Cisco Virtual Office:
Deploying IP Security High Availability

This white paper provides detailed design and implementation information for deploying IP Security (IPsec) High Availability (HA) with Cisco® Virtual Office. Please refer to the Cisco Virtual Office overview (found at http://www.cisco.com/go/cvo) for further information about the solution, its architecture, and all of its components.

Introduction

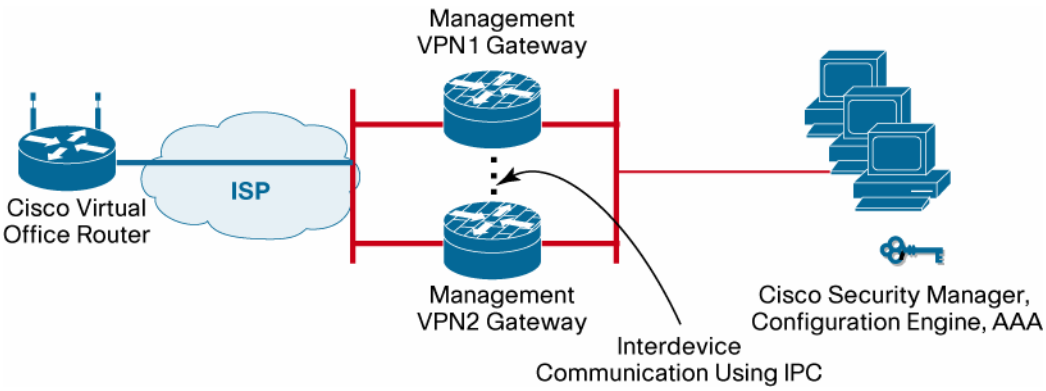
IPSec HA provides an infrastructure for reliable and secure networks, with the goal of providing transparent availability of VPN gateways (such as Cisco IOS® Software based routers). This feature works well for all IPSec-based networks. In the Cisco Virtual Office solution, IPsec HA can be used to provide redundancy—for example, stateful failover and rollback of the gateways—to provide uninterrupted management connectivity to the spokes. For more details on deploying Cisco Virtual Office, please refer to the links provided in the references section.

Topology

In the Cisco Virtual Office deployment, IPsec HA can be incorporated into the management gateways. The topology for the deployment is given in the Cisco Virtual Office overview at http://www.cisco.com/go/cvo.

Redundant management gateways can be deployed using IPsec HA as shown in Figure 1.

Figure 1. Topology for Deploying Redundant Management Gateways Using IPsec HA



Note: Both active and standby gateway routers should be the same platform type and have the same encryption card.

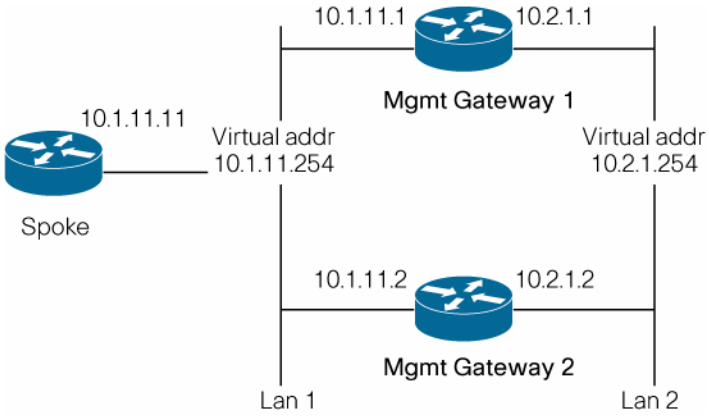
The Hot Standby Router Protocol (HSRP) is used to achieve redundancy between the management gateways. The spoke views the virtual IP address of the HSRP as the IP address of the management gateway. This setup allows any failover on management gateways to be transparent to the spoke. Once an IPsec session is established with the active router (management gateway), the corresponding session's Internet Key Exchange (IKE) security associations (SAs) and IPsec SAs are sent to the standby router, using interprocess

communication (IPC), and both the active and standby routers maintain the session information of the spoke. When the active management gateway goes down, the standby gateway takes over as active and handles the IPsec sessions transparently. This avoids the need to reestablish the session.

Configuration

Figure 2 shows the short version of the topology to map the IP addressing with the configuration examples given in the sections that follow.

