Настройка возможностей высокой готовности для сетей IPSec VPN конфигурации узел-узел

Содержание

Введение

Данный документ описывает новые компоненты с высоким уровнем доступности для сетей IPSec VPN между узлами. Протокол маршрутизатора горячего резервирования (HSRP) часто используется для отслеживания состояния интерфейсов маршрутизаторов для достижения отказоустойчивости между маршрутизаторами. Однако, поскольку никакой внутренней корреляции между IPSec и HSRP не существует, HSRP не отслеживает состояние сопоставлений безопасности IPSec (SA), а IPSec требует специальных схем для синхронизации с восстановлением при отказе HSRP. Освещаются некоторые из схем, используемых для обеспечения более тесной связи между IPSec и HSRP:

- IKE keepalive используется, чтобы IPSec мог своевременно обнаруживать переключение при отказе HSRP.
- Применяемая в заданном интерфейсе маршрутизатора криптокарта соединяется с группой HSRP, уже настроенной на этом интерфейсе, чтобы уведомить IPSec об установке HSRP. При этом также появляется возможность в IPSec использовать виртуальный IP-адрес HSRP в качестве идентификатора протокола ISAKMP для маршрутизаторов HSRP.
- Функция Reverse route injection (RRI) используется для разрешения обновлений сведений о динамической маршрутизации во время переключения при отказе HSRP и IPSec.

Примечание: Этот документ описывает, как использовать Протокол HSRP с VPN. HSRP также используется для отслеживания подведенных каналов поставщика. Для настройки

избыточных каналов поставщика на маршрутизаторах обратитесь к Анализу Уровней IP-сервиса Использование Эхо - операция ICMP. Здесь исходное устройство является маршрутизатором, и целевое устройство является устройством интернет-провайдера.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизаторы серии Cisco 7200
- Релиз 12.3 Программного обеспечения Cisco IOS (7) T1, c7200-a3jk9s-mz.123-7. T1

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация Cisco VPN 7200
- Конфигурация Cisco 7204VXR-1
- Cisco 7204VXR 2 конфигурации
- Конфигурация Cisco 7206-1

Конфигурация 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
```

Конфигурация 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
```

Cisco 7204VXR 2 конфигурации

```
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
```

Конфигурация 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
```

Принципы работы?

Данный пример демонстрирует, как HSRP и аварийное переключение IPSec сотрудничают с помощью вышеупомянутой настройки и конфигурации. Три аспекта выделены в этом примере практического применения:

- Восстановление HSRP после отказа интерфейса.
- Как происходит переключение при отказе IPSec после переключения после отказа HSRP. Как видно, аварийное переключение IPSec здесь будет аварийным переключением "не сохраняющим состояние".
- Как изменения маршрутной информации, вызванные аварийным переключением, динамично обновлены и распространяются к внутренним сетям.

Примечание: Тестовым трафиком здесь являются пакеты протокола ICMP (Internet Control Message Protocol) между IP-адресом обратной связи устройства Cisco 7206-1 (99.99.99.99) и IP-адресом обратной связи устройства Cisco VPN 7200 (20.1.1.1), что имитирует VPN-трафик между двумя узлами.

Обычное состояние (до перехвата управления при отказе)

Перед аварийным переключением Cisco 7204VXR 1 является основным маршрутизатором HSRP, и Cisco VPN 7200 имеет КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC с Cisco 7204VXR 1.

Когда криптокарта настроена на интерфейсе, функция RRI вводит маршрут VPN для соответствия с настроенным списком контроля доступа (ACL) IPSec и **одноранговым** командным оператором **набора** в криптокарте. Этот маршрут добавлен к таблице маршрутизации основного маршрутизатора HSRP 7204VXR-1.

Выходные данные **команды debug crypto ipsec** указывают на добавление маршрута VPN 20.1.1/24 к Routing Information Base (RIB).

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

Таблица маршрутизации на основном маршрутизаторе HSRP приводит к статическому маршруту 20.1.1/24, который перераспределен Протоколом OSPF к дополнительному маршрутизатору HSRP, 7204VXR-2, и к встроенному маршрутизатору, 7206-1.

Следующим переходом для маршрута VPN 20.1.1/24 введенный как статический маршрут в RIB маршрутизатора 7204VXR-1 является IP-адрес удаленного криптографического однорангового узла. В этом случае следующий переход для маршрута VPN 20.1.1/24 172.16.172.69. IP-адрес следующего перехода маршрута VPN решен через поиск рекурсивного маршрута как показано в этой таблице скоростной маршрутизации 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 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

Дополнительный маршрутизатор HSRP и встроенный маршрутизатор 7206-1 изучают этот маршрут VPN через OSPF/. Администраторы сети не должны вводить статический маршрут вручную. Что еще более важно, изменения маршрутизации, вызванные аварийным переключением, обновлены динамично.

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

Маршрутизатор 7204VXR-1 является основным маршрутизатором HSRP, который отслеживает внутренний интерфейс 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)

Можно использовать **команду show track** для наблюдения списка всех объектов, отслеженных 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**

Маршрутизатор 7204VXR-2 является резервным маршрутизатором HSRP. Под обычными рабочими условиями это устройство отслеживает внутренний интерфейс 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)
```

Эти СВЯЗАННЫЕ С IPSEC выходные данные урожая **команд показа** на маршрутизаторе Cisco VPN 7200, который демонстрирует ISAKMP и КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC между Cisco VPN 7200 и основным маршрутизатором HSRP, 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 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:
```

После восстановления при отказе HSRP и IPSec

Аварийное переключение было инициировано путем завершения Fa0/0 на Cisco 7204VXR 1. Вы будете видеть подобное поведение, если другой интерфейс, Fa0/1, не работает, потому что HSRP также отслеживает статус этого интерфейса.

Когда Cisco VPN 7200 не получает ответа на пакеты сообщения поддержки активности IKE, переданные к основному маршрутизатору HSRP, маршрутизатор разъединяет КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC.

Эти выходные данные **команды debug crypto isakmp** показывают, как сообщение поддержки активности IKE обнаруживает простой основного маршрутизатора:

```
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
```

Когда аварийное переключение происходит на Cisco 7204VXR 1 основной маршрутизатор HSRP, устройство становится резервным маршрутизатором. Существующий ISAKMP и КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC разъединены. Cisco 7204VXR 2 дополнительных маршрутизатора HSRP становятся активными и устанавливают новые КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC с Cisco VPN 7200.

Выходные данные **команды debug standby events** показывают события, отнесенные 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
```

Поскольку интерфейс закрыт, изменения состояния HSRP к "Init".

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

Cisco 7204VXR 2 становится активным маршрутизатором HSRP и изменяет его состояние на "Активный".

```
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)
```

С включенным RRI маршруты VPN обновлены динамично во время аварийного переключения. Статический маршрут 20.1.1.0/24 удален, и Cisco 7204VXR, 1 маршрутизатор изучает маршрут из Cisco 7204VXR 2 маршрутизатора.

Выходные данные от **команды show ip route** демонстрируют это динамическое обновление.

```
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
```

Статический маршрут VPN введен в таблицу маршрутизации на Cisco 7204VXR 2 маршрутизатора.

```
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

Встроенный маршрутизатор 7206-1 изучает маршрут 20.1.1/24 удаленному узлу VPN от его маршрутизатора окружения OSPF, 7204VXR-2. Эти изменения маршрутизации происходят динамично через комбинацию HSRP/RRI и 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

После того, как Cisco 7204VXR 2 становится активным маршрутизатором во время аварийного переключения HSRP, трафик VPN между Cisco 7204VXR 2 и маршрутизатором Cisco VPN 7200 переводит в рабочее состояние ISAKMP и КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC.

Выходные данные **show crypto isakmp sa** и **команд show crypto ipsec sa** на маршрутизаторе VPN 7200 показывают здесь:

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:

После того, как исходный главный маршрутизатор HSRP выйдет из состояния аварийного отключения

После того, как сервис восстанавливает на Cisco 7204VXR 1 исходный маршрутизатор основного HSRP, позицию резюме устройства как активный маршрутизатор, потому что это имеет более высокий приоритет и потому что настроен HSRP preempt.

Показ и **результаты выполнения команды debug** от других маршрутизаторов показывают другой переключатель HSRP и IPSec. ISAKMP и КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC восстановлены автоматически, и изменения маршрутной информации обновлены динамично.

Этот пример выходных данных показывает, что маршрутизатор 7204VXR-1 изменяет свое состояние на "Активный".

```
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
```

Маршрутизатор 7204VXR-2 изменяет свое состояние на "Резерв". Маршрут VPN удален из таблицы маршрутизации.

```
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
```

Дополнительные сведения

- Страница технической поддержки протоколов согласования IPSec и IKE
- Cisco Systems – техническая поддержка и документация