Zone-Based Policy Firewall High Availability

The Zone-Based Policy Firewall High Availability feature enables you to configure pairs of devices to act as backup for each other. High availability can be configured to determine the active device based on a number of failover conditions. When a failover occurs, the standby device seamlessly takes over and starts forwarding traffic and maintaining a dynamic routing table. The Zone-Based Policy Firewall High Availability feature supports active/active high availability, active/standby high availability, and asymmetric routing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Zone-Based Policy Firewall High Availability

- Interfaces attached to a firewall must have the same redundant interface identifier (RII).
- The active and standby devices must have the same zone-based policy firewall configuration.
- The active and standby devices must run on an identical version of the Cisco software. The active and standby devices must be connected through a switch.

- For asymmetric routing traffic to pass, you must configure the pass action for the class-default class.
- If you configure a zone pair between two LAN interfaces, ensure that you configure the same redundancy group (RG) on both interfaces. The zone pair configuration is not supported if LAN interfaces belong to different RGs.

Restrictions for Zone-Based Policy Firewall High Availability

- Asymmetric routing is not supported on interfaces that are a part of a redundancy group (RG).
- Asymmetric routing should not be used for load sharing of WAN links because very high asymmetric routing traffic can cause performance degradation of devices.
- A Layer 2 interface that is converted to a Layer 3 interface by using the **no switchport** command should not be used as a redundancy control link or a data link.
- In an active/active redundancy scenario, there should not be any traffic flow between the interfaces that are part of different RGs. For traffic flow between interfaces, both the interfaces should be part of the same zone or of a different zone with pass action configured between the zones.
- Multiprotocol Label Switching (MPLS) is not supported on asymmetric routing.
- Layer 7 inspection is not HA-aware. If Layer 7 inspection is enabled and the active RG goes down, only Layer 4 sessions will be synchronized to the standby RG; Layer 7 sessions have to be reestablished with the server.
- Zone-based policy firewall supports only Layer 4 protocol inspection with redundancy.
- VRFs are not supported and cannot be configured under ZBFW High Availability data and control interfaces.
- Configuring zone-based policy firewall high availability with NAT and NAT high availability with zone-based policy firewalls is not recommended.

Information About Zone-Based Policy Firewall High Availability

Zone-Based Policy Firewall High Availability Overview

High availability enables network-wide protection by providing fast recovery from faults that may occur in any part of a network. High availability enables rapid recovery from disruptions to users and network applications.

The zone-based policy firewall supports active/active and active/standby high availability failover and asymmetric routing.

The active/active failover allows both devices involved in the failover to forward traffic simultaneously.

When active/standby high availability failover is configured, only one of the devices involved in the failover handles the traffic at one time, while the other device is in a standby mode, periodically synchronizing session information from the active device.

Asymmetric routing supports the forwarding of packets from a standby redundancy group to an active redundancy group for packet handling. If this feature is not enabled, the return TCP packets forwarded to the device that did not receive the initial synchronization (SYN) message are dropped because they do not belong to any known existing session.

Zone-Based Policy Firewall High Availability Operation

You can configure pairs of devices to act as hot standby devices for each other. Redundancy is configured on an interface basis. Pairs of redundant interfaces are known as redundancy groups (RGs). An RG must be configured under the interface in order for the zone-based policy firewall to correctly replicate connections in a high availability setup. In order for the firewall to synchronize connections, an RG must be associated with an interface.

Figure 1 depicts an active/standby load-sharing scenario. It shows how a redundancy group is configured for a pair of devices that has one outgoing interface. Figure 2 depicts an active/active load-sharing scenario. It shows how two redundancy groups are configured for a pair of devices that have two outgoing interfaces.

In both cases, the redundant devices are joined by a configurable control link, a data synchronization link, and an interlink interface. The control link is used to communicate the status of the devices. The data synchronization link is used to transfer stateful information from the firewall and to synchronize the stateful database. The pairs of redundant interfaces are configured with the same unique ID number, known as the redundant interface identifier (RII).

Asymmetric routing is supported as part of the firewall high availability. In a LAN-WAN scenario, where the return traffic enters standby devices, asymmetric routing is supported. To implement the asymmetric routing functionality, configure both the redundant devices with a dedicated interface (interlink interface) for asymmetric

traffic. This dedicated interface will redirect the traffic coming to the standby WAN interface to the active device.

