WLC 컨피그레이션이 포함된 무선 LAN을 통한 클라이언트 VPN 예

목차

소개

이 문서에서는 무선 환경에서 VPN(Virtual Private Network)의 개념을 소개합니다.이 문서에서는 WLC(Wireless LAN Controller)를 통해 무선 클라이언트와 VPN 서버 간에 VPN 터널을 구축하는 것과 관련된 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC에 대한 지식 및 WLC 기본 매개변수를 구성하는 방법
- WPA(Wi-Fi Protected Access) 개념에 대한 지식
- VPN 및 해당 유형에 대한 기본 지식
- IPsec 지식
- 사용 가능한 암호화, 인증 및 해싱 알고리즘에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 4.0.179.8을 실행하는 Cisco 2006 WLC
- Cisco 1000 Series LAP(Lightweight Access Point)
- Cisco IOS® Software 릴리스 12.4(8)를 실행하는 Cisco 3640
- Cisco VPN Client 버전 4.8

참고: 이 문서에서는 3640 라우터를 VPN 서버로 사용합니다.고급 보안 기능을 지원하기 위해 전용 VPN 서버를 사용할 수도 있습니다.

참고: 라우터가 VPN 서버로 작동하려면 기본 IPsec을 지원하는 기능 집합을 실행해야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

배경 정보

VPN은 인터넷과 같은 공용 통신 인프라를 통해 사설 네트워크 내에서 데이터를 안전하게 전송하는 데 사용되는 사설 데이터 네트워크입니다.이 VPN은 터널링 프로토콜 및 보안 절차를 사용하여 데이터 프라이버시를 유지합니다.

원격 액세스 VPN

원격 액세스 VPN 컨피그레이션은 모바일 사용자와 같은 VPN 소프트웨어 클라이언트가 VPN 서버 뒤에 있는 중앙 집중식 네트워크 리소스에 안전하게 액세스할 수 있도록 하는 데 사용됩니다.Cisco 터미널에서 이러한 VPN 서버 및 클라이언트는 Cisco Easy VPN 서버 및 Cisco Easy VPN Remote 디바이스라고도 합니다.

Cisco Easy VPN Remote 장치는 Cisco IOS 라우터, Cisco PIX Security Appliances, Cisco VPN 3002 하드웨어 클라이언트 및 Cisco VPN 클라이언트일 수 있습니다.Cisco Easy VPN Server에서 VPN 터널 연결 시 보안 정책을 수신하는 데 사용됩니다.이렇게 하면 원격 위치의 구성 요구 사항이 최소화됩니다.Cisco VPN Client는 PC, 랩톱 등에 설치할 수 있는 소프트웨어 클라이언트입니다.

Cisco Easy VPN Server는 Cisco IOS 라우터, Cisco PIX Security Appliances 및 Cisco VPN 3000 Concentrator일 수 있습니다.

이 문서에서는 랩톱에서 실행되는 Cisco VPN 클라이언트 소프트웨어를 VPN 클라이언트로 사용하고 Cisco 3640 IOS 라우터를 VPN 서버로 사용합니다.이 문서에서는 IPsec 표준을 사용하여 클라이언트와 서버 간에 VPN 터널을 설정합니다.

IPsec

IPsec은 IETF(Internet Engineering Task Force)에서 개발한 개방형 표준의 프레임워크입니다

.IPsec은 인터넷과 같이 보호되지 않는 네트워크를 통해 민감한 정보를 전송하는 보안을 제공합니다.

IPsec은 IP 패킷 레벨에서 네트워크 데이터 암호화를 제공하며 표준 기반의 강력한 보안 솔루션을 제공합니다.IPsec의 주요 작업은 안전하지 않은 연결을 통해 개인 정보를 교환하도록 허용하는 것입니다.IPsec은 암호화를 사용하여 정보를 가로채기나 도청으로부터 보호합니다.그러나 암호화를 효율적으로 사용하려면 양 당사자 모두 정보의 암호화 및 암호 해독에 사용되는 암호를 공유해야 합니다.

IPsec은 두 단계로 작동하여 공유 비밀의 기밀 교환을 허용합니다.

- 1단계 - 두 IPsec 피어 간에 보안 채널을 설정하는 데 필요한 보안 매개변수의 협상을 처리합니다.1단계는 일반적으로 IKE(Internet Key Exchange) 프로토콜을 통해 구현됩니다.원격 IPsec 피어가 IKE를 수행할 수 없는 경우 사전 공유 키가 있는 수동 컨피그레이션을 사용하여 1단계를 완료할 수 있습니다.
- 2단계 - 1단계에서 설정된 보안 터널을 사용하여 사용자 데이터를 실제로 전송하는 데 필요한 보안 매개변수를 교환합니다.IPsec의 두 단계에서 사용되는 보안 터널은 각 IPsec 엔드포인트에서 사용되는 SA(보안 연결)를 기반으로 합니다.SA는 두 엔드포인트가 모두 사용하는 데 동의하는 인증 및 암호화 유형과 같은 보안 매개변수를 설명합니다.

2단계에서 교환되는 보안 매개변수는 IPsec 터널을 생성하는 데 사용되며, 이는 VPN 클라이언트와 서버 간의 데이터 전송에 사용됩니다.

IPsec 및 해당 컨피그레이션에 대한 자세한 내용은 IPsec 구성을 참조하십시오.

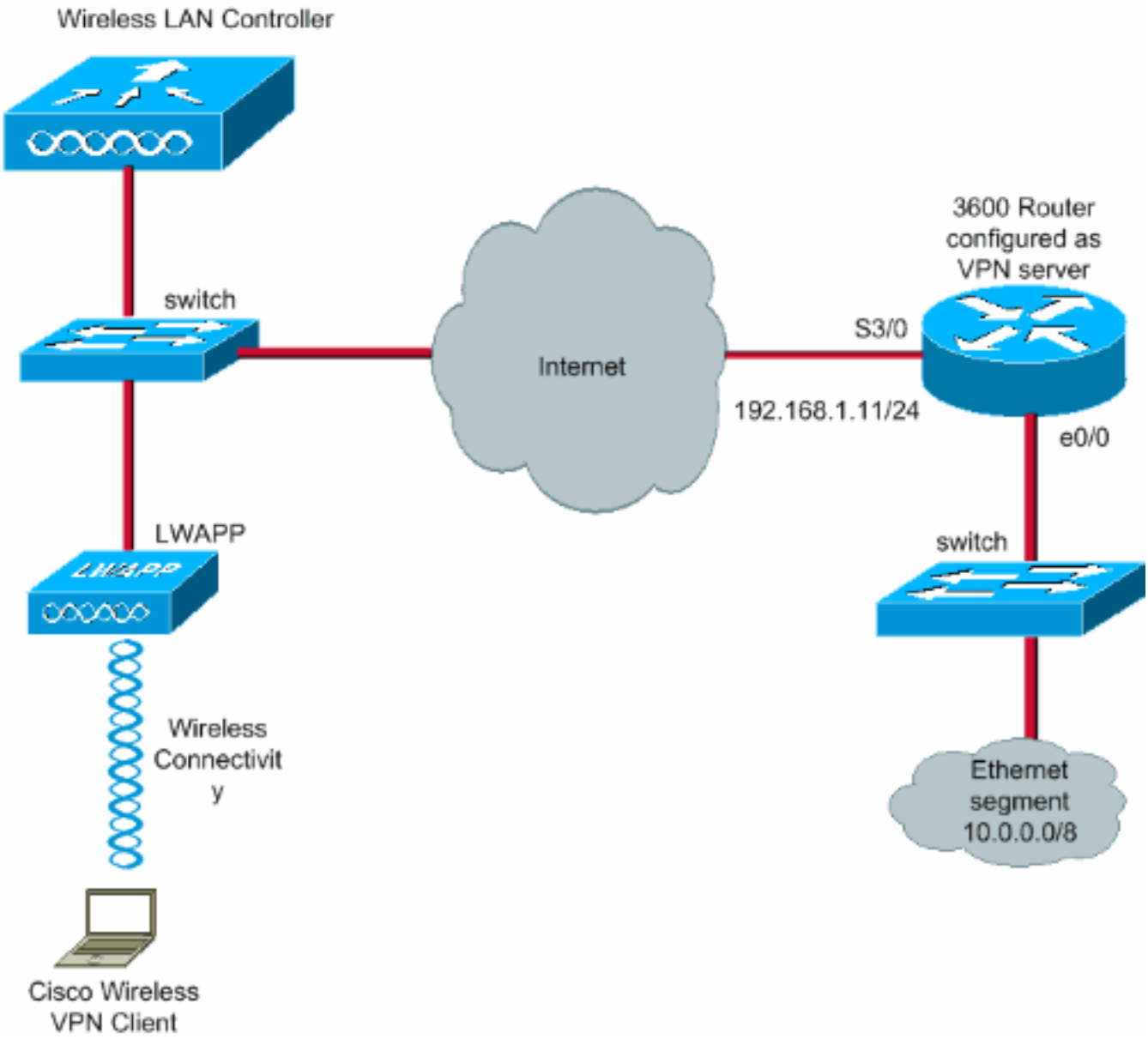
VPN 클라이언트와 서버 간에 VPN 터널이 설정되면 *VPN 서버에 정의된 보안 정책이 클라이언트로 전송됩니다*.이렇게 하면 클라이언트 측의 구성 요구 사항이 최소화됩니다.

