**KFW防火墙旁HA配置案例**

高可靠性配置是每个安全设备的基本配置，本案例将详细介绍KFW防火墙HA配置过程及不同场景的测试。

# 网络部署

如图所示，两台防火墙做HA，提供冗余。Port1为Inside口，Port2为Outside口，Port5和Port6为心跳接口。



# 设备配置

本案例中只介绍防火墙相关的配置，其他配置默认已配好。

配置前请确认两台防火墙满足以下条件。

* 相同的硬盘配置；
* 相同的接口型号和数量；
* 相同的软交换配置；
* 没有接口配置配置了DHCP或PPPoE地址模式；
* 两台APPWay设备具有相同的软件版本；
* 两台APPWay设备设置为相同的运行模式（NAT或透明模式）；
* 两台APPWay设备设置为相同的虚拟机模式。

## 防火墙配置

1. 登陆防火墙A，进入“系统管理>控制面板>状态”页面，在系统信息栏修改防火墙名称为“FirewallA”。



1. 进入“系统管理>配置>高可靠性”页面，进行高可靠性配置。
* 选择模式为“主动-被动”；
* 设备优先级保持默认的“128”；
* 心跳线接口栏勾选Port5和Port6的“应用”选项，并配置优先级为50；
* 勾选Port1和Port2的“端口监控”。



1. 登陆防火墙B，进入“系统管理>控制面板>状态”页面，在系统信息栏修改防火墙名称为“FirewallB”。
2. 进入“系统管理>配置>高可靠性”页面，进行高可靠性配置。
* 选择模式为“主动-被动”；
* 设备优先级配置为“120”；
* 心跳线接口栏勾选Port5和Port6的“应用”选项，并配置优先级为50；
* 勾选Port1和Port2的“端口监控”。



## HA测试

在正确连线和配置HA后，两台防火墙开始进行主备选举，选举优先次序如下。

* 监控端口的状态
* 开机时间
* 优先级
* 序列号
1. 两台防火墙依次开机，FirewallB先开机，5分钟之后FirewallA开机，虽然B的优先级低于A但仍然成为主。



1. 两台防火墙同时开机，开机间隔时间小于5分钟，则优先级高的防火墙A成为主。



1. 通过设置CLI命令忽略开机时间，选举时不考虑开机时间。

#define system ha

(ha)#set override enable

(ha)#end

两台防火墙依次开机，FirewallB先开机，5分钟之后FirewallA开机，忽略开机时间后，优先级高的FirewallA成为了主。

1. 监控的端口失去连接后HA会重新进行选举，主防火墙A监控的Port1端口宕掉后，角色由主变成了从，FirewallB变成了主。（丢失两个Ping包）。



1. 端口恢复正常后，防火墙A重新变为主。



1. 如果两台防火墙的开机时间、监控的端口和优先级都相同，则比较设备序列号，序列号大的设备成为主。



1. 心跳线测试，如果其中一条心跳线断开，则防火墙仍然可以相互联系并保持通信，当两条心跳线都断开时，两个防火墙将失去联系，都成为主，网络瘫痪。

## 主动-主动模式

HA如果是主动-主动模式，则两台防火墙同时转发流量，相互做负载均衡。

1. 主动-主动模式的配置只需要在配置防火墙高可靠性时选择模式为“主动-主动”其他配置和主动-被动一样。



1. 缺省状态下只有病毒扫描的会话重新定向实现负载均衡，如果需要让所有的会话实现负载可通过以下配置命令实现。

#define system ha

(ha)#set load-balance-all enable

(ha)#end

1. 可通过CLI命令设置负载均衡的调度算法。

#define system ha

(ha)#set schedule least-connection

(ha)#end

本防火墙支持的负载均衡调度算法有以下几种。

* + Hub
	+ Least-connection 最少连接
	+ Round-robin (default) 轮询
	+ Weighted round-robin 权重
	+ Random 随机
	+ IP
	+ IP + port