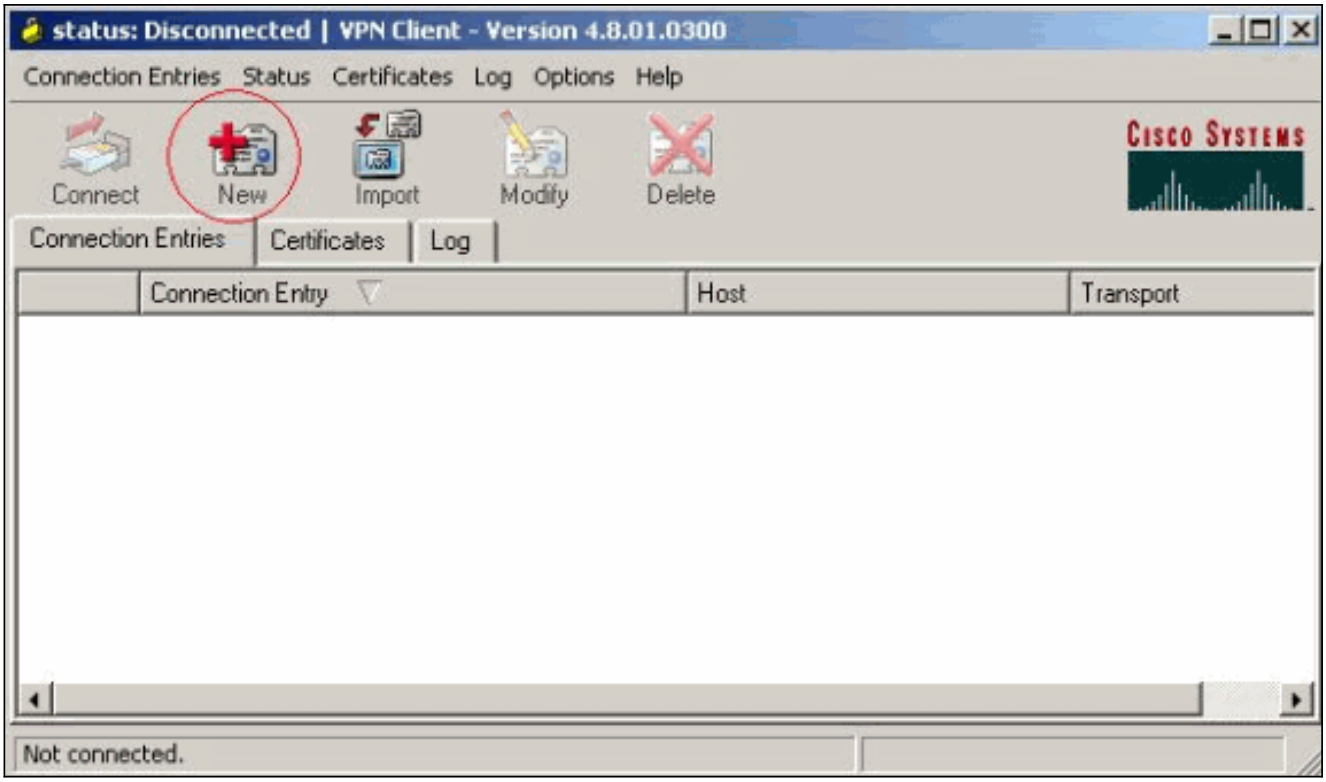
```
!--- Enables Network Address Translation (NAT) !--- of
the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address. ip
nat inside source list 101 interface FastEthernet1/0
overload
!
!--- The access list is used to specify which traffic is
to be translated for the !--- outside Internet. access-
list 101 permit ip any any

!--- Interesting traffic used for policy route. access-
list 144 permit ip 192.168.1.0 0.0.0.255 any
!--- Configures the route map to match the interesting
traffic (access list 144) !--- and routes the traffic to
next hop address 10.11.0.2. ! route-map VPN-Client
permit 10
 match ip address 144
 set ip next-hop 10.11.0.2
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end
```

