

VPN 클라이언트를 사용하여 TACACS+ 및 RADIUS 확장 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[VPN 클라이언트 1.1 설정](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[디버그 출력 샘플](#)

[관련 정보](#)

소개

이 문서에서는 TACACS+ 및 RADIUS IETF(Internet Engineering Task Force) Extended Authentication(Xauth)에 대한 샘플 컨피그레이션을 보여줍니다. Xauth를 사용하면 TACACS+ 또는 RADIUS를 IKE(Internet Key Exchange) 프로토콜 내의 사용자 인증 방법으로 사용하여 VPN(Virtual Private Networks)에 IPsec(IP Security)을 구축할 수 있습니다. 이 기능은 CiscoSecure VPN Client 1.1이 PC에 설치되어 있는 사용자에게 사용자 이름과 비밀번호를 묻는 메시지를 표시한 다음 AAA(Authentication, Authorization, and Accounting) 서버, TACACS+ 또는 RADIUS 데이터베이스에 저장된 정보로 인증을 제공합니다. 인증은 IKE 1단계와 IKE 2단계 사이에 발생합니다. 사용자가 성공적으로 인증하면 2단계 SA(보안 연결)가 설정되고, 그 후에 보호된 네트워크로 안전하게 데이터를 전송할 수 있습니다.

Xauth에는 인증만 포함되며 권한은 부여되지 않습니다(연결이 설정되면 사용자가 이동할 수 있음). 계정(사용자가 이동한 경우)은 구현되지 않습니다.

Xauth를 구현하기 전에 Xauth 없이 컨피그레이션이 작동해야 합니다. 이 예에서는 Xauth 외에 Mode Configuration(Mode Config) 및 NAT(Network Address Translation)를 보여 주지만, Xauth 명령을 추가하기 전에 IPsec 연결이 있다고 가정합니다.

TACACS+ 또는 RADIUS Xauth를 시도하기 전에 로컬 Xauth(라우터의 사용자 이름/비밀번호)가 작동하는지 확인합니다.

[사전 요구 사항](#)

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN 클라이언트 버전 1.1 이상
- Cisco IOS[®] 릴리스 12.1.2.2.T, 12.1.2.2.P(이상)
- RADIUS 인증은 c3640-jo3s56i-mz.121-2.3.T를 실행하는 Cisco 3640에서 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 규칙](#)을 참조하십시오.

