

Configuración de TACACS+ y de la autenticación extendida de RADIUS con VPN Client

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de cliente VPN 1.1](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Información Relacionada](#)

Introducción

Este documento muestra las configuraciones de muestra para Autenticación ampliada (Xauth) de la Fuerza de tareas de ingeniería en Internet (IETF) TACACS+ y RADIUS (IETF). El Xauth le deja desplegar la seguridad IP (IPSec) en el Redes privadas virtuales (VPN) usando el TACACS+ o el RADIUS como su método de autenticación de usuario dentro del protocolo del Internet Key Exchange (IKE). Esta característica proporciona la autenticación a un usuario que tenga CiscoSecure VPN el cliente 1.1 instalado en su PC, indicando al usuario para un nombre de usuario y una contraseña, y después los verifica con la información salvada en el servidor del Authentication, Authorization, and Accounting (AAA), el TACACS+ o la base de datos RADIUS. La autenticación ocurre entre la fase 1 IKE y la fase 2. IKE. Si el usuario autentica con éxito, establecen a una asociación de seguridad de la fase 2 (SA) después de lo cual los datos puede ser enviada con seguridad a la red protegida.

El Xauth incluye la *autenticación* solamente, no *autorización* (donde se establecen los usuarios pueden ir una vez la conexión). *El considerar* (donde fueron los usuarios) no se implementa.

La configuración debe trabajar sin el Xauth antes de implementar el Xauth. Nuestro ejemplo demuestra la configuración de modo (configuración de modo) y el Network Address Translation (NAT) además del Xauth, pero la suposición es que conectividad IPSec está presente antes de agregar los comandos xauth.

Asegúrese que el Xauth local (nombre de usuario/contraseña en el router) trabaja antes de intentar el TACACS+ o el RADIUS Xauth.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 1.1 del cliente VPN (o más adelante)
- El ® del Cisco IOS libera 12.1.2.2.T, 12.1.2.2.P (o más adelante)
- La autenticación de RADIUS fue probada con el Cisco 3640 que ejecutaba c3640-jo3s56i-mz.121-2.3.T

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

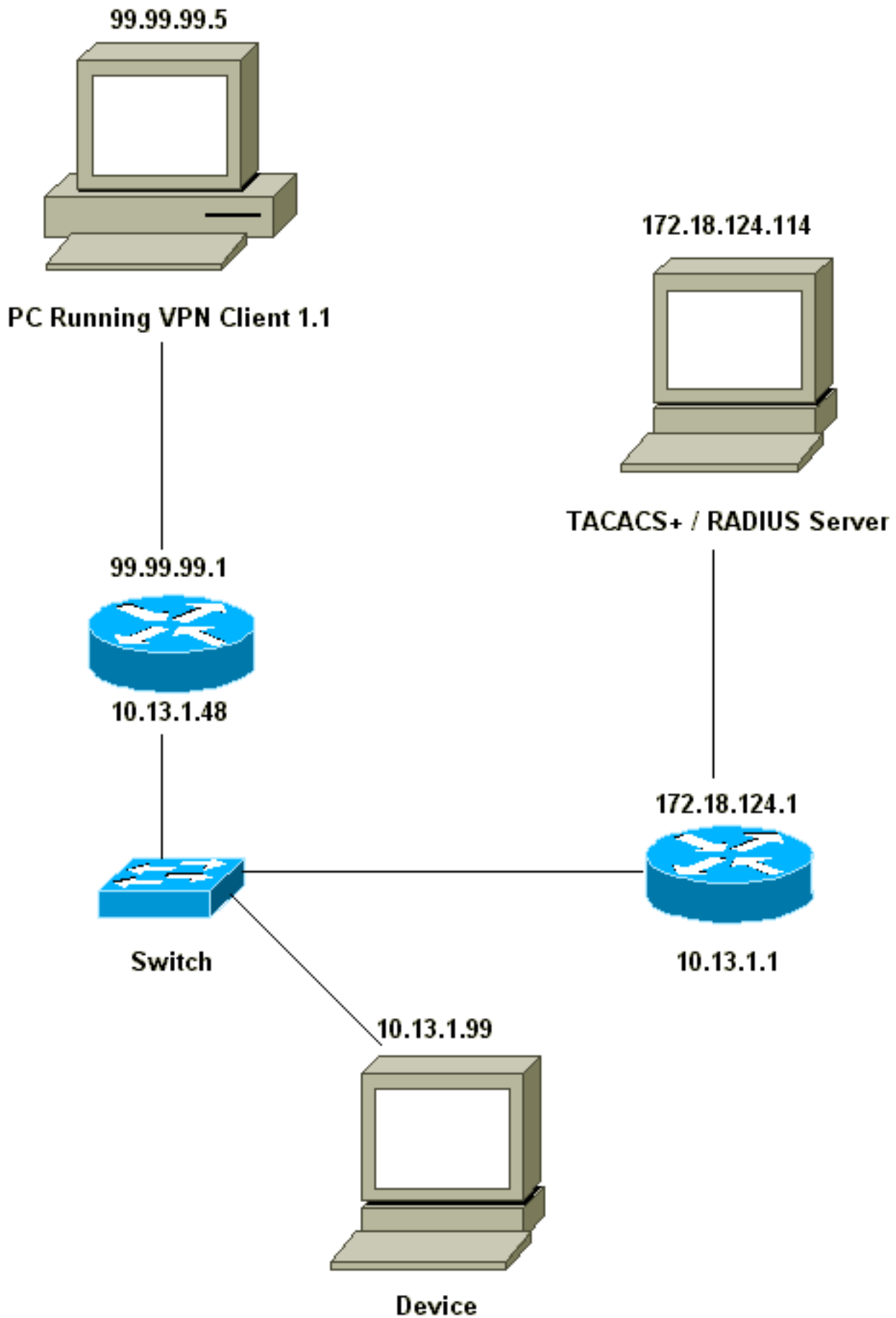
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



