Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

The Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls feature supports high availability (HA) based on redundancy groups (RGs) on IPv6 firewalls. This feature enables you to configure pairs of devices to act as backup for each other. This feature can be configured to determine the active device based on a number of failover conditions. This feature supports the FTP66 application-layer gateway (ALG) for IPv6 packet inspection.

This module provides information about Box-to-Box (B2B) HA support and describes how to configure this feature.

Prerequisites for Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

- Interfaces attached to a firewall must have the same redundant interface identifier (RII).
- Active and standby devices must have the same zone-based policy firewall configuration.
- Active and standby devices must run on identical versions of Cisco software. The active and standby devices must be connected through a switch.
- The box-to-box (B2B) configuration on both active and standby devices should be the same because there is no autosynchronization of the configuration between these devices.

- For asymmetric routing traffic to pass, you must configure the pass action for the class-default class. Class-default class is a system-defined class map that represents all packets that do not match any of the user-defined classes in a policy.
- 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 Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

- Only IPv4 is supported at box-to-box (B2B) interlink interfaces.
- Multiprotocol Label Switching (MPLS) and virtual routing and forwarding (VRF) are not supported.
- Cisco ASR 1006 and 1013 Aggregation Services Routers with dual Embedded Services Processors (ESPs) or dual Route Processors (RPs) in the chassis are not supported, because coexistence of interbox high availability (HA) and intrabox HA is not supported.

  Cisco ASR 1006 and Cisco ASR 1013 Aggregation Services Routers with single ESP and single RP in the chassis support interchassis redundancy.
- If the dual IOS daemon (IOSd) is configured, the device will not support the firewall stateful interchassis redundancy configuration.
- Stateless Network Address Translation 64 (NAT64) with IPv6 firewalls is not supported.

Information About Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

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.

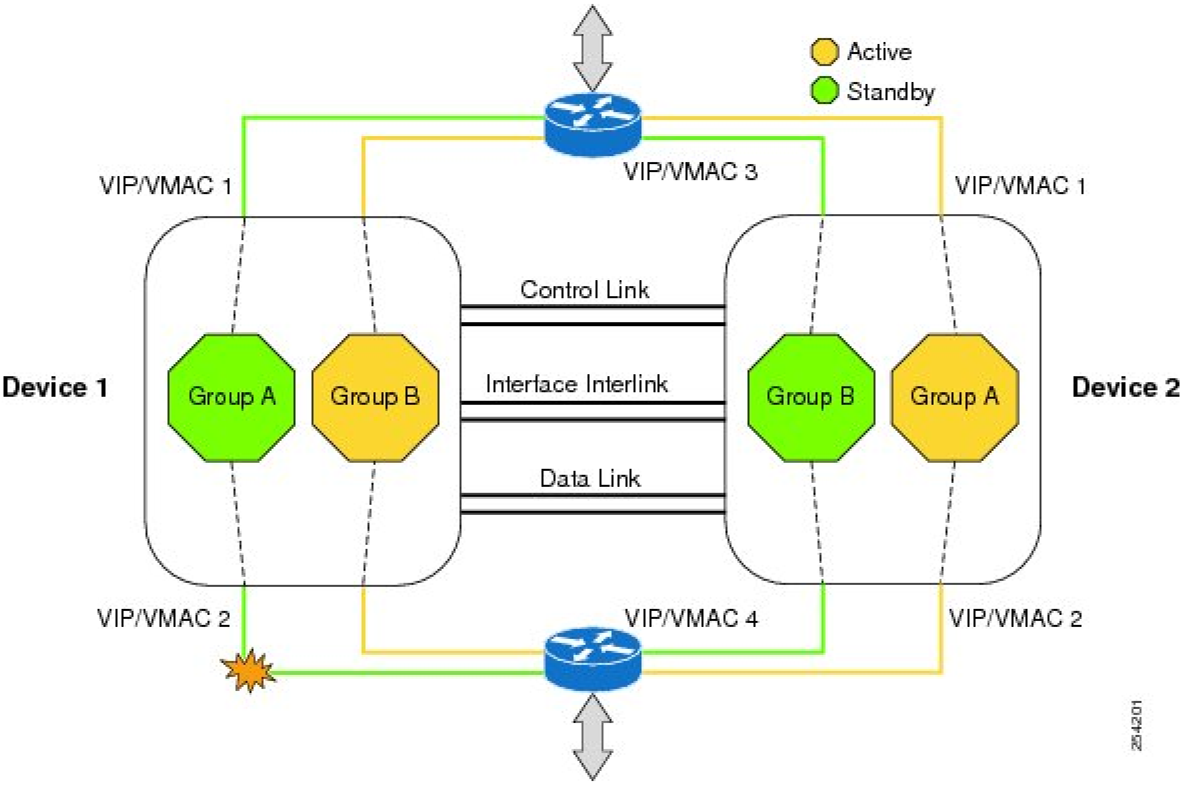
When active/standby high availability failover is configured, only one of the devices involved in the failover handles the traffic at one time, while the other device is in a standby mode, periodically synchronizing session information from the active device.