Figure 1: Redundancy Group—One Outgoing Interface

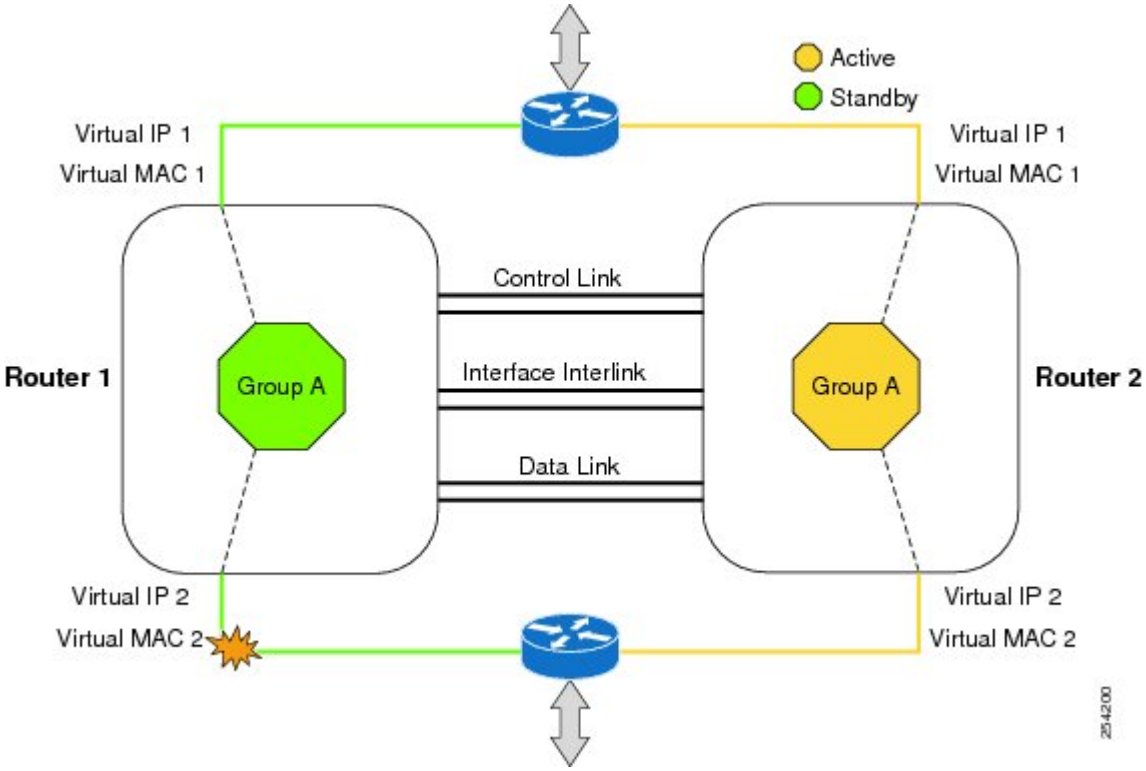
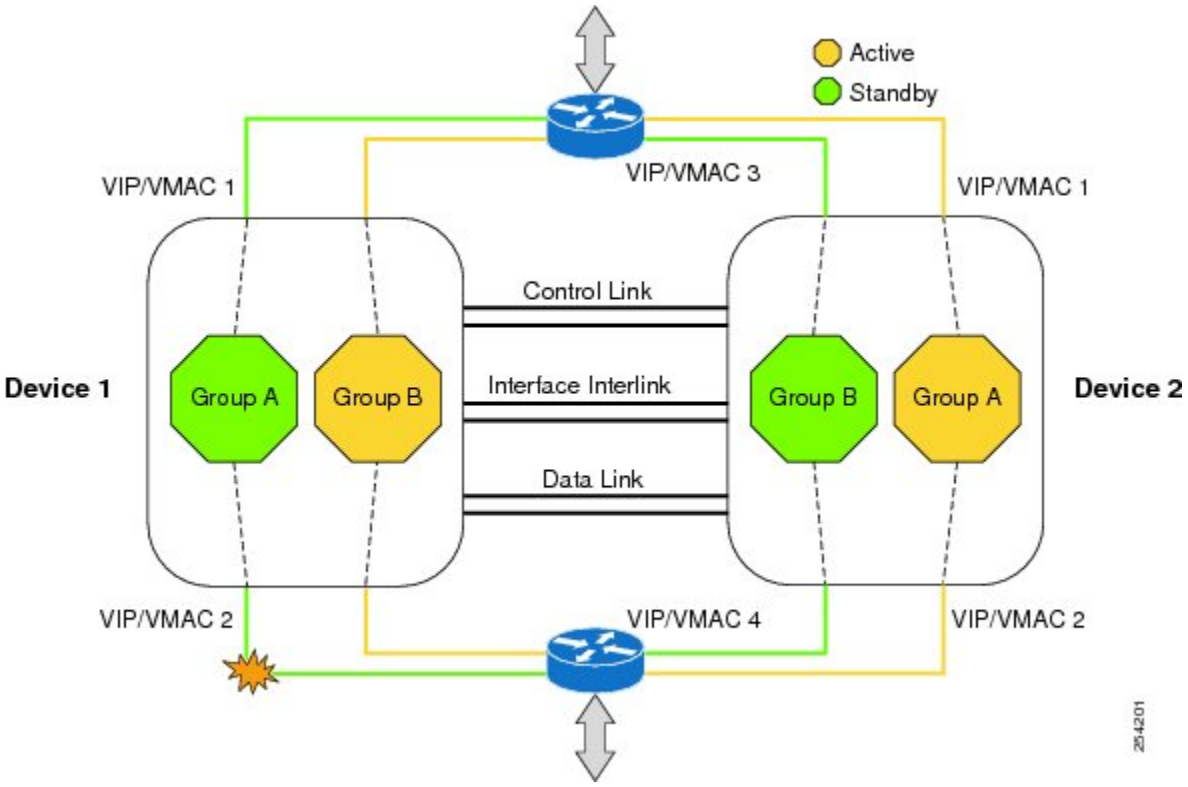


Figure 2: Redundancy Group Configuration—Two Outgoing Interfaces



The status of redundancy group members is determined through the use of hello messages sent over the control link. If either of the devices do not respond to a hello message within a configurable amount of time, the software considers that a failure has occurred, and a switchover is initiated. To detect a failure in milliseconds, the control links run the failover protocol. You can configure the following parameters for hello messages:

- Active timer.
- Standby timer.
- Hello time—The interval at which hello messages are sent.
- Hold time—The amount of time before which the active or standby device is declared to be down.

