ASA/PIX 8.x:CLI 및 ASDM 컨피그레이션으로 다운로드 가능한 ACL을 사용하는 VPN 액세스를 위한 ACS 4.x(Radius 권한 부여) 예

목차

소개

이 문서에서는 네트워크 액세스를 위해 사용자를 인증하도록 보안 어플라이언스를 구성하는 방법에 대해 설명합니다.RADIUS 권한 부여를 암시적으로 활성화할 수 있으므로 이 섹션에는 보안 어플라이언스에서 RADIUS 권한 부여의 컨피그레이션에 대한 정보가 포함되어 있지 않습니다.보안 어플라이언스가 RADIUS 서버에서 받은 액세스 목록 정보를 처리하는 방법에 대한 정보를 제공합니다.

인증 시 보안 어플라이언스에 액세스 목록을 다운로드하거나 액세스 목록 이름을 다운로드하도록 RADIUS 서버를 구성할 수 있습니다.사용자는 사용자별 액세스 목록에서 허용되는 작업만 수행할 수 있습니다.

다운로드 가능한 액세스 목록은 Cisco Secure ACS를 사용하여 각 사용자에게 적절한 액세스 목록을 제공할 때 가장 확장 가능한 방법입니다.다운로드 가능한 액세스 목록 기능 및 Cisco Secure ACS에 대한 자세한 내용은 다운로드 가능한 액세스 제어 목록 및 다운로드 가능한 IP ACL을 전송하도록 RADIUS 서버 구성을 참조하십시오.

ASA 8.3 이상을 참조하십시오.CLI와 함께 다운로드 가능한 ACL을 사용하여 VPN 액세스를 위한 ACS 5.x(RADIUS 권한 부여) 및 8.3 이상 버전의 Cisco ASA에서 동일한 구성을 위한 ASDM 컨피그레이션 예

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
- Cisco Adaptive Security Device Manager 버전 5.x 이상
- Cisco VPN Client Version 4.x 이상
- Cisco Secure Access Control Server 4.x

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.

배경 정보

다운로드 가능한 IP ACL을 사용하여 여러 사용자 또는 사용자 그룹에 적용할 수 있는 ACL 정의 집합을 생성할 수 있습니다.이러한 ACL 정의 집합을 ACL 내용이라고 합니다.또한 NAF를 통합할 때 사용자가 액세스를 원하는 AAA 클라이언트로 전송되는 ACL 내용을 제어합니다.즉, 다운로드 가능한 IP ACL은 하나 이상의 ACL 콘텐츠 정의로 구성되며, 각 ACL은 모든 AAA 클라이언트와 연결된 NAF 또는 (기본적으로) 연결됩니다.NAF는 AAA 클라이언트의 IP 주소에 따라 지정된 ACL 내용의 적용 가능성을 제어합니다.다운로드 가능한 IP ACL을 제어하는 방법 및 NAF에 대한 자세한 내용은

네트워크 액세스 필터 정보를 참조하십시오.

다운로드 가능한 IP ACL은 다음과 같이 작동합니다.

1. ACS가 네트워크에 대한 사용자 액세스 권한을 부여할 때 ACS는 다운로드 가능한 IP ACL이 해당 사용자에게 할당되는지 아니면 사용자 그룹에 할당되었는지 결정합니다.
2. ACS가 사용자 또는 사용자 그룹에 할당된 다운로드 가능한 IP ACL을 찾는 경우 ACL 콘텐츠 항목이 RADIUS 인증 요청을 보낸 AAA 클라이언트와 연결되어 있는지 여부를 결정합니다.
3. ACS는 사용자 세션의 일부로 RADIUS 액세스 수락 패킷, 명명된 ACL을 지정하는 특성 및 명명된 ACL의 버전을 전송합니다.
4. AAA 클라이언트가 캐시에 현재 버전의 ACL이 없다고 응답하면, 즉 ACL이 신규 또는 변경된 경우 ACS는 ACL(신규 또는 업데이트)을 디바이스에 전송합니다.

다운로드 가능한 IP ACL은 각 사용자 또는 사용자 그룹의 RADIUS Cisco av-pair 특성 [26/9/1]에서 ACL의 구성에 대한 대안입니다.다운로드 가능한 IP ACL을 한 번 생성하고 이름을 지정한 다음 이름을 참조하는 경우 해당 사용자 또는 사용자 그룹마다 다운로드 가능한 IP ACL을 할당할 수 있습니다.이 방법은 각 사용자 또는 사용자 그룹에 대해 RADIUS Cisco av 쌍 특성을 구성하는 경우보다 효율적입니다.

또한 NAF를 사용할 경우, 사용하는 AAA 클라이언트에 대해 동일한 사용자 또는 사용자 그룹에 서로 다른 ACL 내용을 적용할 수 있습니다.ACS에서 다운로드 가능한 IP ACL을 사용하도록 AAA 클라이언트를 구성한 후에는 AAA 클라이언트를 추가로 구성할 필요가 없습니다.다운로드 가능한 ACL은 사용자가 설정한 백업 또는 복제 환경 설정에 의해 보호됩니다.

ACS 웹 인터페이스에 ACL 정의를 입력할 때 키워드 또는 이름 항목을 사용하지 마십시오.다른 모든 측면에서, 다운로드 가능한 IP ACL을 적용하려는 AAA 클라이언트에 표준 ACL 명령 구문 및 의미 체계를 사용합니다.ACS에 입력하는 ACL 정의는 하나 이상의 ACL 명령으로 구성됩니다.각 ACL 명령은 별도의 줄에 있어야 합니다.

하나 이상의 명명된 ACL 내용을 다운로드 가능한 IP ACL에 추가할 수 있습니다.기본적으로 각 ACL 콘텐츠는 모든 AAA 클라이언트에 적용되지만, NAF를 정의한 경우, 각 ACL 콘텐츠의 적용 가능성을 NAF에 연결된 AAA 클라이언트에 나열되는 AAA 클라이언트로 제한할 수 있습니다.즉, NAF를 사용할 때 각 ACL 콘텐츠를 다운로드 가능한 단일 IP ACL 내에서 네트워크 보안 전략에 따라 여러 네트워크 디바이스 또는 네트워크 디바이스 그룹에 적용할 수 있습니다.

또한 다운로드 가능한 IP ACL에서 ACL 내용의 순서를 변경할 수 있습니다.ACS는 테이블 상단부터 시작하여 ACL 내용을 검사하고, AAA 클라이언트가 사용된 AAA 클라이언트를 포함하는 NAF를 통해 발견한 첫 번째 ACL 콘텐츠를 다운로드합니다.주문을 설정할 때 가장 널리 적용되는 ACL 내용을 목록에서 더 높게 배치하면 시스템 효율성을 보장할 수 있습니다.NAF에 겹치는 AAA 클라이언트 수가 포함된 경우 좀 더 구체적부터 좀 더 일반적으로만 진행해야 한다는 사실을 깨달아야 합니다.예를 들어, ACS는 All-AAA-Clients NAF 설정을 사용하여 모든 ACL 내용을 다운로드하며 목록에 더 낮은 내용을 고려하지 않습니다.

특정 AAA 클라이언트에서 다운로드 가능한 IP ACL을 사용하려면 AAA 클라이언트는 다음 지침을 따라야 합니다.

- 인증에 RADIUS 사용
- 다운로드 가능한 IP ACL 지원

다음은 다운로드 가능한 IP ACL을 지원하는 Cisco 디바이스의 예입니다.

- ASA 및 PIX 디바이스
- VPN 3000 시리즈 집중 장치

- IOS 버전 12.3(8)T 이상을 실행하는 Cisco 디바이스

다음은 ACL 정의 상자에 VPN 3000/ASA/PIX 7.x+ ACL을 입력하는 데 사용해야 하는 형식의 예입니다.

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

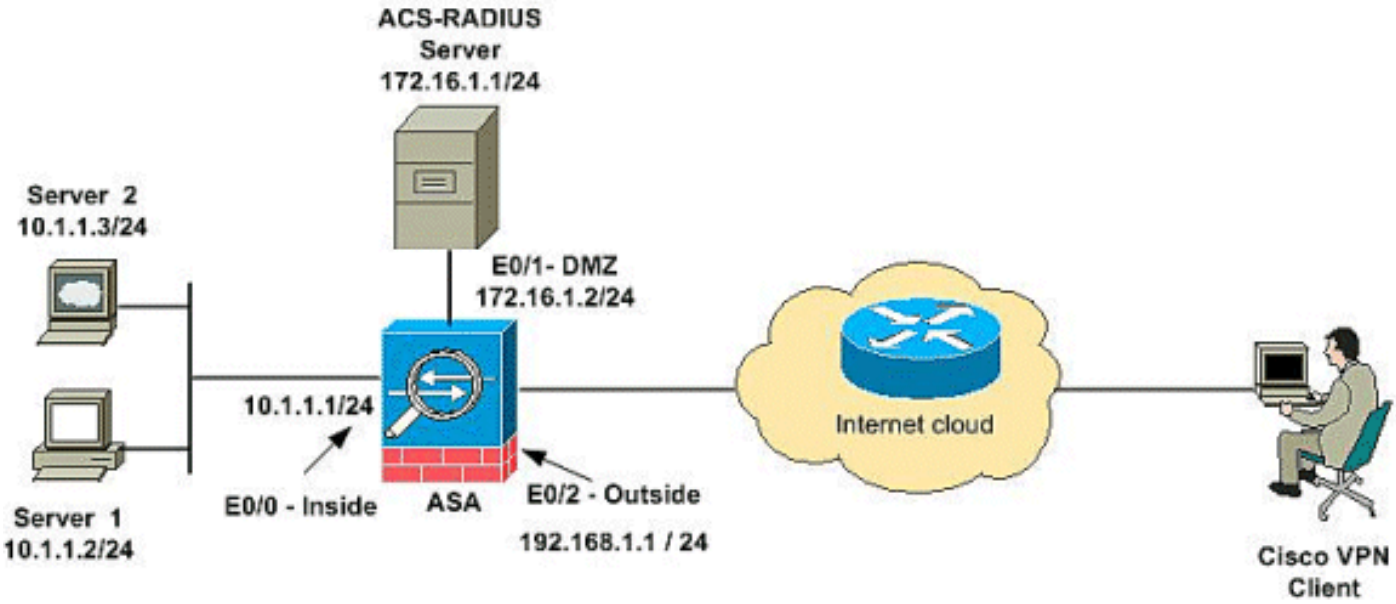
구성

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.

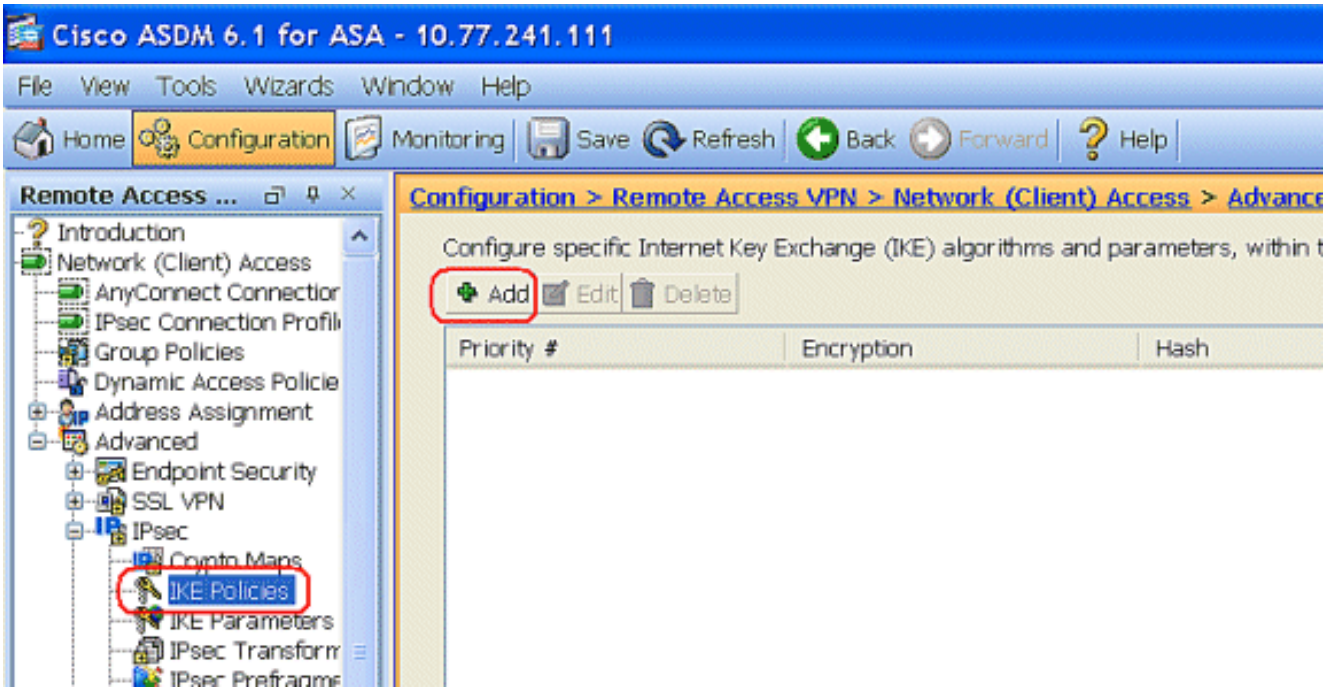
원격 액세스 VPN(IPSec) 구성

ASDM 절차

원격 액세스 VPN을 구성하려면 다음 단계를 완료합니다.

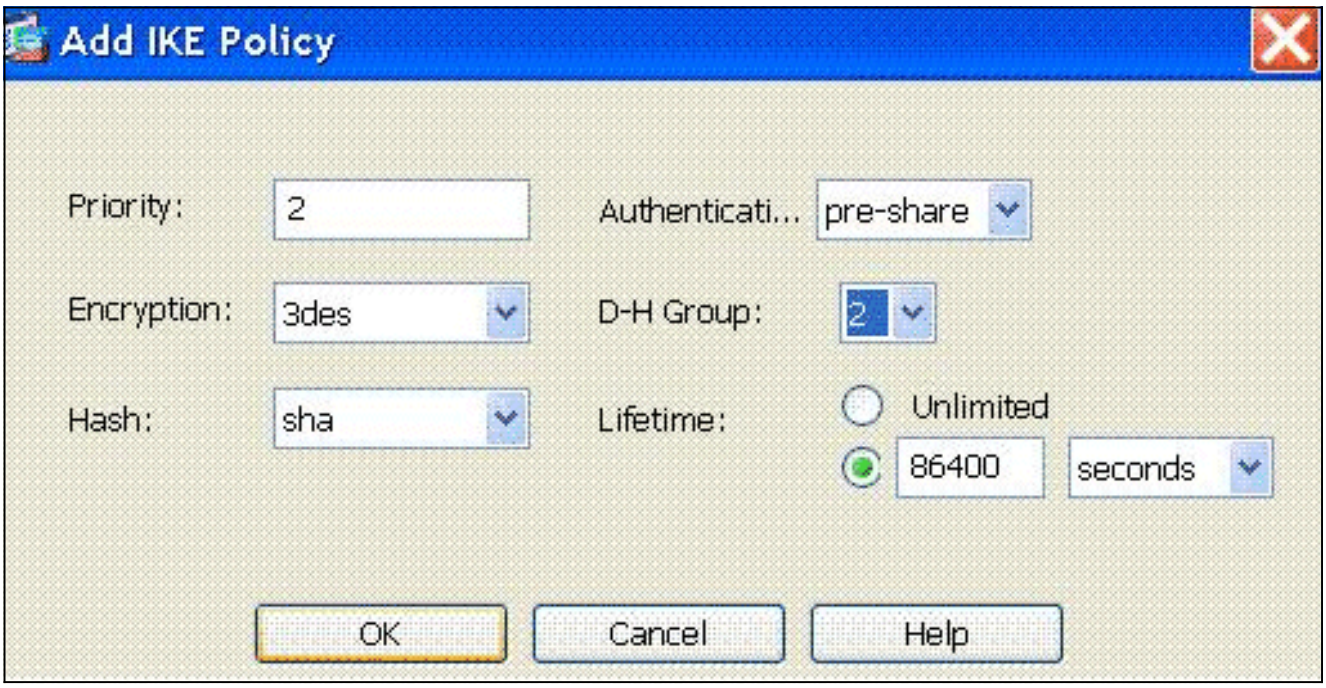
1. ISAKMP **정책을 생성하려면 Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add**를 선택합니다

.