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

네트워크 다이어그램

이 문서에서는 다음 구성을 사용합니다.

- WLC의 관리 인터페이스 IP 주소—172.16.1.10/16
- WLC의 AP-manager 인터페이스 IP 주소—172.16.1.11/16
- 기본 게이트웨이—172.16.1.20/16**참고:** 라이브 네트워크에서 이 기본 게이트웨이는 WLC를 네트워크의 나머지 부분 및/또는 인터넷에 연결하는 즉시 라우터의 수신 인터페이스를 가리켜야 합니다.
- VPN 서버의 IP 주소 s3/0—192.168.1.11/24**참고:** 이 IP 주소는 VPN 서버 측에서 VPN 터널을 종료하는 인터페이스를 가리켜야 합니다.이 예에서 s3/0은 VPN 서버에서 VPN 터널을 종료하는 인터페이스입니다.
- VPN 서버의 LAN 세그먼트는 IP 주소 범위 10.0.0.0/8을 사용합니다.



구성

WLAN 중앙 집중식 아키텍처에서 랩톱과 같은 무선 VPN 클라이언트가 VPN 서버로 VPN 터널을 설정할 수 있도록 하려면 클라이언트가 LDAP(Lightweight Access Point)에 연결되고, 이를 WLC에 등록해야 합니다.이 문서에는 WLC(Wireless LAN Controller)에 대한 LAP(Lightweight AP) 등록에 설명된 로컬 서브넷 브로드캐스트 검색 프로세스를 사용하여 WLC에 이미 등록된 LAP가 있습니다.

다음 단계는 VPN에 대한 WLC를 구성하는 것입니다.

VPN 종료 및 통과

버전 4 이전의 Cisco 4000 Series WLC에서는 IPsec VPN 종료(IPsec 지원)라는 기능이 지원됩니다.이 기능을 사용하면 컨트롤러에서 직접 VPN 클라이언트 세션을 종료할 수 있습니다.요약하면, 이 기능을 통해 컨트롤러 자체가 VPN 서버 역할을 할 수 있습니다.그러나 이를 위해서는 컨트롤러에 별도의 VPN 종료 하드웨어 모듈을 설치해야 합니다.

이 IPsec VPN 지원은 다음에서 사용할 수 없습니다.

- Cisco 2000 Series WLC

- 버전 4.0 이상을 실행하는 모든 WLC

따라서 4.0 이후 버전에서 지원되는 유일한 VPN 기능은 VPN Pass-through입니다.이 기능은 Cisco 2000 Series WLC에서도 지원됩니다.

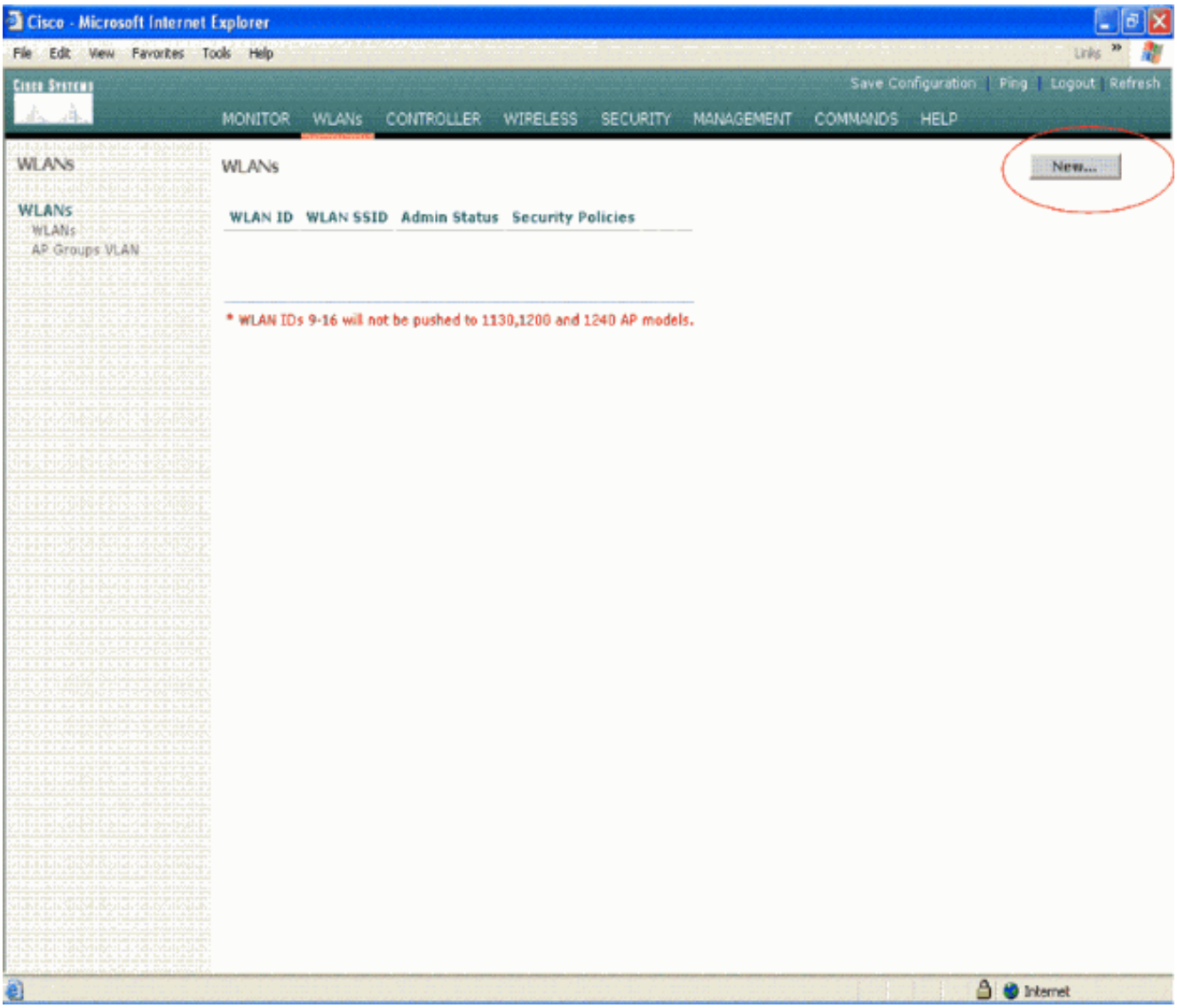
VPN Pass-through는 클라이언트가 특정 VPN 서버에서만 터널을 설정할 수 있도록 하는 기능입니다.따라서 구성된 VPN 서버 및 다른 VPN 서버 또는 인터넷에 안전하게 액세스해야 하는 경우 컨트롤러에서 VPN Pass-through가 활성화된 경우에는 이 작업을 수행할 수 없습니다.이러한 요구 사항에 따라 VPN Pass-through를 비활성화해야 합니다.그러나 적절한 ACL이 생성되어 해당 WLAN에 적용될 때 여러 VPN 게이트웨이에 연결하기 위해 WLC를 패스스루 역할을 하도록 구성할 수 있습니다.따라서 이중화를 위해 여러 VPN 게이트웨이에 연결하려는 경우 VPN 패스스루를 비활성화하고 VPN 게이트웨이에 대한 액세스를 허용하는 ACL을 생성하고 WLAN에 ACL을 적용합니다.

VPN Pass-through용 WLC 구성

VPN Pass-through를 구성하려면 다음 단계를 완료하십시오.

