

# Configuration des fonctions de haute disponibilité pour les VPN IPSec de site à site

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Comment cela fonctionne-t-il?](#)

[Circonstances Normales \(Avant Basculement\)](#)

[Après le basculement HSRP et IPSec](#)

[Après la récupération du routeur principal HSRP d'origine d'une panne](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit les nouvelles fonctionnalités facilement disponibles pour les réseaux VPN IPSec de site à site. Le protocole Hot Standby Router Protocol (HSRP) est souvent employé pour suivre l'état de l'interface des routeurs dans le but de réaliser le basculement entre routeurs. Toutefois, puisqu'aucune corrélation interne n'existe entre les protocoles IPSec et HSRP, le protocole HSRP ne suit pas l'état des associations de sécurité du protocole IPSec et l'IPSec exige des schémas de synchronisation avec le basculement HSRP lorsqu'il se produit. Voici quelques points essentiels des schémas utilisés pour fournir un couplage plus étroit entre les protocoles IPSec et HSRP :

- Le keepalive IKE (Internet Key Exchange) permet à IPSec de détecter le basculement HSRP dans le temps.
- La carte de chiffrement appliquée sur une interface de routeur spécifique est liée au groupe HSRP déjà configuré sur cette interface pour que IPSec prenne en compte la configuration de HSRP. Cela permet également à IPSec d'utiliser l'adresse IP virtuelle HSRP comme identité ISAKMP (Internet Security Association and Key Management Protocol) des routeurs HSRP.
- La fonction d'injection de route inverse (RRI) permet de mettre à jour les informations de routage dynamique pendant le basculement HSRP et IPSec.

**Remarque :** Ce document décrit comment utiliser le protocole HSRP (Hot Standby Router Protocol) avec VPN. Le protocole HSRP est également utilisé pour suivre les liaisons ISP défaillantes. Afin de configurer des liaisons ISP redondantes sur des routeurs, référez-vous à [Analyse des niveaux de service IP à l'aide du fonctionnement d'écho ICMP](#). Ici, le périphérique source est le routeur et le périphérique de destination est le périphérique ISP.

# Conditions préalables

## Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

## Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs de la gamme Cisco 7200
- Logiciel Cisco IOS® Version 12.3(7)T1, c7200-a3jk9s-mz.123-7.T1

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

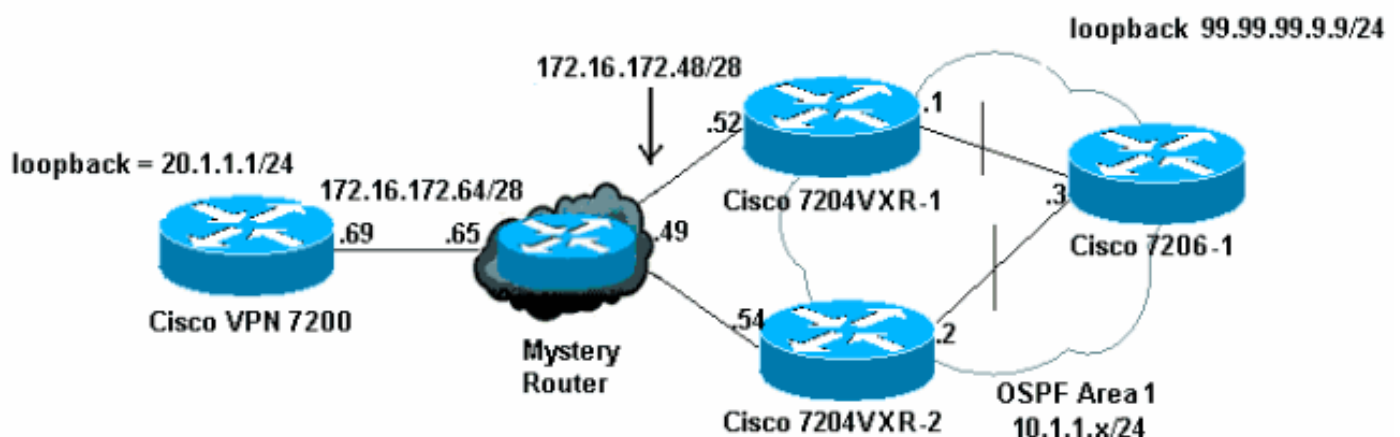
## Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque :** utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :



## Configurations

Ce document utilise les configurations suivantes :

- [Configuration du Cisco VPN 7200](#)
- [Configuration du Cisco 7204VXR-1](#)
- [Configuration du Cisco 7204VXR-2](#)
- [Configuration du Cisco 7206-1](#)

### Configuration du Cisco VPN 7200

```
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
```

### Configuration du 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

```

## Configuration du 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

```

**Configuration du 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
```

## Comment cela fonctionne-t-il?

Cet exemple montre comment HSRP et le basculement IPSec fonctionnent ensemble à l'aide de la configuration et de la configuration ci-dessus. Trois aspects sont mis en évidence dans cette étude de cas :

- Basculement HSRP en raison d'une défaillance de l'interface.
- Comment le basculement IPSec se produit après le basculement HSRP. Comme vous pouvez le voir, le basculement IPSec ici sera un basculement « sans état ».
- La manière dont les modifications des informations de routage provoquées par le basculement sont mises à jour et propagées dynamiquement sur les réseaux internes.

**Remarque :** Le trafic de test ici est constitué de paquets ICMP (Internet Control Message Protocol) entre l'adresse IP de bouclage du Cisco 7206-1 (99.99.99.99) et l'adresse IP de bouclage du Cisco VPN 7200 (20.1.1.1) et simule le trafic VPN entre les deux sites.

## Circonstances Normales (Avant Basculement)

Avant le basculement, le Cisco 7204VXR-1 est le routeur HSRP principal et le Cisco VPN 7200 dispose de SA IPSec avec le Cisco 7204VXR-1.

Lorsque la carte de chiffrement est configurée sur l'interface, la fonctionnalité RRI injecte une route VPN pour correspondre à la liste de contrôle d'accès (ACL) IPsec configurée et à l'instruction de commande **set peer** dans la carte de chiffrement. Cette route est ajoutée à la table de routage du routeur HSRP principal 7204VXR-1.

La sortie de la commande **debug crypto ipsec** indique l'ajout de la route VPN 20.1.1/24 à la base d'informations de routage (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 table de routage sur le routeur HSRP principal fournit une route statique vers 20.1.1/24, qui est redistribuée par OSPF (Open Shortest Path First) au routeur HSRP secondaire, 7204VXR-2, et au routeur interne, 7206-1.

Le saut suivant pour la route VPN 20.1.1/24 injecté en tant que route statique dans le RIB du routeur 7204VXR-1 est l'adresse IP de l'homologue de chiffrement distant. Dans ce cas, le tronçon suivant de la route VPN 20.1.1/24 est 172.16.172.69. L'adresse IP du tronçon suivant de la route VPN est résolue par une recherche de route récursive, comme indiqué dans cette table 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
```

Le routeur HSRP secondaire et le routeur interne 7206-1 apprennent cette route VPN via OSPF/. Les administrateurs réseau n'ont pas besoin d'entrer la route statique manuellement. Plus important encore, les modifications de routage causées par le basculement sont mises à jour dynamiquement.

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
```

Le routeur 7204VXR-1 est le routeur HSRP principal qui suit l'interface interne 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)

Vous pouvez utiliser la commande **show track** pour afficher une liste de tous les objets suivis par HSRP.

```
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**

Le routeur 7204VXR-2 est le routeur HSRP de secours. Dans des conditions opérationnelles normales, ce périphérique suit l'interface interne 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)

Ces commandes **show** liées à IPSec produisent un résultat sur le routeur Cisco VPN 7200 qui illustre les SA ISAKMP et IPSec entre le Cisco VPN 7200 et le routeur HSRP principal, le 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 pcg 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 pcg 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:

## [Après le basculement HSRP et IPSec](#)

Le basculement a été déclenché en arrêtant Fa0/0 sur le Cisco 7204VXR-1. Vous verrez un comportement similaire si l'autre interface, Fa0/1, est désactivée, car HSRP suit également l'état de cette interface.

Lorsque le Cisco VPN 7200 ne reçoit aucune réponse aux paquets IKE keepalive envoyés au routeur HSRP principal, le routeur désactive les SA IPSec.

Cette sortie de commande **debug crypto isakmp** montre comment le keepalive IKE détecte la panne du routeur principal :

```
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

```

Lorsque le basculement se produit sur le routeur HSRP principal Cisco 7204VXR-1, le périphérique devient un routeur de secours. Les SA ISAKMP et IPSec existantes sont désactivées. Le routeur HSRP secondaire Cisco 7204VXR-2 devient actif et établit de nouvelles SA IPSec avec le Cisco VPN 7200.

La sortie de la commande **debug standby events** affiche les événements liés à 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

```

Comme l'interface est arrêtée, l'état HSRP passe à 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)
```

Le Cisco 7204VXR-2 devient le routeur HSRP actif et passe à l'état Actif.

```
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)
```

Lorsque RRI est activé, les routes VPN sont mises à jour dynamiquement pendant le basculement. La route statique 20.1.1.0/24 est supprimée et le routeur Cisco 7204VXR-1 apprend la route à partir du routeur Cisco 7204VXR-2.

Le résultat de la commande **show ip route** illustre cette mise à jour dynamique.

```
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 route VPN statique est injectée dans la table de routage du routeur 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

```

Le routeur interne 7206-1 apprend la route 20.1.1/24 vers l'homologue VPN distant à partir de son routeur voisin OSPF, 7204VXR-2. Ces modifications de routage se produisent de manière dynamique grâce à la combinaison de HSRP/RRI et 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

```

Après que Cisco 7204VXR-2 soit devenu le routeur actif lors du basculement HSRP, le trafic VPN entre les routeurs Cisco 7204VXR-2 et Cisco VPN 7200 active les SA ISAKMP et IPSec.

La sortie des commandes **show crypto isakmp sa** et **show crypto ipsec sa** sur le routeur VPN 7200 est présentée ici :

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:

## [Après la récupération du routeur principal HSRP d'origine d'une panne](#)

Une fois le service restauré sur le routeur principal HSRP d'origine Cisco 7204VXR-1, le périphérique reprend la position de routeur actif car il a une priorité plus élevée et parce que la préemption HSRP est configurée.

La sortie de la commande **show** et **debug** de différents routeurs montre un autre basculement de HSRP et IPsec. Les SA ISAKMP et IPsec sont rétablies automatiquement et les modifications des informations de routage sont mises à jour dynamiquement.



Cet exemple de résultat montre que le routeur 7204VXR-1 change son état en Actif.

```
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
```

Le routeur 7204VXR-2 passe à l'état Veille. La route VPN est supprimée de la table de routage.

```
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
```

## [Informations connexes](#)

- [Page de support de la négociation IPSec/des protocoles IKE](#)

- [Support et documentation techniques - Cisco Systems](#)