Cisco IOS Classic Firewall Stateful Failover High Availability Solution

Introduction

Stateful Failover for the Cisco IOS® Firewall allows a router to continue processing and forwarding firewall session packets after a planned or unplanned outage occurs. A backup (secondary) router automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent and requires neither adjustment nor reconfiguration of any remote peer.

Cisco IOS Classic Firewall

Cisco IOS Classic Firewall creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered Cisco IOS Classic Firewall when exiting through the firewall.

Stateful Failover for the Cisco IOS Firewall

Stateful Failover for the Cisco IOS Firewall is designed to work in conjunction with Stateful Switchover (SSO) and Hot Standby Router Protocol (HSRP).

HSRP provides network redundancy for IP networks, helping ensure that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. That is, HSRP monitors both the inside and outside interfaces so that if either interface goes down, the whole router is deemed to be down and ownership of firewall sessions is passed to the standby router (which transitions to the HSRP active state).

SSO allows the active and standby routers to share firewall session state information so that each router has enough information to become the active router at any time. To configure Stateful Failover for the Cisco IOS Firewall, a network administrator should enable HSRP, assign a virtual IP (VIP) address, and enable the SSO protocol.

Note: High Availability Stateful Failover supports only Cisco IOS Classic Firewall and does not support Cisco IOS Zone-Based Firewall.

Enabling HSRP: IP Redundancy and a Virtual IP Address

HSRP provides two services—IP redundancy and a VIP address. Each HSRP group can provide either or both of these services. Cisco IOS Firewall Stateful Failover uses the IP redundancy services from only one HSRP standby group. It can use the VIP address from one or more HSRP groups. Use the following guidelines to configure HSRP on the outside and inside interfaces of the router.

- Both the inside (private) and outside (public) interfaces must belong to separate HSRP groups, but the HSRP group number can be the same.

- The state of the inside and outside interfaces must be the same -- both interfaces must be in the active state or standby state; otherwise, the packets will not have a route out of the private network.
- Standby priorities should be equal on both active and standby routers. If the priorities are not equal, the higher-priority router will unnecessarily take over as the active router, negatively affecting uptime.
- The interface access control list (ACL) should allow HSRP traffic to flow through.

Each time an active device relinquishes control to become the standby device, the active device reloads. This function helps ensure that the state of the new standby device synchronizes correctly with the new active device.

SSO: Interacting Between the Cisco IOS Firewall Session

SSO is a method of providing redundancy and synchronization for many Cisco IOS Software applications and features. It is necessary for the Cisco IOS Firewall to learn about the redundancy state of the network and to synchronize its internal application state with its redundant peers.

Prerequisites: The HSRP should be configured before enabling SSO.

Prerequisites and Restrictions for Stateful Failover

- This document assumes that you have a complete Cisco IOS Firewall configuration on both active and standby routers.
- The Cisco IOS Firewall configuration that is set up on the active device must be duplicated on the standby device, including firewall protocols inspected, the interface ACLs, the global firewall settings, and the interface firewall configuration.
- Both the active and standby devices must run the identical version of the Cisco IOS Software, and both the active and standby devices must be connected through a hub or switch.
- HSRP requires the inside interface to be connected through LANs.

Device Requirements

- The active and standby Cisco IOS Software routers must be running the same Cisco IOS Software release: Release 12.4(6) T or later.
- Stateful Failover for the Cisco IOS Firewall requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, and they should have the same CPU and memory.

Supported Deployment Scenarios: Stateful Failover for the Cisco IOS Firewall

It is recommended that you implement Stateful Failover in one of the following deployment scenarios:

- Dual-LAN interface
- LAN-WAN interface

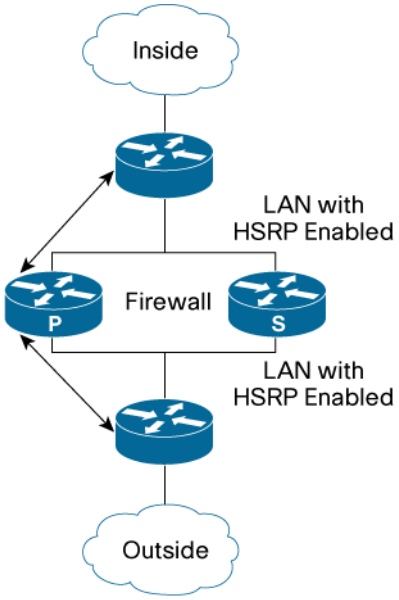
Dual-LAN Interface

In a dual-LAN-interface scenario, the active and standby routers running the firewall are connected to each other through a LAN interface on both the inside and outside (Figure 1).