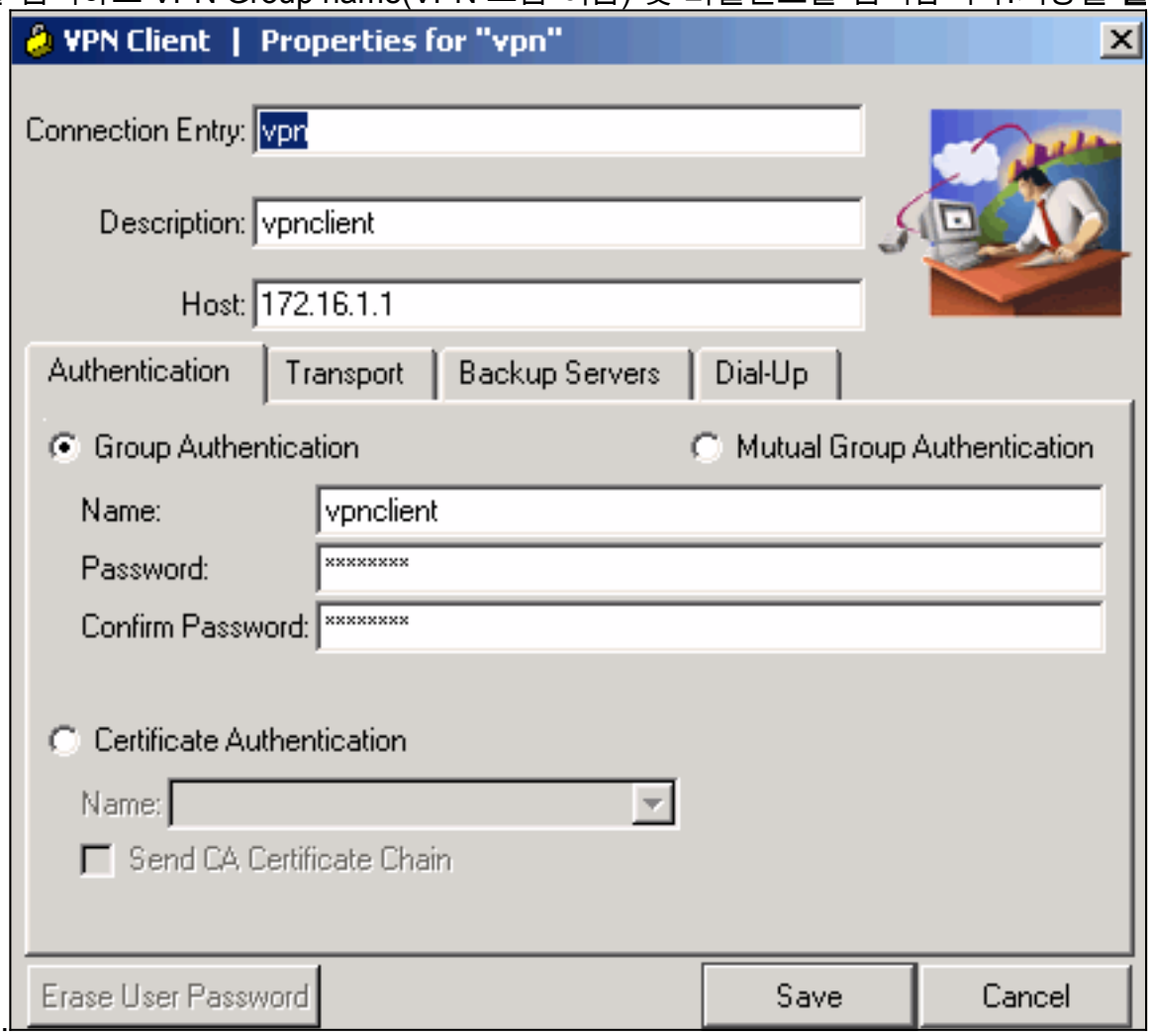
VPN Client 4.8 구성

VPN Client 4.8을 구성하려면 다음 단계를 완료하십시오.

