配置ZBFW高可用性并排除故障

目录

简介

本指南提供主用/备用设置的区域防火墙高可用性(HA)的基本配置、故障排除命令以及功能所发现的常见问题。

Cisco IOS®基于区域的防火墙(ZBFW)支持HA，以便在主用/备用或主用/主用设置中配置两台Cisco IOS路由器。这允许冗余，以防止单点故障。

先决条件

要求

您的版本必须高于Cisco IOS软件版本15.2(3)T。

使用的组件

本文档不限于特定的软件和硬件版本。

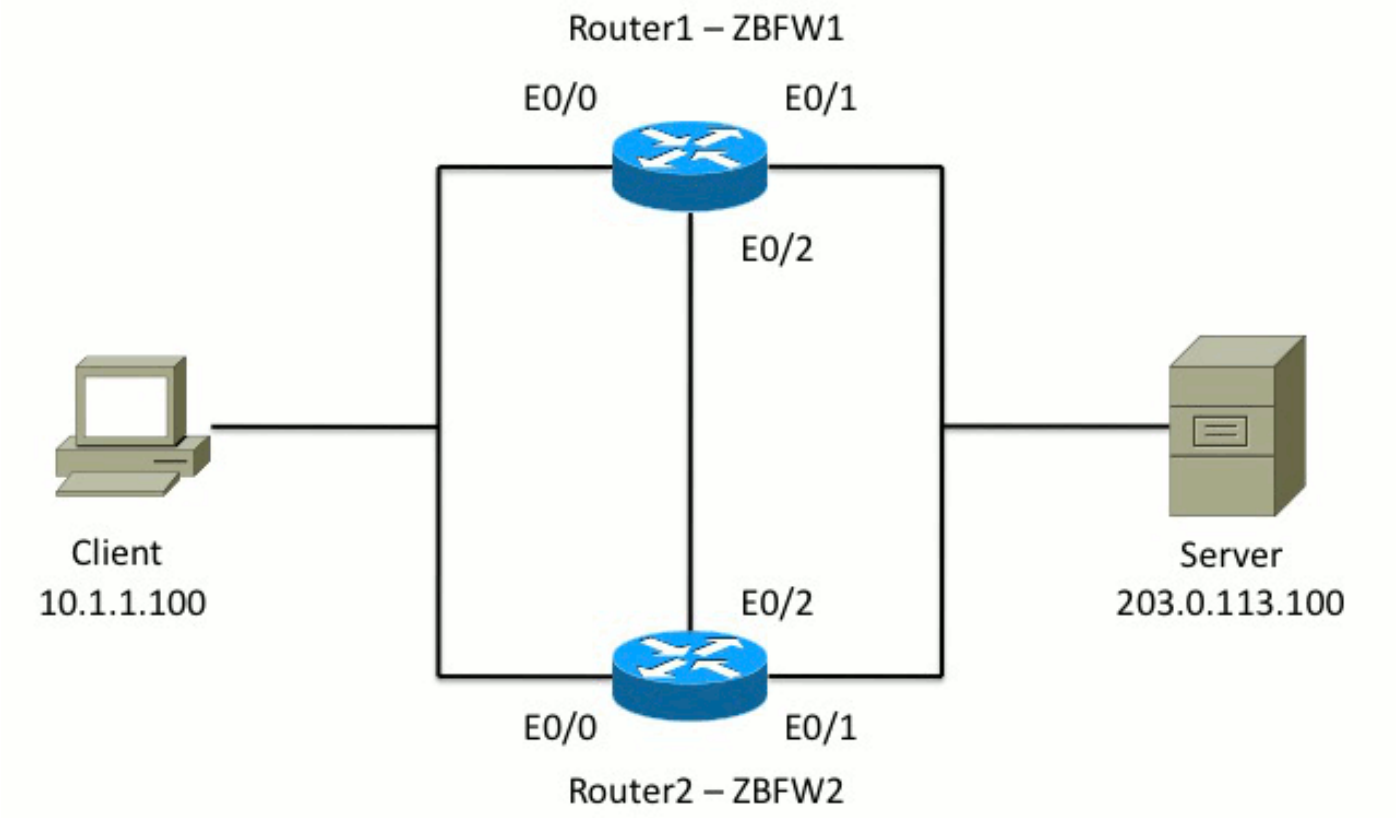
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