HSRP is configured on both the inside and outside interfaces. The next-hop routers in this scenario talk to the High Availability pair through the virtual IP address. In this scenario there are two virtual IP addresses, one on the inside and the other on the outside.

Virtual IP addresses cannot be advertised using routing protocols. You need to create static routes on the next hops to get to the virtual IP address.

Figure 1. Dual-Interface Network Topology



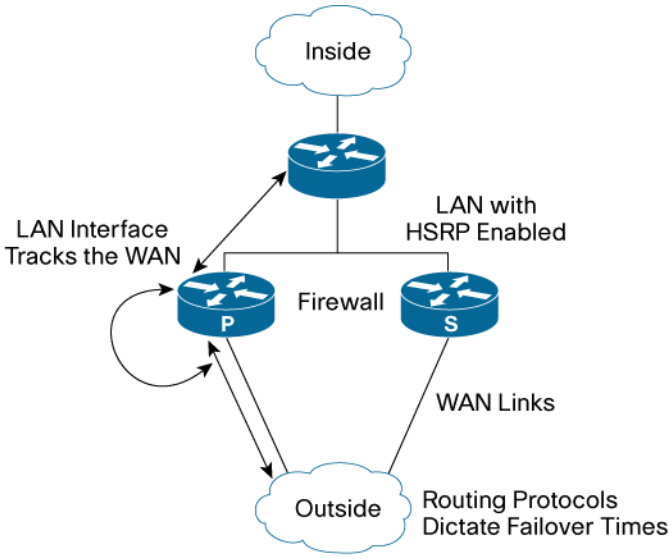
LAN-WAN Interface

In a LAN-WAN scenario, the inside interface of the active standby pair running the firewall is connected through a LAN interface on the inside and a WAN interface on the outside (Figure 2). HSRP is configured on the inside interface. The inside network communicates with the High Availability pair using the inside virtual IP address.

You should configure HSRP tracking on the inside LAN interfaces to track the state of the outside WAN interface. If the outside WAN interface goes down on the active router, the LAN interface that is tracking it reduces the HSRP priority and initiates a failover to the standby router. Traffic from the outside flowing into the HSRP pair should now be directed to the new active device.

In the scenario where the LAN interfaces track the WAN interfaces, the failover to the standby router happens immediately. However, for traffic to start flowing on the new active router, routing convergence needs to happen. The net failover time is dictated by the routing protocol.

Figure 2. LAN WAN Network Topology



How to Configure Stateful Failover for Cisco IOS Firewalls

Configuration tasks for Stateful Failover include:

- Enabling HSRP: IP Redundancy and a Virtual IP Address
- Enabling SSO
- Enabling Stateful Failover for a Cisco IOS Firewall
- Configuring the Cisco IOS Classic Firewall High Availability Update Interval

Enabling HSRP: IP Redundancy and a Virtual IP Address

Use the following commands to enable HSRP on both interfaces of each router (Table 1):

1. **enable**
2. **configure terminal**
3. **interface** type number
4. **standby** standby-group-number **name** standby-group-name
5. **standby** standby-group-number **ip** ip-address
6. **standby** standby-group-number **track** interface-name
7. **standby** [group-number] **preempt**
8. **standby** [group-number] **timers [msec] hellotime** [msec] **holdtime**
9. **standby delay minimum** [min-delay] **reload** [reload-delay]
10. Repeat.