2. 표시된 대로 ISAKMP 정책 세부 정보를 제공합니다

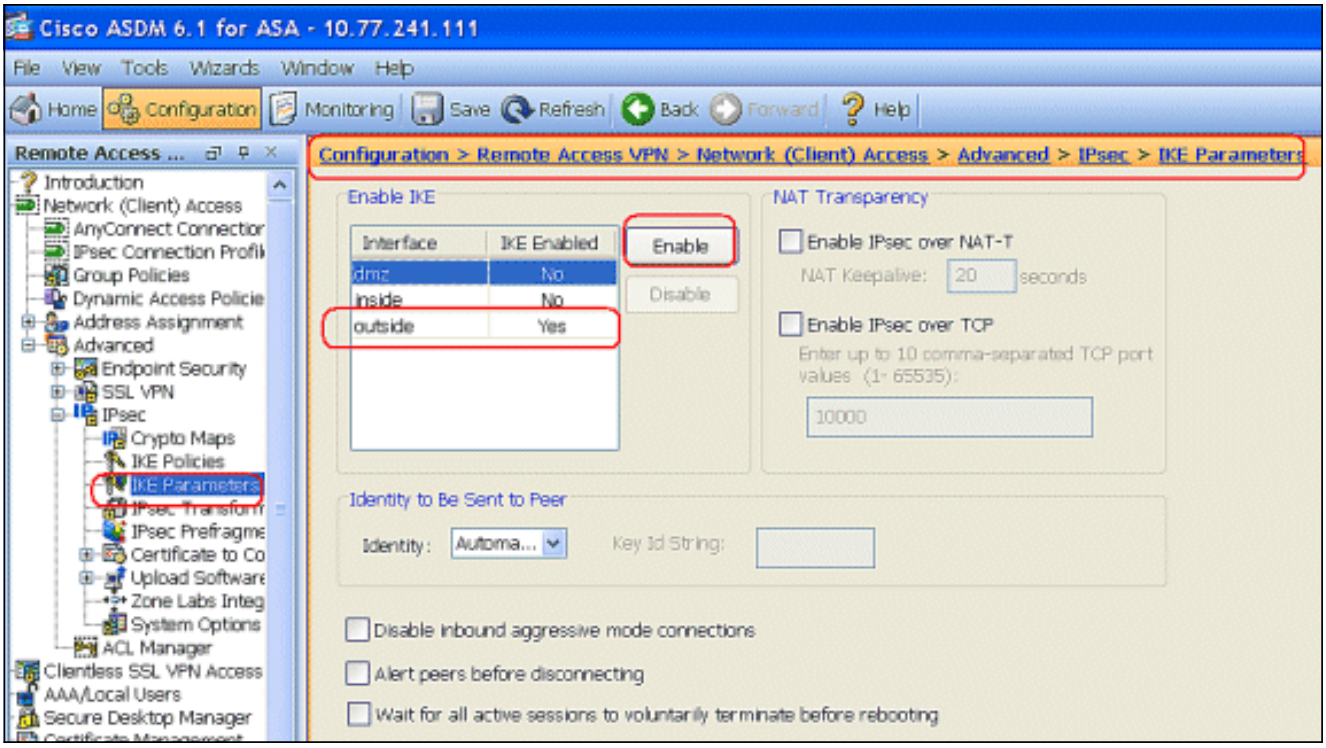
.



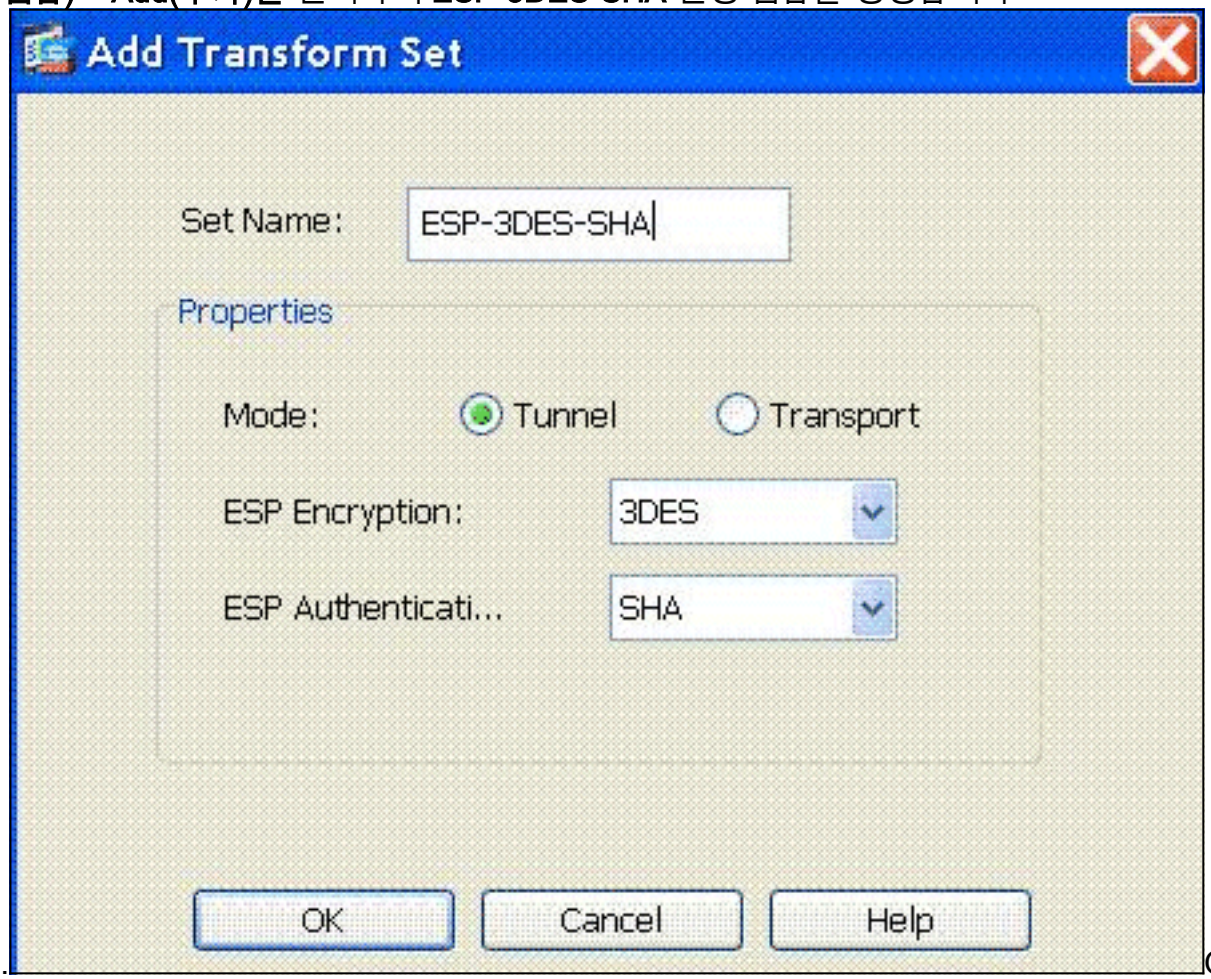
OK(**확인**)와 Apply(적용)를 **클릭합니다**.

3. Configuration **> Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Parameters를 선택하여** 외부 인터페이스에서 IKE를 활성화합니다

.



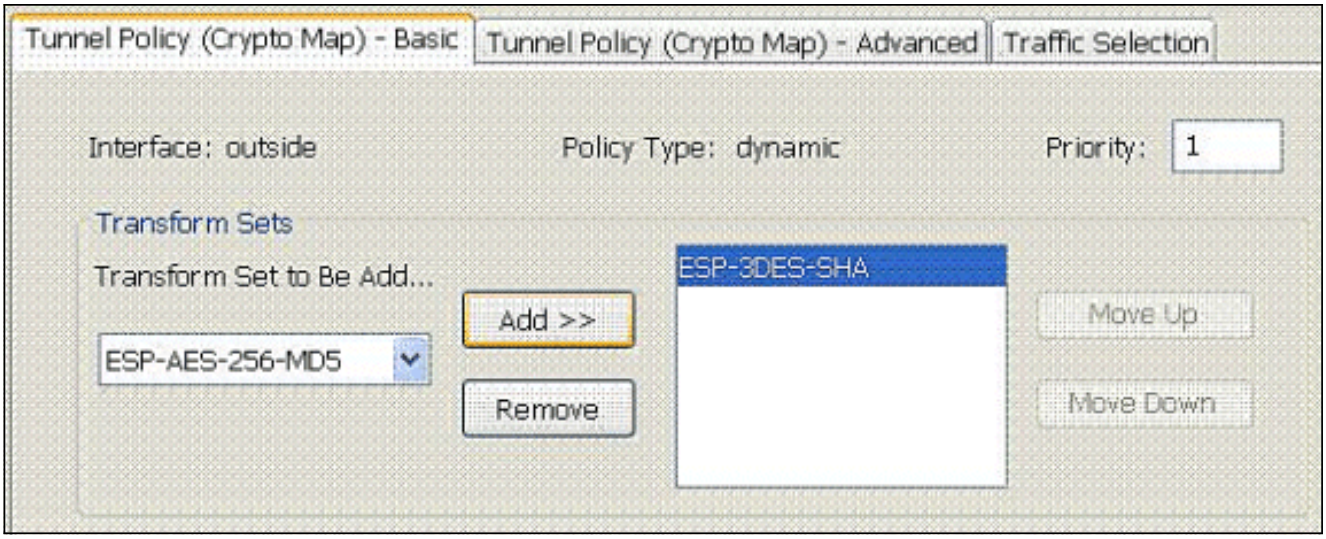
4. Configuration(**구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > IPSec Transform Sets(IPSec 변형 집합) > Add(추가)를** 선택하여 **ESP-3DES-SHA** 변형 집합을 생성합니다



. **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

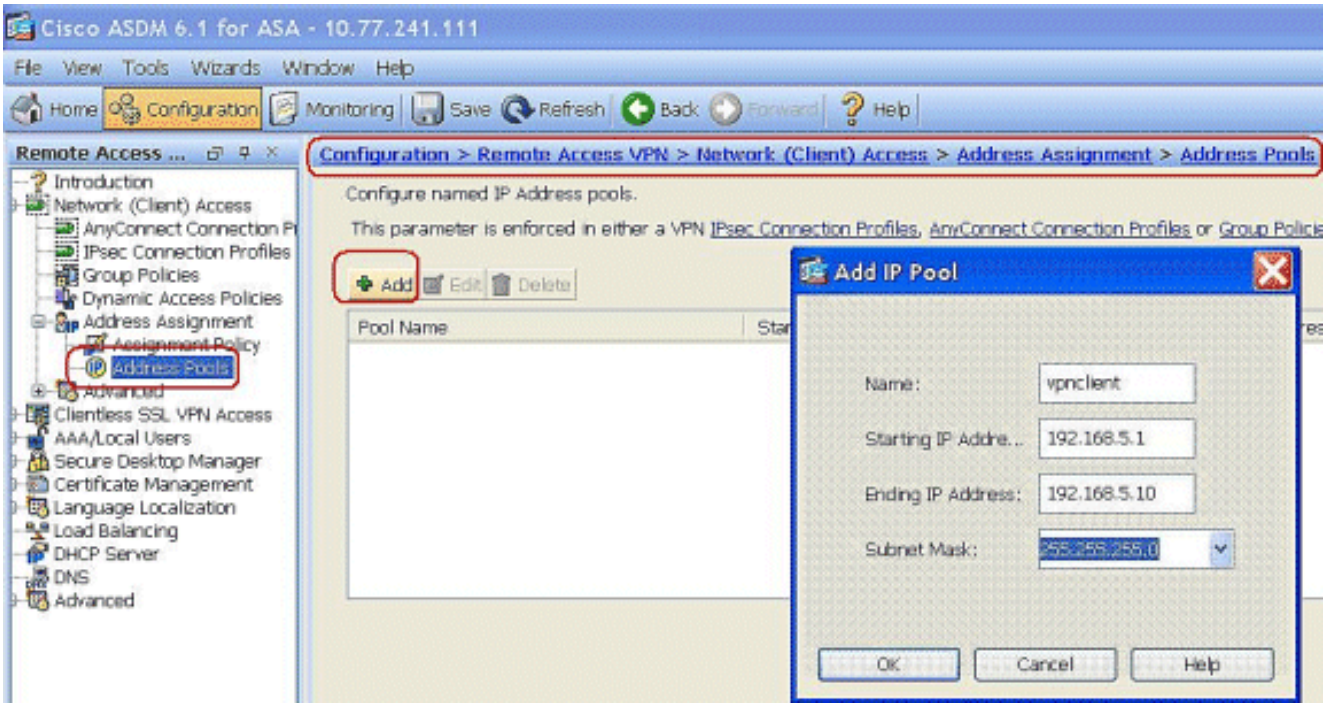
.



OK(**확인**)와 Apply(적용)를 **클릭합니다**.

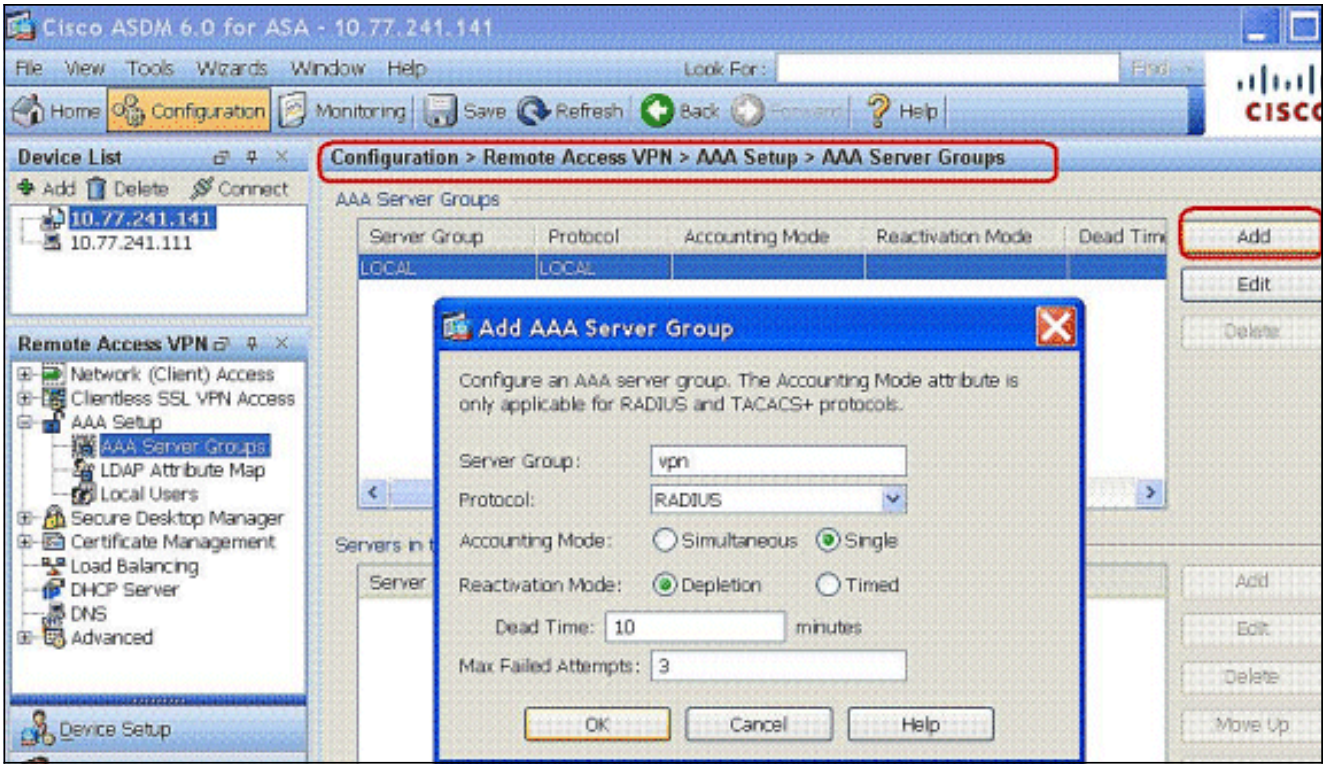
6. Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Address Pools(주소 풀)**를 선택하고 **Add(추가)**를 클릭하여 VPN 클라이언트 사용자에 대한 VPN 클라이언트를 추가합니다

.



