

# IOS 라우터:IPSec 및 VPN 클라이언트 컨피그레이션을 위한 ACS를 통한 인증 프록시 인증 인바운드

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[VPN Client 4.8 구성](#)

[Cisco Secure ACS를 사용하여 TACACS+ 서버 구성](#)

[대체 기능 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

인증 프록시 기능을 사용하면 사용자가 TACACS+ 또는 RADIUS 서버에서 자동으로 검색 및 적용되는 특정 액세스 프로필을 사용하여 네트워크에 로그인하거나 HTTP를 통해 인터넷에 액세스할 수 있습니다. 사용자 프로필은 인증된 사용자로부터 활성 트래픽이 있는 경우에만 활성화됩니다.

이 컨피그레이션은 웹 브라우저를 10.1.1.1에서 시작하여 10.17.17.17으로 표시하도록 설계되었습니다. VPN 클라이언트는 10.17.17.x 네트워크에 연결하기 위해 터널 엔드포인트 10.31.1.111을 통과하도록 구성되어 있으므로 IPSec 터널이 구축되고 PC가 풀 RTP-POOL에서 IP 주소를 가져옵니다(모드 컨피그레이션이 수행되기 때문). 그런 다음 Cisco 3640 라우터에서 인증을 요청합니다. 사용자가 사용자 이름과 비밀번호(10.14.14.3의 TACACS+ 서버에 저장)를 입력하면 서버에서 전달된 액세스 목록이 액세스 목록 118에 추가됩니다.

## 사전 요구 사항

## 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco VPN Client는 Cisco 3640 라우터로 IPSec 터널을 설정하도록 구성됩니다.
- TACACS+ 서버는 인증 프록시에 대해 구성됩니다. 자세한 내용은 "관련 정보" 섹션을 참조하십시오.

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS 소프트웨어 릴리스 12.4
- Cisco 3640 Router
- Windows 버전 4.8용 Cisco VPN Client(모든 VPN 클라이언트 4.x 이상이 작동해야 함)

**참고:** ip auth-proxy 명령은 Cisco IOS Software 릴리스 12.0.5.T에서 도입되었습니다.이 구성은 Cisco IOS Software 릴리스 12.4에서 테스트되었습니다.

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 규칙](#)을 참조하십시오.

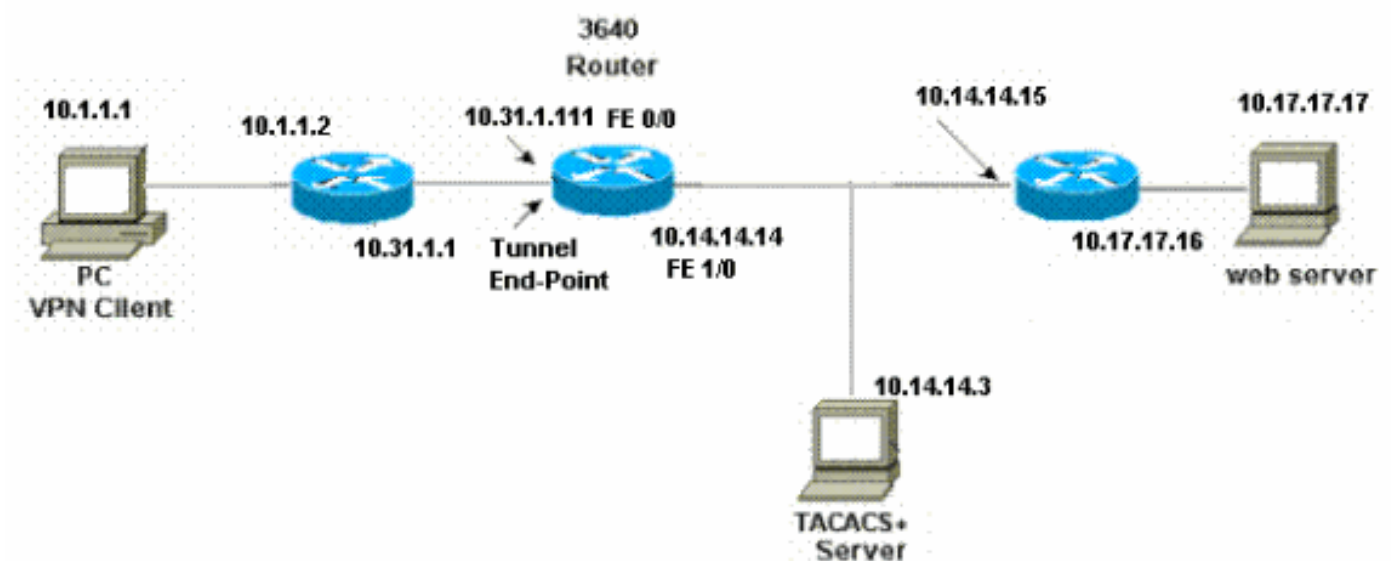
## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용합니다.

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



## 구성

3640 라우터
----------

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
!--- The username and password is used during local
authentication. username rtpuser password 0 rtpuserpass

!--- Enable AAA. aaa new-model

!--- Define server-group and servers for TACACS+. aaa
group server tacacs+ RTP
server 10.14.14.3
!