The hello time defaults to 3 seconds to align with the Hot Standby Router Protocol (HSRP), and the hold time defaults to 10 seconds. You can also configure these timers in milliseconds by using the **timers hellotime msec** command.

To determine which pairs of interfaces are affected by the switchover, you must configure a unique ID for each pair of redundant interfaces. This ID is known as the RII that is associated with the interface.

A switchover to the standby device can occur under other circumstances. Another factor that can cause a switchover is a priority setting that can be configured on each device. The device with the highest priority value will be the active device. If a fault occurs on either the active or the standby device, the priority of the device is decremented by a configurable amount, known as the weight. If the priority of the active device falls below the priority of the standby device, a switchover occurs and the standby device becomes the active device. This default behavior can be overridden by disabling the preemption attribute for the redundancy group. You can also configure each interface to decrease the priority when the Layer 1 state of the interface goes down. The priority that is configured overrides the default priority of a redundancy group.

Each failure event that causes a modification of a redundancy group's priority generates a syslog entry that contains a time stamp, the redundancy group that was affected, the previous priority, the new priority, and a description of the failure event cause.

Another situation that can cause a switchover to occur is when the priority of a device or interface falls below a configurable threshold level.

A switchover to the standby device occurs under the following circumstances:

- Power loss or a reload occurs on the active device (this includes crashes).
- The run-time priority of the active device goes down below that of the standby device.
- The run-time priority of the active device goes down below the configured threshold device.
- The redundancy group on the active device is reloaded manually by using the **redundancy application reload group** *rg-number* command.
- Two consecutive hello messages missed on any monitored interface forces the interface into testing mode. Both devices will verify the link status on the interface and then execute the following tests:
  - Network activity test
  - Address Resolution Protocol (ARP) test
  - Broadcast ping test

Active/Active Failover

In an active/active failover configuration, both devices can process network traffic. Active/active failover generates virtual MAC (VMAC) addresses for interfaces in each redundancy group (RG).

One device in an active/active failover pair is designated as the primary (active) device, and the other is designated as the secondary (standby) device. Unlike with active/standby failover, this designation does not indicate which device becomes active when both devices start simultaneously. Instead, the primary/secondary designation determines the following:

- The device that provides the running configuration to the failover pair when they start simultaneously.
- The device on which the failover RG appears in the active state when devices start simultaneously. Each failover RG in the configuration is configured with a primary or secondary device preference. You can configure both failover RGs to be in the active state on a single device and the standby failover RGs to be on the other device. You can also configure one failover RG to be in the active state and the other RG to be in the standby state on a single device.

Active/Standby Failover

Active/standby failover enables you to use a standby device to take over the functionality of a failed device. A failed active device changes to the standby state, and the standby device changes to the active state. The device that is now in the active state takes over IP addresses and MAC addresses of the failed device and starts processing traffic. The device that is now in the standby state takes over standby IP addresses and MAC addresses. Because network devices do not see any change in the MAC-to-IP address pairing, Address Resolution Protocol (ARP) entries do not change or time out anywhere on the network.

In an active/standby scenario, the main difference between two devices in a failover pair depends on which device is active and which device is a standby, namely which IP addresses to use and which device actively passes the traffic. The active device always becomes the active device if both devices start up at the same time (and are of equal operational health). MAC addresses of the active device are always paired with active IP addresses.