Table 1. Enabling HSRP

	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode
Step 3	**interface** *type number* Example: Router(config)# interface Ethernet 0/0	Configures an interface type for the router and enters interface configuration mode
Step 4	**standby** *standby-group-number* **name** *standby-group-name* Example: Router(config-if)# standby 1 name HA-out	Assigns a user-defined group name to the HSRP redundancy group **Note:** The *standby-group-number* argument should be the same for both routers that are on directly connected interfaces. However, the *standby-group-name* argument should be different between two (or more) groups on the same router. The *standby-group-number* argument can be the same on the other pair of interfaces as well.
Step 5	**standby** *standby-group-number* **ip** *ip-address* Example: Router(config-if)# standby 1 ip 209.165.201.1	Assigns an IP address that is to be “shared” among the members of the HSRP group and owned by the primary IP address **Note:** The virtual IP address must be configured identically on both routers (active and standby) that are on directly connected interfaces.
Step 6	**standby** *standby-group-number* **track** *interface-name* Example: Router(config-if)# standby 1 track Ethernet1/0	Configures HSRP to monitor the second interface so that if either of the two interfaces goes down, HSRP causes failover to the standby device **Note:** Although this command is not required, it is recommended for dual-interface configurations.
Step 7	**standby** [*group-number*] **preempt** Example: Router(config-if)# standby 1 preempt	Enables the active device to relinquish control because of an interface tracking event
Step 8	**standby** [*group-number*] **timers** [msec] *hellotime* [msec] *holdtime* Example: Router(config-if)# standby 1 timers 1 5	(Optional) Configures the time between hello packets and the time before other routers declare the active hot standby or standby router to be down • *holdtime:* Holdtime is the amount of time the routers take to detect types of failure. A larger hold time means that failure detection will take longer. For the best stability, it is recommended that you set the hold time between 5 and 10 times the hello interval time; otherwise, a failover could falsely occur when no actual failure has happened.
Step 9	**standby delay minimum** [*min-delay*] **reload** [*reload-delay*] Example: Router(config-if)# standby delay minimum 120 reload 120	Configures the delay period before the initialization of HSRP groups **Note:** It is suggested that you enter 120 as the value for the *reload-delay* argument and leave the *min-delay* argument at the preconfigured default value.
Step 10	Repeat.	Repeats this task on both routers (active and standby) and on both interfaces of each router.

Examples

The following example shows how to configure HSRP on a router:

```
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
```

```
 standby 1 track Ethernet1/0
 standby delay minimum 120 reload 120
```

After you have successfully configured HSRP on both the inside and outside interfaces, you should enable SSO as described in the following section.

Enabling SSO

Use the following commands to enable SSO, which is used to transfer Cisco IOS Firewall session state information between two routers (Table 2):

1. **enable**
2. **configure terminal**
3. **redundancy inter-device**
4. **scheme standby** standby-group-name
5. **exit**
6. **ipc zone default**
7. **association 1**
8. **protocol sctp**
9. **local-port** local-port-number
10. **local-ip** device-real-ip-address [device-real-ip-address2]
11. **retransmit-timeout** retran-min [msec] retran-max [msec]
12. **path-retransmit** max-path-retries
13. **assoc-retransmit** retries
14. **exit**
15. **remote-port** remote-port-number
16. **remote-ip** peer-real-ip-address [peer-real-ip-address2]

Table 2. Enabling SSO

	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode
Step 3	**redundancy** inter-device Example: Router(config)# redundancy inter-device	Configures redundancy and enters interdevice configuration mode To exit interdevice configuration mode, use the **exit** command. To remove all interdevice configurations, use the **no** form of the command.
Step 4	**scheme standby** *standby-group-name* Example: Router(config-red-interdevice)# scheme standby HA-in	Defines the redundancy scheme that is to be used; currently, "standby" is the only supported scheme • *standby-group-name*: Must match the standby name specified in the **standby name** interface configuration command. Also, the standby name should be the same on both routers. **Note:** Only the active or standby state of the standby group is used for SSO. The VIP address of the standby group is neither required nor used by SSO.
Step 5	exit Example: Router(config-red-interdevice)# exit	Exits interdevice configuration mode