此图显示了配置示例中使用的拓扑。



在示例1中所示的配置中，ZBFW配置为从内部到外部检查TCP、UDP和互联网控制消息协议(ICMP)流量。以粗体显示的配置设置HA功能。在Cisco IOS路由器中，HA通过**redundancy** subconfig命令进行配置。要配置冗余，第一步是在全局检查参数映射中启用冗余。

启用冗余后，输入应用**冗余**子配置，并选择用于控制和数**据**的接**口**。控制接口用于交换有关每台路

由器状态的信息。数据接口用于交换有关应复制的连接的信息。

在示例2中，如果路由器1和路由器2都运行正常，**priority**命令也设置为使路由器1成为该对中的主用设备。使用**preempt**命令（本文档也将进一步讨论），以确保在优先级更改后发生故障。

最后一步是将冗余接**口标识符(RII)**和冗**余组(RG)分**配给每个接口。RII组**号**对于每个接口必须唯一，但对于同一子网中的接口，它必须在设备之间匹配。RII仅在两台路由器同步配置时用于批量同步过程。这是两台路由器同步冗余接口的方式。使用**RG** 以指示通过该接口的连接被复制到HA连接表中。

在示例2中，**使用redundancy group 1** 命令在内部接口上创建虚拟IP(VIP)地址。这可确保HA，因为所有内部用户仅与主用设备处理的VIP通信。

外部接口没有任何RG配置，因为这是WAN接口。路由器1和路由器2的外部接口不属于同一Internet服务提供商(ISP)。 在外部接口上，需要动态路由协议来确保流量传递到正确的设备。

示例 1：路由器1配置片段（主机名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
```

示例 2：路由器2配置片段（主机名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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

确认设备可以相互通信

为了确认设备可以相互查看，您必须验证冗余应用组的运行状态是否为up。然后，确保每台设备都承担了正确的角色，并且可以查看其对等设备的正确角色。在示例3中，ZBFW1处于活动状态，并将其对等体检测为备用。在ZBFW2上，情况正好相反。当两台设备也显示运行状态为up，并且检测到对等体存在时，两台路由器可以通过控制链路成功通信。

示例 3：对等体在线状态检测

```
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
```

示例4中的输出显示了有关两台路由器的控制接口的更精细的输出。输出确认了用于控制流量的物理接口，也确认了对等体的IP地址。

示例 4：精细输出

```
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
```

建立通信后，示例5中的命令可帮助您了解为什么每台设备都处于其特定角色。ZBFW1处于活动状态，因为它的优先级高于对等体。ZBFW1的优先级为200，而ZBFW2的优先级为150。此输出以粗体突出显示。

示例 5：角色状态和优先级

```
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
```

最后一个确认是确保RII组ID分配给每个接口。如果您在两台路由器上输入此命令，它们会进行双重检查，以确保设备之间同一子网上的接口对分配了相同的RII ID。如果未使用相同的唯一RII ID配置它们，则连接不会在两台设备之间复制。参见示例6。

示例 6：确认已分配RII组ID

```
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
```

检验连接是否复制到对等路由器

在示例7中，ZBFW1主动传递连接的流量。连接已成功复制到备用设备ZBFW2。要查看区域防火墙

处理的连接，请使用**show policy-firewall session命**令。

示例 7：已处理的连接

```
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
```

请注意，连接会复制，但传输的字节不会更新。连接状态（TCP信息）通过数据接口定期更新，以确保在发生故障切换事件时流量不受影响。

要获得更精细的输出，请**输入show policy-firewall session zone-pair *<ZP>*ha命**令。它提供与示例7类似的输出，但允许用户将输出限制为仅指定区域对。

收集调试输出

本部分显示产生相关输出以排除此功能故障的debug命令。

在繁忙的路由器上启用调试会非常费力。因此，在启用之前，您应了解其影响。

- debug redundancy application group rii event

  此命令用于确保连接与要正确复制的正确RII组匹配。当流量到达ZBFW时，将检查源接口和目的接口的RII组ID。然后，通过数据链路将该信息传送到对等体。当备用对等体的RII组与主用设备对齐时，将生成示例8中的系统日志，并确认用于复制连接的RII组ID:

  示例 8：系统日志

