ZBFW High Availability Configuration and Troubleshooting TechNote

Document ID: 115956

Contributed by Adam Makovecz, Rama Darbha, and Jay Johnston,
Cisco TAC Engineers.
Nov 05, 2013

Contents

Introduction

This guide provides the basic configuration for Zone Firewall High Availability (HA) for an active/standby setup, as well as troubleshooting commands, and common issues seen with the feature.

Cisco IOS® Zone−Based Firewall (ZBFW) supports HA so that two Cisco IOS routers can be configured in an active/standby or active/active setup. This allows redundancy in order to prevent a single point of failure.

Prerequisites

Requirements

You must have a release later than Cisco IOS Software Release15.2(3)T.

Components Used

This document is not restricted to specific software and hardware versions.

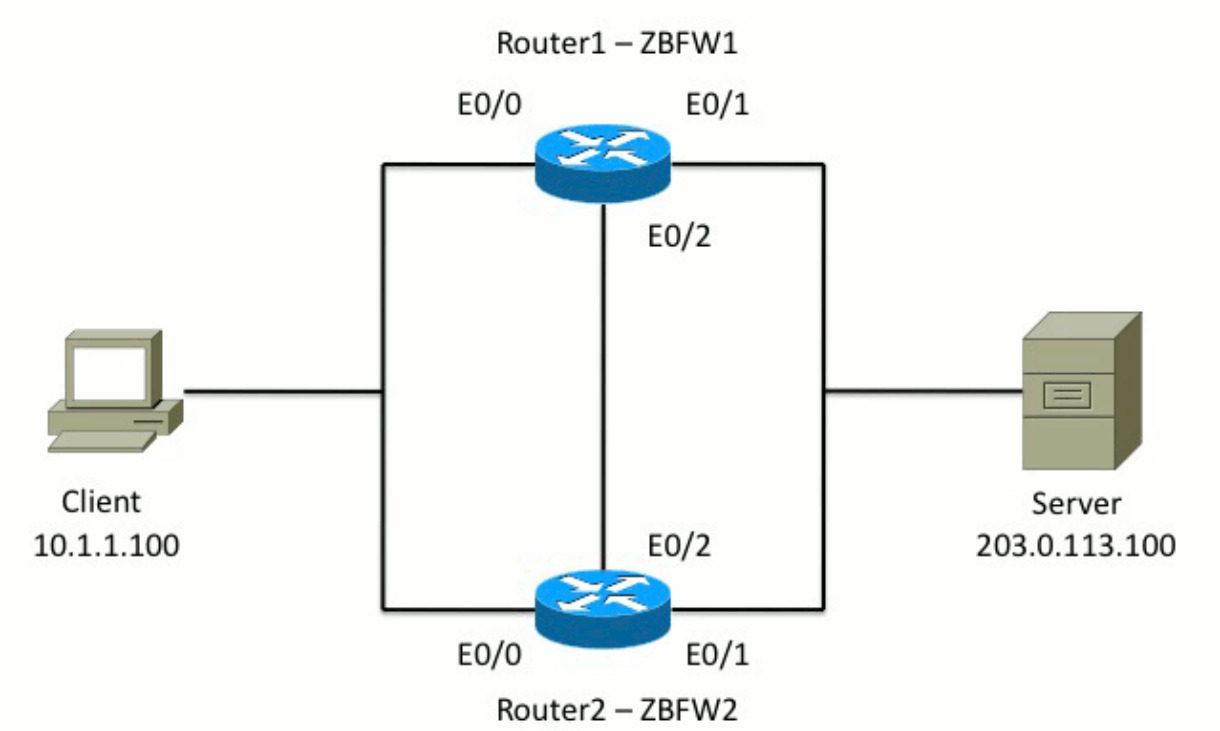
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

This diagram shows the topology used in the configuration examples.



In the configuration shown in Example 1, ZBFW is configured in order to inspect TCP, UDP, and Internet Control Message Protocol (ICMP) traffic from inside to outside. The configuration shown in bold sets up the HA feature. In Cisco IOS routers, HA is configured via the ***redundancy*** subconfig command. In order to configure redundancy, the first step is to enable redundancy in the global inspection parameter map.

After you enable redundancy, enter the ***application redundancy*** subconfig, and select the interfaces that are used for ***control*** and ***data***. The control interface is used in order to exchange information about the state of each router. The data interface is used in order to exchange information about the connections that should be replicated.

In Example 2, the ***priority*** command is also set to make Router 1 the active unit in the pair if both Router 1 and Router 2 are operational. The ***preempt*** command (also discussed further in this document) is used in order to ensure that failure occurs once the priority changes.

