

# RADIUS를 사용하여 Windows용 Cisco IOS 라우터와 Cisco VPN Client 4.x 간 IPsec 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 이론](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[RADIUS 서버 컨피그레이션](#)

[AAA 클라이언트\(라우터\)를 위한 RADIUS 서버 구성](#)

[그룹 인증 및 권한 부여를 위한 RADIUS 서버 구성](#)

[사용자 인증을 위한 RADIUS 서버 구성](#)

[VPN Client 4.8 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[트러블슈팅 명령](#)

[디버그 출력](#)

[라우터 로그](#)


[클라이언트 로그](#)

[관련 정보](#)

---

## 소개

이 문서에서는 그룹 권한 부여 및 사용자 인증을 위해 RADIUS를 사용하여 Cisco IOS 라우터와 Cisco VPN Client 4.x 간의 연결을 구성하는 방법을 보여줍니다. Cisco IOS® Software Release 12.2(8)T 이상에서는 Cisco VPN Client 3.x로부터의 연결을 지원합니다. VPN 클라이언트 3.x 및 4.x는 DH(Diffie Hellman) 그룹 2 정책을 사용합니다. isakmp policy # group 2 명령은 VPN 클라이언트가 연결할 수 있게 합니다.

 참고: 이제 IPsec VPN 어카운팅을 사용할 수 있습니다. 자세한 내용과 샘플 [컨피그레이션](#)은 IPsec [VPN](#) 어카운팅을 참조하십시오.

---


## 사전 요구 사항

### 요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- IPSec에 할당할 주소 풀
- 사전 공유 키가 "cisco123"인 "3000client"라는 그룹
- RADIUS 서버에 대한 그룹 권한 부여 및 사용자 인증

---

 참고: 현재 RADIUS 계정 관리는 지원되지 않습니다.

---

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2(8)T를 실행하는 2611 라우터.
- Windows용 Cisco Secure ACS(모든 RADIUS 서버가 작동해야 함).
- Cisco VPN Client for Windows 버전 4.8(모든 VPN Client 4.x가 작동해야 함)

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.

이는 라우터의 show version 명령의 출력입니다.

```
<#root>
```

```
vpn2611#
```

```
show version
```

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK903S-M), Version 12.2(8)T,
  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
Image text-base: 0x80008070, data-base: 0x81816184

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

vpn2611 uptime is 1 hour, 15 minutes
System returned to ROM by reload
System image file is "flash:c2600-jk9o3s-mz.122-8.T"

cisco 2611 (MPC860) processor (revision 0x203)
  with 61440K/4096K bytes of memory.
Processor board ID JAD04370EEG (2285146560)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

## 배경 이론

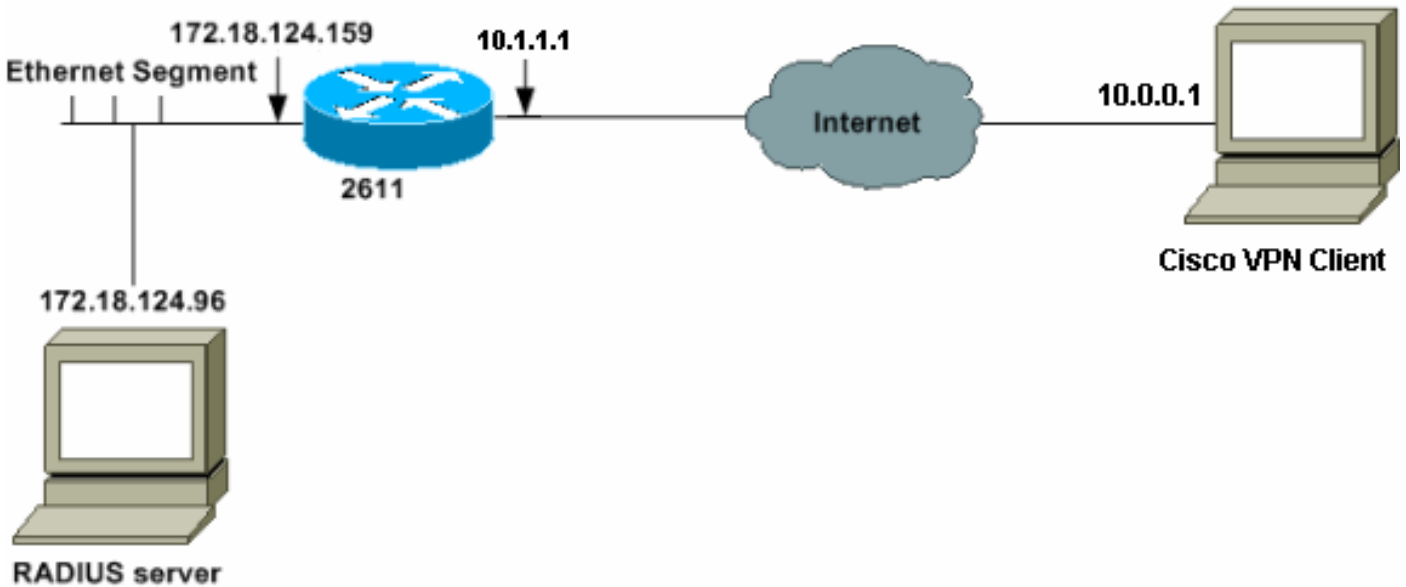
이 문서에서는 RADIUS 서버에 의한 WINS(Windows Internet Naming Service) 및 DNS(Domain Naming Service) 할당과 같은 인증 및 권한 부여를 보여줍니다. RADIUS 서버에 의한 인증 및 라우터에 의한 로컬 권한 부여를 수행하려는 경우, [Configuring IPSec Between a Cisco IOS Router and a Cisco VPN Client 4.x for Windows using RADIUS for User Authentication](#)을 참조하십시오.


## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

### 네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



 참고: 이 예제 네트워크의 IP 주소는 랩 네트워크의 전용 IP 주소이므로 전역 인터넷에서 라우팅할 수 없습니다.

## 설정

2611 라우터

```
<#root>
```

```
vpn2611#
```

```
show run
```

Building configuration...

Current configuration : 1884 bytes

```
!  
version 12.2  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname vpn2611  
!
```

*!--- Enable AAA for user authentication and group authorization.*

```
aaa new-model
```

```
!
```

*!--- In order to enable extended authentication (Xauth) for user authentication,  
!--- enable the*

```
aaa authentication
```

```
commands.
```

*!--- "Group radius" specifies RADIUS user authentication.*

```
aaa authentication login userauthen group radius
```

*!--- In order to enable group authorization,  
!--- enable the*

```
aaa authorization
```

```
commands.
```

```
aaa authorization network groupauthor group radius
```

```
!
```

```
!
```

```
ip subnet-zero
```

```
!
```

```
!
```

```
!
```

```
ip audit notify log
```

```
ip audit po max-events 100
```

```
!
```

*!--- Create an Internet Security Association and  
!--- Key Management Protocol (ISAKMP) policy for Phase 1 negotiations.*

```
crypto isakmp policy 3
```

```
encr 3des
```

```
authentication pre-share
```

```
group 2
```

```
!
```

```
!
```

*!--- Create the Phase 2 policy for actual data encryption.*

```
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
```

*!--- Create a dynamic map and  
!--- apply the transform set that was created.*

```
crypto dynamic-map dynmap 10
set transform-set myset
!
```

*!--- Create the actual crypto map,  
!--- and apply the AAA lists that were created earlier.*

```
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
```

*!--- Apply the crypto map on the outside interface.*

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
half-duplex
crypto map clientmap
!
interface Serial0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 172.18.124.159 255.255.255.0
no keepalive
half-duplex
!
```

*!--- Create a pool of addresses to be assigned to the VPN Clients.*

```
ip local pool ippool 10.16.20.1 10.16.20.200
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip http server
```

```
ip pim bidir-enable
!

