ASA/PIX:DHCP 서버를 사용하여 ASDM 컨피그레이션을 사용하는 IPsec VPN 클라이언트 주소 지정 예

목차

소개

이 문서에서는 DHCP 서버가 ASDM(Adaptive Security Device Manager) 또는 CLI를 사용하여 모든 VPN 클라이언트에 클라이언트 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 클라이언트를 사용하여 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)를 사용하여 Cisco VPN Client(4.x for Windows) 간 원격 액세스 VPN 연결을 설

정하려면 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.

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 ASA 5500 Series Adaptive Security Appliance입니다.

보안 어플라이언스 주소 관리에서는 터널을 통해 사설 네트워크의 리소스와 클라이언트를 연결하는 IP 주소를 구성하고 클라이언트가 사설 네트워크에 직접 연결된 것처럼 작동하도록 해야 합니다.또한 클라이언트에 할당되는 전용 IP 주소만 처리합니다.사설 네트워크의 다른 리소스에 할당된 IP 주소는 VPN 관리의 일부가 아니라 네트워크 관리 권한의 일부입니다.따라서 여기에서 IP 주소를 설명하는 경우, 클라이언트가 터널 엔드포인트로 작동할 수 있도록 하는 사설 네트워크 주소 지정 체계에서 사용할 수 있는 IP 주소를 의미합니다.

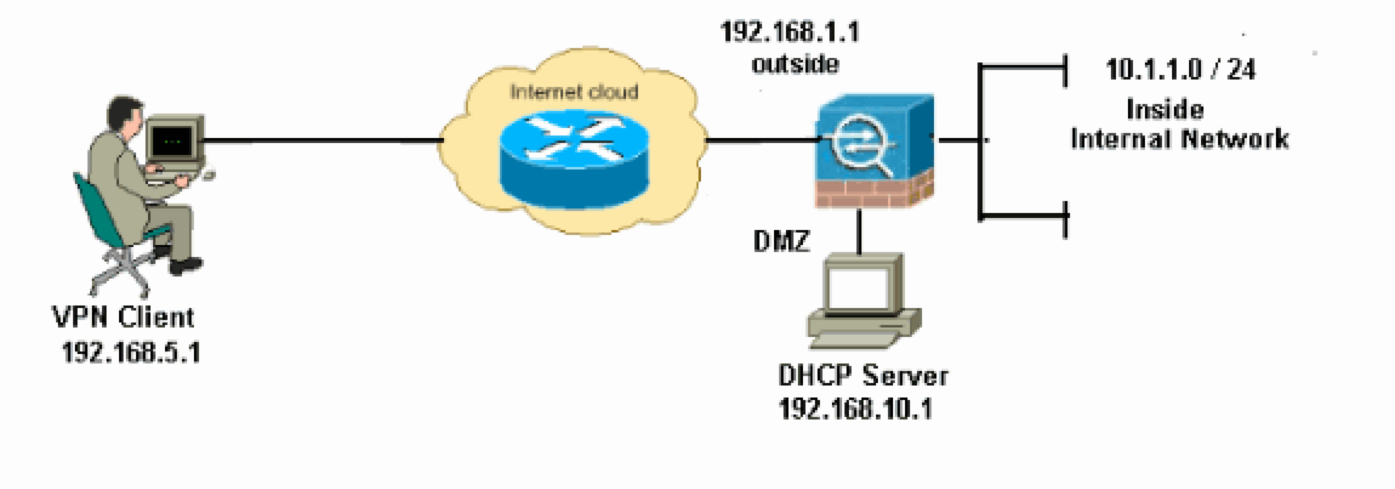
구성

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.



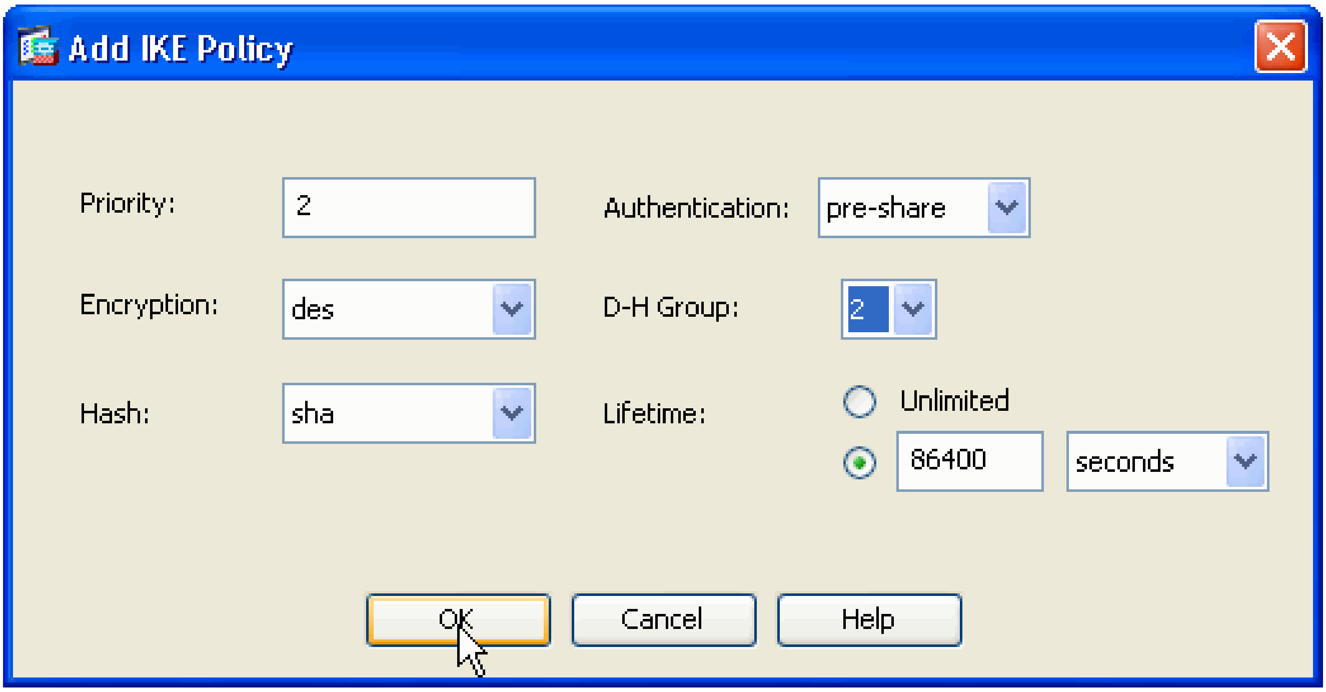
참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

원격 액세스 VPN(IPSec) 구성

ASDM 절차

원격 액세스 VPN을 구성하려면 다음 단계를 완료합니다.

1. ISAKMP **정책** 2를 생성하려면 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add**를 선택합니다
   .



Priority: 2

Authentication: pre-share

Encryption: des

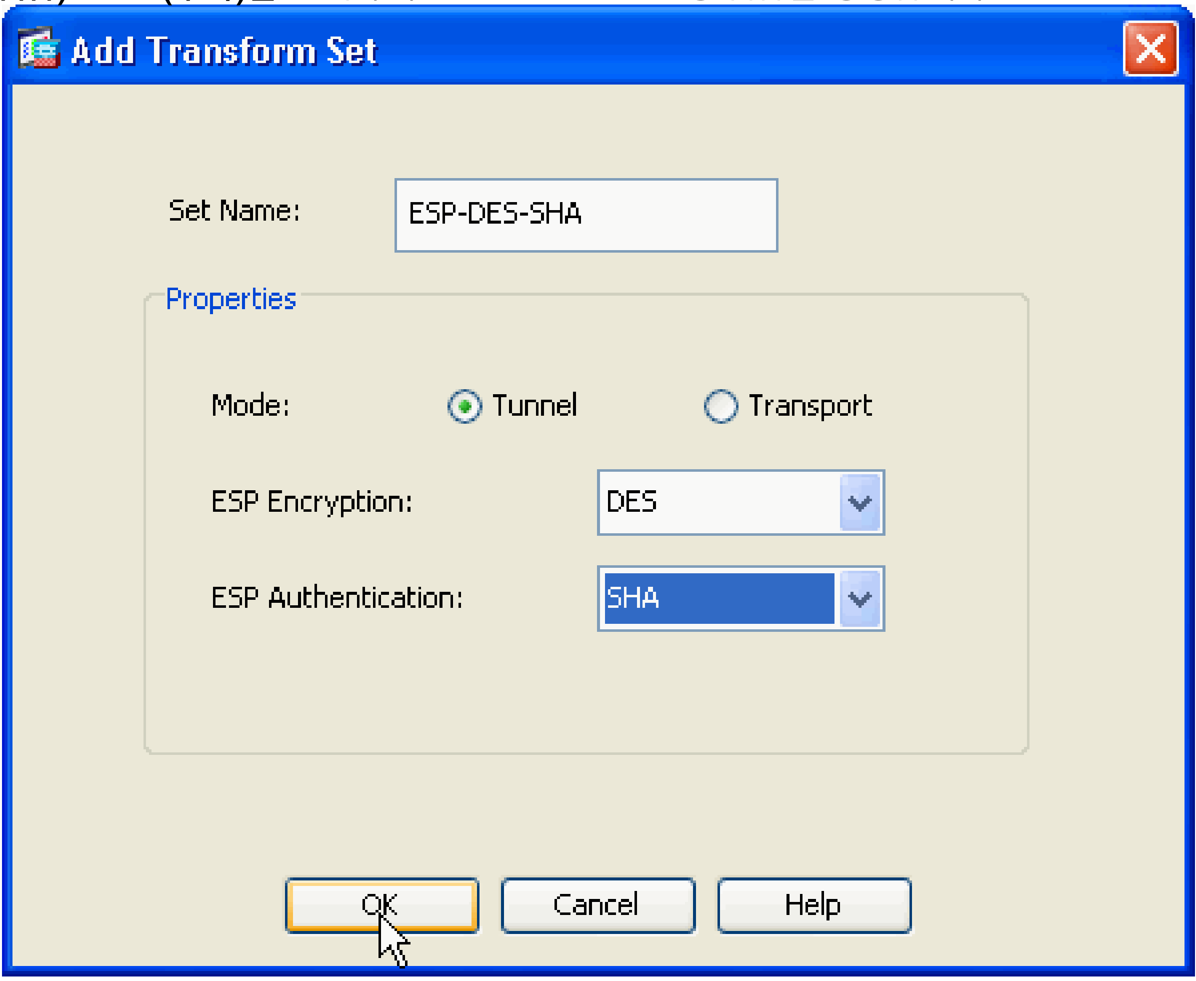
D-H Group: 2

Hash: sha

Lifetime: ○ Unlimited ● 86400 seconds

OK(**확인**)와 Apply(적용)를 **클릭합니다**.