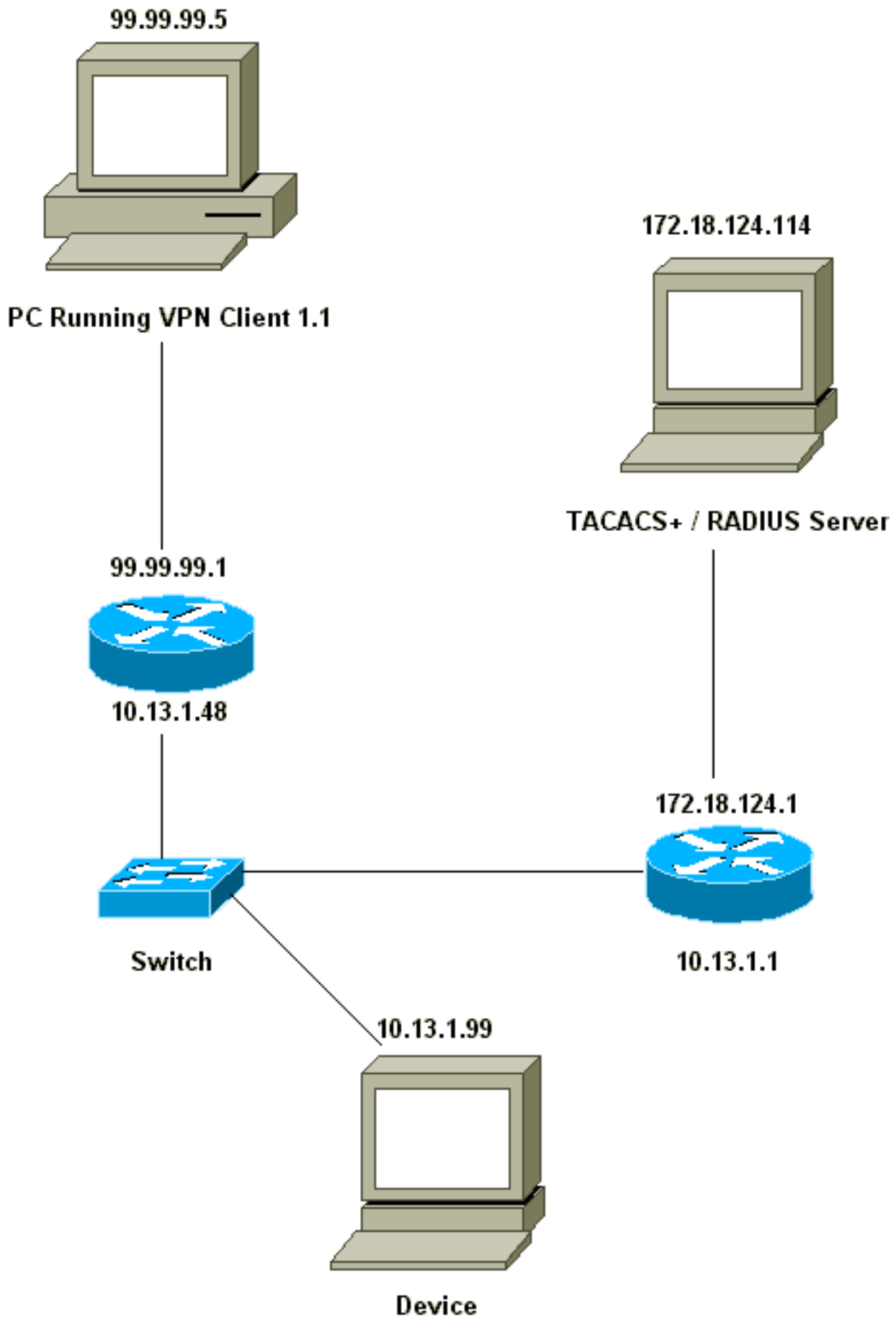
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



[VPN 클라이언트 1.1 설정](#)

Network Security policy:

1- Myconn

My Identity = ip address

Connection security: Secure

Remote Party Identity and addressing

ID Type: IP subnet

10.13.1.0 (range of inside network)

Port all Protocol all

Connect using secure tunnel

ID Type: IP address

99.99.99.1

Pre-shared key = cisco1234

Authentication (Phase 1)

Proposal 1

Authentication method: pre-shared key

Encryp Alg: DES

Hash Alg: MD5

SA life: Unspecified

Key Group: DH 1

Key exchange (Phase 2)

Proposal 1

Encapsulation ESP

Encrypt Alg: DES

Hash Alg: MD5

Encap: tunnel

SA life: Unspecified

no AH

2- Other Connections

Connection security: Non-secure

Local Network Interface

Name: Any

IP Addr: Any

Port: All

라우터에서 Xauth를 활성화하면 사용자가 라우터 내의 디바이스에 연결을 시도할 때(여기서는 ping -t #.#.#) 회색 화면이 나타납니다.

User Authentication for 3660

Username:

Password:

구성

서버 구성

Xauth 인증은 TACACS+ 또는 RADIUS를 통해 수행할 수 있습니다. Xauth 사용자가 Xauth를 수행할 수 있지만 라우터에 텔넷하는 것은 허용되지 않았는지 확인하고자 **aaa authorization exec** 명령을 추가했습니다. RADIUS 사용자에게 "reply-attribute Service-Type=Outbound=5"(Administrative 또는 Login 대신)를 제공했습니다. CiscoSecure UNIX에서는 "아웃바운드", CiscoSecure NT의 "Dialout Framed"입니다. 이러한 사용자가 TACACS+ 사용자인 경우 셸/exec 권한을 부여하지 않습니다.