!--- Create an access control list (ACL) if you want to do split tunneling.
!--- This ACL is referenced in the RADIUS profile.

access-list 108 permit ip 172.18.124.0 0.0.255.255 10.16.20.0 0.0.0.255

!

!--- Specify the IP address of the RADIUS server,
!--- along with the RADIUS shared secret key.

radius-server host 172.18.124.96 auth-port 1645 acct-port 1646 key cisco123

radius-server retransmit 3
call rsvp-sync

!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end

vpn2611#
```

## RADIUS 서버 컨피그레이션

AAA 클라이언트(라우터)를 위한 RADIUS 서버 구성

다음 단계를 완료하십시오.

1. Add Entry(항목 추가)를 클릭하여 라우터를 RADIUS 서버 데이터베이스에 추가합니다.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">340</a>	172.18.124.151	RADIUS (Cisco Aironet)
<a href="#">Aironet-340-Lab</a>	14.36.1.99	RADIUS (Cisco Aironet)
<a href="#">glennitest</a>	172.18.124.120	RADIUS (Cisco IOS/PIX)
<a href="#">router</a>	172.18.124.150	TACACS+ (Cisco IOS)

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Renaming a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)

2. 공유 비밀 키 "cisco123"과 함께 라우터의 IP 주소 "172.18.124.159"를 지정하고 Authenticate Using(사용 인증) 드롭다운 상자에서 RADIUS를 선택합니다.

**Add AAA Client**

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

그룹 인증 및 권한 부여를 위한 RADIUS 서버 구성

다음 단계를 완료하십시오.

1. Add/Edit(추가/수정)를 클릭하여 이름이 3000client인 사용자를 RADIUS 서버에 추가합니다.

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

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, delete users in the database.

**User Setup and External User Databases**

Before Cisco Secure ACS can authenticate users with an external database, you must:

- You must have the database up and running on the external server. For example, if you are using token card authentication, you must have the database up and running on the external server.
- You must have configured the applicable parameters in the external database.

2. Cisco IOS Software 릴리스 15.8.3 및 Cisco IOS XE Software 릴리스 16.9.1 이전에는 이 비밀번호가 Cisco IOS에 대한 특수 키워드였으며, 이는 그룹 프로필을 참조해야 함을 나타냅니다.

다. 원하는 경우 사용자를 Cisco Secure 그룹에 매핑할 수 있습니다. No IP address assignment(IP 주소 할당 없음)가 선택되어 있는지 확인합니다.

Cisco IOS Software 릴리스 15.8.3 및 Cisco IOS XE Software 릴리스 16.9.1 이후에는 AAA 권한 부여에 암호가 필요하며 필수 항목입니다. isakmp 권한 부여 목록 aaa\_list1 password <secret> 명령을 통해 사용되는 비밀번호를 정의하는 것이 좋습니다.

그러면 관리자가 RADIUS 서버에서 <secret> 일치 비밀번호를 구성합니다.





## User Setup

### User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When using a Token Card server for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

---

Group to which the user is assigned:

Group 20

---

Callback

Use group setting

No callback allowed

Callback using this number

Dialup client specifies callback number

Use Microsoft NT callback settings

---

Client IP Address Assignment

Use group settings

No IP address assignment

Assigned by dialup client

Assign static IP address

Assigned by AAA client pool

3. 이 사용자 계정에 의해 VPN 클라이언트로 다시 전달될 그룹 권한 부여 매개변수를 지정합니다.

다음 특성으로 cisco-av-pair를 활성화했는지 확인합니다.

- ipsec:key-exchange=ike

- ipsec: key-exchange=preshared-key
- ipsec:addr-pool=ippool
- ipsec:inac1=108(라우터에서 스플릿 터널링을 사용하는 경우에만 필요함)

또한 다음과 같은 IETF RADIUS 특성을 활성화해야 합니다.

- 특성 6: Service-Type=Outbound
- 특성 64: Tunnel-Type=IP ESP
- 특성 69: Tunnel-Password=cisco123(VPN 클라이언트의 그룹 비밀번호)

완료되면 Submit(제출)을 클릭합니다.

**Checking this option will PERMIT all UNKNOWN Services**

Default (Undefined) Services

---

**Cisco IOS/PIX RADIUS Attributes** ?

[009\001] cisco-av-pair