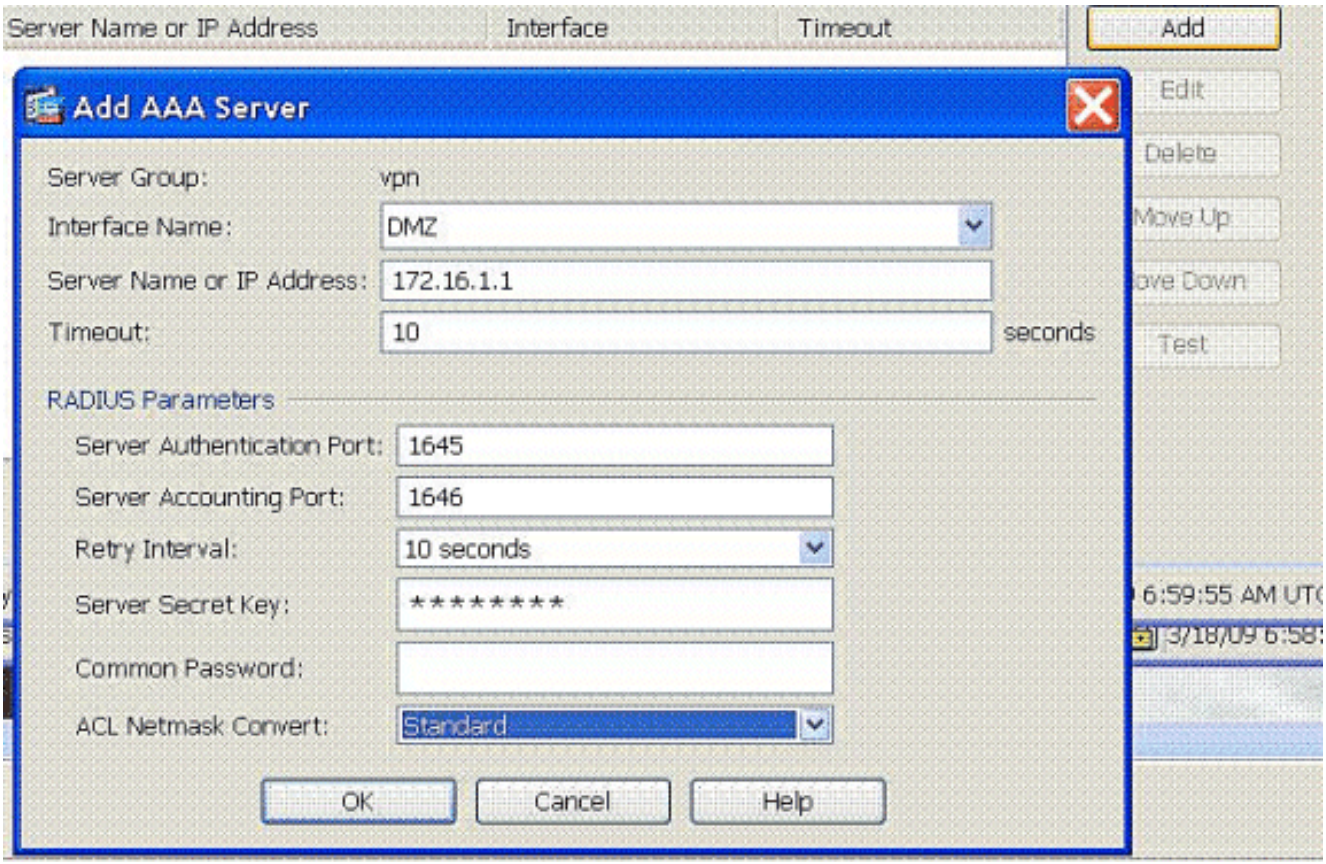
7. Configuration(**컨피그레이션**) > **Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Server Groups(AAA 서버 그룹)**를 선택하고 **Add(추가)**를 클릭하여 AAA 서버 그룹 이름 및 프로토콜을 추가합니다

.



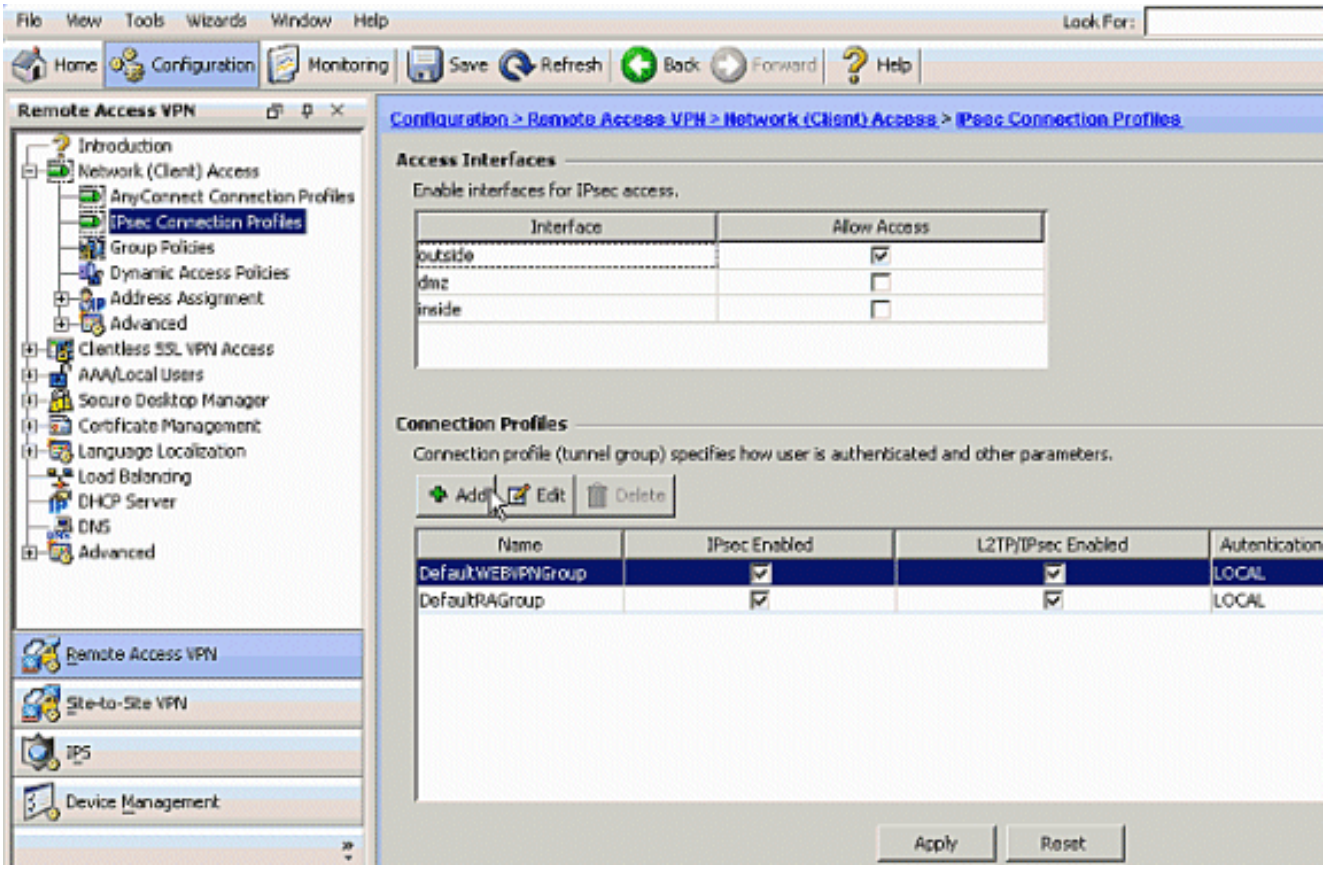
AAA 서버 IP 주소(ACS) 및 연결된 인터페이스를 추가합니다.또한 RADIUS Parameters 영역에 Server Secret 키를 추가합니다.**확인**을 **클릭합니다**

.



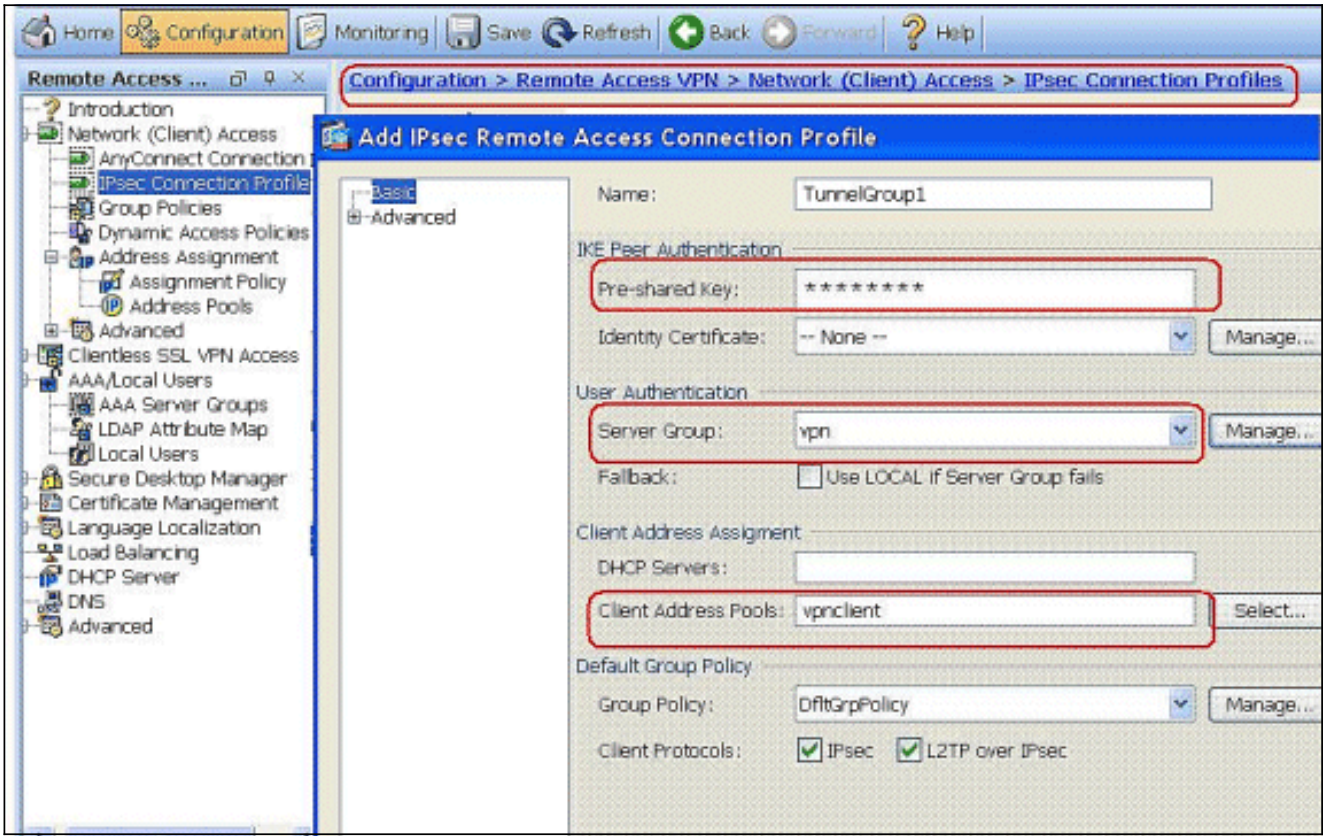
8. Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN)** > **Network (Client) Access(네트워크(클라이언트) 액세스)** > **IPSec Connection Profiles(IPSec 연결 프로파일)** > **Add(추가)**를 선택하여 터널 그룹(예: **TunnelGroup1** 및 Preshared key(사전 공유 키)을 cisco123으로 추가합니다

.



Basic(기본) 탭에서 User Authentication(사용자 인증) 필드에 대해 서버 그룹을 **vpn**으로 선택합니다.VPN **클라이언트** 사용자에 대한 클라이언트 주소 풀로 vpnclient를 선택합니다

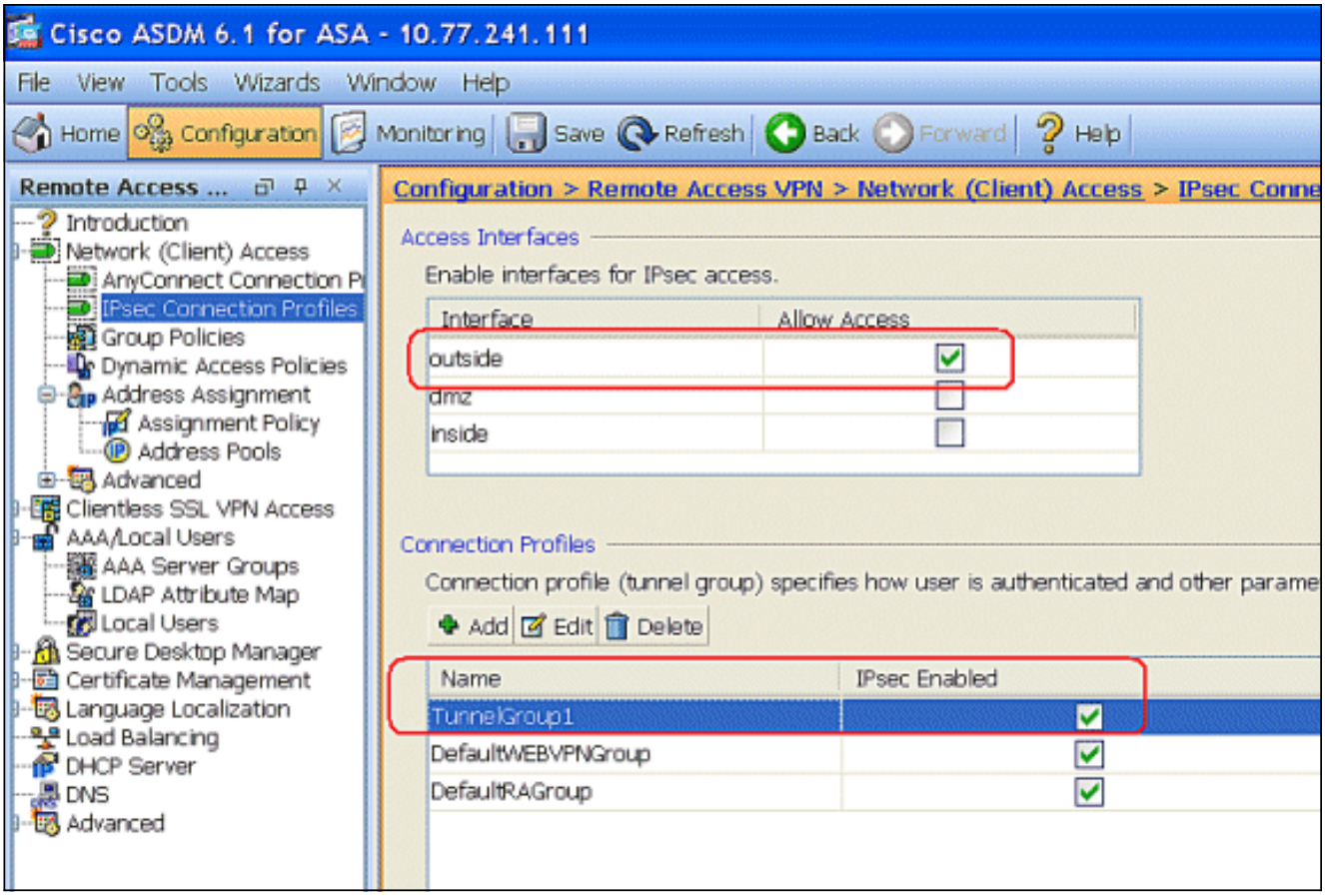
.



확인을 **클릭합니다**.

9. IPSec 액세스에 대해 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 DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
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 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2
access-list new extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
```

```
mtu dmz 1500

ip local pool vpnclient1 192.168.5.1-192.168.5.10 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 !--- Create the AAA server group
"vpn" and specify the protocol as RADIUS. !--- Specify
the CSACS server as a member of the "vpn" group and
provide the !--- location and key. aaa-server vpn
protocol radius
 max-failed-attempts 5
aaa-server vpn (DMZ) host 172.16.1.1
 retry-interval 1
 timeout 30
 key cisco123
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

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. !--- A Triple DES
encryption with !--- the sha hash algorithm is used.
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac

!--- Defines a dynamic crypto map with !--- the
specified encryption settings. crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-3DES-SHA

!--- Binds the dynamic map to the IPsec/ISAKMP process.
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 3des
 hash sha
 group 2
```

```
 lifetime 86400

no crypto isakmp nat-traversal

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
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes
 address-pool vpnclient
 authentication-server-group vpn