TACACS+ 또는 RADIUS Xauth에 대한 라우터 컨피그레이션

Current configuration:

```
!  
version 12.1  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname carter  
!  
!--- Enable AAA and define authentication and  
authorization parameters aaa new-model  
aaa authentication login default group radius|tacacs+  
none  
aaa authentication login xauth_list group radius|tacacs+  
aaa authorization exec default group radius|tacacs+ none  
enable secret 5 $1$VY18$uO2CRnqUzugV0NYtd14Gg0  
enable password ww  
!  
username john password 0 doe  
!  
ip subnet-zero  
ip audit notify log  
ip audit po max-events 100  
cns event-service server  
!  
crypto isakmp policy 10  
hash md5  
authentication pre-share  
crypto isakmp key cisco1234 address 0.0.0.0 0.0.0.0  
crypto isakmp client configuration address-pool local  
ourpool  
!  
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac  
!  
crypto dynamic-map dyna 10  
set transform-set mypolicy  
!  
crypto map test client authentication list xauth_list  
crypto map test client configuration address initiate  
crypto map test client configuration address respond  
crypto map test 5 ipsec-isakmp dynamic dyna  
!  
interface Ethernet0/0  
ip address 10.13.1.48 255.255.255.0  
ip nat inside  
no ip route-cache  
no ip mroute-cache  
no mop enabled  
!  
interface TokenRing0/0  
no ip address  
shutdown  
ring-speed 16  
!  
interface Ethernet2/0  
ip address 99.99.99.1 255.255.255.0  
ip nat outside  
no ip route-cache  
no ip mroute-cache  
no mop enabled  
crypto map test  
!  
interface TokenRing2/0  
no ip address  
shutdown
```

```
ring-speed 16
!
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 99.99.99.50 99.99.99.60 netmask
255.255.255.0
ip nat inside source route-map nonat pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 10.13.1.1
no ip http server
!
access-list 101 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
access-list 101 permit ip 10.13.1.0 0.0.0.255 any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
match ip address 101
!
!--- Define TACACS server host and key parameters
tacacs-server host 172.18.124.114
tacacs-server key cisco
radius-server host 172.18.124.114 auth-port 1645 acct-
port 1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password WW
!
end
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug 명령을 사용하기 전에 디버그 [명령에 대한 중요 정보](#)를 참조하십시오.

- **debug aaa authentication**—AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.
- **debug crypto ipsec** - IPSec 이벤트를 표시합니다.
- **debug crypto key-exchange** - DSS(Digital Signature Standard) 공개 키 교환 메시지를 표시합니다.
- **debug radius** - RADIUS와 관련된 정보를 표시합니다.

- **debug tacacs** - TACACS와 관련된 정보를 표시합니다.
- **clear crypto isakmp** - 지울 연결을 지정합니다.
- **clear crypto sa** - IPSec 보안 연결을 삭제합니다.

디버그 출력 샘플

참고: TACACS+ 디버그는 매우 유사합니다. **debug radius** 명령 대신 **debug tacacs+** 명령을 사용합니다.

```
Carter#show debug
General OS:
  AAA Authentication debugging is on
  Radius protocol debugging is on
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
Carter#term mon
03:12:54: ISAKMP (0:0): received packet from 99.99.99.5 (N) NEW SA
03:12:54: ISAKMP: local port 500, remote port 500
03:12:54: ISAKMP (0:1): Setting client config settings 6269C36C
03:12:54: ISAKMP (0:1): (Re)Setting client xauth list xauth_list
  and state
03:12:54: ISAKMP: Created a peer node for 99.99.99.5
03:12:54: ISAKMP: Locking struct 6269C36C from
  crypto_ikmp_config_initialize_sa
03:12:54: ISAKMP (0:1): processing SA payload. message ID = 0
03:12:54: ISAKMP (0:1): found peer pre-shared key matching 99.99.99.5
03:12:54: ISAKMP (0:1): Checking ISAKMP transform 1 against
  priority 10 policy
03:12:54: ISAKMP:      encryption DES-CBC
03:12:54: ISAKMP:      hash MD5
03:12:54: ISAKMP:      default group 1
03:12:54: ISAKMP:      auth pre-share
03:12:54: ISAKMP (0:1): atts are acceptable. Next payload is 0
03:12:54: CryptoEngine0: generate alg parameter
03:12:54: CRYPTO_ENGINE: Dh phase 1 status: 0
03:12:54: CRYPTO_ENGINE: DH phase 1 status: 0
03:12:54: ISAKMP (0:1): SA is doing pre-shared key authentication using
  id type ID_IPV4_ADDR
03:12:54: ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_SA_SETUP
03:12:54: ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_SA_SETUP
03:12:54: ISAKMP (0:1): processing KE payload. Message ID = 0
03:12:54: CryptoEngine0: generate alg parameter
03:12:54: ISAKMP (0:1): processing NONCE payload. Message ID = 0
03:12:54: ISAKMP (0:1): found peer pre-shared key matching 99.99.99.5
03:12:54: CryptoEngine0: create ISAKMP SKEYID for conn id 1
03:12:54: ISAKMP (0:1): SKEYID state generated
03:12:54: ISAKMP (0:1): processing vendor id payload
03:12:54: ISAKMP (0:1): processing vendor id payload
03:12:54: ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_KEY_EXCH
03:12:55: ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_KEY_EXCH
03:12:55: ISAKMP (0:1): processing ID payload. Message ID = 0
03:12:55: ISAKMP (0:1): processing HASH payload. Message ID = 0
03:12:55: CryptoEngine0: generate hmac context for conn id 1
03:12:55: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
  spi 0, message ID = 0
03:12:55: ISAKMP (0:1): SA has been authenticated with 99.99.99.5
03:12:55: ISAKMP (1): ID payload
  next-payload : 8
```