```
ipsec:key-exchange=ike
ipsec:key-exchange=preshared-key
ipsec:addr-pool=ippool
ipsec:inac1=100
```

---

**IETF RADIUS Attributes** ?

[006] Service-Type Outbound

[007] Framed-Protocol PPP

[027] Session-Timeout 0

[028] Idle-Timeout 0

[064] Tunnel-Type

Tag 1 Value IP ESP

Tag 2 Value

[069] Tunnel-Password

Tag 1 Value cisco123

Tag 2 Value

Submit Delete Cancel

Vendor Specific Attributes(공급업체별 특성)에서 다음 선택적 특성을 활성화할 수도 있습니다.


- ipsec: default-domain=
- ipsec:timeout=
- ipsec:idletime=
- ipsec:dns-servers=
- ipsec:wins-servers=

## 사용자 인증을 위한 RADIUS 서버 구성

다음 단계를 완료하십시오.

1. Cisco Secure 데이터베이스에 VPN 사용자를 추가하려면 Add/Edit를 클릭합니다.

이 예에서 사용자 이름은 cisco입니다.

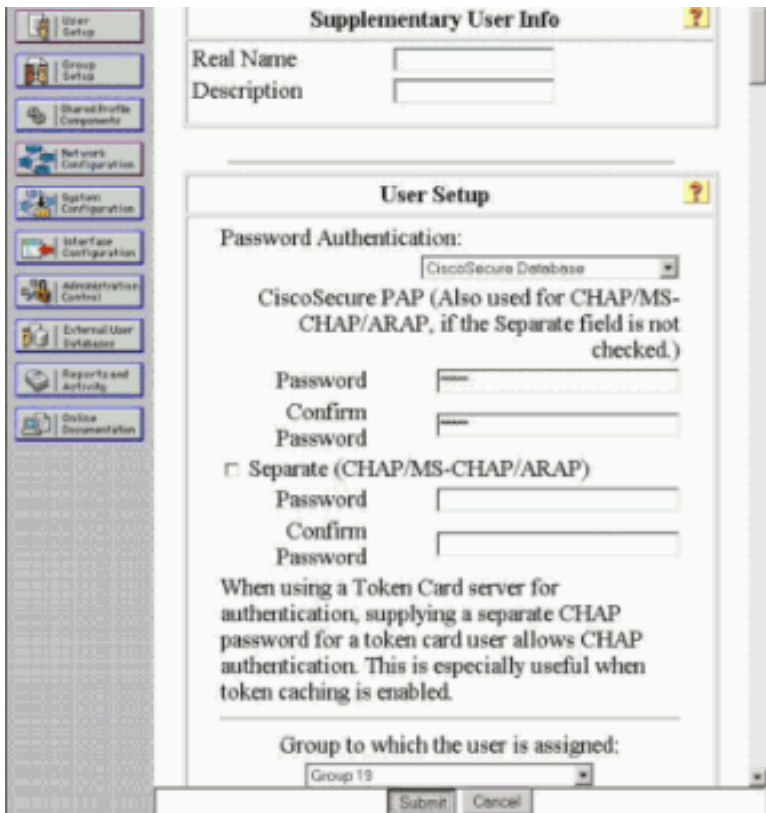


- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

2. 다음 창에서 사용자 cisco의 비밀번호를 지정합니다. 비밀번호도 cisco입니다.

사용자 계정을 그룹에 매핑할 수 있습니다. 완료되면 Submit(제출)을 클릭합니다.



- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