!--- 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#
```

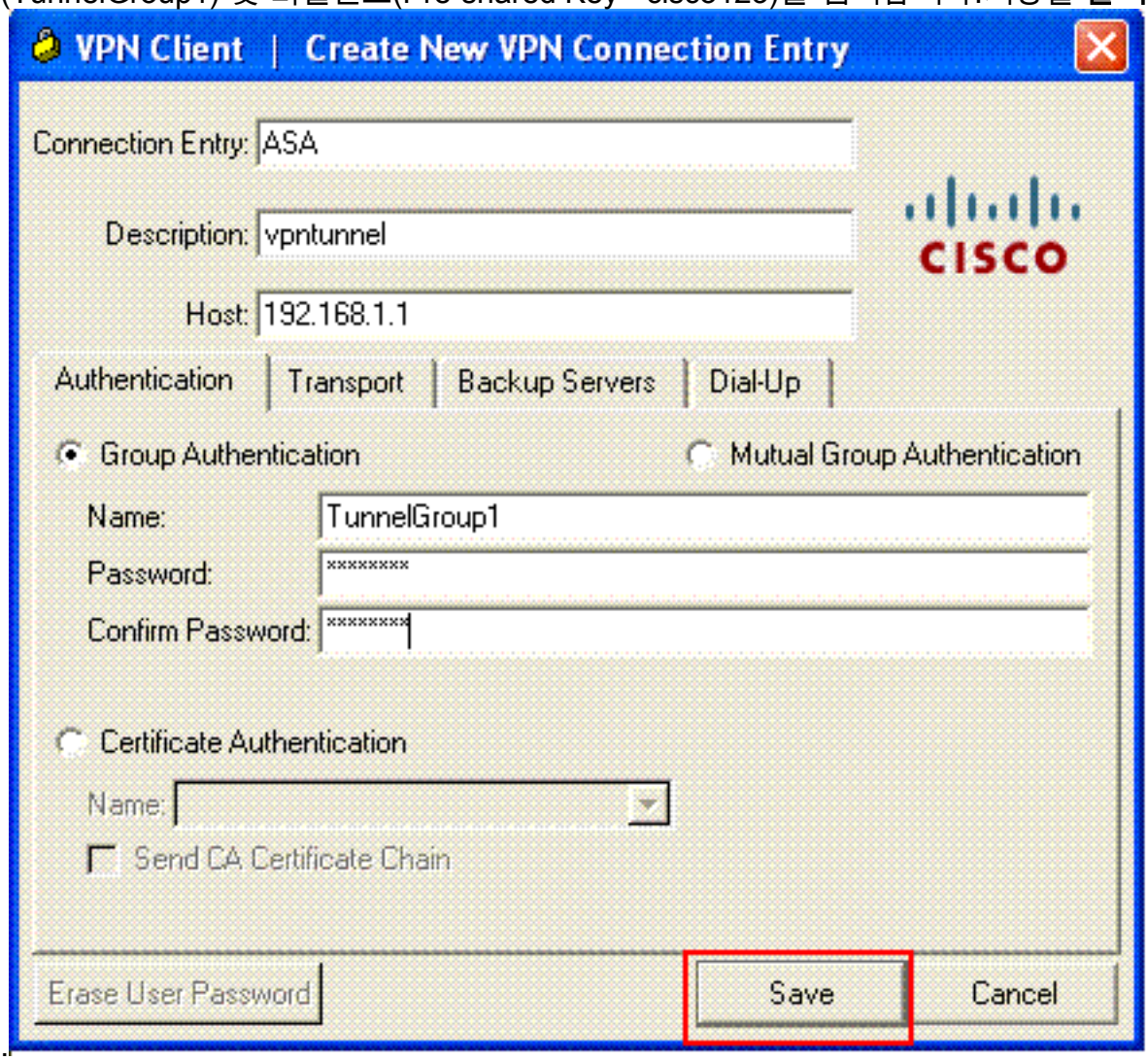
Cisco VPN 클라이언트 컨피그레이션

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.

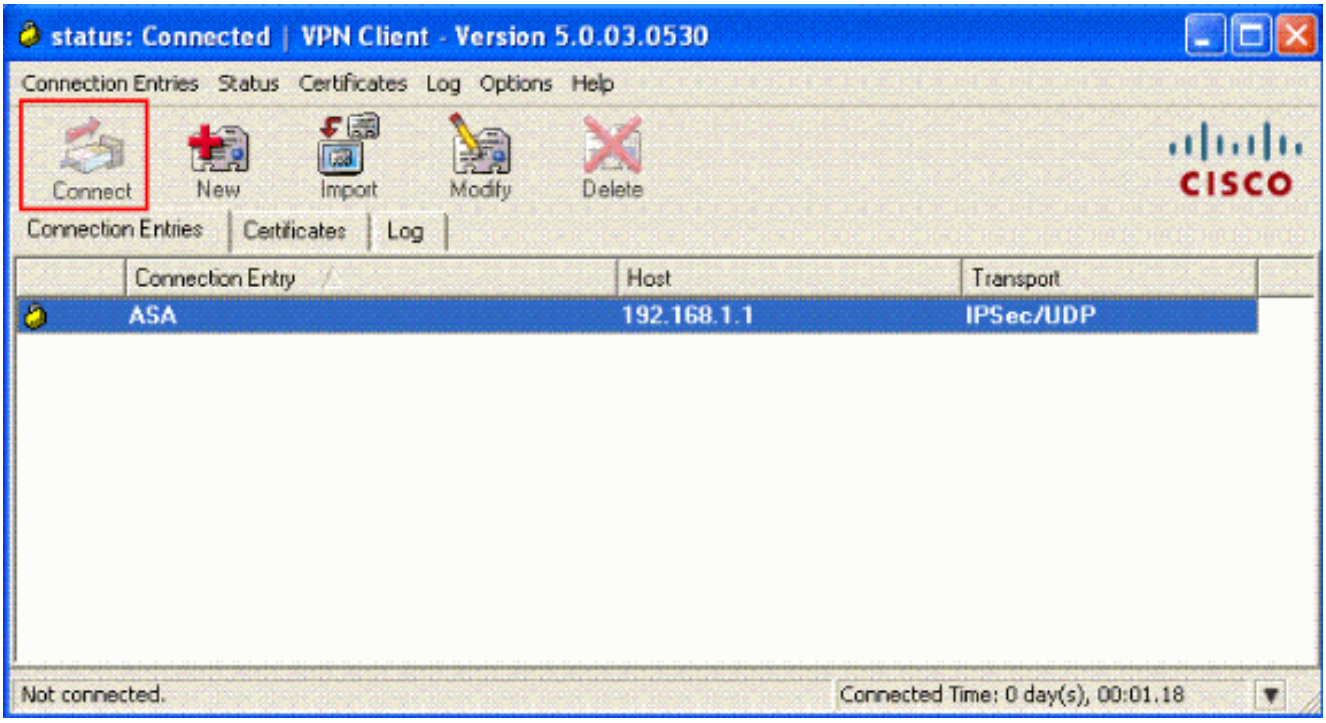
3. 새 연결의 세부 정보를 입력합니다.설명과 함께 연결 항목의 이름을 입력합니다.Host(호스트) 상자**에 ASA의 외부 IP 주소**를 입력합니다.그런 다음 ASA에 구성된 대로 VPN 터널 그룹 이름(TunnelGroup1) 및 비밀번호(Pre-shared Key - cisco123)를 입력합니다.저장을 **클릭합니다**



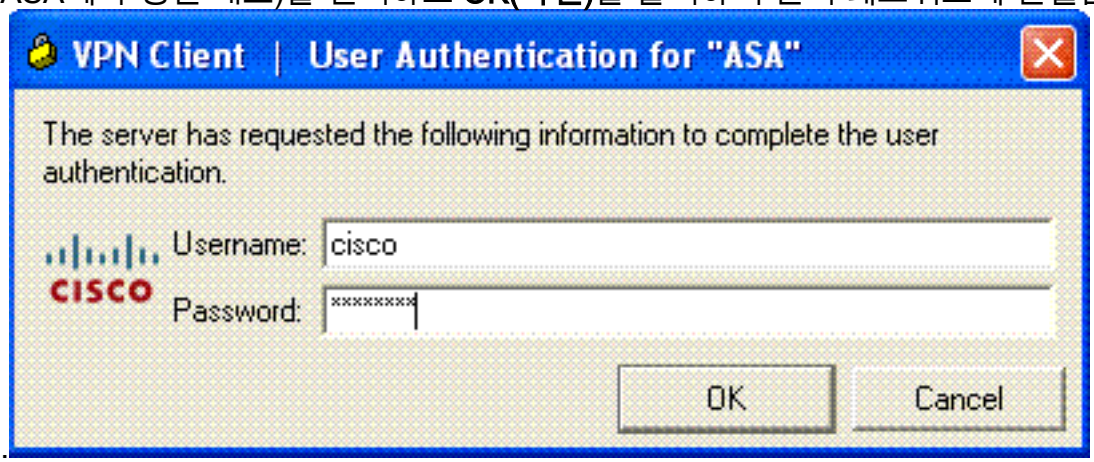
.

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

.



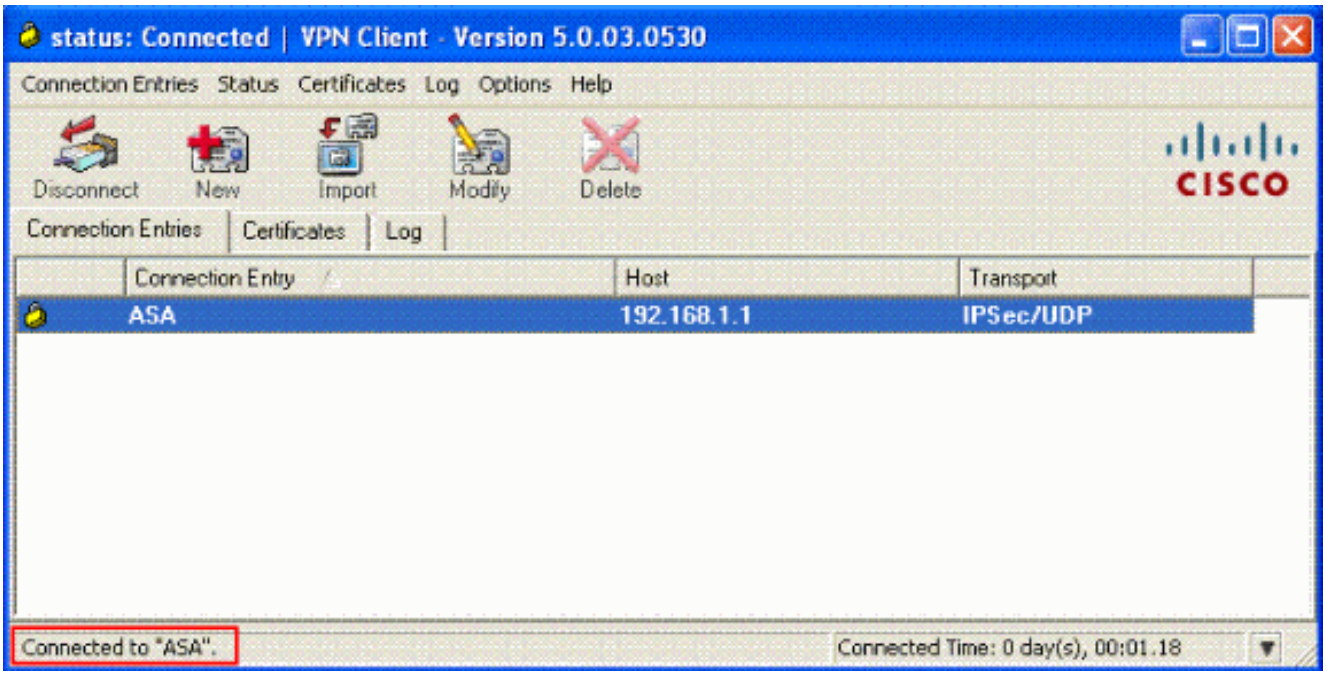
5. 프롬프트가 표시되면 사용자 이름**을 입력합니다.cisco** 및 **비밀번호:password1**(xauth에 대해 ASA에 구성된 대로)을 선택하고 **OK(확인)**를 클릭하여 원격 네트워크에 연결합니다



.

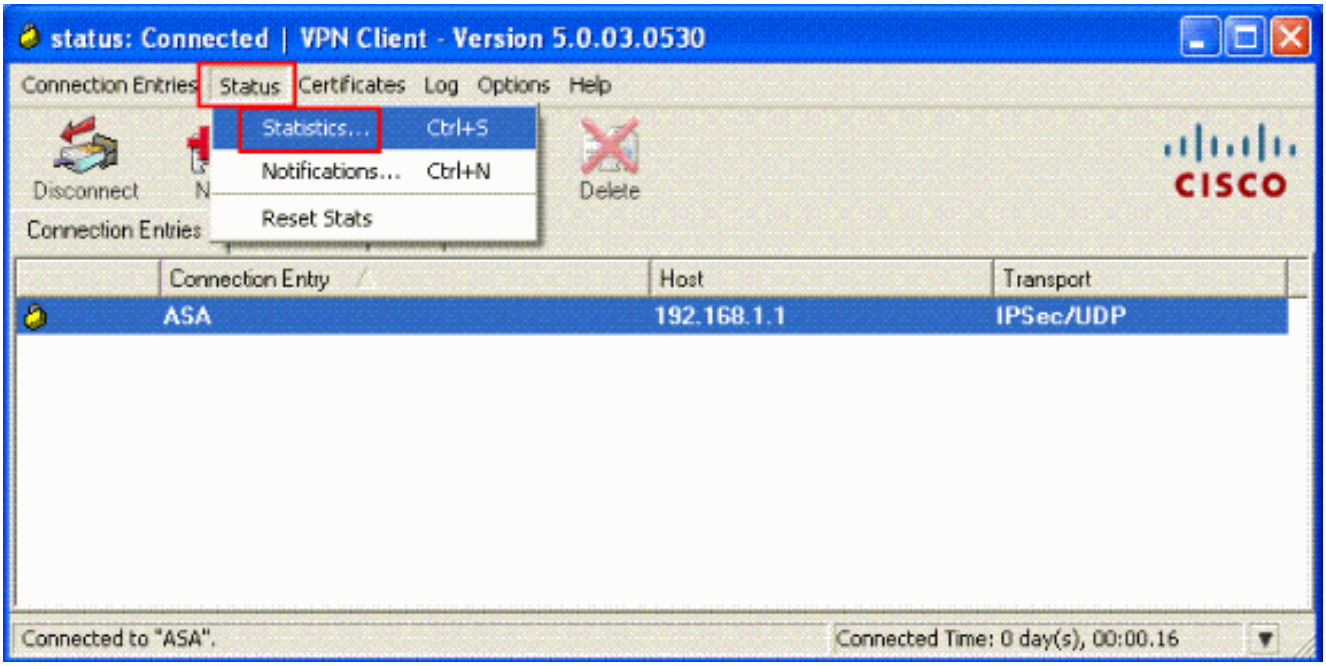
6. VPN 클라이언트는 중앙 사이트의 ASA에 연결됩니다

.



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

.



개별 사용자에 대해 다운로드 가능한 ACL에 대한 ACS 구성

Cisco Secure ACS에서 다운로드 가능한 액세스 목록을 공유 프로필 구성 요소로 구성한 다음 그룹 또는 개별 사용자에게 액세스 목록을 할당할 수 있습니다.

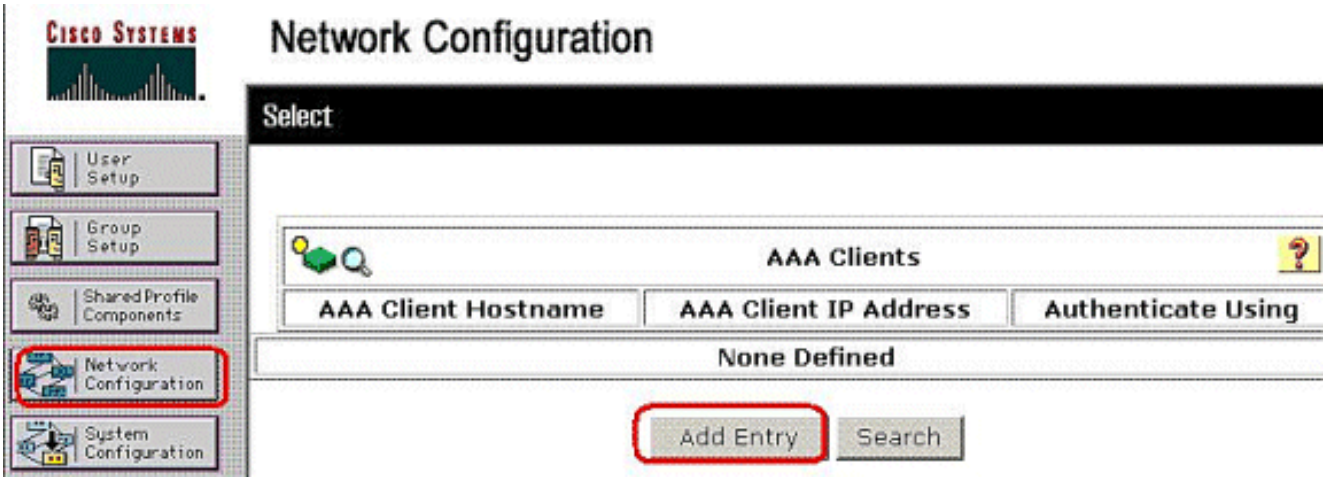
동적 액세스 목록을 구현하려면 RADIUS 서버를 지원하도록 구성해야 합니다.사용자가 인증하면 RADIUS 서버는 다운로드 가능한 액세스 목록 또는 액세스 목록 이름을 보안 어플라이언스에 전송합니다.지정된 서비스에 대한 액세스는 액세스 목록에서 허용되거나 거부됩니다.보안 어플라이언스는 인증 세션이 만료될 때 액세스 목록을 삭제합니다.

이 예에서 IPSec VPN 사용자 **"cisco"는** 성공적으로 인증하고 RADIUS 서버는 보안 어플라이언스에 다운로드 가능한 액세스 목록을 전송합니다."cisco" 사용자는 10.1.1.2 서버에만 액세스할 수 있으며 다른 모든 액세스를 거부합니다.ACL을 확인하려면 Downloadable ACL for User/Group 섹션을 참조하십시오.

Cisco Secure ACS에서 RADIUS를 구성하려면 다음 단계를 완료합니다.

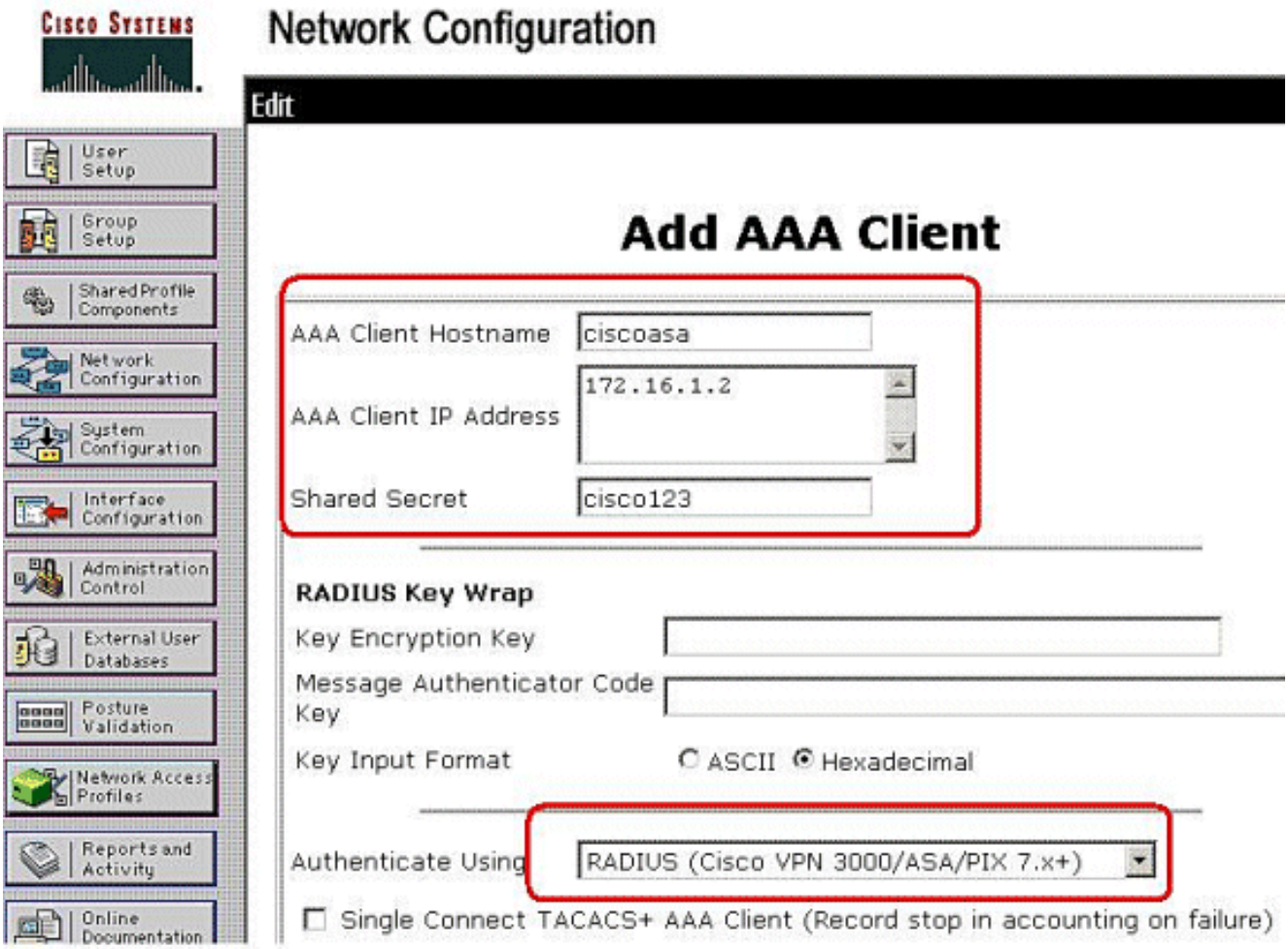
1. 왼쪽에서 **Network Configuration**(네트워크 컨피그레이션)을 선택하고 **Add Entry(항목 추가)**를 클릭하여 RADIUS 서버 데이터베이스에 ASA에 대한 항목을 추가합니다

.



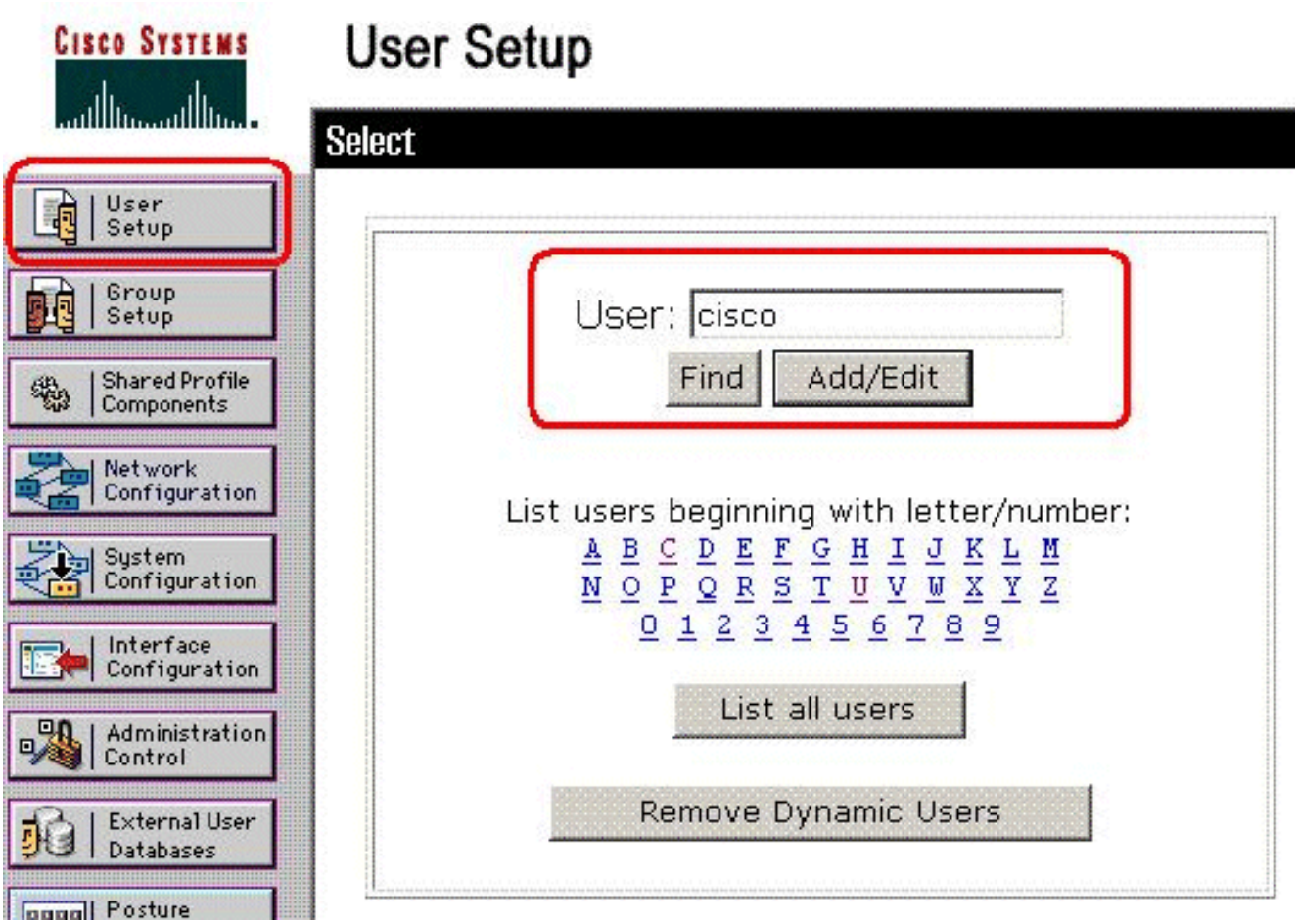
2. Client IP address 필드에 **172.16.1.2**를 입력하고 공유 암호 키 필드에 **"cisco123"**을 입력합니다.Authenticate Using(**인증 사용**) 드롭다운 상자**에서 RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**를 선택합니다.Submit(제출)**을 클릭합니다**

..



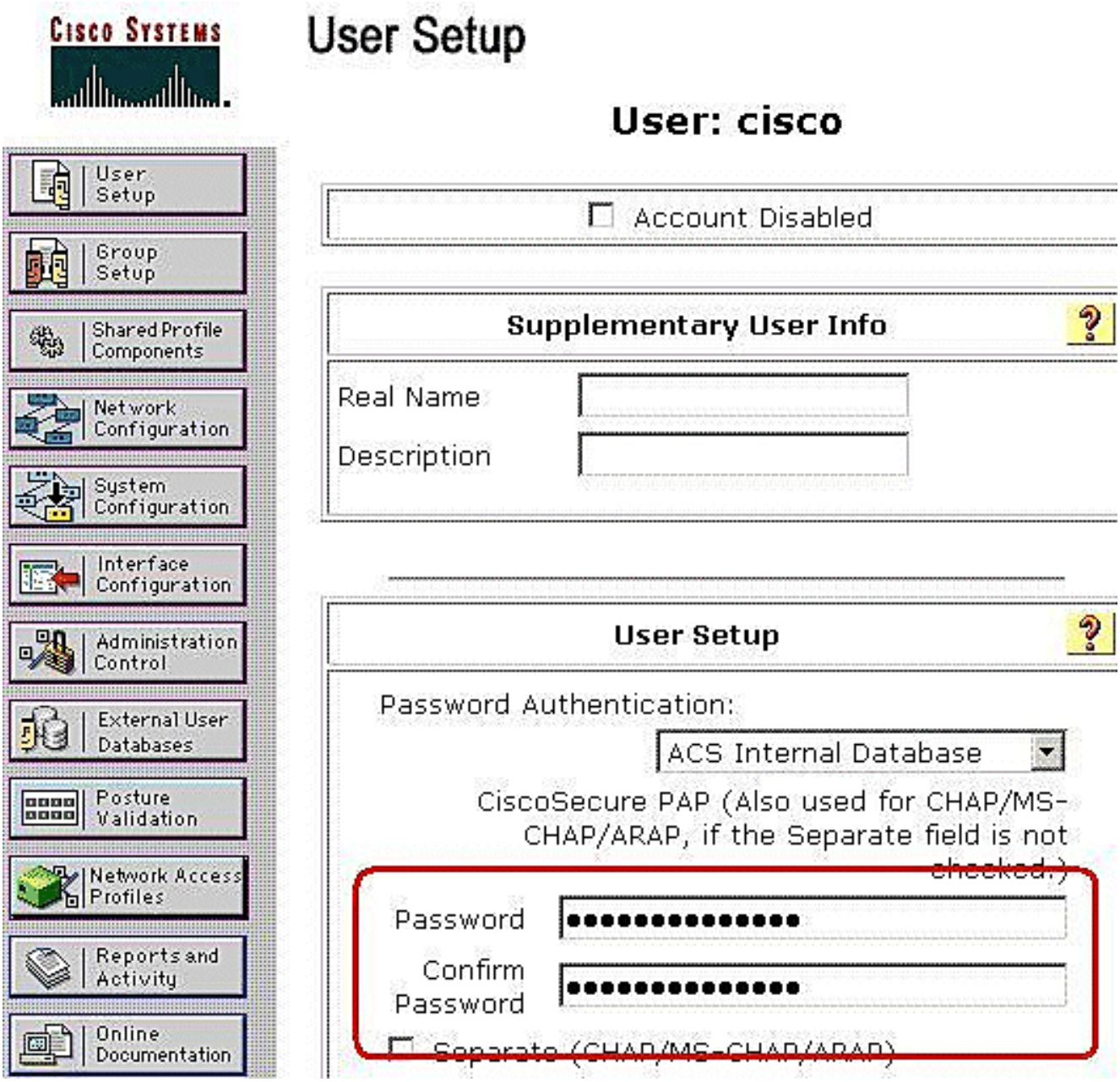
3. Cisco Secure 데이터베이스의 User(사용자) 필드에 사용자 이름을 입력하고 Add/**Edit(추가/수정)를** 클릭합니다.이 예에서 사용자 이름은 **cisco**입니다

.



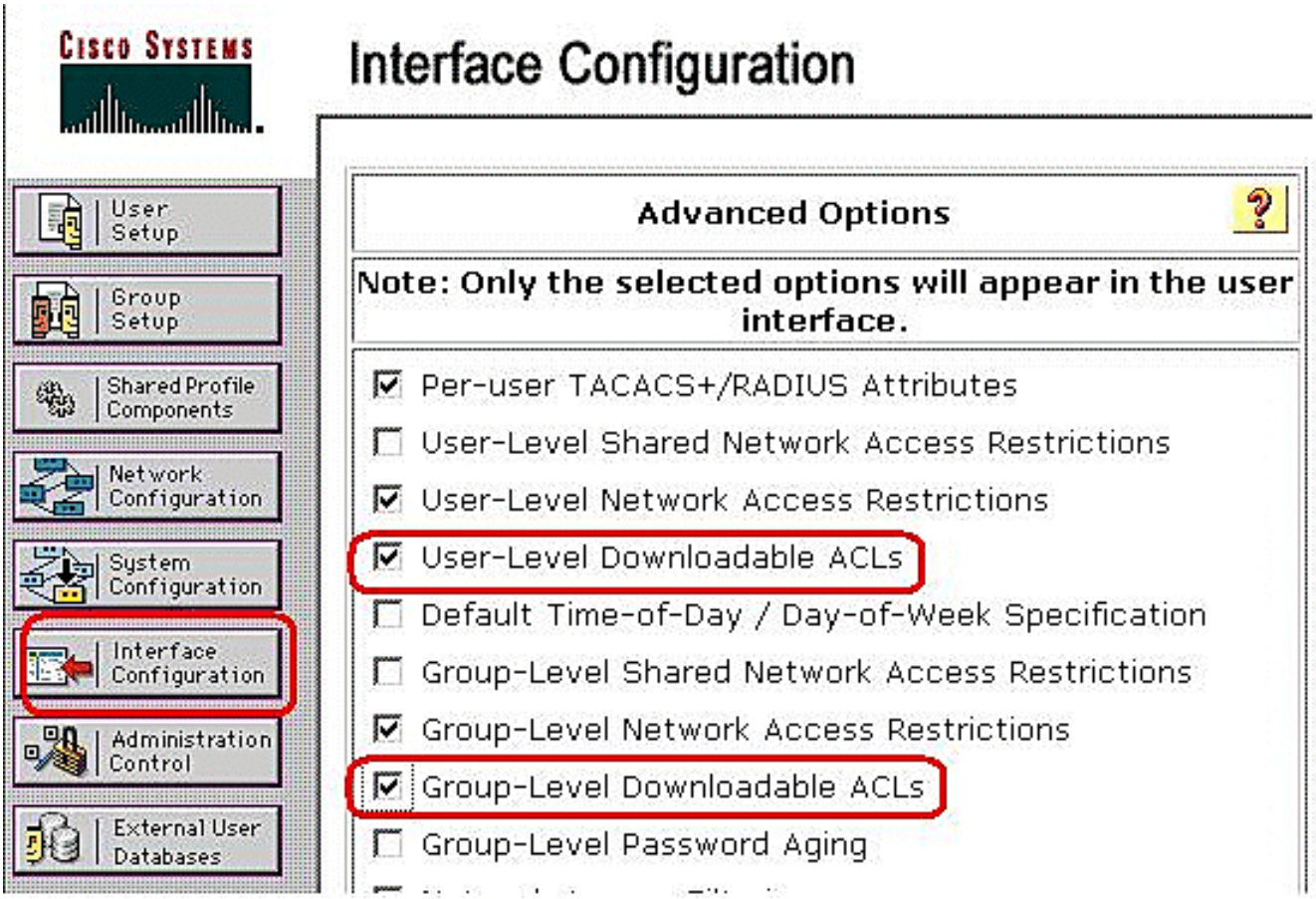
