

# 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

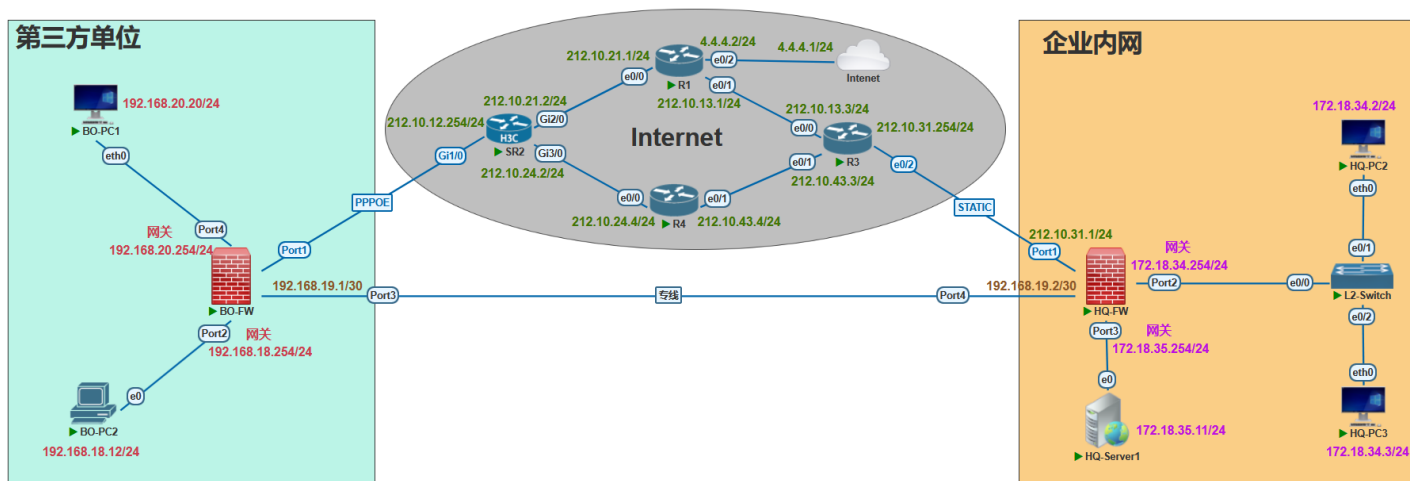
目的NAT转换通俗地讲即将目的地址转换为另一个地址，源地址不变。公网地址访问私网地址的服务器首先是将数据发给服务器所在的局域网的公网地址，在防火墙上则是通过配置VIP（虚拟IP映射）来实现目的NAT。

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**

防火墙 / 地址 / 地址

创建 编辑 删除

定义内网IP地址段

	名称	地址 / 域名	接口
<input type="checkbox"/>	192.168.18.0/24	192.168.18.0/255.255.255.0	任意
<input type="checkbox"/>	192.168.20.0/24	192.168.20.0/255.255.255.0	任意
<input type="checkbox"/>	all	0.0.0.0/0.0.0.0	任意

## 2. 定义区并关联内外网接口-----**系统管理/网络/区**

系统管理 / 网络 / 区

创建 编辑 删除

	名称	屏蔽本区域内的流量	接口成员
<input type="checkbox"/>	Inside	No	port2, port4
<input type="checkbox"/>	Outside	No	port1

## 3. 创建策略并启用NAT-----**防火墙/策略/策略**

防火墙 / 策略 / 策略

编辑输出策略

源接口/区: Inside

源地址: [多选...] 选择之前定义好的内网IP地址网段

目的接口/区: Outside

目的地址: all

时刻表: always

服务: ANY

动作: ACCEPT

记录允许流量

生成UDP反向策略

NAT

不使用 NAT

启用 NAT

动态IP地址池

启用地址映射表

---

防火墙 / 策略 / 策略

创建 编辑 删除 移动到 复制 插入 冲突检查 有效性检查 进入批处理 [列设定]  基于接口查看  清单式查看

	序号	策略ID	源	目的	源地址	目的地址	时刻表	服务	动作	状态
<input type="checkbox"/>	1	1	Inside	Outside	192.168.18.0/24 192.168.20.0/24	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>

### 4.1.3 验证

#### 1. 查看防火墙会话表-----**监控/实时数据/会话分析**

## 转换后源端口变化

#	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	udp	192.168.18.12	60714	8.8.8.8	53	源地址	212.10.12.2	54628
2	udp	192.168.18.12	56791	8.8.8.8	53	源地址	212.10.12.2	49049
3	udp	192.168.18.12	57424	8.8.8.8	53	源地址	212.10.12.2	42526
4	udp	192.168.18.12	56933	8.8.8.8	53	源地址	212.10.12.2	43563
5	udp	192.168.18.12	55077	8.8.8.8	53	源地址	212.10.12.2	32107
6	tcp	192.168.20.20	57032	114.114.114.114	7	源地址	212.10.12.2	35462