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.

Box-to-Box High Availability Operation

You can configure pairs of devices to act as hot standbys for each other. Redundancy is configured per interface. Pairs of redundant interfaces are known as redundancy groups (RGs). Figure 1 depicts an active/active failover scenario. It shows how two redundancy groups are configured for a pair of devices that have two outgoing interfaces.

Figure 1: Redundancy Group Configuration—Two Outgoing Interfaces



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). The routing table is not synced from active to standby.

Asymmetric routing is supported as part of the firewall HA. 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.

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 configured time period, 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 time period before which the active or standby device is declared to be down.

The hello time defaults to three 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 the RII that is associated with the interface.

Reasons for Switchover

Another factor that can cause a switchover is the 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. You can override this default behavior 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 the 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 the 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 below that of the standby device.
- The run-time priority of the active device goes below the configured threshold level.
- 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.

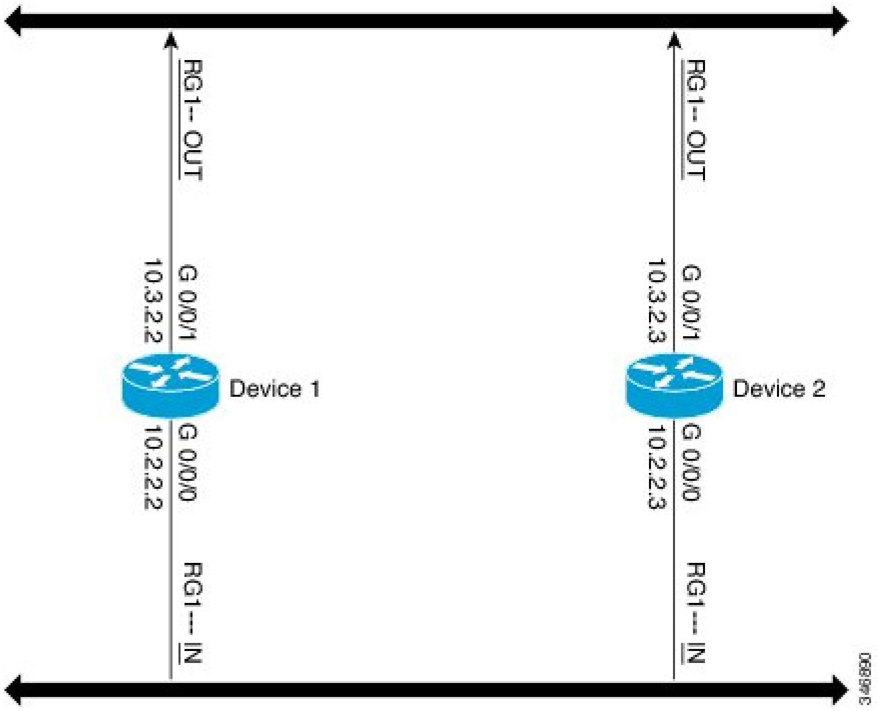
In an active/standby scenario, the main difference between two devices in a failover pair depends on which device is active and which device is a standby, namely which IP addresses to use and which device actively passes the traffic. The active device always becomes the active device if both devices 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.

NAT Box-to-Box High-Availability 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. The figure below shows the NAT box-to-box LAN-LAN topology. Network Address Translation (NAT) is in the active-standby mode and the peers are in one redundancy group (RG). All traffic or a subset of this traffic undergoes NAT translation.

Note Failover is caused by only those failures that the RG infrastructure listens to.

Figure 2: NAT Box-to-Box High-Availability LAN-LAN Topology



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.

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.