4. 다음 창에서 **"cisco"**의 비밀번호를 **입력합니다**. 이 예에서는 비밀번호도 password**1입니다**. 완료되면 **제출을** 누릅니다

.



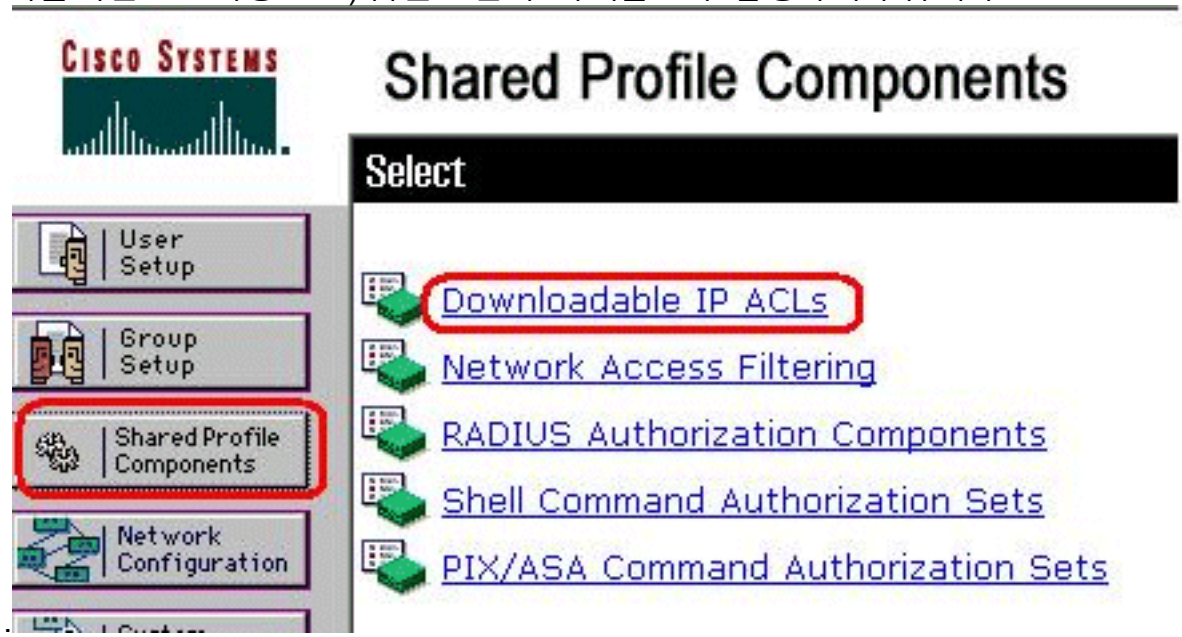
5. 고급 옵션 페이지를 사용하여 ACS에서 표시할 고급 옵션을 결정합니다.사용하지 않는 고급 옵션을 숨기면 ACS 웹 인터페이스의 다른 영역에 표시되는 페이지를 단순화할 수 있습니다 .Interface **Configuration**을 클릭한 다음 **Advanced Options**를 클릭하여 Advanced Options 페이지를 엽니다

.

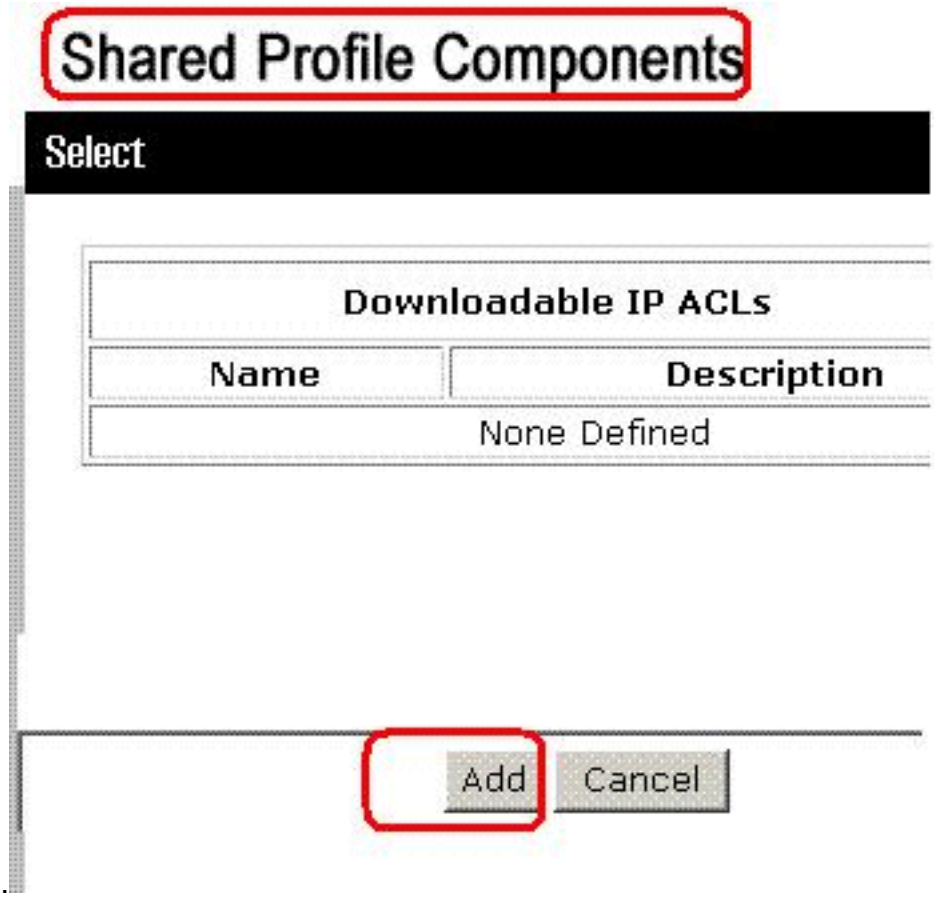


사용자 수준 다운로드 가능 ACL 및 **그룹 수준 다운로드 가능 ACL**에 대한 **확인란을 선택합니다**.**사용자 레벨 다운로드 가능한 ACL** - 이 옵션을 선택하면 User Setup(사용자 설정) 페이지에서 Downloadable ACL(access-control lists)(다운로드 가능한 ACL(액세스 제어 목록)) 섹션을 활성화합니다.**그룹 레벨 다운로드 가능한 ACL** - 이 옵션을 선택하면 그룹 설정 페이지에서 다운로드 가능한 ACLs 섹션을 활성화합니다.

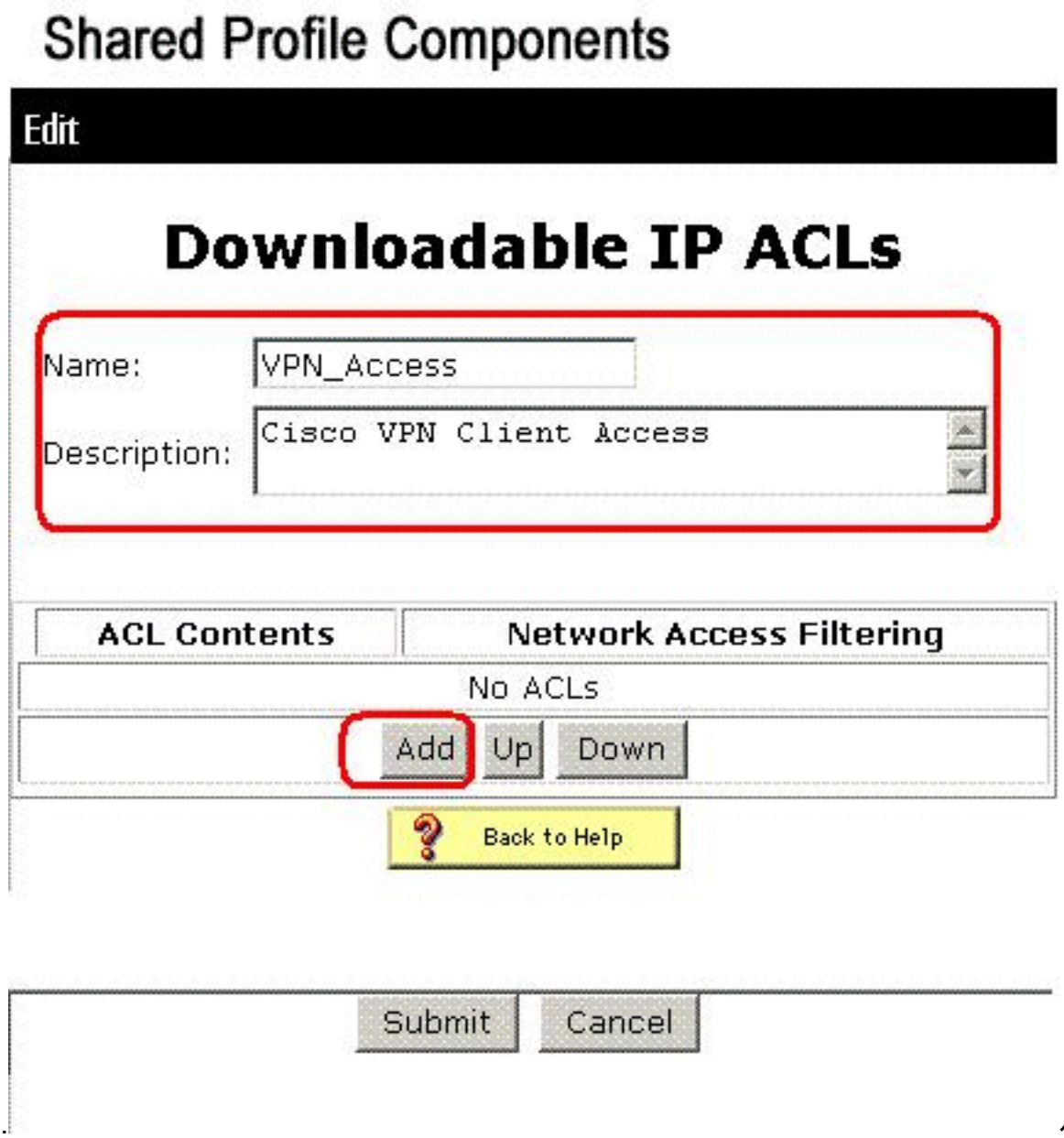
6. 탐색 모음에서 **Shared Profile Components(공유 프로파일 구성 요소)를** 클릭하고 Downloadable **IP ACLs(다운로드 가능한 IP ACL)**를 클릭합니다.**참고:** 다운로드 *가능한 IP ACL이* Shared Profile Components 페이지에 나타나지 않으면 Interface Configuration(인터페이스 컨피그레이션) 섹션의 Advanced Options(고급 옵션) 페이지에서 User-Level Downloadable ACL(사용자 레벨 다운로드 가능 ACL), Group-Level Downloadable ACLs(그룹 레벨 다운로드 가능 ACL) 옵션 또는 두 가지를 모두 활성화해야 합니다



7. Add(**추가)를 클릭합니다**.Downloadable IP ACLs 페이지가 나타납니다

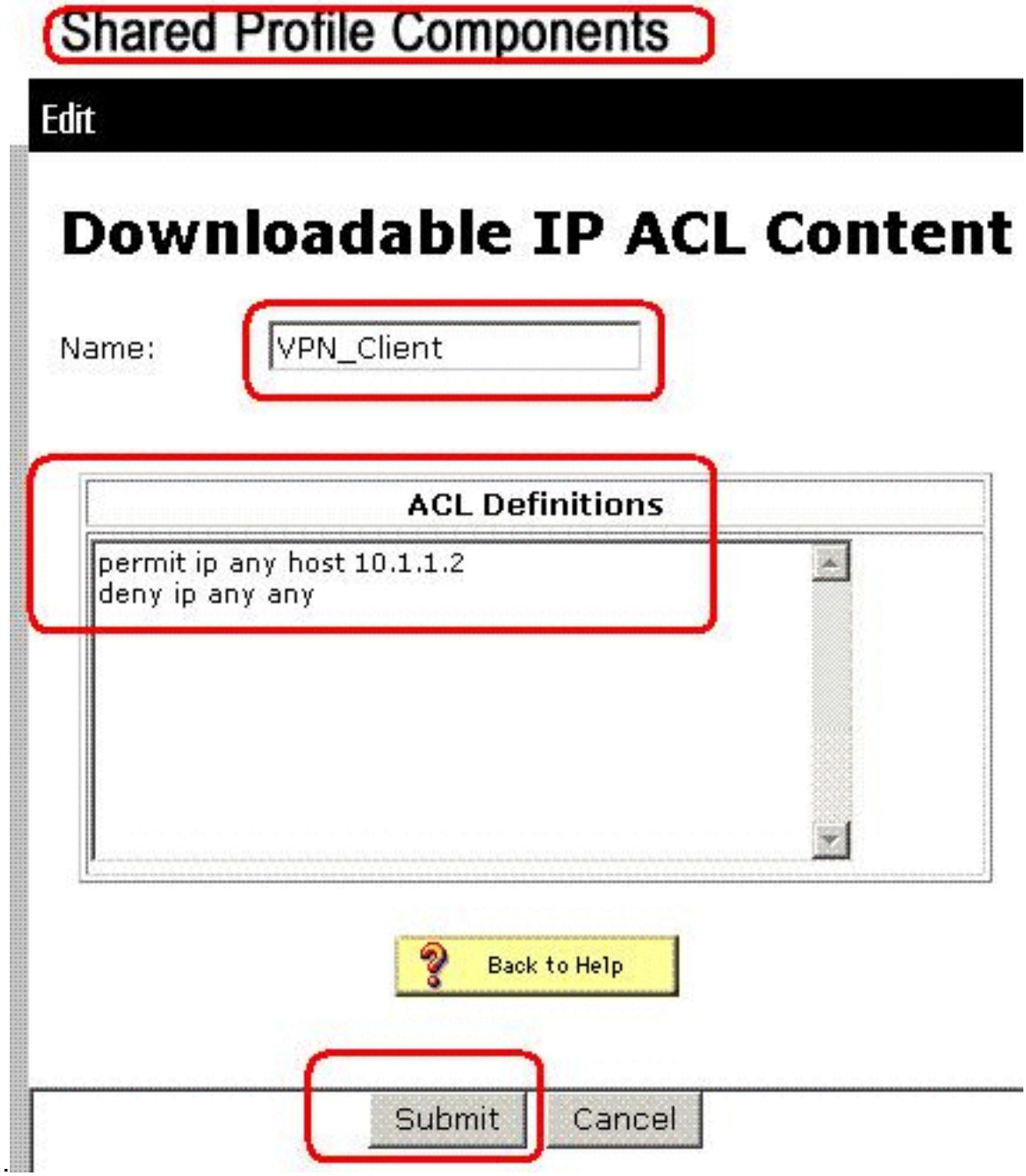


8. Name(이름) 상자에 새 IP ACL의 이름을 입력합니다.**참고:** IP ACL의 이름은 최대 27자를 포함할 수 있습니다.이름에는 공백이나 다음 문자를 사용할 수 없습니다.하이픈(-), 왼쪽 대괄호([), 오른쪽 대괄호(]), 슬래시(/), 백슬래시(\), 따옴표("), 왼쪽 꺾쇠 괄호(<), 오른쪽 꺾쇠 괄호(>) 또는 대시(-).Description(설명) 상자에 새 IP ACL에 대한 설명을 입력합니다.설명은 최대 1,000자까지 입력할 수 있습니다

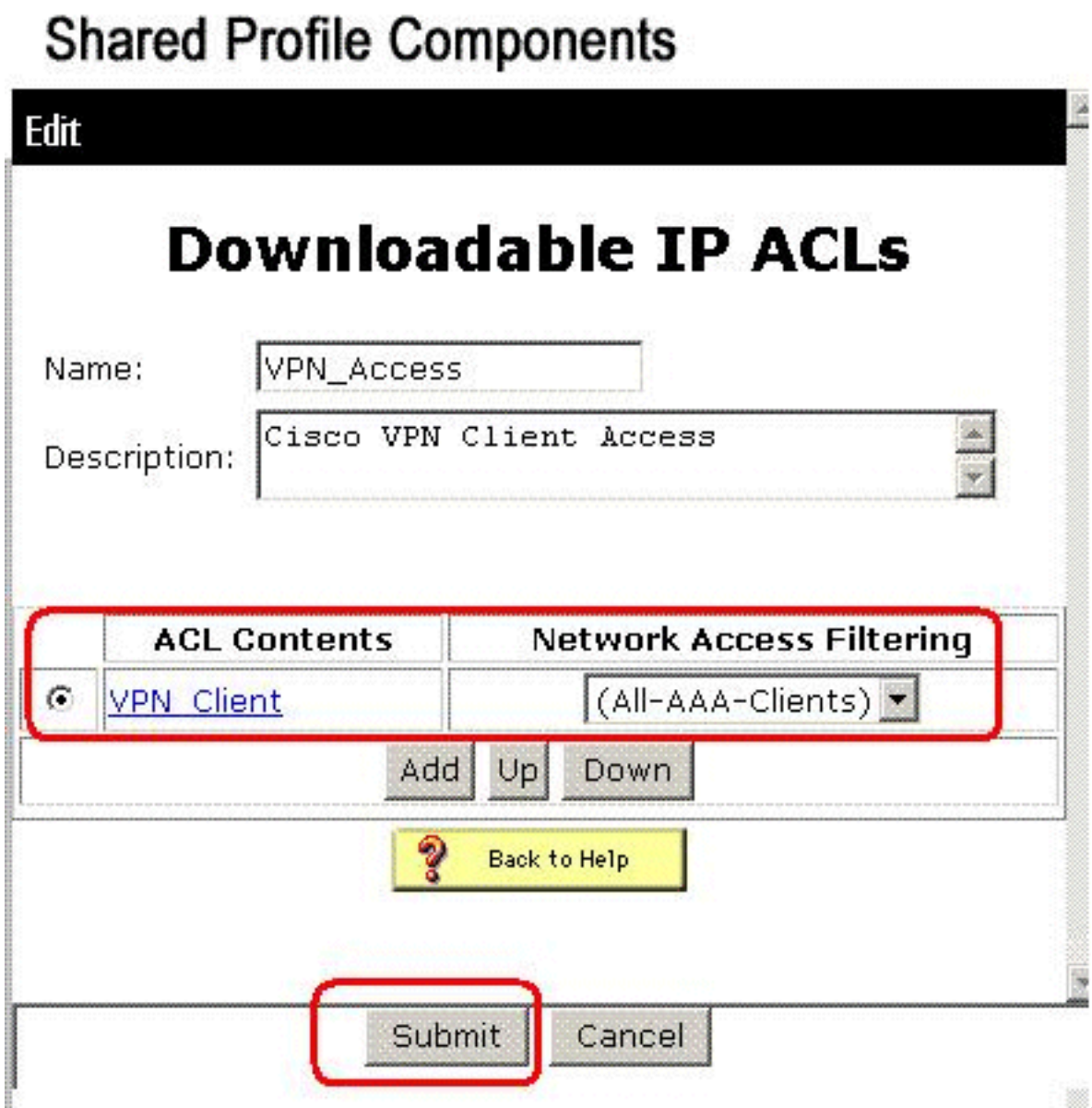


새 IP ACL에 ACL 내용을 추가하려면 Add(추가)를 **클릭합니다**.

9. Name(이름) 상자에 새 ACL 콘텐츠의 이름을 입력합니다.**참고:** ACL 콘텐츠 이름은 최대 27자까지 가능합니다.이름에는 공백이나 다음 문자를 사용할 수 없습니다.하이픈(-), 왼쪽 대괄호([), 오른쪽 대괄호(]), 슬래시(/), 백슬래시(\), 따옴표("), 왼쪽 꺾쇠 괄호(<), 오른쪽 꺾쇠 괄호(>) 또는 대시(-).ACL 정의 상자에 새 ACL 정의를 입력합니다.**참고:** ACS 웹 인터페이스에 ACL 정의를 입력할 때 키워드 또는 이름 항목을 사용하지 마십시오.대신 permit 또는 deny 키워드로 시작합니다.ACL 내용을 저장하려면 Submit(제출)을 **클릭합니다**

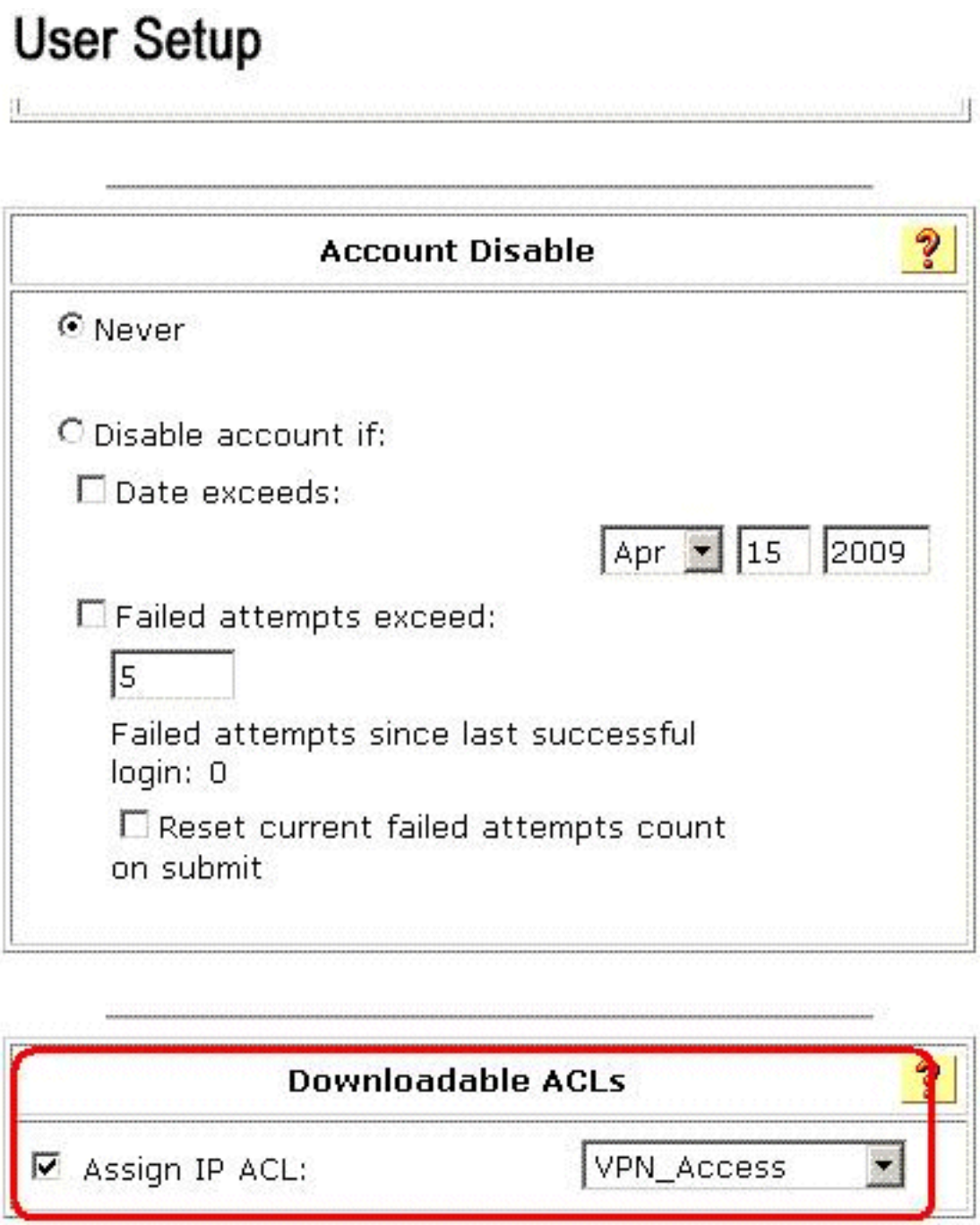


10. Downloadable IP ACLs 페이지가 나타나고 ACL Contents 열에 이름으로 나열된 새 ACL 콘텐츠가 표시됩니다.NAC 콘텐츠에 NAF를 연결하려면 새 ACL 콘텐츠의 오른쪽에 있는 Network Access Filtering(네트워크 액세스 필터링) 상자에서 NAF를 선택합니다.기본적으로 NAF는 (All-AAA-Clients)입니다. NAF를 할당하지 않으면 ACS는 모든 네트워크 디바이스에 ACL 콘텐츠를 연결합니다(기본값



