ZBFW高性能的配置和故障排除TechNote

目录

简介

此指南为区域防火墙高可用性(HA)提供基本配置一个活动/等待设置的、以及被看到的故障排除命令和常见问题以功能。

Cisco IOS基于区域的防火墙(ZBFW)支持HA，以便两个Cisco IOS路由器在一个活动/等待或活动/活动设置可以配置。这允许冗余为了防止单点故障。

先决条件

要求

您比Cisco IOS软件Release15.2(3)T必须有版本后。

使用的组件

本文档不限于特定的软件和硬件版本。

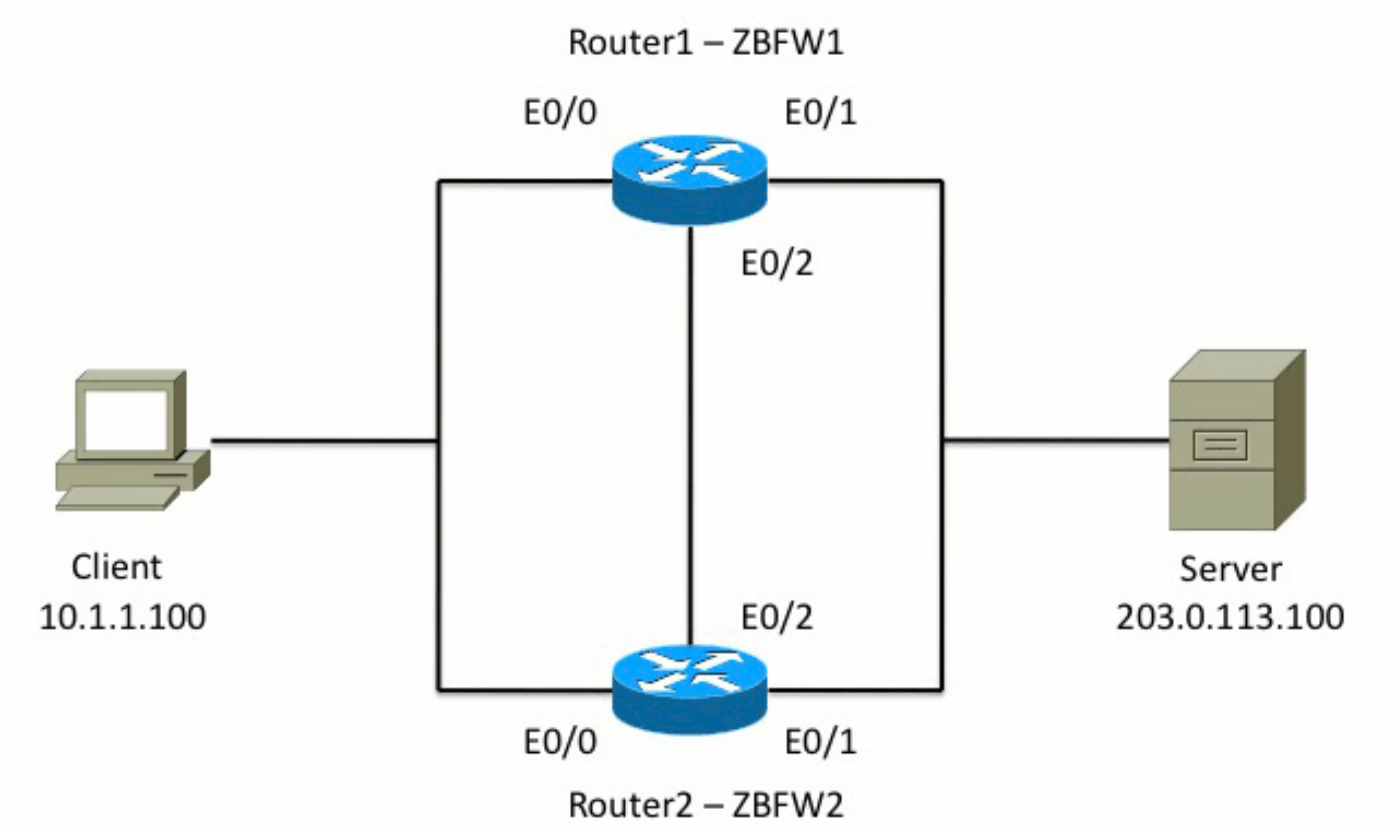
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