**Account Disabled Status**

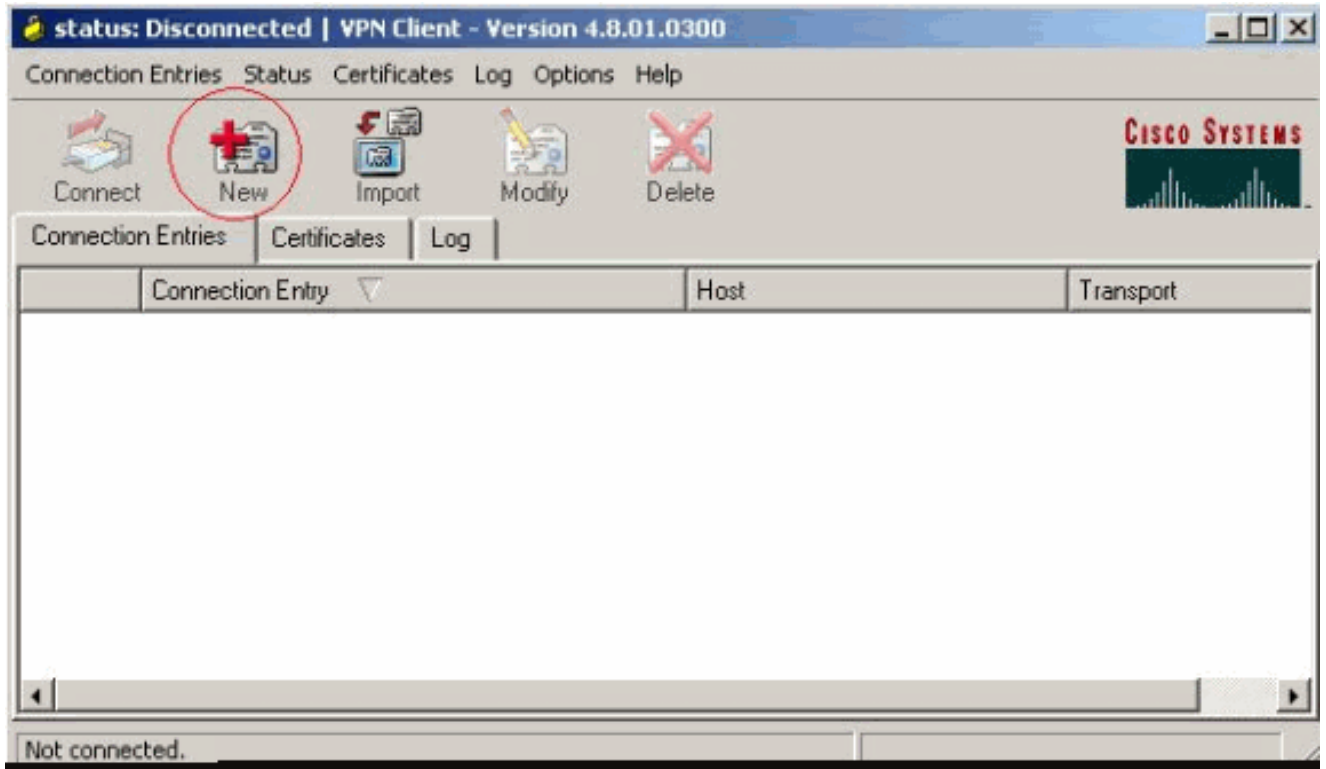
Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

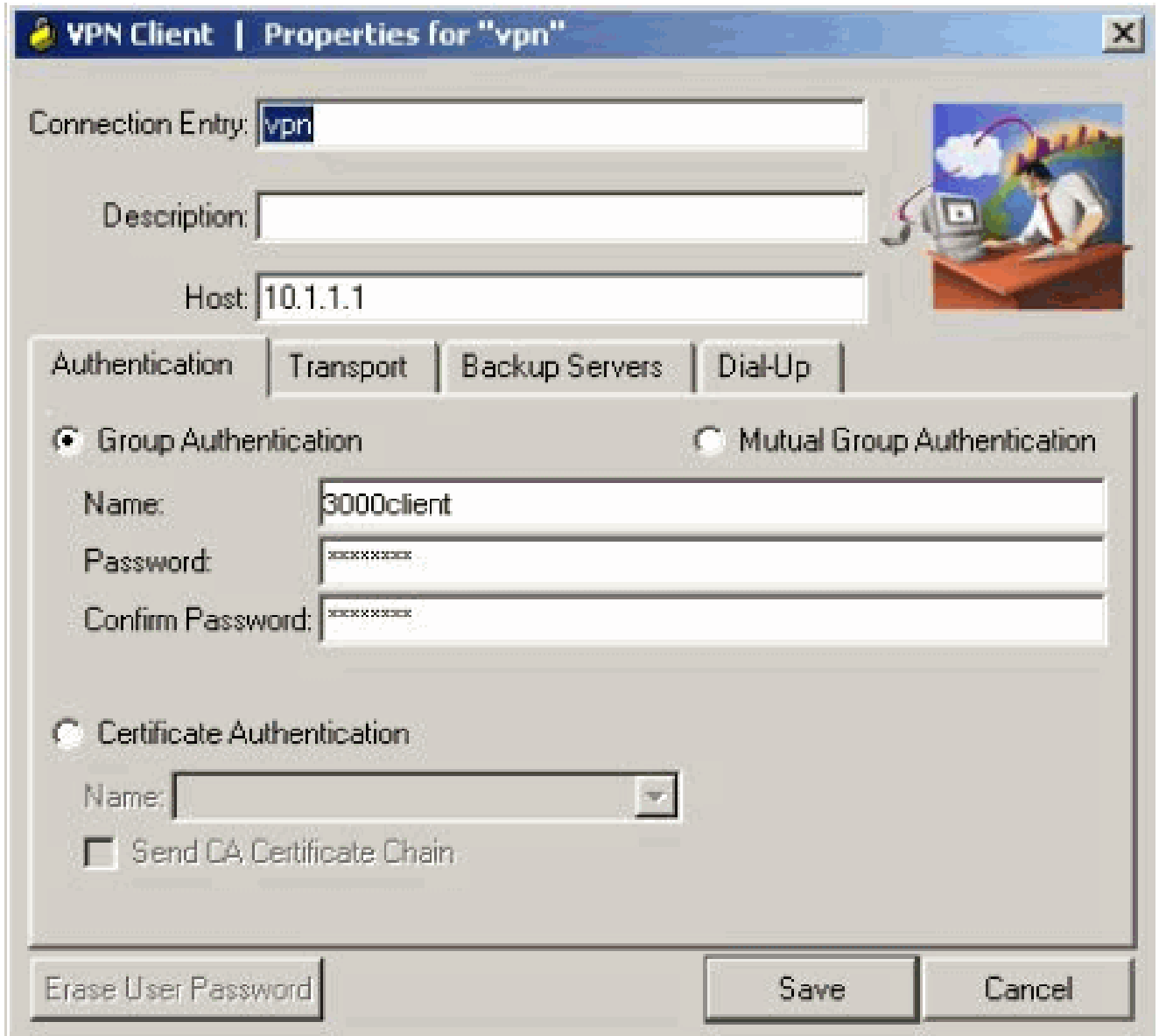
## VPN Client 4.8 컨피그레이션

VPN Client 4.8을 구성하려면 다음 단계를 완료하십시오.

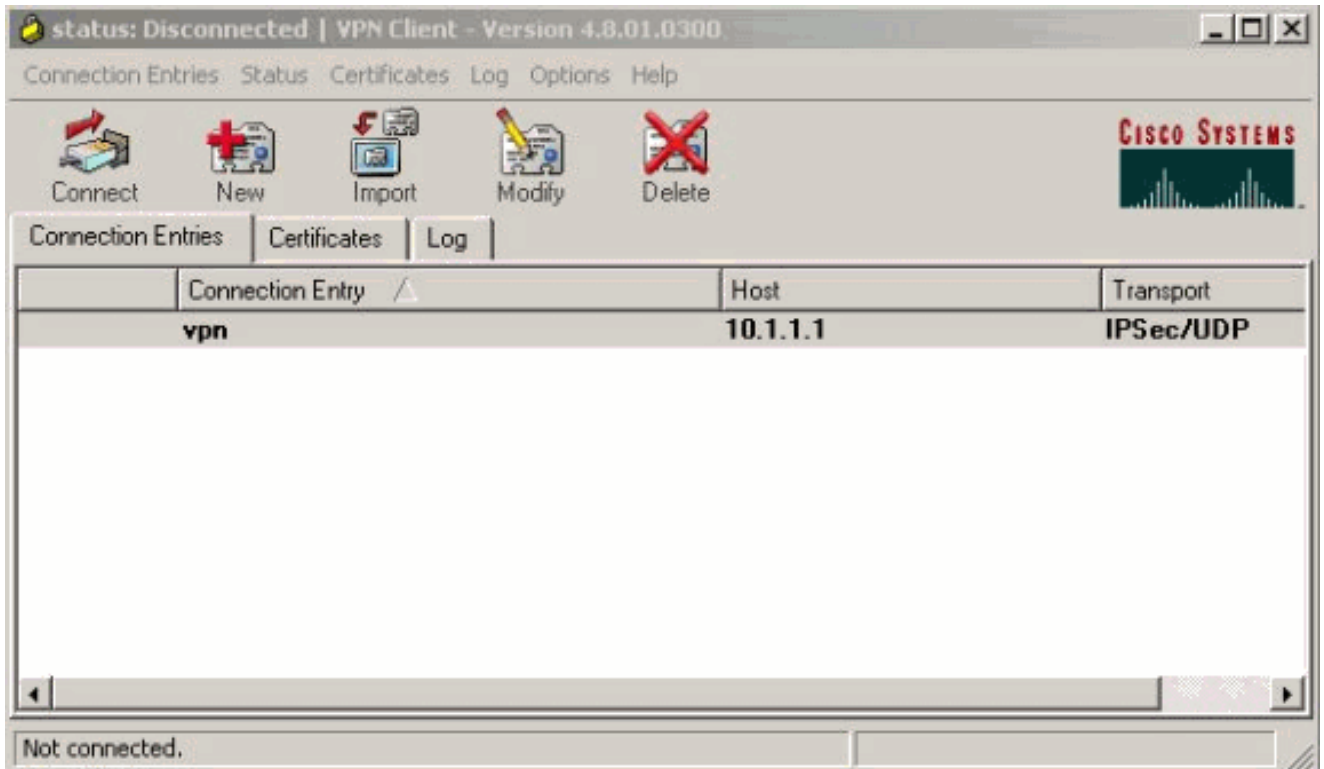
1. Start(시작) > Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > VPN Client(VPN 클라이언트)를 선택합니다.
2. Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창을 실행하려면 New(새로 만들기)를 클릭합니다.



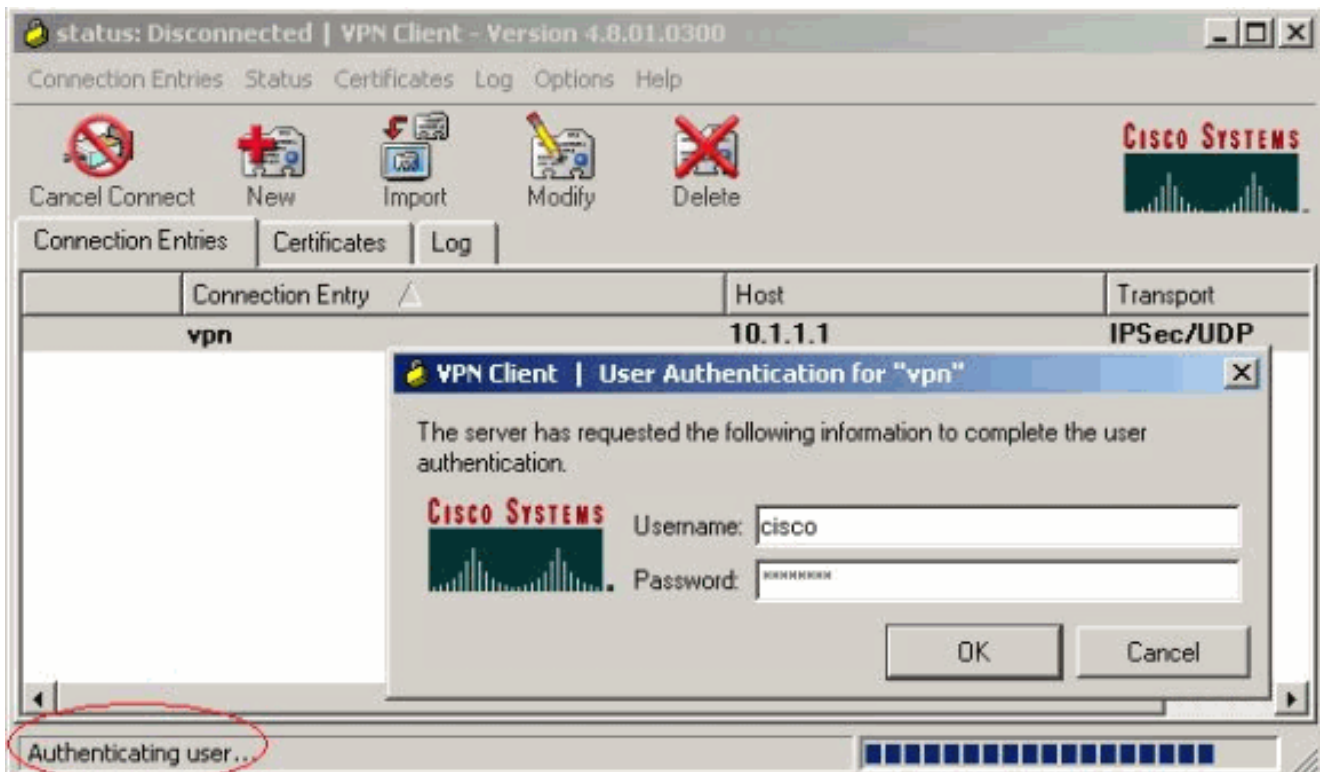
3. 설명과 함께 연결 항목의 이름을 입력합니다. Host(호스트) 상자에 라우터의 외부 IP 주소를 입력합니다. 그런 다음 VPN 그룹 이름과 비밀번호를 입력하고 Save(저장)를 클릭합니다.



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

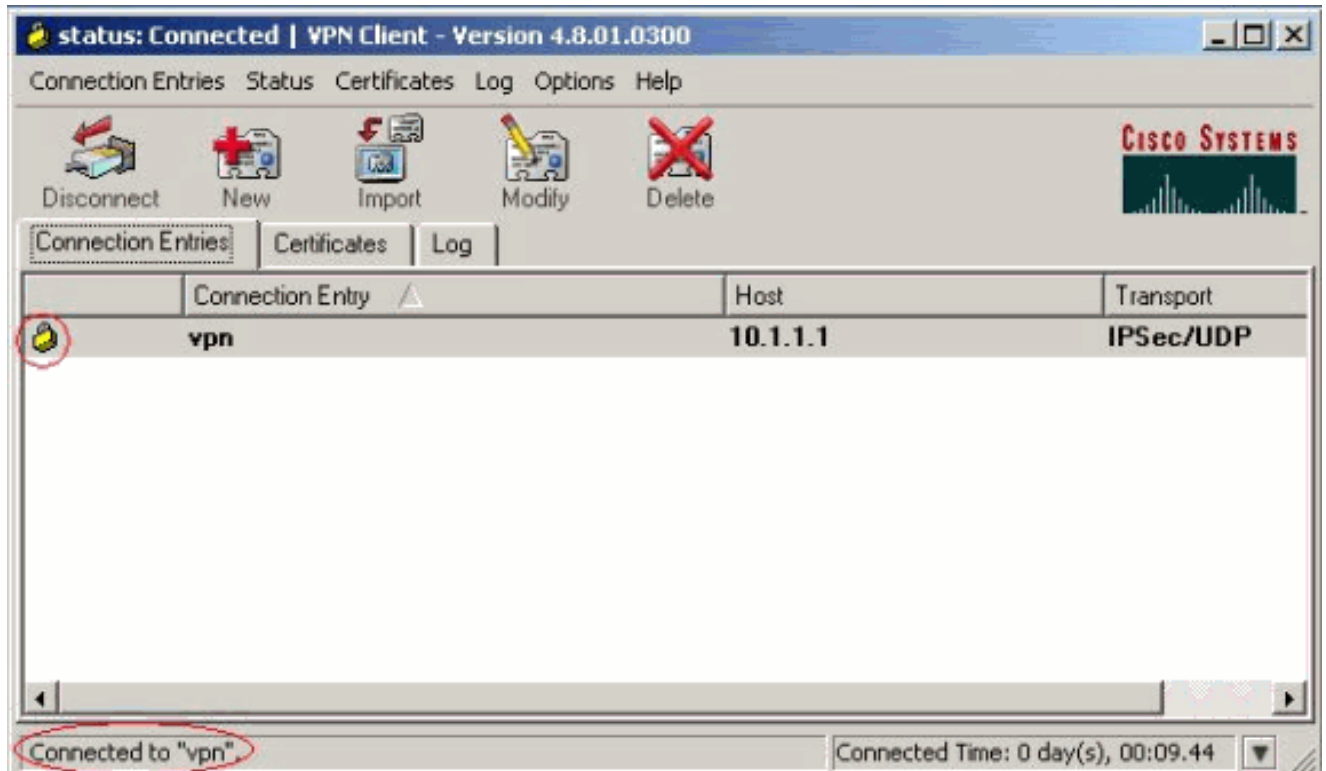


5. 프롬프트가 표시되면 xauth에 대한 사용자 이름 및 비밀번호 정보를 입력하고 OK를 클릭하여 원격 네트워크에 연결합니다.



VPN 클라이언트는 중앙 사이트의 라우터에 연결됩니다.





다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

```
<#root>
```

```
vpn2611#
```

```
show crypto isakmp sa
```

```
dst          src          state          conn-id  slot
10.1.1.1    10.0.0.1
QM_IDLE
          3          0
```

```
vpn2611#
```

```
show crypto ipsec sa interface: Ethernet0/0
```

```
  Crypto map tag: clientmap,
```

```
local addr. 10.1.1.1
```

```
  local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0)
```

```
current_peer: 10.0.0.1
```

```
  PERMIT, flags={}
```

```
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
```



#pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.0.0.1

path mtu 1500, media mtu 1500

current outbound spi: 77AFCCFA

inbound esp sas:

spi: 0xC7AC22AB(3349947051)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow\_id: 1, crypto map: clientmap

sa timing: remaining key lifetime (k/sec): (4608000/3444)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x77AFCCFA(2008009978)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2001, flow\_id: 2, crypto map: clientmap

sa timing: remaining key lifetime (k/sec): (4608000/3444)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0)

current\_peer: 10.0.0.1

PERMIT, flags={}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4

#pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.0.0.1

path mtu 1500, media mtu 1500

current outbound spi: 2EE5BF09

inbound esp sas:

spi: 0x3565451F(895829279)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2002, flow\_id: 3, crypto map: clientmap

sa timing: remaining key lifetime (k/sec): (4607999/3469)

IV size: 8 bytes

replay detection support: Y