!--- In order to set authentication, authorization, and
accounting (AAA) authentication at login, use the aaa
authentication login command in global configuration
mode

aaa authentication login default group RTP local
aaa authentication login userauth local
aaa authorization exec default group RTP none
aaa authorization network groupauth local
aaa authorization auth-proxy default group RTP
enable secret 5 $1$CQHCS$R/07uQ44E2JgVuCsOUWdG1
enable password ww
!
ip subnet-zero
!
!--- Define auth-proxy banner, timeout, and rules. ip
auth-proxy auth-proxy-banner http ^C
Please Enter Your Username and Password:
^C
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
!--- Define ISAKMP policy. crypto isakmp policy 10
hash md5
authentication pre-share
group 2

!--- These commands define the group policy that !--- is
enforced for the users in the group RTPUSERS. !--- This
group name and the key should match what !--- is
configured on the VPN Client. The users from this !---
group are assigned IP addresses from the pool RTP-POOL.
crypto isakmp client configuration group RTPUSERS
key cisco123
pool RTP-POOL
!
!--- Define IPsec transform set and apply it to the
dynamic crypto map. crypto ipsec transform-set RTP-
TRANSFORM esp-des esp-md5-hmac
!
```

```

crypto dynamic-map RTP-DYNAMIC 10
  set transform-set RTP-TRANSFORM
!
!--- Define extended authentication (X-Auth) using the
local database. !--- This is to authenticate the users
before they can !--- use the IPsec tunnel to access the
resources. crypto map RTPCLIENT client authentication
list userauth

!--- Define authorization using the local database. !---
This is required to push the 'mode configurations' to
the VPN Client. crypto map RTPCLIENT isakmp
authorization list groupauth
crypto map RTPCLIENT client configuration address
initiate
crypto map RTPCLIENT client configuration address
respond
crypto map RTPCLIENT 10 ipsec-isakmp dynamic RTP-DYNAMIC
!
interface FastEthernet0/0
  ip address 10.31.1.111 255.255.255.0
  ip access-group 118 in
  no ip directed-broadcast

!--- Apply the authentication-proxy rule to the
interface. ip auth-proxy list_a
  no ip route-cache
  no ip mroute-cache
  speed auto
  half-duplex

!--- Apply the crypto-map to the interface. crypto map
RTPCLIENT
!
interface FastEthernet1/0
  ip address 10.14.14.14 255.255.255.0
  no ip directed-broadcast
  speed auto
  half-duplex
!
!--- Define the range of addresses in the pool. !--- VPN
Clients will have thier 'internal addresses' assigned !-
-- from this pool. ip local pool RTP-POOL 10.20.20.25
10.20.20.50
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.15
ip route 10.1.1.0 255.255.255.0 10.31.1.1

!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPsec
packets !--- to enable the Cisco VPN Client to establish
the IPsec tunnel. !--- The last line of the access-list
118 permits communication !--- between the TACACS+
server and the 3640 router to enable !--- authentication
and authorization. All other traffic is denied. access-
list 118 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111
access-list 118 permit udp 10.1.1.0 0.0.0.255 host
10.31.1.111 eq isakmp
access-list 118 permit tcp host 10.14.14.3 host
10.31.1.111

```