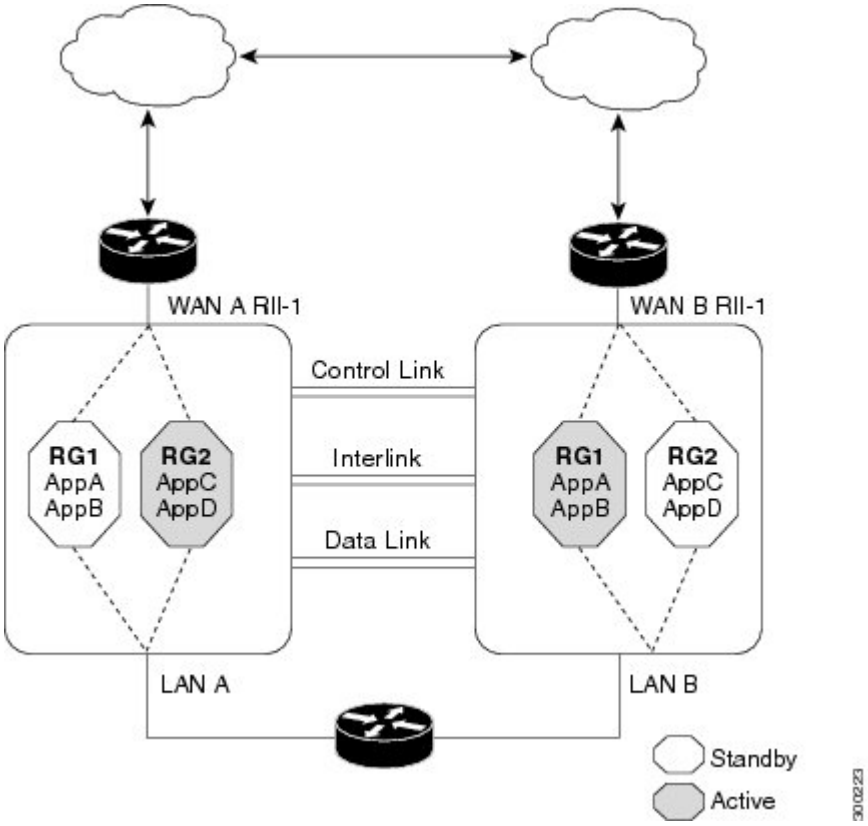
Asymmetric Routing Overview

Asymmetric routing occurs when packets from TCP or UDP connections flow in different directions through different routes. In asymmetric routing, packets that belong to a single TCP or UDP connection are forwarded through one interface in a redundancy group (RG), but returned through another interface in the same RG. In asymmetric routing, the packet flow remains in the same RG. When you configure asymmetric routing, packets received on the standby RG are redirected to the active RG for processing. If asymmetric routing is not configured, the packets received on the standby RG may be dropped.

Asymmetric routing determines the RG for a particular traffic flow. The state of the RG is critical in determining the handling of packets. If an RG is active, normal packet processing is performed. In case the RG is in a standby state and you have configured asymmetric routing and the **asymmetric-routing always-divert enable** command, packets are diverted to the active RG. Use the **asymmetric-routing always-divert enable** command to always divert packets received from the standby RG to the active RG.

The figure below shows an asymmetric routing scenario with a separate asymmetric-routing interlink interface to divert packets to the active RG.

Figure 3: Asymmetric Routing Scenario



The following rules apply to asymmetric routing:

- 1:1 mapping exists between the redundancy interface identifier (RII) and the interface.
- 1:*n* mapping exists between the interface and an RG. (An asymmetric routing interface can receive traffic from and send traffic to multiple RGs. For a non asymmetric-routing interface (normal LAN interface), a 1:1 mapping exists between the interface and the RG.)
- 1:*n* mapping exists between an RG and applications that use it. (Multiple applications can use the same RG).
- 1:1 mapping exists between an RG and the traffic flow. The traffic flow must map only to a single RG. If a traffic flow maps to multiple RGs, an error occurs.
- 1:1 or 1:*n* mapping can exist between an RG and an asymmetric-routing interlink as long as the interlink has sufficient bandwidth to support all the RG interlink traffic.

Asymmetric routing consists of an interlink interface that handles all traffic that is to be diverted. The bandwidth of the asymmetric-routing interlink interface must be large enough to handle all expected traffic that is to be diverted. An IPv4 address must be configured on the asymmetric-routing interlink interface, and the IP address of the asymmetric routing interface must be reachable from this interface.

Note We recommend that the asymmetric-routing interlink interface be used for interlink traffic only and not be shared with high availability control or data interfaces because the amount of traffic on the asymmetric-routing interlink interface could be quite high.

WAN-LAN Topology

In a WAN-LAN topology, two devices are connected through LAN interfaces on the inside and WAN interfaces on the outside. There is no control on the routing of return traffic received through WAN links.

WAN links can be provided by the same service provider or different service providers. In most cases, WAN links are provided by different service providers. To utilize WAN links to the maximum, configure an external device to provide a failover.

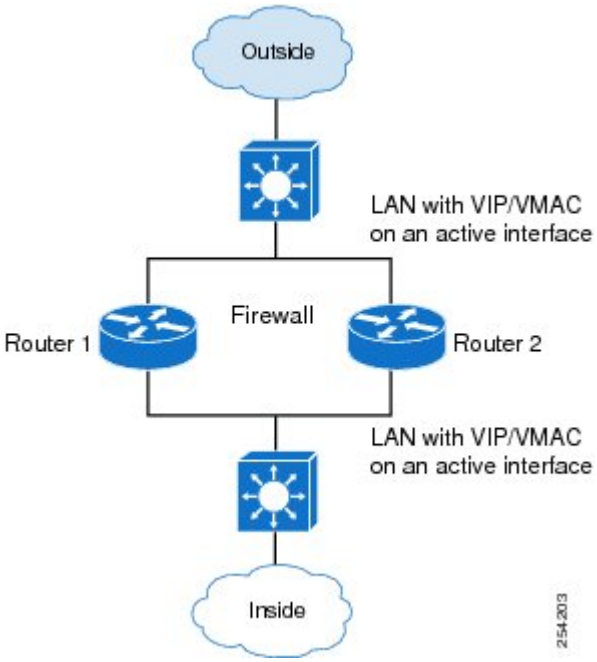
On LAN-based interfaces, a high availability virtual IP address is required to exchange client information and for faster failover. On WAN-based interfaces, the **redundancy group** *id* **ip** *virtual-ip* **decrement** *value* command is used for failover.

LAN-LAN Topology

In a LAN-LAN topology, all participating devices are connected to each other through LAN interfaces on both the inside and the outside. In this scenario, the traffic is often directed to the correct firewall if static routing is configured on the upstream or downstream devices to an appropriate virtual IP address. The dynamic routing configuration supported on LAN-facing interfaces must not introduce a dependency on routing protocol

convergence; otherwise, fast failover requirements will not be met. The figure below shows a LAN-LAN topology.