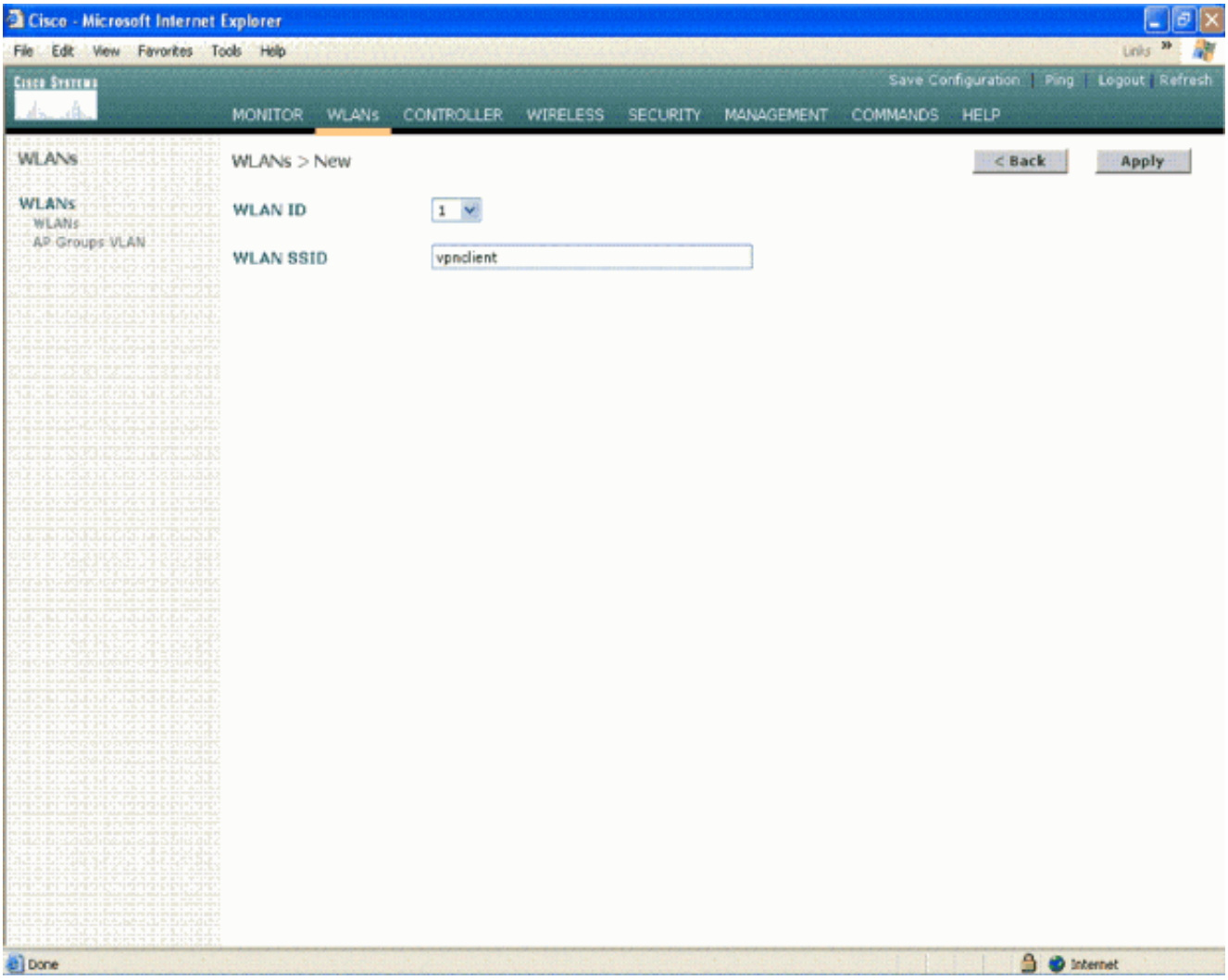
1. WLC GUI에서 **WLAN**을 클릭하여 WLANs 페이지로 이동합니다.
2. 새 WLAN을 생성하려면 **New**(새로 만들기)를 클릭합니다

.



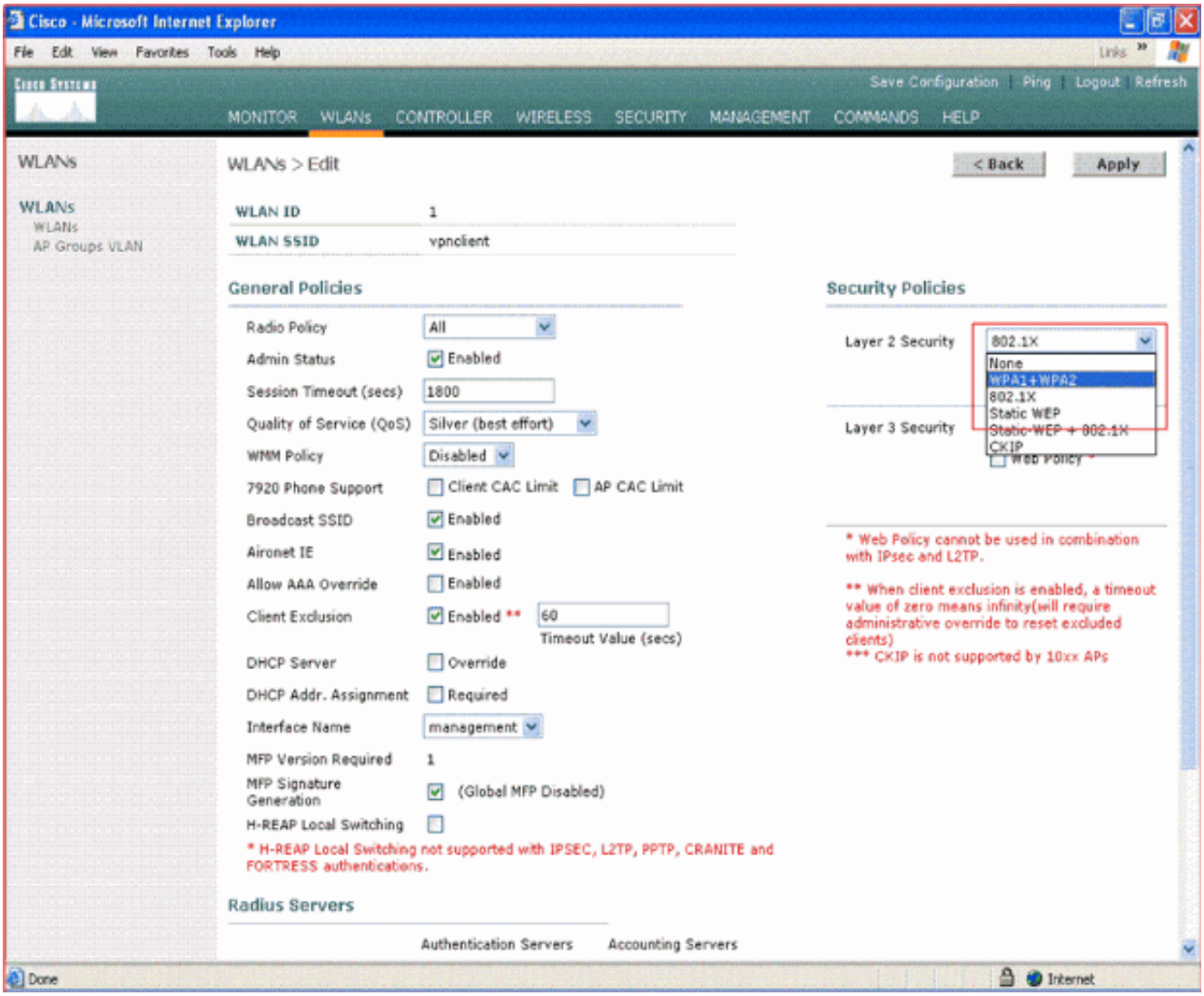
3. 이 예에서 WLAN SSID는 vpnclient**로** 명명됩니다.Apply를 **클릭합니다**

.