FTP66 ALG Support Overview

Firewalls support the inspection of IPv6 packets and stateful Network Address Translation 64 (NAT64). For FTP to work over IPv6 packet inspection, the application-layer gateway (ALG) (also called the application-level gateway [ALG]), FTP66, is required. The FTP66 ALG is also called all-in-one FTP ALG and one FTP ALG.

The FTP66 ALG supports the following:

- Firewall IPv4 packet inspection
- Firewall IPv6 packet inspection
- NAT configuration
- NAT64 configuration (along with FTP64 support)
- NAT and firewall configuration
- NAT64 and firewall configuration

The FTP66 ALG has the following security vulnerabilities:

- Packet segmentation attack—The FTP ALG state machine can detect segmented packets, and the state machine processing is stopped until a complete packet is received.
- Bounce attack—The FTP ALG does not create doors (for NAT) or pinholes (for firewalls) with a data port number less than 1024. The prevention of a bounce attack is activated only when the firewall is enabled.

How to Configure Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

Configuring a Redundancy Group Protocol

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**

4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. **timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}
8. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*}
9. **end**

DETAILED STEPS

Procedure

	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	**redundancy** **Example:** `Device(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**application redundancy** **Example:** `Device(config-red)# application redundancy`	Enters redundancy application configuration mode.
Step 5	**protocol** *id* **Example:** `Device(config-red-app)# protocol 1`	Specifies the protocol instance that will be attached to a control interface and enters redundancy application protocol configuration mode.
Step 6	**name** *group-name* **Example:** `Device(config-red-app-prtcl)# name prot1`	(Optional) Configures the redundancy group (RG) with a name.

Step 7	**timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}
	Example:
	`Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9`
		Specifies the interval between when hello messages are sent and the time period before which a device is declared to be down.

Step 8	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*} **Example:**	Specifies the authentication information.

	Command or Action	Purpose
	`Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	

Step 9	**end**
	Example:
	`Device(config-red-app-prtcl)# end`
		Exits redundancy application protocol configuration mode and enters privileged EXEC mode.

Configuring a Redundancy Application Group

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **shutdown**
8. **priority** *value* [**failover threshold** *value*]
9. **preempt**
10. **track** *object-number* {**decrement** *value* | **shutdown**}
11. **end**

DETAILED STEPS

Procedure

	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	**redundancy** **Example:** `Device(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**application redundancy** **Example:** `Device(config-red)# application redundancy`	Enters redundancy application configuration mode.

	Command or Action	Purpose
Step 5	**group** *id* **Example:** `Device(config-red-app)# group 1`	Enters redundancy application group configuration mode.
Step 6	**name** *group-name* **Example:** `Device(config-red-app-grp)# name group1`	(Optional) Specifies an optional alias for the protocol instance.
Step 7	**shutdown** **Example:** `Device(config-red-app-grp)# shutdown`	(Optional) Shuts down a redundancy group manually.
Step 8	**priority** *value* [**failover threshold** *value*] **Example:** `Device(config-red-app-grp)# priority 100 failover threshold 50`	(Optional) Specifies the initial priority and failover threshold for a redundancy group.
Step 9	**preempt** **Example:** `Device(config-red-app-grp)# preempt`	Enables preemption on the group and enables the standby device to preempt the active device regardless of the priority.

Step 10	**track** *object-number* {**decrement** *value* | **shutdown**}
	Example:
	`Device(config-red-app-grp)# track 200 decrement 200`
		Specifies the priority value of a redundancy group that will be decremented if an event occurs.

Step 11	**end**
	Example:
	`Device(config-red-app-grp)# end`
		Exits redundancy application group configuration mode and enters privileged EXEC mode.

Configuring a Control Interface and a Data Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **end**

DETAILED STEPS

Procedure

	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	**redundancy** **Example:** `Device(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**application redundancy** **Example:** `Device(config-red)# application redundancy`	Enters redundancy application configuration mode.
Step 5	**group** *id* **Example:** `Device(config-red-app)# group 1`	Enters redundancy application group configuration mode.
Step 6	**data** *interface-type interface-number* **Example:** `Device(config-red-app-grp)# data GigabitEthernet 0/0/0`	Specifies the data interface that is used by the redundancy group.
Step 7	**control** *interface-type interface-number* **protocol** *id* **Example:** `Device(config-red-app-grp)# control gigabitethernet 0/0/2 protocol 1`	Specifies the control interface that is used by the redundancy group. • This interface is also associated with an instance of the control interface protocol.
Step 8	**timers delay** *seconds* [**reload** *seconds*] **Example:** `Device(config-red-app-grp)# timers delay 100 reload 400`	Specifies the time that a redundancy group will take to delay role negotiations that start after a fault occurs or the system is reloaded.