```

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x2EE5BF09(786808585)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3469)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

```
vpn2611#
```

```
show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	0	0
2000	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	0	5
2001	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	5	0
2002	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	0	6
2003	Ethernet0/0	10.1.1.1	set	HMAC_SHA+3DES_56_C	4	0

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결합니다.

### 트러블슈팅 명령

debug 명령을 사용하기 전에 [debug 명령에 대한 중요한 정보](#)를 참조하십시오.

- debug crypto ipsec - IPSec 연결에 대한 디버그 정보를 표시합니다.
- debug crypto isakmp - IPSec 연결에 대한 디버그 정보를 표시하고, 양쪽 끝의 비호환성으로 인해 거부된 첫 번째 특성 집합을 표시합니다.
- debug crypto engine — 암호화 엔진의 정보를 표시합니다.
- debug aaa authentication(aaa 인증 디버그) - AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- debug aaa authorization radius(aaa 권한 부여 라디오) - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.
- debug radius - RADIUS 서버와 라우터 간의 통신 문제 해결에 대한 정보를 표시합니다.

### 디버그 출력

이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 라우터의 디버그 정보를 제공합니다.

## 라우터 로그

<#root>

vpn2611#

show debug

General OS:

AAA Authorization debugging is on  
Radius protocol debugging is on  
Radius packet protocol debugging is on

Cryptographic Subsystem:

Crypto ISAKMP debugging is on  
Crypto IPSEC debugging is on

vpn2611#

1w0d: ISAKMP (0:0): received packet from 10.0.0.1 (N) NEW SA

1w0d: ISAKMP: local port 500, remote port 500

1w0d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state

1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 from  
crypto\_ikmp\_config\_initialize\_sa, count 2

1w0d: ISAKMP (0:2): processing SA payload. message ID = 0

1w0d: ISAKMP (0:2): processing ID payload. message ID = 0

1w0d: ISAKMP (0:2): processing vendor id payload

1w0d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major

1w0d: ISAKMP (0:2): vendor ID is XAUTH

1w0d: ISAKMP (0:2): processing vendor id payload

1w0d: ISAKMP (0:2): vendor ID is DPD

1w0d: ISAKMP (0:2): processing vendor id payload

1w0d: ISAKMP (0:2): vendor ID is Unity

1w0d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy

1w0d: ISAKMP: encryption 3DES-CBC

1w0d: ISAKMP: hash SHA

1w0d: ISAKMP: default group 2

1w0d: ISAKMP: auth XAUTHInitPreShared

1w0d: ISAKMP: life type in seconds

1w0d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w0d: ISAKMP (0:2): atts are acceptable. Next payload is 3

1w0d: ISAKMP (0:2): processing KE payload. message ID = 0

1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 0

1w0d: ISAKMP (0:2): processing vendor id payload

1w0d: ISAKMP (0:2): processing vendor id payload

1w0d: ISAKMP (0:2): processing vendor id payload

1w0d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1

1w0d: AAA/MEMORY: create\_user (0x830CAF28) user='3000client' ruser='NULL'  
ds0=0 port='ISAKMP-ID-AUTH' rem\_addr='10.0.0.1' authen\_type=NONE  
service=LOGIN priv=0 initial\_task\_id='0'

1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_AM\_EXCH  
Old State = IKE\_READY New State = IKE\_R\_AM\_AAA\_AWAIT

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552):

Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET

1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(66832552) user='3000client'

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV service=ike

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV  
protocol=ipsec

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): found list  
"groupauthor"

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): Method=radius  
(radius)

1w0d: RADIUS: authenticating to get author data  
1w0d: RADIUS: ustruct sharecount=3  
1w0d: Radius: radius\_port\_info() success=0 radius\_nas\_port=1

1w0d: RADIUS: Send to ISAKMP-ID-AUTH id 60 172.18.124.96:1645,  
Access-Request, len 83

1w0d: RADIUS: authenticator AF EC D3 AD D6 39 4F 7D - A0 5E FC 64 F5 DE  
A7 3B  
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159  
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]

1w0d: RADIUS: User-Name [1] 12 "3000client"

1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"  
1w0d: RADIUS: User-Password [2] 18 \*  
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]

1w0d: RADIUS: Received from id 60 172.18.124.96:1645, Access-Accept, len  
176

1w0d: RADIUS: authenticator 52 BA 0A 38 AC C2 2B 6F - A0 77 64 93 D6 19  
78 CF  
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]  
1w0d: RADIUS: Vendor, Cisco [26] 30  
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"  
1w0d: RADIUS: Vendor, Cisco [26] 40  
1w0d: RADIUS: Cisco AVpair [1] 34 "ipsec:key-exchange=preshared-key"  
1w0d: RADIUS: Vendor, Cisco [26] 30  
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"  
1w0d: RADIUS: Vendor, Cisco [26] 23  
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inac1=108"  
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]  
1w0d: RADIUS: Tunnel-Password [69] 21 \*  
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83198648

1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"  
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"  
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"  
1w0d: RADIUS: cisco AVPair "ipsec:inac1=108"  
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09  
1w0d: RADIUS: TAS(1) created and enqueued.  
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123

1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,  
tunnel\_type=esp  
1w0d: RADIUS: free TAS(1)  
1w0d: AAA/AUTHOR (66832552): Post authorization status = PASS\_REPL  
1w0d: ISAKMP: got callback 1  
AAA/AUTHOR/IKE: Processing AV key-exchange=ike  
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key  
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool  
AAA/AUTHOR/IKE: Processing AV inac1=108  
AAA/AUTHOR/IKE: Processing AV tunnel-type\*esp  
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123  
AAA/AUTHOR/IKE: Processing AV tunnel-tag\*1  
1w0d: ISAKMP (0:2): SKEYID state generated

1w0d: ISAKMP (0:2): SA is doing pre-shared key authentication plus XAUTH using id type ID\_IPV4\_ADDR  
1w0d: ISAKMP (2): ID payload  
next-payload : 10  
type : 1  
protocol : 17  
port : 500  
length : 8  
1w0d: ISAKMP (2): Total payload length: 12  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) AG\_INIT\_EXCH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, PRESHARED\_KEY\_REPLY  
Old State = IKE\_R\_AM\_AAA\_AWAIT New State = IKE\_R\_AM2

1w0d: AAA/MEMORY: free\_user (0x830CAF28) user='3000client' ruser='NULL' port='ISAKMP-ID-AUTH' rem\_addr='10.0.0.1' authen\_type=NONE service=LOGIN priv=0  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) AG\_INIT\_EXCH  
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 0  
1w0d: ISAKMP (0:2): processing NOTIFY INITIAL\_CONTACT protocol 1 spi 0, message ID = 0, sa = 831938B0  
1w0d: ISAKMP (0:2): Process initial contact, bring down existing phase 1 and 2 SA's  
1w0d: ISAKMP (0:2): returning IP addr to the address pool: 10.16.20.1  
1w0d: ISAKMP (0:2): returning address 10.16.20.1 to pool  
1w0d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w0d: ISAKMP (0:2): SA has been authenticated with 10.0.0.1  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): purging node -1377537628  
1w0d: ISAKMP: Sending phase 1 responder lifetime 86400

1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_AM\_EXCH  
Old State = IKE\_R\_AM2 New State = IKE\_P1\_COMPLETE

1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(key\_engine\_delete\_sas): rec'd delete notify from ISAKMP  
1w0d: IPSEC(key\_engine\_delete\_sas): delete all SAs shared with 10.0.0.1  
1w0d: ISAKMP (0:2): Need XAUTH  
1w0d: AAA: parse name=ISAKMP idb type=-1 tty=-1  
1w0d: AAA/MEMORY: create\_user (0x830CAF28) user='NULL' ruser='NULL' ds0=0 port='ISAKMP' rem\_addr='10.0.0.1' authen\_type=ASCII service=LOGIN priv=0 initial\_task\_id='0'  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_INTERNAL, IKE\_PHASE1\_COMPLETE  
Old State = IKE\_P1\_COMPLETE New State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT

1w0d: ISAKMP: got callback 1  
1w0d: ISAKMP/xauth: request attribute XAUTH\_TYPE\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_MESSAGE\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_USER\_NAME\_V2  
1w0d: ISAKMP/xauth: request attribute XAUTH\_USER\_PASSWORD\_V2  
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID = -1021889193  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_START\_LOGIN  
Old State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT New State = IKE\_XAUTH\_REQ\_SENT

1w0d: ISAKMP (0:1): purging node 832238598  
1w0d: ISAKMP (0:1): purging node 1913225491  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.

message ID = -1021889193  
1w0d: ISAKMP: Config payload REPLY  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_TYPE\_V2 unexpected  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_USER\_NAME\_V2  
1w0d: ISAKMP/xauth: reply attribute XAUTH\_USER\_PASSWORD\_V2  
1w0d: ISAKMP (0:2): deleting node -1021889193 error FALSE reason "done with xauth request/reply exchange"  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_REPLY  
0ld State = IKE\_XAUTH\_REQ\_SENT New State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT

1w0d: RADIUS: ustruct sharecount=2  
1w0d: Radius: radius\_port\_info() success=0 radius\_nas\_port=1

1w0d: RADIUS: Send to ISAKMP id 61 172.18.124.96:1645, Access-Request, len 72

1w0d: RADIUS: authenticator 98 12 4F C0 DA B9 48 B8 - 58 00 BA 14 08 8E  
87 C0  
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159  
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]

1w0d: RADIUS: User-Name [1] 7 "cisco"

1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"  
1w0d: RADIUS: User-Password [2] 18 \*

1w0d: RADIUS: Received from id 61 172.18.124.96:1645, Access-Accept, len 26

1w0d: RADIUS: authenticator 00 03 F4 E1 9C 61 3F 03 - 54 83 E8 27 5C 6A  
7B 6E  
1w0d: RADIUS: Framed-IP-Address [8] 6 255.255.255.255  
1w0d: RADIUS: saved authorization data for user 830CAF28 at 830F89F8  
1w0d: ISAKMP: got callback 1  
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =  
-547189328  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_CONT\_LOGIN  
0ld State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT New State = IKE\_XAUTH\_SET\_SENT

1w0d: AAA/MEMORY: free\_user (0x830CAF28) user='cisco' ruser='NULL'  
port='ISAKMP' rem\_addr='10.0.0.1' authen\_type=ASCII service=LOGIN  
priv=0  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF\_XAUTH  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -547189328  
1w0d: ISAKMP: Config payload ACK  
1w0d: ISAKMP (0:2): XAUTH ACK Processed  
1w0d: ISAKMP (0:2): deleting node -547189328 error FALSE reason "done with transaction"  
1w0d: ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_ACK  
0ld State = IKE\_XAUTH\_SET\_SENT New State = IKE\_P1\_COMPLETE

1w0d: ISAKMP (0:2): Input = IKE\_MESG\_INTERNAL, IKE\_PHASE1\_COMPLETE  
0ld State = IKE\_P1\_COMPLETE New State = IKE\_P1\_COMPLETE

1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.  
message ID = -1911189201  
1w0d: ISAKMP: Config payload REQUEST  
1w0d: ISAKMP (0:2): checking request:  
1w0d: ISAKMP: IP4\_ADDRESS  
1w0d: ISAKMP: IP4\_NETMASK  
1w0d: ISAKMP: IP4\_DNS  
1w0d: ISAKMP: IP4\_NBNS  
1w0d: ISAKMP: ADDRESS\_EXPIRY