). ACL 콘텐츠의 순서를 설정하려면 ACL 정의에 대한 라디오 버튼을 클릭한 다음 **Up** 또는 **Down을** 클릭하여 목록에서 위치를 변경합니다.IP ACL을 저장하려면 Submit(제출)을 **클릭합니다.참고:** ACL 콘텐츠의 순서는 중요합니다.위에서 아래로 ACS는 All-AAA-Clients 기본 설정(사용되는 경우)을 포함하는 적용 가능한 NAC 설정이 있는 첫 번째 ACL 정의만 다운로드합니다.일반적으로 ACL 콘텐츠 목록은 가장 구체적인(좁은) NAC가 있는 NF에서 가장 일반적인(All-AAA-Clients) NF가 있는 NAC로 진행됩니다.**참고:** ACS는 새 IP ACL을 입력하며 이는 즉시 적용됩니다.예를 들어, IP ACL이 PIX 방화벽과 함께 사용되는 경우, 다운로드 가능한 IP ACL이 사용자 또는 그룹 프로필에 할당된 사용자의 인증을 시도하는 PIX 방화벽으로 IP ACL을 전송할 수 있습니다.

11. 사용자 설정 페이지로 이동하여 사용자 페이지를 편집합니다.Downloadable ACLs(다운로드 가능한 ACL) 섹션에서 Assign **IP ACL:(IP ACL 할당:**확인란을 선택합니다.목록에서 IP ACL을 선택합니다.사용자 계정 옵션 구성을 완료한 경우 **Submit**(제출)을 클릭하여 옵션을



기록합니다.

그룹에 대해 다운로드 가능한 ACL을 위한 ACS 구성

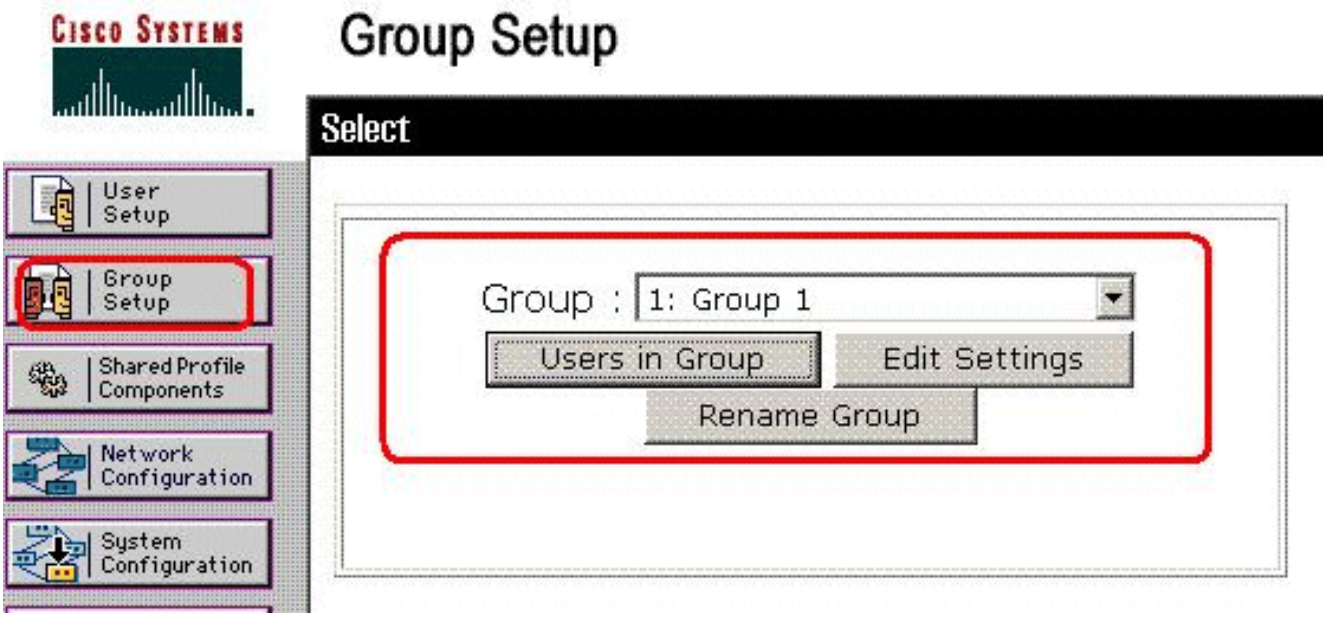
Configure ACS for Downloadable ACL for Individual User(개별 사용자에 대해 다운로드 가능한 ACL을 위한 ACS 구성) 1~9단계를 완료하고 Cisco Secure ACS에서 그룹에 대해 다운로드 가능한 ACL을 구성하려면 다음 단계를 수행합니다.

이 예에서는 IPSec VPN 사용자 "cisco"가 VPN 그룹에 속합니다.VPN 그룹 정책은 그룹의 모든 사용자에게 적용됩니다.

VPN 그룹 사용자 **"cisco"가** 성공적으로 인증되고 RADIUS 서버가 보안 어플라이언스에 다운로드 가능한 액세스 목록을 전송합니다."cisco" 사용자는 10.1.1.2 서버에만 액세스할 수 있으며 다른 모든 액세스를 거부합니다.ACL을 확인하려면 Downloadable ACL for User/Group 섹션을 참조하십시오.

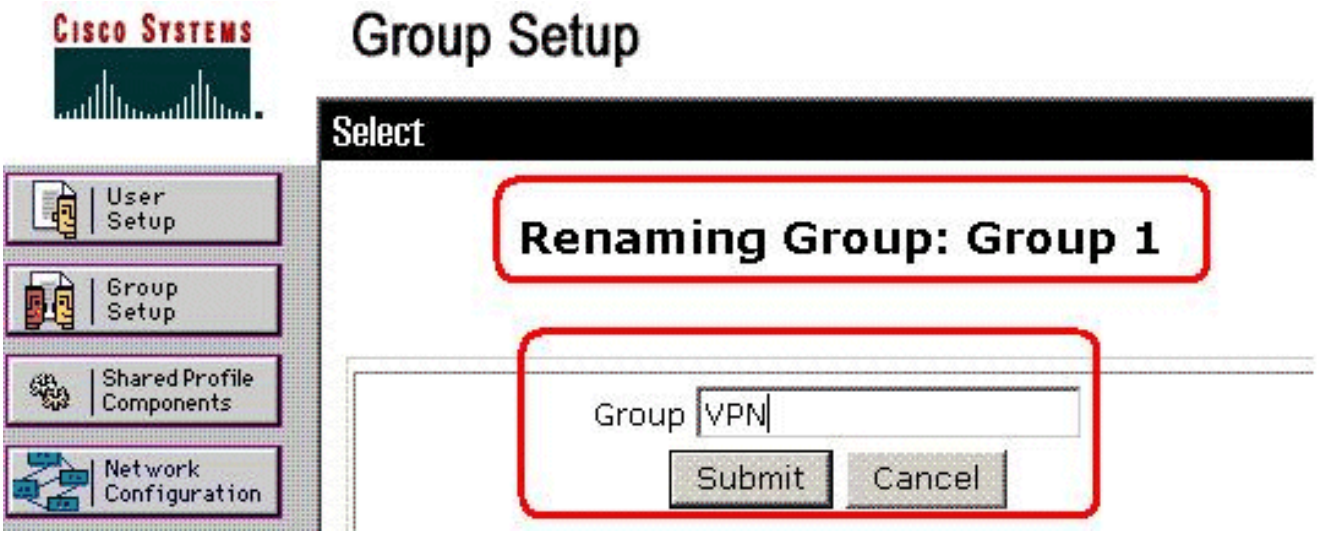
1. 탐색 모음에서 **그룹 설정**을 클릭합니다.그룹 설정 선택 페이지가 열립니다

.

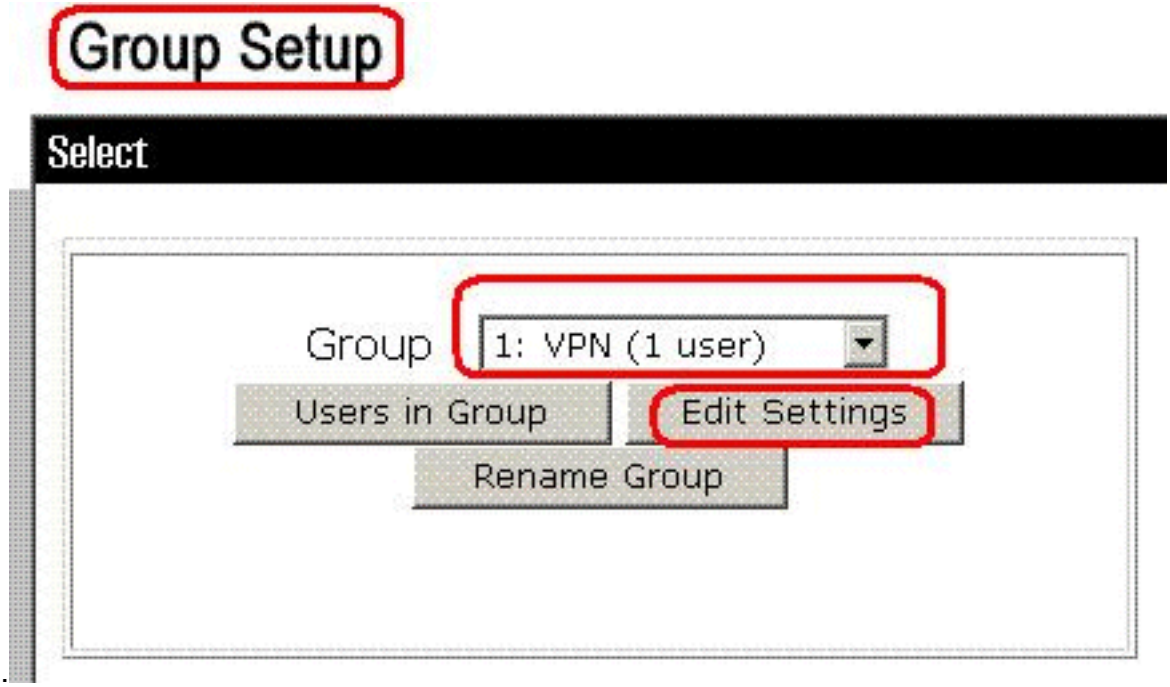


2. 그룹 1의 이름을 **VPN**으로 바꾸고 Submit(제출)을 **클릭합니다**

.

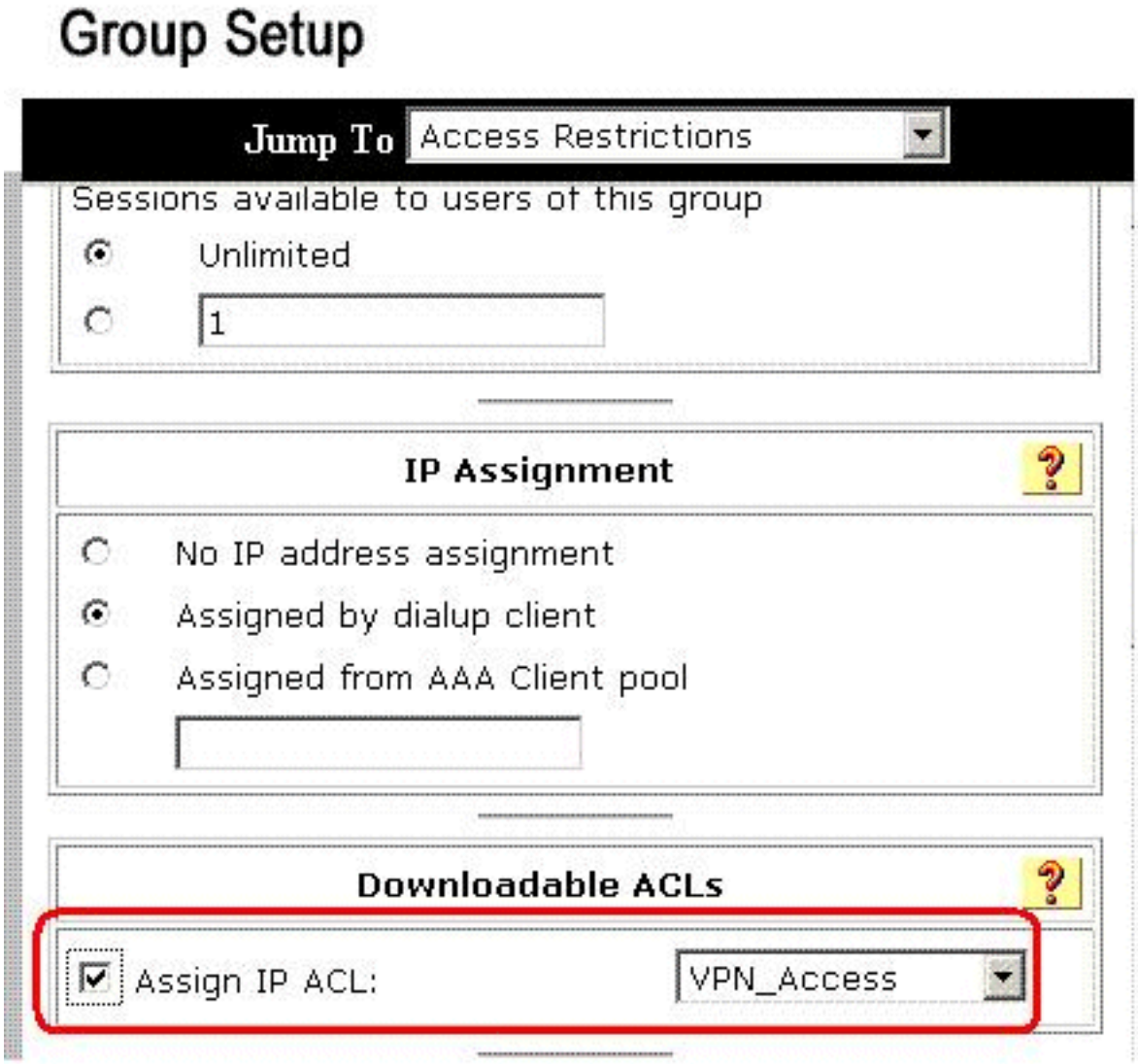


3. 그룹 목록에서 그룹을 선택한 다음 **설정 편집**을 클릭합니다

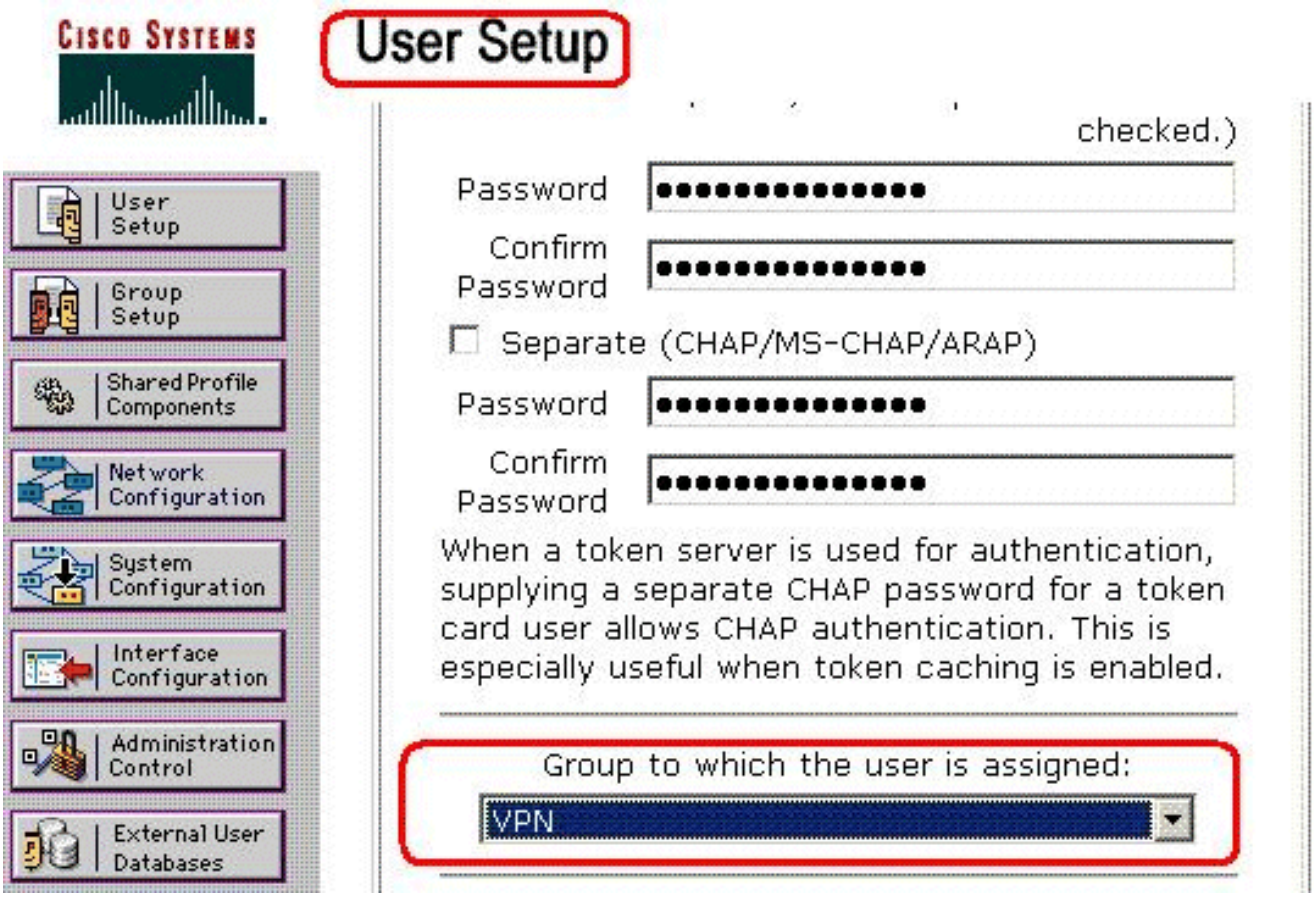


.

4. Downloadable ACLs(다운로드 가능한 ACL) 섹션에서 Assign **IP ACL(IP ACL 할당)** 확인란을 클릭합니다.목록에서 IP ACL을 선택합니다



5. 방금 만든 그룹 설정을 저장하려면 Submit(제출)을 **클릭합니다**.
6. 사용자 설정으로 이동하여 그룹에 추가하려는 사용자를 편집합니다.**VPN**.완료되면 Submit(제출)을 **클릭합니다**



이제 VPN 그룹에 대해 구성된 다운로드 가능한 ACL이 이 사용자에게 적용됩니다.

7. 다른 그룹 설정을 계속 지정하려면 이 장에서 해당하는 다른 절차를 수행합니다

사용자 그룹에 대한 IETF RADIUS 설정 구성

사용자가 인증할 때 RADIUS 서버에서 보안 어플라이언스에 이미 생성한 액세스 목록의 이름을 다운로드하려면 다음과 같이 IETF RADIUS filter-id 특성(특성 번호 11)을 구성합니다.