```
type          : 1
protocol      : 17
port         : 500
length       : 8
03:12:55: ISAKMP (1): Total payload length: 12
03:12:55: CryptoEngine0: generate hmac context for conn id 1
03:12:55: CryptoEngine0: clear DH number for conn id 1
03:12:55: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:12:55: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:12:55: ISAKMP (0:1): (Re)Setting client xauth list
xauth_list and state
03:12:55: ISAKMP (0:1): Need XAUTH
03:12:55: AAA: parse name=ISAKMP idb type=-1 tty=-1
03:12:55: AAA/MEMORY: create_user (0x6269AD80) user='' ruser=''
port='ISAKMP' rem_addr='99.99.99.5' authen_type=ASCII
service=LOGIN priv=0
03:12:55: AAA/AUTHEN/START (2289801324): port='ISAKMP'
list='xauth_list' action=LOGIN service=LOGIN
03:12:55: AAA/AUTHEN/START (2289801324): found list xauth_list
03:12:55: AAA/AUTHEN/START (2289801324): Method=radius (radius)
03:12:55: AAA/AUTHEN (2289801324): status = GETUSER
03:12:55: ISAKMP: got callback 1
03:12:55: ISAKMP/xauth: request attribute XAUTH_TYPE
03:12:55: ISAKMP/xauth: request attribute XAUTH_MESSAGE
03:12:55: ISAKMP/xauth: request attribute XAUTH_USER_NAME
03:12:55: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
03:12:55: CryptoEngine0: generate hmac context for conn id 1
03:12:55: ISAKMP (0:1): initiating peer config to 99.99.99.5.
ID = -280774539
03:12:55: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:00: ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH
-280774539 ...
03:13:00: ISAKMP (0:1): incrementing error counter on sa:
retransmit phase 2
03:13:00: ISAKMP (0:1): incrementing error counter on sa:
retransmit phase 2
03:13:00: ISAKMP (0:1): retransmitting phase 2 -280774539 CONF_XAUTH
03:13:00: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:02: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:13:02: ISAKMP (0:1): processing transaction payload from
99.99.99.5. Message ID = -280774539
03:13:02: CryptoEngine0: generate hmac context for conn id 1
03:13:02: ISAKMP: Config payload REPLY
03:13:02: ISAKMP/xauth: reply attribute XAUTH_TYPE
03:13:02: ISAKMP/xauth: reply attribute XAUTH_USER_NAME
03:13:02: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD
03:13:02: AAA/AUTHEN/CONT (2289801324): continue_login (user='(undef)')
03:13:02: AAA/AUTHEN (2289801324): status = GETUSER
03:13:02: AAA/AUTHEN (2289801324): Method=radius (radius)
03:13:02: AAA/AUTHEN (2289801324): status = GETPASS
03:13:02: AAA/AUTHEN/CONT (2289801324): continue_login (user='zeke')
03:13:02: AAA/AUTHEN (2289801324): status = GETPASS
03:13:02: AAA/AUTHEN (2289801324): Method=radius (radius)
03:13:02: RADIUS: ustruct sharecount=2
03:13:02: RADIUS: Initial Transmit ISAKMP id 29 172.18.124.114:1645,
Access-Request, len 68
03:13:02: Attribute 4 6 0A0D0130
03:13:02: Attribute 61 6 00000000
03:13:02: Attribute 1 6 7A656B65
03:13:02: Attribute 31 12 39392E39
03:13:02: Attribute 2 18 D687A79D
03:13:02: RADIUS: Received from id 29 172.18.124.114:1645,
Access-Accept, Len 26
03:13:02: Attribute 6 6 00000005
```


03:13:02: RADIUS: saved authorization data for user 6269AD80
at 62634D0C
03:13:02: AAA/AUTHEN (2289801324): status = PASS
03:13:02: ISAKMP: got callback 1
03:13:02: CryptoEngine0: generate hmac context for conn id 1
03:13:02: ISAKMP (0:1): initiating peer config to 99.99.99.5.
ID = -280774539
03:13:02: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:03: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:13:03: ISAKMP (0:1): processing transaction payload from 99.99.99.5.
Message ID = -280774539
03:13:03: CryptoEngine0: generate hmac context for conn id 1
03:13:03: ISAKMP: Config payload ACK
03:13:03: ISAKMP (0:1): deleting node -280774539 error FALSE
reason "done with transaction"
03:13:03: ISAKMP (0:1): allocating address 10.2.1.2
03:13:03: CryptoEngine0: generate hmac context for conn id 1
03:13:03: ISAKMP (0:1): initiating peer config to 99.99.99.5.
ID = 2130856112
03:13:03: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_ADDR
03:13:03: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_ADDR
03:13:03: ISAKMP (0:1): processing transaction payload
from 99.99.99.5. Message ID = 2130856112
03:13:03: CryptoEngine0: generate hmac context for conn id 1
03:13:03: ISAKMP: Config payload ACK
03:13:03: ISAKMP (0:1): peer accepted the address!
03:13:03: ISAKMP (0:1): adding static route for 10.2.1.2
03:13:03: ISAKMP (0:1): installing route 10.2.1.2 255.255.255.255
99.99.99.5
03:13:03: ISAKMP (0:1): deleting node 2130856112 error FALSE
reason "done with transaction"
03:13:03: ISAKMP (0:1): Delaying response to QM request.
03:13:04: ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE
03:13:04: ISAKMP (0:1): (Re)Setting client xauth list xauth_list
and state
03:13:04: CryptoEngine0: generate hmac context for conn id 1
03:13:04: ISAKMP (0:1): processing HASH payload. Message ID = -1651205463
03:13:04: ISAKMP (0:1): processing SA payload. Message ID = -1651205463
03:13:04: ISAKMP (0:1): Checking IPsec proposal 1
03:13:04: ISAKMP: transform 1, ESP_DES
03:13:04: ISAKMP: attributes in transform:
03:13:04: ISAKMP: authenticator is HMAC-MD5
03:13:04: ISAKMP: encaps is 1
03:13:04: validate proposal 0
03:13:04: ISAKMP (0:1): atts are acceptable.
03:13:04: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 99.99.99.1, src= 99.99.99.5,
dest_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.2.1.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= ESP-Des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
03:13:04: validate proposal request 0
03:13:04: ISAKMP (0:1): processing NONCE payload.
Message ID = -1651205463
03:13:04: ISAKMP (0:1): processing ID payload.
Message ID = -1651205463
03:13:04: ISAKMP (1): ID_IPV4_ADDR src 10.2.1.2 prot 0 port 0
03:13:04: ISAKMP (0:1): processing ID payload.
Message ID = -1651205463
03:13:04: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 10.13.1.0/255.255.255.0
port 0 port 0
03:13:04: ISAKMP (0:1): asking for 1 spis from ipsec
03:13:04: IPSEC(key_engine): got a queue event...