```
1w0d: ISAKMP: APPLICATION_VERSION
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
1w0d: ISAKMP: DEFAULT_DOMAIN
1w0d: ISAKMP: SPLIT_INCLUDE
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
1w0d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) user='3000client' ruser='NULL'
ds0=0 port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0 initial_task_id='0'
1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
0ld State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746):
Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3098118746)
user='3000client'
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV
service=ike
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV
protocol=ipsec
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): found list
"groupauthor"
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): Method=radius
(radius)
1w0d: RADIUS: authenticating to get author data
1w0d: RADIUS: ustruct sharecount=3
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1
1w0d: RADIUS: Send to ISAKMP-GROUP-AUTH id 62 172.18.124.96:1645,
Access-Request, len 83
1w0d: RADIUS: authenticator 32 C5 32 FF AB B7 E4 68 - 9A 68 5A DE D5 56
0C BE
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]
1w0d: RADIUS: User-Name [1] 12 "3000client"
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Received from id 62 172.18.124.96:1645, Access-Accept, len
176
1w0d: RADIUS: authenticator DF FA FE 21 07 92 4F 10 - 75 5E D6 96 66 70
19 27
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"
1w0d: RADIUS: Vendor, Cisco [26] 40
1w0d: RADIUS: Cisco AVpair [1] 34
"ipsec:key-exchange=preshared-key"
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inac1=108"
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83143E64
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inac1=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
```

```
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123
1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (3098118746): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inacl=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): attributes sent in message:
1w0d: Address: 0.2.0.0
1w0d: ISAKMP (0:2): allocating address 10.16.20.2
1w0d: ISAKMP: Sending private address: 10.16.20.2
1w0d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w0d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address:
86395
1w0d: ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork
Operating System Software
IOS (tm) C2600 Software (C2600-JK903S-M), Version 12.2(8)T, RELEASE
SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w0d: ISAKMP: Sending split include name 108 network 14.38.0.0 mask
255.255.0.0 protocol 0, src port 0, dst port 0

1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w0d: ISAKMP (0:2): responding to peer config from 10.0.0.1. ID =
-1911189201
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF_ADDR
1w0d: ISAKMP (0:2): deleting node -1911189201 error FALSE reason ""
1w0d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 132557281
1w0d: ISAKMP (0:2): processing SA payload. message ID = 132557281
1w0d: ISAKMP (0:2): Checking IPsec proposal 1
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
hmac_alg 1) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w0d: ISAKMP (0:2): Checking IPsec proposal 2
1w0d: ISAKMP: transform 1, ESP_3DES
```



1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 4, trans 3,  
hmac\_alg 0) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 3  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3,  
hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 4  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
  
1w0d: ISAKMP (0:2): atts are acceptable.  
  
1w0d: IPSEC(validate\_proposal\_request): proposal part #1,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1),  
remote\_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 132557281  
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281  
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281  
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(spi\_response): getting spi 245824456 for SA  
from 10.1.1.1 to 10.0.0.1 for prot 3  
1w0d: ISAKMP: received ke message (2/1)  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MSG\_FROM\_IPSEC,  
IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
  
1w0d: ISAKMP (0:2): Creating IPsec SAs  
1w0d: inbound SA from 10.0.0.1 to 10.1.1.1

(proxy 10.16.20.2 to 10.1.1.1)  
1w0d: has spi 0xEA6FBC8 and conn\_id 2000 and flags 4  
1w0d: lifetime of 2147483 seconds  
1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy  
10.1.1.1 to 10.16.20.2 )  
1w0d: has spi 1009463339 and conn\_id 2001 and flags C  
1w0d: lifetime of 2147483 seconds

1w0d: ISAKMP (0:2): deleting node 132557281 error FALSE reason "quick mode  
done (await())"  
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE\_MESG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_R\_QM2 New State = IKE\_QM\_PHASE2\_COMPLETE

1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(initialize\_sas): ,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),  
remote\_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 2147483s and 0kb,  
spi= 0xEA6FBC8(245824456), conn\_id= 2000, keysize= 0, flags= 0x4  
1w0d: IPSEC(initialize\_sas): ,  
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),  
remote\_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 2147483s and 0kb,  
spi= 0x3C2B302B(1009463339), conn\_id= 2001, keysize= 0, flags= 0xC  
1w0d: IPSEC(create\_sa): sa created,  
(sa) sa\_dest= 10.1.1.1, sa\_prot= 50,  
sa\_spi= 0xEA6FBC8(245824456),  
sa\_trans= esp-3des esp-sha-hmac , sa\_conn\_id= 2000  
1w0d: IPSEC(create\_sa): sa created,  
(sa) sa\_dest= 10.0.0.1, sa\_prot= 50,  
sa\_spi= 0x3C2B302B(1009463339),  
sa\_trans= esp-3des esp-sha-hmac , sa\_conn\_id= 2001  
1w0d: ISAKMP: received ke message (4/1)  
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 for  
crypto\_ikmp\_config\_handle\_kei\_mess, count 3  
1w0d: ISAKMP (0:1): purging SA., sa=83196748, delme=83196748  
1w0d: ISAKMP: Unlocking CONFIG struct 0x830BF118 on return of attributes,  
count 2  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): processing HASH payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): processing SA payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): Checking IPsec proposal 1  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3,  
hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): skipping next ANDed proposal (1)  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds

1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: ISAKMP (0:2): Checking IPsec proposal 2  
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 4, trans 3, hmac\_alg 0) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 3  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-MD5  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported  
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0  
1w0d: ISAKMP (0:2): Checking IPsec proposal 4  
1w0d: ISAKMP: transform 1, ESP\_3DES  
1w0d: ISAKMP: attributes in transform:  
1w0d: ISAKMP: authenticator is HMAC-SHA  
1w0d: ISAKMP: encaps is 1  
1w0d: ISAKMP: SA life type in seconds  
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B  
1w0d: ISAKMP (0:2): atts are acceptable.  
1w0d: IPSEC(validate\_proposal\_request): proposal part #  
vpn2611#1,  
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,  
local\_proxy= 14.38.0.0/255.255.0.0/0/0 (type=4),  
remote\_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-3des esp-sha-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908  
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec  
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE\_MESG\_FROM\_PEER,  
IKE\_QM\_EXCH  
Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE  
  
1w0d: IPSEC(key\_engine): got a queue event...  
1w0d: IPSEC(spi\_response): getting spi 593097454 for SA  
from 10.1.1.1 to 10.0.0.1  
vpn2611#  
vpn2611#2 for prot 3  
1w0d: ISAKMP: received ke message (2/1)  
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM\_IDLE  
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE\_MESG\_FROM\_IPSEC,  
IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
  
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM\_IDLE  
  
1w0d: ISAKMP (0:2): Creating IPsec SAs  
1w0d: inbound SA from 10.0.0.1 to 10.1.1.1  
(proxy 10.16.20.2 to 14.38.0.0)  
1w0d: has spi 0x2359F2EE and conn\_id 2002 and flags 4  
1w0d: lifetime of 2147483 seconds

```

1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy
14.38.0.0 to 10.16.20.2 )
1w0d: has spi 1123818858 and conn_id 2003 and flags C
1w0d: lifetime of 2147483 seconds

1w0d: ISAKMP (0:2): deleting node -1273332908 erro
vpn2611#un ar FALSE reason "quick mode done (await())"
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x2359F2EE(593097454), conn_id= 2002, keysize= 0, flags= 0x4
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sh11
All possible debugging has been turned off
vpn2611#a-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysize= 0, flags= 0xC
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0x2359F2EE(593097454),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2002
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.1, sa_prot= 50,
sa_spi= 0x42FC1D6A(1123818858),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003

```

## 클라이언트 로그

로그를 보기 위해 VPN 클라이언트에서 LogViewer를 시작합니다. 구성된 모든 클래스에 대해 필터가 High(높음)로 설정되어 있는지 확인합니다. 다음은 샘플 로그 출력입니다.

```

1 16:48:10.203 03/05/02 Sev=Info/6 DIALER/0x63300002
Initiating connection.

2 16:48:10.203 03/05/02 Sev=Info/4 CM/0x63100002
Begin connection process

3 16:48:10.223 03/05/02 Sev=Info/4 CM/0x63100004
Establish secure connection using Ethernet

4 16:48:10.223 03/05/02 Sev=Info/4 CM/0x63100026
Attempt connection with server "10.1.1.1"

5 16:48:10.223 03/05/02 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 10.1.1.1.

```

6 16:48:10.273 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 10.1.1.1

7 16:48:10.273 03/05/02 Sev=Info/4 IPSEC/0x63700014  
Deleted all keys

8 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x6300002F  
Received ISAKMP packet: peer = 10.1.1.1

9 16:48:10.994 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, KE, ID, NON, HASH)  
from 10.1.1.1

10 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059  
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

11 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000001  
Peer is a Cisco-Unity compliant peer

12 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059  
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

13 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000001  
Peer supports DPD

14 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059  
Vendor ID payload = 2D275A044215F48F531958AB2578EB2D

15 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059  
Vendor ID payload = 09002689DFD6B712

16 16:48:11.025 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK AG \*(HASH, NOTIFY:STATUS\_INITIAL\_CONTACT) to 10.1.1.1

17 16:48:11.045 03/05/02 Sev=Info/5 IKE/0x6300002F  
Received ISAKMP packet: peer = 10.1.1.1

18 16:48:11.045 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK INFO \*(HASH, NOTIFY:STATUS\_RESP\_LIFETIME)  
from 10.1.1.1

19 16:48:11.045 03/05/02 Sev=Info/5 IKE/0x63000044  
RESPONDER-LIFETIME notify has value of 86400 seconds

20 16:48:11.045 03/05/02 Sev=Info/5 IKE/0x63000046  
This SA has already been alive for 1 seconds,  
setting expiry to 86399 seconds from now

21 16:48:11.075 03/05/02 Sev=Info/5 IKE/0x6300002F  
Received ISAKMP packet: peer = 10.1.1.1

22 16:48:11.075 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 10.1.1.1

23 16:48:11.075 03/05/02 Sev=Info/4 CM/0x63100015  
Launch xAuth application

24 16:48:14.920 03/05/02 Sev=Info/4 CM/0x63100017  
xAuth application returned

25 16:48:14.920 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 10.1.1.1

26 16:48:14.990 03/05/02 Sev=Info/5 IKE/0x6300002F  
Received ISAKMP packet: peer = 10.1.1.1

27 16:48:14.990 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 10.1.1.1

28 16:48:14.990 03/05/02 Sev=Info/4 CM/0x6310000E  
Established Phase 1 SA. 1 Phase 1 SA in the system

29 16:48:15.000 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 10.1.1.1

30 16:48:15.010 03/05/02 Sev=Info/5 IKE/0x6300005D  
Client sending a firewall request to concentrator

31 16:48:15.010 03/05/02 Sev=Info/5 IKE/0x6300005C  
Firewall Policy: Product=Cisco Integrated Client,  
Capability= (Centralized Policy Push).

32 16:48:15.010 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 10.1.1.1

33 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300002F  
Received ISAKMP packet: peer = 10.1.1.1

34 16:48:15.141 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 10.1.1.1

35 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x63000010  
MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_ADDRESS: , value = 10.16.20.2

36 16:48:15.141 03/05/02 Sev=Info/5 IKE/0xA3000017  
MODE\_CFG\_REPLY: The received (INTERNAL\_ADDRESS\_EXPIRY) attribute and value  
(86395) is not supported

37 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300000E  
MODE\_CFG\_REPLY: Attribute = APPLICATION\_VERSION, value = Cisco Internetwork  
Operating System Software IOS (tm) C2600 Software (C2600-JK903S-M),  
Version 12.2(8)T, RELEASE SOFTWARE (fc2)  
TAC Support: <http://www.cisco.com/tac>  
Copyright (c) 1986-2002 by cisco Systems, Inc.  
Compiled Thu 14-Feb-02 16:50 by ccai

38 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300000D  
MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SPLIT\_INCLUDE (# of split\_nets),  
value = 0x00000001

39 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300000F  
SPLIT\_NET #1  
subnet = 172.18.124.0  
mask = 255.255.255.0  
protocol = 0  
src port = 0  
dest port=0

40 16:48:15.141 03/05/02 Sev=Info/4 CM/0x63100019  
Mode Config data received

41 16:48:15.151 03/05/02 Sev=Info/5 IKE/0x63000055  
Received a key request from Driver for IP address 10.1.1.1,  
GW IP = 10.1.1.1

42 16:48:15.151 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID, ID) to 10.1.1.1

43 16:48:15.361 03/05/02 Sev=Info/4 IPSEC/0x63700014  
Deleted all keys

44 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x6300002F  
Received ISAKMP packet: peer = 10.1.1.1

45 16:48:15.461 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK QM \*(HASH, SA, NON, ID, ID,  
NOTIFY:STATUS\_RESP\_LIFETIME) from 10.1.1.1

46 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000044  
RESPONDER-LIFETIME notify has value of 3600 seconds

47 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000045  
RESPONDER-LIFETIME notify has value of 4608000 kb

48 16:48:15.461 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK QM \*(HASH) to 10.1.1.1

49 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000058  
Loading IPsec SA (Message ID = 0x07E6A9E1 OUTBOUND SPI = 0x0EA6FBC8  
INBOUND SPI = 0x3C2B302B)

50 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000025  
Loaded OUTBOUND ESP SPI: 0x0EA6FBC8

51 16:48:15.471 03/05/02 Sev=Info/5 IKE/0x63000026  
Loaded INBOUND ESP SPI: 0x3C2B302B

52 16:48:15.471 03/05/02 Sev=Info/4 CM/0x6310001A  
One secure connection established

53 16:48:15.511 03/05/02 Sev=Info/6 DIALER/0x63300003  
Connection established.

54 16:48:15.581 03/05/02 Sev=Info/6 DIALER/0x63300008  
MAPI32 Information - Outlook not default mail client

55 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x63700010  
Created a new key structure

56 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x6370000F  
Added key with SPI=0xc8fba60e into key list

57 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x63700010  
Created a new key structure

58 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x6370000F  
Added key with SPI=0x2b302b3c into key list

59 16:48:26.357 03/05/02 Sev=Info/5 IKE/0x63000055  
Received a key request from Driver for IP address 172.18.124.159,  
GW IP = 10.1.1.1

60 16:48:26.357 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID, ID) to 10.1.1.1

61 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x6300002F

Received ISAKMP packet: peer = 10.1.1.1

62 16:48:26.668 03/05/02 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK QM \*(HASH, SA, NON, ID, ID,  
NOTIFY:STATUS\_RESP\_LIFETIME) from 10.1.1.1

63 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000044  
RESPONDER-LIFETIME notify has value of 3600 seconds

64 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000045  
RESPONDER-LIFETIME notify has value of 4608000 kb

65 16:48:26.668 03/05/02 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK QM \*(HASH) to 10.1.1.1

66 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000058  
Loading IPsec SA (Message ID = 0xB41A7B54 OUTBOUND SPI = 0x2359F2EE  
INBOUND SPI = 0x42FC1D6A)

67 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000025  
Loaded OUTBOUND ESP SPI: 0x2359F2EE

68 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000026  
Loaded INBOUND ESP SPI: 0x42FC1D6A

69 16:48:26.668 03/05/02 Sev=Info/4 CM/0x63100022  
Additional Phase 2 SA established.

## 관련 정보

- [IPSec 협상/IKE 프로토콜 지원](#)
- [코멘트 요청\(RFC\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.