Figure 4: LAN-LAN Scenario



Exclusive Virtual IP Addresses and Exclusive Virtual MAC Addresses

Virtual IP (VIP) addresses and virtual MAC (VMAC) addresses are used by security applications to control interfaces that receive traffic. An interface is paired with another interface, and these interfaces are associated with the same redundancy group (RG). The interface that is associated with an active RG exclusively owns the VIP and VMAC. The Address Resolution Protocol (ARP) process on the active device sends ARP replies for any ARP request for the VIP, and the Ethernet controller for the interface is programmed to receive packets destined for the VMAC. When an RG failover occurs, the ownership of the VIP and VMAC changes. The interface that is associated with the newly active RG sends a gratuitous ARP and programs the interface's Ethernet controller to accept packets destined for the VMAC.

IPv6 Support

You can assign each redundancy group (RG) on a traffic interface for both IPv4 and IPv6 virtual IP (VIP) addresses under the same redundancy interface identifier (RII). Each RG uses a unique virtual MAC (VMAC) address per RII. For an RG, the IPv6 link-local VIP and global VIP coexist on an interface.

You can configure an IPv4 VIP, a link-local IPv6 VIP, and/or a global IPv6 VIP for each RG on a traffic interface. IPv6 link-local VIP is mainly used when configuring static or default routes, whereas IPv6 global VIP is widely used in both LAN and WAN topologies.

You must configure a physical IP address before configuring an IPv4 VIP.

Virtual Fragmentation Reassembly

Virtual fragmentation reassembly (VFR) enables the firewall to create dynamic access control lists (ACLs) to protect the network from various fragmentation attacks. VFR is high availability-aware. When the firewall is enabled for high availability, fragmented packets that arrive on the standby redundancy group (RG) are redirected to the active redundancy group. Use the **ip virtual-reassembly** command to enable VFR on an interface.

Note VFR should not be enabled on a device that is placed on an asymmetric path. The reassembly process requires all fragments within an IP datagram. Devices placed in the asymmetric path may not receive all IP fragments, and the fragment reassembly will fail.

How to Configure Zone-Based Policy Firewall High Availability

Configuring Application Redundancy and Redundancy Application Groups

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **redundancy**
5. **log dropped-packets enable**
6. **exit**
7. **redundancy**
8. **application redundancy**
9. **group** *id*
10. **name** *group-name*
11. **preempt**
12. **priority** *value*
13. **control** *interface-type interface-number* **protocol** *id*
14. **data** *interface-type interface-number*
15. **asymmetric-routing interface** *type number*
16. Configure Step 7 to Step 11 to create another redundancy group on the same device.
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect global** **Example:** `Device(config)# parameter-map type inspect global`	Defines a global inspect parameter map and enters parameter-map type inspect configuration mode.
Step 4	**redundancy** **Example:** `Device(config-profile)# redundancy`	Enables firewall high availability.
Step 5	**log dropped-packets enable** **Example:** `Device(config-profile)# log dropped-packets enable`	Enables logging of packets dropped by the firewall.
Step 6	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
Step 7	**redundancy** **Example:** `Device(config)# redundancy`	Enters redundancy configuration mode.
Step 8	**application redundancy** **Example:** `Device(config-red)# application redundancy`	Configures application redundancy and enters redundancy application configuration mode.
Step 9	**group** *id* **Example:** `Device(config-red-app)# group 1`	Configures a group and enters redundancy application group configuration mode.

	Command or Action	Purpose
Step 10	**name** *group-name* **Example:** `Device(config-red-app-grp)# name RG1`	Configures a redundancy group with a name.
Step 11	**preempt** **Example:** `Device(config-red-app-grp)# preempt`	Enables preemption on the redundancy group.
Step 12	**priority** *value* **Example:** `Device(config-red-app-grp)# priority 230`	Specifies a group priority and a failover threshold value for a redundancy group.
Step 13	**control** *interface-type interface-number* **protocol** *id* **Example:** `Device(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1`	Configures the control interface type and number for a redundancy group.
Step 14	**data** *interface-type interface-number* **Example:** `Device(config-red-app-grp)# data gigabitethernet 0/0/1`	Configures the data interface type and number for a redundancy group.
Step 15	**asymmetric-routing interface** *type number* **Example:** `Device(config-red-app-grp)# asymmetric-routing interface gigabitethernet 0/0/1`	Enables asymmetric routing on an interface.
Step 16	Configure Step 7 to Step 11 to create another redundancy group on the same device.	—
Step 17	**end** **Example:** `Device(config-red-app-grp)# end`	Exits redundancy application group configuration mode and returns to privileged EXEC mode.

Configuring a Firewall for High Availability

In this task, you will do the following:

- Configure a firewall.
- Create a security source zone.