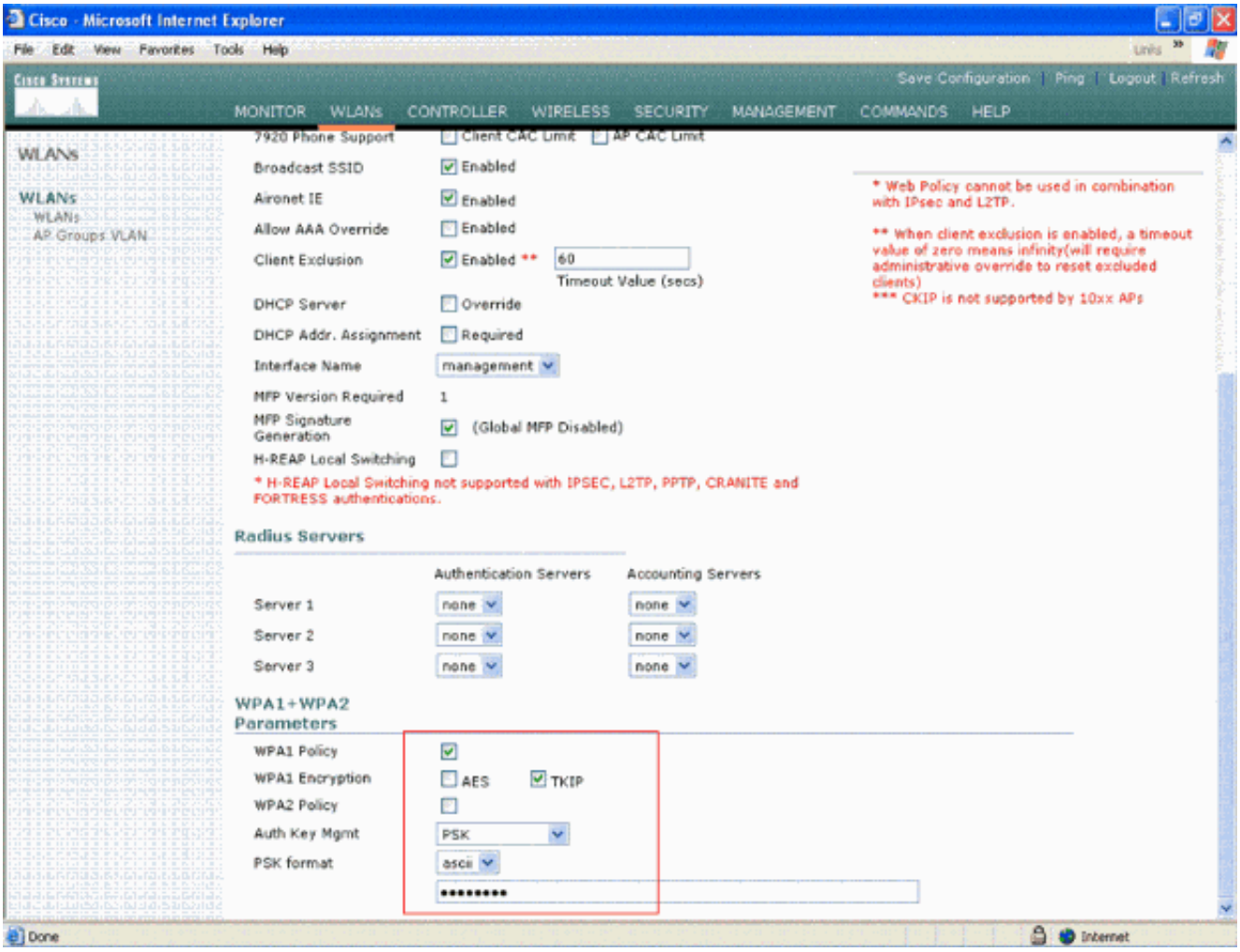
4. 레이어 2 보안을 사용하여 vpnclient SSID를 구성합니다. *이는 선택 사항입니다.*이 예에서는 **WPA1+WPA2**를 보안 유형으로 사용합니다

.



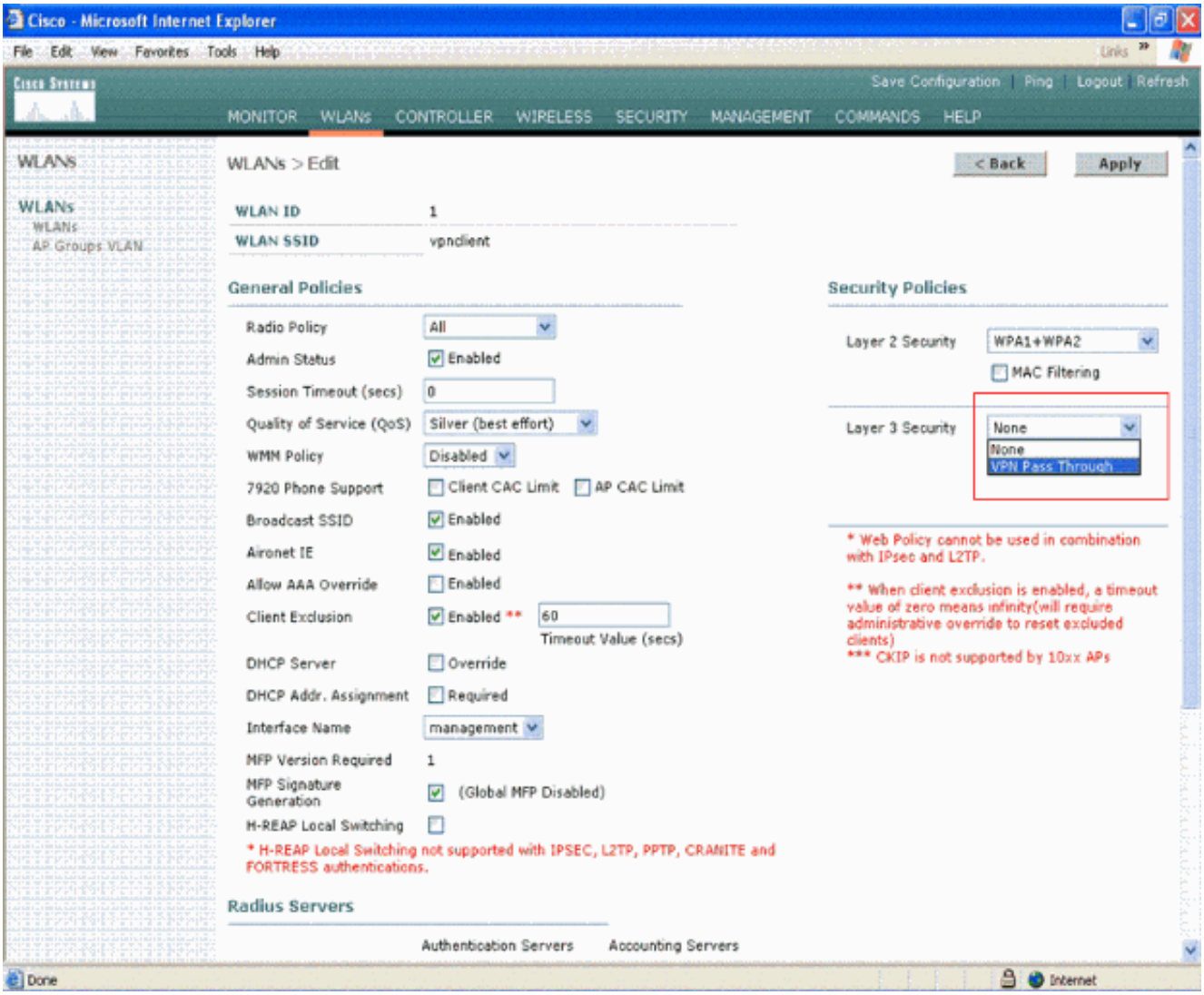
5. 사용할 WPA 정책 및 인증 키 관리 유형을 구성합니다.이 예에서는 인증 키 관리**에 PSK(Pre-Shared Key)를** 사용합니다.PSK를 선택한 후 PSK 형식으로 ASCII를 선택하고 PSK 값을 입력합니다.이 SSID에 속하는 클라이언트가 이 WLAN과 연결되려면 무선 클라이언트의 SSID 컨피그레이션에서 이 값이 동일해야 합니다

.



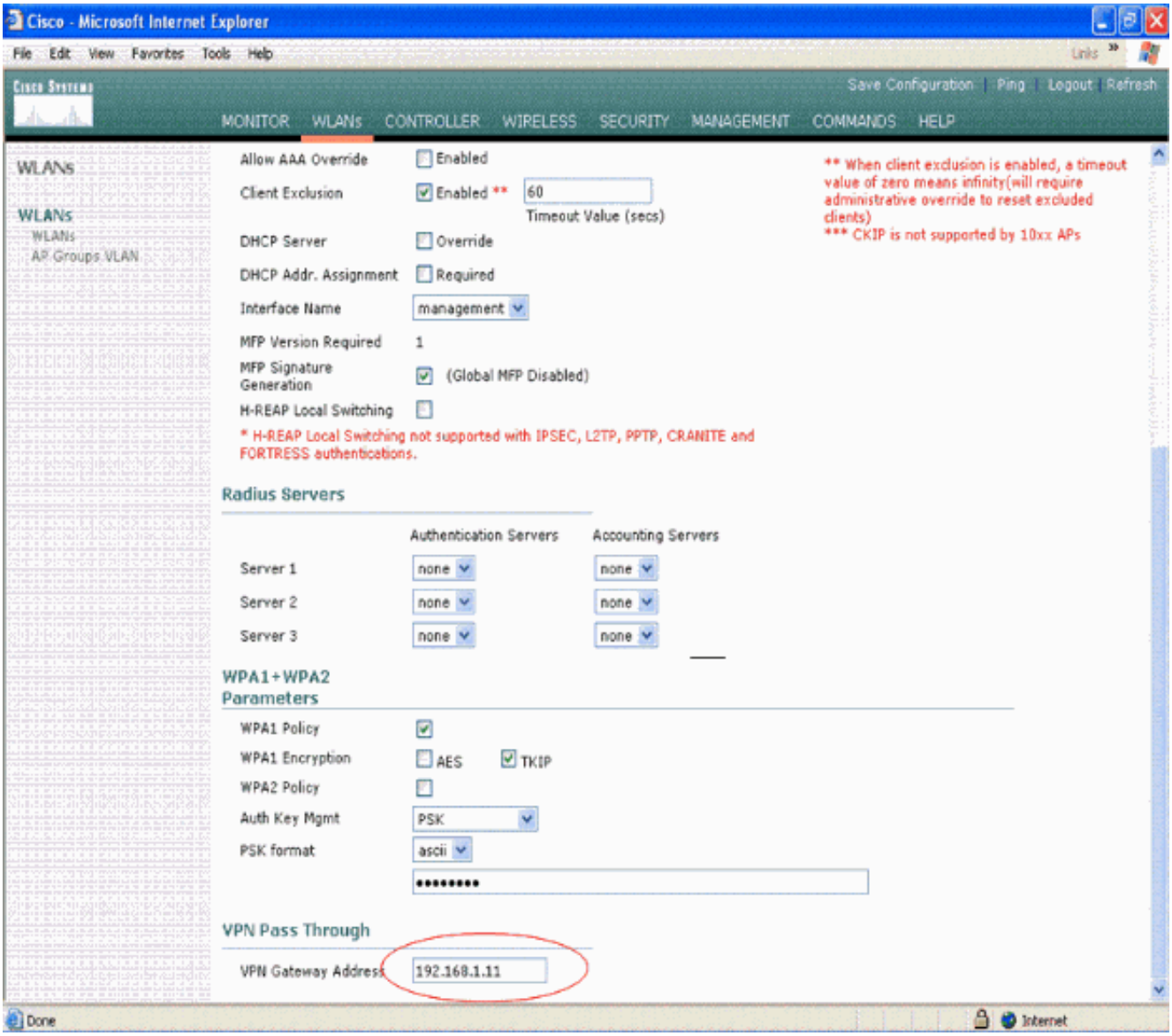
6. VPN Pass-through를 Layer 3 Security로 선택합니다.여기 예가 있습니다