The final step is to assign the ***Redundant Interface Identifier (RII)*** and ***Redundancy Group (RG)*** to each interface. The ***RII*** group number has to be unique for each interface, but it must match across devices for interfaces in the same subnet. The RII is only used for the bulk sync process when the two routers synchronize configuration. This is how the two routers synchronize redundant interfaces. The ***RG*** is used in order to indicate that connections through that interface are replicated into the HA connection table.

In Example 2, the ***redundancy group 1*** command is used in order to create a virtual IP (VIP) address on the inside interface. This ensures HA, because all internal users only communicate with the VIP, for which the active unit processes.

The outside interface does not have any RG configuration because this is the WAN interface. The outside interface of both Router 1 and Router 2 do not belong to the same Internet Service Provider (ISP). On the outside interface, a dynamic routing protocol is required in order to ensure that traffic passes to the correct device.

Example 1: Router 1 Configuration Snippet (Hostname ZBFW1)

```
parameter-map type inspect global
 redundancy
 log dropped-packets enable
!
redundancy
 application redundancy
  group 1
   name ZBFW_HA
   preempt
   priority 200
   control Ethernet0/2 protocol 1
   data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
 match class-map PROTOCOLS
 match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
 class type inspect INSIDE_TO_OUTSIDE_CMAP
  inspect
 class class-default
  drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
 permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
 redundancy rii 100
 redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
 ip address 203.0.113.1 255.255.255.0
```

```
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 redundancy rii 200
```

Example 2: Router 2 Configuration Snippet (Hostname ZBFW2)

```
parameter-map type inspect global
 redundancy
 log dropped-packets enable
!
redundancy
 application redundancy
  group 1
   name ZBFW_HA
   preempt
   priority 200
   control Ethernet0/2 protocol 1
   data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
 match class-map PROTOCOLS
 match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
 class type inspect INSIDE_TO_OUTSIDE_CMAP
  inspect
 class class-default
  drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
 permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
 redundancy rii 100
 redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
 ip address 203.0.113.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 redundancy rii 200
```

Troubleshoot

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

Confirm that Devices Can Communicate with Each Other

In order to confirm that devices can see each other, you must verify that the operational state of the redundancy application group is up. Then, ensure that each device has taken the correct role, and can see its peer in its correct roles. In Example 3, ZBFW1 is active and detects its peer as standby. This is reversed on ZBFW2. When both devices also show that the operational state is up, and their peer presence is detected, the two routers can successfully communicate across the control link.

Example 3: Peer Presence Detection

```
ZBFW1# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY COLD-BULK
!
ZBFW2#  show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
          RF state: STANDBY COLD-BULK
          Peer RF state: ACTIVE
```

The output in Example 4 shows more granular output about the control interface of the two routers. The output confirms the physical interface used for control traffic, and it also confirms the IP address of the peer.

Example 4: Granular Output

```
ZBFW1#  show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.2 Standby RGs: 1 BFD handle: 0

ZBFW1#  show redundancy application data-interface group 1
 The data interface for rg[1] is Ethernet0/2
!
ZBFW2#  show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
```

```
Peer: 10.60.1.1 Active RGs: 1 BFD handle: 0

ZBFW2#  show redundancy application data-interface group 1
 The data interface for rg[1] is Ethernet0/2
```

When the communication is established, the command in Example 5 helps you understand why each device is in its particular role. ZBFW1 is active because it has a higher priority than its peer. ZBFW1 has a priority of ***200***, while ZBFW2 has a priority of ***150***. This output is highlighted in bold.

Example 5: Role Status and Priority

```
ZBFW1#  show redundancy application protocol group 1

RG Protocol RG 1
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.60.1.2, priority 150, intf Et0/2
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Ethernet0/2
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 249, Bytes 15438, HA Seq 0, Seq Number 249, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 0, RX 0
        Standby Peer: Present. Hold Timer: 10000
                Pkts 237, Bytes 8058, HA Seq 0, Seq Number 252, Pkt Loss 0

!
ZBFW2#  show redundancy application protocol group 1

RG Protocol RG 1
------------------
        Role: Standby
        Negotiation: Enabled
        Priority: 150
        Protocol state: Standby-cold
        Ctrl Intf(s) state: Up
        Active Peer: address 10.60.1.1, priority 200, intf Et0/2
        Standby Peer: Local
        Log counters:
                role change to active: 0
                role change to standby: 1
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0
```

```
RG Media Context for RG 1
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Ethernet0/2
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 232, Bytes 14384, HA Seq 0, Seq Number 232, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 0, RX 0
        Active Peer: Present. Hold Timer: 10000
                Pkts 220, Bytes 7480, HA Seq 0, Seq Number 229, Pkt Loss 0
```

The last confirmation is to ensure that the RII group ID is assigned to each interface. If you enter this command on both routers, they double−check in order to ensure that the interface pairs on the same subnet between devices are assigned the same RII ID. If they are not configured with the same unique RII ID, connections do not replicate between the two devices. See Example 6.