Figure 2. Topology for Configuration Examples



The configuration examples provided here use public key infrastructure (PKI) so spokes connected using PKI will failover automatically.

The same deployment scenarion will also work with pre-shared keys.

Configuration on Management Gateway 1

```
! Configures redundancy and enters inter-device configuration mode.
redundancy inter-device
 scheme standby ha-in
!
!
! The commands below configure interprocess communication (IPC)
between the two gateways.
! “IPC zone default” initiates communication link between active and
standby routers.
! The subcommand “association” sets up association between active and
standby routers and
! uses the Stream Control Transmission Protocol (SCTP) as the
transport protocol. The next few
! lines define the local and remote SCTP port and IP address. Note,
though, that local port
! defined on this router should match the remote port configured on
peer router. The local and
! remote IP address should NOT be virtual IP address. The path-
retransmit defines number of
! SCTP retries before failing an association, and retransmit-timeot
defines maximum amount of
! time SCTP waits before retransmitting data
```

```
ipc zone default
 association 1
no shutdown
protocol sctp
    local-ip 10.2.1.1
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.2.1.2
!
!
! Define trustpoint
crypto pki trustpoint cvo-ios-ca-server
 enrollment mode ra
 enrollment url http://enrollment_url
 serial-number
 subject-name cn=sname
 revocation-check none
 auto-enroll 70
!
!
! Specify isakmp policy
crypto isakmp policy 1
 encr aes 256
!
!
! Specify the transform set
crypto ipsec transform-set t2 esp-aes 256 esp-sha-hmac
!
!
! This command allows the user to modify the interval in which an IP
redundancy-enabled crypto
! map sends anti-replay updates from the active router to the standby
router
crypto map ha_dynamic redundancy replay-interval inbound 10 outbound
1000
!
!
! This interface redundancy is configured using HSRP. This interface
is used for inter-device
! communication using SCTP protocol between active and standby
gateways
interface GigabitEthernet0/3
 ip address 10.2.1.1 255.255.255.0
 standby delay minimum 30 reload 60
 standby 2 ip 10.2.1.254
 standby 2 timers 1 10
 standby 2 preempt
 standby 2 name ha-in
 standby 2 track Ethernet1/1
```

```
!
!
! This interface is configured for redundancy using HSRP. The spoke
communicates with the
! active management gateway using the virtual IP address of this
interface
interface Ethernet1/1
 ip address 10.1.11.1 255.255.0.0
 standby delay minimum 30 reload 60
 standby 1 ip 10.1.11.254
 standby 1 timers 1 10
 standby 1 preempt
 standby 1 name ha-out
 standby 1 track GigabitEthernet0/3
 crypto map ha_dynamic redundancy ha-out stateful
```

Configuration on Management Gateway 2

```
! Configures redundancy and enters inter-device configuration mode.
Currently only “standby”
! scheme is supported. Note that the name of the standby “ha-in” must
match with the standby
! group name defined under the interface
redundancy inter-device
 scheme standby ha-in
!
!
! Define trustpoint
crypto pki trustpoint cvo-ios-ca-server
 enrollment mode ra
 enrollment url http://enrollment_url
 serial-number
 subject-name cn=s_name
 revocation-check none
 auto-enroll 70
!
! Specify isakmp policy
crypto isakmp policy 1
 encr aes 256
!
!
! Specify the transform set
crypto ipsec transform-set t2 esp-aes 256 esp-sha-hmac
!
!
! Configures inter-device communication and uses SCTP transport
protocol to communicate
! between active and standby association
ipc zone default
 association 1
```

```
no shutdown
protocol sctp
    local-ip 10.2.1.2
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.2.1.1
!
!
! This command allows the user to modify the interval at which an IP
redundancy-enabled crypto
! map sends anti-replay updates from the active router to the standby
router
crypto map ha_dynamic redundancy replay-interval inbound 10 outbound
1000
!
!
! This interface redundancy is configured using HSRP. This interface
is used for inter-device
! communication using SCTP protocol between active and standby
gateways
interface GigabitEthernet0/3
 ip address 10.2.1.2 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex auto
 speed 10
 media-type rj45
 no negotiation auto
 standby delay minimum 30 reload 60
 standby 2 ip 10.2.1.254
 standby 2 timers 1 10
 standby 2 preempt
 standby 2 name ha-in
!
!
! This interface is configured for redundancy using HSRP. The spoke
communicates with the
! active management gateway using the virtual IP address of this
interface
interface Ethernet1/1
 ip address 10.1.11.2 255.255.0.0
 standby delay minimum 30 reload 60
 standby 1 ip 10.1.11.254
 standby 1 timers 1 10
 standby 1 preempt
 standby 1 name ha-out
 standby 1 track GigabitEthernet0/3
 crypto map ha_dynamic redundancy ha-out stateful
```

Configuration on Spoke

```
! Specify trustpoint
crypto pki trustpoint cvo-ios-ca-server
 enrollment mode ra
 enrollment url http://enrollment_url
 serial-number
 ip-address none
 revocation-check none
 source interface BVI1
 auto-enroll 75
!
!
! Specify isakmp policy
crypto isakmp policy 1
 encr aes 256
!
!
! Specify the transform set
crypto ipsec transform-set t2 esp-aes 256 esp-sha-hmac
!
!
! Specify the crypto map
crypto map test_1 1 ipsec-isakmp
 set peer 10.1.11.254
 set transform-set t2
 match address test_1
!
!
! Apply crypto map to interface
interface FastEthernet4
 ip address 110.1.11.11 255.255.0.0
 duplex auto
 crypto map test_1
!
!
! Define ACL for traffic to encrypt
ip access-list extended test_1
 permit ip host 10.1.11.11 host 10.2.1.254
 …
```

Troubleshooting and Show Commands

To help troubleshoot possible HSRP-related configuration problems, issue any of the following HSRP-related debug commands.

`debug standby errors`	`Debug HSRP errors`
`debug standby events`	`Debug HSRP events`
`debug standby packets [terse]`	`Display all HSRP packets except hellos and advertisements`

To help troubleshoot possible interdevice configuration problems, issue the following command.

`debug redundancy`	Debug Redundancy Facility options

To help troubleshoot possible IPSec HA-related problems, issue any of the following commands.

`debug crypto ha`	Debug Crypto High Availability (generic) debug
`debug crypto ipsec ha detail`	Debug IPsec High Availability detailed
`debug crypto ipsec ha update`	Debug IPsec High Availability updates
`debug crypto isakmp ha`	Debug ISAKMP High Availability

The following show and clear commands display the state of the devices and the state of crypto sessions.

`show redundancy [states | inter-device]`	Show Redundancy Facility states or interdevice information, respectively
`show standby`	Show HSRP information
`show crypto isakmp sa [active | standby]`	Show HA-enabled ISAKMP SAs in the active or standby state, respectively
`show crypto ipsec sa [active | standby]`	Show HA-enabled IPSec SAs in the active or standby state, respectively
`show crypto session [active | standby]`	Show HA-enabled crypto sessions in the active or standby state, respectively
`show crypto ha`	Show Crypto High Availability information
`clear crypto isakmp [active | standby]`	Clear all HA-enabled IKE SAs in active or standby state, respectively
`clear crypto sa [active | standby]`	Clear all HA-enabled IPSec SAs in active or standby state, respectively
`clear crypto session [active | standby]`	Clear HA-enabled crypto sessions in the active or standby state, respectively

Deployment Considerations

- IPsec HA is supported only on limited platforms. The platform list includes the Cisco 7206 and 7301 Routers, the Cisco 3800 Integrated Services Router, and the Cisco 6500 Catalyst Switch.

- When a router is first configured for interdevice redundancy, the router has to be reloaded for the configuration to take effect.
- When one of the interfaces of an active router goes down, the standby takes over as active and handles all the operations. However, the previous active undergoes a reload and eventually stabilizes as standby (provided the priority of the router is at or below the current active router).
- It is mandatory that the routers be connected via a hub or a switch. In the event that routers are connected back to back, note that anytime the active router reloads, the standby also reloads. This defeats the purpose of IPsec HA.

References

- Configuration guide for stateful failover for IPsec: http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d03f2.html#wp1049370
- HSRP FAQ: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml
- CVO Deployment Guide: http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns430/ns855/deployment_guide_c22-493157.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-492665-00 09/08