KFW防火墙NAT功能配置案例

现在的网络网络环境中，NAT功能几乎是必不可少的，KFW防火墙也配置了各种NAT功能满足用户的上网需求。

## 1、网络拓扑

如图所示，内网用户使用172.16.1.0/24网段进行通信，使用221.221.155.0/29网段上外网，使用防火墙进行地址转换。其中防火墙Port1为外网口，Port2为内网口。



## 2、基本NAT配置

1. 登陆防火墙，进入“系统管理>网络>接口”页面，选择Port1，单击“编辑”按钮，配置IP地址221.221.155.2/29。



1. 单击“OK”按钮，保存配置。
2. 选择Port2，单击“编辑”按钮，配置IP地址172.16.1.254/24。



1. 单击“OK”按钮，保存配置。
2. 进入“防火墙>策略>策略”页面，单击“创建”按钮，配置策略放行内网访问外网的流量，同时启用端口NAT功能。



1. 进入“路由>静态>静态路由”页面，选择默认路由进行编辑。



1. 单击“OK”按钮，完成配置，内网用户可以正常访问外网，并通过外网口Port1的公网地址进行转换。

## 3，服务器映射配置

内网Web服务器172.16.1.10/24需要单独的公网地址与外界进行通信，可以在防火墙上配置地址映射。

1. 登陆防火墙，进入“防火墙>虚拟IP>虚拟IP”，单击“创建”按钮，配置地址映射。



1. 单击“OK”按钮，完成配置。
2. 进入“防火墙>策略>策略”页面，单击“创建”按钮，添加策略，允许访问内网Web服务器。



1. 单击“OK”按钮，完成配置，外部可访问Web服务器，同时Web服务器访问网络时使用公网地址221.221.155.6。
2. 如果Web服务器只开放80端口，则需配置映射时进行端口映射。



1. 策略不变，则外网只能访问Web服务器的80端口，同时该Web服务器访问外网使用Port1端口的NAT功能，而不再使用映射的公网地址。
2. 如果映射时，公网地址使用外网端口地址，而且外网口地址是通过DHCP或PPPoE获取的，则公网IP地址范围可配置为0.0.0.0，映射时自动选择外网口获取的地址。



1. 如果需要映射的服务器是一段地址，则可以编辑映射关系，设置为IP地址范围，此时内网地址与公网地址从开始IP为一一映射关系，如下图映射关系为172.16.1.10映射221.221.155.3，172.16.1.11映射221.221.155.4，172.16.1.12映射221.221.155.5，172.16.1.13映射221.221.155.6。



## 4、NAT地址池配置

如果用户有多个公网地址，希望通过NAT转换时都可以用到，则可以建立NAT Pool。

1. 登陆防火墙，进入“防火墙>虚拟IP>IP池”页面，单击“创建”按钮，新建IP地址池。



1. 进入“防火墙>策略>策略”页面，编辑内网访问外网的策略，选择“启用NAT”，并勾选“动态IP地址池”，选择“NAT Pool”。



1. 单击“OK”按钮，完成配置，则内网访问外网时，使用“NAT Pool”中的公网地址进行转换，并且会依次循环的选择每一个公网地址。

## 5、中央NAT表配置

如果内网地址是多个地址段，公网地址也是多个地址段，则可以配置中央NAT表，统一进行转换。

1. 登陆防火墙，进入“防火墙>地址>地址”页面，创建需要访问外网的地址范围。





1. 进入“防火墙>虚拟IP>IP池”页面，创建NAT转换公网地址池。





1. 进入“防火墙>策略>显式NAT表”页面，单击“创建”按钮，新建NAT转换表，源地址选择要进行转换的内网地址段，转换地址选择动态IP池。



1. 进入“防火墙>策略>策略”页面，编辑策略，内网访问外网使用中央NAT表。



1. 单击“OK”按钮，完成配置，内网用户可以访问外网，并使用NAT地址表中的转换关系。