Example 6: Confirm RII Group ID is Assigned

```
ZBFW1# show redundancy rii
 No. of RIIs in database: 2
 Interface                        RII Id     decrement
  Ethernet0/1                  :   200           0
  Ethernet0/0                  :   100           0
!
ZBFW2# show redundancy rii
 No. of RIIs in database: 2
 Interface                        RII Id     decrement
Ethernet0/1                   :   200           0
Ethernet0/0                   :   100           0
```

Verify that Connections Replicate to the Peer Router

In Example 7, ZBFW1 actively passes traffic for a connection. The connection is successfully replicated to the standby device ZBFW2. In order to view the connections processed by the zone firewall, use the ***show policy−firewall session*** command.

Example 7: Connections Processed

```
ZBFW1#show policy−firewall session
       Session B2704178 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
   SIS_OPEN/TCP_ESTAB
         Created 00:00:31, Last heard 00:00:30
         Bytes sent (initiator:responder) [37:79]
         HA State: ACTIVE, RG ID: 1
     Established Sessions = 1

ZBFW2#show policy−firewall session
       Session B2601288 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
   SIS_OPEN/TCP_ESTAB
         Created 00:00:51, Last heard never
         Bytes sent (initiator:responder) [0:0]
         HA State: STANDBY, RG ID: 1
     Established Sessions = 1
```

Notice that the connection replicates, but the bytes transferred are not updated. The connection state (TCP information) is updated regularly through the data interface in order to ensure that traffic is not affected if a failover event occurs.

For more granular output, enter the ***show policy−firewall session zone−pair <ZP> ha*** command. It provides similar output as Example 7, but it allows the user to restrict the output to only the zone−pair specified.

Gather Debug Output

This section shows the debug commands that produce relevant output in order to troubleshoot this feature.

The enablement of debugs can be very strenuous on a busy router. Therefore, you should understand the impact before you enable them.

- ***debug redundancy application group rii event***

  This command is used in order to make sure connections match the correct RII group to be replicated properly. When traffic arrives on the ZBFW, the source and destination interfaces are checked for an RII group ID. This information is then communicated across the data link to the peer. When the standby peer's RII group aligns with the active units, then the syslog in Example 8 is generated, and confirms the RII group IDs that are used in order to replicate the connection:

  Example 8: Syslog

```
debug redundancy application group rii event
debug redundancy application group rii error
!
*Feb  1 21:13:01.378: [RG−RII−EVENT]:  get idb: rii:100
*Feb  1 21:13:01.378: [RG−RII−EVENT]:  get idb: rii:200
```

- ***debug redundancy application group protocol all***

  This command is used in order to confirm that the two peers can see each other. The peer IP address is confirmed in the debugs. As seen in Example 9, ZBFW1 sees its peer in the standby state with IP address ***10.60.1.2***. The reverse is true for ZBFW2.

  Example 9: Confirm Peer IPs in Debugs

```
debug redundancy application group protocol all
!
ZBFW1#
*Feb  1 21:35:58.213: RG−PRTCL−MEDIA: RG Media event, rg_id=1, role=Standby,
   addr=10.60.1.2, present=exist, reload=0, intf=Et0/2, priority=150.
*Feb  1 21:35:58.213: RG−PRTCL−MEDIA: [RG 1] [Active/Active] set peer_status 0.
*Feb  1 21:35:58.213: RG−PRTCL−MEDIA: [RG 1] [Active/Active] priority_event
```

```
   'media: low priority from standby', role_event 'no event'.
*Feb  1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] select fsm event,
   priority_event=media: low priority from standby, role_event=no event.
*Feb  1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] process FSM event
   'media: low priority from standby'.
*Feb  1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] no FSM transition

ZBFW2#
*Feb  1 21:36:02.283: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Active,
   addr=10.60.1.1, present=exist, reload=0, intf=Et0/2, priority=200.
*Feb  1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot]
   set peer_status 0.
*Feb  1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot] priority_event
   'media: high priority from active', role_event 'no event'.
*Feb  1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] select
   fsm event, priority_event=media: high priority from active, role_event=no event.
*Feb  1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] process
   FSM event 'media: high priority from active'.
*Feb  1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] no FSM
   transition
```

Common Issues

This section details some common issues that are encountered.

Control and Data Interface Selection

Here are some tips for the control and data VLANs:

- Do not include the control and data interfaces in the ZBFW configuration. They are only used in order to communicate with each other; therefore, there is no need to secure these interfaces.
- The control and data interfaces can be on the same interface or VLAN. This preserves ports on the router.