```

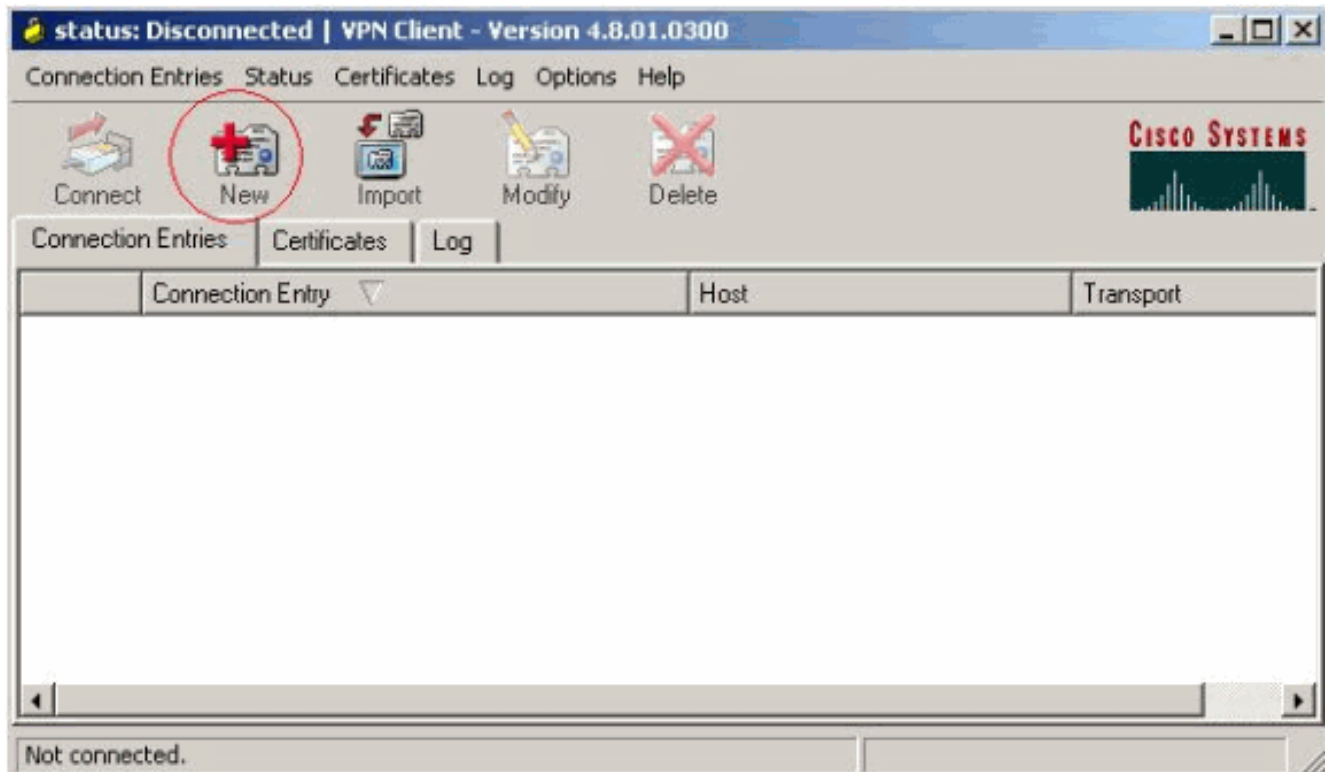
!
!--- Define the IP address and the key for the TACACS+
server. tacacs-server host 10.14.14.3 key cisco
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
!
end

```

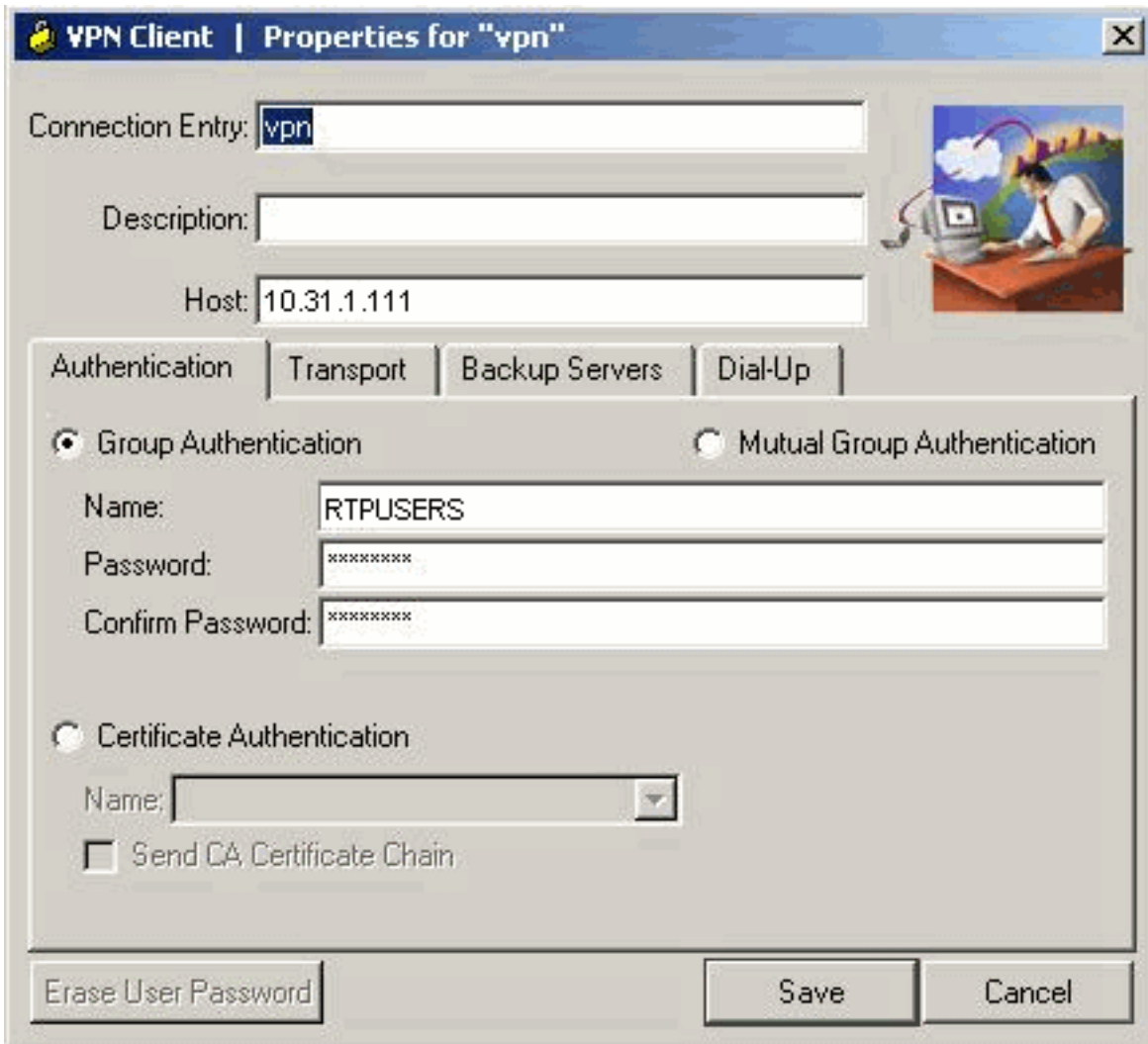
