

# Configuración de un Router IPsec Par Dinámico de LAN a LAN y Clientes VPN

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Cliente VPN](#)

[Verificación](#)

[Verificar números de secuencia de mapa criptográfico](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Esta configuración muestra una configuración de LAN a LAN entre dos routers en un entorno de hub-spoke. Cisco VPN Clients también conectan con el hub y utilizan Autenticación ampliada (Xauth).

El router spoke en este escenario obtiene su dirección IP dinámicamente a través de DHCP. El uso del protocolo de configuración dinámica de host (DHCP) es habitual en situaciones en las que el spoke se conecta a Internet a través de un módem DSL o por cable. Esto se debe a que el ISP a menudo aprovisiona las direcciones IP de forma dinámica mediante DHCP en estas conexiones de bajo coste.

Sin configuración adicional, el uso de una clave precompartida comodín en el router hub no es posible en esta situación. Esto se debe a que Xauth para las conexiones VPN Client rompe la conexión de LAN a LAN. Sin embargo, cuando inhabilita Xauth, reduce la capacidad de autenticar clientes VPN.

La introducción de perfiles ISAKMP en Cisco IOS® Software Release 12.2(15)T hace posible esta configuración ya que puede coincidir en otras propiedades de la conexión (grupo de clientes VPN, dirección IP de peer, nombre de dominio completamente calificado [FQDN], etc.) en lugar de sólo en la dirección IP de peer. Los perfiles ISAKMP son el tema de esta configuración.

Nota: También puede utilizar la palabra clave no-xauth con el comando crypto isakmp key para saltar Xauth para los pares LAN a LAN. Consulte [Capacidad para Inhabilitar Xauth para Peers](#)

[IPSec Estáticos](#) y [Configuración de IPSec entre Dos Routers y un Cisco VPN Client 4.x](#) para obtener más información.

La [configuración del router spoke](#) en este documento se puede replicar en todos los otros routers spoke que se conectan al mismo hub. La única diferencia entre radios es la lista de acceso que hace referencia al tráfico que se va a cifrar.

Consulte [Ejemplo de Configuración de Cliente y Servidor EzVPN en el Mismo Router](#) para obtener más información sobre el escenario donde puede configurar un router como un Cliente EzVPN y un servidor en la misma interfaz.

Consulte [Túneles de LAN a LAN en un Concentrador VPN 3000 con un Firewall PIX Configurado para DHCP](#) para configurar la Serie de Concentradores Cisco VPN 3000 para crear túneles IPsec dinámicamente con los Firewalls Cisco PIX remotos que utilizan DHCP para obtener direcciones IP en sus interfaces públicas.

Consulte [Ejemplo de Configuración de Túnel IPsec LAN-to-LAN en un Concentrador VPN 3000 con un Router Cisco IOS Configurado para DHCP](#) para configurar la Serie de Concentradores VPN 3000 para crear túneles IPsec dinámicamente con dispositivos VPN remotos que reciben direcciones IP dinámicas en sus interfaces públicas.

Consulte [Ejemplo de Configuración de IPSec entre un Router IOS Estático y un PIX/ASA 7.x Dinámico con NAT](#) para habilitar el Dispositivo de Seguridad PIX/ASA para aceptar las conexiones IPsec dinámicas del router IOS®.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

Los perfiles IPsec se introdujeron en Cisco IOS Software Release 12.2(15)T. Debido al ID de bug de Cisco [CSCea7140](#) (sólo clientes [registrados](#)), necesita ejecutar la versión 12.3(3) o posterior del software del IOS de Cisco, o la versión 12.3(2)T o posterior del software del IOS de Cisco para que esta configuración funcione correctamente. Estas configuraciones se probaron con estas versiones de software:

- Software Cisco IOS versión 12.3(6a) en el router hub
- Software Cisco IOS versión 12.2(23a) en el router spoke (puede ser cualquier versión crypto)
- Cisco VPN Client versión 4.0(4) en Windows 2000

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). If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

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

## Configurar

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

Nota: Utilice la [herramienta de búsqueda de comandos](#) (solo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

## Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.