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

此图表显示用于配置示例的拓扑。



在示例1显示的配置中， ZBFW配置为了检查TCP，UDP和互联网控制消息协议(ICMP)流量从里向外。在粗体显示的配置设置HA功能。在Cisco IOS路由器中， HA通过**冗余**subconfig命令配置。为了配置冗余，第一步将启用在全局检查参数地图的冗余。

在您启用冗余后，请输入**应用程序冗余**subconfig，并且选择使用**控制**和**数据的**接口。控制接口用于

为了交换关于每个路由器的状态的信息。数据接口用于为了交换关于应该复制的连接的信息。

在示例2，如果路由器1和Router2是可操作的， **priority命令**也设置做路由器1在对的活动装置。**优先占用**命令(也讨论进一步在本文)用于为了保证失败一次发生优先级更改。

最后一步是分配**冗余接口标识符(RII)**和**冗余组(RG)**对每个接口。**RII**组编号必须是唯一为每个接口，但是必须在接口的设备间配比在相同子网。当两路由器同步配置时， RII只使用大批同步进程。这是两路由器如何同步冗余接口。**RG**用于为了表明连接通过该接口复制到HA连接表。

在示例2，**冗余组1**命令用于为了创建在内部接口的一个Virtual IP (VIP)地址。这保证HA，因为所有内部用户只通信与VIP，活动装置单元操作。

因为这是广域网接口，外部接口没有任何RG配置。路由器1和Router2外部接口不属于同样互联网服务提供商。在外部接口，动态路由协议要求为了保证流量通过到正确设备。

示例 1：路由器1配置片断(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：Router2配置片断(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。

确认设备能彼此连通

为了确认设备能互相看到，您必须验证冗余应用组的操作状态是UP。然后，请保证每个设备占领了正确角色，并且能看到其其正确角色的对等体。在示例3， ZBFW1是活跃的并且检测其对等体作为待机。这在ZBFW2被倒转。当两个设备也显示操作状态是UP时，并且他们的对等体在线状态检测，两路由器能在控制链路间成功通信。

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
```

在示例4的输出显示关于两路由器的控制接口的更加粒状的输出。输出确认用于控制流量的物理接口，并且也确认对等体的IP地址。

示例 4：粒状输出

```
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
```

当通信建立时，in命令示例5帮助您知道每个设备为什么在其特定的角色。因为比其对等体，有一高优先级ZBFW1是活跃的。而ZBFW2有优先级150，ZBFW1有优先级200。此输出用黑体字表示。

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
```

最后确认是保证RII Group ID分配到每个接口。如果输入此on命令两路由器，他们复核为了保证在相同子网的接口对在设备之间分配同一个RII ID。如果他们没有配置与同一个唯一RII ID，连接不复制在两个设备之间。参见示例6。

示例 6：确认RII Group ID分配

```
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
```