Absent RII Group

The RII group must be applied on both the LAN and WAN interfaces. The LAN interfaces must be on the same subnet, but the WAN interfaces can be on separate subnets. If there is an RII group absent on an interface, this syslog occurs in the output of ***debug redundancy application group rii event*** and ***debug redundancy application group rii error***:

```
000515: Dec 20 14:35:07.753 EST: FIREWALL*: RG not found for ID 0
```

Automatic Failover

In order to configure automatic failover, the ZBFW HA must be configured in order to track a Service Level Agreement (SLA) object, and dynamically decrease the priority based on this SLA event. In Example 10, ZBFW HA tracks the link status of the ***GigabitEthernet0*** interface. If this interface goes down, the priority is reduced so that the peer device is more favored.

Example 10: ZBFW HA Automatic Failover Configuration

```
redundancy
 application redundancy
  group 1
   name ZBFW_HA
   preempt
   priority 230
```

```
   control Vlan801 protocol 1
   data Vlan801
   track 1 decrement 200
!
track 1 interface GigabitEthernet0 line-protocol

redundancy
 application redundancy
  group 1
   name ZBFW_HA
   preempt
   priority 180
   control Vlan801 protocol 1
   data Vlan801
```

Sometimes the ZBFW HA does not automatically failover even though there is a decreased priority event. This is because the ***preempt*** keyword is not configured under both devices. The ***preempt*** keyword has different functionality than in Hot Standby Router Protocol (HSRP) or Adaptive Security Appliance (ASA) failover. In ZBFW HA, the ***preempt*** keyword allows a failover event to occur if the priority of the device changes. This is documented in the Security Configuration Guide: Zone−Based Policy Firewall, Cisco IOS Release 15.2M&T. Here's an extract from the Zone−Based Policy Firewall High Availability chapter:

"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 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."

These outputs indicate the proper state:

```
ZBFW01#show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT

ZBFW01#show redundancy application faults group 1
Faults states Group 1 info:
         Runtime priority: [230]
                RG Faults RG State: Up.
                         Total # of switchovers due to faults:           0
                         Total # of down/up state changes due to faults: 0
```

These logs are generated on the ZBFW without any debugs enabled. This log shows when the device becomes active:

```
*Feb  1 21:47:00.579: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
   Init to Standby
```

```
*Feb  1 21:47:09.309: %RG_PROTOCOL−5−ROLECHANGE: RG id 1 role change from Standby
   to Active
*Feb  1 21:47:19.451: %RG_VP−6−BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
   complete.
*Feb  1 21:47:19.456: %RG_VP−6−STANDBY_READY: RG group 1 Standby router is in
   SSO state
```

This log shows when the device goes on standby:

```
*Feb  1 21:47:07.696: %RG_VP−6−BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
   complete.
*Feb  1 21:47:07.701: %RG_VP−6−STANDBY_READY: RG group 1 Standby router is in
   SSO state
*Feb  1 21:47:09.310: %RG_PROTOCOL−5−ROLECHANGE: RG id 1 role change from Active
   to Init
*Feb  1 21:47:19.313: %RG_PROTOCOL−5−ROLECHANGE: RG id 1 role change from
   Init to Standby
```

Asymmetric Routing

Asymmetric routing support is outined in the Asymmetric Routing Support guide.

In order to configure asymmetric routing, add the features to both the redundancy application group global configuration and the interface sub−configuration. It is important to note that asymmetric routing and an RG cannot be enabled on the same interface, because it is not supported. This is due to how asymmetric routing works. When an interface is designated for asymmetric routing, it cannot be part of HA connection replication at that point, because the routing is inconsistent. Configuring an RG confuses the router, because an RG specifies that an interface is part of HA connection replication.

Example 11: Asymmetric Routing Configuration

```
redundancy
 application redundancy
  group 1
    asymmetric−routing interface Ethernet0/3

interface Ethernet0/1
  redundancy asymmetric−routing enable
```

This configuration must be applied on both routers in the HA pair.

The ***Ethernet0/3*** interface listed previously is a new dedicated link between the two routers. This link is used exclusively in order to pass asymmetrically−routed traffic between the two routers. This is why it should be a dedicated link equivalent to the externally−facing interface.

Related Information

- ***Security Configuration Guide: Zone−Based Policy Firewall, Cisco IOS Release 15.2M&T***
- ***Zone−Based Policy Firewall High Availability Security Configuration Guide***
- ***Cisco IOS 15.2M&T***
- ***Cisco IOS Firewall***
- ***Security Product Field Notices***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Nov 05, 2013 Document ID: 115956