## Configuraciones

En este documento, se utiliza esta configuración de red:

- [Configuración del hub](#)
- [Configuración de radio](#)

Configuración del h

```
<#root>
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname
Hub
!
no logging on
!
username gfullage password 7 0201024E070A0E2649
aaa new-model
!
!
aaa authentication login clientauth local
aaa authorization network groupauthor local
```

```
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
!
!
!--- Keyring that defines wildcard pre-shared key.

crypto keyring spokes
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!

crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
!
!--- VPN Client configuration for group "testgroup" !--- (this name is configured in the VPN Client).

crypto isakmp client configuration group testgroup
  key cisco321
  dns 1.1.1.1 2.2.2.2
  wins 3.3.3.3 4.4.4.4
  domain cisco.com
  pool ippool
!
!--- Profile for LAN-to-LAN connection, that references !--- the wildcard pre-shared key and a wildcard

crypto isakmp profile L2L
  description LAN-to-LAN for spoke router(s) connection
  keyring spokes
  match identity address 0.0.0.0

!--- Profile for VPN Client connections, that matches !--- the "testgroup" group and defines the Xauth

crypto isakmp profile VPNclient
  description VPN clients profile
  match identity group testgroup
  client authentication list clientauth
  isakmp authorization list groupauthor
  client configuration address respond
!
!

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
!--- Two instances of the dynamic crypto map !--- reference the two previous IPsec profiles.
```

```
crypto dynamic-map dynmap 5
  set transform-set myset
  set isakmp-profile VPNclient
crypto dynamic-map dynmap 10
  set transform-set myset
  set isakmp-profile L2L
```

```
!
!
```

*!--- Crypto-map only references the two !--- instances of the previous dynamic crypto map.*

```
crypto map mymap 10 ipsec-isakmp dynamic dynmap
```

```
!
!
!
```

```
interface FastEthernet0/0
  description Outside interface
  ip address 10.48.67.181 255.255.255.224
  no ip mroute-cache
  duplex auto
  speed auto
```

```
crypto map mymap
```

```
!
```

```
interface FastEthernet0/1
  description Inside interface
  ip address 10.1.1.1 255.255.254.0
```

```
  duplex auto
  speed auto
  no keepalive
```

```
!
```

```
ip local pool ippool 10.5.5.1 10.5.5.254
```

```
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.48.66.181
```

```
!
!
```

```
call rsvp-sync
```

```
!
!
```

```
dial-peer cor custom
```

```
!
!
```

```
line con 0
  exec-timeout 0 0
  escape-character 27
```

```
line aux 0
```

```
line vty 0 4
```

```
  password 7 121A0C041104
```

```
!
!
```

end

## Configuración de radio

<#root>

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname
```

Spoke

```
!
no logging on
!
ip subnet-zero
no ip domain lookup
!
ip cef
!
!
```

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 10.48.67.181
```

```
!
!
```

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

```
!
```

*!--- Standard crypto map on the spoke router !--- that references the known hub IP address.*

```
crypto map mymap 10 ipsec-isakmp
  set peer 10.48.67.181
  set transform-set myset
  match address 100
```

```
!
!
```

```
controller ISA 5/1
```

```
!
!
```

```
interface FastEthernet0/0
  description Outside interface
```

```
ip address dhcp
```

```

duplex auto
speed auto

crypto map mymap

!
interface FastEthernet0/1
description Inside interface
ip address 10.2.2.2 255.255.255.0
duplex auto
speed auto
no keepalive
!
interface ATM1/0
no ip address
shutdown
no atm ilmi-keepalive
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.2.3
no ip http server
no ip http secure-server
!
!

!--- Standard access-list that references traffic to be !--- encrypted. This is the only thing that ne

access-list 100 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255

!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password cisco
login
!
!
end

```

## Cliente VPN

Cree una nueva entrada de conexión que haga referencia a la dirección IP del router hub. El nombre del grupo en este ejemplo es "testgroup" y la contraseña es "cisco321". Esto puede verse en la [configuración](#) del [router hub](#).