验证连接复制品到对等`路由器

在示例7中， ZBFW1积极地通过连接的流量。连接顺利地复制对暂挂设备ZBFW2。为了查看区域防火墙处理的连接，使用**session命令显示的策略防火墙**。

示例7 ：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
```

注意连接复制品，然而转接的字节没有更新。连接状态(TCP信息)通过数据接口有规律地更新为了保证流量不受影响，如果故障切换事件发生。

对于更加粒状的输出，请输入**显示策略防火墙会话区域对*<ZP>*** ha命令。它提供相似的输出作为示例7，但是允许用户限制输出到指定的仅区域对。

聚集Debug输出

此部分显示生成相关输出为了排除故障此功能的调试指令。

调试的启动可以是非常吃力的在繁忙的路由器。所以，在您启用他们前，您应该了解影响。

- **debug redundancy应用组rii事件**

  此命令用于为了确保连接匹配正确RII组将适当地复制。当流量在ZBFW时到达，源和目的接口被检查RII Group ID。此信息在对对等体的数据链路间然后被传达。当暂挂对等体的RII组与活动装置时对齐，然后在示例8的Syslog生成，并且确认使用为了复制连接的RII Group ID ：

  示例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应用组协议全部**

  此命令用于为了确认两对等体能互相看到。对端IP地址在调试被确认。如在示例9中看到，ZBFW1在有IP地址10.60.1.2的备用状态看到其对等体。反向真实对ZBFW2。

  示例9 ：调试的确认对等体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

此部分选派遇到的一些常见问题。

控制和数据接口选择

这是控制和数据VLAN的一些提示：

- 请勿在ZBFW配置里包括控制和数据接口。他们只用于为了彼此通信;因此，没有需要巩固这些接口。
- 控制和数据接口可以在同样接口或VLAN。这保留路由器的端口。

缺少RII组

RII组在LAN和广域网接口必须应用。LAN接口必须在相同子网，但是广域网接口可以在独立子网。如果有RII组缺少在接口，此Syslog在**debug redundancy应用组rii事件**和**debug redundancy应用组rii错误中**输出发生：

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

自动故障切换

为了配置自动故障切换，必须配置ZBFW HA为了跟踪一个服务级别协议对象和动态地减小根据此SLA事件的优先级。在示例10中， ZBFW HA跟踪**GigabitEthernet0**接口的链接状态。如果此接口断开，减少优先级，以便对等设备是支持。

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不自动故障切换，即使有一个减小的优先级事件。这是因为**优先占用**关键字没有配置在两个设备下。**优先占用**关键字有另外功能比在热备份路由协议(HSRP)或可适应安全工具(ASA)故障切换。在ZBFW HA中，如果设备的优先级更改，**优先占用**关键字允许故障切换事件发生。这在安全配置指南描述：基于区域的策略防火墙， Cisco IOS版本15.2M&T。这是从基于区域的策略防火墙高性能的章节的解压缩：

“对暂挂设备的一个切换能在其他情况下发生。能导致切换的另一个要素是在每个设备可以配置的优先级设置。有最高优先级的值的设备是活动设备。如果故障在活动或暂挂设备发生，设备的优先级由一可配置数量减少，叫作权重。如果活动设备的优先级在暂挂设备的优先级之下下跌，切换发生，并且暂挂设备变为活动设备。此默认行为可以改写由禁用冗余组的抢占属性。当接口的第1层状态断开时，您能也配置每个接口减小优先级。配置的优先级改写冗余组的默认优先级”。

这些输出指示相应的状态：

```
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生成，不用启用的任何调试。当设备变得激活，此日志显示：

```
*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
```

当设备在待机，去此日志显示：

```
*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

不对称路由支持在不对称路由支持指南outined。

为了配置不对称路由，请添加功能到冗余应用组全局配置和接口SUB配置。注释该不对称路由是重要的，并且RG在同一个接口不可能启用，因为不支持。这归结于不对称路由如何工作。当接口被选定不对称路由时，它不可以那时是HA连接复制的一部分，因为路由不一致。配置RG混淆路由器，因为RG指定接口是HA连接复制的一部分。

示例11 ：不对称路由配置

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

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

在HA对的两路由器必须应用此配置。

以前列出的Ethernet0/3接口是两路由器之间的一条新的专用链路。此链路完全使用为了通过不对称已路由流量在两路由器之间。这就是为什么它应该是专用链路等同到外部面对的接口。

相关信息

- 安全配置指南：基于区域的策略防火墙， Cisco 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
- Cisco IOS 15.2M&T
- Cisco IOS 防火墙
- 安全产品售后通知
- 技术支持和文档 - Cisco Systems