تكوين ميزات التوفر العالي لشبكات VPN الخاصة ب IPSec من موقع إلى موقع

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوينات
كيف تعمل؟
الظروف العادية (قبل تجاوز الفشل)
بعد تجاوز فشل HSRP و IPSec
بعد إسترداد الموجه الأساسي HSRP الأصلي من انقطاع
معلومات ذات صلة

المقدمة

يصف هذا المستند الميزات الجديدة عالية التوفر لشبكات VPN IPSec من موقع إلى موقع. غالبا ما يتم إستخدام بروتوكول الموجه الاحتياطي الفعال (HSRP) لتعقب حالة واجهة الموجهات لتحقيق تجاوز الفشل بين الموجهات. ومع ذلك، نظرا لعدم وجود إرتباط داخلي بين IPSec و HSRP، لا يتعقب HSRP حالة اقترانات أمان IPSec (SAs) ويتطلب IPSec مخططات للمزامنة مع تجاوز فشل HSRP عند حدوثه. هذه بعض الميزات البارزة للخطط المستخدمة لتوفير اقتران أوثق بين IPSec و HSRP:

- يتم إستخدام Keepalive لتبادل مفتاح الإنترنت (IKE) للسماح ل IPSec باكتشاف تجاوز فشل HSRP في الوقت المناسب.
- يتم ربط خريطة التشفير المطبقة على واجهة موجه معينة بمجموعة HSRP التي تم تكوينها بالفعل على تلك الواجهة لتوعية IPSec بإعداد HSRP. وهذا يسمح أيضا IPSec باستخدام عنوان IP الظاهري HSRP كهوية بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) لموجهات HSRP.
- يتم إستخدام ميزة إدخال المسار العكسي (RRI) للسماح بتحديثات معلومات التوجيه الديناميكية أثناء تجاوز فشل HSRP و IPSec.

ملاحظة: يوضح هذا المستند كيفية إستخدام بروتوكول الموجه الاحتياطي الفعال (HSRP) مع VPN. يتم إستخدام HSRP أيضا لتعقب إرتباطات ISP الفاشلة. راجع تحليل مستويات خدمة IP باستخدام عملية صدى ICMP من أجل تكوين إرتباطات ISP المكررة على الموجهات. هنا المصدر أداة المسحاج تخديد والغاية أداة ال isp.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموجّهات من السلسلة 7200 من Cisco
- برنامج IOS® الإصدار 12.3(7)T1-c7200-a3jk9s-mz.123-7.T1، T1 من Cisco

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

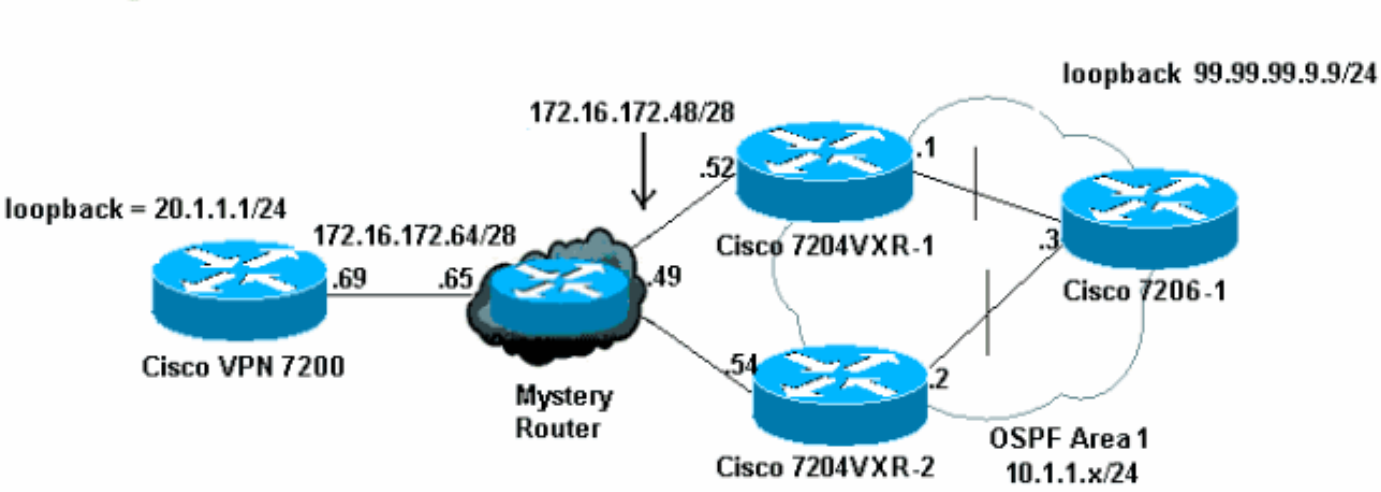
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين Cisco VPN 7200
- التكوين Cisco من 7204VXR-1
- التكوين Cisco من 7204VXR-2

- التكوين 7206-1 من Cisco

تكوين 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
```

التكوين 7204VXR-1 من Cisco

```
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
```

التكوين 2-7204VXR من Cisco

```
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
```

التكوين 7206-1 من Cisco

```
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
```

كيف تعمل؟

يوضح هذا المثال كيفية عمل التغلب على أعطال HSRP و IPSec معا باستخدام عمليتي الإعداد والتكوين المذكورتين أعلاه. تبرز دراسة الحالة هذه ثلاثة جوانب:

- تجاوز فشل HSRP بسبب فشل الواجهة.
- كيف يحدث تجاوز فشل IPSec بعد تجاوز فشل HSRP. كما يمكن ملاحظته، سيكون تجاوز فشل بروتوكول IPSec هنا عبارة عن تجاوز فشل "عديم الحالة".
- كيف يتم تحديث تغييرات معلومات التوجيه التي يتسبب فيها تجاوز الفشل بشكل ديناميكي ونشرها على الشبكات الداخلية.

ملاحظة: حركة مرور الاختبار هنا هي حزم بروتوكول رسائل التحكم في الإنترنت (ICMP) بين عنوان IP للاسترجاع الخاص ب 99.99.99.99) Cisco 7206-1) وعنوان IP للاسترجاع الخاص ب 20.1.1.1) Cisco VPN 7200) ويحاكي حركة مرور VPN بين الموقعين.

الظروف العادية (قبل تجاوز الفشل)

قبل تجاوز الفشل، يكون Cisco 7204VXR-1 هو موجه HSRP الرئيسي ويمتلك Cisco VPN 7200 IPSec SAs مع Cisco 7204VXR-1.

عندما يتم تكوين خريطة التشفير على الواجهة، تقوم ميزة RRI باحتواء مسار VPN لمطابقة قائمة التحكم في الوصول (ACL) التي تم تكوينها إلى IPSec وبيان أمر **تعيين النظير** في خريطة التشفير. تتم إضافة هذا المسار إلى جدول توجيه الموجه 7204VXR-1 الأساسي من HSRP.

يشير إخراج الأمر **debug crypto ipSec** إلى إضافة مسار VPN 20.1.1/24 إلى قاعدة معلومات التوجيه (RIB).

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

ينتج جدول التوجيه على موجه HSRP الأساسي مسار ثابت إلى 24/20.1.1، والذي يتم إعادة توزيعه من خلال فتح أقصر مسار أولا (OSPF) إلى الموجه HSRP الثانوي، 7204VXR-2، وإلى الموجه الداخلي، 7206-1.

الخطوة التالية لمسار VPN 20.1.1/24 التي تم حقنها كمسار ساكن إستاتيكي إلى نقطة الوصول (RIB) للموجه 7204VXR-1 هي عنوان IP الخاص بنظير التشفير البعيد. في هذه الحالة، ال التالي ل ال VPN ممر 24/20.1.1 هو 172.16.172.69. يتم حل عنوان IP الخاص بالخطوة التالية من مسار VPN عبر بحث مسار متكرر كما هو موضح في جدول إعادة التوجيه السريع هذا من Cisco:

```
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

is subnetted, 1 subnets 99.0.0.0/32
O 99.99.99.99 [110/2] via 10.1.1.3, 00:11:21, FastEthernet0/1
is subnetted, 1 subnets 20.0.0.0/24
S 20.1.1.0 [1/0] via 172.16.172.69
is subnetted, 2 subnets 172.16.0.0/28
C 172.16.172.48 is directly connected, FastEthernet0/0
S 172.16.172.64 [1/0] via 172.16.172.49
is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
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
version 66, epoch 0, cached adjacency 172.16.172.49 ,20.1.1.0/24
packets, 0 bytes 0
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
```

يتعلم الموجه الثانوي HSRP والموجه الداخلي 7206-1 مسار شبكة VPN هذا عبر OSPF/. لا يحتاج مسؤولو الشبكة إلى إدخال المسار الثابت يدويا. والأهم من ذلك، يتم تحديث تغييرات التوجيه التي يتسبب فيها تجاوز الفشل بشكل ديناميكي.

```
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

is subnetted, 1 subnets 99.0.0.0/32
O 99.99.99.99 [110/2] via 10.1.1.3, 00:29:31, FastEthernet1/0
is subnetted, 1 subnets 20.0.0.0/24
```

```
O E2     20.1.1.0 [110/20] via 10.1.1.1, 00:11:06, FastEthernet1/0
                                  is subnetted, 2 subnets 172.16.0.0/28
        C     172.16.172.48 is directly connected, FastEthernet0/0
                        S      172.16.172.64 [1/0] via 172.16.172.49
                  is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
                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

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

الموجه 7204VXR-1 هو موجه HSRP الأساسي الذي يتتبع الواجهة الداخلية Fa0/1.

```
                                                        7204VXR-1#show standby
                                                  FastEthernet0/0 - Group 1
                                                          State is Active
                                          state changes, last state change 03:21:20 2
                                                  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
```

يمكنك إستخدام الأمر **show track** لعرض قائمة بكافة الكائنات التي تم تعقبها بواسطة HSRP.

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

الموجه 7204VXR-2 هو الموجه HSRP الاحتياطي. في ظروف التشغيل العادية، يتتبع هذا الجهاز الواجهة الداخلية Fa1/0.

```
7204VXR-2#show standby
FastEthernet0/0 - Group 1
State is Standby
  state change, last state change 02:22:30 1
  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)
```

تقوم أوامر **العرض** هذه المتعلقة ب**IPSec** بالإخراج على الموجه Cisco VPN 7200 Router الذي يوضح شبكات ISAKMP و IPSec بين Cisco VPN 7200 وموجه HSRP الأساسي، 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  K         23:49:52   1  psk   md5   des
(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
                             QM_IDLE   1          0   172.16.172.69  172.16.172.53


                                                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
```

بعد تجاوز فشل HSRP و IPSec

تم تشغيل تجاوز الفشل بإيقاف تشغيل Fa0/0 على Cisco 7204VXR-1. سترى سلوكا مماثلا إذا كانت الواجهة الأخرى، Fa0/1، معطلة لأن HSRP يتعقب أيضا حالة هذه الواجهة.

عندما لا يستقبل Cisco VPN 7200 أي إستجابة لحزم IKE keepalive المرسلة إلى موجه HSRP الأساسي، يقوم الموجه بفك تشفير IPSec SAs.

يعرض إخراج أمر **debug crypto isakmp** هذا كيفية اكتشاف IKE keepalive لانقطاع اتصال الموجه الرئيسي:

```
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
```

عندما يحدث تجاوز الفشل على موجه HSRP الأساسي Cisco 7204VXR-1، يصبح الجهاز موجه إستعداد. تم تدمير شبكات ISAKMP و IPSec الحالية. يصبح الموجه HSRP Secondary Cisco 7204VXR-2 نشطا وينشئ شبكات IPSec جديدة باستخدام Cisco VPN 7200.

يعرض إخراج الأمر **debug standby events** الأحداث المتعلقة ب 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
```

نظرا لإيقاف تشغيل الواجهة، تتغير حالة HSRP إلى "Init".

```
paal#show standby
FastEthernet0/0 - Group 1
(State is Init (interface down
state changes, last state change 00:07:29 3
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
```

يصبح Cisco 7204VXR-2 هو موجه HSRP النشط ويغير حالته إلى "نشط".

```
(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
state changes, last state change 00:10:38 2
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
```

مع تمكين تقنية RRI، يتم تحديث مسارات الشبكات الخاصة الظاهرية (VPN) بشكل ديناميكي أثناء تجاوز الفشل. تتم إزالة المسار الثابت 24/20.1.1.0، ويتعلم الموجه Cisco 7204VXR-1 المسار من الموجه Cisco 7204VXR-2.

يوضح الإخراج من الأمر **show ip route** هذا التحديث الديناميكي.

```
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

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

يتم حقن مسار الشبكة الخاصة الظاهرية (VPN) الثابتة في جدول التوجيه على الموجه 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
```

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

يعلم الموجه الداخلي 7206-1 المسار 24/20.1.1 إلى نظير شبكة VPN البعيد من الموجه المجاور OSPF الخاص به، 7204VXR-2. تحدث تغييرات التوجيه هذه بشكل ديناميكي من خلال الجمع بين HSRP/RRI و 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

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

بعد أن يصبح 7204VXR-2 Cisco الموجه النشط أثناء تجاوز فشل HSRP، تجلب حركة مرور بيانات VPN بين 7204VXR-2 Cisco وموجه 7200 Cisco VPN وكيل Isakmp و IPSec SAs.

يتم عرض إخراج الأمر **show crypto isakmp sa** و**show crypto ipSec** على الموجه 7200 VPN هنا:

```
                                                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  23:53:47 K        172.16.172.69  172.16.172.53   1
                              des  md5   psk
                                                (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
                                  QM_IDLE 1       0   172.16.172.69   172.16.172.53

                                                  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
```

بعد إسترداد الموجه الأساسي HSRP الأصلي من انقطاع

بعد إسترداد الخدمة على الموجه الأساسي HSRP الأصلي 7204VXR-1 من Cisco، يستأنف الجهاز وضعه كموجه نشط لأنه يتمتع بأولوية أعلى ولأنه تم تكوين استباق HSRP.

يعرض إخراج الأمر **show** و**debug** من موجهات مختلفة محول آخر من HSRP و IPSec. تتم إعادة إنشاء شبكات ISAKMP و IPSec تلقائيا، ويتم تحديث تغييرات معلومات التوجيه بشكل ديناميكي.

يوضح إخراج النموذج هذا أن الموجه 7204VXR-1 يقوم بتغيير حالته إلى "نشط".

```
                                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
```

يغير الموجه 7204VXR-2 حالته إلى "وضع الاستعداد". تتم إزالة مسار شبكة VPN من جدول التوجيه.

```
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
```

معلومات ذات صلة

- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).