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Los comandos de depuración que se ejecutan en el router hub pueden confirmar que los parámetros correctos coinciden para las conexiones spoke y VPN Client.

[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 Debug](#) antes de utilizar los comandos debug.

- show ip interface: muestra la asignación de la dirección IP al router spoke.
- show crypto isakmp sa detail—Muestra las IKE SAs, que se han configurado entre los iniciadores IPsec. Por ejemplo, el router spoke y el cliente VPN, y el router hub.
- show crypto ipsec sa—Muestra las SAs IPsec, que se han configurado entre los iniciadores IPsec. Por ejemplo, el router spoke y el cliente VPN, y el router hub.
- debug crypto isakmp — Muestra mensajes acerca de eventos de intercambio de claves por Internet (IKE).
- debug crypto ipsec — Muestra eventos de IPsec.
- debug crypto engine: muestra los eventos del motor criptográfico.

Este es el resultado del comando show ip interface f0/0.

```
<#root>
spoke#
show ip interface f0/0
FastEthernet0/1 is up, line protocol is up
Internet address is 10.100.2.102/24
Broadcast address is 255.255.255.255
Address determined by DHCP
```

Ésta es la salida del comando show crypto isakmp sa detail.

```
<#root>
hub#
show crypto isakmp sa detail
```



Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

C-id	Local	Remote	I-VRF	Encr	Hash	Auth	DH	Lifetime	Cap.
1	10.48.67.181	10.100.2.102		3des	sha	psk	2	04:15:43	
2	10.48.67.181	10.51.82.100		3des	sha		2	05:31:58	CX

Ésta es la salida del comando show crypto ipsec sa.

```
<#root>
```

```
hub#
```

```
show crypto ipsec sa
```

```
interface: FastEthernet0/0
```

```
Crypto map tag: mymap, local addr. 10.48.67.181
```

```
protected vrf:
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/0/0)
```

```
current_peer: 10.51.82.100:500
```

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

```
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
```

```
#pkts decaps: 189, #pkts decrypt: 189, #pkts verify 189
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

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

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.48.67.181, remote crypto endpt.: 10.51.82.100
```

```
path mtu 1500, ip mtu 1500
```

```
current outbound spi: B0C0F4AC
```

```
inbound esp sas:
```

```
spi: 0x7A1AB8F3(2048571635)
```

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

```
in use settings ={Tunnel, }
```

```
slot: 0, conn id: 2004, flow_id: 5, crypto map: mymap
```

```
sa timing: remaining key lifetime (k/sec): (4602415/3169)
```

```
IV size: 8 bytes
```

```
replay detection support: Y
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xB0C0F4AC(2965435564)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2005, flow\_id: 6, crypto map: mymap  
sa timing: remaining key lifetime (k/sec): (4602445/3169)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:

local ident (addr/mask/prot/port): (10.1.0.0/255.255.0.0/0/0)  
remote ident (addr/mask/prot/port): (10.2.0.0/255.255.0.0/0/0)

current\_peer: 10.100.2.102:500  
PERMIT, flags={}  
#pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19  
#pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0

local crypto endpt.: 10.48.67.181, remote crypto endpt.: 10.100.2.102  
path mtu 1500, ip mtu 1500  
current outbound spi: 5FBE5408

inbound esp sas:

spi: 0x9CD7288C(2631346316)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2002, flow\_id: 3, crypto map: mymap  
sa timing: remaining key lifetime (k/sec): (4569060/2071)  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x5FBE5408(1606308872)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2003, flow\_id: 4, crypto map: mymap  
sa timing: remaining key lifetime (k/sec): (4569060/2070)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcg sas:

Este resultado de depuración se ha recopilado en el router hub, cuando el router spoke inicia IKE y SAs IPsec.

<#root>

```
ISAKMP (0:0): received packet from 10.100.2.102 dport 500 sport 500
          Global (N) NEW SA
ISAKMP: local port 500, remote port 500
ISAKMP: insert sa successfully sa = 63D5BE0C
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_MM1

ISAKMP (0:1): processing SA payload. message ID = 0
ISAKMP: Looking for a matching key for 10.100.2.102 in default

ISAKMP: Looking for a matching key for 10.100.2.102 in spokes : success
ISAKMP (0:1): found peer pre-shared key matching 10.100.2.102

ISAKMP (0:1) local preshared key found
ISAKMP : Scanning profiles for xauth ... L2L VPNclient
ISAKMP (0:1) Authentication by xauth preshared
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

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

CryptoEngine0: generate alg parameter
CRYPTO_ENGINE: Dh phase 1 status: 0
CRYPTO_ENGINE: Dh phase 1 status: 0
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP (0:1): Old State = IKE_R_MM1 New State = IKE_R_MM1

ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port
          500 (R) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP (0:1): Old State = IKE_R_MM1 New State = IKE_R_MM2

ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500
          Global (R) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP (0:1): Old State = IKE_R_MM2 New State = IKE_R_MM3

ISAKMP (0:1): processing KE payload. message ID = 0
CryptoEngine0: generate alg parameter
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP: Looking for a matching key for 10.100.2.102 in default
ISAKMP: Looking for a matching key for 10.100.2.102 in spokes : success
ISAKMP (0:1): found peer pre-shared key matching 10.100.2.102
CryptoEngine0: create ISAKMP SKEYID for conn id 1
ISAKMP (0:1): SKEYID state generated
```

```
ISAKMP (0:1): processing vendor id payload
ISAKMP (0:1): speaking to another IOS box!
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP (0:1): Old State = IKE_R_MM3 New State = IKE_R_MM3

ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port 500
(R) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP (0:1): Old State = IKE_R_MM3 New State = IKE_R_MM4

ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500
Global (R) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP (0:1): Old State = IKE_R_MM4 New State = IKE_R_MM5

ISAKMP (0:1): processing ID payload. message ID = 0
ISAKMP (0:1): ID payload
next-payload : 8
type : 1
address : 10.100.2.102
protocol : 17
port : 500
length : 12

ISAKMP (0:1): peer matches L2L profile

ISAKMP: Looking for a matching key for 10.100.2.102 in default
ISAKMP: Looking for a matching key for 10.100.2.102 in spokes : success

ISAKMP (0:1): Found ADDRESS key in keyring spokes

ISAKMP (0:1): processing HASH payload. message ID = 0
CryptoEngine0: generate hmac context for conn id 1

ISAKMP (0:1): SA authentication status: authenticated
ISAKMP (0:1): SA has been authenticated with 10.100.2.102

ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP (0:1): Old State = IKE_R_MM5 New State = IKE_R_MM5

ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (0:1): ID payload
next-payload : 8
type : 1
address : 10.48.67.181
protocol : 17
port : 500
length : 12
ISAKMP (1): Total payload length: 12
CryptoEngine0: generate hmac context for conn id 1
CryptoEngine0: clear dh number for conn id 1
ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port 500
(R) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP (0:1): Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```

*!--- IKE phase 1 is complete.*

```
ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500 Global
```

```
(R) QM_IDLE
ISAKMP: set new node 904613356 to QM_IDLE
CryptoEngine0: generate hmac context for conn id 1
ISAKMP (0:1): processing HASH payload. message ID = 904613356
ISAKMP (0:1): processing SA payload. message ID = 904613356
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1 (Tunnel)
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 3600
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-SHA
CryptoEngine0: validate proposal

ISAKMP (0:1): atts are acceptable.

IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.48.67.181, remote= 10.100.2.102,

local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.2.0.0/255.255.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),

lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
CryptoEngine0: validate proposal request
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
ISAKMP (0:1): processing NONCE payload. message ID = 904613356
ISAKMP (0:1): processing ID payload. message ID = 904613356
ISAKMP (0:1): processing ID payload. message ID = 904613356
ISAKMP (0:1): asking for 1 spis from ipsec
ISAKMP (0:1): Node 904613356, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
IPSEC(key_engine): got a queue event...
IPSEC(spi_response):

getting spi 4172528328 for SA from 10.48.67.181 to
10.100.2.102 for prot 3

ISAKMP: received ke message (2/1)
CryptoEngine0: generate hmac context for conn id 1
ISAKMP (0:1): sending packet to 10.100.2.102 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:1): Node 904613356, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
ISAKMP (0:1): received packet from 10.100.2.102 dport 500 sport 500 Global
(R) QM_IDLE
CryptoEngine0: generate hmac context for conn id 1
CryptoEngine0: ipsec allocate flow
CryptoEngine0: ipsec allocate flow

ISAKMP (0:1): Creating IPsec SAs
inbound SA from 10.100.2.102 to 10.48.67.181 (f/i) 0/ 0

(proxy 10.2.0.0 to 10.1.0.0)
has spi 0xF8B3BAC8 and conn_id 2000 and flags 2
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
has client flags 0x0

outbound SA from 10.48.67.181 to 10.100.2.102 (f/i) 0/ 0
(proxy 10.1.0.0 to 10.2.0.0 )
```

```
has spi 1757151497 and conn_id 2001 and flags A
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
has client flags 0x0
ISAKMP (0:1): deleting node 904613356 error FALSE reason "quick mode done (await)"
ISAKMP (0:1): Node 904613356, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:1): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.48.67.181, remote= 10.100.2.102,
local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.2.0.0/255.255.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0xF8B3BAC8(4172528328), conn_id= 2000, keysize= 0, flags= 0x2
IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.48.67.181, remote= 10.100.2.102,
local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.2.0.0/255.255.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0x68BC0109(1757151497), conn_id= 2001, keysize= 0, flags= 0xA
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(add mtree): src 10.1.0.0, dest 10.2.0.0, dest_port 0
```

```
IPSEC(create_sa): sa created,
```

```
(sa) sa_dest= 10.48.67.181, sa_prot= 50,
sa_spi= 0xF8B3BAC8(4172528328),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
```

```
IPSEC(create_sa): sa created,
```

```
(sa) sa_dest= 10.100.2.102, sa_prot= 50,
sa_spi= 0x68BC0109(1757151497),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
```

Este resultado de depuración se ha recopilado en el router hub, cuando el cliente VPN inicia las SA IKE e IPsec.

<#root>

```
ISAKMP (0:0): received packet from 10.51.82.100 dport 500 sport 500 Global
(N) NEW SA
ISAKMP: local port 500, remote port 500
ISAKMP: insert sa successfully sa = 63D3D804
ISAKMP (0:2): processing SA payload. message ID = 0
ISAKMP (0:2): processing ID payload. message ID = 0
ISAKMP (0:2): ID payload
next-payload : 13
type : 11
group id : testgroup
protocol : 17
port : 500
length : 17

ISAKMP (0:2): peer matches VPNclient profile
```

ISAKMP: Looking for a matching key for 10.51.82.100 in default  
ISAKMP: Looking for a matching key for 10.51.82.100 in spokes : success  
ISAKMP: Created a peer struct for 10.51.82.100, peer port 500  
ISAKMP: Locking peer struct 0x644AFC7C, IKE refcount 1 for  
crypto\_ikmp\_config\_initialize\_sa  
ISAKMP (0:2): Setting client config settings 644AFCF8

**ISAKMP (0:2): (Re)Setting client xauth list and state**

ISAKMP (0:2): processing vendor id payload  
ISAKMP (0:2): vendor ID seems Unity/DPD but major 215 mismatch  
ISAKMP (0:2): vendor ID is Xauth  
ISAKMP (0:2): processing vendor id payload  
ISAKMP (0:2): vendor ID is DPD  
ISAKMP (0:2): processing vendor id payload  
ISAKMP (0:2): vendor ID seems Unity/DPD but major 123 mismatch  
ISAKMP (0:2): vendor ID is NAT-T v2  
ISAKMP (0:2): processing vendor id payload  
ISAKMP (0:2): vendor ID seems Unity/DPD but major 194 mismatch  
ISAKMP (0:2): processing vendor id payload  
ISAKMP (0:2): vendor ID is Unity  
ISAKMP (0:2) Authentication by xauth preshared

*!--- Check of ISAKMP transforms against the configured ISAKMP policy.*

ISAKMP (0:2): Checking ISAKMP transform 9 against priority 10 policy  
ISAKMP: encryption 3DES-CBC  
ISAKMP: hash SHA  
ISAKMP: default group 2  
ISAKMP: auth XAUTHInitPreShared  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B  
ISAKMP (0:2):

**atts are acceptable.**

Next payload is 3

CryptoEngine0: generate alg parameter  
CRYPTO\_ENGINE: Dh phase 1 status: 0  
CRYPTO\_ENGINE: Dh phase 1 status: 0  
ISAKMP (0:2): processing KE payload. message ID = 0  
CryptoEngine0: generate alg parameter  
ISAKMP (0:2): processing NONCE payload. message ID = 0  
ISAKMP (0:2): vendor ID is NAT-T v2  
ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_AM\_EXCH  
ISAKMP (0:2): Old State = IKE\_READY New State = IKE\_R\_AM\_AAA\_AWAIT

ISAKMP: got callback 1  
CryptoEngine0: create ISAKMP SKEYID for conn id 2  
ISAKMP (0:2): SKEYID state generated  
ISAKMP (0:2): constructed NAT-T vendor-02 ID  
ISAKMP (0:2): SA is doing pre-shared key authentication plus XAUTH  
using id type ID\_IPV4\_ADDR  
ISAKMP (0:2): ID payload  
next-payload : 10  
type : 1  
address : 10.48.67.181  
protocol : 17  
port : 0  
length : 12  
ISAKMP (2): Total payload length: 12

```
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500
(R) AG_INIT_EXCH
ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
ISAKMP (0:2): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global
(R) AG_INIT_EXCH
ISAKMP (0:2): processing HASH payload. message ID = 0
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): processing NOTIFY_INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 63D3D804
ISAKMP (0:2): SA authentication status: authenticated
ISAKMP (0:2): Process initial contact,
bring down existing phase 1 and 2 SA's with local 10.48.67.181 remote
10.51.82.100 remote port 500
ISAKMP (0:2): returning IP addr to the address pool
IPSEC(key_engine): got a queue event...
ISAKMP:received payload type 17
ISAKMP:received payload type 17

ISAKMP (0:2): SA authentication status: authenticated
ISAKMP (0:2): SA has been authenticated with 10.51.82.100

CryptoEngine0: clear dh number for conn id 1
ISAKMP: Trying to insert a peer 10.48.67.181/10.51.82.100/500/,
and inserted successfully.
ISAKMP: set new node 1257790711 to CONF_XAUTH
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:2): purging node 1257790711
ISAKMP: Sending phase 1 responder lifetime 86400

ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:2): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

ISAKMP (0:2): Need XAUTH
ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

ISAKMP: got callback 1
ISAKMP: set new node 955647754 to CONF_XAUTH
```

*!--- Extended authentication begins.*

```
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2

CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): initiating peer config to 10.51.82.100. ID = 955647754
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500
(R) CONF_XAUTH
ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN
ISAKMP (0:2): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State =
IKE_XAUTH_REQ_SENT

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global
(R) CONF_XAUTH
ISAKMP (0:2): processing transaction payload from 10.51.82.100. message
ID = 955647754
```



CryptoEngine0: generate hmac context for conn id 2  
ISAKMP: Config payload REPLY

*!--- Username/password received from the VPN Client.*

ISAKMP/xauth: reply attribute XAUTH\_USER\_NAME\_V2  
ISAKMP/xauth: reply attribute XAUTH\_USER\_PASSWORD\_V2

ISAKMP (0:2): deleting node 955647754 error FALSE reason "done with  
xauth request/reply exchange"  
ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_REPLY  
ISAKMP (0:2): Old State = IKE\_XAUTH\_REQ\_SENT New State =  
IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT

ISAKMP: got callback 1  
ISAKMP: set new node -1118110738 to CONF\_XAUTH  
CryptoEngine0: generate hmac context for conn id 2  
ISAKMP (0:2): initiating peer config to 10.51.82.100. ID = -1118110738  
ISAKMP (0:2): sending packet to 10.51.82.100 my\_port 500 peer\_port  
500 (R) CONF\_XAUTH  
ISAKMP (0:2): Input = IKE\_MESG\_FROM\_AAA, IKE\_AAA\_CONT\_LOGIN  
ISAKMP (0:2): Old State = IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT New State =  
IKE\_XAUTH\_SET\_SENT

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global  
(R) CONF\_XAUTH  
ISAKMP (0:2): processing transaction payload from 10.51.82.100. message  
ID = -1118110738  
CryptoEngine0: generate hmac context for conn id 2

*!--- Success*

ISAKMP: Config payload ACK

**ISAKMP (0:2): XAUTH ACK Processed**

ISAKMP (0:2): deleting node -1118110738 error FALSE reason "done with transaction"  
ISAKMP (0:2): Input = IKE\_MESG\_FROM\_PEER, IKE\_CFG\_ACK  
ISAKMP (0:2): Old State = IKE\_XAUTH\_SET\_SENT New State = IKE\_P1\_COMPLETE

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

ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500  
Global (R) QM\_IDLE  
ISAKMP: set new node -798495444 to QM\_IDLE  
ISAKMP (0:2): processing transaction payload from 10.51.82.100. message  
ID = -798495444

CryptoEngine0: generate hmac context for conn id 2  
ISAKMP: Config payload REQUEST  
ISAKMP (0:2): checking request:  
ISAKMP: IP4\_ADDRESS  
ISAKMP: IP4\_NETMASK  
ISAKMP: IP4\_DNS  
ISAKMP: IP4\_NBNS  
ISAKMP: ADDRESS\_EXPIRY  
ISAKMP: UNKNOWN Unknown Attr: 0x7000  
ISAKMP: UNKNOWN Unknown Attr: 0x7001

```
ISAKMP: DEFAULT_DOMAIN
ISAKMP: SPLIT_INCLUDE
ISAKMP: UNKNOWN Unknown Attr: 0x7003
ISAKMP: UNKNOWN Unknown Attr: 0x7007
ISAKMP: UNKNOWN Unknown Attr: 0x7009
ISAKMP: APPLICATION_VERSION
ISAKMP: UNKNOWN Unknown Attr: 0x7008
ISAKMP: UNKNOWN Unknown Attr: 0x700A
ISAKMP: UNKNOWN Unknown Attr: 0x7005
ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

ISAKMP: got callback 1
ISAKMP (0:2): attributes sent in message:
Address: 0.2.0.0

ISAKMP (0:2): allocating address 10.5.5.1
ISAKMP: Sending private address: 10.5.5.1
ISAKMP: Sending IP4_DNS server address: 1.1.1.1
ISAKMP: Sending IP4_DNS server address: 2.2.2.2
ISAKMP: Sending IP4_NBNS server address: 3.3.3.3
ISAKMP: Sending IP4_NBNS server address: 4.4.4.4

ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86386
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7000)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7001)
ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7003)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7007)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7009)
ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork Operating
System Software
IOS (tm) 7200 Software (C7200-IK9S-M), Version 12.3(6a), RELEASE SOFTWARE (fc4)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 02-Apr-04 15:52 by kellythw
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7008)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x700A)
ISAKMP (0/2): Unknown Attr: UNKNOWN (0x7005)
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): responding to peer config from 10.51.82.100. ID = -798495444
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500 (R) CONF_ADDR
ISAKMP (0:2): deleting node -798495444 error FALSE reason ""
ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
ISAKMP (0:2): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:2): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```

*!--- IKE phase 1 and Config Mode complete. !--- Check of IPsec proposals against configured transform s*

```
ISAKMP (0:2): Checking IPsec proposal 12
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1 (Tunnel)
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
CryptoEngine0: validate proposal
ISAKMP (0:2): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.48.67.181, remote= 10.51.82.100,
```

```
local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 10.5.5.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
CryptoEngine0: validate proposal request
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
ISAKMP (0:2): processing NONCE payload. message ID = 381726614
ISAKMP (0:2): processing ID payload. message ID = 381726614
ISAKMP (0:2): processing ID payload. message ID = 381726614
ISAKMP (0:2): asking for 1 spis from ipsec
ISAKMP (0:2): Node 381726614, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:2): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 2048571635 for SA
from 10.48.67.181 to 10.51.82.100 for prot 3
ISAKMP: received ke message (2/1)
CryptoEngine0: generate hmac context for conn id 2
ISAKMP (0:2): sending packet to 10.51.82.100 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP (0:2): Node 381726614, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
ISAKMP (0:2): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
ISAKMP (0:2): received packet from 10.51.82.100 dport 500 sport 500 Global
(R) QM_IDLE
CryptoEngine0: generate hmac context for conn id 2
CryptoEngine0: ipsec allocate flow
CryptoEngine0: ipsec allocate flow
ISAKMP: Locking peer struct 0x644AFC7C, IPSEC refcount 1 for for stuff_ke
ISAKMP (0:2): Creating IPsec SAs
inbound SA from 10.51.82.100 to 10.48.67.181 (f/i) 0/ 0
(proxy 10.5.5.1 to 0.0.0.0)
has spi 0x7A1AB8F3 and conn_id 2004 and flags 2
lifetime of 2147483 seconds
has client flags 0x0
outbound SA from 10.48.67.181 to 10.51.82.100 (f/i) 0/ 0 (proxy 0.0.0.0 to 10.5.5.1 )
has spi -1329531732 and conn_id 2005 and flags A
lifetime of 2147483 seconds
has client flags 0x0
ISAKMP (0:2): deleting node 381726614 error FALSE reason "quick mode done (await)"
ISAKMP (0:2): Node 381726614, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:2): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.)
```

#### INBOUND

```
local= 10.48.67.181, remote= 10.51.82.100,

local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
remote_proxy= 10.5.5.1/0.0.0.0/0/0 (type=1),

protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 2147483s and 0kb,
spi= 0x7A1AB8F3(2048571635), conn_id= 2004, keysize= 0, flags= 0x2
IPSEC(initialize_sas): ,
(key eng. msg.)
```

#### OUTBOUND

```
local= 10.48.67.181, remote= 10.51.82.100,

local_proxy= 0.0.0.0/0.0.0.0/0/0
```

```

(type=4),
remote_proxy= 10.5.5.1/0.0.0.0/0/0

(type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 2147483s and 0kb,
spi= 0xB0C0F4AC(2965435564), conn_id= 2005, keysize= 0, flags= 0xA
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(kei_proxy): head = mymap, map->ivrf = , kei->ivrf =
IPSEC(add mtree): src 0.0.0.0, dest 10.5.5.1, dest_port 0

IPSEC(create_sa):

sa created,

(sa) sa_dest= 10.48.67.181, sa_prot= 50,
sa_spi= 0x7A1AB8F3(2048571635),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2004
IPSEC(create_sa):

sa created,

(sa) sa_dest= 10.51.82.100, sa_prot= 50,
sa_spi= 0xB0C0F4AC(2965435564),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2005

```

## Verificar números de secuencia de mapa criptográfico

Si los peers estáticos y dinámicos están configurados en el mismo mapa crypto, el orden de las entradas de mapa crypto es muy importante. El número de secuencia de la entrada de mapa crypto dinámica debe ser mayor que todas las otras entradas de mapa crypto estáticas. Si las entradas estáticas están numeradas más arriba que la entrada dinámica, las conexiones con esos pares fallan.

A continuación, se proporciona un ejemplo de un mapa crypto numerado correctamente que contiene una entrada estática y una entrada dinámica. Observe que la entrada dinámica tiene el número de secuencia más alto y que se ha dejado espacio para agregar entradas estáticas adicionales:

```

<#root>

crypto dynamic-map dynmap 20
set transform-set myset
crypto map mymap 10 ipsec-isakmp
match address 100
set peer 172.16.77.10
set transform-set myset

crypto map mymap 60000 ipsec-isakmp dynamic dynmap

```

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- [Configuración del perfil IPsec](#)
- [Nuevas funciones del software Cisco IOS versión 12.2\(15\)T](#)
- [Página de Soporte del Protocolo IKE/la Negociación de IPSec](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).