## VPN Client 4.8 구성

VPN Client 4.8을 구성하려면 다음 단계를 완료하십시오.

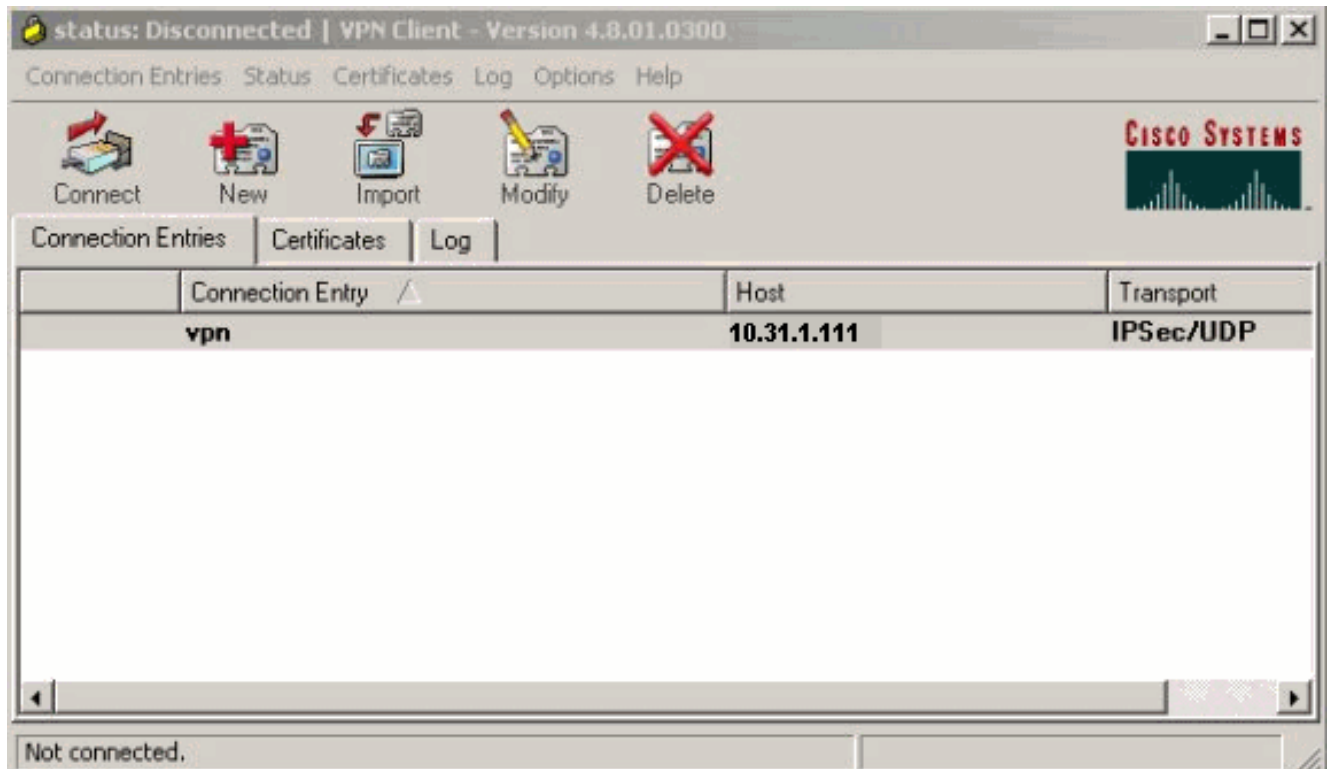
1. Start(시작) > Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > VPN Client(VPN 클라이언트)를 선택합니다.
2. New(새로 만들기)를 클릭하여 Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창을 시작합니다



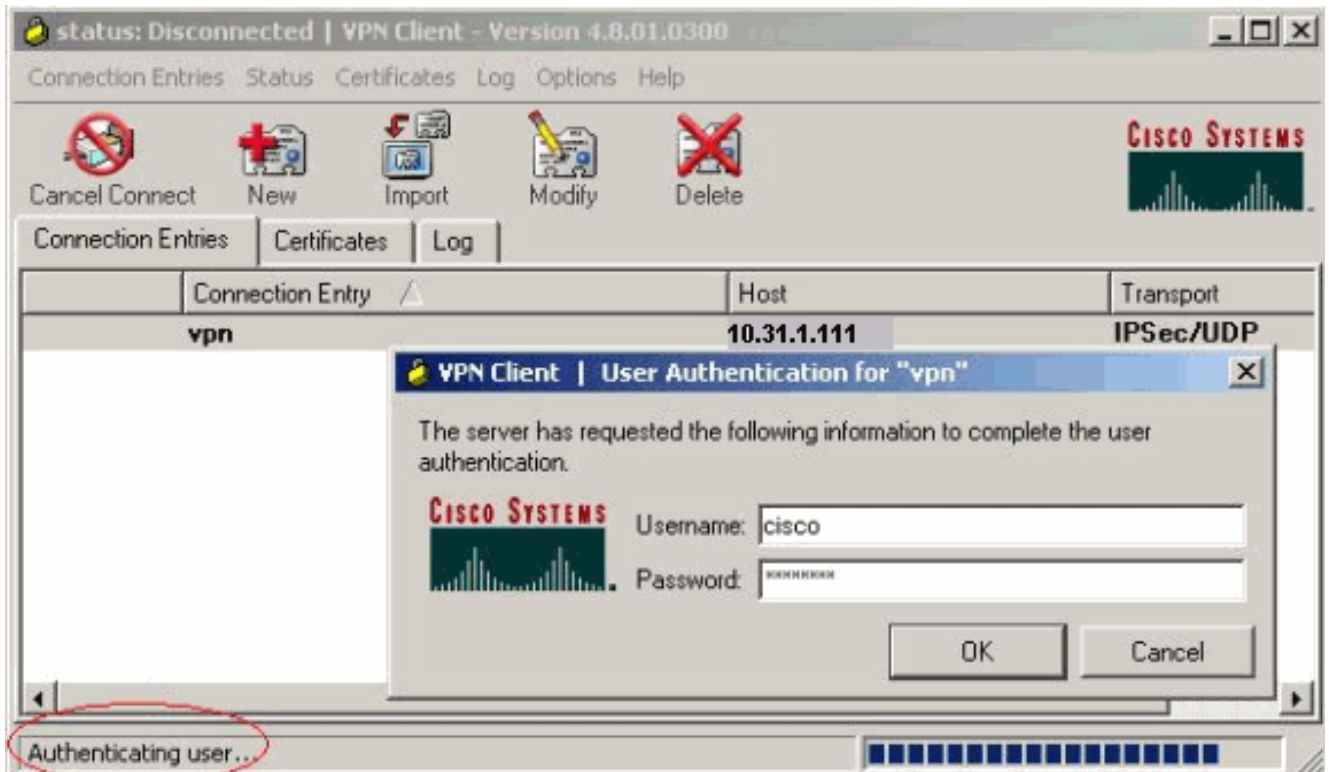
