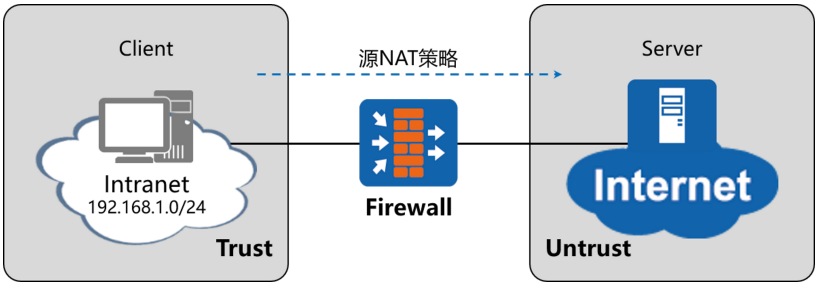
基于防火墙的NAT

一、防火墙NAT的基本概念

1、多个内部用户共享少量公网地址访问Internet时，可使用源NAT技术进行实现

2、源NAT技术只根据数据的源IP地址进行转换



二、源NAT的2种转换方式

1、不带端口转换的地址池方式【No-PAT】：

内部私网用户共享地址池中的IP地址，按照一个私网IP地址对应一个公网IP地址的方式进行转换；地址转换时不进行端口转换，地址池中IP的个数就是最多可同时上网的私网用户数；适用于某些服务需要使用特定的源端口，不允许进行源端口转换的场景

2、带端口转换的地址池方式【NAPT】：

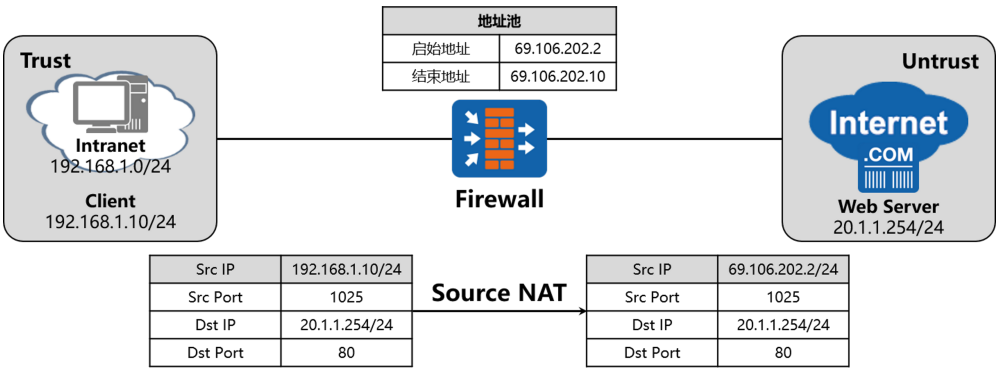
适用于私网用户较多的大中型网络环境，多个私网用户可以共同使用一个公网IP地址，根据端口区分不同用户，可支持同时上网的用户数量更多

源NAT转换方式	阐述	场景
NAT No-PAT	只转换数据的IP地址，不转换端口	需要上网的私网用户数量少，公网IP地址数量与同时上网的最大私网用户数量基本相同
NAPT	同时转换数据的IP地址和端口	公网IP地址数量少，需要上网的私网用户数量大

三、NAT No-PAT

1、NAT No-PAT亦可称之为【一对一地址转换】，仅对数据的源IP地址进行转换，而不转换端口号码

2、配置NAT No-PAT后，设备会为有实际流量的数据流建立Server-map表，用于存放私网IP地址与公网IP地址的映射关系。设备根据这种映射关系对报文的地址进行转换，然后进行转发



Src IP	192.168.1.10/24
Src Port	1025
Dst IP	20.1.1.254/24
Dst Port	80

Source NAT

Src IP	69.106.202.2/24
Src Port	1025
Dst IP	20.1.1.254/24
Dst Port	80

Server-map Table

Direction	Protocol	S-IP [New-S-IP]	D-IP	Zone
Obverse	Any	192.168.1.10 [69.106.202.2]	Any	-
Direction	Protocol	S-IP	D-IP [New-D-IP]	Zone
Reverse	Any	Any	69.106.202.2 [192.168.1.10]	-

Session Table

Protocol	S-IP:S-Port [New-S-IP:New-S-Port]	D-IP:D-Port
HTTP	192.168.1.10:1025 [69.106.202.2:1025]	20.1.1.254:80

3、当Host访问Web Server时，FW的处理过程如下：

3.1、FW收到Host发送的报文后，根据目的IP地址判断报文需要在Trust区域和Untrust区域之间流动，通过安全策略检查后继而查找NAT策略，发现需要对报文进行地址转换