```
filter-id=acl_name
```

VPN 그룹 사용자 **"cisco"가** 성공적으로 인증되고 RADIUS 서버는 보안 어플라이언스에 이미 생성한 액세스 목록에 대한 ACL 이름(새 이름)을 다운로드합니다."cisco" 사용자는 10.1.1.2 서버를 **제외한** ASA 네트워크 내부에 있는 모든 디바이스에 액세스할 수 있습니다.ACL을 확인하려면 Filter-Id ACL 섹션을 참조하십시오.

예와 같이 **new**라는 ACL이 ASA에서 필터링하도록 구성됩니다.

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

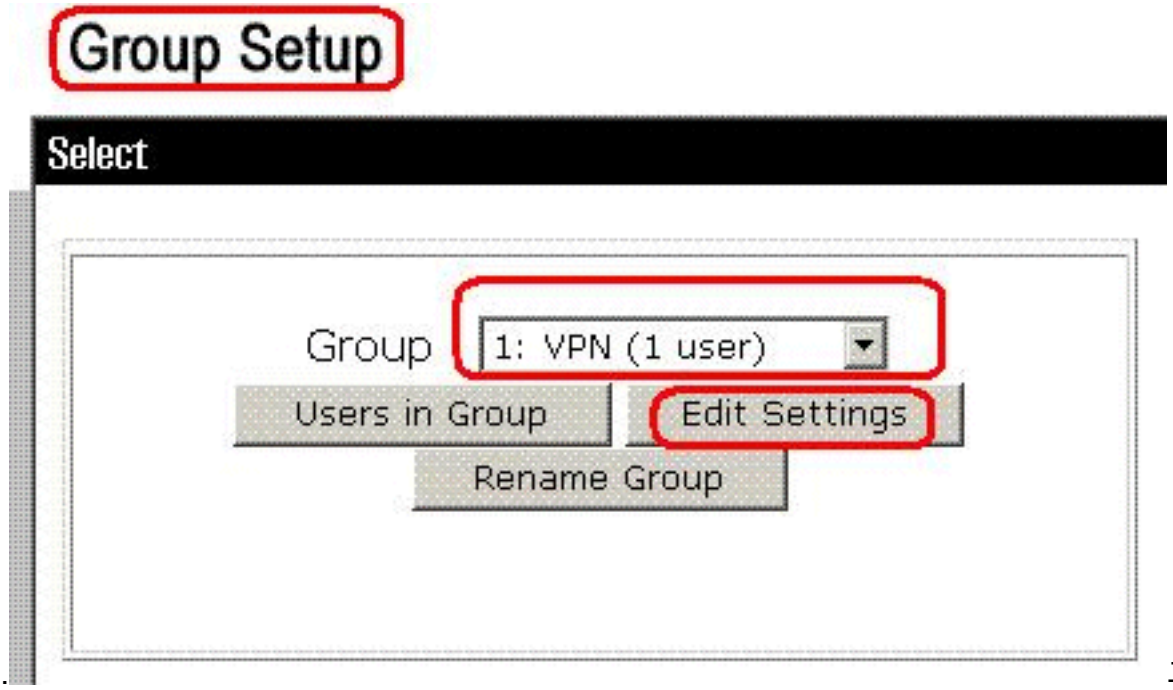
이러한 매개변수는 true인 경우에만 나타납니다.구성

- 네트워크 컨피그레이션에서 RADIUS 프로토콜 중 하나를 사용하는 AAA 클라이언트
- 웹 인터페이스의 Interface Configuration(인터페이스 컨피그레이션) 섹션에 있는 RADIUS(IETF) 페이지의 그룹 레벨 RADIUS 특성

RADIUS 특성은 ACS에서 요청 AAA 클라이언트로 각 사용자에 대한 프로필로 전송됩니다.

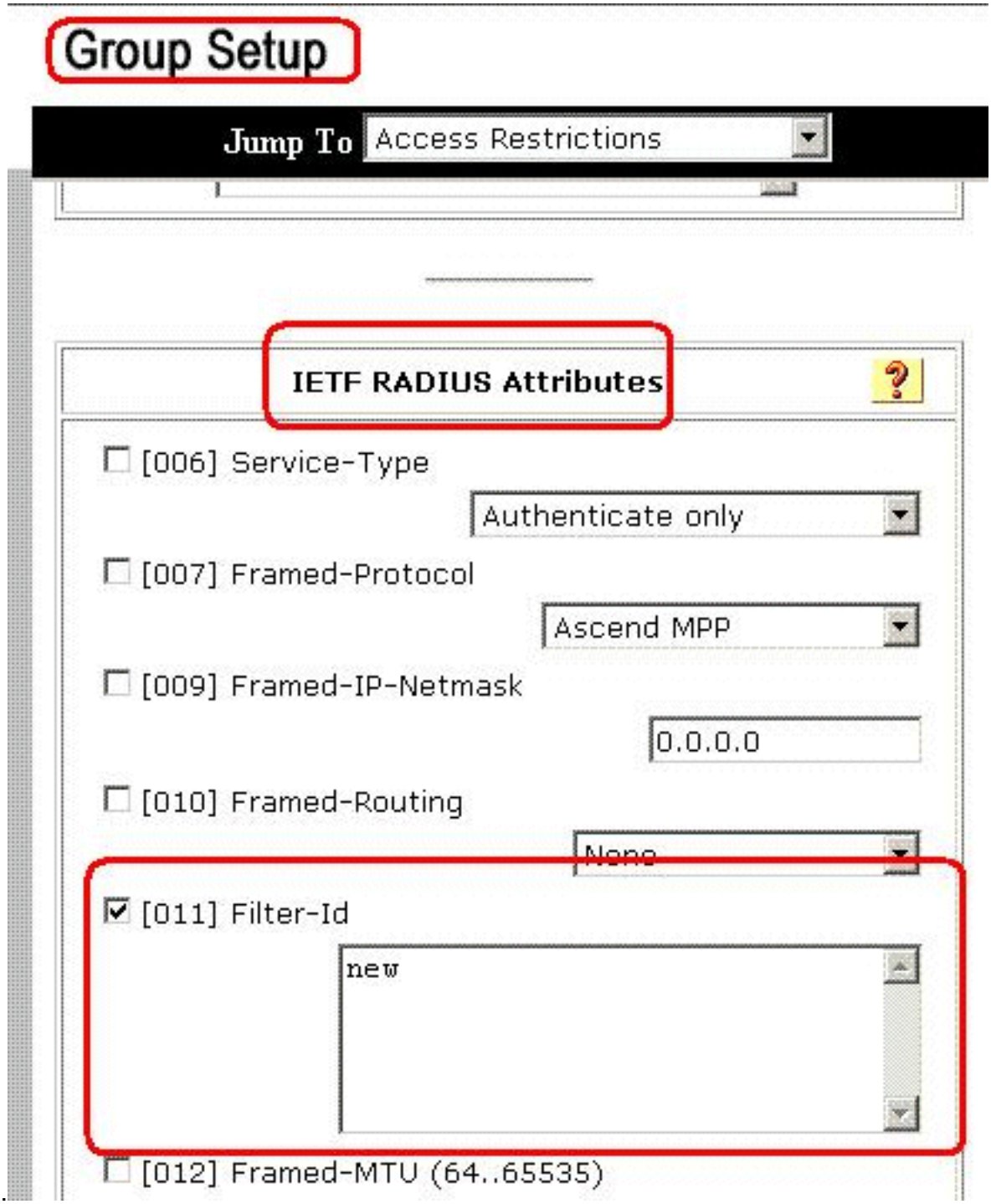
현재 그룹의 각 사용자에 대해 권한 부여로 적용할 IETF RADIUS 특성 설정을 구성하려면 다음 작업을 수행합니다.

1. 탐색 모음에서 **그룹 설정**을 클릭합니다.그룹 설정 선택 페이지가 열립니다.
2. 그룹 목록에서 그룹을 선택한 다음 **설정 편집**을 클릭합니다



그룹 이름이 그룹 설정 페이지 상단에 나타납니다.

3. IEFT RADIUS Attributes(IEFT RADIUS 특성)로 스크롤합니다.각 IETF RADIUS 특성에 대해 현재 그룹에 권한을 부여해야 합니다.**[011] Filter-Id** 특성의 확인란을 선택한 다음 필드의 특성에 대한 권한 부여에서 ASA 정의 ACL 이름(**새**)을 추가합니다.ASA *show running configuration* 출력을 참조하십시오



4. 방금 만든 그룹 설정을 저장하고 즉시 적용하려면 **제출** 및 **적용**을 클릭합니다.**참고:** 그룹 설정을 저장하고 나중에 적용하려면 제출을 **클릭합니다**.변경 사항을 구현할 준비가 되면 System Configuration(시스템 컨피그레이션) **> Service Control(서비스 제어)을** 선택합니다.그런 다음 Restart(**재시작)를** 선택합니다.

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.

암호화 명령 표시

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