	Command or Action	Purpose
Step 6	ipc zone default Example: Router(config)# ipc zone default	Configures the interdevice communication protocol, Inter-Process Communication (IPC), and enters IPC zone configuration mode Use this command to initiate the communication link between the active router and standby routers.
Step 7	association 1 Example: Router(config-ipczone)# association 1	Configures an association between the two devices and enters IPC association configuration mode
Step 8	protocol sctp Example: Router(config-ipczone-assoc)# protocol sctp	Configures Stream Control Transmission Protocol (SCTP) as the transport protocol and enters SCTP protocol configuration mode
Step 9	**local-port** *local-port-number* Example: Router(config-ipc-protocol-sctp)# local-port 5000	Defines the local SCTP port number that is used to communicate with the redundant peer and puts you in IPC transport-SCTP local configuration mode • *local-port-number*: There is not a default value. This argument must be configured for the local port to enable interdevice redundancy. Valid port values are 1 to 65535. The local port number should be the same as the remote port number on the peer router.
Step 10	**local-ip** *device-real-ip-address* [*device-real-ip-address2*] Example: Router(config-ipc-local-sctp)# local-ip 10.0.0.1	Defines at least one local IP address that is used to communicate with the redundant peer The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global Virtual Route Forwarding (VRF) process. A virtual IP address cannot be used.
Step 11	**retransmit-timeout** *retran-min* [*msec*] *retran-max* [*msec*] Example: Router(config-ipc-local-sctp)# retransmit-timeout 300 10000	Configures the maximum amount of time, in milliseconds, that SCTP waits before retransmitting data • *retran-min*: 300 to 60000; default: 300 • *retran-max*: 300 to 60000; default: 600
Step 12	**path-retransmit** *max-path-retries* Example: Router(config-ipc-local-sctp)# path-retransmit 10	Configures the number of consecutive retransmissions SCTP performs before failing a path within an association • *max-path-retries*: 2 to 10; default: 4 retries
Step 13	**assoc**-interface Ethernet0/0 *retries* Example: Router(config-ipc-local-sctp)# ip address 209.165.201.1 255.255.255.224 -retransmit 10	Configures the number of consecutive retransmissions SCTP performs before failing an association • *retries*: 2 to 10; default: 4 retries
Step 14	**exit** Example: Router(config-ipc-local-sctp)# exit	Exits IPC transport-SCTP local configuration mode
Step 15	**remote-port** *remote-port-number* Example: Router(config-ipc-protocol-sctp)# remote-port 5000	Defines the remote SCTP port number that is used to communicate with the redundant peer and puts you in IPC transport-SCTP remote configuration **Note:** *remote-port-number*: There is not a default value. This argument must be configured for the remote port to enable interdevice redundancy. Valid port values are 1 to 65535. The remote port number should be the same as the local port number on the peer router.
Step 16	**remote-ip** *peer-real-ip-address* [*peer-real-ip-address2*] Example: Router(config-ipc-remote-sctp)# remote-ip 10.0.0.2	Defines at least one remote IP address of the redundant peer that is used to communicate with the local device All remote IP addresses must refer to the same device. A virtual IP address cannot be used.

Examples

The following example shows how to enable SSO:

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 10
   remote-port 5000
    remote-ip 10.0.0.2
!
```

Enabling Stateful Failover for a Cisco IOS Firewall

Use the following commands to enable Stateful Failover for the Cisco IOS Firewall (Table 3):

1. enable
2. configure terminal
3. interface [interface-name]
4. ip inspect [rule] in |out redundancy stateful [hsrp-group-name]
5. exit

Table 3. Enabling Stateful Failover

	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode
Step 3	**interface [interface-name]** Example: Router (config)# interface interface1	Defines the interface
Step 4	**ip inspect [rule] in|out redundancy stateful [hsrp-group-name]** Example: Router (config)# ip inspect rule1 in/out redundancy stateful group101	Enables Stateful Failover for this inspect rule **Note:** The hsrp-group-name is the same hsrp-group-name used in the SSO configuration.
Step 5	**exit** Example: Router (config)# exit	Exits global configuration mode

Configuring the Cisco IOS Firewall High Availability Update Interval

Use the following commands to change the amount of time between each update to the standby router (Table 4). The default interval is 10 seconds.

1. **enable**
2. **configure terminal**
3. **ip inspect redundancy update seconds** [10-60]
4. **exit**

Table 4. Configuring Cisco IOS Firewall High Availability Update Interval

	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode
Step 3	ip inspect redundancy update seconds [10-60] Example: Router (config)# ip inspect redundancy upate seconds 20	Changes the amount of time between each update to the standby router; the default interval of 10 seconds is used if you do not specify a value
Step 4	**exit** Example: Router (config)# exit	Exits global configuration mode

Configuration Examples for Stateful Failover

This section includes configurations of the active and standby routers.

RouterA

```
RouterA#sh run
Building configuration...