- Create a security destination zone.
- Create a security zone pair by using the configured source and destination zones.
- Configure an interface as a zone member.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **parameter-map type inspect global**
7. **redundancy**
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect**
12. **exit**
13. **class class-default**
14. **drop**
15. **exit**
16. **exit**
17. **zone security** *zone-name*
18. **exit**
19. **zone security** *zone-name*
20. **exit**
21. **zone-pair security** *zone-pair-name* **source** *zone-name* **destination** *zone-name*
22. **service-policy type inspect** *policy-map-name*
23. **exit**
24. **zone-pair security** *zone-pair-name* **source** *zone-name* **destination** *zone-name*
25. **service-policy type inspect** *policy-map-name*
26. **exit**
27. **interface** *type number*
28. **ip address** *ip-address mask*
29. **encapsulation dot1q** *vlan-id*
30. **zone-member security** *security-zone-name*
31. **end**
32. **show policy-firewall session zone-pair ha**
33. **debug policy-firewall ha**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map type inspect match-any** *class-map-name* **Example:** `Device(config)# class-map type inspect match-any cmap-l4-Protocol`	Defines the class on which an action is to be performed and enters policy-map class configuration mode.
Step 4	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol tcp`	Configures a match criterion for a class map on the basis of the specified protocol.
Step 5	**exit** **Example:** `Device(config-cmap)# exit`	Exits policy-map class configuration mode and returns to global configuration mode.
Step 6	**parameter-map type inspect global** **Example:** `Device(config)# parameter-map type inspect global`	Defines a global inspect parameter map and enters parameter-map type inspect configuration mode.
Step 7	**redundancy** **Example:** `Device(config-profile)# redundancy`	Enables firewall high availability.
Step 8	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
Step 9	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect pmap-l4-Protocols`	Creates a protocol-specific inspect type policy map and enters policy-map configuration mode.

	Command or Action	Purpose
Step 10	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect cmap-l4-Protocol`	Defines the class on which an action is to be performed and enters policy-map class configuration mode.
Step 11	**inspect** **Example:** `Device(config-pmap-c)# inspect`	Enables stateful packet inspection.
Step 12	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 13	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Configures the default class on which an action is to be performed and enters policy-map class configuration mode.
Step 14	**drop** **Example:** `Device(config-pmap-c)# drop`	Drops packets that are sent to a device.
Step 15	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 16	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.
Step 17	**zone security** *zone-name* **Example:** `Device(config)# zone security TWAN`	Creates a security zone and enters security zone configuration mode. • You need two security zones to create a zone pair: a source and a destination zone.
Step 18	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 19	**zone security** *zone-name* **Example:** `Device(config)# zone security DATA`	Creates a security zone and enters security zone configuration mode. • You need two security zones to create a zone pair: a source and a destination zone.
Step 20	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 21	**zone-pair security** *zone-pair-name* **source** *zone-name* **destination** *zone-name* **Example:** `Device(config)# zone-pair security zp-TWAN-DATA source TWAN destination data`	Creates a zone pair to which interfaces can be assigned and enters security zone-pair configuration mode.
Step 22	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect pmap-l4-Protocols`	Attaches a firewall policy map to a zone pair.
Step 23	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone-pair configuration mode and returns to global configuration mode.
Step 24	**zone-pair security** *zone-pair-name* **source** *zone-name* **destination** *zone-name* **Example:** `Device(config)# zone-pair security zp-DATA-TWAN source DATA destination TWAN`	Creates a zone pair to which interfaces can be assigned and enters security zone-pair configuration mode.
Step 25	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect pmap-l4-Protocols`	Attaches a firewall policy map to a zone pair.
Step 26	**exit** **Example:** `Device(config-sec-zone-pair)# exit`	Exits security zone pair configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 27	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an IP address for the subinterface.
Step 28	**ip address** *ip-address mask* **Example:** `Device(config-subif)# ip address 10.1.1.1 255.255.255.0`	Configures an IP address for the subinterface.
Step 29	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-subif)# encapsulation dot1q 2`	Sets the encapsulation method used by the interface.
Step 30	**zone-member security** *security-zone-name* **Example:** `Device(config-subif)# zone-member security private`	Configures the interface as a zone member. • For the *security-zone-name* argument, you must configure one of the zones that you had configured by using the **zone security** command. • When an interface is in a security zone, all traffic to and from that interface (except traffic going to the device or initiated by the device) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone pair to which you apply a policy. If the policy permits traffic (via **inspect** or **inspect** actions), traffic can flow through the interface.
Step 31	**end** **Example:** `Device(config-sec-zone-pair)# end`	Exits security zone pair configuration mode and returns to privileged EXEC mode.
Step 32	**show policy-firewall session zone-pair ha** **Example:** `Device# show policy-firewall session zone-pair ha`	(Optional) Displays the firewall HA sessions pertaining to a zone pair.
Step 33	**debug policy-firewall ha** **Example:** `Device# debug policy-firewall ha`	(Optional) Displays messages about firewall events.

Configuring a Redundancy Application Group on a WAN Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **ip tcp adjust-mss** *max-segment-size*
8. **redundancy rii** *RII-identifier*
9. **redundancy asymmetric-routing enable**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/2.1`	Configures a subinterface and enters subinterface configuration mode.
Step 4	**description** *string* **Example:** `Device(config-subif)# description wan interface`	Adds a description to an interface configuration.
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-subif)# ip address 10.0.0.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 6	**zone-member security** *zone-name* **Example:** `Device(config-subif)# zone-member security TWAN`	Configures the interface as a zone member while configuring a firewall. • For the *zone-name* argument, you must configure one of the zones that you had configured by using the **zone security** command. • When an interface is in a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone pair to which you apply a policy. If the policy permits traffic (via inspect or pass actions), traffic can flow through the interface.
Step 7	**ip tcp adjust-mss** *max-segment-size* **Example:** `Device(config-subif)# ip tcp adjust-mss 1360`	Adjusts the maximum segment size (MSS) value of TCP SYN packets going through a router.
Step 8	**redundancy rii** *RII-identifier* **Example:** `Device(config-subif)# redundancy rii 360`	Configures an RII for redundancy group-protected traffic interfaces.
Step 9	**redundancy asymmetric-routing enable** **Example:** `Device(config-subif)# redundancy asymmetric-routing enable`	Associates a redundancy group with an interface that is used for asymmetric routing.
Step 10	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and enters privileged EXEC mode.