.



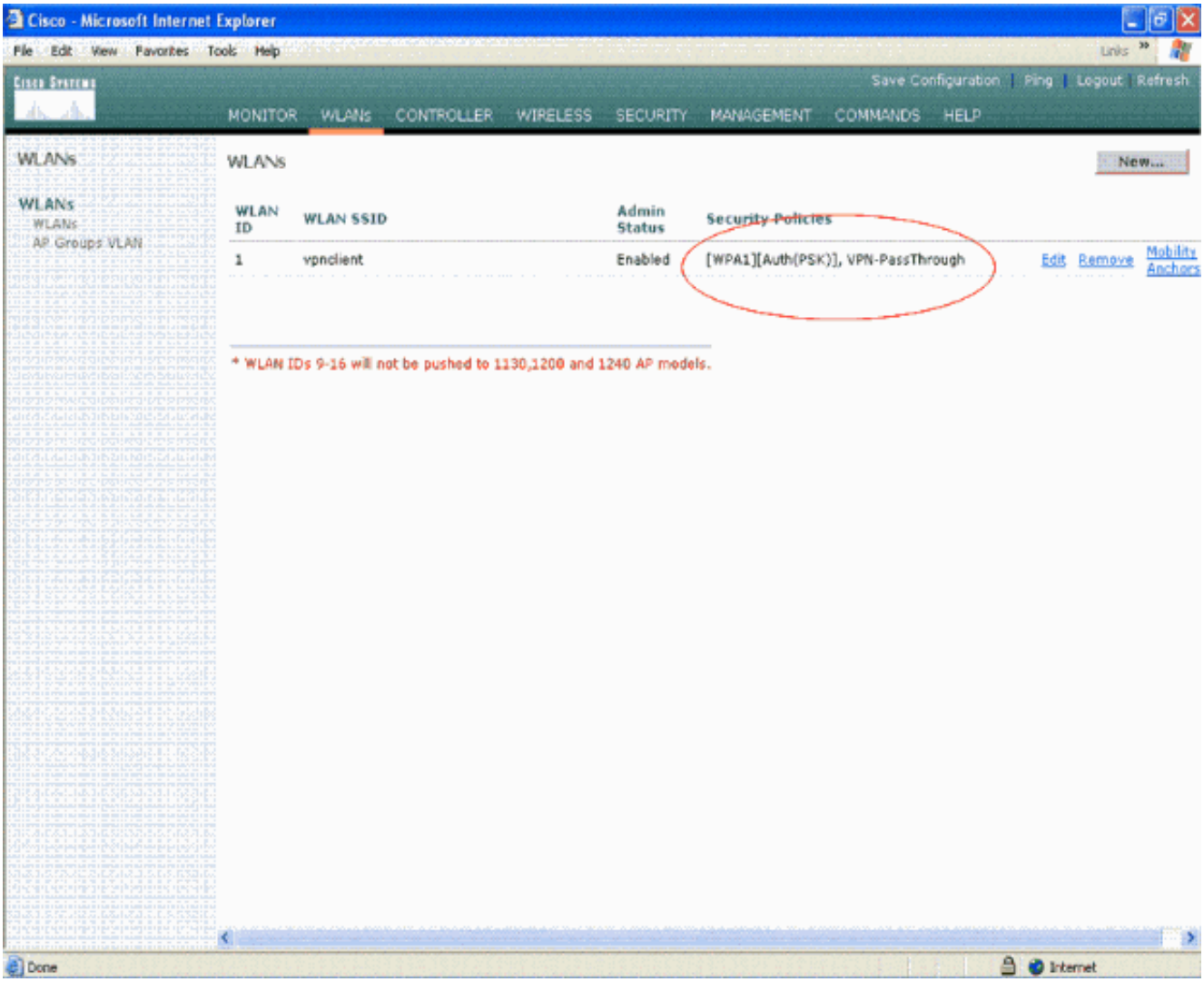
7. VPN Pass-through를 Layer 3 보안으로 선택하면 이 예와 같이 VPN 게이트웨이 주소를 추가합니다.이 게이트웨이 주소는 서버 측에서 VPN 터널을 종료하는 인터페이스의 IP 주소여야 합니다.이 예에서 VPN 서버에 있는 s3/0 인터페이스(192.168.1.11/24)의 IP 주소는 구성할 게이트웨이 주소입니다

.



8. Apply를 **클릭합니다**.vpnclient라는 WLAN이 이제 VPN Pass-through에 대해 구성됩니다

.



VPN 서버 컨피그레이션

이 컨피그레이션에서는 Cisco 3640 라우터를 VPN 서버로 표시합니다.

참고: 이 컨피그레이션에서는 간소화를 위해 고정 라우팅을 사용하여 엔드포인트 간의 IP 연결성을 유지합니다.RIP(Routing Information Protocol), OSPF(Open Shortest Path First) 등의 동적 라우팅 프로토콜을 사용하여 연결 상태를 유지할 수 있습니다.

참고: 클라이언트와 서버 간에 IP 연결이 없는 경우에는 터널이 설정되지 않습니다.

참고: 이 문서에서는 사용자가 네트워크에서 동적 라우팅을 활성화하는 방법을 알고 있다고 가정합니다.

Cisco 3640 Router

```
vpnrouter#show running-config

Building configuration...

Current configuration : 1623 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiation. hash md5
!--- Choose the hash algorithm to be md5. authentication
pre-share
!--- The authentication method selected is pre-shared.
group 2
!--- With the group command, you can declare what size
modulus to !--- use for Diffie-Hellman calculation.
Group 1 is 768 bits long, !--- and group 2 is 1024 bits
long.


crypto isakmp client configuration group employee key
cisco123 pool mypool1
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!--- Create a dynamic map and apply the transform set
that was created. !--- Set reverse-route for the VPN
server. crypto dynamic-map mymap 10 set transform-set
myset reverse-route
!
```

```
crypto map clientmap isakmp authorization list employee
!--- Create the crypto map.
crypto map clientmap client configuration address crypto
map clientmap 10 ipsec-isakmp dynamic mymap
!
!--- Apply the employee group list that was created
earlier.



!
!
!
!
interface Ethernet0/0
 ip address 10.0.0.20 255.0.0.0
 half-duplex
!
interface Serial3/0
 ip address 192.168.1.11 255.255.255.0
 clock rate 64000
 no fair-queue
 crypto map clientmap
!--- Apply the crypto map to the interface. ! interface
Serial3/1 no ip address shutdown ! interface Serial3/2
no ip address shutdown ! interface Serial3/3 no ip
address shutdown ! interface Serial3/4 no ip address
shutdown ! interface Serial3/5 no ip address shutdown !
interface Serial3/6 no ip address shutdown ! interface
Serial3/7 no ip address shutdown ip local pool mypool
10.0.0.50 10.0.0.60
!--- Configure the Dynamic Host Configuration Protocol
!--- (DHCP) pool which assigns the tunnel !--- IP
address to the wireless client. !--- This tunnel IP
address is different from the IP address !--- assigned
locally at the wireless client (either statically or
dynamically). ip http server no ip http secure-server !
ip route 172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! !
control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 ! ! end ip subnet-zero . . . ! end
```

참고: 이 예에서는 그룹 인증만 사용합니다.개별 사용자 인증을 사용하지 않습니다.