3. 설명과 함께 연결 항목의 이름을 입력합니다.Host(호스트) 상자에 라우터의 외부 IP 주소를 입력합니다.그런 다음 VPN 그룹 이름과 비밀번호를 입력하고 Save(저장)를 클릭합니다



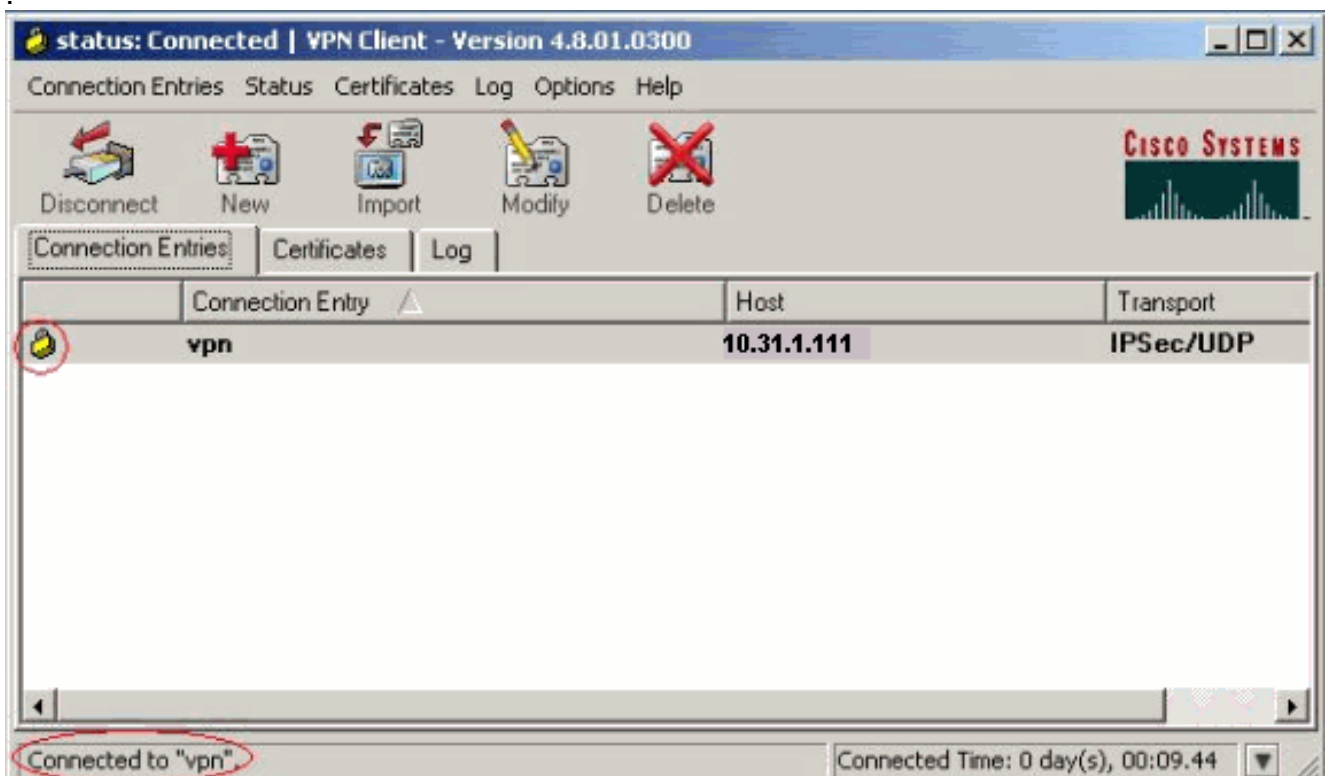
4. 사용할 연결을 클릭하고 VPN Client 주 창에서 **Connect(연결)**를 클릭합니다



5. 프롬프트가 표시되면 xauth에 대한 사용자 이름 및 비밀번호 정보를 입력하고 **OK(확인)**를 클릭하여 원격 네트워크에 연결합니다