## 转换后源地址为出接口地址

## 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**

名称	地址 / 域名	接口
172.18.34.0/24	172.18.34.0/255.255.255.0	任意
172.18.35.0/24	172.18.35.0/255.255.255.0	任意

#### 2. 定义区并关联内外网接口-----**系统管理/网络/区**

名称	屏蔽本区域内的流量	接口成员
Inside	No	port2, port3
Outside	No	port1

#### 3. 定义IP地址池-----**防火墙/虚拟IP/IP池**

名称

IP地址范围/子网

#### 4. 创建策略并启用NAT-----防火墙/策略/策略

源接口/区

源地址  多选

目的接口/区

目的地址  多选

时刻表

服务  多选

动作

记录允许流量

生成UDP反向策略

点击多选，选择之前定义的IP地址段

NAT

不使用 NAT

启用 NAT  动态IP地址池

启用地址映射表

选择之前创建的IP地址池

防火墙 / 策略 / 策略

[ 列设定 ]  基于接口查看  清单式查看

■	序列号	策略ID	源	目的	源地址	目的地址	时刻表	服务	动作	状态	计数	NAT	IP池
<input type="checkbox"/>	1	2	Inside	Outside	<ul style="list-style-type: none"> <li>● 172.18.34.0/24</li> <li>● 172.18.35.0/24</li> </ul>	all	always	● ANY	ACCEPT	<input checked="" type="checkbox"/>	460 / 58 KB	<input checked="" type="checkbox"/>	212.10.31.88-95

### 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**

防火墙 / 地址 / 地址

地址名称

子网/IP范围

接口

防火墙 / 地址 / 地址

地址名称

子网/IP范围

接口

## 2. 定义IP地址池-----**防火墙/虚拟IP/IP池**

防火墙 / 虚拟IP / IP 池

编辑动态IP池

名称

IP地址范围/子网

## 3. 创建地址映射表-----**防火墙/策略/地址映射表**

防火墙 / 策略 / 地址映射表

选择之前创建的host172.18.34.2和host172.18.34.3

编辑 NAT

源地址

转换地址

转换前源端口

转换后端口

选择之前创建的IP地址池212.10.31.2-3

固化转换前后的源端口号范围，如果要求转换前后的源端口号一致，则转换前后端口范围设置成一样即可

## 4. 创建策略并启用地址映射表-----**防火墙/策略/策略**

防火墙 / 策略 / 策略

编辑输出策略

源接口/区

源地址

目的接口/区

目的地址

时刻表

服务

动作

记录允许流量

生成UDP反向策略

NAT

不使用 NAT

启用 NAT  动态IP地址池

启用地址映射表

策略的源地址目的地址  
服务等可根据实际需求  
做进一步细化控制，本  
例默认不做限制

### 4.3.3 验证

#### 1. 查看防火墙会话表----**监控/实时数据/会话分析**

#	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	1000	192.168.6.1	443	源地址	212.10.31.2	3000
2	tcp	172.18.34.3	1000	192.168.6.1	443	源地址	212.10.31.3	3000
3	tcp	172.18.34.2	1001	192.168.6.1	443	源地址	212.10.31.2	3001
4	tcp	172.18.34.3	1001	192.168.6.1	443	源地址	212.10.31.3	3001

转换前端口1000-1001  
转换后端口3000-3001

#	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	800	192.168.6.1	443	源地址	212.10.31.1	877
2	tcp	172.18.34.3	800	192.168.6.1	443	源地址	212.10.31.1	522
3	tcp	172.18.34.2	900	192.168.6.1	443	源地址	212.10.31.1	969
4	tcp	172.18.34.3	900	192.168.6.1	443	源地址	212.10.31.1	525

不在地址映射表范围的源端口，防火墙的处理方式为源地址转换为出口IP转换后的源端口取值不固定。

## 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

防火墙 / 虚拟IP / 虚拟IP

编辑映射关系

名称: VIP\_212.10.31.11-172.18.35.11 → 名称自定义，方便理解即可!

公网接口: port1

类型: 静态NAT

公网IP地址范围: 212.10.31.11 → 公网IP和内网IP的映射关系为1对1，如果有多个可以创建连续的1对1映射关系。

内网IP地址或范围: 172.18.35.11

端口转发

协议:  TCP  UDP  SCTP

外网服务端口: 8080 → 外网服务端口和内网服务端口的映射关系为1对1. 可以一次创建多个连续的1对1映射。

内网服务端口: 80

OK 取消

##### 2. 配置策略调用虚拟IP-----防火墙/策略/策略



源接口/区: Outside

源地址: all

目的接口/区: Inside

目的地址: VIP\_212.10.31.11-172.18.35.11

时刻表: always

服务: ANY

动作: ACCEPT

记录允许流量

生成UDP反向策略

在目的地址处调用之前创建的虚拟IP

NAT

不使用 NAT

启用 NAT

启用地址映射表

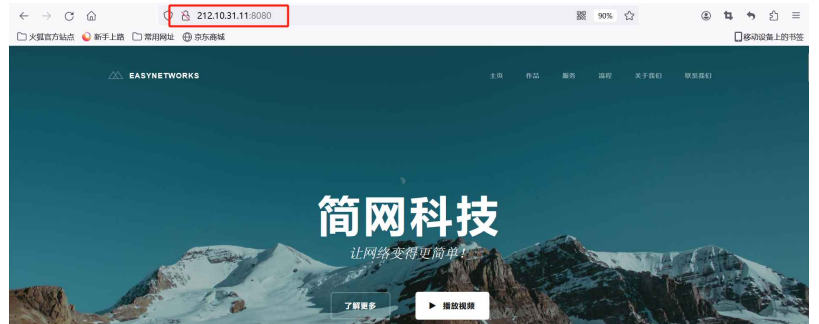
动态IP地址池

关于此处是否需要启用NAT，需要考虑的是外网访问内网的流量是否存在回程路由。在此例中我们出口防火墙是有一条缺省路由指向外网，所以不需要启用NAT。但在一些第三方单位接入的场景中，双方路由是完全隔离且不能随意互相引入，这时候就需要考虑启用源NAT转换。

### 5.1.3 验证

#### 1. 查看防火墙会话表----**监控/实时数据/会话分析**

#	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	192.168.6.2	26038	212.10.31.11	8080	目标地址	172.18.35.11	80
2	tcp	192.168.6.2	26037	212.10.31.11	8080	目标地址	172.18.35.11	80
3	tcp	192.168.6.2	26043	212.10.31.11	8080	目标地址	172.18.35.11	80
4	tcp	192.168.6.2	26042	212.10.31.11	8080	目标地址	172.18.35.11	80
5	tcp	192.168.6.2	26041	212.10.31.11	8080	目标地址	172.18.35.11	80
6	tcp	192.168.6.2	26040	212.10.31.11	8080	目标地址	172.18.35.11	80



## 5.2 通过VIP实现一对一的源NAT

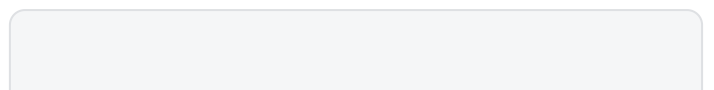
### 5.2.1 需求

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**



防火墙 / 虚拟IP / 虚拟IP

编辑映射关系

名称: VIP-Static\_1to1

公网接口: port1

类型: 静态NAT

公网IP地址范围: 212.10.31.2      212.10.31.3

内网IP地址或范围: 172.18.34.2      172.18.34.3

端口转发

OK    取消

```

1  define firewall vip
2  edit "VIP-Static_1to1"
3      set extintf "port1"
4      set extip 212.10.31.2
5      set mappedip 172.18.34.2-
6          172.18.34.3
7      set nat-source-vip enable
8  next
9  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

防火墙 / 策略 / 策略

编辑输出策略

源接口/区: Outside

源地址: all

目的接口/区: Inside

目的地址: VIP-Static\_1to1

时刻表: always

服务: ANY

动作: ACCEPT

记录允许流量

生成UDP反向策略

NAT

不使用 NAT

启用 NAT     动态IP地址池

启用地址映射表

如果只是想实现源地址的一对一映射, 此处动作可以设置为拒绝

防火墙 / 策略 / 策略

编辑输出策略

源接口/区: Inside

源地址: [多选...]

目的接口/区: Outside

目的地址: all

时刻表: always

服务: ANY

动作: ACCEPT

记录允许流量

生成UDP反向策略

NAT

不使用 NAT

启用 NAT     动态IP地址池

启用地址映射表

防火墙 / 策略 / 策略

创建   编辑   删除   移动到   复制   插入   冲突检查   有效性检查   进入批处理

[列设定]    基于接口查看    清单式查看

序号	策略ID	源	目的	源地址	目的地址	时刻表	服务	动作	状态	计数
1	2	Inside	Outside	host172.18.34.2 host172.18.34.3	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	0 / 0 B
2	8	Outside	Inside	all	VIP-Static_1to1	always	ANY	DENY	<input checked="" type="checkbox"/>	0 / 0 B

## 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