

为站点间 IPSec VPN 配置高可用特性

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[它如何运转？](#)

[正常情况（在故障切换之前）](#)

[在 HSRP 和 IPSec 故障切换以后](#)

[在最初的 HSRP 主路由器从停机中恢复之后](#)

[相关信息](#)

简介

本文描述新，站点至站点IPSec VPN网络的高可用性功能。热备份路由协议(HSRP)是常用的跟踪路由器接口状态达到在路由器之间的故障切换。然而，因为内部相关性不存在IPSec和HSRP之间，HSRP不跟踪IPSec安全关联(SAS)的状态，并且IPSec要求机制为了与HSRP故障切换同步，当发生时。这些是用于的机制的一些优点提供在IPSec和HSRP之间的一个更加接近的联结：

- Internet Key Exchange (IKE) Keepalive用于允许IPSec检测HSRP故障切换及时。
- 在一个特定路由器接口应用的加密映射与在该接口已经配置的HSRP组联接意识IPSec HSRP设置。这也允许IPSec使用HSRP虚拟IP地址作为HSRP路由器的互联网安全协会和密钥管理协议 (ISAKMP)标识。
- 在HSRP和IPSec故障切换期间，反向路由注入(RRI)功能用于允许动态路由信息更新。

注意： 本文描述如何以VPN使用热备份路由协议(HSRP)。HSRP也用于跟踪失败的ISP链路。为了配置在路由器的冗余的ISP链路，参考[分析IP服务级别使用ICMP回音操作](#)。在这里source设备路由器，并且目的地设备是ISP设备。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 7200 系列路由器
- Cisco IOS软件版本12.3(7)T1，c7200-a3jk9s-mz.123-7.T1

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用 [命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- [Cisco VPN 7200配置](#)
- [思科7204VXR-1配置](#)
- [思科7204VXR-2配置](#)
- [Cisco 7206-1配置](#)

Cisco VPN 7200配置

```
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
```

思科7204VXR-1配置

```
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
```

思科7204VXR-2配置

```
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

```

Cisco 7206-1配置

```

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

```

它如何运转？

此示例展示HSRP和IPSec故障切换使用上述设立和配置，如何。三个方面在这种情况下突出显示学习：

- 由于HSRP的故障切换建立接口失败。
- IPSec故障切换如何在HSRP故障切换以后发生。和能被看到，此处IPSec故障切换将是“无状态的”故障切换。
- 故障切换引起的路由信息更改如何动态地更新并且被传播对内部网络。

注意： 此处测试流量是在Cisco 7206-1 (99.99.99.99)的环回IP地址和Cisco VPN 7200之间

(20.1.1.1)的环回IP地址的互联网控制消息协议(ICMP)数据包并且模拟在两个站点之间的VPN流量。

正常情况 (在故障切换之前)

在故障切换前，思科7204VXR-1是主要的HSRP路由器，并且Cisco VPN 7200有与思科7204VXR-1的IPSec SAS。

当加密映射在接口时配置，RRI功能注入VPN路由匹配已配置的IPSec访问控制表(ACL)和**set peer**命令语句在加密映射。此路由被添加到主要的HSRP路由器7204VXR-1的路由表。

输出**debug crypto ipsec**命令指示VPN路由20.1.1/24的新增内容对路由信息库(RIB)。

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

在主要的HSRP路由器的路由表产生静态路由对20.1.1/24，由开放最短路径优先(OSPF)再分布对附属HSRP路由器，7204VXR-2和对内部路由器，7206-1。

作为静态路由VPN路由的20.1.1/24下一跳被注入的路由器7204VXR-1 RIB是远程加密对等体的IP地址。在这种情况下，VPN路由的20.1.1/24下一跳是172.16.172.69。VPN路由的下一跳的IP地址通过递归路由查找是解决的如此Cisco快速转发表所显示：

```
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
```

附属HSRP路由器和内部路由器7206-1通过OSPF学习此VPN路由。网络管理员不需要手工输入静态路由。更加重要地，故障切换引起的路由更改动态地更新。

```
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

路由器7204VXR-1是跟踪内部接口Fa0/1的主要的HSRP路由器。

```
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)
```

您能使用show track命令发现HSRP跟踪的所有对象列表。

```
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
```

路由器7204VXR-2是备用HSRP路由器。在正常工作状态下，此设备跟踪内部接口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" (cfdg)
```

这些IPSec相关的显示在展示ISAKMP和IPSec SAS在Cisco VPN 7200和主要的HSRP路由器之间的Cisco VPN 7200路由器输出的命令产量，思科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 pcp 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 pcp 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:
```

[在 HSRP 和 IPSec 故障切换以后](#)

故障切换由在思科7204VXR-1的关闭Fa0/0触发。您将看到相似的行为，如果另一个接口，Fa0/1，发生故障，因为HSRP也跟踪此接口状况。

当Cisco VPN 7200不收到答复到IKE keepalive数据包被发送对主要的HSRP路由器时，路由器切断IPSec SAS。

此debug crypto isakmp命令输出显示IKE Keepalive如何检测主路由器的中断：

```
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
```

当故障切换在思科7204VXR-1主要的HSRP路由器时发生，设备变为备用路由器。现有ISAKMP和IPSec SAS被切断。思科7204VXR-2附属HSRP路由器变为激活并且设立新的IPSec SAS用Cisco VPN 7200。

输出debug standby events命令显示与HSRP涉及的事件。

```
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
由于接口被关闭，对“Init的”HSRP状态更改。
```

```
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)
思科7204VXR-2变为有效HSRP路由器并且更改其状态对“激活”。
```

```
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)
在故障切换期间，当RRI启用，VPN路由动态地更新。静态路由20.1.1.0/24删除，并且思科
7204VXR-1路由器学习从思科7204VXR-2路由器的路由。
```

从show ip route命令的输出展示此动态更新。

```
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
静态VPN路由被注入在思科7204VXR-2路由器的路由表。
```

```
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

内部路由器7206-1学习20.1.1/24路由对从其OSPF邻居路由器的远程VPN对等设备，7204VXR-2。这些路由更改通过HSRP/RRI和OSPF的组合动态地发生。

```
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
```

在HSRP故障切换期间后，在思科7204VXR-2变为活动路由器，在思科7204VXR-2和Cisco VPN 7200路由器之间的VPN流量启动ISAKMP和IPSec SAS。

show crypto isakmp sa和**show crypto ipsec sa on**命令的输出VPN 7200路由器显示此处：

```
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:

[在最初的 HSRP 主路由器从停机中恢复之后](#)

在服务在思科7204VXR-1原始HSRP主路由器后恢复，设备恢复安置作为活动路由器，因为它有一个更高优先级，并且，因为Hsrp preempt配置。

从另外路由器的show and debug命令输出显示HSRP和IPSec另一个切换。ISAKMP和IPSec SAS自动地被重建，并且路由信息更改动态地更新。

此输出示例:显示路由器7204VXR-1更改其状态对“激活”。

```
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
```

路由器7204VXR-2更改其状态对“待机”。VPN路由从路由表删除。

```
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
```

[相关信息](#)

- [IPsec 协商/IKE 协议支持页](#)
- [技术支持和文档 - Cisco Systems](#)