VPN 클라이언트는 중앙 사이트의 라우터에 연결됩니다



## Cisco Secure ACS를 사용하여 TACACS+ 서버 구성

Cisco Secure ACS에서 TACACS+를 구성하려면 다음 단계를 완료합니다.

1. 사용자 자격 증명을 확인하려면 Cisco Secure ACS를 찾도록 라우터를 구성해야 합니다. 예를 들면 다음과 같습니다.

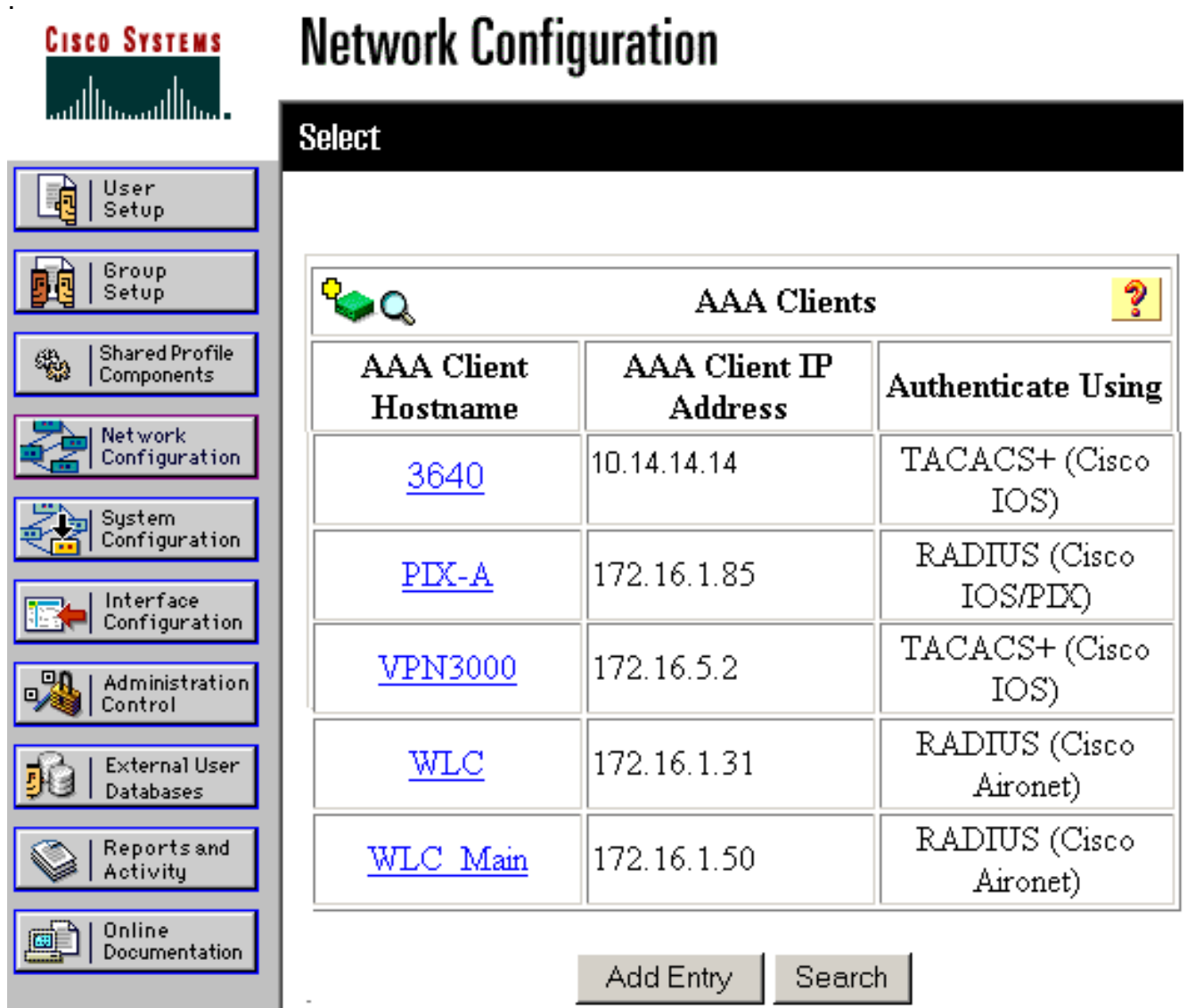
```
3640 (config) #
```