VPN 클라이언트 컨피그레이션

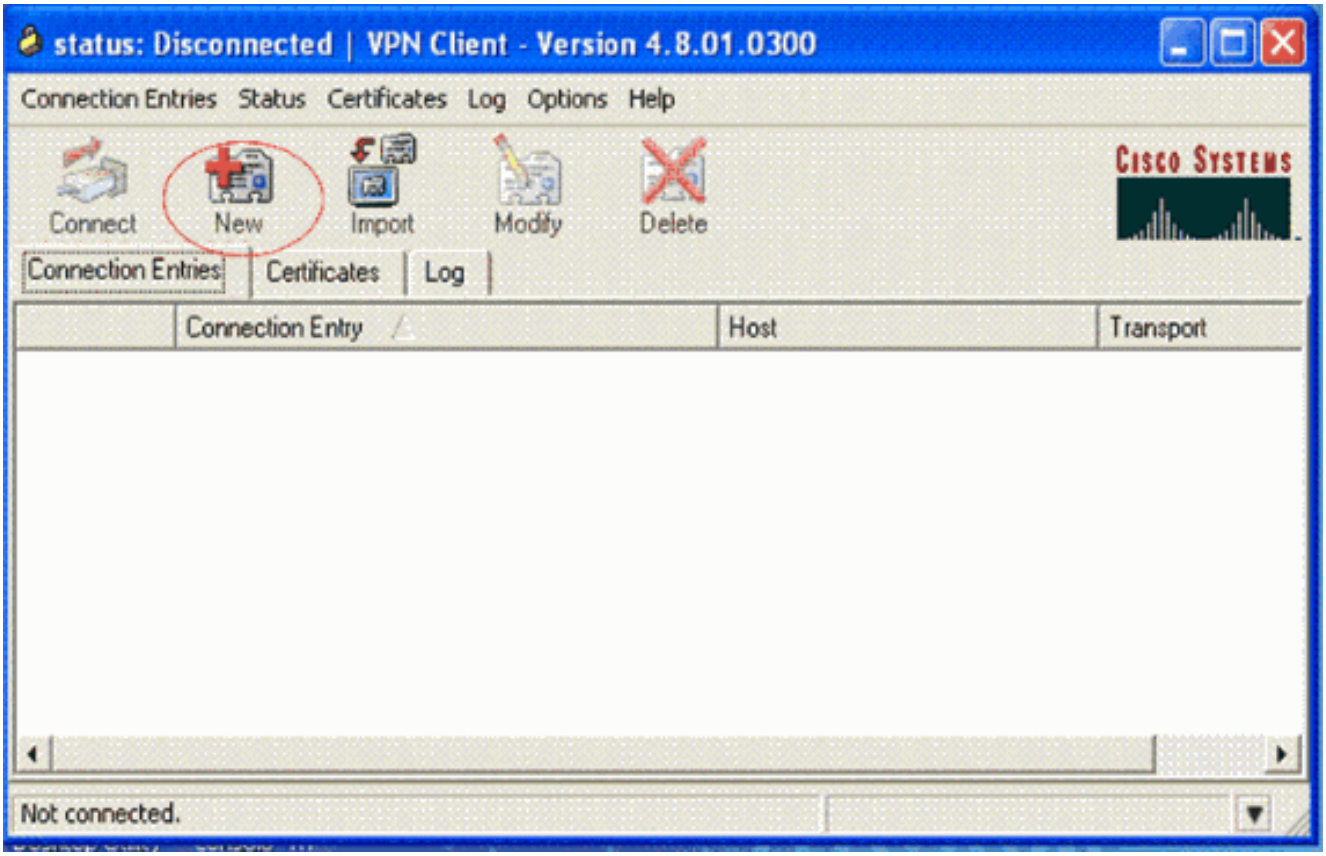
소프트웨어 VPN 클라이언트는 Cisco.com Software Center에서 다운로드할 수 있습니다.

참고: 일부 Cisco 소프트웨어는 CCO 사용자 이름 및 비밀번호로 로그인해야 합니다.

VPN 클라이언트를 구성하려면 다음 단계를 완료합니다.

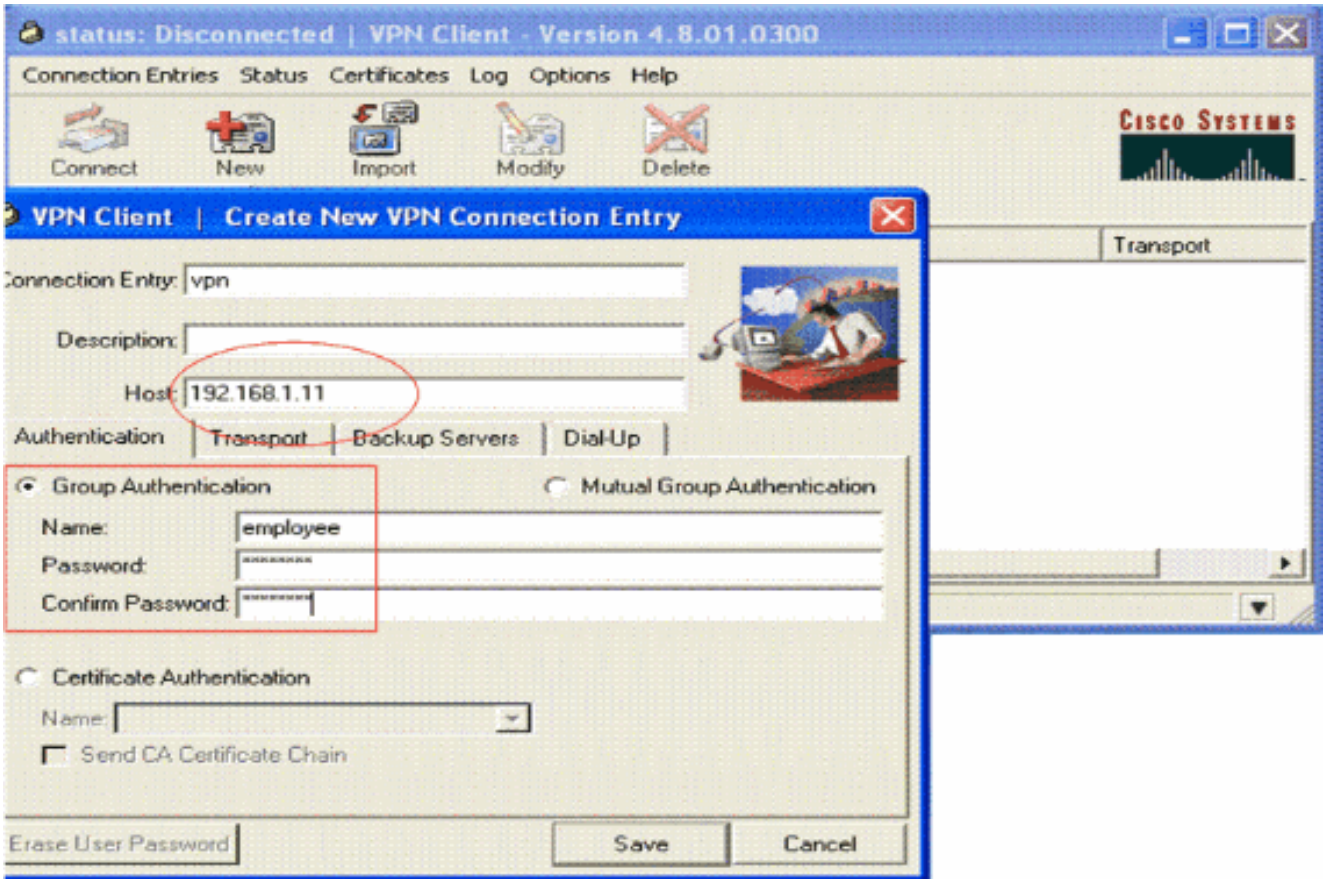
1. 무선 클라이언트(랩톱)에서 **시작 > 프로그램 > Cisco Systems VPN Client > VPN Client**를 선택하여 VPN 클라이언트에 액세스합니다.VPN 클라이언트가 설치된 기본 위치입니다.
2. Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창을 시작하려면 New(새로 만들기)를 클릭합니다

   .



3. 설명과 함께 연결 항목의 이름을 입력합니다.이 예에서는 *vpn을 사용합니다*.설명 필드는 선택 사항입니다.Host(호스트) 상자에 VPN 서버의 IP 주소를 입력합니다.그런 다음 VPN Group Name(VPN 그룹 이름) 및 Password(비밀번호)를 입력하고 Save(**저장)**를 클릭합니다

.