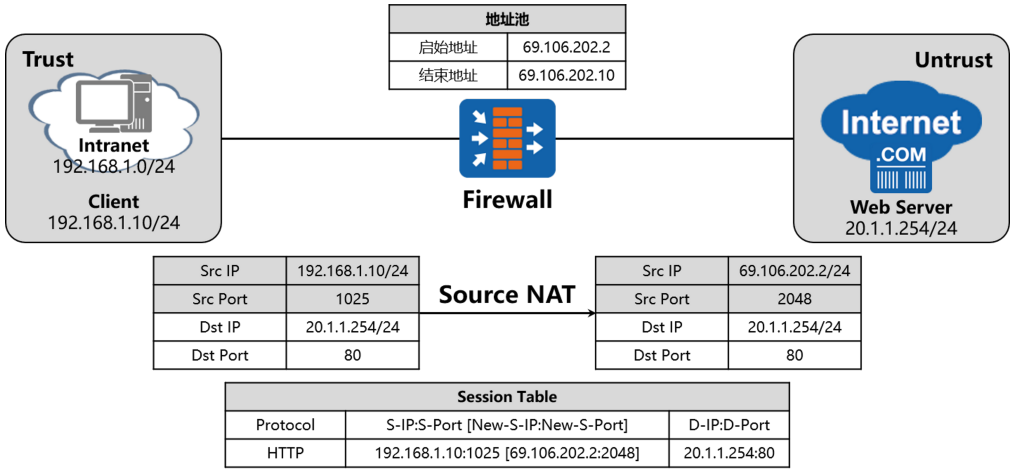
3.2、FW从NAT地址池中选择一个空闲的公网IP地址，替换报文的源IP地址，并建立Server-map表和会话表，然后将报文发送至Internet

3.3、FW收到Web Server响应Host的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的目的地址替换为Host的IP地址，然后将报文发送至Intranet

4、此方式下，公网地址和私网地址属于一对一转换。如果地址池中的地址已经全部分配出去，则剩余内网主机访问外网时不会进行NAT转换，直到地址池中有空闲地址时才会进行NAT转换

四、NAPT

1、NAPT属于【多对一的地址转换】，在转换过程中同时转换数据的源IP地址与端口号码



2、当Host访问Web Server时，FW的处理过程如下：

2.1、FW收到Host发送的报文后，根据目的IP地址判断报文需要在Trust区域和Untrust区域之间流动，通过安全策略检查后继而查找NAT策略，发现需要对报文进行地址转换

2.2、FW从NAT地址池中选择一个公网IP地址，替换报文的源IP地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至Internet

2.3、FW收到Web Server响应Host的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的目的地址替换为Host的IP地址，将报文的目的端口号替换为原始的端口号，然后将报文发送至Intranet

3、此方式下，由于地址转换的同时还进行端口的转换，可以实现多个私网用户共同使用一个公网IP地址上网，FW根据端口区分不同用户，所以可以支持同时上网的用户数量更多

五、公网用户访问私网内部服务器场景

1、通过NAT Server【服务器映射】功能，可以实现外部网络用户通过公网地址访问私网内部服务器的需求

2、NAT Server功能即将某个公网IP地址映射为服务器的私网IP地址

3、NAT Server提供了公网地址与私网地址的静态映射关系

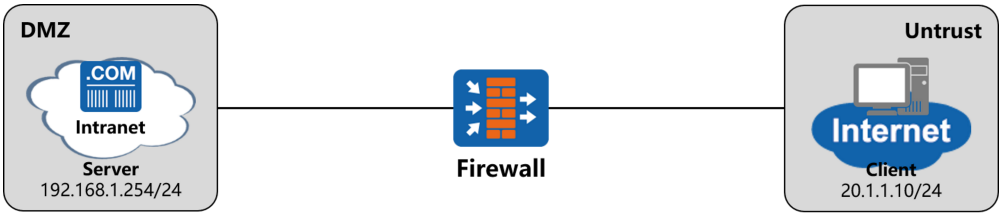
4、进行地址映射时，可选择是否允许端口转换

5、在使用NAT Server功能时，外网的用户向内部服务器主动发起访问请求，该用户的IP地址和端口号都是不确定的，唯一可以确定的是内部服务器的IP地址和所提供服务的端口号

6、配置NAT Server成功后，设备会自动生成Server-map表项，用于存放Globle地址与Inside地址的映射关系

7、设备根据这种映射关系对报文的地址进行转换并转发；每个生效的NAT Server都会生成正反方向两个静态的Server-map；该表项将一直存在除非静态映射的配置被删除

8、在FW上配置NAT Server，确定公网地址和私网地址的映射关系；配置完成后，FW将会自动生成Server-Map表项，用于存放公网地址和私网地址的映射关系



Src IP	20.1.1.10/24
Src Port	3535
Dst IP	192.168.1.254/24
Dst Port	80

NAT Server

Src IP	20.1.1.10/24
Src Port	3535
Dst IP	69.106.202.1/24
Dst Port	80

Server-map Table

Direction	Protocol	S-IP	D-IP:D-Port [New-D-IP:New-D-Port]
Obverse	TCP	Any	69.106.202.1:80 [192.168.1.254:80]

Session Table

Protocol	S-IP:S-Port	D-IP:D-Port [New-D-IP:New-D-Port]
HTTP	20.1.1.10:3535	69.106.202.1:80 [192.168.1.254:80]

9、当Client访问Server时，FW的处理过程如下：

9.1、FW收到Internet上用户访问69.106.202.1的报文的首包后，查找并匹配到Server-Map表项，将报文的目的IP地址转换为192.168.1.254

9.2、FW根据目的IP地址判断报文需要在Untrust区域和DMZ区域之间流动，通过域间安全策略检查后建立会话表，然后将报文发送至Intranet

9.3、FW收到Server响应Client的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的源地址替换为69.106.202.1，然后将报文发送至Internet

9.4、后续Client继续发送给Server的报文，FW都会直接根据会话表项的记录对其进行转换，而不会再去查找Server-map表项

10、FW在进行地址映射的过程中还可以选择是否允许端口转换，是否允许服务器采用公网地址上网，以满足不同场景的需求

六、基于防火墙的NAT及NAT Server的配置

详细配置见实验手册