```
aaa group server tacacs+ RTP
```

```
3640 (config) #
```

[tacacs-server host 10.14.14.3 key cisco](#)

2. 왼쪽에서 **Network Configuration(네트워크 컨피그레이션)**을 선택하고 **Add Entry(항목 추가)**를 클릭하여 TACACS+ 서버 데이터베이스 중 하나에서 라우터에 대한 항목을 추가합니다.라우터 컨피그레이션에 따라 서버 데이터베이스를 선택합니다

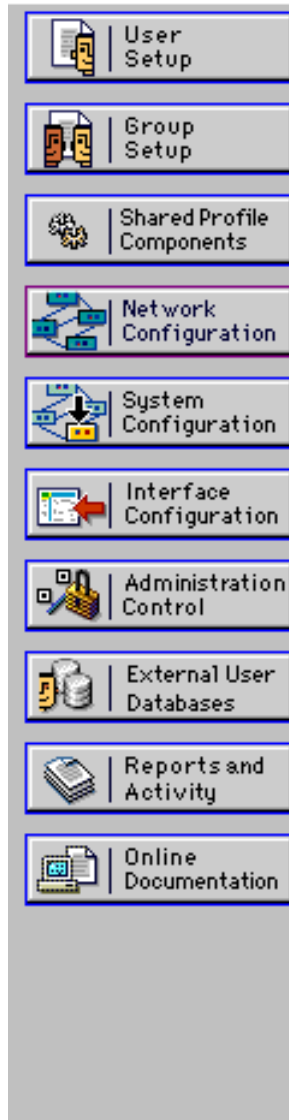


The screenshot shows the Cisco Network Configuration web interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled 'Network Configuration' and 'Select'. It displays a table of AAA Clients with columns for Hostname, IP Address, and Authentication Method. The table contains six entries, including '3640' which is highlighted in blue. Below the table are 'Add Entry' and 'Search' buttons.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">3640</a>	10.14.14.14	TACACS+ (Cisco IOS)
<a href="#">PIX-A</a>	172.16.1.85	RADIUS (Cisco IOS/PDX)
<a href="#">VPN3000</a>	172.16.5.2	TACACS+ (Cisco IOS)
<a href="#">WLC</a>	172.16.1.31	RADIUS (Cisco Aironet)
<a href="#">WLC Main</a>	172.16.1.50	RADIUS (Cisco Aironet)

3. 키는 3640 라우터와 Cisco Secure ACS 서버 간에 인증하는 데 사용됩니다.인증을 위해 TACACS+ 프로토콜을 선택하려면 Authenticate Using 드롭다운 메뉴에서 **TACACS+(Cisco IOS)**를 선택합니다





### Add AAA Client

AAA Client Hostname	<input type="text" value="3640"/>
AAA Client IP Address	<input type="text" value="10.14.14.14"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

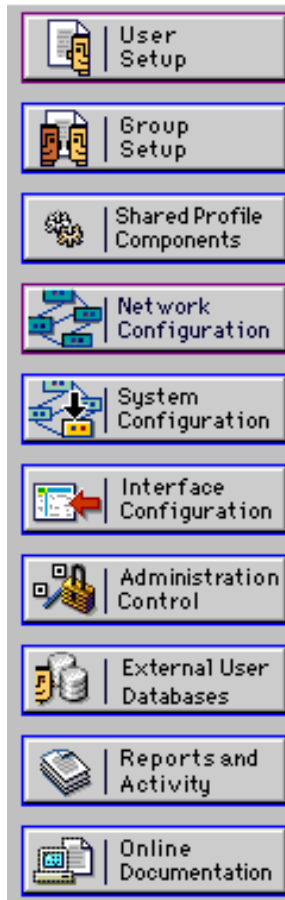
Submit

Submit + Restart

Cancel

4. Cisco Secure 데이터베이스의 User(사용자) 필드에 사용자 이름을 입력한 다음 Add/Edit(추가/수정)를 클릭합니다. 이 예에서는 사용자 이름이 rtpuser입니다

## Select



User:

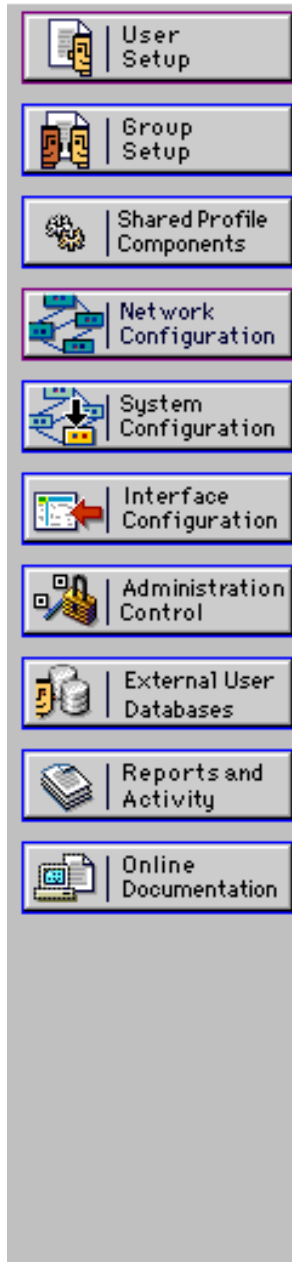
List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)  
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)  
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

5. 다음 창에서 rtpuser의 비밀번호를 입력합니다. 이 예에서는 비밀번호가 rtpuserpass입니다. 원하는 경우 사용자 계정을 그룹에 매핑할 수 있습니다. 완료되면 Submit(제출)을 클릭합니다



## User Setup



Supplementary User Info	
Real Name	<input type="text" value="rtpuser"/>
Description	<input type="text"/>

User Setup		
Password Authentication:		
	<input type="text" value="CiscoSecure Database"/>	
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)		
Password	<input type="password" value="*"/>	
Confirm Password	<input type="password" value="*"/>	
<input type="checkbox"/> Separate (CHAP/MS-CHAP/ARAP)		
Password	<input type="password"/>	
Confirm Password	<input type="password"/>	
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is		
<input type="button" value="Submit"/>	<input type="button" value="Delete"/>	<input type="button" value="Cancel"/>

### 대체 기능 구성

기본 RADIUS 서버를 사용할 수 없게 되면 라우터는 다음 활성 백업 RADIUS 서버로 장애 조치됩니다. 기본 서버를 사용할 수 있는 경우에도 라우터는 계속해서 보조 RADIUS 서버를 계속 사용합니다. 일반적으로 기본 서버는 높은 성능과 기본 서버입니다. 보조 서버를 사용할 수 없는 경우 로컬 데이터베이스를 [aaa authentication login default group RTP local](#) 명령을 사용하여 인증에 사용할 수 있습니다.

### 다음을 확인합니다.

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

PC와 Cisco 3640 라우터 간에 IPSec 터널을 설정합니다.

PC에서 브라우저를 열고 <http://10.17.17.17>으로 이동합니다. Cisco 3640 라우터는 이 HTTP 트래픽을 인터셉트하고 인증 프록시를 트리거하며 사용자 이름과 비밀번호를 입력하라는 메시지를 표시합니다. Cisco 3640은 인증을 위해 사용자 이름/비밀번호를 TACACS+ 서버로 전송합니다. 인증에 성공하면 웹 서버(10.17.17.17)에서 웹 페이지를 볼 수 있습니다.

일부 **show** 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- [show ip access-lists](#)—방화벽 라우터에 구성된 표준 및 확장 ACL을 표시합니다(동적 ACL 항목 포함). 사용자가 인증하는지 여부에 따라 동적 ACL 항목이 정기적으로 추가되고 제거됩니다. 이 출력은 auth-proxy가 트리거되기 전에 access-list 118을 표시합니다.