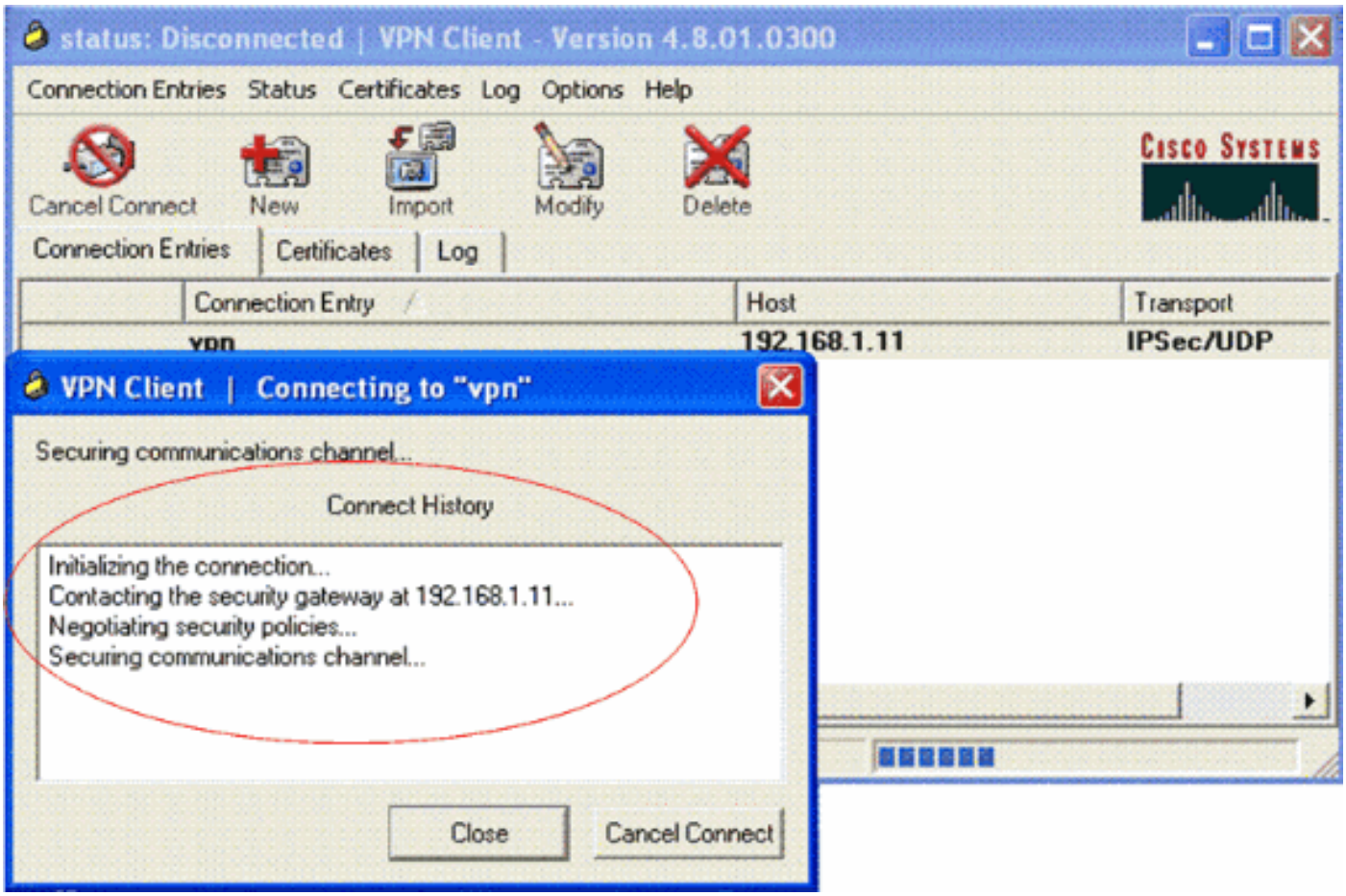
참고: 여기에 구성된 그룹 이름 및 비밀번호는 VPN 서버에 구성된 것과 동일해야 합니다.이 예에서는 Name *employee* 및 Password cisco*123을 사용합니다.*

다음을 확인합니다.

이 컨피그레이션을 확인하려면 무선 클라이언트에서 WLC에 구성된 동일한 보안 매개변수를 사용하여 SSID vpnclient를 구성하고 이 WLAN에 클라이언트를 연결합니다.새 프로파일을 사용하여 무선 클라이언트를 구성하는 방법을 설명하는 여러 문서가 있습니다.

무선 클라이언트가 연결되면 VPN Client로 이동하여 구성한 연결을 클릭합니다.그런 다음 VPN Client 주 창에서 Connect(연결)를 클릭합니다.

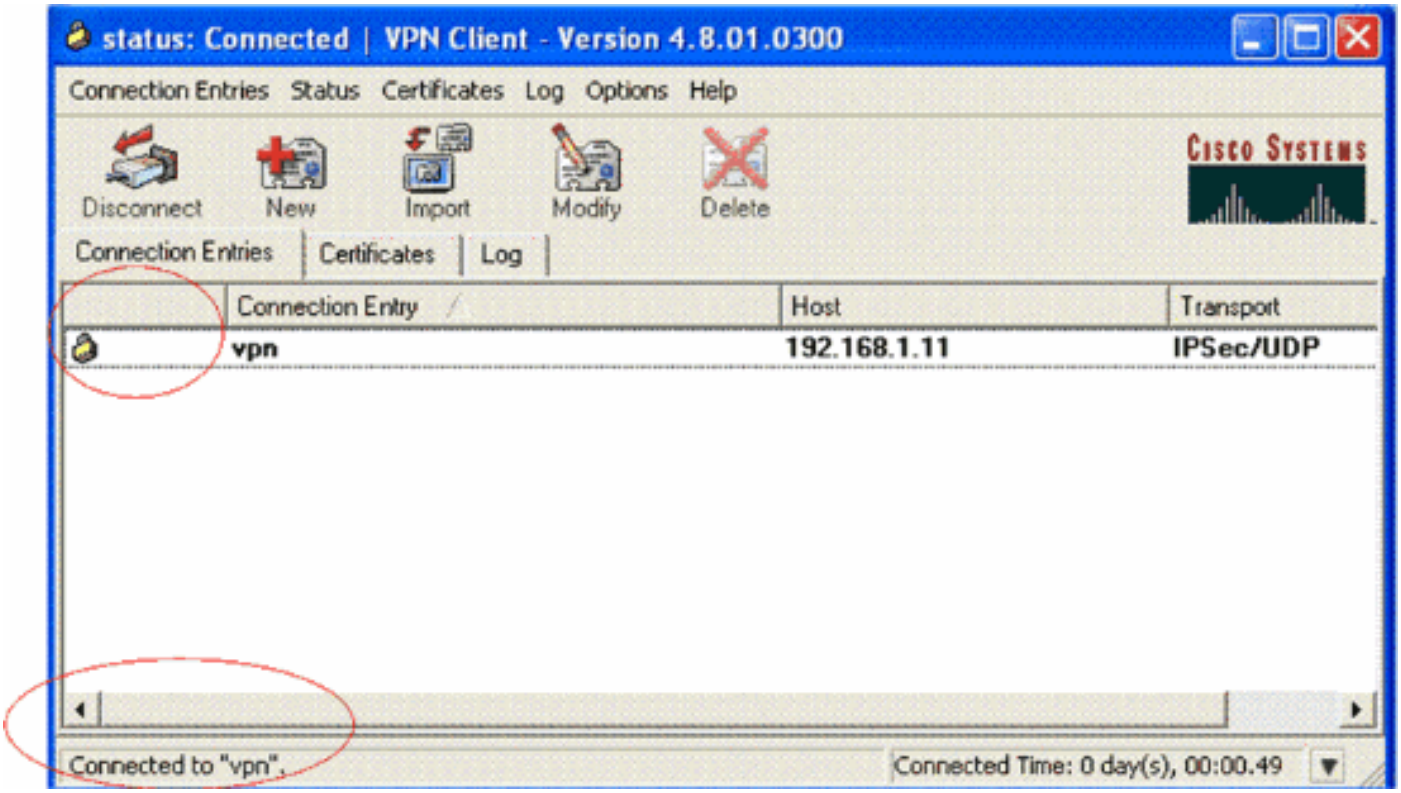
클라이언트와 서버 간에 협상된 1단계 및 2단계 보안 매개변수를 확인할 수 있습니다.



