

# Configurazione dell'autenticazione estesa TACACS+ e RADIUS con il client VPN

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Installazione di VPN Client 1.1](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Output di esempio del comando debug](#)

[Informazioni correlate](#)

## Introduzione

In questo documento vengono illustrate configurazioni di esempio per l'autenticazione estesa TACACS+ e RADIUS Internet Engineering Task Force (IETF) (Xauth). Xauth consente di distribuire la protezione IP (IPSec) sulle reti VPN (Virtual Private Network) utilizzando TACACS+ o RADIUS come metodo di autenticazione dell'utente all'interno del protocollo IKE (Internet Key Exchange). Questa funzionalità consente l'autenticazione degli utenti che hanno installato Cisco Secure VPN Client 1.1 sul proprio PC. A tale scopo, gli utenti devono immettere un nome utente e una password e quindi verificare le informazioni memorizzate nel server di autenticazione, autorizzazione e accounting (AAA), nel database TACACS+ o RADIUS. L'autenticazione viene eseguita tra la fase 1 di IKE e la fase 2 di IKE. Se l'autenticazione viene eseguita correttamente, viene stabilita un'associazione di sicurezza (SA) di fase 2 dopo la quale i dati possono essere inviati in modo sicuro alla rete protetta.

Xauth include solo l'*autenticazione*, non l'*autorizzazione* (dove gli utenti possono andare una volta stabilita la connessione). L'*accounting* (dove sono stati utilizzati gli utenti) non è implementato.

La configurazione deve funzionare senza Xauth prima di implementare Xauth. Nell'esempio viene illustrata la configurazione della modalità (configurazione della modalità) e Network Address Translation (NAT) oltre a Xauth, ma si presume che sia presente la connettività IPSec prima di aggiungere i comandi Xauth.

Verificare il funzionamento di Xauth locale (nome utente/password sul router) prima di provare TACACS+ o RADIUS Xauth.

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- VPN Client versione 1.1 (o successiva)
- Cisco IOS<sup>®</sup> release 12.1.2.2.T, 12.1.2.2.P (o successive)
- L'autenticazione RADIUS è stata testata con Cisco 3640 con c3640-jo3s56i-mz.121-2.3.T

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

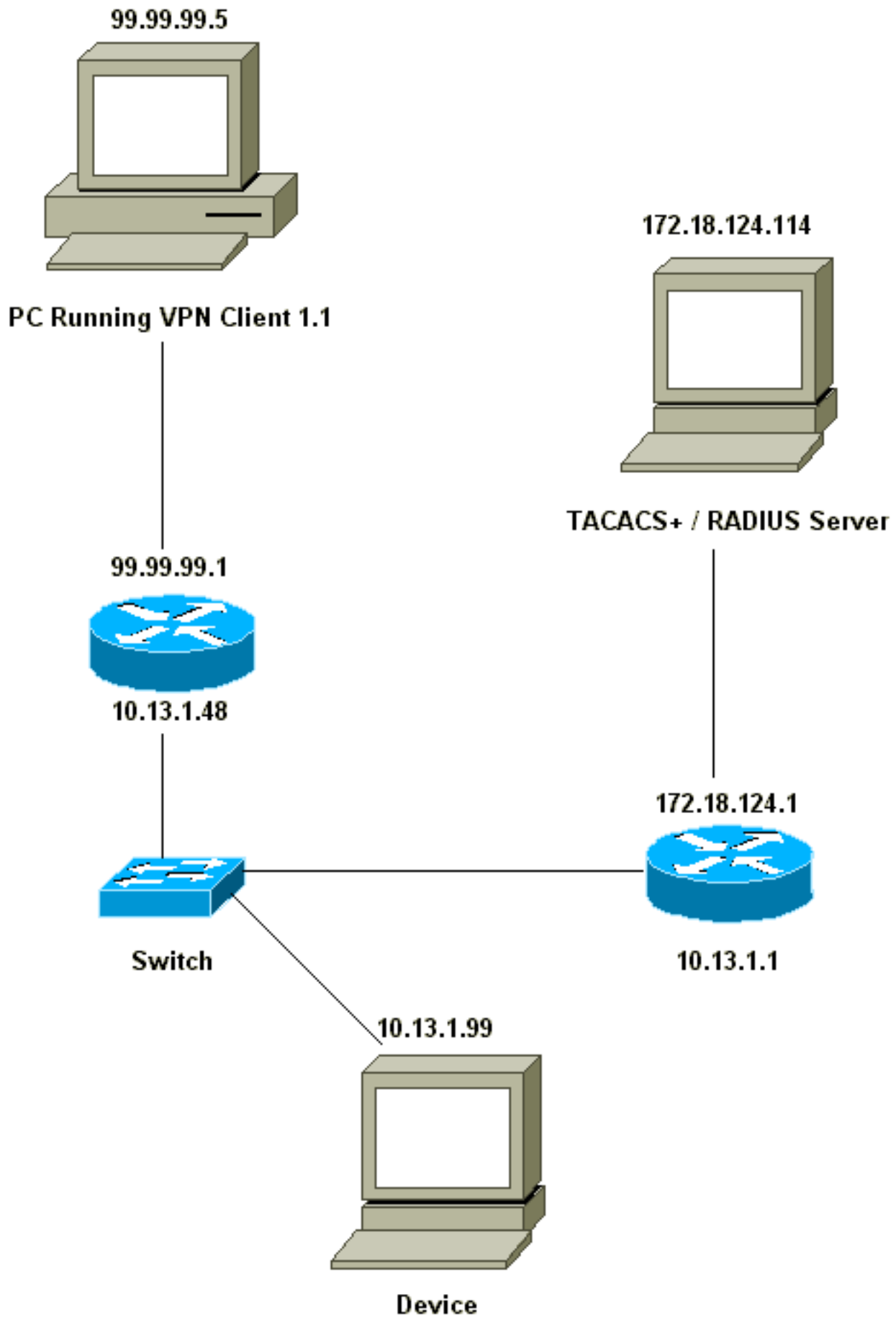
## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



