Configure IPsec Redundancy with HSRP for IKEv2 Route-based Tunnel on Cisco Routers

Contents

Introduction

This document describes how to Configure IPsec redundancy with HSRP for IKEv2 route-based tunnel on Cisco routers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Site-To-Site VPN
- Hot Standby Router Protocol [HSRP]
- Basic knowledge of IPsec & IKEv2

Components Used

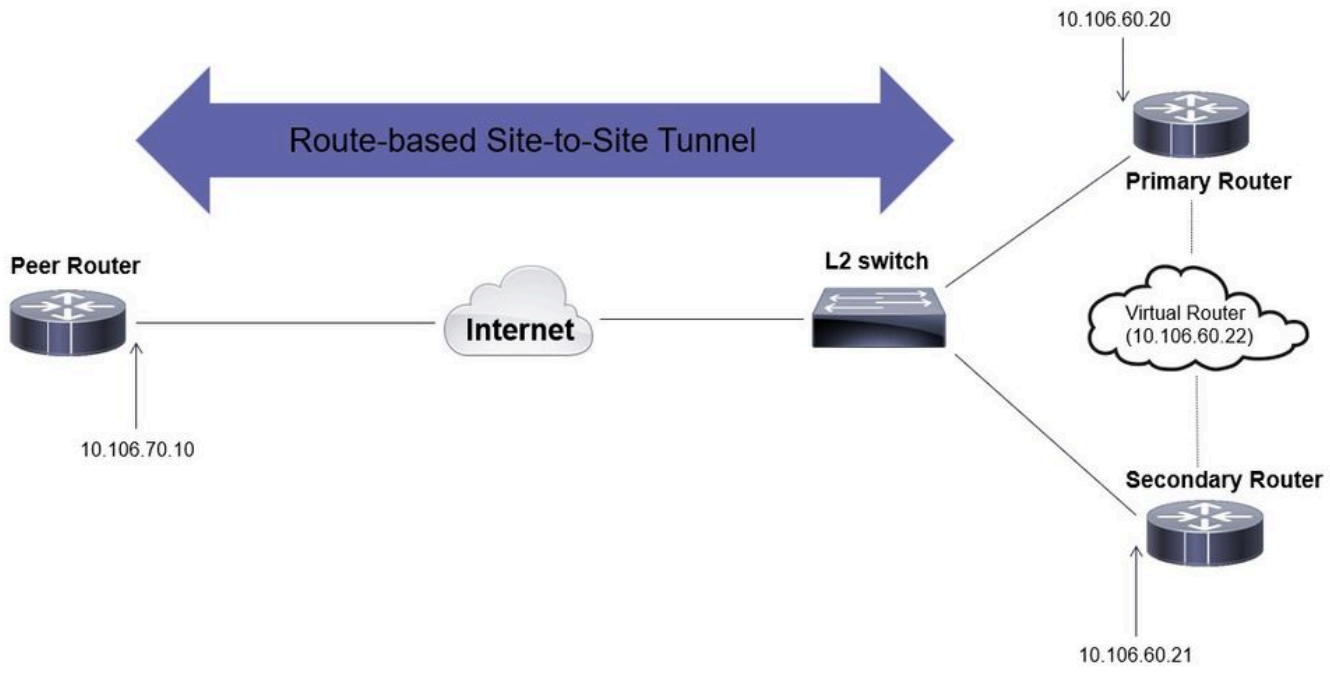
The information in this document is based on these software and hardware versions:

- Cisco CSR1000v router running IOS XE Software, version 17.03.08a
- Layer 2 switch running Cisco IOS Software, version 15.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Primary/Secondary Router Configurations

Configure the Physical Interface with HSRP

Configure the physical interfaces of the primary (with a higher priority) and the secondary (with a default priority of 100) routers:

Primary Router:

```
interface GigabitEthernet1
 ip address 10.106.60.20 255.255.255.0
 standby 1 ip 10.106.60.22
 standby 1 priority 105
 standby 1 preempt
 standby 1 name VPN-HSRP
```

Secondary Router:

```
interface GigabitEthernet1
 ip address 10.106.60.21 255.255.255.0
 standby 1 ip 10.106.60.22
 standby 1 preempt
 standby 1 name VPN-HSRP
```

Note: Ensure that the default primary router is configured with a higher priority in order to make it the active peer even when both routers are up and running without any issues. For this example, the primary has been configured with a priority of 105 whereas the secondary router has a priority of

100 (which is the default for HSRP).

Configure the IKEv2 Proposal and Policy

Configure an IKEv2 proposal with the encryption, hashing and DH group of your choice and map it to a IKEv2 policy.

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configure the Keyring

Configure the keyring to store the pre-shared key that will be used to authenticate the peer.

```
crypto ikev2 keyring keys
 peer 10.106.70.10
  address 10.106.70.10
  pre-shared-key local C!sco123
  pre-shared-key remote C!sco123
```

Configure the IKEv2 Profile

Configure the IKEv2 profile and attach the keyring to it. Set the local address to the virtual IP address being used for HSRP and the remote address as the IP of the internet-facing interface of the router.

```
crypto ikev2 profile IKEv2_PROF
 match identity remote address 10.106.70.10 255.255.255.255
 identity local address 10.106.60.22
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
```

Configure the IPsec Transform-Set

Configure the phase 2 parameters of encryption and hashing using the IPsec transform-set.

```
crypto ipsec transform-set ipsec-prop esp-aes 256 esp-sha256-hmac
```

Configure the IPsec Profile

Configure the IPsec profile to map the IKEv2 profile and the IPsec transform set. The IPsec profile will be applied to the tunnel interface.

```
crypto ipsec profile IPsec_PROF
 set transform-set ipsec-prop
 set ikev2-profile IKEv2_PROF
```

Configure the Virtual Tunnel Interface

Configure the virtual tunnel interface to specify the tunnel source and destination. These IPs will be used to encrypt the traffic over the tunnel. Ensure that the IPsec profile is also applied to this interface as shown below.

```
interface Tunnel0
 ip address 10.10.10.10 255.255.255.0
 tunnel source 10.106.60.22
 tunnel mode ipsec ipv4
 tunnel destination 10.106.70.10
 tunnel protection ipsec profile IPsec_PROF
```

Note: You will need to specify the virtual IP that is being used for HSRP as the tunnel source. Using the physical interface, in this scenario GigabitEthernet1, will cause the tunnel negotiation to fail.

Configure the Dynamic and/or Static Routing

You have to configure the routing with dynamic routing protocols and/or static routes depending on the requirement and the network design. For this example, a combination of EIGRP and a static route is used to establish the underlay communication and the flow of the overlay data traffic over the site-to-site tunnel.

```
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 10.106.60.0 0.0.0.255

ip route 192.168.30.0 255.255.255.0 Tunnel0
```

Note: Ensure that the tunnel interface subnet, which in this scenario is 10.10.10.0/24, is getting advertised.

Peer Router Configurations

Configure the IKEv2 Proposal and Policy

Configure an IKEv2 proposal with the encryption, hashing and DH group of your choice and map it to an IKEv2 policy.

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy IKEv2_POL
```

```
 proposal prop-1
```

Configure the Keyring

Configure the keyring to store the pre-shared key that will be used to authenticate the peer.

```
crypto ikev2 keyring keys
 peer 10.106.60.22
  address 10.106.60.22
  pre-shared-key local C!sco123
  pre-shared-key remote C!sco123
```

Note: The peer IP address used here will be the virtual IP address that is configured in the peer's HSRP configuration. Ensure that you are not configuring the keyring for the physical interface IP of the primary/secondary peer.

Configure the IKEv2 Profile

Configure the IKEv2 profile and attach the keyring to it. Set the local address as the IP of the internet-facing interface of the router and the remote address to the virtual IP address being used for HSRP on the primary/secondary peer.

```
crypto ikev2 profile IKEv2_PROF
 match identity remote address 10.106.60.22 255.255.255.255
 identity local address 10.106.70.10
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
```

Configure the IPsec Transform-Set

Configure the phase 2 parameters of encryption and hashing using the IPsec transform-set.

```
crypto ipsec transform-set ipsec-prop esp-aes 256 esp-sha256-hmac
```

Configure the IPsec Profile

Configure the IPsec profile to map the IKEv2 profile and the IPsec transform set. The IPsec profile will be applied to the tunnel interface.

```
crypto ipsec profile IPsec_PROF
 set transform-set ipsec-prop
 set ikev2-profile IKEv2_PROF
```

Configure the Virtual Tunnel Interface

Configure the virtual tunnel interface to specify the tunnel source and destination. The tunnel destination has to be set as the virtual IP used for HSRP on the primary/secondary peer. Ensure that the IPsec profile is also applied to this interface as shown.

```
interface Tunnel0
 ip address 10.10.10.11 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.106.60.22
 tunnel protection ipsec profile IPsec_PROF
```

Configure the Dynamic and/or Static Routing

Configure the required routes with dynamic routing protocols or static routes similar to how you have for the other endpoint.

```
router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.106.70.0 0.0.0.255

ip route 192.168.10.0 255.255.255.0 Tunnel0
```

Verify

To understand the expected behaviour, the following three scenarios are presented.

Scenario 1. Both Primary and Secondary Routers are Active

Since the primary router is configured with a higher priority, the IPsec tunnel gets negotiated and established on this router. To verify the state of the two routers, you can use the show standbycommand.

<#root>

```
pri-router#show standby
GigabitEthernet1 - Group 1

State is Active


7 state changes, last state change 00:00:21
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.864 secs
Preemption enabled

Active router is local



Standby router is 10.106.60.21, priority 100 (expires in 9.872 sec)


Priority 105 (configured 105)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 1/1

sec-router#show standby
GigabitEthernet1 - Group 1

State is Standby
```

```
11 state changes, last state change 00:00:49
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.888 secs
Preemption enabled

Active router is 10.106.60.20, priority 105 (expires in 8.768 sec)


Standby router is local


Priority 100 (default 100)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 0/1
```

To verify the phase 1 (IKEv2) and phase 2 (IPsec) security associations for the tunnel, you can use the `show crypto ikev2 sa`and `show crypto ipsec sa`commands.

```
pri-router#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id            Local          Remote         fvrf/ivrf   Status
1              10.106.60.22/500 10.106.70.10/500   none/none   READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify:
Life/Active Time: 86400/444 sec

IPv6 Crypto IKEv2 SA

pri-router#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.106.60.22

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.106.70.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 36357, #pkts encrypt: 36357, #pkts digest: 36357
#pkts decaps: 36354, #pkts decrypt: 36354, #pkts verify: 36354
#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.: 10.106.60.22, remote crypto endpt.: 10.106.70.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x4967630D(1231512333)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xBA711B5E(3127974750)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
```

```
conn id: 2216, flow_id: CSR:216, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607986/3022)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x4967630D(1231512333)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2215, flow_id: CSR:215, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607992/3022)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Scenario 2. Primary Router is Inactive and the Secondary Router is Active

In a scenario where the primary router experiences an outage or goes down, the secondary router will become the active router and the site-to-site tunnel will get negotiated with this router.

The HSRP state of the secondary router can again be verified using the `show standby` command.

<#root>

```
sec-router#show standby
GigabitEthernet1 - Group 1

State is Active


12 state changes, last state change 00:00:37
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.208 secs
Preemption enabled

Active router is local


Standby router is unknown
Priority 100 (default 100)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 1/1
```

Furthermore, you will also observe the following logs when this disruption occurs. These logs also show that the secondary router is now active and the Tunnel has been established.

```
*Jul 18 10:28:21.881: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Standby -> Active
*Jul 18 10:28:44.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to
```

To check the phase 1 and phase 2 security associations, you can again use the show crypto ikev2 saand show crypto ipsec saas shown here.

```
sec-router#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id            Local            Remote       fvrf/ivrf   Status
1               10.106.60.22/500 10.106.70.10/500  none/none   READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify:
Life/Active Time: 86400/480 sec

IPv6 Crypto IKEv2 SA

sec-router# show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.106.60.22

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.106.70.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 112, #pkts encrypt: 112, #pkts digest: 112
#pkts decaps: 112, #pkts decrypt: 112, #pkts verify: 112
#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.: 10.106.60.22, remote crypto endpt.: 10.106.70.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0xFC4207BF(4232185791)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x5F6EE796(1601103766)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2170, flow_id: CSR:170, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607988/3107)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
```

```
spi: 0xFC4207BF(4232185791)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2169, flow_id: CSR:169, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607993/3107)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Scenario 3. Primary Router Comes Back Up and the Secondary Goes on Standby

Once the primary router is restored and is no longer down, it becomes the active router again as it has a higher priority configured and the secondary router goes to standby mode.

During this scenario, you see these logs on the primary and secondary routers when this transition happens.

On the primary router, these logs appear:

```
*Jul 18 11:47:46.590: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Listen -> Active
*Jul 18 11:48:07.945: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to
```

On the secondary router, you see these logs that show that the secondary router has again become the standby router:

```
*Jul 18 11:47:46.370: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Active -> Speak
*Jul 18 11:47:52.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to
*Jul 18 11:47:57.806: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Speak -> Standby
```

To check the status of the Phase 1 and Phase 2 security associations, you can use the show crypto ikev2 saand **show crypto ipsec sa**to verify the same.

Note: If you have multiple tunnels configured on the routers which are up and running, you can use the show crypto session remote X.X.X.X and show crypto ipsec sa peer X.X.X.X commands to check the phase 1 and phase 2 status of the tunnel.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

These debugs can be enabled to troubleshoot the IKEv2 tunnel.

```
debug crypto ikev2
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
```

Note: If you wish to troubleshoot only one tunnel (which must be the case if the device is in production), you must enable conditional debugs using the command, debug crypto condition peer ipv4 x.x.x.x.