Configuring a Redundancy Application Group on a LAN Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **encapsulation dot1q** *vlan-id*
6. **ip vrf forwarding** *name*
7. **ip address** *ip-address mask*
8. **zone-member security** *zone-name*
9. **redundancy rii** *RII-identifier*
10. **redundancy group** *id* **ip** *ip-address* **exclusive**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/2.1`	Configures a subinterface and enters subinterface configuration mode.
Step 4	**description** *string* **Example:** `Device(config-subif)# description lan interface`	Adds a description to an interface configuration.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-subif)# encapsulation dot1q 18`	Sets the encapsulation method used by the interface.

	Command or Action	Purpose
Step 6	**ip vrf forwarding** *name* **Example:** `Device(config-subif)# ip vrf forwarding trust`	Associates a VPN routing and forwarding (VRF) instance with an interface or subinterface. • The command will not be configured if the specified VRF is not configured.
Step 7	**ip address** *ip-address mask* **Example:** `Device(config-subif)# ip address 10.0.0.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 8	**zone-member security** *zone-name* **Example:** `Device(config-subif)# zone-member security data`	Configures the interface as a zone member. • For the *zone-name* argument, you must configure one of the zones that you had configured by using the **zone security** command while configuring a firewall. • When an interface is in a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone pair to which you apply a policy. If the policy permits traffic (via inspect or pass actions), traffic can flow through the interface.
Step 9	**redundancy rii** *RII-identifier* **Example:** `Device(config-subif)# redundancy rii 100`	Configures an RII for redundancy group-protected traffic interfaces.
Step 10	**redundancy group** *id* **ip** *ip-address* **exclusive** **Example:** `Device(config-subif)# redundancy group 1 ip 10.0.0.1 exclusive`	Configures a virtual IP address for the redundancy group.
Step 11	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and enters privileged EXEC mode.

Configuration Examples for Zone-Based Policy Firewall High Availability

Example: Configuring Application Redundancy and Redundancy Application Groups

```
configure terminal
 parameter-map type inspect global
  redundancy
  log dropped-packets enable
!
  redundancy
   application redundancy
    group 1
     name RG1
     preempt
     priority 230
     control gigabitethernet 0/0/1 protocol 1
     data gigabitethernet 0/0/1
     asymmetric-routing gigabitethernet 0/0/1
```

Example: Configuring a Firewall for High Availability

```
configure terminal
 class-map type inspect match-any cmap-l4-Protocol
  match protocol tcp
!
 parameter-map type inspect global
  redundancy
!
 policy-map type inspect pmap-l4-Protocols
  class type inspect cmap-l4-Protocol
   inspect
!
  class class-default
   drop
!
!
 zone security TWAN
!
 zone security DATA
!
 zone-pair security zp-TWAN-DATA source TWAN destination DATA
  service-policy type inspect pmap-l4-Protocols
!
 zone-pair security zp-DATA-TWAN source DATA destination TWAN
  service-policy type inspect pmap-l4-Protocols
!
 interface gigabitethernet 0/0/0
  ip address 10.1.1.1 255.255.255.0
  encapsulation dot1q 2
  zone member security private
```

Example: Configuring a Redundancy Application Group on a WAN Interface

The following example shows how to configure redundancy groups for a WAN-LAN scenario:

```
interface gigabitethernet 0/0/2
 description wan interface
 ip 10.0.0.1 255.255.255.0
 zone-member security TWAN
 ip tcp adjust-mss 1360
 redundancy rii 360
 redundancy asymmetric-routing enable
```

The following is a sample WAN–LAN active/active configuration in which two devices have two LAN interfaces and one WAN interface. Two redundancy groups (RG1 and RG2) are configured on each device, and LAN interfaces are bound to one redundancy group. The WAN link is shared by both the RGs. RG1 is active on Device 1 and RG2 is active on Device 2.

```
! Configuration on Device 1:
redundancy
 application
  group 1
   name RG1
   priority 205 failover-threshold 200
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
   asymmetric-routing gigabitethernet 0/0/3
  group 2
   name RG2
   priority 195 failover-threshold 190
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
   asymmetric-routing gigabitethernet 0/0/3
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface pos 2/1
 redundancy rii 210 decrement 100
 redundancy asymmetric-routing enable
 zone-member security ha-out
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-in
!
!
interface gigabitethernet 0/1
 redundancy rii 2
```

```
 redundancy 1 ip 192.168.7.2 exclusive decrement 50
 zone-member security ha-in
!
! Configuration on Device 2:
redundancy
 application
  group 1
   name RG1
   priority 195 failover-threshold 190
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
   asymmetric-routing gigabitethernet 0/0/3
  group 2
   name RG2
   priority 205 failover-threshold 200
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
   asymmetric-routing gigabitethernet 0/0/3
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface pos 2/1
 redundancy rii 210 decrement 100
 redundancy asymmetric-routing enable
 zone-member security ha-out
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-in
!
!
interface gigabitethernet 0/1
 redundancy rii 2
 redundancy 2 ip 192.168.7.2 exclusive decrement 50
 zone-member security ha-in
```