Step 9	**end**
	Example:
	`Device(config-red-app-grp)# end`
		Exits redundancy application group configuration mode and enters privileged EXEC mode.

Configuring a LAN Traffic 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. **ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
8. **zone-member security** *zone-name*
9. **redundancy rii** *RII-identifier*
10. **redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*]
11. **end**

DETAILED STEPS

Procedure

	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 2/0/2`	Configures an interface and enters interface configuration mode.
Step 4	**description** *string* **Example:** `Device(config-if)# description lan interface`	(Optional) Adds a description to an interface configuration.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if)# encapsulation dot1q 18`	Sets the encapsulation method used by the interface.

	Command or Action	Purpose
Step 6	**ip vrf forwarding** *name* **Example:** `Device(config-if)# 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	**ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
	Example:
	`Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64`
		Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

Step 8	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone member security z1`	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-if)# redundancy rii 100`	Configures an RII for redundancy group-protected traffic interfaces.
Step 10	**redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*] **Example:** `Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 exclusive decrement 50`	Enables the redundancy group (RG) traffic interface configuration.

Step 11	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and enters privileged EXEC mode.

Configuring a WAN Traffic Interface

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
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

Procedure

	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 2/1/0`	Configures an interface and enters interface configuration mode.
Step 4	**description** *string* **Example:** `Device(config-if)# description wan interface`	(Optional) Adds a description to an interface configuration.

Step 5	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
	Example:
	`Device(config-if)# ipv6 address 2001:DB8:2222::/48`
		Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

Step 6	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security z2`	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

	Command or Action	Purpose
		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-if)# 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-if)# redundancy rii 360`	Configures an RII for redundancy group-protected traffic interfaces.
Step 9	**redundancy asymmetric-routing enable** **Example:** `Device(config-if)# redundancy asymmetric-routing enable`	Associates a redundancy group with an interface that is used for asymmetric routing.

Step 10	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and enters privileged EXEC mode.

Configuring an IPv6 Firewall

The steps to configure an IPv4 firewall and an IPv6 firewall are the same. To configure an IPv6 firewall, you must configure the class map in such a way that only an IPv6 address family is matched.

The **match protocol** command applies to both IPv4 and IPv6 traffic and can be included in either an IPv4 policy or an IPv6 policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**

14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf-definition** *vrf-name* **Example:** `Device(config)# vrf-definition VRF1`	Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.
Step 4	**address-family ipv6** **Example:** `Device(config-vrf)# address-family ipv6`	Enters VRF address family configuration mode and configures sessions that carry standard IPv6 address prefixes.
Step 5	**exit-address-family** **Example:** `Device(config-vrf-af)# exit-address-family`	Exits VRF address family configuration mode and enters VRF configuration mode.
Step 6	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 7	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect ipv6-param-map`	Enables a global inspect-type parameter map for the firewall to connect thresholds, timeouts, and other parameters that pertain to the inspect action, and enters parameter-map type inspect configuration mode.

	Command or Action	Purpose
Step 8	**sessions maximum** *sessions* **Example:** `Device(config-profile)# sessions maximum 10000`	Sets the maximum number of allowed sessions that can exist on a zone pair.
Step 9	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 10	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* **Example:** `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	Establishes a port to application mapping (PAM) by using the IPv6 access control list (ACL).
Step 12	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list ipv6-acl`	Defines an IPv6 access list and enters IPv6 access list configuration mode.
Step 13	**permit ipv6 any any** **Example:** `Device(config-ipv6-acl)# permit ipv6 any any`	Sets permit conditions for an IPv6 access list.
Step 14	**exit** **Example:** `Device(config-ipv6-acl)# exit`	Exits IPv6 access list configuration mode and enters global configuration mode.
Step 15	**class-map type inspect match-all** *class-map-name* **Example:** `Device(config)# class-map type inspect match-all ipv6-class`	Creates an application-specific inspect type class map and enters QoS class-map configuration mode.
Step 16	**match access-group name** *access-group-name* **Example:** `Device(config-cmap)# match access-group name ipv6-acl`	Configures the match criteria for a class map on the basis of the specified ACL.
Step 17	**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 18	**exit** **Example:**	Exits QoS class-map configuration mode and enters global configuration mode.

