ASA/PIX:CLI 및 ASDM 컨피그레이션을 사용하는 IPSec VPN 클라이언트의 고정 IP 주소 지정 예

목차

소개

이 문서에서는 ASDM(Adaptive Security Device Manager) 또는 CLI를 사용하여 VPN 클라이언트에 고정 IP 주소를 제공하도록 Cisco 5500 Series ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.ASDM은 직관적이고 사용하기 쉬운 웹 기반 관리 인터페이스를 통해 세계적인 수준의 보안 관리 및 모니터링을 제공합니다.Cisco ASA 컨피그레이션이 완료되면 Cisco VPN Client를 통해 확인할 수 있습니다.

Cisco VPN Client(4.x for Windows)와 PIX 500 Series Security Appliance 7.x 간의 원격 액세스 VPN 연결을 설정하려면 Windows 2003 IAS RADIUS를 사용하는 PIX/ASA 7.x 및 Cisco VPN Client 4.x(Active Directory에 대해) 인증 컨피그레이션 예를 참조하십시오.원격 VPN 클라이언트 사용자는 Microsoft Windows 2003 IAS(Internet Authentication Service) RADIUS 서버를 사용하여 Active Directory에 대해 인증합니다.

확장 인증(Xauth)을 위해 Cisco VPN Client(4.x for Windows)와 PIX 500 Series Security Appliance 7.x(ACS 버전 3.2) 간의 원격 액세스 VPN 연결을 설정하려면 Cisco Secure ACS Authentication Configuration(Cisco Secure ACS 인증 컨피그레이션)의 PIX/ASA 7.x 및 Cisco VPN Client 4.x를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에서는 ASA가 완전히 작동 중이고 Cisco ASDM 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

참고: ASDM 또는 PIX/ASA 7.x에 대한 HTTPS 액세스 허용을 참조하십시오.ASDM 또는 SSH(Secure Shell)에서 디바이스를 원격으로 구성할 수 있도록 하려면 Inside 및 Outside Interface Configuration Example의 SSH를 사용합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 7.x 이상
- Adaptive Security Device Manager 버전 5.x 이상
- Cisco VPN Client Version 4.x 이상

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.

관련 제품

이 컨피그레이션은 Cisco PIX Security Appliance 버전 7.x 이상에서도 사용할 수 있습니다.

표기 규칙

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

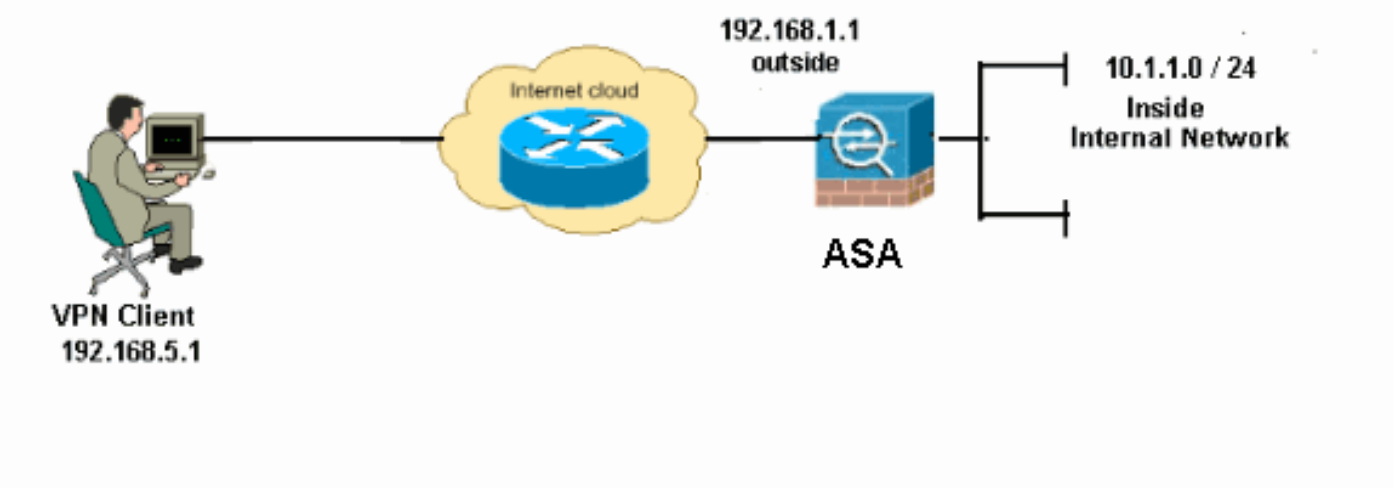
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



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

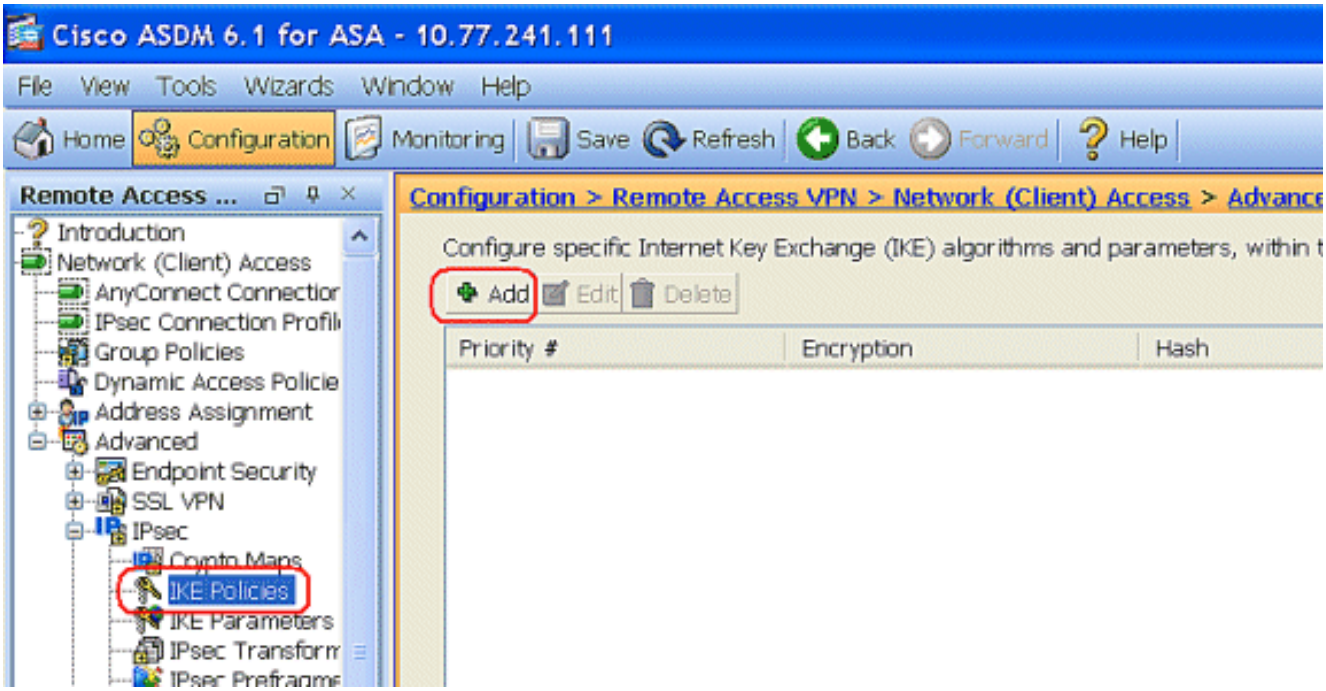
원격 액세스 VPN(IPSec) 구성

ASDM 절차

원격 액세스 VPN을 구성하려면 다음 단계를 완료합니다.