```
03:13:04: IPSEC(spi_response): getting spi 570798685 for SA
    from 99.99.99.5      to 99.99.99.1      for prot 3
03:13:04: ISAKMP: received ke message (2/1)
03:13:04: CryptoEngine0: generate hmac context for conn id 1
03:13:04: ISAKMP (0:1): sending packet to 99.99.99.5 (R) QM_IDLE
03:13:04: ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE
03:13:04: CryptoEngine0: generate hmac context for conn id 1
03:13:04: ipsec allocate flow 0
03:13:04: ipsec allocate flow 0
03:13:04: ISAKMP (0:1): Creating IPsec SAs
03:13:04:      inbound SA from 99.99.99.5 to 99.99.99.1
    (proxy 10.2.1.2 to 10.13.1.0)
03:13:04:      has spi 0x2205B25D and conn_id 2000 and flags 4
03:13:04:      outbound SA from 99.99.99.1 to 99.99.99.5
    (proxy 10.13.1.0 to 10.2.1.2)
03:13:04:      has spi -1338747879 and conn_id 2001 and flags 4
03:13:04: ISAKMP (0:1): deleting node -195511155 error FALSE
    reason "saved qm no longer needed"
03:13:04: ISAKMP (0:1): deleting node -1651205463 error FALSE
    reason "quick mode done (await())"
03:13:04: IPSEC(key_engine): got a queue event...
03:13:04: IPSEC(initialize_sas): ,
    (key eng. msg.) dest= 99.99.99.1, src= 99.99.99.5,
    dest_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x2205B25D(570798685), conn_id= 2000,
    keysize= 0, flags= 0x4
03:13:04: IPSEC(initialize_sas): ,
    (key eng. msg.) src= 99.99.99.1, dest= 99.99.99.5,
    src_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xB0345419(2956219417), conn_id= 2001,
    keysize= 0, flags= 0x4
03:13:04: IPSEC(create_sa): sa created,
    (sa) sa_dest= 99.99.99.1, sa_prot= 50,
    sa_spi= 0x2205B25D(570798685),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
03:13:04: IPSEC(create_sa): sa created,
    (sa) sa_dest= 99.99.99.5, sa_prot= 50,
    sa_spi= 0xB0345419(2956219417),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
03:13:04: ISAKMP: received ke message (4/1)
03:13:04: ISAKMP: Locking struct 6269C36C for IPSEC
03:13:05: IPSEC(decapsulate): error in decapsulation
    crypto_ipsec_sa_exists
```

[관련 정보](#)

- [Cisco VPN 클라이언트 지원 페이지](#)
- [IPSec 협상/IKE 프로토콜 지원 페이지](#)
- [TACACS+\(Terminal Access Controller Access Control System\) 지원 페이지](#)
- [원격 인증 RADIUS\(Dial-In User Service\) 지원 페이지](#)
- [의견 요청](#)
- [기술 지원 및 문서 - Cisco Systems](#)