The following is a sample active/standby LAN-WAN configuration with one LAN interface and one WAN interface on each device. Only one redundancy group (RG1) is configured, and it is active on Device 1 and on the standby on Device 2. The VIP address is owned by the LAN interface of the active device.

```
! Configuration on Device 1 (active):
redundancy
 application
  group 1
   name RG1
   priority 205 failover-threshold 200
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
   asymmetric-routing gigabitethernet 0/0/3
!
!
```

```
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface pos 2/1
 redundancy rii 210 decrement 100
 redundancy asymmetric-routing enable
 zone-member security ha-out
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-in


! Configuration on Device 2(standby):
redundancy
 application
  group 1
   name RG1
   priority 195 failover-threshold 190
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
   asymmetric-routing gigabitethernet 0/0/3
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface pos 2/1
 redundancy rii 210 decrement 100
 redundancy asymmetric-routing enable
 zone-member security ha-out
!
interface gigabitethernet 0/0
 redundancy rii 1
```

```
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-in
```

Example: Configuring a Redundancy Application Group on a LAN Interface

```
interface gigabitethernet 0/0/2
 description lan interface
 ip address 10.0.0.1 255.255.255.0
 zone member security data
 redundancy rii 100
 redundancy group 1 ip 10.0.0.1 exclusive
```

The following is an active/active LAN-LAN configuration that has a device with two LAN interfaces for both upstream and downstream traffic. Two redundancy groups (RG1 and RG2) are configured on each device. The pairing for each LAN upstream and LAN downstream links exists, and each pair is made part of a single redundancy group. In this scenario, the VIP addresses and VMAC address ownership is exclusively restricted to the active interface and hence there is no possibility of asymmetric routing.

```
! Configuration on Device 1:
redundancy
 application
  group 1
   name RG1
   priority 205 failover-threshold 200
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
  group 2
   name RG2
   priority 195 failover-threshold 190
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-in
!
!
interface gigabitethernet 0/1
 redundancy rii 2
 redundancy 2 ip 10.3.1.254 exclusive decrement 50
 zone-member security ha-in
!
!
interface gigabitethernet 1/0
 redundancy rii 210 decrement 100
```

```
 redundancy 1 ip 10.2.1.254 exclusive decrement 50
 zone-member security ha-out
!
interface gigabitethernet 1/1
 redundancy rii 110 decrement 100
 redundancy 2 ip 10.4.1.254 exclusive decrement 50
 zone-member security ha-out
!
! Configuration on Device 2:
redundancy
 application
  group 1
   name RG1
   priority 195 failover-threshold 190
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
  group 2
   name RG2
   priority 205 failover-threshold 200
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-in
!
!
interface gigabitethernet 0/1
 redundancy rii 2
 redundancy 2 ip 10.3.1.254 exclusive decrement 50
 zone-member security ha-in
!
!
interface gigabitethernet 1/0
 redundancy rii 210 decrement 100
 redundancy 1 ip 10.2.1.254 exclusive decrement 50
 zone-member security ha-out
!
interface gigabitethernet 1/1
 redundancy rii 110 decrement 100
 redundancy 2 ip 10.4.1.254 exclusive decrement 50
 zone-member security ha-out
```

The following is an active/standby LAN-LAN configuration. This configuration is similar to the active/standby WAN-LAN configuration in which each device has one LAN interface for both upstream and downstream

traffic. Only one redundancy group (RG1) is configured and each interface is made part of this redundancy group.

```
! Configuration on Device 1 (active):
redundancy
 application
  group 1
   name RG1
   priority 205 failover-threshold 200
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-out
!
!
interface gigabitethernet 1/0
 redundancy rii 210 decrement 100
 redundancy 1 ip 10.2.1.254 exclusive decrement 50
 zone-member security ha-out
!
! Configuration on Device 2(standby):
redundancy
 application
  group 1
   name RG1
   priority 195 failover-threshold 190
   control gigabitethernet 0/0/1 protocol 1
   data gigabitethernet 0/0/2
!
!
parameter-map type inspect global
 redundancy
 redundancy delay 10
!
class-map type inspect match-all ha-class
 match protocol tcp
!
!
policy-map type inspect ha-policy
 class type inspect ha-class
  inspect
 class class-default
  drop
!
zone security ha-in
!
```

```
zone security ha-out
!
zone-pair security ha-in-out source ha-in destination ha-out
 service-policy type inspect ha-policy
!
!
interface gigabitethernet 0/0
 redundancy rii 1
 redundancy 1 ip 10.1.1.254 exclusive decrement 50
 zone-member security ha-out
!
!
interface gigabitethernet 1/0
 redundancy rii 210 decrement 100
 redundancy 1 ip 10.2.1.254 exclusive decrement 50
 zone-member security ha-out
```

Feature Information for Zone-Based Policy Firewall High Availability

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Zone-Based Policy Firewall High Availability

Feature Name	Releases	Feature Information
Zone-Based Policy Firewall High Availability	15.2(3)T	The Zone-Based Policy Firewall High Availability feature enables you to configure pairs of routers to act as backup for each other. High availability (HA) can be configured to determine the active router based on a number of failover conditions. When a failover occurs, the standby router seamlessly takes over and starts forwarding traffic and maintaining a dynamic routing table. The Zone-Based Policy Firewall High Availability feature supports active/active HA, active/standby HA, and asymmetric routing. The following commands were introduced or modified: **debug policy-firewall**, **redundancy**, and **show policy-firewall**.