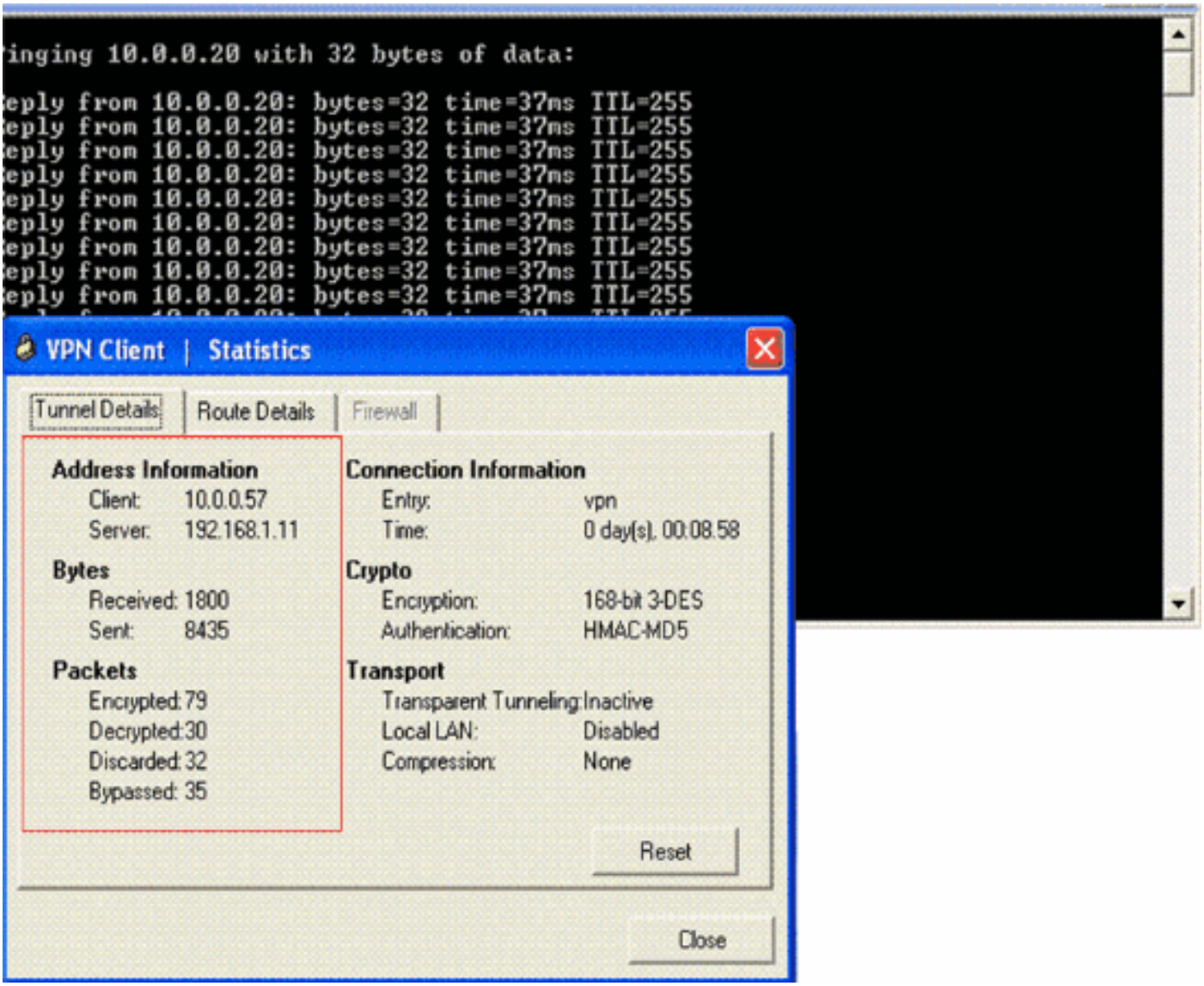
참고: 이 VPN 터널을 설정하려면 VPN 클라이언트와 서버 간에 IP 연결이 있어야 합니다.VPN 클라이언트가 보안 게이트웨이(VPN 서버)에 연결할 수 없는 경우 터널이 설정되지 않고 클라이언트 측에 경고 상자가 다음 메시지와 함께 표시됩니다.

```
Reason 412: The remote peer is no longer responding
```

클라이언트와 서버 간에 VPN 터널이 제대로 설정되도록 하려면 설정된 VPN 클라이언트 옆에 있는 잠금 아이콘을 찾을 수 있습니다.상태 표시줄에는 **"vpn"에 연결됨**이 **표시됩니다**. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다.



또한 VPN 클라이언트에서 서버 측의 LAN 세그먼트로 데이터를 전송하거나 그 반대로 전송할 수 있는지 확인합니다.VPN Client 주 메뉴에서 Status(상태) **> Statistics(통계)를** 선택합니다.여기에서 터널을 통해 전달되는 암호화 및 암호 해독된 패킷의 통계를 찾을 수 있습니다.



이 스크린샷에서는 클라이언트 주소를 10.0.0.57으로 볼 수 있습니다. 이 주소는 VPN 서버가 1단계 협상 성공 후 로컬에서 구성된 풀에서 클라이언트에 할당하는 주소입니다.터널이 설정되면 VPN 서버는 경로 테이블의 이 할당된 DHCP IP 주소에 경로를 자동으로 추가합니다.

또한 클라이언트가 서버에서 서버로 데이터를 전송하는 동안 암호화된 패킷의 수가 증가하고 역방향 데이터 전송 중에 해독된 패킷의 수가 증가하는 것을 볼 수 있습니다.

참고: WLC는 VPN Pass-through에 대해 구성되어 있으므로 클라이언트는 패스스루에 대해 구성된 VPN 게이트웨이(여기서는 VPN 서버192.168.1.11)에 연결된 세그먼트만 액세스할 수 있습니다.다른 모든 트래픽을 필터링합니다.

동일한 구성으로 다른 VPN 서버를 구성하고 VPN 클라이언트에서 이 VPN 서버에 대한 새 연결 항목을 구성하여 이를 확인할 수 있습니다.이제 이 VPN 서버로 터널을 설정하려고 시도해도 성공하지 못합니다.이는 WLC가 이 트래픽을 필터링하고 VPN Pass-through에 대해 구성된 VPN 게이트웨이 주소에만 터널을 허용하기 때문입니다.

VPN 서버의 CLI에서 컨피그레이션을 확인할 수도 있습니다.

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.

VPN 서버에서 사용되는 이러한 **show** 명령은 터널 상태를 확인하는 데 유용할 수 있습니다.

- show crypto **session** 명령은 터널 상태를 확인하는 데 사용됩니다.다음은 이 명령의 출력 예입니다.

```
Crypto session current status

Interface: Serial3/0
Session status: UP-ACTIVE
Peer: 172.16.1.20 port 500
  IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58
        Active SAs: 2, origin: dynamic crypto map
```

- show crypto **isakmp policy는** 구성된 1단계 매개변수를 보는 데 사용됩니다.

문제 해결

Verify(**확인**) 섹션에 설명된 debug 및 **show** 명령을 사용하여 문제를 해결할 수도 있습니다.

- **디버그 암호화 isakmp**
- **디버그 암호화 ipsec**
- **암호화 세션 표시**

- VPN 서버의 **debug crypto isakmp** 명령은 클라이언트와 서버 간의 1단계 협상 프로세스 전체를 표시합니다.다음은 성공적인 1단계 협상의 예입니다.

```
---------------------------------------------------------------------
 -------------------------------------------------------------
---------------------------------------------------------------
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14
   against priority 1 policy
*Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC
*Aug 28 10:37:29.515: ISAKMP:      hash MD5
*Aug 28 10:37:29.515: ISAKMP:      default group 2
*Aug 28 10:37:29.515: ISAKMP:      auth pre-share
*Aug 28 10:37:29.515: ISAKMP:      life type in seconds
*Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Aug 28
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA authentication status:
authenticated
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact,
  bring down existing phase 1 and 2 SA's with local 192.168.1.11
  remote 172.16.1.20 remote port 500
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
  the address pool: 10.0.0.57
*Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade
  1583442981 to QM_IDLE
*Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY
  RESPONDER_LIFETIME protocol 1
spi 1689265296, message ID = 1583442981
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to
  172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981
*Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400
```

```
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2
  New State = IKE_P1_COMPLETE
```

- VPN 서버의 **debug crypto ipsec** 명령은 성공적인 1단계 IPsec 협상 및 VPN 터널 생성을 표시합니다.예를 들면 다음과 같습니다.

```
----------------------------------------------------------------------
 ----------------------------------------------------------------
----------------------------------------------------------------------
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for
  peer or rekeying for peer 172.16.1.20
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added
  10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0
*Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F
*Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58,
  dest_port 0

*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.11, sa_proto= 50,
    sa_spi= 0x8538A817(2235082775),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.20, sa_proto= 50,
    sa_spi= 0xFFC80936(4291299638),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

관련 정보

- IPsec(IP Security) 암호화 소개
- IPsec 협상/IKE 프로토콜 지원 페이지
- IPsec 네트워크 보안 구성
- Cisco Easy VPN Q&A
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0
- 무선 LAN 컨트롤러 컨피그레이션의 ACL 예
- WLC(Wireless LAN Controller) FAQ
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems