防火墙NAT应用案例

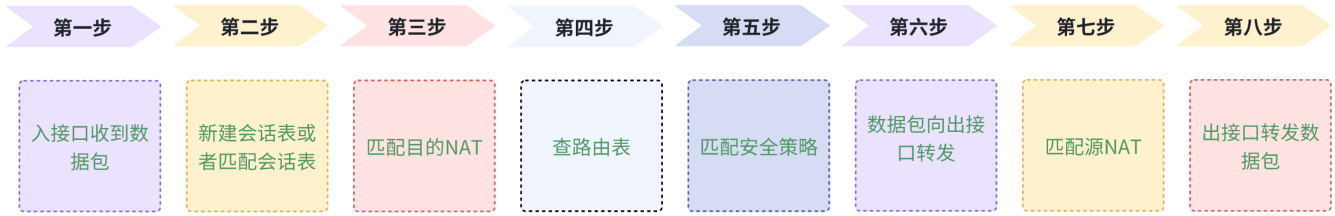
一、部署前提

- 使用版本：本配置举例是在V4.2-build0001-230926版本上进行配置和验证的。
- 本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺 省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置 不冲突。
- 本文档假设您具备一定数通知识基础，仅关注防火墙的配置说明。

二、功能原理

2.1 防火墙处理流程

数据包从防火墙通过时的处理流程为：



2.2 源NAT

源NAT转换通俗地讲即将源地址转换为另一个地址，目的地址不变。局域网的私网地址需要将源地址转换为公网地址才能访问外网。防火墙在具体配置上提供三种选择：

- **启用NAT：**即多（内网IP）对一(出接口IP)的源地址映射，通过不同的源端口号来区分流量。
- **动态IP地址池：**通过关联ip-pool实现多对多的源地址转换，但这类转换后的源地址和源端口都是随机的且不可控。需要注意的是IP-pool一旦创建其包含的IP即会在网络中做出ARP响应，不管其是否在策略里调用。
- **启用地址映射表（即中央NAT表）：**允许管理员对源端口映射有更多的控制，它允许对具有固定端口行为的源端口范围映射进行控制。例如，通过使用从1000-1500到5000-5500的源端口映射，该特性将确保源端口映射从1000- 5000、1001- 5001、…、1500- 5500。

> 💡 **注：**由于中央NAT表特性继承了固定端口行为，这意味着中央NAT表的部署场景必须确保IP范围的唯一映射，就像一对一的静态NAT一样。如果需要多对一源的NAT，则该特性将不适合这

种环境，因为来自不同pc的传入端口可能使用相同的源端口号访问相同的Internet公共服务器。

2.3 目的NAT

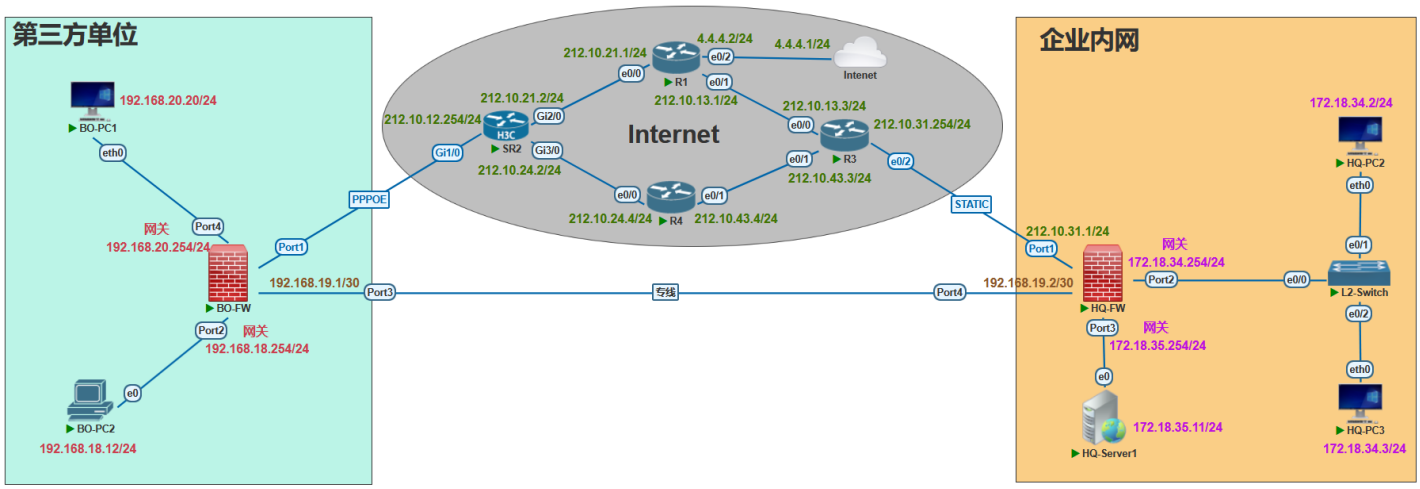
目的NAT转换通俗地讲即将目的地址转换为另一个地址，源地址不变。公网地址访问私网地址的服务器首先是将数据发给服务器所在的局域网的公网地址，在防火墙上则是通过配置VIP（虚拟IP映射）来实现目的NAT.

虚拟 IP 地址通常用于匹配的外部（公共）内部（私人）的目的地IP 地址的NAT（DNAT）。这是类似于使用一个 IP 池具有可预测的静态地址映射和一对一的优势。这类的虚拟 IP 可以有效的保护内网服务器的真实地址，是NAT 实现的一个目的之一。地址转换技术可以有效的隐藏内部局域网中的主机，因此同时是一种有效的网络安全保护技术。

三、组网拓扑

如下图所示，第三方单位（拨号方式获取动态公网IP）和企业（有固定公网IP地址段）分别接入了Internet。

同时因业务需要第三方单位和企业之间拉有一条点对点专线。



四、源NAT应用

4.1 启用NAT

4.1.1 需求

1. 第三方单位通过pppoe拨号上网（获取的动态公网IP）。
2. 第三方单位内网PC需要访问Internet。

4.1.2 配置

1. 定义内网IP地址段对象-----***防火墙/地址/地址***

2. 定义区并关联内外网接口-----***系统管理/网络/区***

3. 创建策略并启用NAT-----***防火墙/策略/策略***

4.1.3 验证

1. 查看防火墙会话表----***监控/实时数据/会话分析***

4.2 动态IP地址池

4.2.1 需求

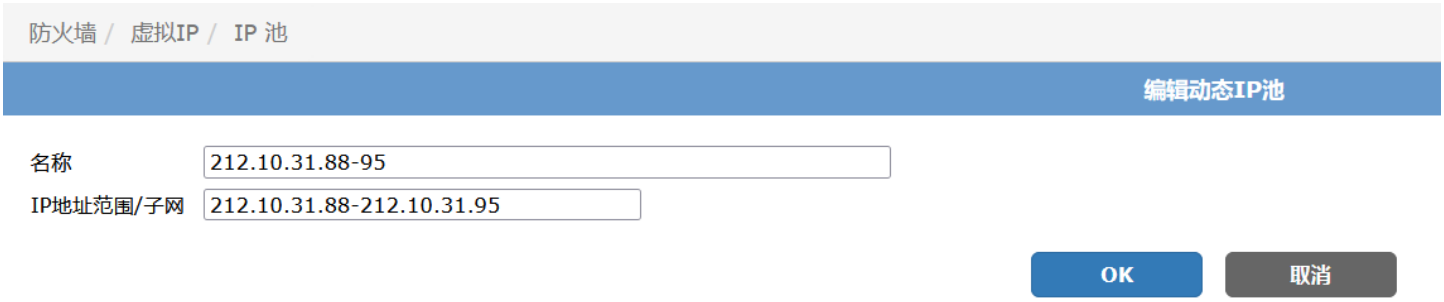
企业有多个公网IP，为更合理高效的使用公网IP资源。专门分配一段公网IP（212.10.31.88-95）给内网用户访问Internet使用。

4.2.2 配置

1. 定义内网IP地址段对象-----***防火墙/地址/地址***

2. 定义区并关联内外网接口-----***系统管理/网络/区***

3. 定义IP地址池-----***防火墙/虚拟IP/IP池***



4. 创建策略并启用NAT-----***防火墙/策略/策略***

4.2.3 验证

1. 查看防火墙会话表----***监控/实时数据/会话分析***

1 / 1 总计: 17 清除所有的过滤条目

#	协议	源地址	源端口	目标地址	目标端口	NAT	NAT翻译地址	NAT翻译端口	策略ID
1	udp	172.18.35.11	55914	8.8.8.8	53	源地址	212.10.31.91	51236	2
2	tcp	172.18.35.11	50600	142.250.204.74	443	源地址	212.10.31.91	49126	2
3	tcp	172.18.35.11	50601	172.217.24.234	443	源地址	212.10.31.91	29671	2
4	tcp	172.18.35.11	50598	142.250.204.42	443	源地址	212.10.31.91	33256	2
5	udp	172.18.35.11	57531	8.8.8.8	53	源地址	212.10.31.91	29941	2
6	tcp	172.18.35.11	50599	172.217.24.106	443	源地址	212.10.31.91	51689	2
7	tcp	172.18.34.2	1800	114.114.114.114	883	源地址	212.10.31.90	39238	2
8	tcp	172.18.35.11	50596	142.250.199.74	443	源地址	212.10.31.91	53226	2
9	tcp	172.18.35.11	50590	58.254.137.226	443	源地址	212.10.31.91	40912	2
10	udp	172.18.35.11	57605	8.8.8.8	53	源地址	212.10.31.91	30539	2
11	tcp	172.18.35.11	50597	142.250.207.74	443	源地址	212.10.31.91	42987	2
12	tcp	172.18.35.11	50602	142.250.204.106	443	源地址	212.10.31.91	58852	2
13	udp	172.18.35.11	59865	114.114.114.114	53	源地址	212.10.31.91	29591	2
14	tcp	172.18.35.11	50594	142.250.66.106	443	源地址	212.10.31.91	42988	2
15	tcp	172.18.34.3	3800	8.8.8.8	6788	源地址	212.10.31.91	58518	2
16	tcp	172.18.35.11	50603	142.250.204.138	443	源地址	212.10.31.91	39909	2
17	tcp	172.18.35.11	50595	142.250.66.138	443	源地址	212.10.31.91	61421	2

4.3 启用地址映射表

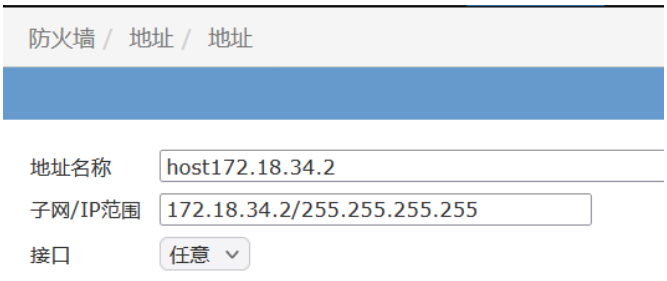
4.3.1 需求

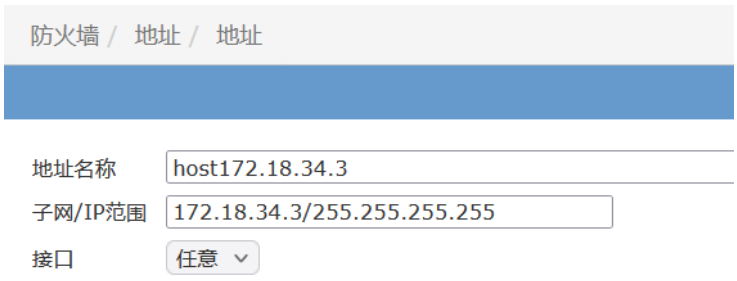
企业终端HQ-PC2和HQ-PC3某一应用向Internet服务器上传数据时要求源端口连续固定。

	源地址	转换后源地址	源端口范围	转换后源端口范围
HQ-PC2	172.18.34.2	212.10.31.2	1000-1500	3000-3500
HQ-PC3	172.18.34.3	212.10.31.3	1000-1500	3000-3500

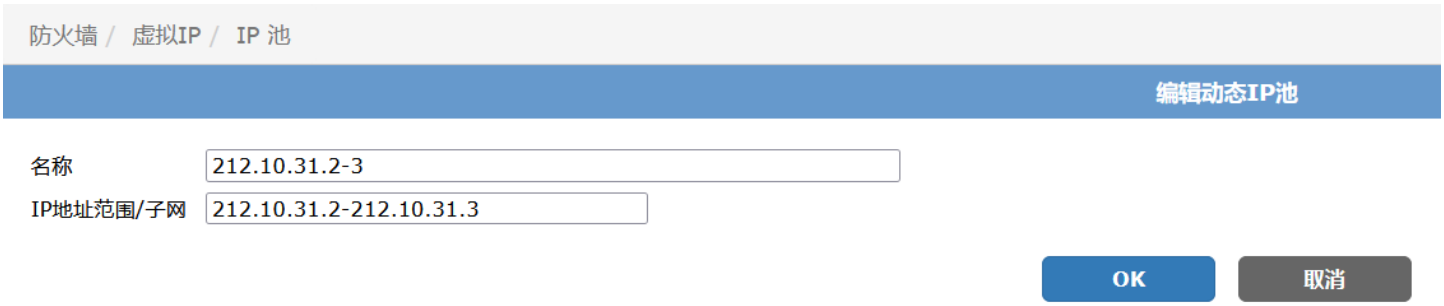
4.3.2 配置

1. 定义内网IP地址段对象-----***防火墙/地址/地址***

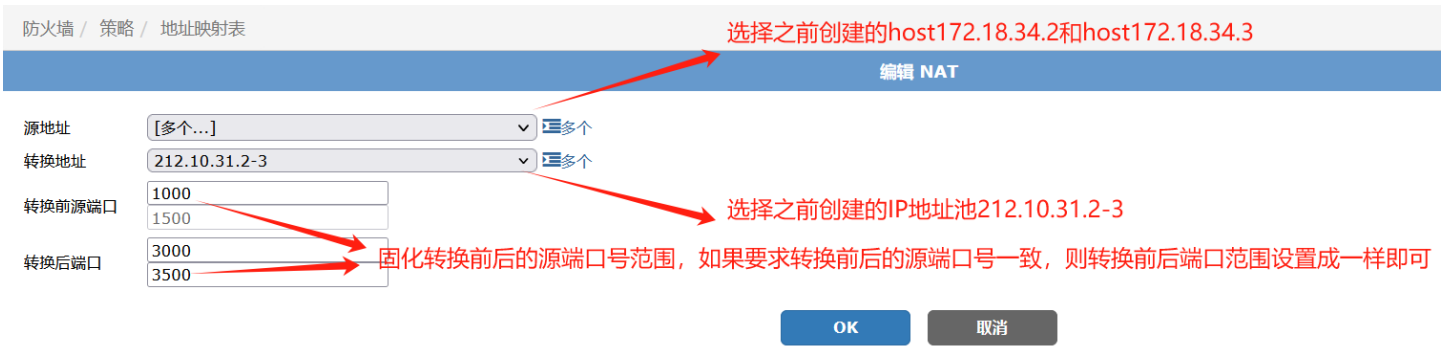




2. 定义IP地址池-----***防火墙/虚拟IP/IP池***



3. 创建地址映射表-----***防火墙/策略/地址映射表***



4. 创建策略并启用地址映射表-----***防火墙/策略/策略***

4.3.3 验证

1. 查看防火墙会话表----***监控/实时数据/会话分析***

五、目的NAT应用

5.1 VIP-虚拟IP地址

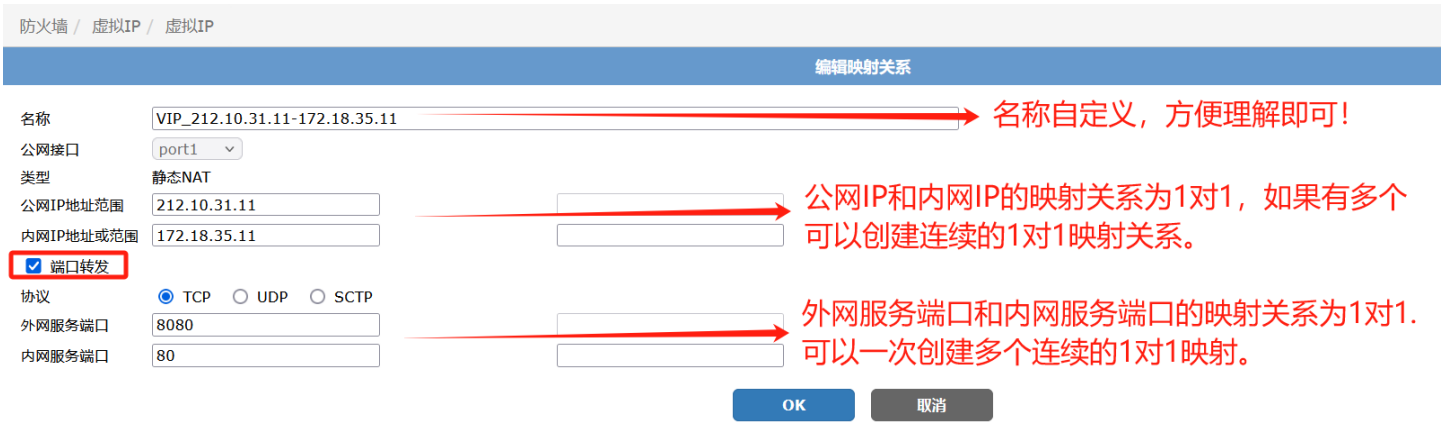
5.1.1 需求

企业的服务器HQ-Server1(172.18.35.11) 向Internet提供Web服务。同时因为http服务的默认80端口在运营商网络一般是被禁止的，所以同时需要做目的端口转换。

服务器	内网IP	内网端口	映射公网IP	映射公网端口
HQ-Server1	172.18.35.11	80	212.10.31.11	8080

5.1.2 配置

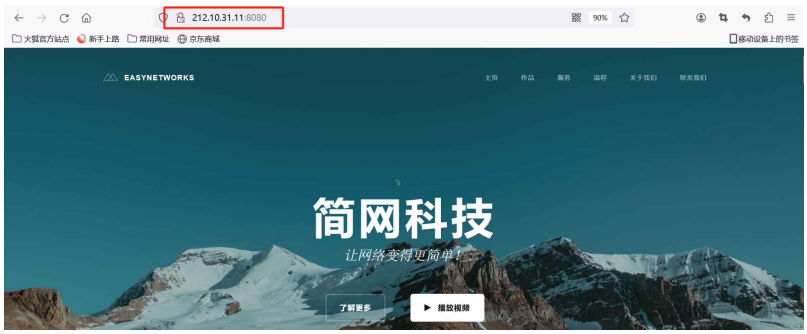
1. 定义虚拟IP（VIP）-----***防火墙/虚拟IP/虚拟IP***



2. 配置策略调用虚拟IP-----***防火墙/策略/策略***

5.1.3 验证

1. 查看防火墙会话表----***监控/实时数据/会话分析***



5.2 通过VIP实现一对一的源NAT

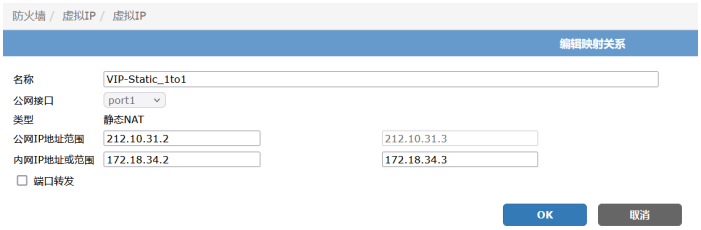
5.2.1 需求

企业终端HQ-PC2和HQ-PC3实现一对一的源地址转换。

终端	内网IP	内网端口	映射公网IP	映射公网端口
HQ-PC2	172.18.34.2	1-65535	212.10.31.2	1-65535
HQ-PC3	172.18.34.3	1-65535	212.10.31.3	1-65535

5.2.2 配置

1. 定义虚拟IP（VIP）-----***防火墙/虚拟IP/虚拟IP***



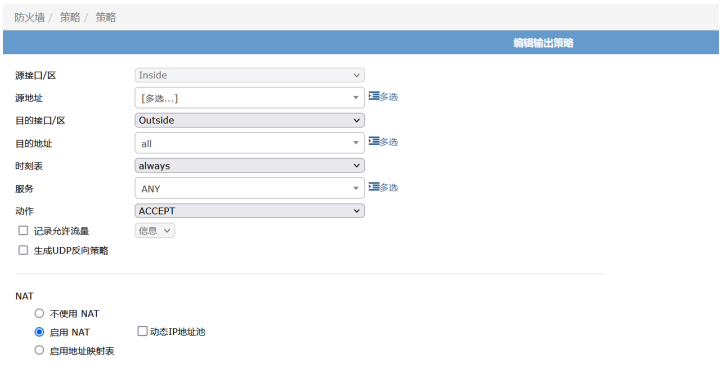

```
define firewall vip
edit "VIP-Static_1to1"
        set extintf "port1"
        set extip 212.10.31.2
        set mappedip 172.18.34.2-172.18.34.3
        set nat-source-vip enable
    next
end
```

注：nat-source-vip

disable:对出VIP外部接口的流量，只强制源NAT映射的IP为外部IP。

enable:对所有流量强制源NAT映射IP为VIP的外部IP

2. 配置策略调虚拟IP-----***防火墙/策略/策略***



5.2.3 验证

1. 查看防火墙会话表----***监控/实时数据/会话分析***


会话列表
转换前后源端口一对一
分离
1
/ 1
总计: 2
清除所有的过滤条目
协议 源地址 源端口 目标地址 目标端口 NAT NAT翻译地址 NAT翻译端口
1 tcp 172.18.34.2 8080 114.114.114.114 69 源地址 212.10.31.2 8080
2 tcp 172.18.34.3 8080 114.114.114.114 69 源地址 212.10.31.3 8080
源地址转换映射的是VIP组的映射关系，而不是出接口IP