防火墙镜像流量配置示例

镜像功能在4.2版本中支持



实验拓扑如上：

实验需求如下：

将KFW M2/1口的双向数据流量镜像到M5/1口（此为示例，用户可根据实际需要镜像单向或双向流量），然后连接到监控分析平台进行数据流量分析，在KFW做镜像配置达到需求，在KFW M5/1上可以抓到镜像过来的数据流量。

测试仪地址：192.168.1.67/24

测试仪client:10.1.1.2/24 GW:10.1.1.1/24

测试仪server:10.2.2.2/24 GW:10.2.2.1/24

配置如下：

* KFW部署为NAT模式，M2/1、M2/2配置IP地址



* KFW策略中配置放行策略



* 进入KFW命令行界面进行配置，命令如下

define system mirror-config

edit mirror

 set span enable

 set span-source-port M2/1

 set span-dest-port M5/1

 set span-direction both

 end

* 测试仪client端向server端注入流量，在KFW M5/1上抓包观察

dump sniffer packet m5/1 none 4



此时说明实验成功，KFW通过镜像配置达到实验目的。