2. 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



Set Name: ESP-DES-SHA

Properties

Mode: ● Tunnel ○ Transport

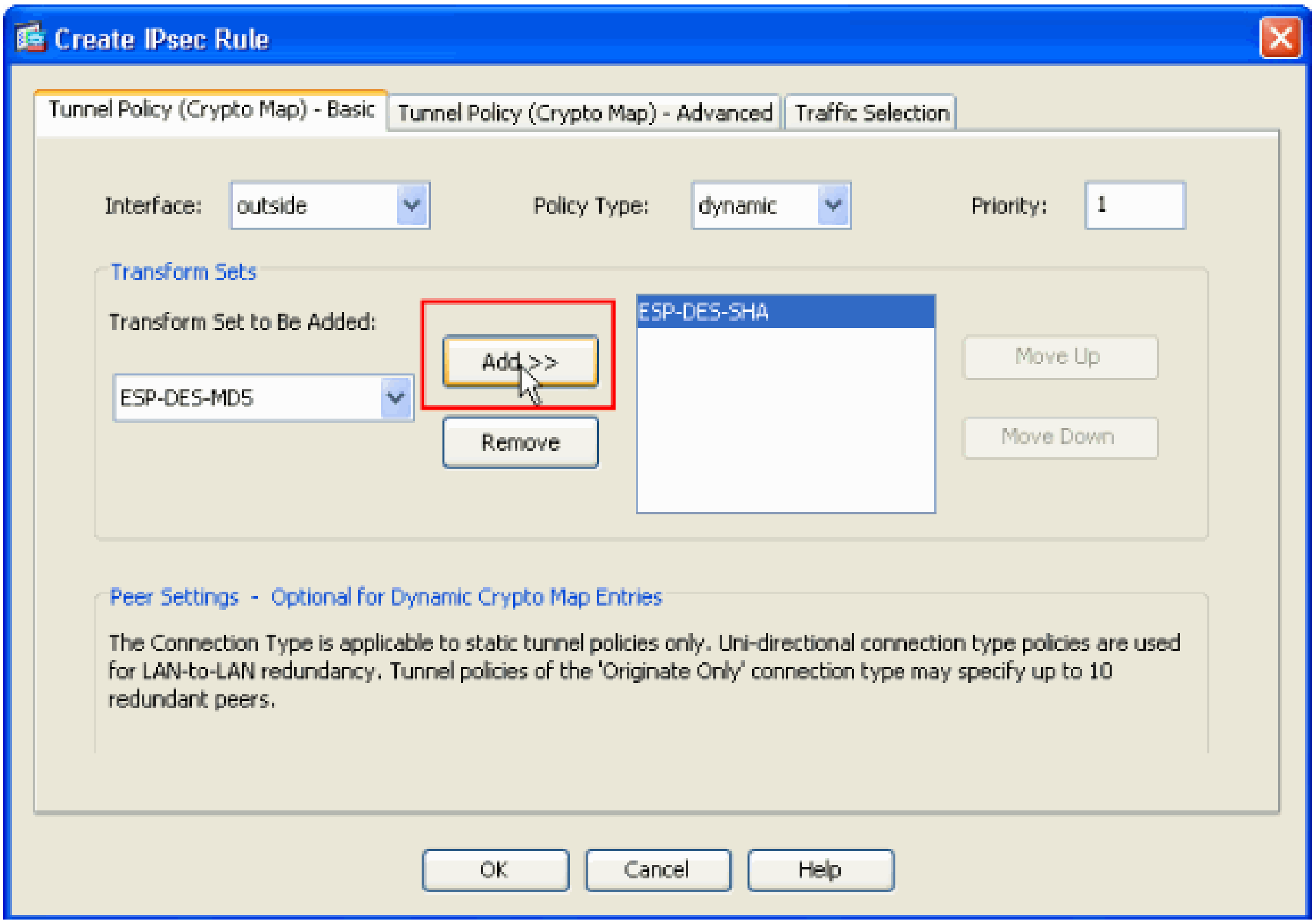
ESP Encryption: DES

ESP Authentication: SHA

.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 > Crypto Maps(암호화 맵) > Add(추가)를 선택하여** 우선순위 1의 동적 정책으로 암호화 맵을 생성합니다

.


Create IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Transform Sets
Add >>
Remove
Move Up
Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries
OK
Cancel
Help

Interface: outside

Policy Type: dynamic

Priority: 1

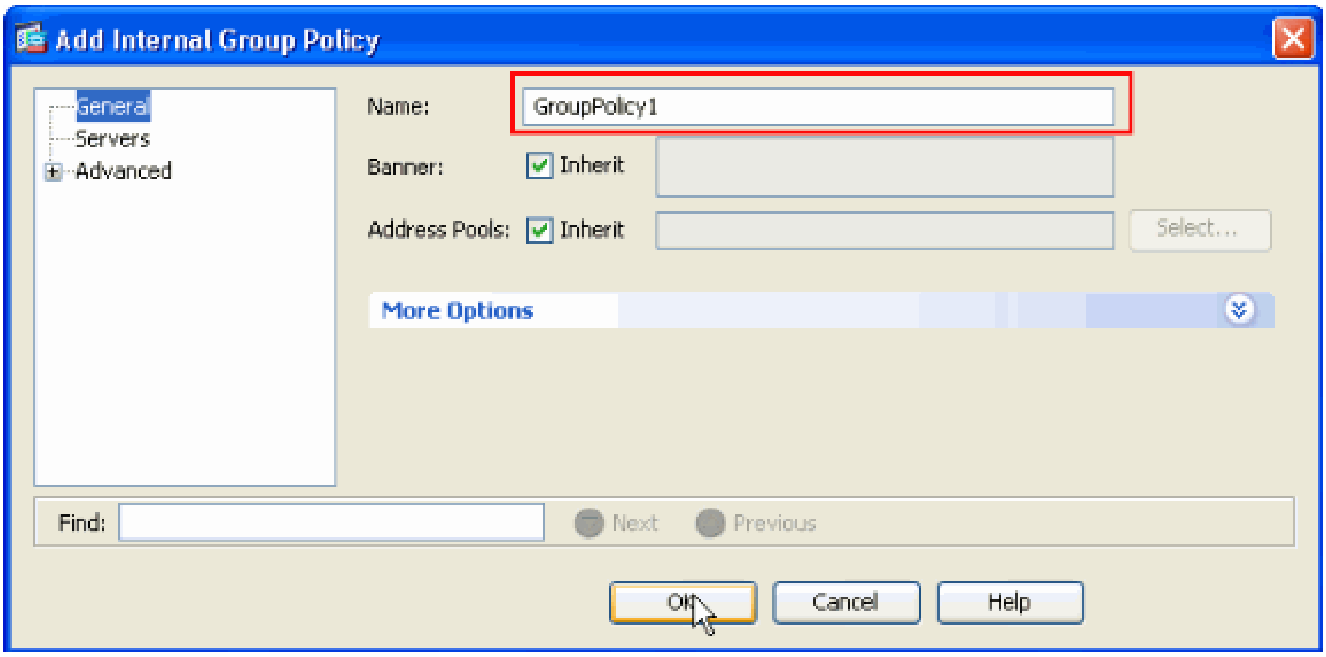
Transform Set to Be Added: ESP-DES-MD5

ESP-DES-SHA

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

OK(**확인**)와 Apply(적용)를 **클릭합니다**.

4. 그룹 정책(예: **GroupPolicy1**)을 생성하려면 **Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > Group Policies(그룹 정책) > Add(추가)>Internal Group Policies(내부 그룹 정책)**를 선택합니다
   .



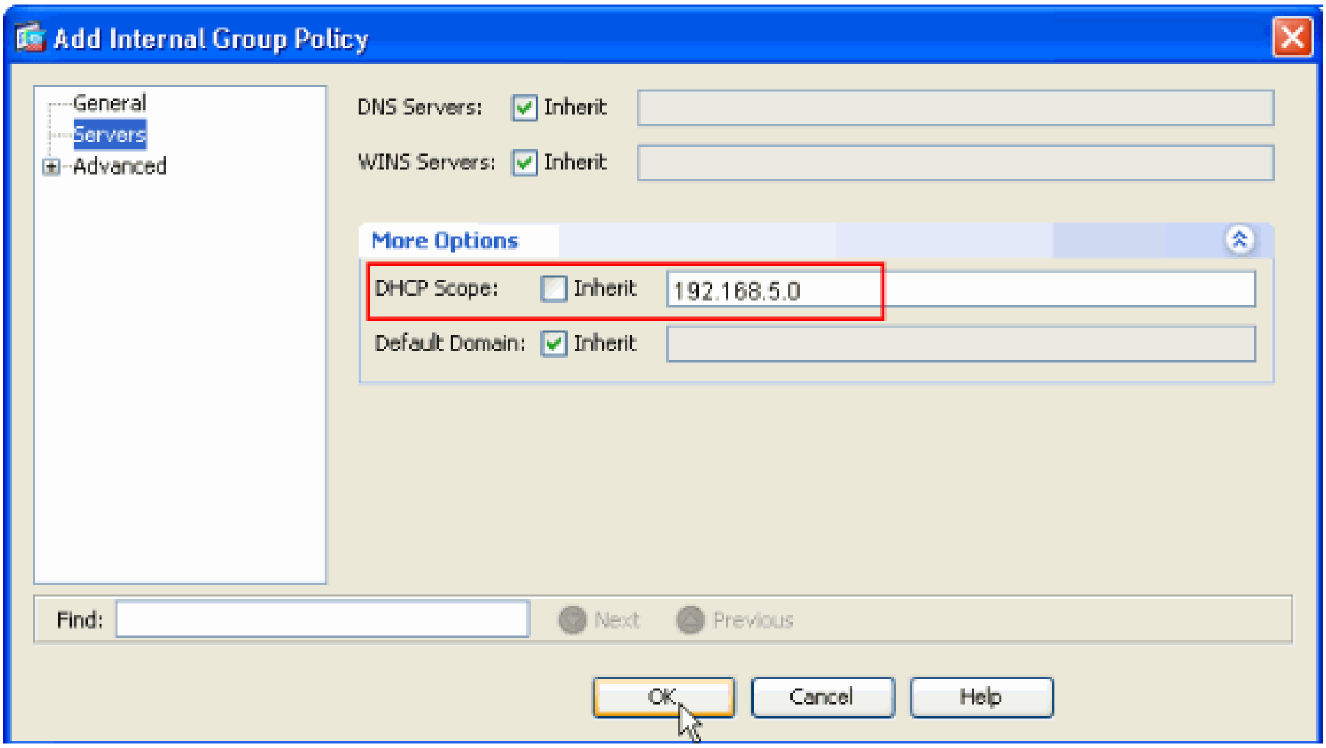
Name: GroupPolicy1

Banner: ☑ Inherit

Address Pools: ☑ Inherit

OK(**확인**)와 Apply(적용)를 **클릭합니다**.

5. VPN 클라이언트 사용자**가** 동적으로 할당되도록 **DHCP 범위를 구성하려면 Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add>Internal Group Policies>Servers>>를** 선택합니다
   .



Add Internal Group Policy

DNS Servers: ☑ Inherit

WINS Servers: ☑ Inherit

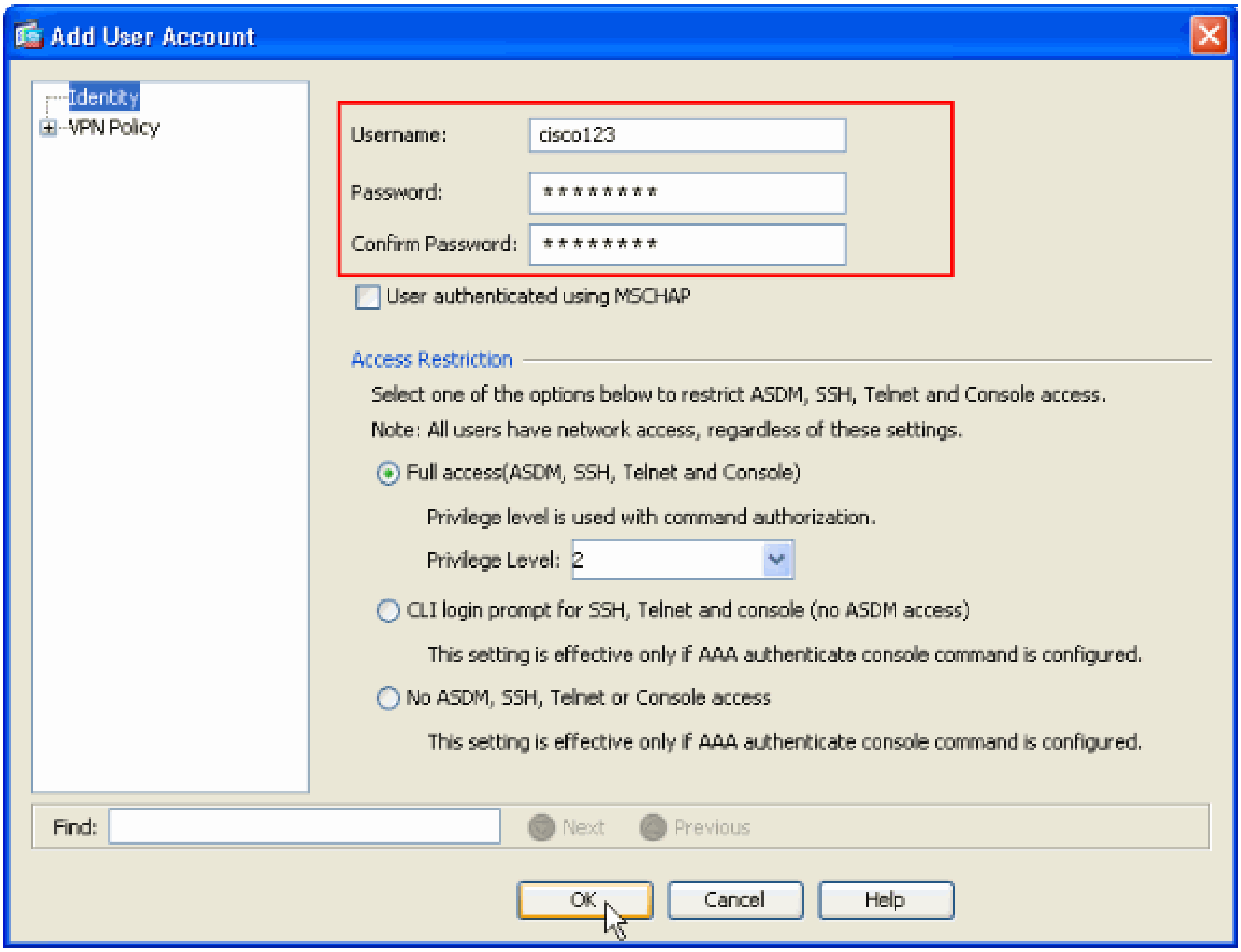
DHCP Scope: □ Inherit 192.168.5.0

Default Domain: ☑ Inherit

OK(**확인**)와 Apply(적용)를 **클릭합니다.참고:** DHCP 범위 구성은 선택 사항입니다.자세한 내용은 [DHCP 주소 지정 구성](#)을 참조하십시오.

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

.



Add User Account

Username: cisco123

Password: ********

Confirm Password: ********

□ User authenticated using MSCHAP

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if AAA authenticate console command is configured.

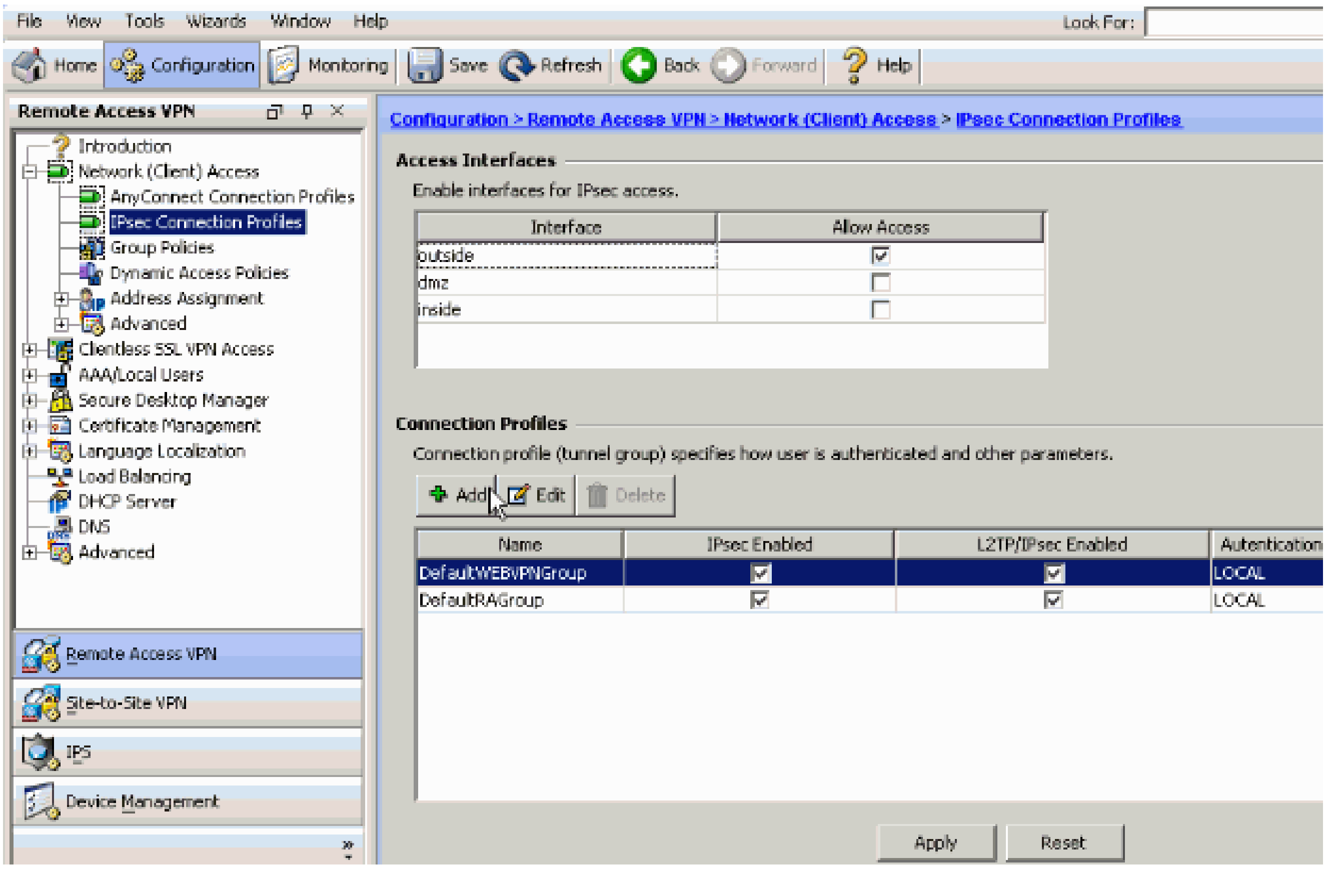
○ No ASDM, SSH, Telnet or Console access

This setting is effective only if AAA authenticate console command is configured.

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

트워크(클라이언트) 액세스) > IPSec Connection Profiles(IPSec 연결 프로파일) > Add(추가)>를 선택하여 터널 그룹(예: **TunnelGroup1** 및 Preshared key as cisco123)을 추가합니다

.



Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☑
dmz	☐
inside	☐

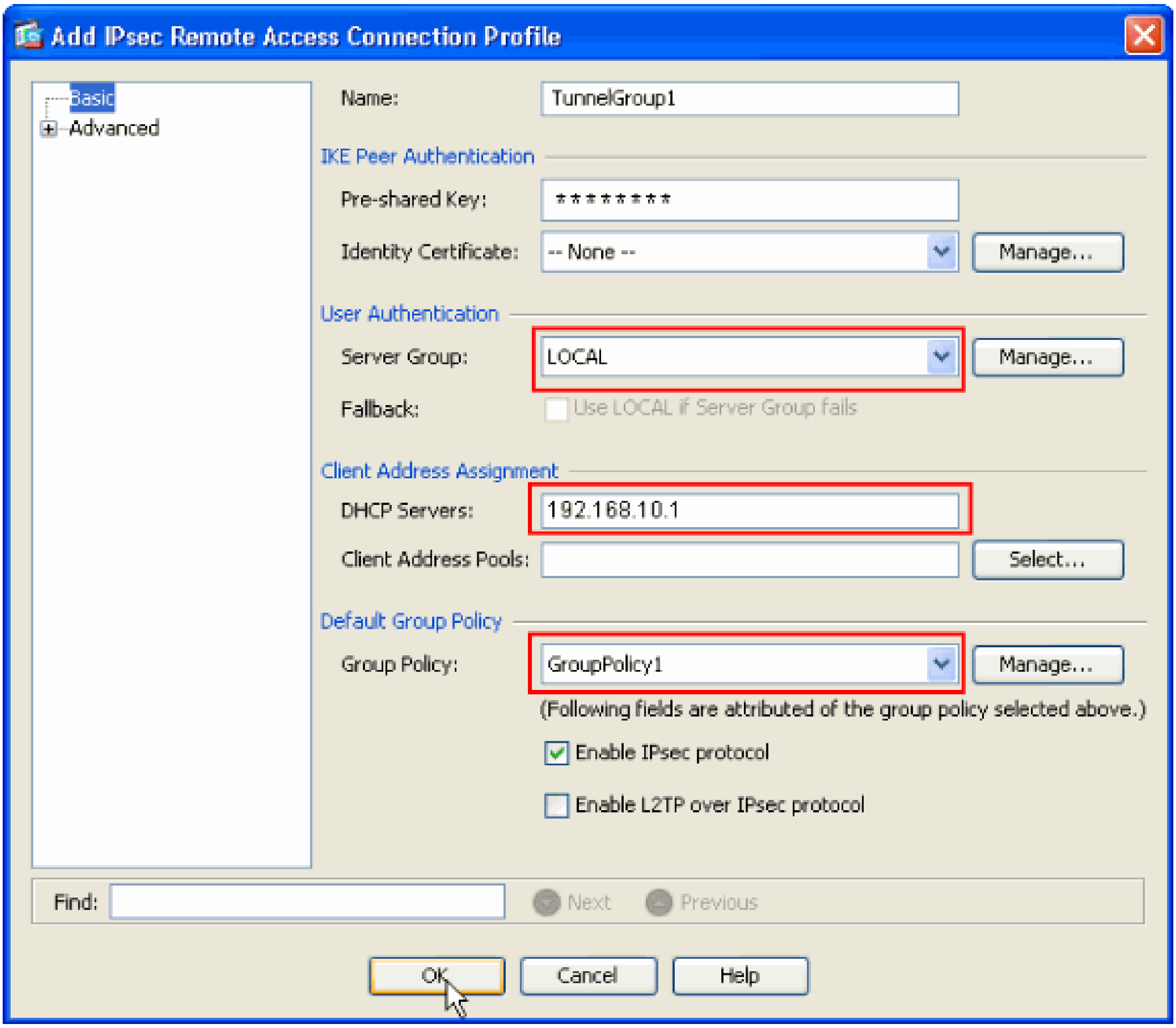
Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Name	IPsec Enabled	L2TP/IPsec Enabled	Autentication
DefaultWEBVPNGroup	☑	☑	LOCAL
DefaultRAGroup	☑	☑	LOCAL

Basic(**기본**) 탭 아래에서 User Authentication(사용자 인증) 필드에 대해 LOCAL(로컬)로 서버 그룹을 선택합니다.Default **Group** Policy(기본 그룹 정책) 필드에 대한 Group Policy(그룹 정책)를 선택합니다.DHCP 서버에 제공된 공간에 DHCP 서버 IP 주소를 **제공합니다**

.



Add IPsec Remote Access Connection Profile

- Basic
- Advanced

Name: TunnelGroup1

IKE Peer Authentication

Pre-shared Key: ********

Identity Certificate: -- None --

User Authentication

Server Group: LOCAL

Fallback: □ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers: 192.168.10.1

Client Address Pools:

Default Group Policy

Group Policy: GroupPolicy1

(Following fields are attributed of the group policy selected above.)

☑ Enable IPsec protocol

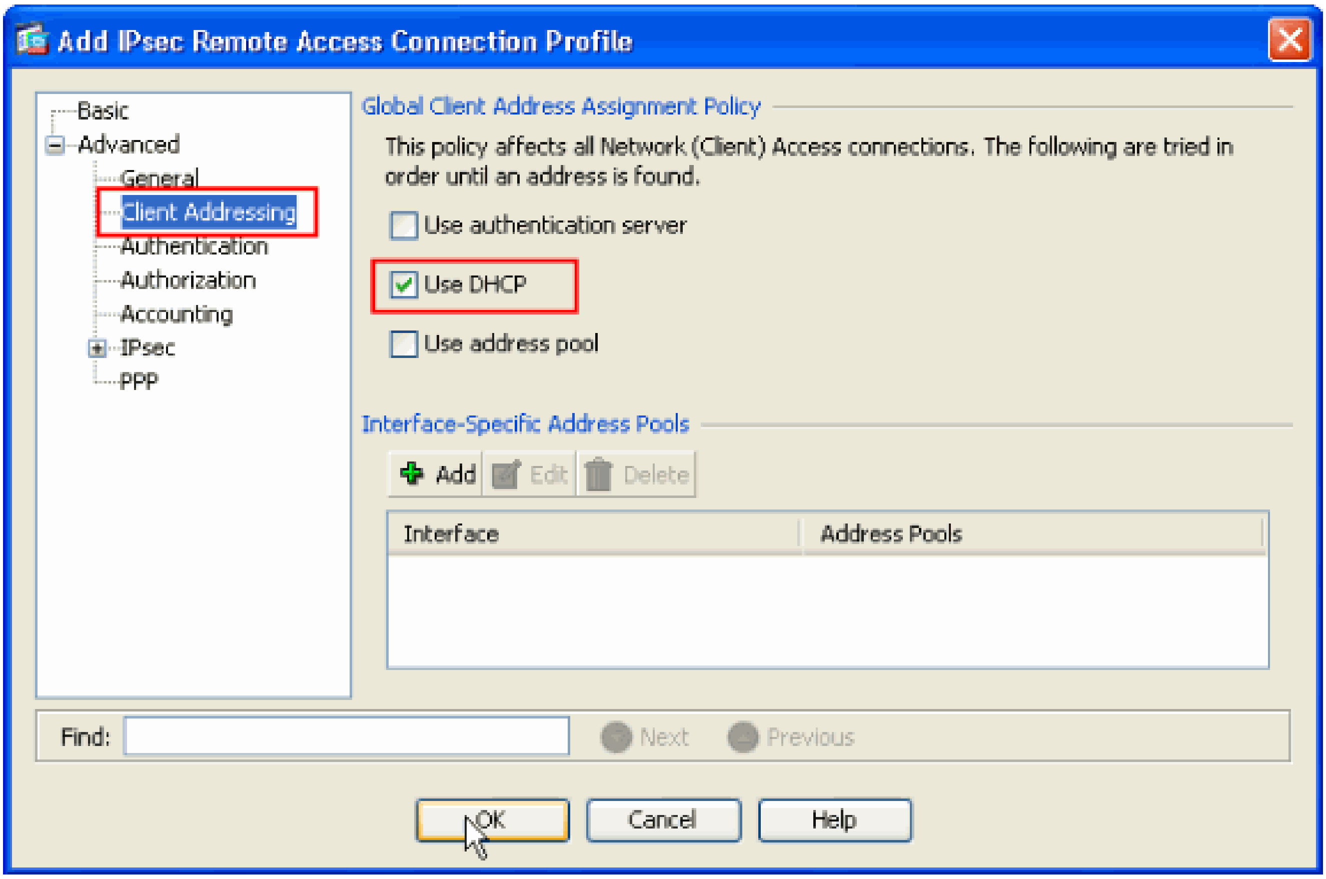
□ Enable L2TP over IPsec protocol

Find:

확인을 클릭합니다.

8. Advanced(**고급) > Client Addressing(클라이언트 주소 지정) >**을 선택하고 **Use DHCP** for the DHCP server to assign IP Address to assign VPN Client(DHCP 서버**에 DHCP 사용**) 확인란을 선택합니다.**참고: Use authentication server** and **Use address pool(인증 서버 사용** 및 **주소 풀 사용)** 확인란**의 선택을 취소해야 합니다**

.



This policy affects all Network (Client) Access connections. The following are tried in order until an address is found.

☐ Use authentication server

☑ Use DHCP

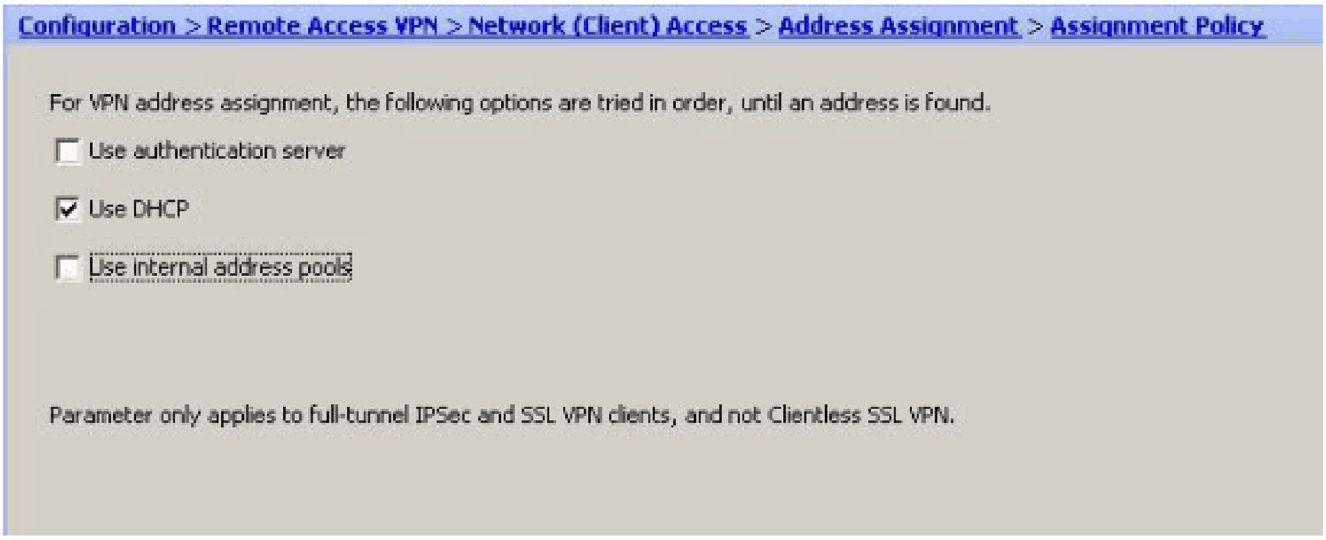
☐ Use address pool

ASDM 6.x 구성

ASDM 경로 측면에서 일부 사소한 수정 사항을 제외하고 ASDM 버전 6.x에서는 동일한 ASDM 컨피그레이션이 잘 작동합니다.특정 필드에 대한 ASDM 경로의 ASDM 버전 6.2 이상과 차이가 있습니다.기존 경로와 함께 수정된 내용은 아래에 나와 있습니다.여기서는 모든 주요 ASDM 버전에 대해 그래픽 이미지가 동일하게 유지되는 경우에는 그래픽 이미지가 첨부되지 않습니다.

1. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > IKE Policies(IKE 정책) > Add(추가)
2. 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)
3. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > Crypto Maps(암호화 맵) > Add(추가)
4. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) > Add(추가) > Internal Group Policies(내부 그룹 정책)를 선택합니다.
5. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) > Add(추가) > Internal Group Policies(내부 그룹 정책) > Servers(서버)를 선택합니다.
6. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > AAA Setup/Local Users(AAA 설정/로컬 사용자) > Local Users(로컬 사용자) > Add(추가)를 선택합니다.
7. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > IPSec Connection Profiles(IPSec 연결 프로파일) > Add(추가)
8. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Assignment Policy(할당 정책)를 선택합니다

.



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy

For VPN address assignment, the following options are tried in order, until an address is found.

☐ Use authentication server

☑ Use DHCP

☐ Use internal address pools

Parameter only applies to full-tunnel IPSec and SSL VPN clients, and not Clientless SSL VPN.

이 세 가지 옵션은 기본적으로 활성화되어 있습니다.Cisco ASA는 VPN 클라이언트에 주소를 할당하기 위해 동일한 순서를 따릅니다.다른 두 옵션의 선택을 취소하면 Cisco ASA는 aaa 서버 및 로컬 풀 옵션을 확인하지 않습니다.기본적으로 활성화된 옵션은 show run all을 사용하여 **확인할** 수 있습니다. **vpn-add** 명령**에서|**.다음은 참조의 샘플 출력입니다.

```
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 0
```

이 명령에 대한 자세한 내용은 vpn-addr-assign을 참조하십시오.

CLI를 사용하여 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 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
```

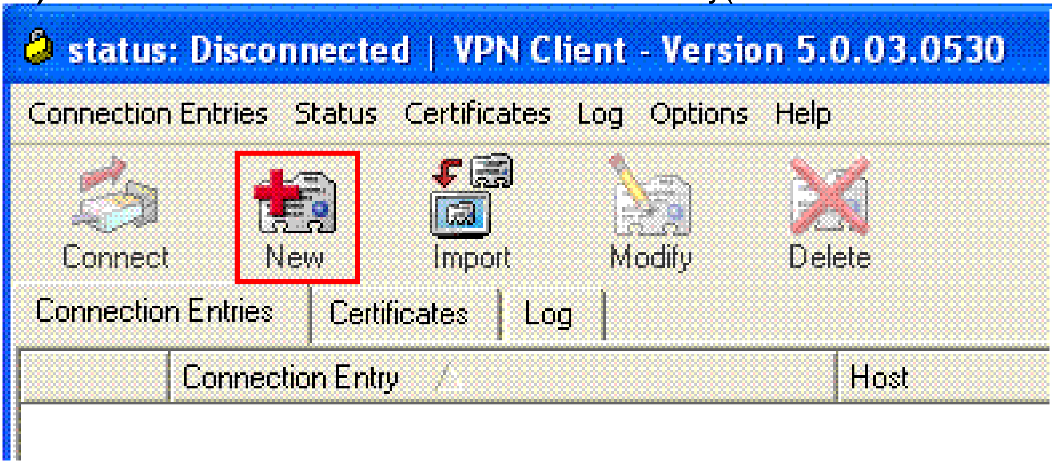
```
outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 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 DHCP Server and now by AAA or the Local
pool.The CLI vpn-addr-assign dhcp for VPN address
assignment through DHCP Server is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign local

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 GroupPolicy1 internal
```

```
group-policy GroupPolicy1 attributes

!--- define the DHCP network scope in the group
policy.This configuration is Optional dhcp-network-scope
192.168.5.0

!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. username cisco123
password ffIRPGpDSOJh9YLq encrypted

!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access !--- Define the DHCP server address to the
tunnel group. tunnel-group TunnelGroup1 general-
attributes default-group-policy GroupPolicy1 dhcp-server
192.168.10.1

!--- 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#
```

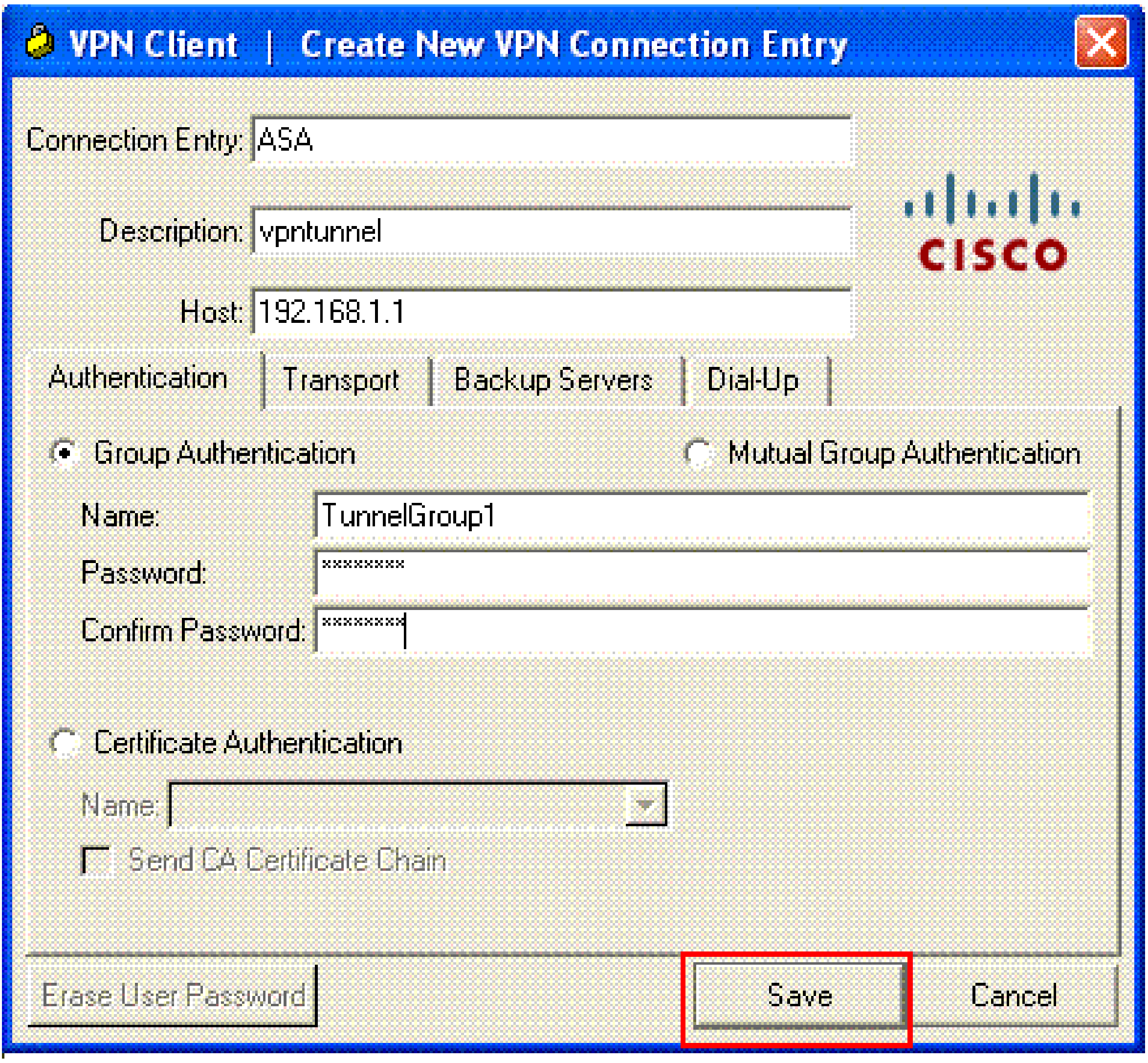
Cisco VPN 클라이언트 컨피그레이션

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) 창을 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**



VPN Client | Create New VPN Connection Entry

Connection Entry: ASA

Description: vpntunnel

Host: 192.168.1.1

● Group Authentication ○ Mutual Group Authentication

Name: TunnelGroup1

Password: ********

Confirm Password: ********

○ Certificate Authentication

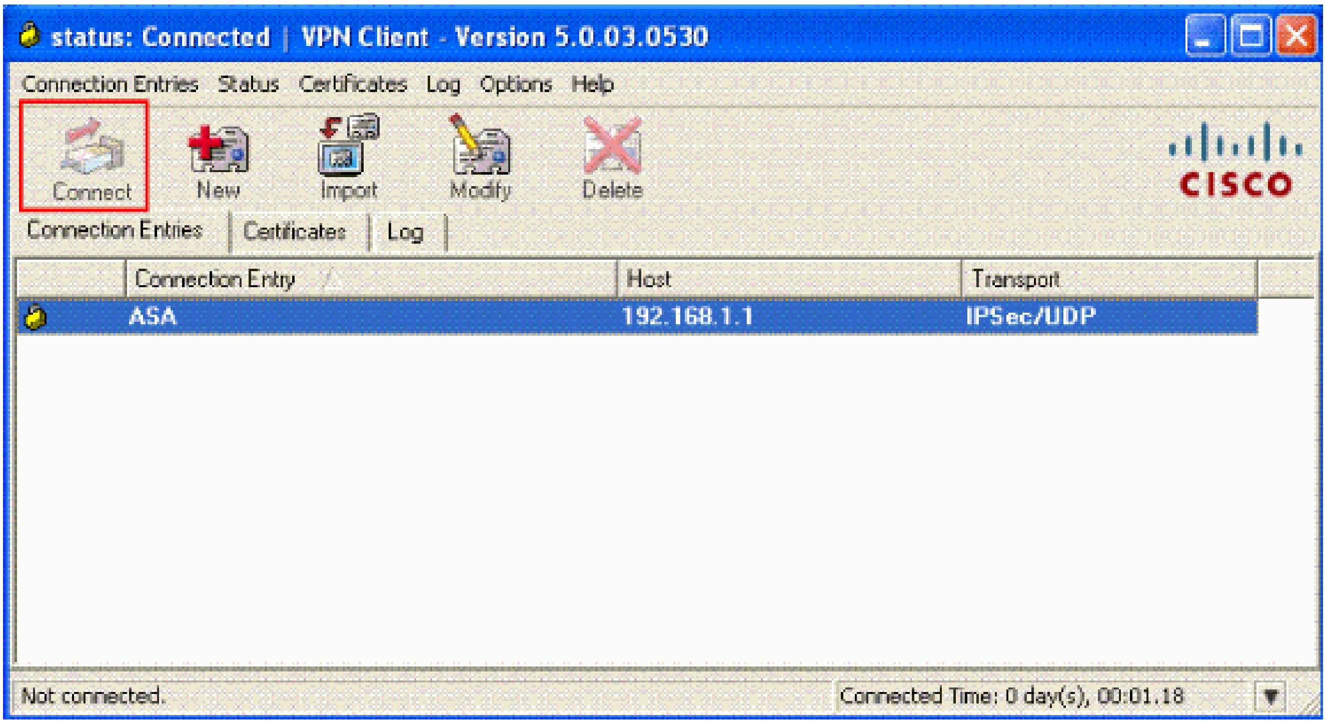
Name:

□ Send CA Certificate Chain

.

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

.

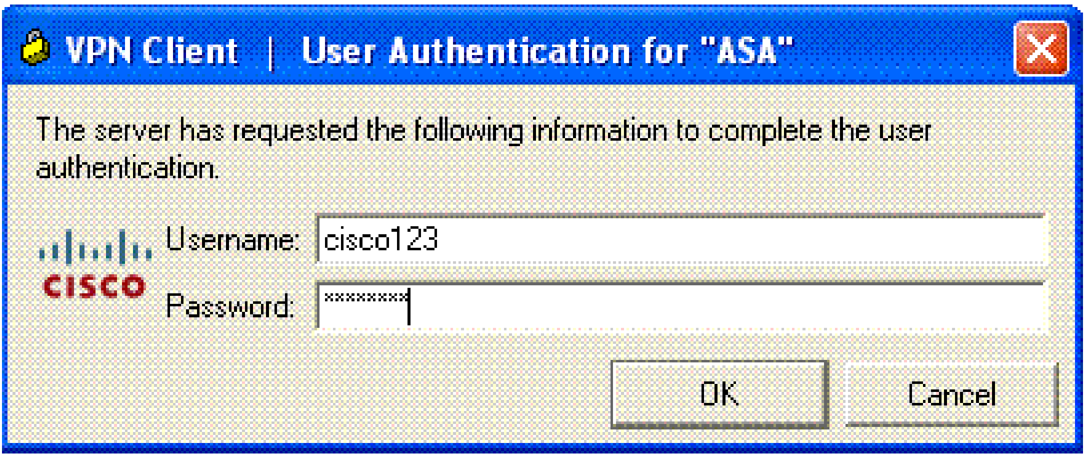


status: Connected | VPN Client - Version 5.0.03.0530

	Connection Entry	Host	Transport
	ASA	192.168.1.1	IPSec/UDP

Not connected. Connected Time: 0 day(s), 00:01.18

5. 프롬프트가 표시되면 사용자 이름**을 입력합니다.**cisco123 및 **비밀번호:**cisco123은 위의 ASA에서 xauth에 대해 구성된 대로 구성한 다음 **OK**(확인)를 클릭하여 원격 네트워크에 연결



VPN Client | User Authentication for "ASA"

The server has requested the following information to complete the user authentication.

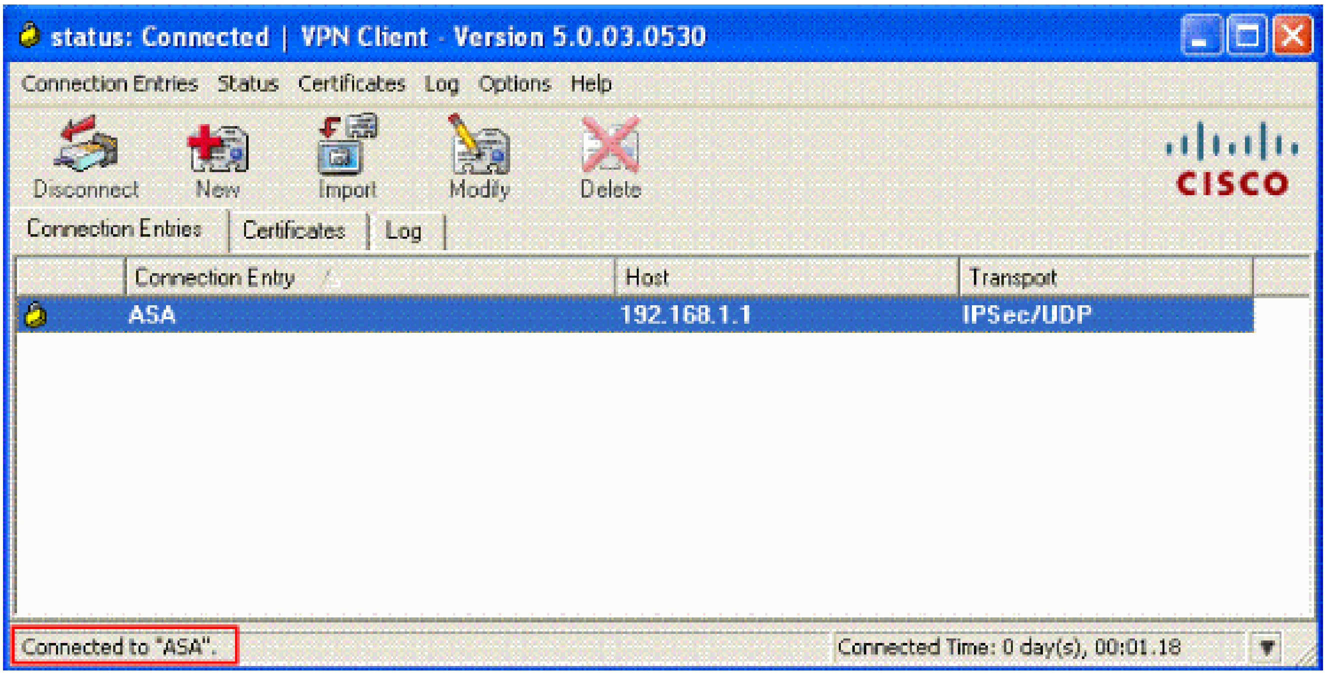
Username: cisco123

Password: ********

합니다.

6. VPN 클라이언트는 중앙 사이트의 ASA에 연결됩니다

.



status: Connected | VPN Client - Version 5.0.03.0530

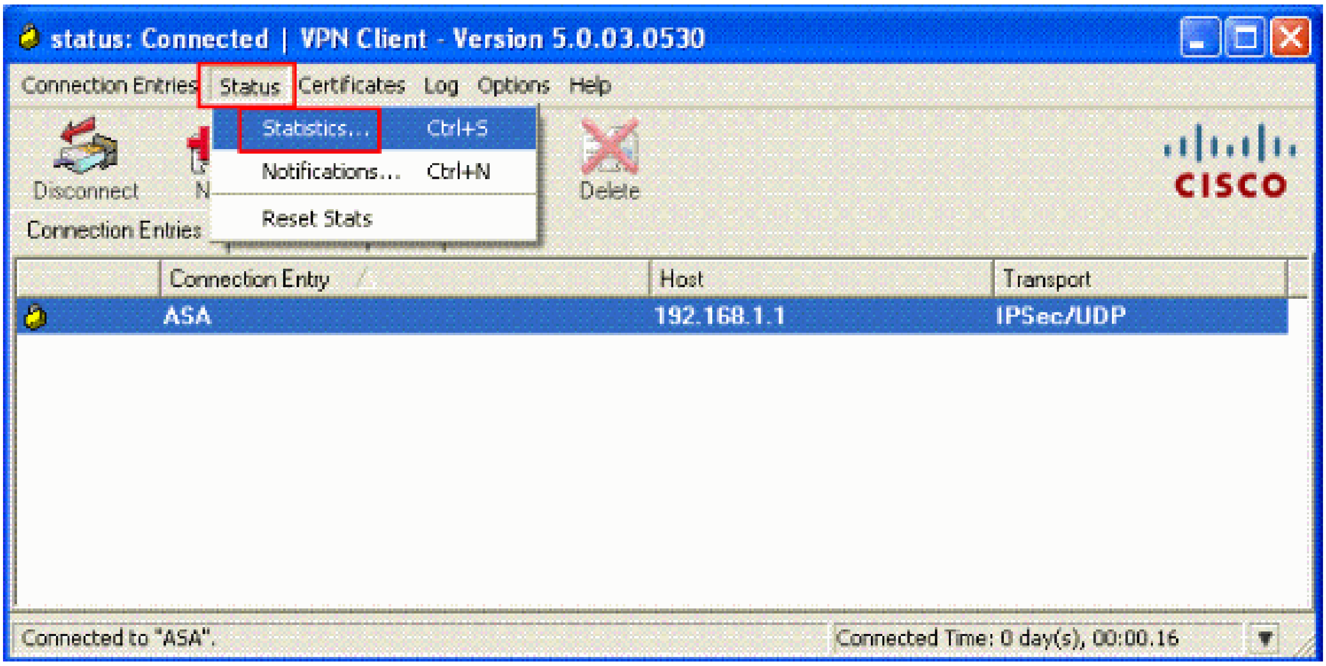
Connection Entry	Host	Transport
ASA	192.168.1.1	IPSec/UDP

Connected to "ASA".

Connected Time: 0 day(s), 00:01.18

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

.



status: Connected | VPN Client - Version 5.0.03.0530

Connection Entry	Host	Transport
ASA	192.168.1.1	IPSec/UDP

Connected to "ASA".

Connected Time: 0 day(s), 00:00.16

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.

```
ASA #show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 10, 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: 192.168.1.2, username: cisco123
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
      #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 192.168.1.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C2C25E2B

    inbound esp sas:
      spi: 0x69F8C639 (1777911353)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xC2C25E2B (3267517995)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y

ASA #show 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: 192.168.1.2
```

```
    Type     : user               Role     : responder
    Rekey    : no                 State    : AM_ACTIVE
```

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.

샘플 디버그 출력

- ASA 8.0
- Windows용 VPN Client 5.0

ASA 8.0

```
ASA#debug crypto isakmp 7
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
 (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 856
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta
tion capability flags:  Main Mode:        True  Aggressive Mode:  False
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V
ID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun
nelGroup1
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g IKE SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr
oposal # 1, Transform # 13 acceptable  Matches global IKE entry # 2
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ISAKMP SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin
g keys for Responder...
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
 hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Cisco Unity VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing xauth V6 VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing dpd vid payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Fragmentation VID + extended capabilities payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti
ga/Cisco VPN3000/Cisco ASA GW VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 368
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE
 (0) total length : 116
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
 hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g notify payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408)
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received
Cisco Unity client VID
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing blank hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing qm hash payload
```

```
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a
1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8
a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a
ttr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g MODE_CFG Reply attributes.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: IP Compression = disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, User (cisco123) authenticated.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143
60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14
360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg ACK attributes
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26
63a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg Request attributes
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 net mask!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DNS server address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for WINS server address!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unsupported transaction mode attribute: 5
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Banner!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Save PW setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Default Domain Name!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split Tunnel List!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split DNS!
```

```
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for PFS setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unknown transaction mode attribute: 28684
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Application Version!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Client Type: WinNT  Client Application Version: 5.0.03.0530
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for FWTYPE!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12
3!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for UDP Port!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e
nabled)
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Assigned private IP address 192.168.5.1 to remote user
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Send Client Browser Proxy Attributes!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu
ded in the mode-cfg reply
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266
3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, PHASE 1 COMPLETED
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection:
DPD
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P1 rekey timer: 950 seconds.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, sending notify message
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44
35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
 NONE (0) total length : 1022
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing ID payload
```

```
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received remote Proxy Host data in ID Payload:  Address 192.168.5.1, Proto
col 0, Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0, Mask
 0.0.0.0, Protocol 0, Port 0
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, QM IsRekeyed old sa not found by addr
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, IKE Remote Peer configured for crypto map: dynmap
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing IPSec SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IPSec SA Proposal # 14, Transform # 1 acceptable  Matches global IPS
ec SA entry # 10
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, IKE: requesting SPI!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, oakley constucting quick mode
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec SA payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon
ds
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing proxy ID
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Transmitting Proxy Id:
  Remote host: 192.168.5.1  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541
f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 176
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, loading all IPSEC SAs
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Security negotiation complete for User (cisco123)  Responder, Inbound SPI
= 0x31de01d8, Outbound SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P2 rekey timer: 27360 seconds.
```

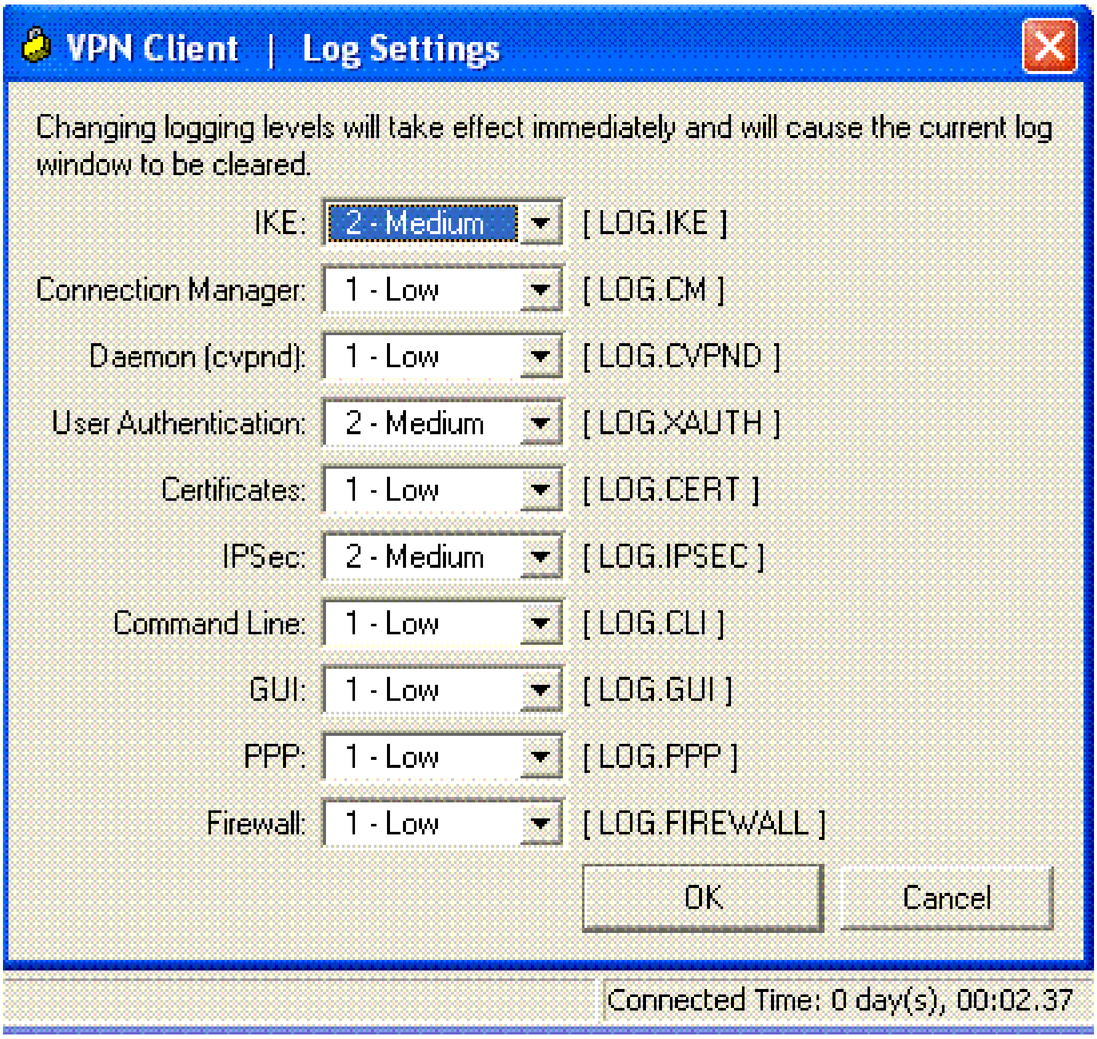
```
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Adding static route for client address: 192.168.5.1
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, PHASE 2 COMPLETED (msgid=541f8e43)
Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78
f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8
0
```

```
ASA#debug crypto ipsec 7
```

```
!--- Deletes the old SAs. ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID:
0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted
inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context,
SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule
ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC:
Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 !--- Creates new SAs. ASA#
IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI :
0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime
: 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound
SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp
Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating
outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU :
1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC:
Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound
encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore
Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt
rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src
addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src
ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI
0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating
inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0
bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed
inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context
0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes
VCID : 0x00000000 Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed
outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner
rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI
0xC921E280 Rule ID: 0xD5123250 IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr:
192.168.5.1 Src mask: 255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0
Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false
SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule
ID: 0xD556AF60 IPSEC: New inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask:
255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op :
ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A
Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC:
New inbound permit rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst
addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports
Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0
```

Windows용 VPN Client 5.0

Log > **Log settings(로그 설정)**를 선택하여 VPN 클라이언트에서 로그 레벨을 활성화합니다.

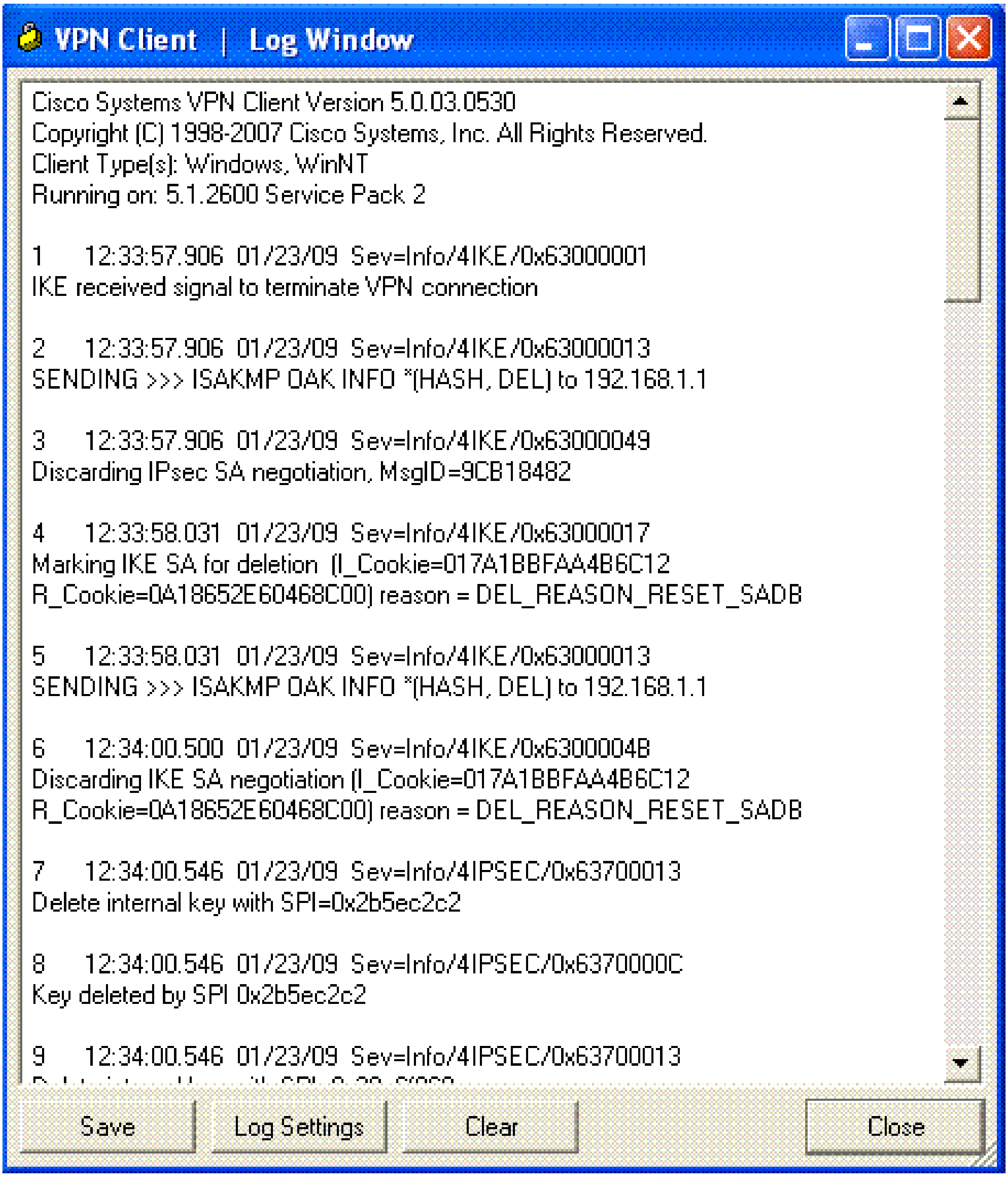


Changing logging levels will take effect immediately and will cause the current log window to be cleared.

IKE:	2 - Medium	[LOG.IKE]
Connection Manager:	1 - Low	[LOG.CM]
Daemon (cvpnd):	1 - Low	[LOG.CVPND]
User Authentication:	2 - Medium	[LOG.XAUTH]
Certificates:	1 - Low	[LOG.CERT]
IPSec:	2 - Medium	[LOG.IPSEC]
Command Line:	1 - Low	[LOG.CLI]
GUI:	1 - Low	[LOG.GUI]
PPP:	1 - Low	[LOG.PPP]
Firewall:	1 - Low	[LOG.FIREWALL]

Connected Time: 0 day(s), 00:02.37

Log **> Log Window**를 선택하여 VPN 클라이언트의 로그 항목을 봅니다.



```
Cisco Systems VPN Client Version 5.0.03.0530
Copyright (C) 1998-2007 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000001
IKE received signal to terminate VPN connection

2      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1

3      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000049
Discarding IPsec SA negotiation, MsgID=9CB18482

4      12:33:58.031  01/23/09  Sev=Info/4IKE/0x63000017
Marking IKE SA for deletion  (I_Cookie=017A1BBFAA4B6C12
R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB

5      12:33:58.031  01/23/09  Sev=Info/4IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1

6      12:34:00.500  01/23/09  Sev=Info/4IKE/0x6300004B
Discarding IKE SA negotiation (I_Cookie=017A1BBFAA4B6C12
R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB

7      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2b5ec2c2

8      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2b5ec2c2

9      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x63700013
```

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