```
ciscoasa# sh crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active
   and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.10.2
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
ciscoasa#
```

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

```
ciscoasa# sh crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1,
   local addr: 192.168.1.1

      local ident (addr/mask/prot/port):
   (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
   (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.10.2, username: cisco
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 65, #pkts encrypt:
   65, #pkts digest: 65
      #pkts decaps: 65, #pkts decrypt:
   65, #pkts verify: 65
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed:
   0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures:
   0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0,
   #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.1.1,
   remote crypto endpt.: 192.168.10.2

      path mtu 1500, ipsec overhead 58,
   media mtu 1500
      current outbound spi: EEF0EC32

    inbound esp sas:
      spi: 0xA6F92298 (2801345176)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec):
   28647
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xEEF0EC32 (4008766514)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec): 28647
         IV size: 8 bytes
```

```
            replay detection support: Y
```

사용자/그룹에 대해 다운로드 가능한 ACL

사용자 Cisco에 대해 다운로드 가능한 ACL을 확인합니다.ACL은 CSACS에서 다운로드됩니다.

```
ciscoasa(config)# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
   192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411

access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic)
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
   ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
   ip any any (hitcnt=40) 0x7c718bd1
```

필터 ID ACL

[011] Filter-Id가 Group - VPN에 적용되었으며 그룹의 사용자는 ASA에 정의된 ACL(새 항목)에 따라 필터링됩니다.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
   255.255.255.0 192.168.5.0 255.255.255.0
   (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip
   any host 10.1.1.2 (hitcnt=4) 0xb247fec8
access-list new line 2 extended permit ip any any
   (hitcnt=39) 0x40e5d57c
```

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 Adaptive Security Device Manager
- IPsec 협상/IKE 프로토콜 지원 페이지
- Cisco VPN 클라이언트 지원 페이지
- Windows용 Cisco Secure Access Control Server
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems