

# Configuración de funciones de alta disponibilidad para VPN IPsec sitio a sitio

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[¿Cómo funciona?](#)

[Circunstancia Normal \(Previa al Failover\)](#)

[Después de una recuperación en caso de fallas de HSRP e IPsec](#)

[Después del HSRP original, el router principal se recupera de una interrupción](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento describe las nuevas características de gran disponibilidad para redes VPN IPsec sitio a sitio. HSRP (Hot Standby Router Protocol) se usa frecuentemente para seguir el estado de la interfaz de los routers para alcanzar la tolerancia a fallos entre los routers. Sin embargo, como no existe ninguna correlación interna entre IPsec y HSRP, el HSRP no sigue el estado de las asociaciones de seguridad IPsec (SA) e IPsec requiere los esquemas para sincronizar con la falla de HSRP cuando ocurre. Estos son algunos de los aspectos más importantes de los esquemas usados para proporcionar un acoplamiento más cercano entre IPsec y HSRP:

- La señal de Mantenimiento de intercambio de claves de Internet (IKE) se usa para permitir que IPsec detecte a tiempo una falla de HSRP.
- La correspondencia de criptografía aplicada a una interfaz de router específica se vincula al grupo HSRP ya configurado en esa interfaz para que IPsec detecte la configuración de HSRP. Esto también permite que IPsec use la dirección IP virtual de HSRP como la identidad (ISAKMP) del protocolo de administración de clave y Asociación de Seguridad de Internet de los routers.
- La función de Inyección de ruta inversa (RRI) se usa para permitir actualizaciones de información sobre el ruteo dinámico durante las fallas de HSRP e IPsec.

**Nota:** Este documento describe cómo utilizar el protocolo de router de espera activa (HSRP) con VPN. HSRP también se utiliza para realizar un seguimiento de los links ISP fallidos. Para configurar links ISP redundantes en routers, consulte [Análisis de Niveles de Servicio IP Usando la Operación de Eco ICMP](#). Aquí el dispositivo de origen es el router y el dispositivo de destino es el dispositivo ISP.

# Prerequisites

## Requirements

No hay requisitos previos específicos para este documento.

## Componentes Utilizados

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

- Cisco 7200 Series Routers
- Software Cisco IOS® versión 12.3(7)T1, c7200-a3jk9s-mz.123-7.T1

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

## Convenciones

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

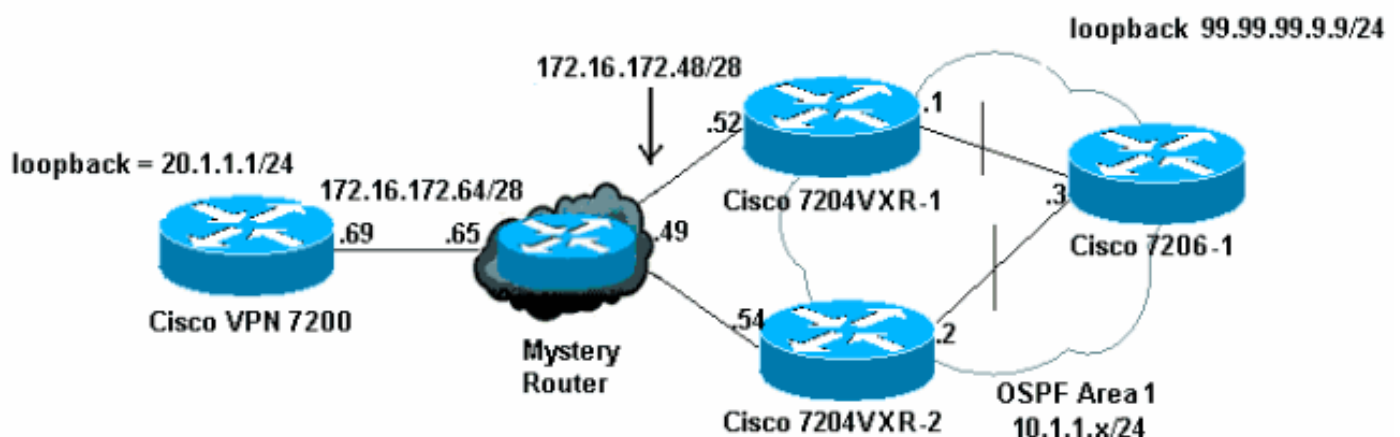
## Configurar

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

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

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

En este documento, se utilizan estas configuraciones:

- [Configuración de VPN 7200 de Cisco](#)
- [Configuración de Cisco 7204VXR-1](#)
- [Configuración de Cisco 7204VXR-2](#)
- [Configuración de Cisco 7206-1](#)

### Configuración de VPN 7200 de Cisco

```
vpn7200#show run
Building configuration...

Current configuration : 1854 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vpn7200
!
!
ip subnet-zero
ip cef
!--- Defines ISAKMP policy and IKE pre-shared key for !-
-- IKE authentication. Note that 172.16.172.53 is the !-
-- HSRP virtual IP address of the remote HSRP routers.
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 172.16.172.53 !---
IKE keepalive to detect the IPSec liveness of the remote
!--- VPN router. When HSRP failover happens, IKE
keepalive !--- will detect the HSRP router switchover.
crypto isakmp keepalive 10 ! ! crypto ipsec transform-
set myset esp-des esp-md5-hmac !--- Defines crypto map.
Note that the peer address is the !--- HSRP virtual IP
address of the remote HSRP routers. crypto map vpn 10
ipsec-isakmp set peer 172.16.172.53 set transform-set
myset match address 101 ! interface Loopback0 ip address
20.1.1.1 255.255.255.255 ! interface FastEthernet0/0 ip
address 10.48.66.66 255.255.254.0 duplex full speed 100
! interface FastEthernet0/1 ip address 172.16.172.69
255.255.255.240 duplex full speed 100 crypto map vpn !
ip classless ip route 10.1.1.0 255.255.255.0
172.16.172.65 ip route 99.99.99.99 255.255.255.255
172.16.172.65 ip route 172.16.172.48 255.255.255.240
172.16.172.65 no ip http server ! access-list 101 permit
ip 20.1.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 101
permit ip 20.1.1.0 0.0.0.255 host 99.99.99.99 ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! end
```

### Configuración de Cisco 7204VXR-1

```
7204VXR-1#show run
Building configuration...

Current configuration : 1754 bytes
!
version 12.3
```

```

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7204VXR-1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
!
ip cef!
!--- Defines ISAKMP policy. crypto isakmp policy 1 hash
md5 authentication pre-share crypto isakmp key cisco123
address 172.16.172.69 crypto isakmp keepalive 10 ! !
crypto ipsec transform-set myset esp-des esp-md5-hmac !-
-- Defines crypto map. Note that "reverse-route" !---
turns on the RRI feature. crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.69 set transform-set myset match
address 101 reverse-route ! ! !--- Define HSRP under the
interface. HSRP will track the !--- internal interface
as well. HSRP group name must be !--- defined here and
will be used for IPsec configuration. !--- The
"redundancy" keyword in the crypto map command !---
specifies the HSRP group to which IPsec will couple. !--
- In normal circumstances, this router will be the HSRP
!--- primary router since it has higher priority than
the !--- other HSRP router. interface FastEthernet0/0 ip
address 172.16.172.52 255.255.255.240 duplex full speed
100 standby 1 ip 172.16.172.53 standby 1 priority 200
standby 1 preempt standby 1 name VPNHA standby 1 track
FastEthernet0/1 150 crypto map vpn redundancy VPNHA !
interface FastEthernet0/1 ip address 10.1.1.1
255.255.255.0 duplex full speed 100 ! interface ATM1/0
no ip address shutdown no atm ilmi-keepalive ! interface
FastEthernet3/0 no ip address shutdown duplex half !
interface ATM6/0 no ip address shutdown no atm ilmi-
keepalive !--- Define dynamic routing protocol and re-
distribute static !--- route. This enables dynamic
routing information update !--- during the HSRP/IPsec
failover. All the "VPN routes" !--- that are injected in
the routing table by RRI as static !--- routes will be
redistributed to internal networks. ! router ospf 1 log-
adjacency-changes redistribute static subnets network
10.1.1.0 0.0.0.255 area 0 ! ip classless ip route
172.16.172.64 255.255.255.240 172.16.172.49 no ip http
server no ip http secure-server ! ! !--- Defines VPN
traffic. The destination IP subnet will be !--- injected
into the routing table as static routes by RRI. access-
list 101 permit ip 10.1.1.0 0.0.0.255 20.1.1.0 0.0.0.255
access-list 101 permit ip host 99.99.99.99 20.1.1.0
0.0.0.255 ! line con 0 exec-timeout 0 0 stopbits 1 line
aux 0 stopbits 1 line vty 0 4 ! ! ! end

```

## Configuración de Cisco 7204VXR-2

```
7204VXR-2#show run
```

```

Building configuration...

Current configuration : 2493 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7204VXR-2
!
boot-start-marker
boot system flash disk1:c7200-a3jk9s-mz.123-7.T1
boot-end-marker
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
ip host rund 10.48.92.61
!
!
ip cef
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.16.172.69
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.69
set transform-set myset
match address 101
reverse-route
!
!--- During normal operational conditions this router !-
-- will be the standby router. interface FastEthernet0/0
ip address 172.16.172.54 255.255.255.240 ip directed-
broadcast duplex full standby 1 ip 172.16.172.53 standby
1 preempt standby 1 name VPNHA standby 1 track
FastEthernet1/0 crypto map vpn redundancy VPNHA !
interface FastEthernet1/0 ip address 10.1.1.2
255.255.255.0 ip directed-broadcast duplex full !
interface FastEthernet3/0 ip address 10.48.67.182
255.255.254.0 ip directed-broadcast shutdown duplex full
! router ospf 1 log-adjacency-changes redistribute
static subnets network 10.1.1.0 0.0.0.255 area 0 ! ip
classless ip route 172.16.172.64 255.255.255.240
172.16.172.49 no ip http server no ip http secure-server
! ! ! access-list 101 permit ip 10.1.1.0 0.0.0.255
20.1.1.0 0.0.0.255 access-list 101 permit ip host
99.99.99.99 20.1.1.0 0.0.0.255 ! line con 0 exec-timeout
0 0 transport preferred all transport output all
stopbits 1 line aux 0 transport preferred all transport
output all stopbits 1 line vty 0 4 login transport
preferred all transport input all transport output all !
! ! end

```

**Configuración de Cisco 7206-1**

```

7206-1#show run
Building configuration...

Current configuration : 1551 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 7206-1
!
ip subnet-zero
no ip source-route
ip cef
!
interface Loopback0
ip address 99.99.99.99 255.255.255.255
!
interface FastEthernet0/0
shutdown
duplex full
speed 100
!
!--- Define dynamic routing protocol. All the "VPN
routes" !--- will be learned and updated dynamically
from upstream HSRP !--- routers using the dynamic
routing protocols. interface FastEthernet0/1 ip address
10.1.1.3 255.255.255.0 duplex full speed 100 ! router
ospf 1 log-adjacency-changes passive-interface Loopback0
network 10.1.1.0 0.0.0.255 area 0 network 99.99.99.99
0.0.0.0 area 0 ! ip classless no ip http server ! ! !
line con 0 exec-timeout 0 0 line aux 0 line vty 0 4
login ! end

```

## ¿Cómo funciona?

Este ejemplo demuestra cómo HSRP y la conmutación por fallas IPsec funcionan juntos usando la configuración y configuración anteriores. En este caso práctico se destacan tres aspectos:

- Falla de HSRP debido a error de interfaz.
- Cómo se produce el error de IPsec tras un error de HSRP. Como se puede ver, la conmutación por fallas IPsec aquí será una conmutación por fallas "sin información de estado".
- Cómo se actualizan y propagan dinámicamente a las redes internas los cambios en la información de ruteo causados por la conmutación por fallas.

**Nota:** El tráfico de prueba aquí son los paquetes de protocolo de mensajes de control de Internet (ICMP) entre la dirección IP de loopback del Cisco 7206-1 (99.99.99.99) y la dirección IP de loopback del Cisco VPN 7200 (20.1.1.1) y simula el tráfico VPN entre los dos sitios.

## Circunstancia Normal (Previa al Failover)

Antes de la conmutación por fallas, el Cisco 7204VXR-1 es el router HSRP principal y el Cisco VPN 7200 tiene SA IPsec con el Cisco 7204VXR-1.

Cuando el mapa criptográfico se configura en la interfaz, la función RRI inserta una ruta VPN para que coincida con la lista de control de acceso (ACL) IPsec configurada y la instrucción de comando **set peer** en el mapa criptográfico. Esta ruta se agrega a la tabla de ruteo del router HSRP 7204VXR-1 primario.

El resultado del comando **debug crypto ipsec** indica la adición de la ruta VPN 20.1.1/24 a la Base de información de routing (RIB).

```
IPSEC(rte_mgr): VPN Route Added 20.1.1.0 255.255.255.0
via 172.16.172.69 in IP DEFAULT TABLE
```

La tabla de ruteo del router HSRP primario proporciona una ruta estática a 20.1.1/24, que es redistribuida por Open Shortest Path First (OSPF) al router HSRP secundario, 7204VXR-2, y al router interno, 7206-1.

El siguiente salto para la ruta VPN 20.1.1/24 inyectada como ruta estática en el RIB del router 7204VXR-1 es la dirección IP del par criptográfico remoto. En este caso, el salto siguiente para la ruta VPN 20.1.1/24 es 172.16.172.69. La dirección IP del siguiente salto de la ruta VPN se resuelve mediante una búsqueda de ruta recursiva como se muestra en esta tabla de Cisco Express Forwarding:

```
7204VXR-1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF,
        IA - OSPF inter area, N1 - OSPF NSSA external type 1,
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
        E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
        L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
    99.0.0.0/32 is subnetted, 1 subnets
O       99.99.99.99 [110/2] via 10.1.1.3, 00:11:21, FastEthernet0/1
    20.0.0.0/24 is subnetted, 1 subnets
S       20.1.1.0 [1/0] via 172.16.172.69
    172.16.0.0/28 is subnetted, 2 subnets
C       172.16.172.48 is directly connected, FastEthernet0/0
S       172.16.172.64 [1/0] via 172.16.172.49
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, FastEthernet0/1
S       10.48.66.0/23 [1/0] via 10.1.1.2
```

```
7204VXR-1#show ip cef 20.1.1.0 detail
```

```
20.1.1.0/24, version 66, epoch 0, cached adjacency 172.16.172.49
0 packets, 0 bytes
via 172.16.172.69, 0 dependencies, recursive
next hop 172.16.172.49, FastEthernet0/0 via 172.16.172.64/28
valid cached adjacency
```

El router HSRP secundario y el router interno 7206-1 aprenden esta ruta VPN a través de OSPF/. Los administradores de red no necesitan introducir la ruta estática manualmente. Lo que es más importante, los cambios de ruteo causados por la conmutación por fallas se actualizan dinámicamente.

7204VXR-2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF,  
IA - OSPF inter area, N1 - OSPF NSSA external type 1,  
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,  
E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,  
L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,  
\* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.48.66.1 to network 0.0.0.0

```
99.0.0.0/32 is subnetted, 1 subnets
O    99.99.99.99 [110/2] via 10.1.1.3, 00:29:31, FastEthernet1/0
20.0.0.0/24 is subnetted, 1 subnets
O E2  20.1.1.0 [110/20] via 10.1.1.1, 00:11:06, FastEthernet1/0
172.16.0.0/28 is subnetted, 2 subnets
C    172.16.172.48 is directly connected, FastEthernet0/0
S    172.16.172.64 [1/0] via 172.16.172.49
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, FastEthernet1/0
C    10.48.66.0/23 is directly connected, FastEthernet3/0
S*   0.0.0.0/0 [1/0] via 10.48.66.1
```

7206-1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF,  
IA - OSPF inter area, N1 - OSPF NSSA external type 1,  
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,  
E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,  
L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,  
\* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```
99.0.0.0/32 is subnetted, 1 subnets
C    99.99.99.99 is directly connected, Loopback0
20.0.0.0/24 is subnetted, 1 subnets
O E2  20.1.1.0 [110/20] via 10.1.1.1, 00:14:01, FastEthernet0/1
172.16.0.0/28 is subnetted, 1 subnets
O E2  172.16.172.64 [110/20] via 10.1.1.1, 00:32:21, FastEthernet0/1
      [110/20] via 10.1.1.2, 00:32:21, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, FastEthernet0/1
O E2  10.48.66.0/23 [110/20] via 10.1.1.2, 00:32:22, FastEthernet0/1
```

El router 7204VXR-1 es el router HSRP primario que realiza un seguimiento de la interfaz interna Fa0/1.

7204VXR-1#show standby

```
FastEthernet0/0 - Group 1
State is Active
2 state changes, last state change 03:21:20
Virtual IP address is 172.16.172.53
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.172 secs
Preemption enabled
Active router is local
Standby router is 172.16.172.54,
```



```
priority 100 (expires in 7.220 sec)
Priority 200 (configured 200)
Track interface FastEthernet0/1 state Up decrement 150
IP redundancy name is "VPNHA" (cfgd)
```

Puede utilizar el comando **show track** para ver una lista de todos los objetos de los que HSRP realiza un seguimiento.

```
7204VXR-1#show track
Track 1 (via HSRP)
Interface FastEthernet0/1 line-protocol
Line protocol is Up
1 change, last change 03:18:22
Tracked by:
HSRP FastEthernet0/0 1
```

El router 7204VXR-2 es el router HSRP en espera. En condiciones de funcionamiento normales, este dispositivo realiza un seguimiento de la interfaz interna Fa1/0.

```
7204VXR-2#show standby
FastEthernet0/0 - Group 1
State is Standby
1 state change, last state change 02:22:30
Virtual IP address is 172.16.172.53
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.096 secs
Preemption enabled
Active router is 172.16.172.52,
priority 200 (expires in 7.040 sec)
Standby router is local
Priority 100 (default 100)
Track interface FastEthernet1/0 state Up decrement 10
IP redundancy name is "VPNHA" (cfgd)
```

Estos comandos **show** relacionados con IPSec producen resultados en el router Cisco VPN 7200 que muestran las SAs ISAKMP e IPSec entre Cisco VPN 7200 y el router HSRP primario, el Cisco 7204VXR-1.

```
7204VXR-1#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         172.16.172.53  172.16.172.69      des   md5   psk   1   23:49:52   K
Connection-id:Engine-id = 1:1(software)
```

```
7204VXR-1#show crypto ipsec sa
interface: FastEthernet0/0
Crypto map tag: vpn, local addr. 172.16.172.53

protected vrf:
local ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
```

current\_peer: 172.16.172.69:500  
PERMIT, flags={origin\_is\_acl,}  
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5  
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.53, remote crypto endpt.: 172.16.172.69  
path mtu 1500, media mtu 1500  
current outbound spi: 44E0B22B

inbound esp sas:  
spi: 0x5B23F22E(1529082414)  
transform: esp-des esp-md5-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2000, flow\_id: 1, crypto map: vpn  
crypto engine type: Software, engine\_id: 1  
sa timing: remaining key lifetime (k/sec): (4504144/2949)  
ike\_cookies: B57A9DC9 FA2D627B F70FEDF6 FAAF9E34  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcsp sas:

outbound esp sas:  
spi: 0x44E0B22B(1155576363)  
transform: esp-des esp-md5-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2001, flow\_id: 2, crypto map: vpn  
crypto engine type: Software, engine\_id: 1  
sa timing: remaining key lifetime (k/sec): (4504145/2949)  
ike\_cookies: B57A9DC9 FA2D627B F70FEDF6 FAAF9E34  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcsp sas:

vpn7200#**show crypto isakmp sa**

dst	src	state	conn-id	slot
172.16.172.53	172.16.172.69	QM_IDLE	1	0

7204VXR-2#**show crypto ipsec sa**

interface: FastEthernet0/1  
Crypto map tag: vpn, local addr. 172.16.172.69

local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)  
current\_peer: 172.16.172.53  
PERMIT, flags={origin\_is\_acl,}  
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10  
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0  
#send errors 5, #recv errors 0

local crypto endpt.: 172.16.172.69, remote crypto endpt.: 172.16.172.53

```
path mtu 1500, ip mtu 1500
current outbound spi: 5B23F22E
```

```
inbound esp sas:
spi: 0x44E0B22B(1155576363)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2029, flow_id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607997/2824)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x5B23F22E(1529082414)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2030, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607998/2824)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

## [Después de una recuperación en caso de fallas de HSRP e IPSec](#)

La conmutación por fallas se desencadenó al apagar Fa0/0 en el Cisco 7204VXR-1. Verá un comportamiento similar si la otra interfaz, Fa0/1, está inactiva porque HSRP también realiza un seguimiento del estado de esta interfaz.

Cuando Cisco VPN 7200 no recibe respuesta a los paquetes keepalive IKE enviados al router HSRP primario, el router destruye las SA IPSec.

Esta salida del comando **debug crypto isakmp** muestra cómo el keepalive IKE detecta la interrupción del router primario:

```
ISAKMP (0:1): received packet from 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = 1585108592
ISAKMP (0:1): processing NOTIFY ITS_ALIVE protocol 1
spi 0, message ID = 1585108592, sa = 61C3E754
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node -1484552386
ISAKMP (0:1): deleting node 1585108592 error FALSE
      reason "informational (in) state 1"
ISAKMP (0:1): purging node 642343711
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node -523181212
ISAKMP (0:1): purging node -2089541867
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 1671177686
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 1706520344
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
```

```

ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 503375209
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 1272270610
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): peer not responding!
ISAKMP (0:1): peer does paranoid keepalives.

ISAKMP (0:1): phase 1 going away; let's be paranoid.
ISAKMP (0:1): Bring down phase 2's
ISAKMP (0:1): That phase 1 was the last one of its kind.
    Taking phase 2's with us.
ISAKMP (0:1): peer does paranoid keepalives.

ISAKMP (0:1): deleting SA reason "P1 errcounter exceeded
    (PEERS_ALIVE_TIMER)" state (I)
    QM_IDLE (peer 172.16.172.53) input queue 0
IPSEC(key_engine): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.172.53
IPSEC(delete_sa): deleting SA,
(sa) sa_dest= 172.16.172.69, sa_prot= 50,
sa_spi= 0x44E0B22B(1155576363),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2029
IPSEC(delete_sa): deleting SA,
(sa) sa_dest= 172.16.172.53, sa_prot= 50,
sa_spi= 0x5B23F22E(1529082414),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2030
ISAKMP (0:1): sending packet to 172.16.172.53 (I) MM_NO_STATE
ISAKMP (0:1): purging node -248155233
ISAKMP (0:1): peer does paranoid keepalives.

IPSEC(key_engine): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.172.53
ISAKMP (0:1): purging node 958118275

```

Quando ocurre la conmutación por fallas en el router HSRP primario Cisco 7204VXR-1, el dispositivo se convierte en un router en espera. Las SAs ISAKMP e IPsec existentes se desactivan. El router HSRP secundario Cisco 7204VXR-2 se activa y establece nuevas SA IPsec con Cisco VPN 7200.

La salida del comando **debug standby events** muestra eventos relacionados con HSRP.

```

HSRP: Fa0/0 API Software interface going down
HSRP: Fa0/0 API Software interface going down
HSRP: Fa0/0 Interface down
HSRP: Fa0/0 Grp 1 Active: b/HSRP disabled
HSRP: Fa0/0 Grp 1 Active router is unknown, was local
HSRP: Fa0/0 Grp 1 Standby router is unknown, was 172.16.172.54
HSRP: Fa0/0 Grp 1 Active -> Init
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Init
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Active -> Init
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.
    Peer 172.16.172.69:500 Id: 172.16.172.69
HSRP: Fa0/0 Grp 1 Redundancy enquiry for VPNHA succeeded
HSRP: Fa0/0 API Add active HSRP addresses to ARP table
%LINK-5-CHANGED: Interface FastEthernet0/0,
    changed state to administratively down
HSRP: API Hardware state change
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,

```

changed state to down

Debido a que la interfaz se apaga, el estado HSRP cambia a "Init".

```
paal#show standby
FastEthernet0/0 - Group 1
State is Init (interface down)
3 state changes, last state change 00:07:29
Virtual IP address is 172.16.172.53
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption enabled
Active router is unknown
Standby router is unknown
Priority 200 (configured 200)
Track interface FastEthernet0/1 state Up decrement 150
IP redundancy name is "VPNHA" (cfgd)
```

Cisco 7204VXR-2 se convierte en el router HSRP activo y cambia su estado a "Activo".

```
HSRP: Fa0/0 Grp 1 Standby: c/Active timer expired (172.16.172.52)
HSRP: Fa0/0 Grp 1 Active router is local, was 172.16.172.52
HSRP: Fa0/0 Grp 1 Standby router is unknown, was local
HSRP: Fa0/0 Grp 1 Standby -> Active (active 0->1, passive 2->1)
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Standby -> Active
!--- VPN route 20.1.1.0/24 is added to the routing table. IPSEC(rte_mgr): VPN Route Added
20.1.1.0 255.255.255.0 via 172.16.172.69 in IP DEFAULT TABLE 7204VXR-2#show standby
FastEthernet0/0 - Group 1
State is Active
2 state changes, last state change 00:10:38
Virtual IP address is 172.16.172.53
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.116 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Track interface FastEthernet1/0 state Up decrement 10
IP redundancy name is "VPNHA" (cfgd)
```

Con RRI habilitado, las rutas VPN se actualizan dinámicamente durante el failover. La ruta estática 20.1.1.0/24 se elimina y el router Cisco 7204VXR-1 aprende la ruta del router Cisco 7204VXR-2.

El resultado del comando **show ip route** muestra esta actualización dinámica.

```
7204VXR-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

```
99.0.0.0/32 is subnetted, 1 subnets
O 99.99.99.99 [110/2] via 10.1.1.3, 02:46:16, FastEthernet0/1
20.0.0.0/24 is subnetted, 1 subnets
O E2 20.1.1.0 [110/20] via 10.1.1.2, 00:08:35, FastEthernet0/1
172.16.0.0/28 is subnetted, 1 subnets
O E2 172.16.172.64 [110/20] via 10.1.1.2, 00:07:56, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.0/24 is directly connected, FastEthernet0/1
S 10.48.66.0/23 [1/0] via 10.1.1.2
```

La ruta VPN estática se inyecta en la tabla de ruteo del router Cisco 7204VXR-2.

```
7204VXR-2#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
99.0.0.0/32 is subnetted, 1 subnets
O 99.99.99.99 [110/2] via 10.1.1.3, 03:04:18, FastEthernet1/0
20.0.0.0/24 is subnetted, 1 subnets
S 20.1.1.0 [1/0] via 172.16.172.69
172.16.0.0/28 is subnetted, 2 subnets
C 172.16.172.48 is directly connected, FastEthernet0/0
S 172.16.172.64 [1/0] via 172.16.172.49
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, FastEthernet1/0
```

El router interno 7206-1 aprende la ruta 20.1.1/24 al par VPN remoto desde su router vecino OSPF, 7204VXR-2. Estos cambios de ruteo ocurren dinámicamente a través de la combinación de HSRP/RRI y OSPF.

```
7206-1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
99.0.0.0/32 is subnetted, 1 subnets
C 99.99.99.99 is directly connected, Loopback0
20.0.0.0/24 is subnetted, 1 subnets
O E2 20.1.1.0 [110/20] via 10.1.1.2, 00:13:55, FastEthernet0/1
172.16.0.0/28 is subnetted, 1 subnets
O E2 172.16.172.64 [110/20] via 10.1.1.2, 00:13:17, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.0/24 is directly connected, FastEthernet0/1
O E2 10.48.66.0/23 [110/20] via 10.1.1.2, 03:06:08, FastEthernet0/1
```

Después de que el Cisco 7204VXR-2 se convierta en el router activo durante la conmutación por

fallas de HSRP, el tráfico VPN entre el Cisco 7204VXR-2 y el Cisco VPN 7200 activa las SA de ISAKMP e IPsec.

La salida de los comandos **show crypto isakmp sa** y **show crypto ipsec sa** en el router VPN 7200 se muestra aquí:

```
7204VXR-2#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.
1 172.16.172.53 172.16.172.69 des md5 psk 1 23:53:47 K
Connection-id:Engine-id = 1:1(software)
```

```
7204VXR-2#show crypto ipsec sa
```

```
interface: FastEthernet0/0
Crypto map tag: vpn, local addr. 172.16.172.53
```

```
protected vrf:
```

```
local ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.172.69:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#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.: 172.16.172.53, remote crypto endpt.: 172.16.172.69
path mtu 1500, media mtu 1500
current outbound spi: 83827275
```

```
inbound esp sas:
```

```
spi: 0x8D70E8A3(2372987043)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4453897/3162)
ike_cookies: 95074F89 3FF73F2B F70FEDF6 5998090C
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x83827275(2206364277)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
crypto engine type: Software, engine_id: 1
```

```
sa timing: remaining key lifetime (k/sec): (4453898/3162)
ike_cookies: 95074F89 3FF73F2B F70FEDF6 5998090C
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas: vpn7200#show crypto isa sa
dst src state conn-id slot
172.16.172.53 172.16.172.69 QM_IDLE 1 0

vpn7200#show crypto ipsec sa

interface: FastEthernet0/1
Crypto map tag: vpn, local addr. 172.16.172.69

local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)
current_peer: 172.16.172.53
PERMIT, flags={origin_is_acl,}
#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 decompress failed: 0
#send errors 6, #recv errors 0

local crypto endpt.: 172.16.172.69, remote crypto endpt.: 172.16.172.53
path mtu 1500, ip mtu 1500
current outbound spi: 8D70E8A3

inbound esp sas:
spi: 0x83827275(2206364277)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2029, flow_id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607997/3070)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8D70E8A3(2372987043)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2030, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607998/3070)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

## [Después del HSRP original, el router principal se recupera de una interrupción](#)

Después de que el servicio se recupera en el router primario HSRP original Cisco 7204VXR-1, el dispositivo vuelve a posicionarse como router activo porque tiene una prioridad más alta y porque se configura HSRP preempt.



El resultado del comando **show** y **debug** de diferentes routers muestra otro switchover de HSRP e IPSec. Las SA ISAKMP e IPSec se restablecen automáticamente y la información de ruteo se actualiza dinámicamente.

Este ejemplo de salida muestra que el router 7204VXR-1 cambia su estado a "Activo".

```
HSRP: Fa0/0 API 172.16.172.52 is not an HSRP address
HSRP: Fa0/0 API MAC address update
HSRP: Fa0/0 API Software interface coming up
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
HSRP: API Hardware state change
HSRP: Fa0/0 API Software interface coming up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
  changed state to up
HSRP: Fa0/0 Interface up
HSRP: Fa0/0 Starting minimum interface delay (1 secs)
HSRP: Fa0/0 Interface min delay expired
HSRP: Fa0/0 Grp 1 Init: a/HSRP enabled
HSRP: Fa0/0 Grp 1 Init -> Listen
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Init -> Backup
HSRP: Fa0/0 Grp 1 Listen: c/Active timer expired (unknown)
HSRP: Fa0/0 Grp 1 Listen -> Speak
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Backup -> Speak
HSRP: Fa0/0 Grp 1 Speak: d/Standby timer expired (unknown)
HSRP: Fa0/0 Grp 1 Standby router is local
HSRP: Fa0/0 Grp 1 Speak -> Standby
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Speak -> Standby
HSRP: Fa0/0 Grp 1 Redundancy enquiry for VPNHA succeeded
HSRP: Fa0/0 Grp 1 Standby: c/Active timer expired (unknown)
HSRP: Fa0/0 Grp 1 Active router is local
HSRP: Fa0/0 Grp 1 Standby router is unknown, was local
HSRP: Fa0/0 Grp 1 Standby -> Active
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Standby -> Active
HSRP: Fa0/0 Grp 1 Active: i/Resign rcvd (100/172.16.172.54)
HSRP: Fa0/0 Grp 1 Redundancy group VPNHA state Active -> Active
HSRP: Fa0/0 Grp 1 Redundancy group VPNHA state Active -> Active
HSRP: Fa0/0 Grp 1 Standby router is 172.16.172.54
```

El router 7204VXR-2 cambia su estado a "En espera". La ruta VPN se elimina de la tabla de ruteo.

```
HSRP: Fa0/0 Grp 1 Standby router is 172.16.172.52
HSRP: Fa0/0 Grp 1 Hello in 172.16.172.52 Active pri 200 vIP 172.16.172.53
hel 3000 hol 10000 id 0000.0c07.ac01
HSRP: Fa0/0 Grp 1 Active router is 172.16.172.52, was local
HSRP: Fa0/0 Grp 1 Standby router is unknown, was 172.16.172.52
HSRP: Fa0/0 Grp 1 Active: g/Hello rcvd from
  higher pri Active router (200/172.16.172.52)
HSRP: Fa0/0 Grp 1 Active -> Speak (active 1->0, passive 0->1)
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Active -> Speak
HSRP: Fa0/0 Grp 1 Speak: d/Standby timer expired (unknown)
HSRP: Fa0/0 Grp 1 Standby router is local
HSRP: Fa0/0 Grp 1 Speak -> Standby (active 0, passive 1)
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Speak -> Standby
HSRP: Fa0/0 Grp 1 Redundancy enquiry for VPNHA succeeded
addr 172.16.172.53 name VPNHA state Speak
active 172.16.172.52 standby 172.16.172.54
!--- The VPN route is removed. IPSEC(rte_mgr): VPN Route Removed 20.1.1.0 255.255.255.0 via
```

172.16.172.69 in IP DEFAULT TABLE

## [Información Relacionada](#)

- [Página de Soporte de IPSec Negotiation/IKE Protocols](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)