[Configuración de cliente VPN 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
```

Con el Xauth habilitado en el router, cuando el usuario intenta conectar con un dispositivo dentro del router (aquí hicimos un ping - t #.#.#.#), una pantalla gris sube:

```
User Authentication for 3660
Username:
Password:
```

[Configuraciones](#)

Configuración del servidor

La autenticación Xauth se puede hacer por el TACACS+ o por el RADIUS. Quisimos estar seguros que se permitió a los usuarios del Xauth hacer el Xauth, pero no permitido al telnet al router, así que agregamos el **comando aaa authorization exec**. Dimos contestación-atributo Service-Type=Outbound=5" a los usuarios de RADIUS el "(en vez de administrativo o del login). En el CiscoSecure UNIX, esto es "saliente"; en el CiscoSecure NT éste es "Framed del dialout." Si éstos fueran usuarios TACACS+, no les daríamos los permisos del shell/del ejecutivo.

Configuración del router para el TACACS+ o el 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

```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos

comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

- debug aaa authentication — Muestra información sobre autenticación de AAA/TACACS+.
- debug crypto isakmp — Muestra mensajes acerca de eventos IKE.
- debug crypto ipsec — Muestra eventos de IPSec.
- **debug crypto key-exchange** — Mensajes de intercambio de la clave pública del Digital Signature Standard (DSS) de las demostraciones.
- debug radius - Muestra información asociada con RADIUS.
- debug tacacs - Muestra información asociada con el TACACS.
- **borre el isakmp crypto** — Especifica qué conexión a borrar.
- **borre el sa crypto** — Asociaciones de seguridad IPSec de las cancelaciones.

Ejemplo de resultado del comando debug

Nota: El debug TACACS+ sería muy similar. Utilice el comando **debug tacacs+** en vez del 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): attrs 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
```

[Información Relacionada](#)

- [Página de soporte para cliente Cisco VPN](#)
- [Página de Soporte de IPSec Negotiation/IKE Protocols](#)
- [Página de soporte del Terminal Access Controller Access Control System \(TACACS+\)](#)
- [Página de soporte del Remote Authentication Dial-In User Service \(RADIUS\)](#)
- [Request For Comments](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)