	Command or Action	Purpose
	`Device(config-cmap)# exit`	
Step 19	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect ipv6-policy`	Creates a protocol-specific inspect type policy map and enters QoS policy-map configuration mode.

Step 20	**class type inspect** *class-map-name*
	Example:
	`Device(config-pmap)# class type inspect ipv6-class`
		Specifies the traffic class on which an action is to be performed and enters QoS policy-map class configuration mode.

Step 21	**inspect** [*parameter-map-name*] **Example:** `Device(config-pmap-c)# inspect ipv6-param-map`	Enables stateful packet inspection.

Step 22	**end**
	Example:
	`Device(config-pmap-c)# end`
		Exits QoS policy-map class configuration mode and enters privileged EXEC mode.

Configuring Zones and Applying Zones to Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address/prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**zone security** *zone-name* **Example:** `Device(config)# zone security z1`	Creates a security zone and enters security zone configuration mode.
Step 4	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.
Step 5	**zone security** *zone-name* **Example:** `Device(config)# zone security z2`	Creates a security zone and enters security zone configuration mode.
Step 6	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.
Step 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] **Example:** `Device(config)# zone-pair security in-2-out source z1 destination z2`	Creates a zone pair and enters security zone-pair configuration mode.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	Attaches a policy map to a top-level policy map.
Step 9	**exit** **Example:** `Device(config-sec-zone-pair)# exit`	Exits security zone-pair configuration mode and enters global configuration mode.
Step 10	**interface** *type number* **Example:**	Configures a subinterface and enters subinterface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface gigabitethernet 0/0/0.1`	
Step 11	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface or a subinterface.
Step 12	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-subif)# encapsulation dot1q 2`	Sets the encapsulation method used by the interface.
Step 13	**zone-member security** *zone-name* **Example:** `Device(config-subif)# zone member security z1`	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. • 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 the 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 14	**end**
	Example:
	`Device(config-subif)# end`
		Exits subinterface configuration mode and enters privileged EXEC mode.

Step 15	**show policy-map type inspect zone-pair sessions** **Example:** `Device# show policy-map type inspect zone-pair sessions`	Displays the stateful packet inspection sessions created because a policy map is applied on a specified zone pair. • The output of this command displays both IPv4 and IPv6 firewall sessions.

Example

The following sample output from the **show policy-map type inspect zone-pair sessions** command displays the translation of packets from an IPv6 address to an IPv4 address and vice versa:

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
```

```
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
         Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [0:0]
```

The following sample output from the **show policy-map type inspect zone-pair sessions** command displays the translation of packets from an IPv6 address to an IPv6 address:

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

Configuration Examples for Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

Example: Configuring a Redundancy Group Protocol

The following example shows how to configure a redundancy group with timers set for hello time and hold time messages:

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

Example: Configuring a Redundancy Application Group

The following example shows how to configure a redundancy group named group1 with priority and preempt attributes:

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover-threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 200 decrement 200
Device(config-red-app-grp)# end
```

Example: Configuring a Control Interface and a Data Interface

```
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# end
```

Example: Configuring a LAN Traffic Interface

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/0/2
Device(config-if)# description lan interface
Device(config-if)# encapsulation dot1q 18
Device(config-if)# ip vrf forwarding trust
Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
Device(config-if)# zone member security z1
Device(config-if)# redundancy rii 100
Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE exclusive
decrement 50
Device(config-if)# end
```

Example: Configuring a WAN Traffic Interface

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

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/1/0
Device(config-if)# description wan interface
Device(config-if)# ipv6 address 2001:DB8:2222::/48
Device(config-if)# zone-member security z2
Device(config-if)# ip tcp adjust-mss 1360
Device(config-if)# redundancy rii 360
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

Example: Configuring an IPv6 Firewall

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

Example: Configuring Zones and Applying Zones to Interfaces

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

Additional References for Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Firewall commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

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 Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls

Feature Name	Releases	Feature Information
Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls	Cisco IOS XE Release 3.8S	The Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls feature supports high availability (HA) based on redundancy groups (RGs) on IPv6 firewalls. This feature enables you to configure pairs of devices to act as backup for each other. This feature can be configured to determine the active device based on a number of failover conditions. No commands were introduced or modified.
Box-to-Box High Availability Support for IPv6 Zone-Based Firewalls	Cisco IOS XE Release 3.8S	In Cisco IOS XE Release 3.10S, support was added for the Cisco ISR 4400 Series Routers.