[Installazione di VPN Client 1.1](#)

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

Se Xauth è abilitato sul router, quando l'utente tenta di connettersi a un dispositivo all'interno del router (qui è stato eseguito un ping -t #.#.#.#), viene visualizzata una schermata grigia:

User Authentication for 3660

Username:

Password:

## [Configurazioni](#)

### Configurazione server

L'autenticazione Xauth può essere eseguita tramite TACACS+ o RADIUS. Per essere certi che agli utenti Xauth fosse consentito eseguire Xauth, ma che non fosse consentito connettersi al router in modalità telnet, è stato aggiunto il comando **aaa authorization exec**. Agli utenti RADIUS è stato assegnato il comando "reply-attribute Service-Type=Outbound=5" (anziché Amministrativo o Accesso). In Cisco Secure UNIX, questo valore è "In uscita"; in CiscoSecure NT questo è "Dialout Framed". Se si trattasse di utenti TACACS+, non verrebbero concesse loro autorizzazioni shell/exec.

### Configurazione router per TACACS+ o RADIUS Xauth

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
```

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Comandi per la risoluzione dei problemi

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

- **debug aaa authentication:** visualizza le informazioni sull'autenticazione AAA/TACACS+.
- **debug crypto isakmp:** visualizza i messaggi sugli eventi IKE.
- **debug crypto ipsec:** visualizza gli eventi IPsec.
- **debug crypto key-exchange:** visualizza i messaggi di scambio di chiave pubblica DSS (Digital

Signature Standard).

- **debug radius** - Visualizza le informazioni associate a RADIUS.
- **debug tacacs**: visualizza le informazioni associate al TACACS.
- **clear crypto isakmp** - Specifica la connessione da cancellare.
- **clear crypto sa**: elimina le associazioni di protezione IPsec.

## [Output di esempio del comando debug](#)

**Nota:** il debug TACACS+ sarebbe molto simile. Usare il comando **debug tacacs+** anziché il comando **debug radius**.

```
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
```

## [Informazioni correlate](#)

- [Pagina di supporto per Cisco VPN Client](#)
- [Pagina di supporto per la negoziazione IPsec/I protocolli IKE](#)
- [Pagina di supporto per Terminal Access Controller Access Control System \(TACACS+\)](#)
- [Pagina di supporto RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [Richiesta di commenti](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)