Current configuration : 2502 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby HAin
!
!
redundancy
```

```
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 10
   remote-port 5000
    remote-ip 10.0.0.2
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
no network-clock-participate slot 1
!
!
ip cef
!
!
ip inspect max-incomplete high 20000000
ip inspect max-incomplete low 20000000
ip inspect one-minute high 20000000
ip inspect one-minute low 20000000
ip inspect tcp idle-time 36000
ip inspect tcp max-incomplete host 20000000 block-time 0
ip inspect name ha-protocols tcp
ip inspect redundancy update seconds 30
!
voice-card 0
 no dspfarm
!
!
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex full
 speed 100
 media-type rj45
 standby delay minimum 120 reload 120
 standby 1 ip 10.0.0.3
 standby 1 timers 1 5
 standby 1 preempt
 standby 1 name HAin
 standby 1 track GigabitEthernet0/1
```

```
!
interface GigabitEthernet0/1
 ip address 211.0.0.1 255.255.255.0
 ip access-group fw-ha-acl in
 ip inspect ha-protocols out redundancy stateful HAin
 duplex auto
 speed auto
 media-type rj45
 standby delay minimum 120 reload 120
 standby 2 ip 211.0.0.3
 standby 2 timers 1 5
 standby 2 preempt
 standby 2 name HAout
 standby 2 track GigabitEthernet0/0
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
!
interface FastEthernet0/1/8
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
!
```

```
interface Vlan1
 no ip address
!
ip route 0.0.0.0 0.0.0.0 80.80.80.1
!
!
ip http server
no ip http secure-server
!
ip access-list extended fw-ha-acl
 permit ip host 211.0.0.2 host 211.0.0.1
 permit ip host 211.0.0.1 host 211.0.0.2
 deny   ip any any
!
ip sla responder

!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line 130
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end

RouterA#
```

RouterB

```
RouterB#sh run
Building configuration...

Current configuration : 2088 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby HAin
!
!
redundancy
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 10
   remote-port 5000
    remote-ip 10.0.0.2
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
!
!
ip cef
!
!
ip inspect max-incomplete high 20000000
ip inspect max-incomplete low 20000000
```

```
ip inspect one-minute high 20000000
ip inspect one-minute low 20000000
ip inspect tcp idle-time 36000
ip inspect tcp max-incomplete host 20000000 block-time 0
ip inspect name ha-protocols tcp
ip inspect redundancy update seconds 30
!
!
voice-card 0
 no dspfarm
!
!
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex full
 speed 1000
 media-type rj45
 standby delay reload 120
 standby 1 ip 10.0.0.3
 standby 1 timers 1 5
 standby 1 preempt
 standby 1 name HAin
 standby 1 track GigabitEthernet0/1
!
interface GigabitEthernet0/1
 ip address 211.0.0.1 255.255.255.0
 ip access-group fw-ha-acl in
 ip inspect ha-protocols out redundancy stateful HAin
 duplex full
 speed 1000
 media-type rj45
 standby delay reload 120
 standby 2 ip 211.0.0.3
 standby 2 timers 1 5
 standby 2 preempt
 standby 2 name HAout
 standby 2 track GigabitEthernet0/0
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
```

```
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
!
interface FastEthernet0/1/8
!
interface Vlan1
 no ip address
!
!
!
ip http server
no ip http secure-server
!
ip access-list extended fw-ha-acl
 permit ip host 211.0.0.2 host 211.0.0.1
 permit ip host 211.0.0.1 host 211.0.0.2
 deny   ip any any
!
ip sla responder
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end

RouterB#
```

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 C11-472858-00 05/08