  ```
  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

  此命令用于确认两个对等体是否可以看到对方。对等IP地址在调试中确认。如示例9所示，ZBFW1将其对等体看到其处于IP地址为**10.60.1.2的备用状态**。ZBFW2的情况正好相反。

示例 9：确认调试中的对等IP

```
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
```

常见问题

本节详细介绍所遇到的一些常见问题。

控制和数据接口选择

以下是控制和数据VLAN的一些提示：

- 请勿在ZBFW配置中包含控制接口和数据接口。它们只用于相互通信；因此，无需保护这些接口。
- 控制接口和数据接口可以位于同一接口或VLAN上。这会保留路由器上的端口。

缺席RII组

RII组必须同时应用于LAN和WAN接口。LAN接口必须位于同一子网中，但WAN接口可以位于不同的子网中。如果接口上没有RII组，则在debug redundancy application group rii event和debug redundancy application group ri **error的输出中**会出**现此系统日志**:

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

自动故障切换

要配置自动故障切换，必须配置ZBFW HA以跟踪服务级别协议(SLA)对象，并根据此SLA事件动态降低优先级。在示例10中，ZBFW HA跟踪GigabitEthernet0接口**的链路**状态。如果此接口关闭，优先级会降低，以便对等设备更受青睐。

示例 10：ZBFW HA自动故障切换配置

```
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
```

有时，ZBFW HA不会自动进行故障切换，即使优先级事件减少。这是因为未在两台设**备下**配置preempt关键字。**preempt**关键字的功能与热备份路由器协议(HSRP)或自适应安全设备(ASA)故障切换中的功能不同。在ZBFW HA中，**preempt**关键字允许在设备的优先级发生更改时发生故障切换事件。安全配置指南中对[此进行了说明：基于区域的策略防火墙，Cisco IOS版本15.2M&T](#)。以下是“基于区域的策略防火墙高可用性”一章的摘要：

“在其他情况下，可能会切换到备用设备。导致切换的另一个因素是可在每台设备上配置的优先级设置。优先级值最高的设备是活动设备。如果主用设备或备用设备上发生故障，则设备的优先级会减去可配置的量，称为权重。如果主用设备的优先级低于备用设备的优先级，则会发生切换，备用设备将成为主用设备。通过禁用冗余组的抢占属性可以覆盖此默认行为。您还可以配置每个接口，以在接口的第1层状态关闭时降低优先级。配置的优先级会覆盖冗余组的默认优先级。”

这些输出指示正确的状态：

```
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
```

这些日志在ZBFW上生成，但未启用任何调试。此日志显示设备何时变为活动状态：

```
*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
```

此日志显示设备何时处于备用状态：

```
*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
```

非对称路由

非对称路由支持在“非对称路由支持指南”中介绍。

要配置非对称路由，请将这些功能添加到冗余应用组全局配置和接口子配置。请注意，不能在同一接口上启用非对称路由和RG，因为不支持它。这是由于非对称路由的工作原理。当接口被指定用于非对称路由时，由于路由不一致，因此该接口在此时不能成为HA连接复制的一部分。配置RG会使路由器混淆，因为RG指定接口是HA连接复制的一部分。

示例 11：非对称路由配置

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

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

此配置必须应用于HA对中的两台路由器。

前面列出的Ethernet0/3接口是两台路由器之间的一条新专用链路。此链路专门用于在两台路由器之间传递非对称路由流量。这就是为什么它应该是与面向外部的接口等效的专用链路。

相关信息

- 安全配置指南：基于区域的策略防火墙，思科IOS版本15.2M&T
- 基于区域的策略防火墙高可用性安全配置指南
- 思科IOS 15.2M&T
- Cisco IOS 防火墙
- 安全产品现场通知
- 技术支持和文档 - Cisco Systems