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

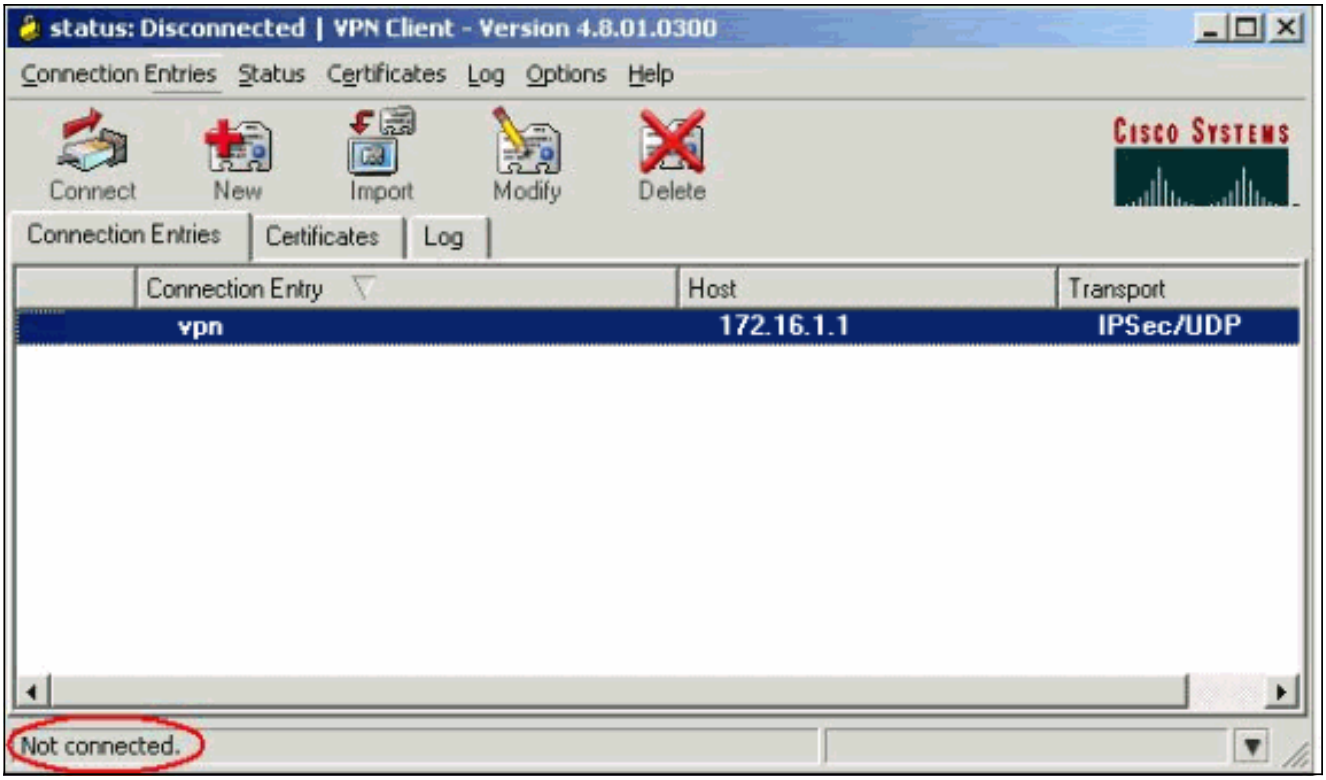


3. Connection Entry(연결 항목)의 이름과 설명을 입력하고 Host(호스트) 상자에 라우터의 외부 IP 주소를 입력하고 VPN Group name(VPN 그룹 이름) 및 비밀번호를 입력합니다.저장을 클릭합니다.



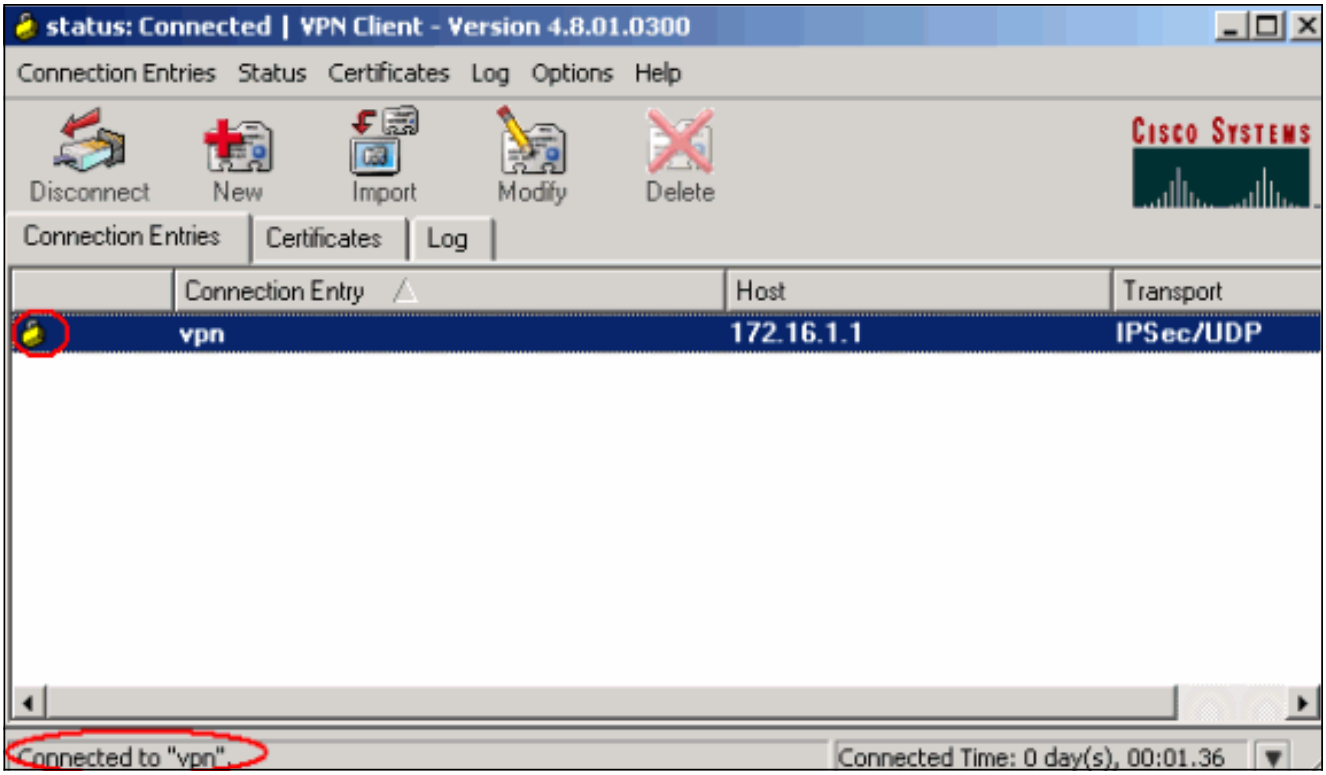
4. 사용할 연결을 클릭하고 VPN Client 주 창에서 **Connect(연결)**를 클릭합니다

.

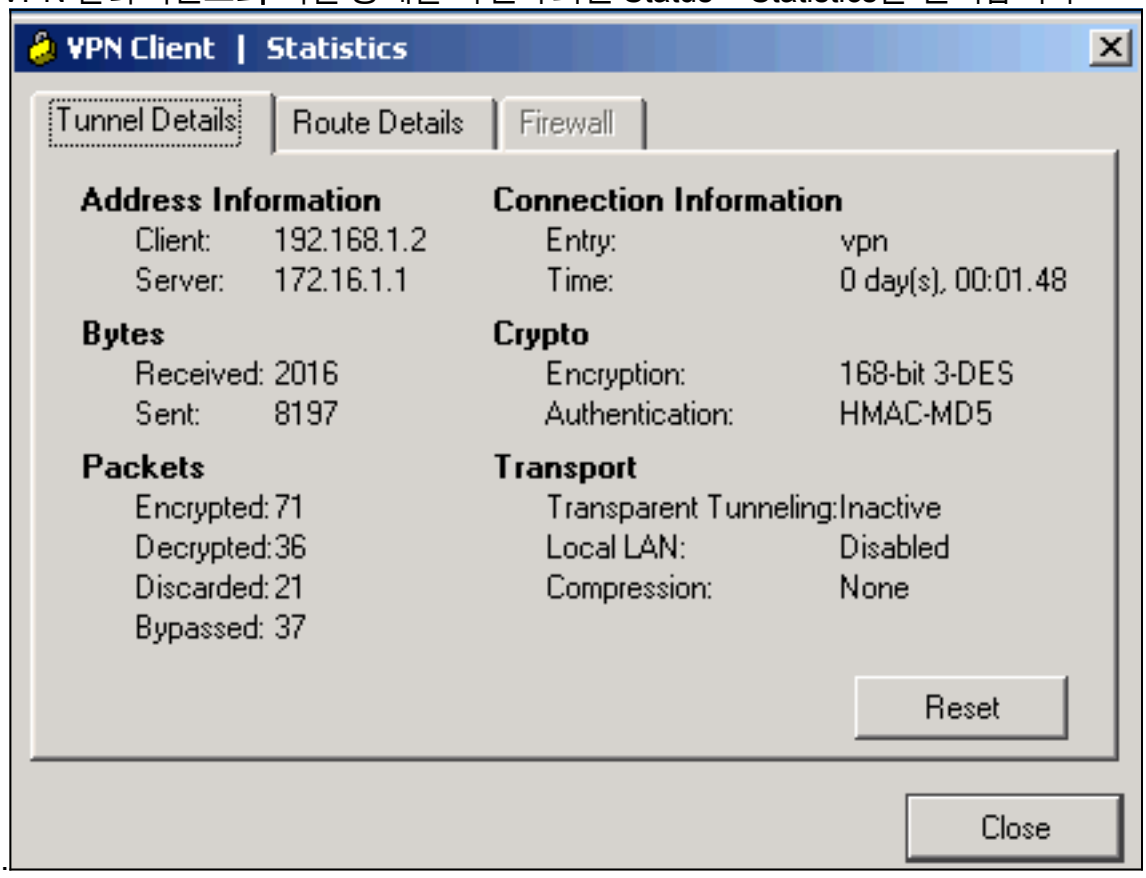


5. 프롬프트가 표시되면 Xauth에 대한 사용자 이름 및 비밀번호 정보를 입력하고 **OK**를 클릭하여 원격 네트워크에 연결합니다

6. VPN 클라이언트는 중앙 사이트의 라우터에 연결됩니다



7. VPN 클라이언트의 터널 통계를 확인하려면 Status > Statistics를 선택합니다



.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

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

- **show crypto isakmp sa** - 피어의 현재 IKE SA(Security Associations)를 모두 표시합니다.

```
VPN#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: clientmap, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={}
    #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270
    #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0xEF7C20EA(4017889514)

     inbound esp sas:
      spi: 0x17E0CBEC(400608236)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: clientmap
        sa timing: remaining key lifetime (k/sec): (4530341/3288)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xEF7C20EA(4017889514)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: clientmap
        sa timing: remaining key lifetime (k/sec): (4530354/3287)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 표시합니다.

```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        QM_IDLE              15    0 ACTIVE
```

문제 해결

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 ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

관련 정보

- IPsec 협상/IKE 프로토콜
- Cisco VPN Client - 제품 지원
- Cisco 라우터 - 제품 지원
- 기술 지원 및 문서 – Cisco Systems