```
3640#show ip access-lists 118
Extended IP access list 118
10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (321 matches)
20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (276 matches)
30 permit tcp host 10.14.14.3 host 10.31.1.111 (174 matches)
```

이 출력은 auth-proxy가 트리거되고 사용자가 성공적으로 인증한 후 access-list 118을 표시합니다.

```
3640#show ip access-lists 118
Extended IP access list 118
permit tcp host 10.20.20.26 any (7 matches)
permit udp host 10.20.20.26 any (14 matches)
permit icmp host 10.20.20.26 any
10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (379 matches)
20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (316 matches)
30 permit tcp host 10.14.14.3 host 10.31.1.111 (234 matches)
```

액세스 목록의 처음 세 행은 이 사용자에게 대해 정의되고 TACACS+ 서버에서 다운로드한 항목입니다.

- [show ip auth-proxy cache](#)—인증 프록시 항목 또는 실행 중인 인증 프록시 컨피그레이션을 표시합니다. 호스트 IP 주소, 소스 포트 번호, 인증 프록시의 시간 제한 값, 인증 프록시를 사용하는 연결의 상태를 나열하는 cache 키워드. 인증 프록시 상태가 ETAB이면 사용자 인증이 성공합니다.

```
3640#show ip auth-proxy cache
Authentication Proxy Cache
Client IP 10.20.20.26 Port 1705, timeout 5, state ESTAB
```

## 문제 해결

확인 및 디버깅 명령과 다른 문제 해결 정보는 [인증 프록시 문제 해결](#)을 참조하십시오.

참고: debug 명령을 실행하기 전에 [디버그 명령에 대한 중요 정보를 참조하십시오](#).

## 관련 정보

- [인증 프록시 구성](#)
- [Cisco IOS의 인증 프록시 컨피그레이션](#)
- [TACACS+ 및 RADIUS 서버에서 인증 프록시 구현](#)
- [Cisco VPN 클라이언트 지원 페이지](#)
- [IOS 방화벽 지원 페이지](#)
- [IPSec 지원 페이지](#)
- [RADIUS 지원 페이지](#)
- [RFC\(Request for Comments\)](#)

- [TACACS/TACACS+ 지원 페이지](#)
- [IOS 설명서의 TACACS+](#)
- [Technical Support - Cisco Systems](#)