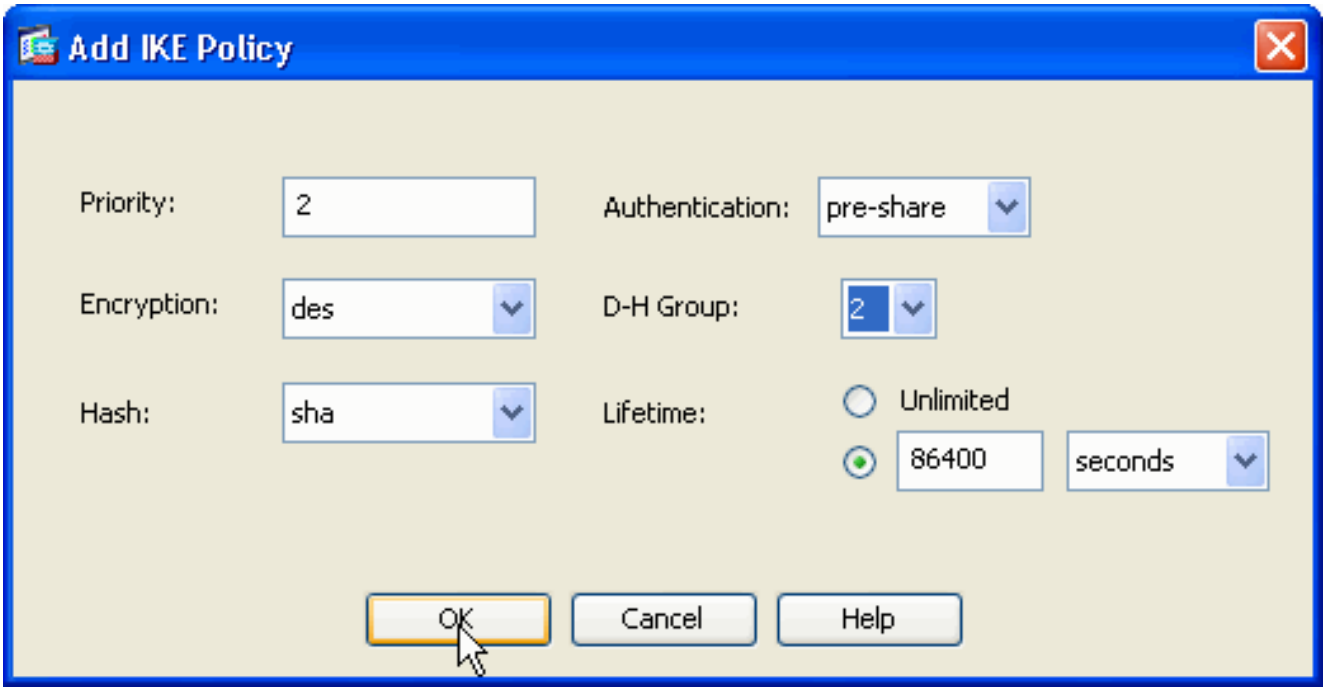
1. ISAKMP **정책을** 생성하려면 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add**를 선택합니다

.



2. ISAKMP 정책 세부 정보를 제공합니다

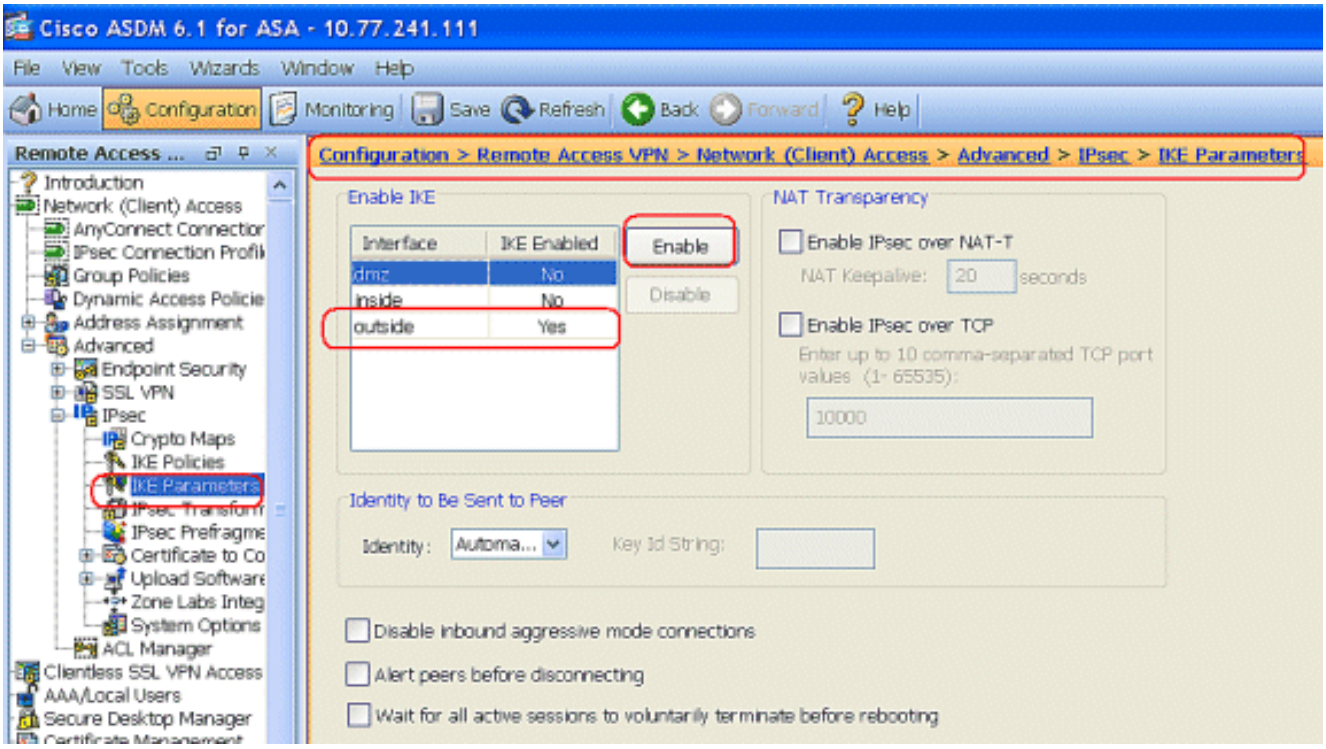
.



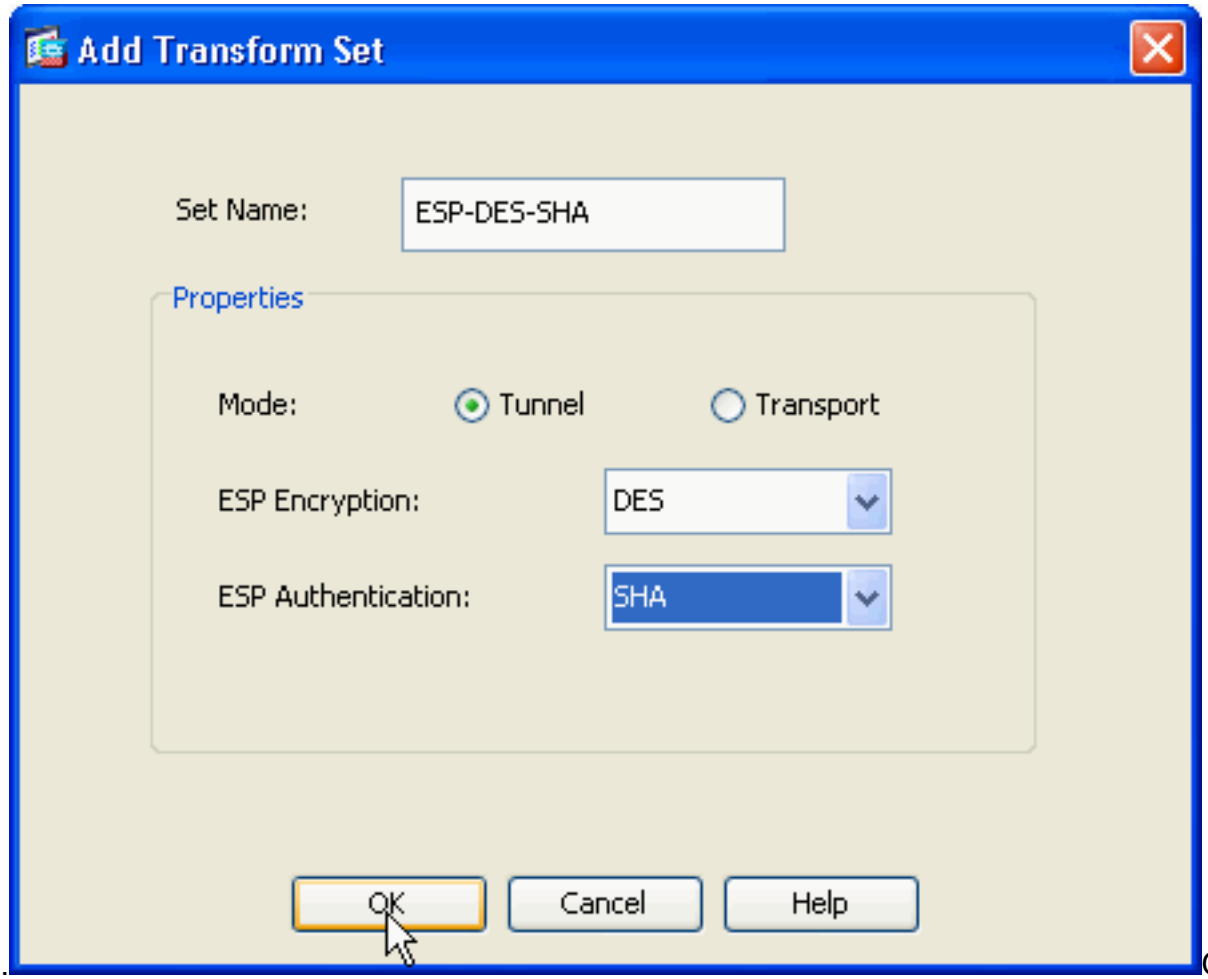
OK(**확인**)와 Apply(적용)를 **클릭합니다**.

3. Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > IKE Parameters(IKE 매개변수)를 선택하여** 외부 인터페이스에서 IKE를 활성화합니다

.



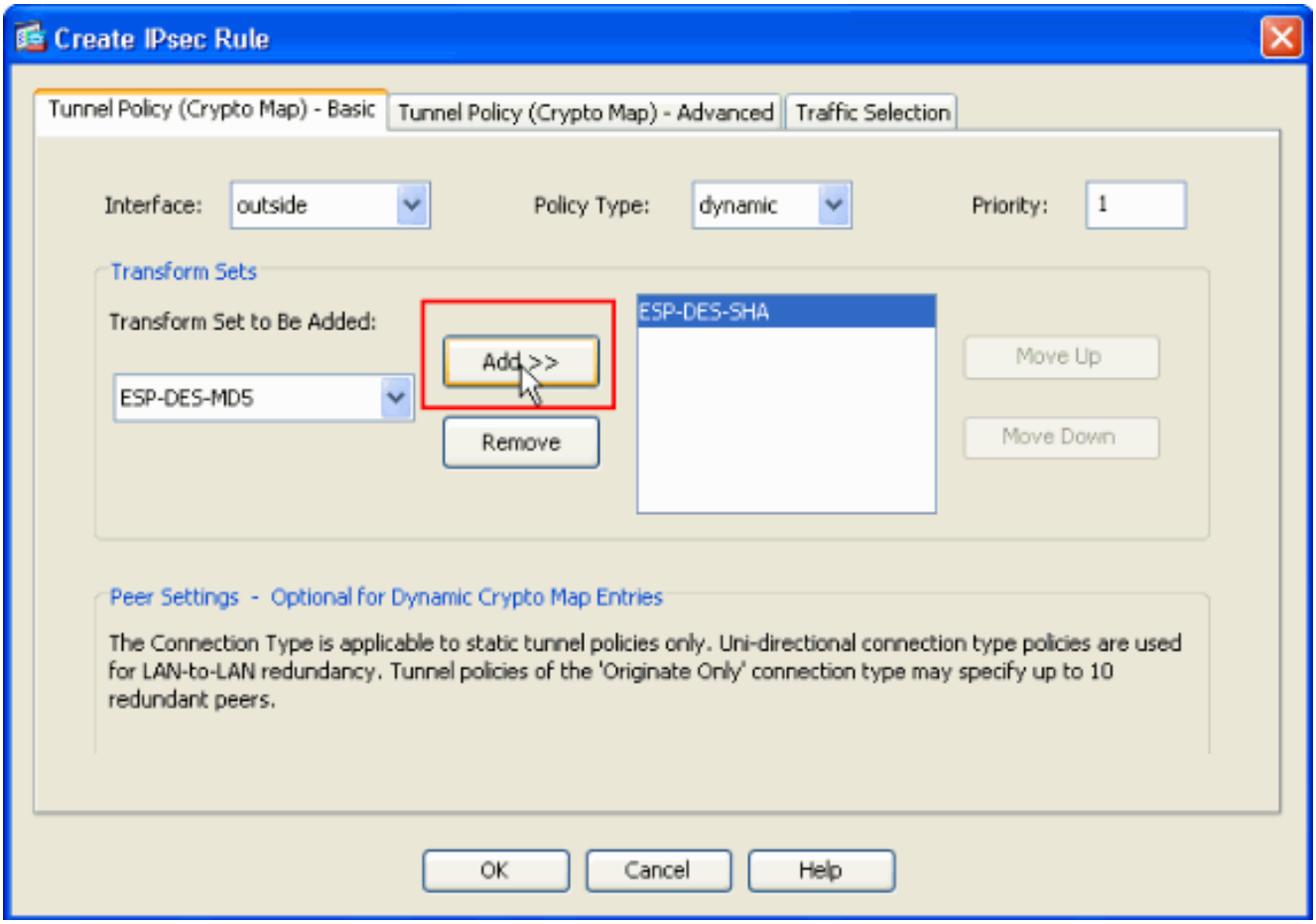
4. Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > IPSec Transform Sets(IPSec 변형 집합) > Add(추가)를** 선택하여 **ESP-DES-SHA** 변형 집합을 생성합니다



. OK(**확인**)와 Apply(적용)를 **클릭합니다**.

5. Configuration(**구성**) **> Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > Crypto Maps(암호화 맵) > Add(추가)를 선택하여** 우선순위 1의 동적 정책으로 암호화 맵을 생성합니다

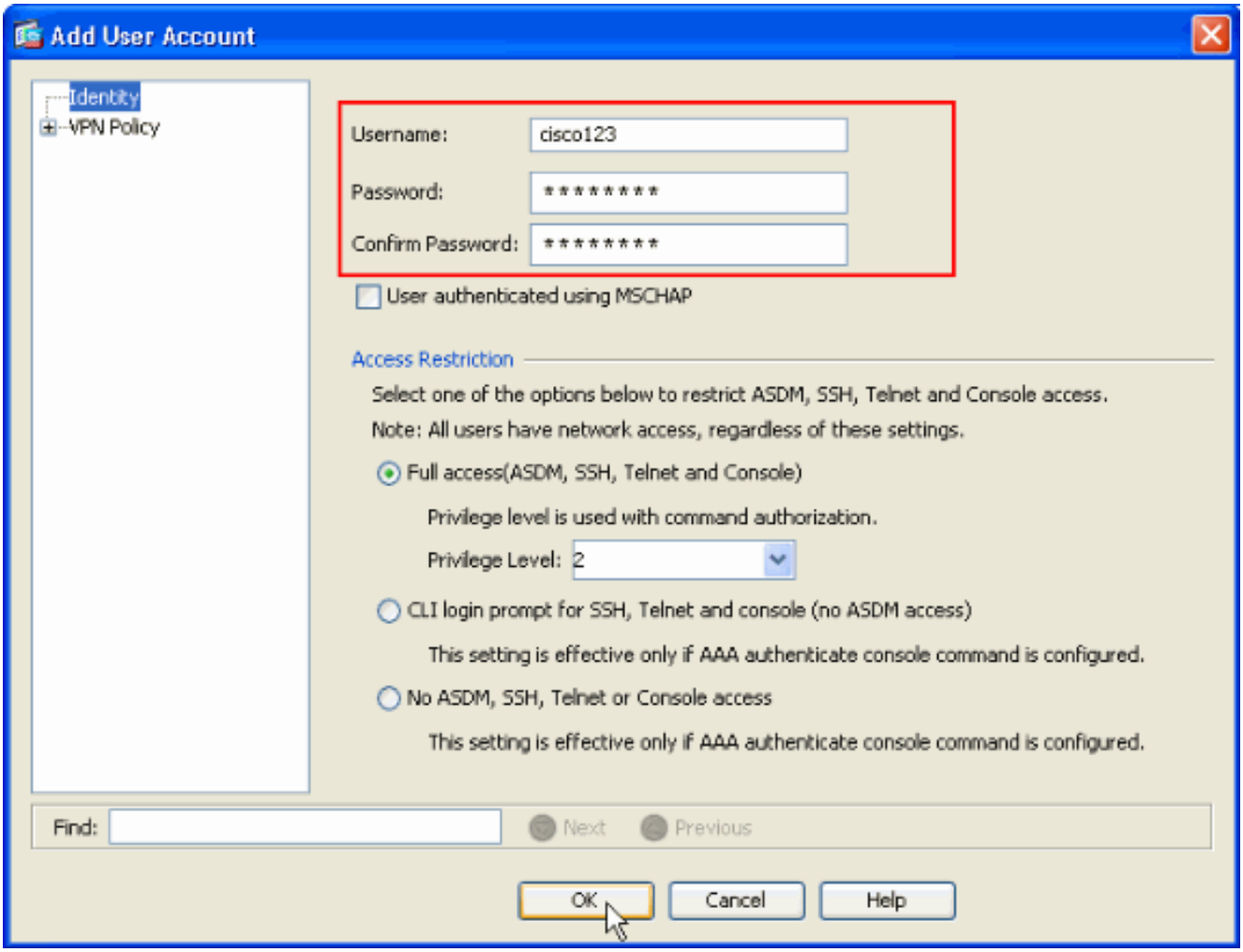
.



OK(**확인**)와 Apply(적용)를 **클릭합니다**.

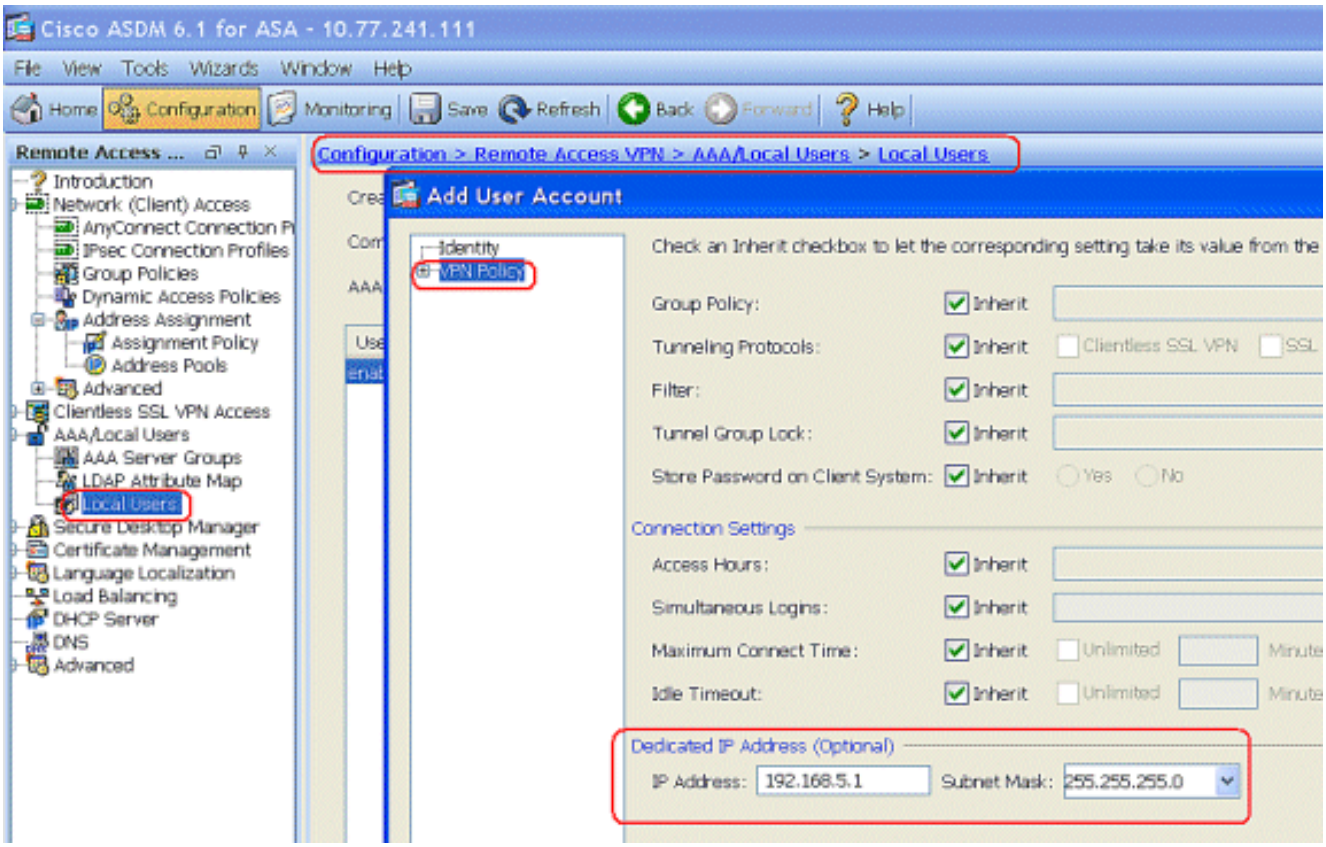
6. VPN 클라이언트 액세스를 위한 사용자 계정(예: 사용자 이름 - cisco123 및 비밀번호 - cisco123)을 생성하려면 Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN)** > **AAA Setup(AAA 설정)** > **Local Users(로컬 사용자)** > **Add(추가)를** 선택합니다

.



7. VPN **Policy(VPN 정책)**로 이동하여 사용자 "cisco123"의 **Static/Dedicated IP Address(고정/전용 IP 주소)**를 다음과 같이 추가합니다

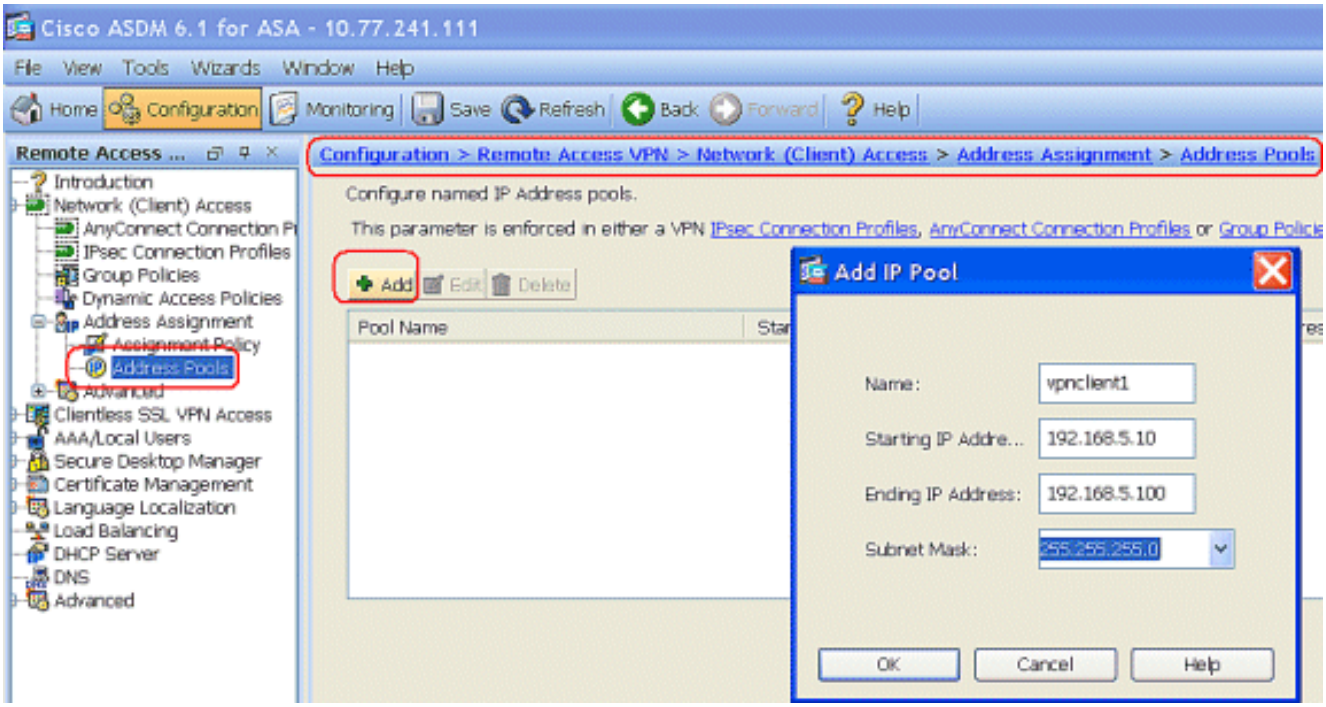
.



8. Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN)** > **Network (Client) Access(네**

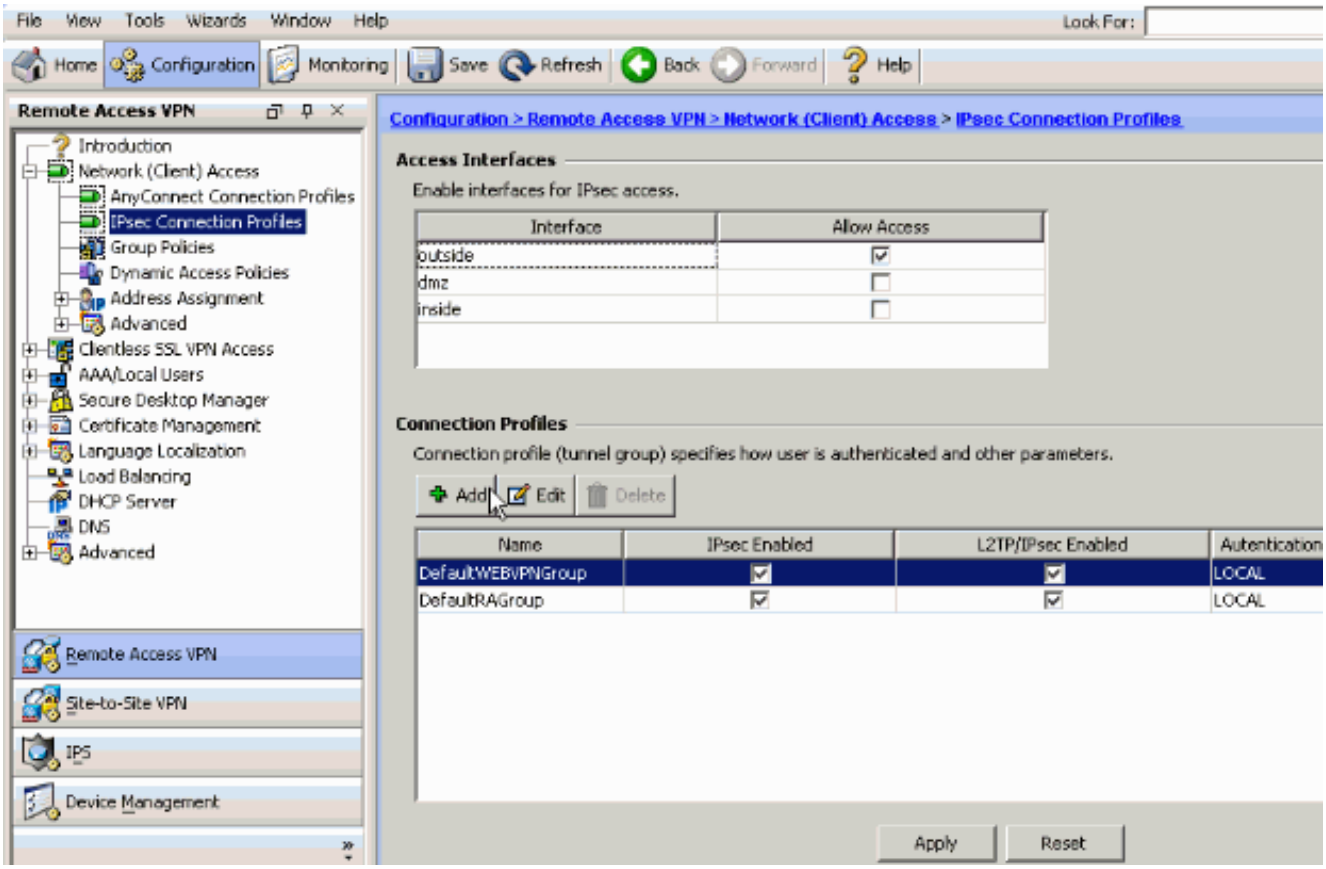
트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Address Pools(주소 풀)를 선택하고 **Add(추가)**를 클릭하여 VPN 클라이언트 사용자용 VPN 클라이언트를 추가합니다

.



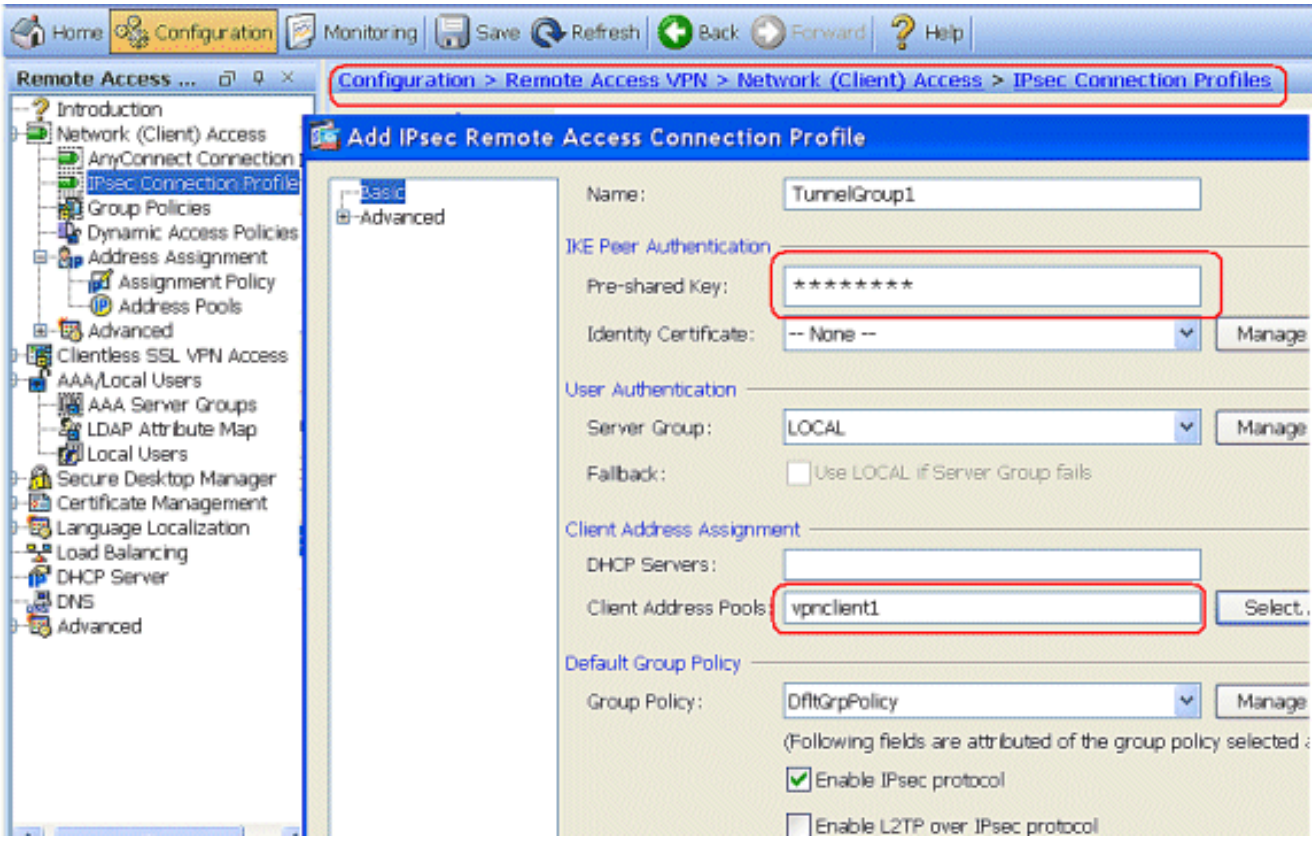
9. 표시된 대로 터널 그룹(예: TunnelGroup1 및 Preshared key as cisco123)을 추가하려면 Configuration(**구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > IPSec Connection Profiles(IPSec 연결 프로파일) > Add(추가)를 선택합니다**

.



Basic(**기본**) 탭에서 User Authentication(사용자 인증) 필드에 대해 LOCAL(로컬)로 서버 그룹을 선택합니다.VPN **클라이언트** 사용자에 대한 클라이언트 주소 풀로 vpnclient1을 선택합니다

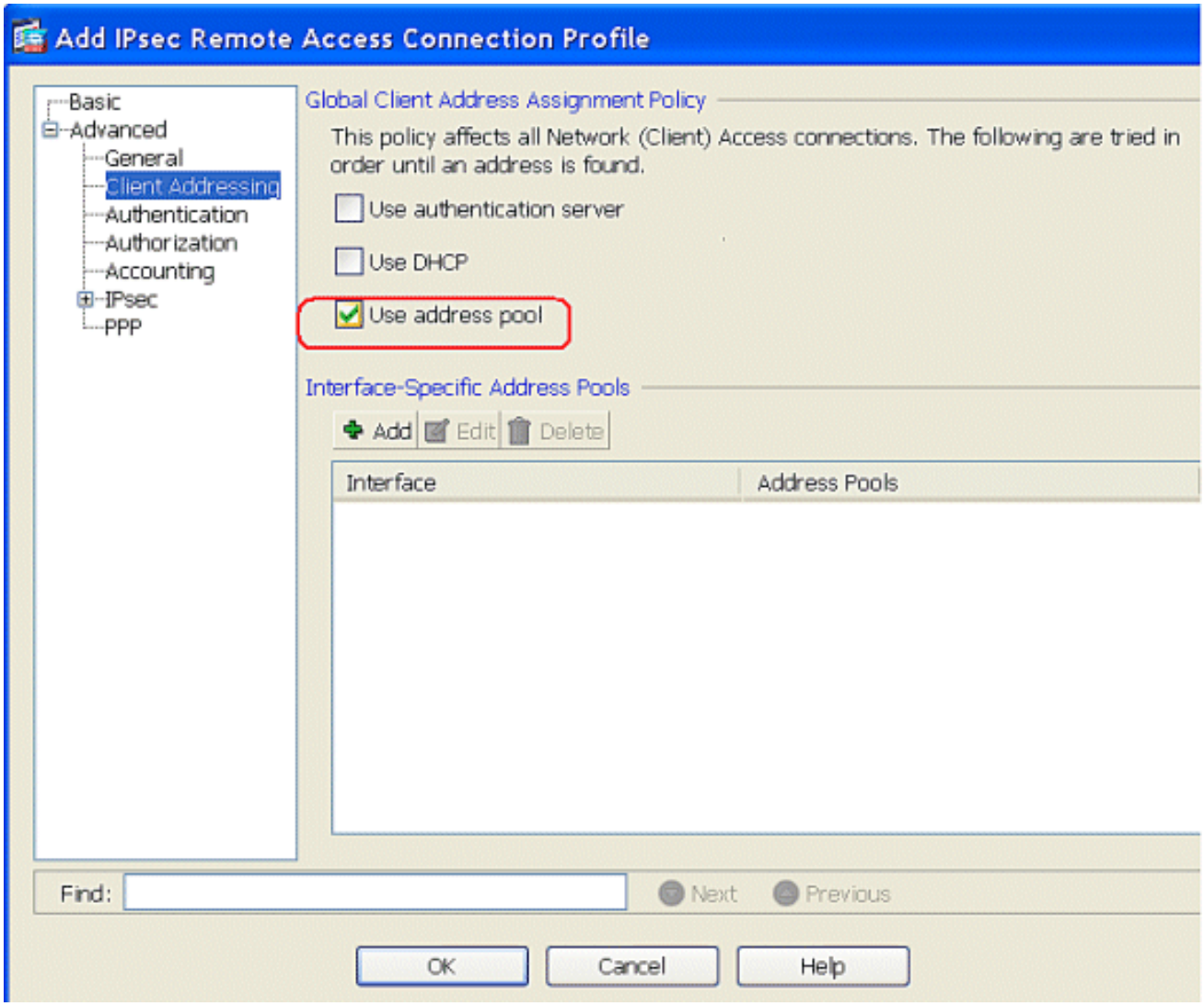
.



확인을 **클릭합니다**.

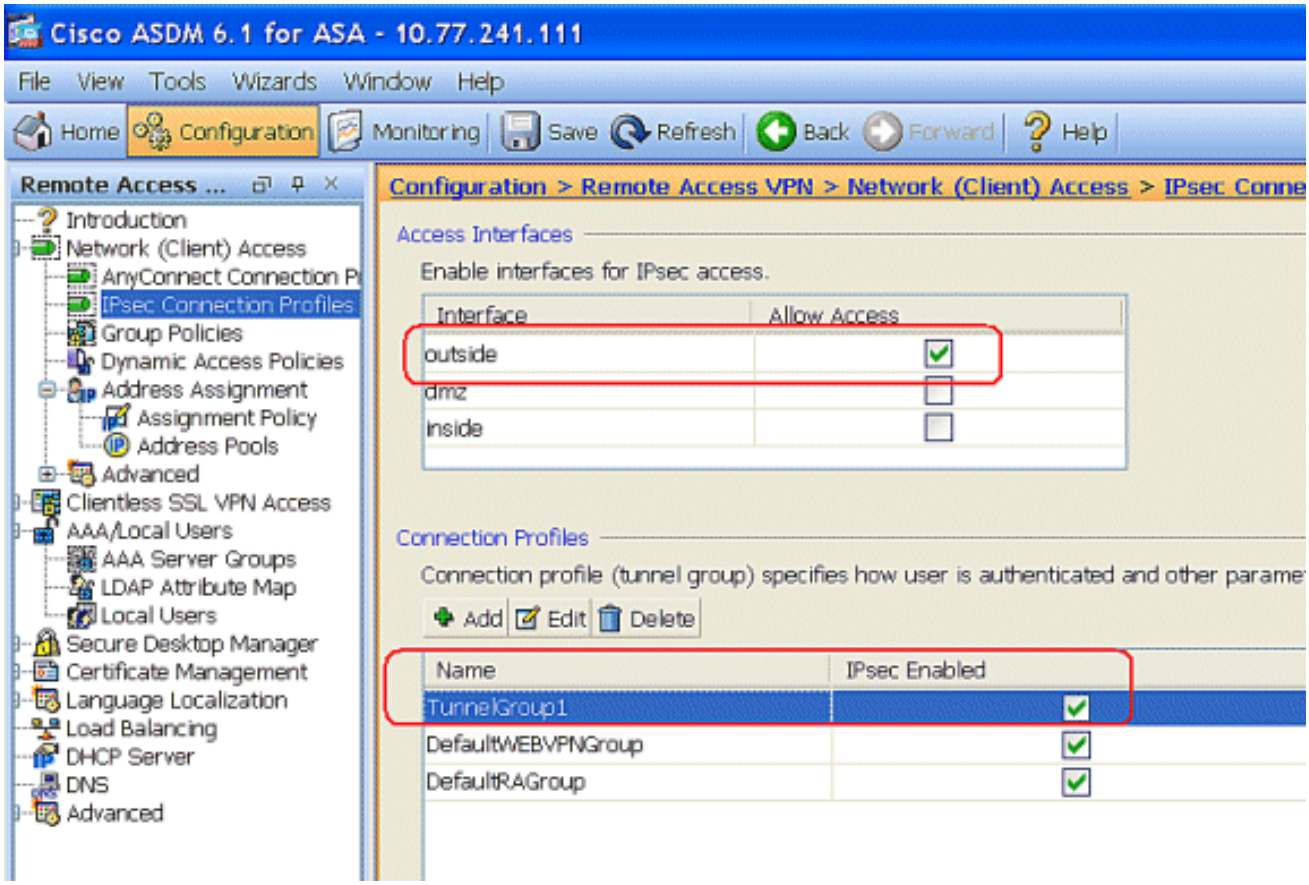
10. Advanced(**고급**) **> Client Addressing(클라이언트 주소 지정)**을 선택하고 **Use address pool(주소 풀 사용)** 확인란을 선택하여 VPN 클라이언트에 IP 주소를 할당합니다.**참고: Use authentication server** and **Use DHCP**(**인증 서버 사용** 및 **DHCP 사용**) 확인란**의 선택을 취소해야 합니다**

    .



확인을 **클릭합니다**.

11. IPSec 액세스를 위한 외부 인터페이스를 활성화합니다.Apply(**적용**)를 클릭하여 진행합니다
.



CLI로 ASA/PIX 구성

명령행에서 VPN 클라이언트에 IP 주소를 제공하도록 DHCP 서버를 구성하려면 다음 단계를 완료합니다.사용되는 각 명령에 대한 자세한 내용은 원격 액세스 VPN 구성 또는 Cisco ASA 5500 Series Adaptive Security Appliances-Command Reference를 참조하십시오.

ASA 디바이스에서 컨피그레이션 실행

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0

no failover
icmp unreachable rate-limit 1 burst-size 1

!--- Specify the location of the ASDM image for ASA to
```

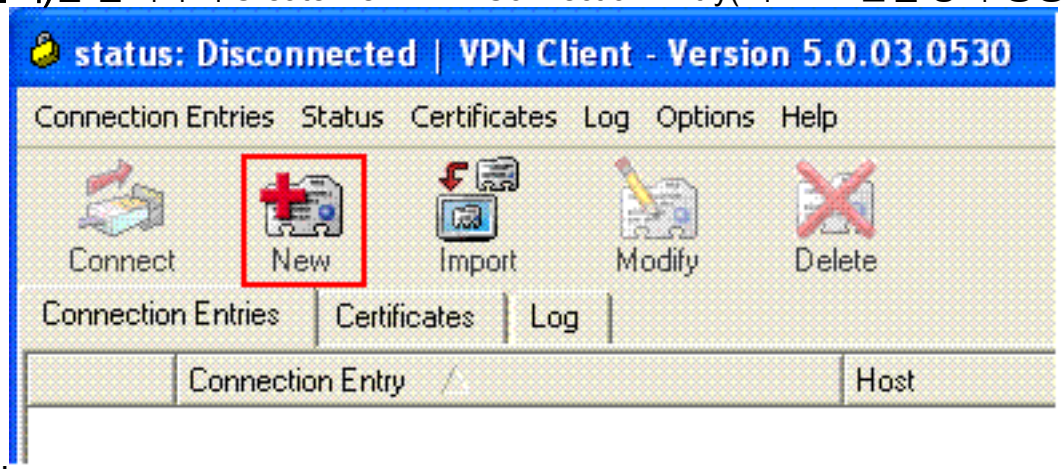
```
fetch the image for ASDM access. asdm image disk0:/asdm-
613.bin no asdm history enable arp timeout 14400 global
(outside) 1 192.168.1.5 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 192.168.1.2 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute dynamic-access-policy-
record DfltAccessPolicy http server enable http 0.0.0.0
0.0.0.0 inside no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart crypto ipsec transform-set
ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-DES-SHA crypto
map outside_map 1 ipsec-isakmp dynamic outside_dyn_map
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside !--- PHASE 1 CONFIGURATION
---! !--- This configuration uses ISAKMP policy 2. !---
The configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 2 authentication pre-share
encryption des hash sha group 2 lifetime 86400 no crypto
isakmp nat-traversal !--- Specifies that the IP address
to the vpn clients are assigned by the local and not by
AAA or dhcp. The CLI vpn-addr-assign local for VPN
address assignment through ASA is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign dhcp

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
```

```
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal

!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode

username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
  vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

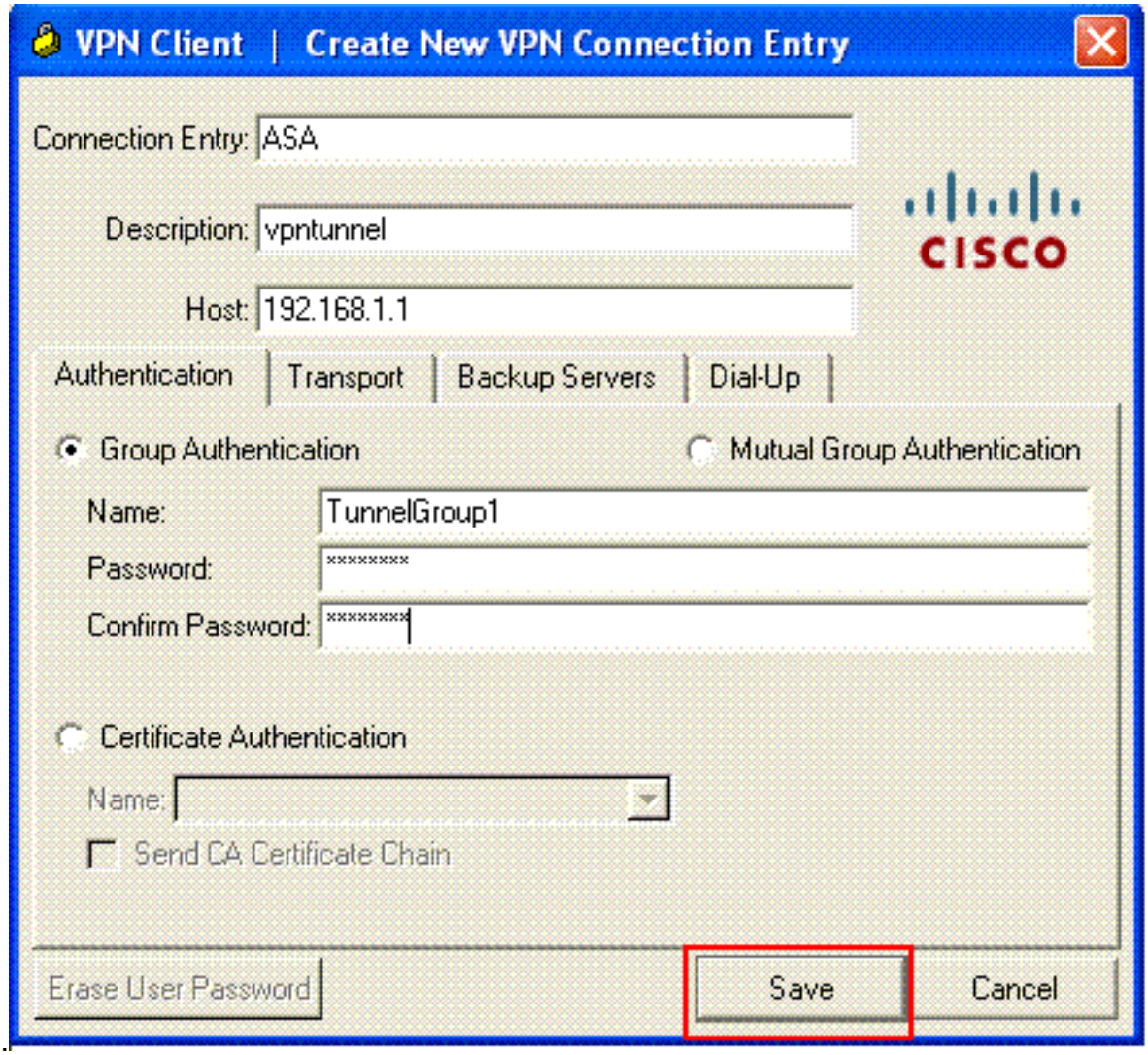
Cisco VPN 클라이언트 컨피그레이션

ASA가 성공적으로 구성되었는지 확인하기 위해 Cisco VPN Client를 사용하여 Cisco ASA에 연결하려고 시도합니다.

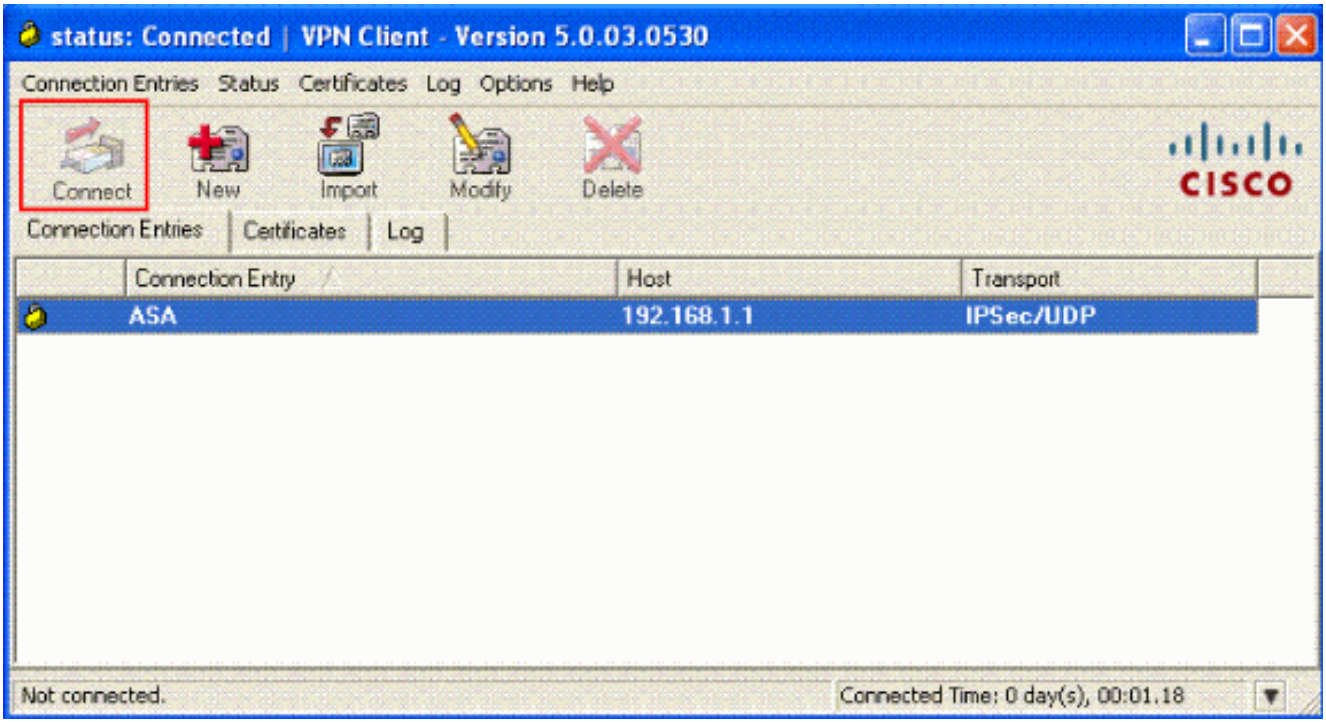
1. Start(**시작**) > **Programs(프로그램)** > **Cisco Systems VPN Client(Cisco Systems VPN 클라이언트)** > **VPN Client(VPN 클라이언트)를 선택합니다**.
2. New(**새로 만들기**)를 클릭하여 Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창



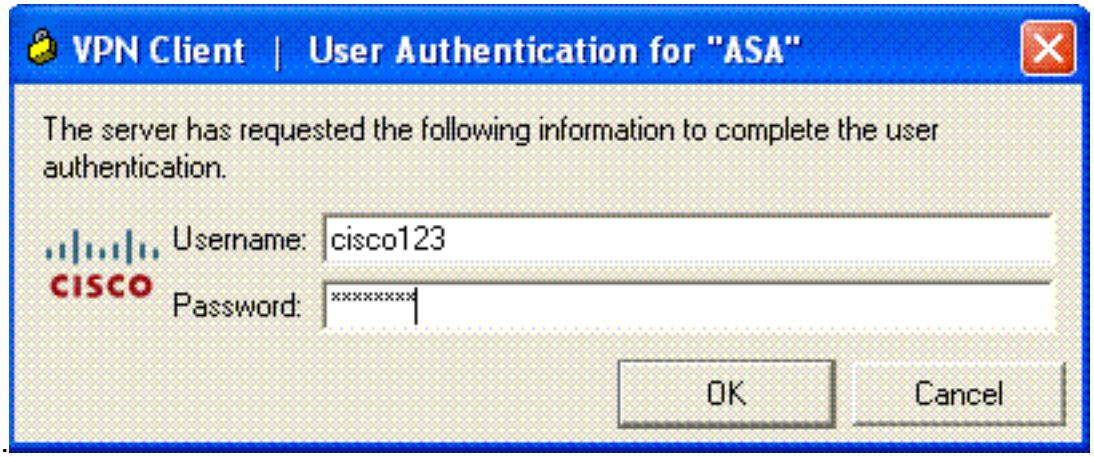
을 시작합니다.
3. 새 연결의 세부 정보를 입력합니다.설명과 함께 연결 항목의 이름을 입력합니다.Host(호스트) 상자**에 ASA의 외부 IP 주소**를 입력합니다.그런 다음 ASA에 구성된 대로 VPN 터널 그룹 이름(TunnelGroup1) 및 비밀번호(Pre-shared Key - cisco123)를 입력합니다.저장을 **클릭합니다**



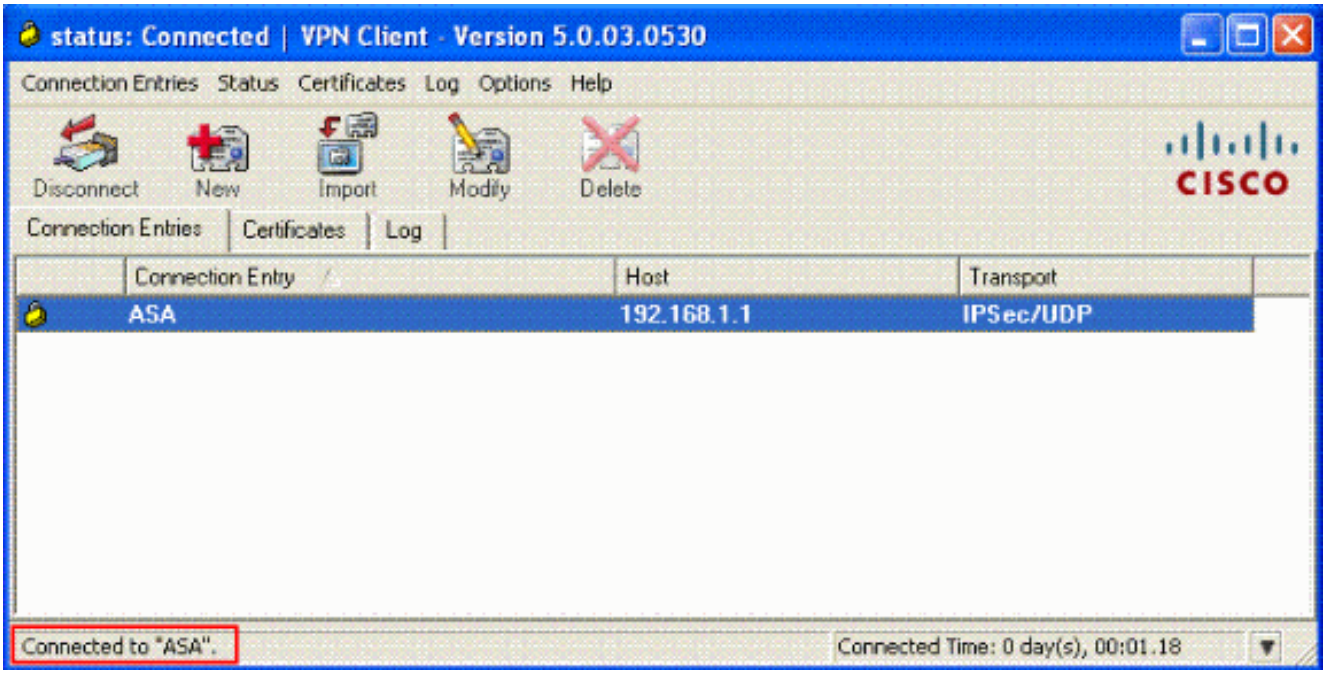
4. 사용할 연결을 클릭하고 VPN Client 주 창에서 **Connect(연결)**를 클릭합니다



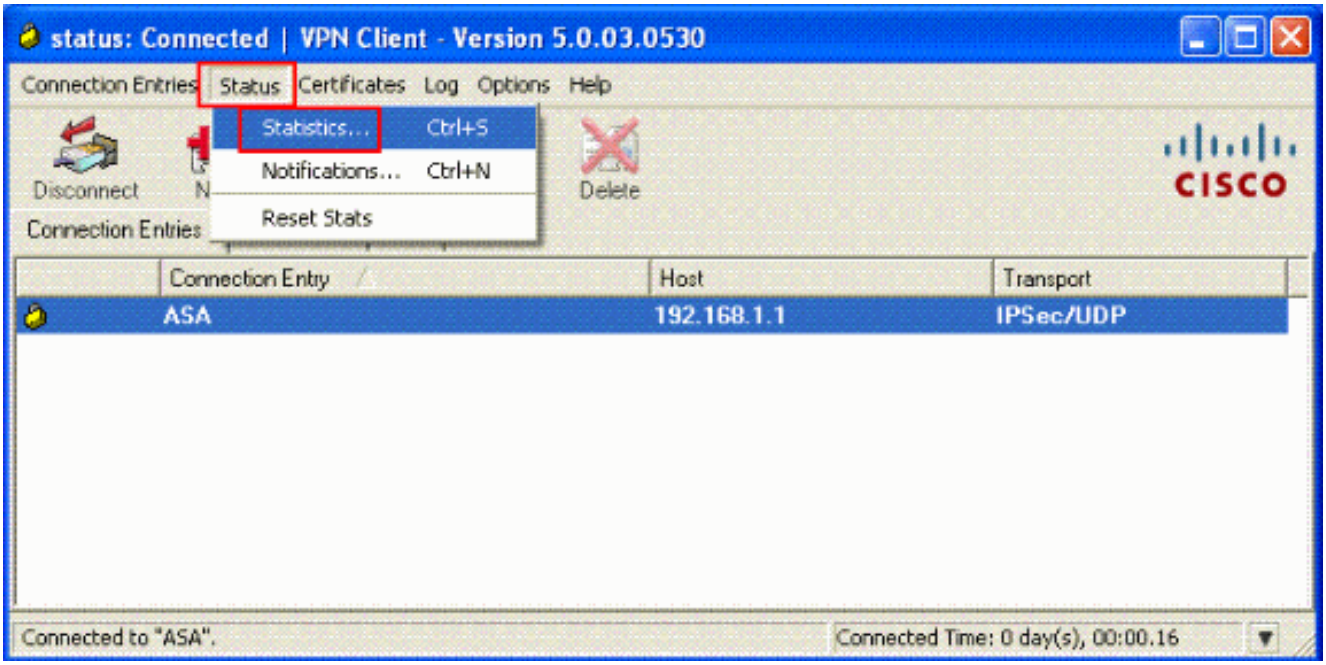
5. 프롬프트가 표시되면 사용자 이름**을 입력합니다.cisco123** 및 **비밀번호:cisco123**은 ASA for Xauth에 구성된 대로 **OK**(확인)를 클릭하여 원격 네트워크에 연결합니다



6. VPN 클라이언트는 중앙 사이트의 ASA에 연결됩니다



7. 연결이 성공적으로 설정되면 Status 메뉴에서 Statistics를 선택하여 터널의 세부 정보를 확인합니다



다음을 확인합니다.

show 명령

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.

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

문제 해결

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

참고: 원격 액세스 IPSec VPN 문제 해결에 대한 자세한 내용은 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션을 참조하십시오.

보안 연결 지우기

문제를 해결할 때 변경한 후 기존 보안 연결을 지워야 합니다.PIX의 특권 모드에서 다음 명령을 사용합니다.

- **clear [crypto] ipsec sa** - 활성 IPSec SA를 삭제합니다.crypto 키워드는 선택 사항입니다.
- **clear [crypto] isakmp sa** - 활성 IKE SA를 삭제합니다.crypto 키워드는 선택 사항입니다.

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 7** - 2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp 7** - 1단계의 ISAKMP 협상을 표시합니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliances 지원 페이지
- Cisco ASA 5500 Series Adaptive Security Appliances 명령 참조
- Cisco PIX 500 Series 보안 어플라이언스 지원 페이지
- Cisco PIX 500 Series Security Appliances 명령 참조
- Cisco Adaptive Security Device Manager
- IPSec 협상/IKE 프로토콜 지원 페이지
- Cisco VPN 클라이언트 지원 페이지

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems