

HCIE-Security 备考指南

NAT 策略



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security NAT 策略需要掌握的知识点.....	1
NAT 简介.....	1
NAT 处理流程	2
源 NAT	4
服务器映射	6
目的 NAT	8
NAT ALG.....	9
NAT 应用场景	11
NAT FAQ.....	15
使用限制和注意事项.....	18
配置源 NAT	19
举例：私网用户通过地址池方式的源 NAT 策略访问 Internet.....	22
配置服务器静态映射	28
举例：外部网络用户通过服务器静态映射功能访问内部服务器（双向 NAT）	34
配置服务器负载均衡	41
举例：服务器负载均衡.....	44
配置目的 NAT	49
配置 NAT ALG	51
处理 NAT 故障	53
配置了源 NAT 策略后，内部网络无法访问 Internet	53
现象描述.....	54
定位思路.....	54
处理步骤.....	54
配置了服务器静态映射后，外部网络无法访问内部服务器	56
现象描述.....	57
定位思路.....	57
处理步骤.....	58
HCIE-Security 模拟面试问题及面试建议	60

HCIE-Security NAT 策略需要掌握的知识点

- 描述 NAT 技术原理
- 掌握 NAT 配置命令的基本功能
- 配置上网、服务发布
- 配置双出口场景 NAT
- 配置服务器负载均衡
- NAT 故障排除

NAT 简介

定义和目的

NAT (Network Address Translation) 是一种地址转换技术，可以将 IPv4 报文头中的地址转换为另一个地址。通常情况下，利用 NAT 技术将 IPv4 报文头中的私网地址转换为公网地址，可以实现位于私网的多个用户使用少量的公网地址同时访问 Internet。因此，NAT 技术常用来解决随着 Internet 规模的日益扩大而带来的 IPv4 公网地址短缺的问题。

说明：

NGFW 还支持 IPv6 与 IPv4 的地址转换，以实现 IPv4 网络与 IPv6 网络之间能够正常通信，详细请参见 [NAT64](#)。

分类

根据应用场景的不同，NAT 可以分为以下三类：

- 源 NAT (Source NAT)：用来使多个私网用户能够同时访问 Internet。
- 服务器映射：用来使外网用户能够访问私网服务器。
- 目的 NAT (Destination NAT)：用来使手机上网的业务流量送往正确的 WAP 网关。

NAT 更详细的分类及特点，如[表 1](#)所示。

表 1 NAT 分类				
分类		转换内容	是否转换端口	特点
源 NAT	地址池方式	源 IP 地址	可选	采用地址池中的公网地址为私网

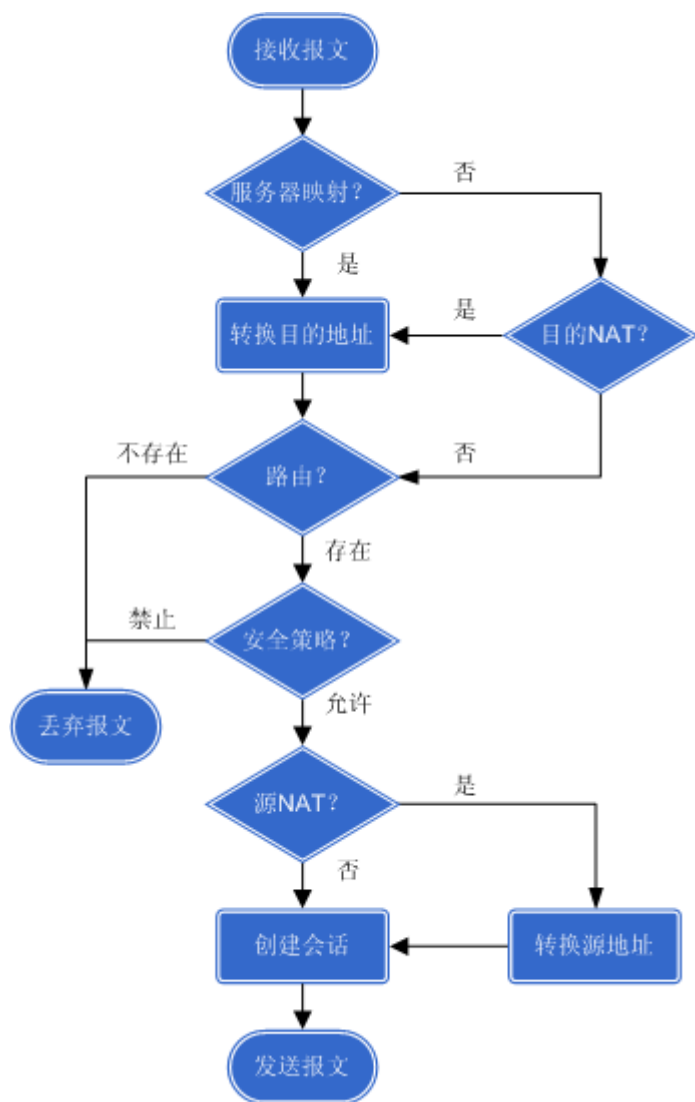
表 1 NAT 分类				
分类		转换内容	是否转换端口	特点
				用户进行地址转换，适合大量的私网用户访问 Internet 的场景。
	出接口地址方式（Easy IP）	源 IP 地址	是	内网主机直接借用公网接口的 IP 地址访问 Internet，特别适用于公网接口 IP 地址是动态获取的情况。
服务器映射	静态映射（NAT Server）	目的 IP 地址	可选	公网地址和私网地址一对一进行映射，用在公网用户访问私网内部服务器的场景。
	服务器负载均衡	目的 IP 地址	可选	用在多个内网服务器提供相同的服务，对外虚拟出一个服务器，对用户的访问流量进行负载均衡的场景。
目的 NAT		目的 IP 地址	可选	主要用在转换手机用户 WAP 网关地址，使手机用户可以正常上网的场景。

NAT 处理流程

了解 NAT 的处理流程，有助于您理解和配置 NAT 功能。

除自身的配置之外，NAT 能否正常工作也受路由、安全策略等功能影响，从整体上掌握设备对 NAT 的处理流程，可以为后续配置和排错提供帮助。NAT 的处理流程如[图 1](#)所示。

图 1 NAT 处理流程示意图



如上图所示，NAT 处理流程简述如下：

1. NGFW 收到报文后，查找服务器映射生成的 Server-Map 表，如果报文匹配到 Server-Map 表，则根据表项转换报文的目的地址，然后进行步骤 3 处理；如果报文没有匹配到 Server-Map 表，则进行步骤 2 处理。
2. 查找目的 NAT，如果报文符合目的 NAT 的匹配条件，则转换报文的目的地址后进行路由处理；如果报文不符合目的 NAT 的匹配条件，则直接进行路由处理。
3. 根据报文当前的信息查找路由（包括策略路由），如果找到路由，则进入步骤 4 处理；如果没有找到路由，则丢弃报文。
4. 查找安全策略，如果安全策略允许报文通过，则进行源 NAT 处理；如果安全策略不允许报文通过，则丢弃报文。

5. 查找源 NAT，如果报文符合源 NAT 的匹配条件，则转换报文的源地址，然后创建会话；如果报文不符合源 NAT 的匹配条件，则直接创建会话。
6. NGFW 发送报文。

了解 NAT 在报文转发流程中大致位置，有利于您在配置设备时合理安排数据，以及业务出现故障时定位故障产生的原因。例如，安全策略的处理顺序位于服务器映射和源 NAT 之间，因此在安全策略的规则中指定源/目的地址信息时，目的地址应为经过服务器映射处理后的服务器私网地址，源地址应为源 NAT 转换前的私网地址。

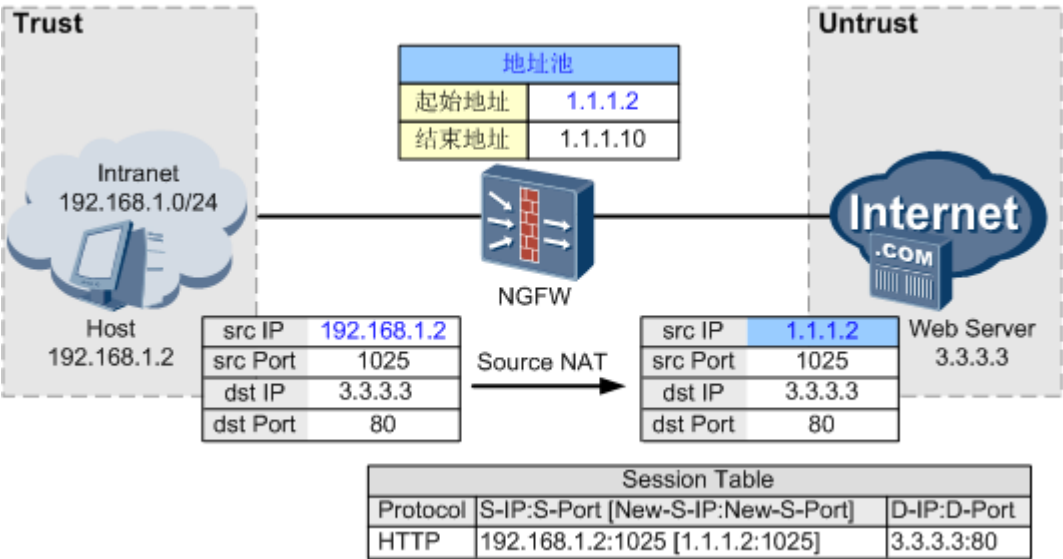
源 NAT

源 NAT 指的是对报文中的源地址进行转换，不同的应用场景下实现源 NAT 的方式也不相同。

不带端口转换的地址池方式

不带端口转换的地址池方式通过配置 NAT 地址池来实现，NAT 地址池中可以包含多个公网地址。转换时只转换地址，不转换端口，实现私网地址到公网地址一对一的转换。如图 1 所示。

图 1 源 NAT（不带端口转换的地址池方式）工作原理示意图



如图 1 所示，当 Host 访问 Web Server 时，NGFW 的处理过程如下：

1. NGFW 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。

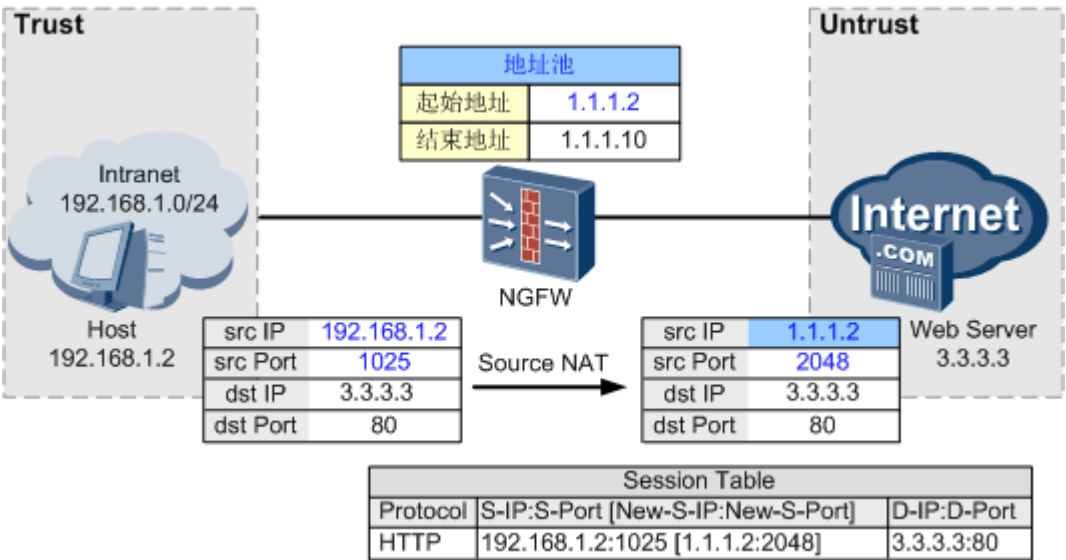
2. NGFW 从 NAT 地址池中选择一个空闲的公网 IP 地址，替换报文的源 IP 地址，并建立会话表，然后将报文发送至 Internet。
3. NGFW 收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的目的地地址替换为 Host 的 IP 地址，然后将报文发送至 Intranet。

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。

带端口转换的地址池方式

带端口转换的地址池方式通过配置 NAT 地址池来实现，NAT 地址池中可以包含一个或多个公网地址。转换时同时转换地址和端口，即可实现多个私网地址共用一个或多个公网地址的需求，如 [图 2](#) 所示。

图 2 源 NAT（带端口转换的地址池方式）工作原理示意图



如 [图 2](#) 所示，当 Host 访问 Web Server 时，NGFW 的处理过程如下：

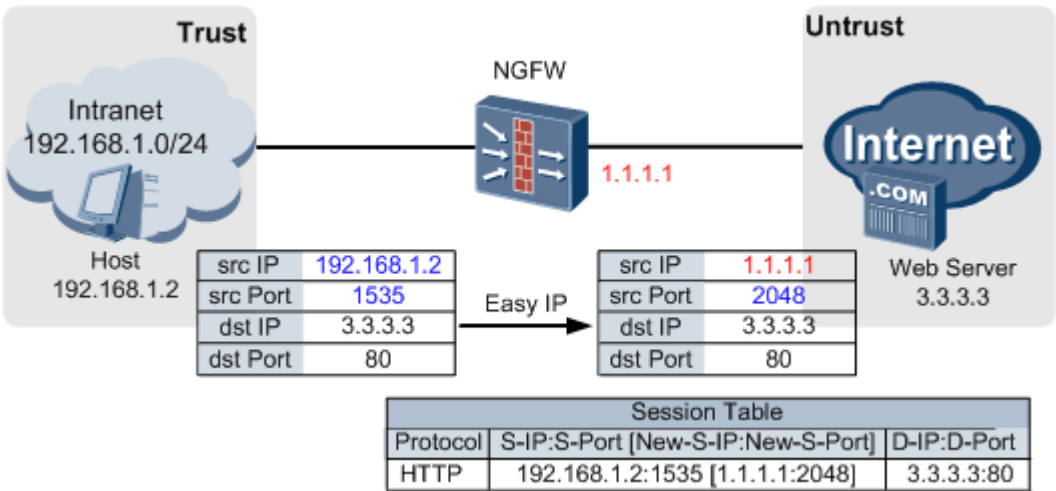
1. NGFW 收到 Host 发送的报文后，根据目的 IP 地址判断报文需要在 Trust 区域和 Untrust 区域之间流动，通过安全策略检查后继而查找 NAT 策略，发现需要对报文进行地址转换。
2. NGFW 从 NAT 地址池中选择一个公网 IP 地址，替换报文的源 IP 地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至 Internet。
3. NGFW 收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的目的地地址替换为 Host 的 IP 地址，将报文的端口号替换为原始的端口号，然后将报文发送至 Intranet。

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，NGFW 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。

出接口地址方式

出接口地址方式也称为 Easy IP，即直接使用接口的公网地址作为转换后的地址，不需要配置 NAT 地址池。转换时同时转换地址和端口，即可实现多个私网地址共用外网接口的公网地址的需求，如图 3 所示。

图 3 Easy IP 工作原理示意图



如图 3 所示，当 Host 访问 Web Server 时，NGFW 的处理过程如下：

1. NGFW 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. NGFW 使用与 Internet 连接的接口的公网 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。
3. NGFW 收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 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。

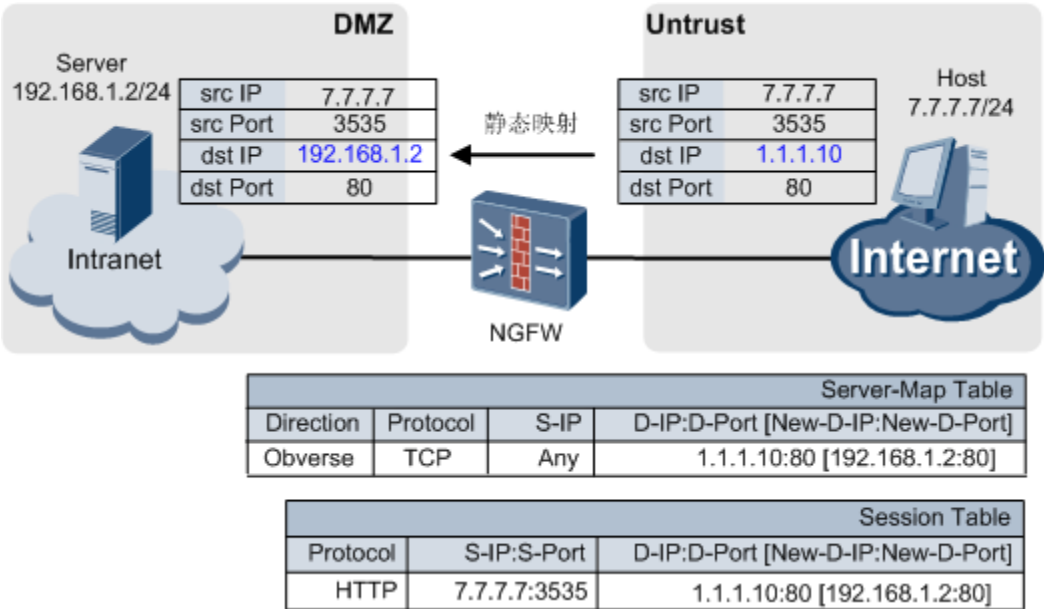
服务器映射

服务器映射分为静态映射和服务器负载均衡。静态映射属于一对一的映射，一个公网地址对应一个内网服务器；服务器负载均衡属于一对多映射，用来将外网用户访问内网服务器的流量按照一定的算法分配到特定的内网服务器上。

静态映射

静态映射也称 NAT Server，是一种转换报文目的 IP 地址的方式，它提供了公网地址和私网地址的映射关系，将报文中的公网地址转换为与之对应的私网地址。

图 1 静态映射工作原理示意图



在 NGFW 上配置静态映射，确定公网地址和私网地址的映射关系。配置完成后，NGFW 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，该表项将一直存在除非静态映射的配置被删除。典型的 Server-Map 表如下所示：

```
<NGFW> display firewall server-map
server-map item(s)

-----

Nat Server, any -> 1.1.1.10:80[192.168.1.2:80], Zone: ---
Protocol: tcp(Appro: http), Left-Time: --:--:--, Addr-Pool: ---
VPN: public -> public
```

如图 1 所示，当 Host 访问 Server 时，NGFW 的处理过程如下：

1. NGFW 收到 Internet 上用户访问 1.1.1.10 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 192.168.1.2。
2. NGFW 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。

3. NGFW 收到 Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的源地址替换为 1.1.1.10，然后将报文发送至 Internet。
4. 后续 Host 继续发送给 Server 的报文，NGFW 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。

另外，NGFW 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。

服务器负载均衡

服务器负载均衡就是 NGFW 按照事先配置的负载均衡算法，将访问同一个 IP 地址的用户流量分配到不同的服务器上。

配置负载均衡后，在访问用户看来，他们访问的是同一个服务器，而实际上 NGFW 将他们的请求分送给了不同的服务器进行处理。这样可以分别利用各个服务器的处理能力，达到流量分担的目的，保障了服务器的可用性，得到最佳的网络扩展性。

NGFW 支持简单轮询、加权轮询和源地址哈希三种算法：

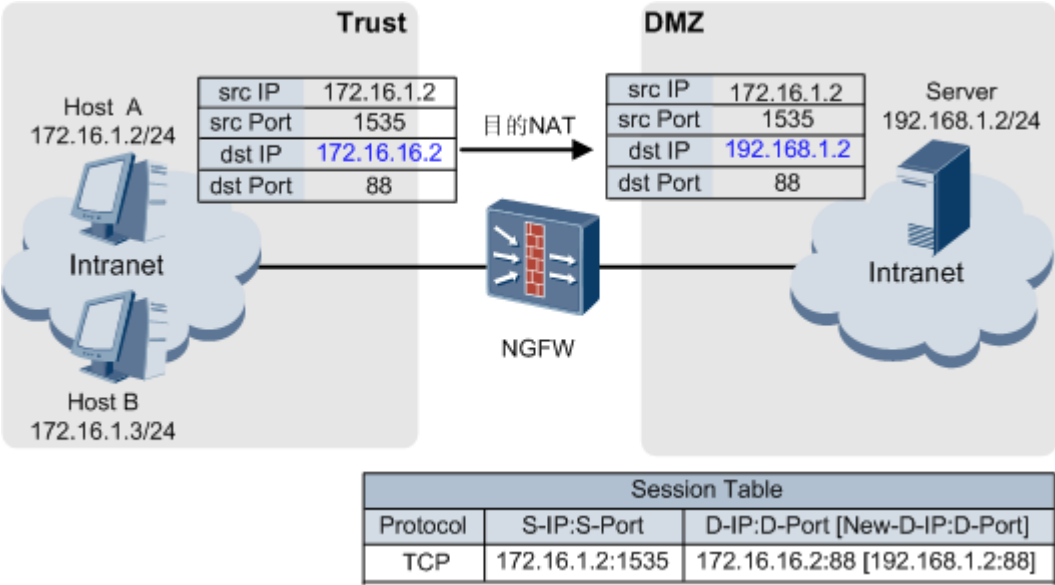
- 简单轮询：根据流量的带宽均分到各个内网服务器上，使每台服务器的负载相同。
- 加权轮询：根据每台内网服务器的权值比例（权重）来分配流量，使每台服务器的负载比例与权值比例相同。新增内网服务器时，重新计算权值比例，按新的权值比例来分配流量。
- 源地址哈希：根据流量的源地址进行 Hash 计算，保证相同源地址的流量由同一台内网服务器处理。

NGFW 还支持周期性探测真实服务器，即向真实服务器发送健康性检测报文。如果能收到真实服务器回应的报文，说明真实服务器可用；如果多次收不到服务器的回应报文，NGFW 将禁止使用该真实服务器，将流量按配置好的策略分配到其他真实服务器上。

目的 NAT

目的 NAT 是一种转换报文目的 IP 地址的方式，将符合特定条件的报文的目的地址以及目的端口转换为指定的地址及端口。其中特定条件包含“安全区域”和“ACL”两项，即设备只对来自某一安全区域且命中特定 ACL 的报文进行目的 NAT。

图 1 目的 NAT 工作原理示意图



如图 1 所示，当 Host A 访问 Server 时，NGFW 的处理过程如下：

1. NGFW 收到 Host A 发送的报文后，根据 Trust 安全区域内配置的目的 NAT，将报文的目的 IP 地址由 172.16.16.2 转换为 192.168.1.2。
2. NGFW 根据转换后的目的 IP 地址判断报文需要在 Trust 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 Server。
3. NGFW 收到 Server 响应 Host A 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的源地址替换为 172.16.16.2，然后将报文发送至 Host A。

NAT ALG

介绍 NAT ALG 功能的实现原理。

通常情况下，NAT 只对报文中 IP 头部的地址信息和 TCP/UDP 头部的端口信息进行转换，不关注报文载荷的信息。但是对于一些特殊的协议（如 FTP 协议），其报文载荷中也携带了地址或端口信息，而报文载荷中的地址或端口信息往往是由通信的双方动态协商生产的，管理员并不能为其提前配置好相应的 NAT 规则。如果提供 NAT 功能的设备不能识别并转换这些信息，将会影响到这些协议的正常使用。

NGFW 提供 NAT ALG (Application Level Gateway) 功能，可以对报文的载荷字段进行解析，识别并转换其中包含的重要信息，保证类似 FTP 的多通道协议可以顺利的进行地址转换而不影响其正常使用。

下面以 FTP（File Transfer Protocol）协议为例，简要描述其工作原理。

FTP 协议的 NAT ALG 处理

FTP 协议是一个典型的多通道协议，在其工作过程中，FTP Client 和 FTP Server 之间将会建立两条连接（也称为通道）：控制连接和数据连接。控制连接用来传输 FTP 指令和参数，数据连接用来传输数据。

FTP 协议包括两种工作模式：主动模式和被动模式。主动模式中，FTP Server 主动向 FTP Client 发起数据连接；被动模式中，FTP Server 被动接收 FTP Client 发起的数据连接。无论是主动模式还是被动模式，在控制连接交互报文的载荷中，都包含用于建立数据连接的 IP 地址和端口号信息。

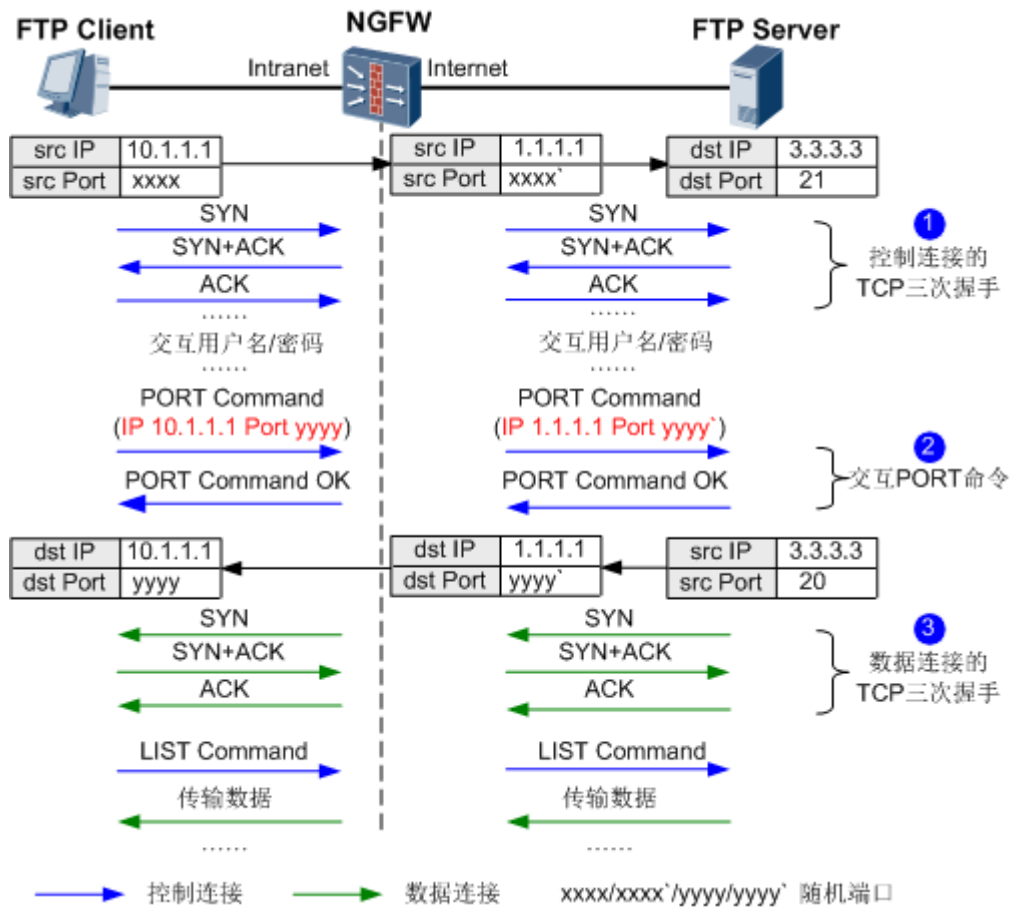
如果在 FTP Client 和 FTP Server 之间部署了 NAT 设备，这就要求 NAT 设备必须能够识别出控制连接中包含的 IP 地址和端口号并进行处理，否则数据连接无法成功建立，FTP 协议不能正常工作。

下面以 FTP 协议工作在主动模式为例，介绍 NAT ALG 功能对 FTP 协议的处理过程。

如[图 1](#)所示，FTP Client 位于私有网络，FTP Server 位于公共网络。NGFW 对 FTP 协议的报文处理过程如下：

1. FTP Client 通过源 NAT 地址转换后可以访问 FTP Server，与 FTP Server 完成 FTP 控制连接的 TCP 三次握手，并交付用户名和密码信息。
2. NGFW 收到 FTP Client 发送的 PORT 命令报文后，将报文载荷字段中携带的私网地址和端口替换为公网地址和新的端口，然后发送至 FTP Server。
3. NGFW 收到 FTP Server 请求建立数据连接的报文后，替换报文的目地址和目的端口为原始的地址和端口，然后发送至 FTP Client。由此保证数据连接可以成功建立，FTP 协议正常工作。

图 1 NAT ALG 工作原理示意图一



除 FTP 协议外，NGFW 还支持对 DNS、H. 323、ICQ、ILS、MGCP、MMS、MSN、NETBIOS、PPTP、QQ、RTSP、SIP 和 SQLNET 协议提供 NAT ALG 功能。

NAT ALG 与 ASPF 的关系

差异点：

- 开启 ASPF 功能的目的是识别多通道协议，并自动为其开放相应的安全策略。
- 开启 NAT ALG 功能的目的是识别多通道协议，并自动转换报文载荷中的 IP 地址和端口信息。

共同点：二者使用相同的配置。开启其中一个功能，另一功能同时生效。

NAT 应用场景

介绍常见的几种 NAT 应用场景。

- [私网用户访问 Internet](#)

通过源 NAT 策略对 IPv4 报文头中的源地址进行转换，可以实现私网用户通过公网 IP 地址访问 Internet 的目的。

- [公网用户访问私网内部服务器](#)

通过服务器映射功能，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。

- [私网用户使用公网 IP 地址访问私网内部服务器](#)

源 NAT 和服务器映射功能结合使用，可以实现私网用户使用公网地址访问私网内部服务器的需求。

- [移动终端访问无线网络](#)

通过目的 NAT 功能，使设备将终端发往错误 WAP 网关地址的报文自动转发到正确的 WAP 网关。

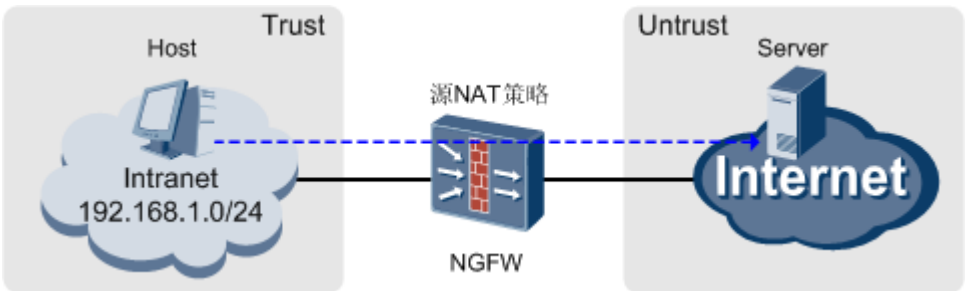
私网用户访问 Internet

通过源 NAT 策略对 IPv4 报文头中的源地址进行转换，可以实现私网用户通过公网 IP 地址访问 Internet 的目的。

在学校、公司中经常会有多个用户共享少量公网地址访问 Internet 的需求，通常情况下可以使用源 NAT 技术来实现。

如图 1 所示 NGFW 部署在网络边界处，通过部署源 NAT 策略，可以将私有网络用户访问 Internet 的报文的源地址转换为公网地址，从而实现私网用户接入 Internet 的目的。

图 1 源 NAT 策略示意图



从实际使用的角度来还可以将源 NAT 分为以下几种应用场景：

表 1 源 NAT 分类	
分类	场景
不带端口转换的地址池方式	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

表 1 源 NAT 分类	
分类	场景
	IP 地址的方式进行转换。地址转换的同时不进行端口转换，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。
带端口转换的地址池方式	一般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，所以可以支持同时上网的用户数量更多。
出接口地址方式（Easy IP）	直接使用出接口的 IP 地址作为转换后的公网地址，适用于接口动态获得公网地址的网络环境。

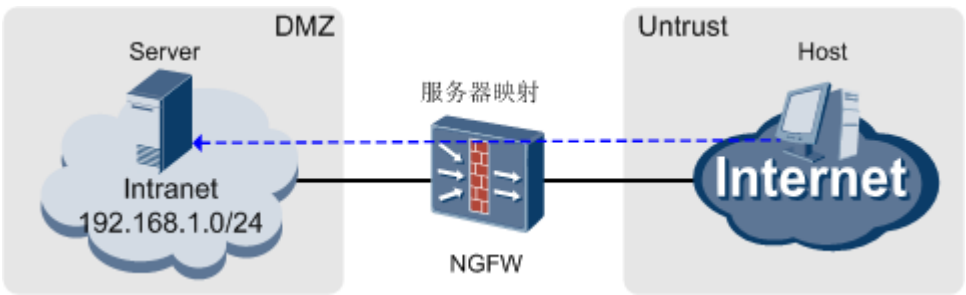
公网用户访问私网内部服务器

通过服务器映射功能，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。

学校或公司会提供 Web、FTP 等服务供公网中的用户访问，服务器一般部署在私网，通过服务器映射功能使公网用户可以访问到这些位于私网的服务器。

如图 1 所示，NGFW 提供服务器映射功能，将某个公网 IP 地址映射为服务器的私网 IP 地址，相当于为外部网络提供一个“接口”，使外部网络的用户可以通过该公网 IP 地址来访问私网内部服务器。

图 1 外部网络用户访问私网内部服务器示意图



从实际使用的角度来还可以将服务器映射分为以下两种应用场景：

表 1 服务器映射分类	
分类	场景
静态映射	适用一个服务器对应一个公网 IP 地址的场景。
服务器负载均衡	适用于多个服务器对外提供相同的服务，使用同一个公网 IP 地址，共同分担用户访问流量的场景。

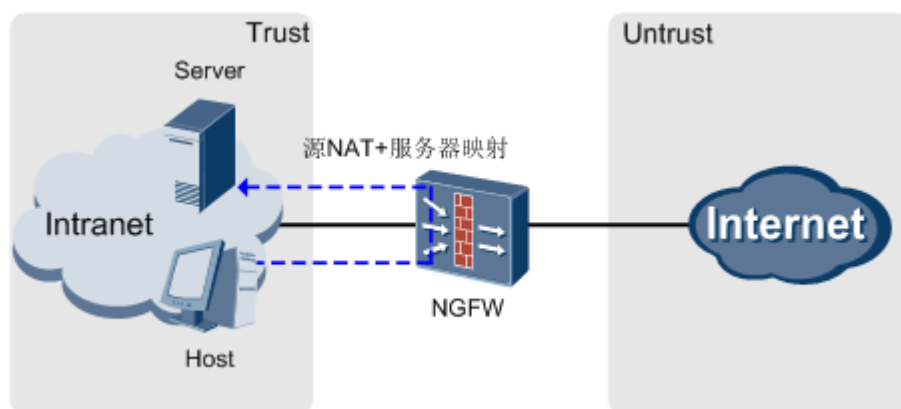
私网用户使用公网 IP 地址访问私网内部服务器

源 NAT 和服务器映射功能结合使用，可以实现私网用户使用公网地址访问私网内部服务器的需求。

私网用户与内部服务器都位于内网时，如果私网用户也希望像公网用户一样，使用公网地址来访问内部服务器，此时可以通过源 NAT 和服务器映射配合工作来实现。

如图 1 所示，NGFW 提供源 NAT 和服务器映射功能，当私网用户使用公网地址访问内部服务器时，将报文的源和目的地址都进行转换。私网用户与内部服务器之间交互的报文都经由 NGFW 处理。

图 1 私网用户使用公网地址访问私网内部服务器示意图



移动终端访问无线网络

通过目的 NAT 功能，使设备将终端发往错误 WAP 网关地址的报文自动转发到正确的 WAP 网关。

手机用户需要通过登录 WAP（Wireless Application Protocol）网关来实现上网的功能。目前，大量用户直接从国外购买手机使用，这些手机出厂时，缺省设置的 WAP 网关地址与本国 WAP 网关地址不符，且无法自行修改，从而导致用户不能移动上网。

为解决这一问题，无线网络中，在 WAP 网关与用户之间部署 NGFW。通过在 NGFW 上配置目的 NAT 功能，使这部分手机用户能够正常获取网络资源。

如图 1 所示，当手机用户上网时，NGFW 将数据报文的目的 IP 地址转换为已配置好的 WAP 网关的 IP 地址，并送往 WAP 网关。

图 1 手机用户上网目的 NAT 组网图



NAT FAQ

NAT 策略常见疑问的回答。

NGFW 是否支持透明模式下（业务接口工作在交换模式）的源 NAT 的配置？

支持，但只支持采用地址池中的地址做为转换后的源地址，不支持采用出接口地址做为转换后的源地址。

如果 NAT 策略中配置了多条策略，报文的匹配原则是什么？

如果 NAT 策略中配置了多条策略，设备将会按照策略的显示顺序从上到下依次匹配。只要匹配到一条策略就不再继续匹配剩下的策略。

什么情况下需要配置黑洞路由？

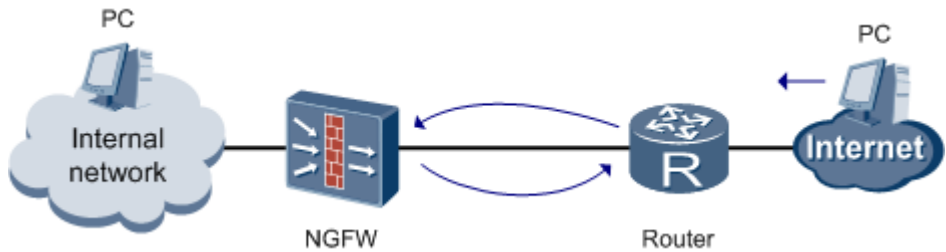
当 NAT 地址池地址与设备连接外网接口的地址在不同的网段时，需要配置黑洞路由。

黑洞路由有以下两方面的作用：

- 避免 NGFW 与上行路由设备之间产生路由环路

[图 1](#) 如所示，正常情况下，内部网络中的用户主动访问外部网络，并使用地址池地址作为转换后的公网地址。当外部网络中的用户主动访问地址池中的地址时，NGFW 收到报文后，由于没有匹配到会话表，将会根据路由表将报文转发至 Router。Router 收到报文后会继续转发给 NGFW，由此报文将在 NGFW 和 Router 之间循环转发，直到 TTL 为 0 后被丢弃。当外部网络中有大量的恶意用户主动访问地址池地址时，将会影响 NGFW 和 Router 的处理性能。

图 1 路由环路示意图



为了避免上述情况，在 NGFW 上配置目的地址为地址池地址的 32 位黑洞路由，外网主动访问地址池地址的报文匹配到黑洞路由后直接被丢弃，不会在 NGFW 和 Router 之间循环转发。

对于服务器静态映射来说，也需要在配置目的地址为公网地址的 32 位黑洞路由，使外网访问公网地址但没有匹配到 Server-Map 的报文匹配到黑洞路由后直接被丢弃，不会在 NGFW 和上行路由设备之间循环转发。

- 引入到动态协议中并发布出去，使上行路由设备学习到去往地址池地址的路由

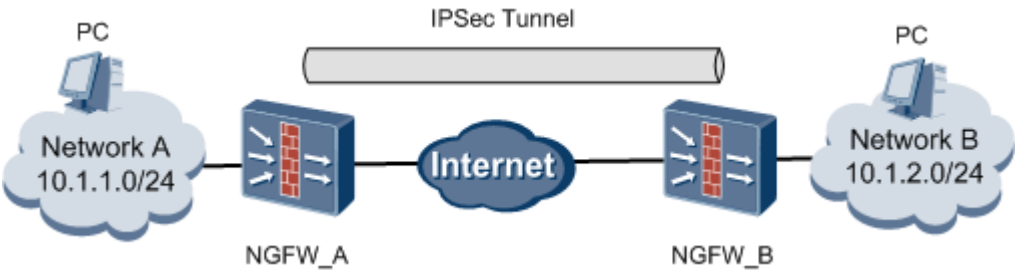
当 NGFW 和上行路由设备上开启动态路由协议（如 OSPF）时，为了简化配置，希望上行路由设备可以自动学习到去往地址池地址的路由，但是在动态路由协议中无法直接引用地址池地址。

为了实现上述需求，可以配置目的地址为地址池地址的 32 位黑洞路由，引入到动态协议中并发布出去，使上行路由设备学习到去往地址池地址的路由。

配置 NAT 和 VPN 功能同时工作时有什么注意事项？

NAT 和 VPN 功能同时工作时，请您精确定义 NAT 策略的匹配条件，确保 NAT 功能不会将原本是需要进行 VPN 封装的数据流做地址转换。

图 2 NAT 和 IPSec VPN 同时工作的示意图



以 NAT 和 IPSec VPN 同时工作为例，如图 2 所示，Network A 和 Network B 通过 NGFW 连接 Internet，同时 Network A 和 Network B 中的 PC 通过 IPSec 隧道相互访问。

在这种情况下，Network A 和 Network B 访问 Internet 的数据流都要进行 NAT 转换，而经过 IPSec 隧道封装的数据流不需要进行 NAT 转换，故要在配置 NAT 策略时进行区分。如图 3 所示，以 NGFW_A 的配置为例：

图 3 NAT 策略区分

<input type="checkbox"/> 名称	源安全区域	目的安全区域/出接口	源地址	目的地址	动作	转换后源地址
<input type="checkbox"/> rule1	trust	untrust/---	172.16.1.0/24	172.16.2.0/24		
<input type="checkbox"/> rule2	trust	untrust/---	172.16.1.0/24	any		addressgroup1

同理，在 NGFW_B 上配置 NAT 策略时也需要进行区分，与 NGFW_A 上的配置不同之处在于源地址/目的地址不同。

NAT 地址池中的地址是否必须为连续的地址？

否。

NAT 地址池是由“起始地址”和“结束地址”划定的一段 IP 地址范围，使用排除地址功能可以排除这个 IP 地址范围内某些特殊的 IP 地址。因此 NAT 地址池中的地址不一定是连续的地址。

另外，“起始地址”和“结束地址”也可以相同，此时 NAT 地址池中只有一个地址。

配置源 NAT 策略时，安全策略中指定的源地址是转换前的地址还是转换后的地址？

转换前的地址。

设备对报文进行地址转换时，先查找域间的安全策略，只有通过安全策略检查，并且命中了域间 NAT 策略中定义的匹配条件的报文才会进行地址转换。因此域间安全策略中指定的源地址为转换前的地址，即私网地址。

配置服务器映射时，安全策略中指定的目的地址是转换前的地址还是转换后的地址？

转换后的地址。

设备收到匹配上 Server-Map 表的报文后，先转换报文的目的地址，然后再检查安全策略，因此安全策略中指定的源地址为转换后的地址，即私网地址。

如何查看源 NAT 策略对报文进行地址转换的次数？

在“源 NAT 策略列表”中，“命中次数”列的数字即表示源 NAT 策略对报文进行地址转换的次数。

是否可以将设备接口的 IP 地址配置为 NAT 地址池中的地址？

可以。

是否可以将地址池中的地址配置为服务器静态映射的公网地址？

可以。

内部网络的用户如何通过公网地址访问位于同一安全区域内同一网段的内部服务器？

首先配置一条源 NAT 策略，其源安全区域和目的安全区域均为用户和内部服务器所在的安全区域，将内网用户的源 IP 地址转换为公网 IP 地址。然后再配置一条服务器静态映射策略，将去往服务器公网地址的报文目的 IP 地址转换为私网地址。

设备在关闭状态检测功能后是否还支持地址转换功能？

关闭状态检查功能后，设备可以支持地址转换功能。

使用限制和注意事项

配置 NAT 之前请先阅读使用限制和注意事项。

使用限制

直接将设备接口的地址配置为服务器静态映射的公网地址后，无法通过该接口的地址使用 Web 方式或 Telnet 方式对设备进行管理，也无法对设备进行 Ping 探测。

如果在实际应用中确实需要将设备接口的地址配置为服务器静态映射的公网地址，又需要通过该接口的地址对设备进行远程管理，您可以在配置服务器静态映射时选择允许端口转换，并配置协议和端口号，以缩小地址和端口转换的范围，从而避免与访问设备本身的需求相冲突。

注意事项

- 当 NAT 地址池地址与 NGFW 连接公网接口的地址在不同的网段时，需要配置目的地址为 NAT 地址池地址的黑洞路由，避免 NGFW 与上行路由设备之间产生路由环路。
- 当 NAT 与 VPN 功能同时工作时，请精确定义 NAT 策略的匹配条件，确保 NAT 功能不会将原本是需要进行 VPN 封装的数据流做地址转换。

- 配置服务器静态映射时，如果内网服务器的私网端口和其对外发布的公网端口同时使用了非知名端口，则需要配置端口映射功能，使 NGFW 可以将这些访问非知名端口的报文识别为知名服务的报文。

配置源 NAT

源 NAT 是指对发起连接的 IP 报文头中的源地址进行转换，通常用于实现内部用户访问外部网络的目的。

背景信息

源 NAT 将私网地址转换为公网地址有两种方式：

- 地址池方式：如果目前有多个公网地址可以使用，一般采用地址池方式。此方式需要创建 NAT 地址池以限定可使用的公网地址范围。
- 出接口地址方式（Easy IP）：如果目前只有设备的公网接口上的公网地址可用，一般采用出接口地址方式。此方式可以让内网主机直接借用公网接口的 IP 地址访问 Internet，特别适用于公网接口 IP 地址是动态获取的情况。

操作步骤

1. 可选：配置 NAT 地址池。当采用地址池方式进行源地址转换时需要配置。

- a. 在系统视图下创建 NAT 地址池并进入 NAT 地址池视图。

```
nat address-group address-group-name
```

NAT 地址池创建完成后，可以使用 **description** *description* 命令对该地址池进行描述，帮助管理员记忆该 NAT 地址池的用途。

- b. 配置 NAT 地址池中包含的地址段。

```
section [section-id | section-name] start-address end-address
```

一个地址池只支持配置一个地址段。也支持将地址池配置为仅包含单个 IP 地址，以实现内部主机固定转换为特定的公网 IP 地址。

地址段配置完成后，可以使用 **exclude-ip** *ipv4-address1* [**to** *ipv4-address2* | **mask** { *mask-address* | *mask-length* }] 命令剔除地址池中某些特殊的 IP 地址。

- c. 配置地址池的转换模式。

```
nat-mode { pat | no-pat }
```

pat 表示地址转换的同时进行端口的转换，**no-pat** 表示地址转换的同时不进行端口的转换，允许端口转换才可以使多个内网主机同时使用同一个公网 IP 地址访问 Internet。

如果不允许端口转换，私网地址和公网地址将进行一对一的转换。当地址池中的地址已经全部分配出去，剩余私网地址将不会进行 NAT 转换，直到有其他主机释放公网 IP 地址。

缺省情况下，NAT 地址的转换模式为 **pat** 模式，该模式下可以使用 exclude-port *port1* [*to port2*] 命令剔除地址池中某些特殊的端口，端口取值范围为 2048~65535。

- d. **可选：**配置设备发送 NAT 地址池中地址的免费 ARP。

如果用户是先配置 NAT 地址池，后配置公网接口地址，且公网接口地址与 NAT 地址池中地址在同一网段，则需要完成该步骤手动配置设备发送 NAT 地址池中地址的免费 ARP；

如果用户是先配置公网接口地址，后配置 NAT 地址池，且 NAT 地址池中地址与公网接口地址在同一网段，设备会自动发送 NAT 地址池中地址的免费 ARP，用户不需要配置该步骤。

1. 在系统视图下进入公网接口的接口视图。

```
interface interface-type interface-number
```

2. 配置设备发送 NAT 地址池中地址的免费 ARP。

```
nat arp-gratuitous send
```

2. 在系统视图下进入 NAT 策略视图。

```
nat-policy
```

3. 在 NAT 策略视图下创建 NAT 规则并进入 NAT 规则视图。如果创建了多条 NAT 规则，设备会从上到下依次进行匹配。如果流量匹配了某个 NAT 规则，将不再进行下一个规则的匹配。

```
rule name rule-name
```

NAT 规则创建完成后，可以使用 **description** *description* 命令对该规则进行描述，帮助管理员记忆该规则的用途。

4. 配置源 NAT 规则的匹配条件。

在匹配流量时各种匹配条件均为可选配置，缺省情况下为“any”。如果配置，则满足所配置条件的流量才会匹配成功。如果不配置，相当于不对该匹配条件进行要求。

- 配置需匹配流量的源 IP 地址。

```
source-address { address-set address-set-name <1-6> | ipv4-address [ ipv4-mask-length | mask mask-address ] | ipv6-address ipv6-prefix-length | range { ipv4-start-address ipv4-end-address | ipv6-start-address ipv6-end-address } | mac-address <1-6> | any }
```

- 配置需匹配流量的目的地址。

```
destination-address { address-set address-set-name <1-6> | ipv4-address [ ipv4-mask-length | mask mask-address ] | ipv6-address ipv6-prefix-length | range { ipv4-start-address ipv4-end-address | ipv6-start-address ipv6-end-address } | mac-address <1-6> | any }
```



说明：

当使用 MAC 地址作为策略匹配条件时，需注意：

- 如果 NGFW 与内网之间直连或通过二层交换机相连，可以直接以 MAC 地址作为匹配条件。
- 如果 NGFW 与内网之间通过三层网络设备相连，首先需要配置 NGFW 的跨三层 MAC 识别功能，再以 MAC 地址作为匹配条件。

- 配置流量的源安全区域，通常为内部网络所在安全区域。

```
source-zone { zone-name <1-6> | any }
```

- 配置流量的目的安全区域或出接口。目的安全区域与出接口互斥，配置时只能选择其中的一种。
 - 配置流量的目的安全区域，通常为外部网络所在安全区域。

```
destination-zone zone-name
```

- 配置流量的出接口。

`egress-interface interface-type interface-number`

- 配置需匹配流量的服务集。

`service { service-name <1-6> | any }`

5. 配置 NAT 规则的动作。

`action { nat { { address-group address-group name } | easy-ip } | no-nat }`

nat 表示对该数据流进行 NAT 转换，**no-nat** 表示不对该数据流进行 NAT 转换。**no-nat** 动作主要用于配置一些特殊客户端。例如需要对 192.168.1.0/24 网段内除 192.168.1.2 以外的所有主机进行转换，可以利用 NAT 策略的匹配优先级，先配置一条对 192.168.1.2 主机不转换的策略，再配置一条对 192.168.1.0/24 网段转换的策略。

address-group 表示使用含有多个公网地址的 NAT 地址池来作为转换后流量的源地址，**easy-ip** 表示使用该条流量最终的出接口的 IP 地址来作为转换后的流量的源地址。当选择 **easy-ip** 方式时，系统通过查询路由自动找到对应的出接口。

说明：

NGFW 支持透明模式下（业务接口工作在交换模式）的源 NAT 配置，但只支持采用地址池中的地址做为转换后的源地址，不支持采用出接口地址做为转换后的源地址。

6. **可选：**当内部服务器需要提供多通道协议（如 FTP、QQ、MSN 等）的服务时，还需要配置 NAT ALG，以对这些协议在通信过程中临时协商出来的随机端口进行 NAT 转换。

说明：

缺省情况下，ftp 协议已开启该功能。

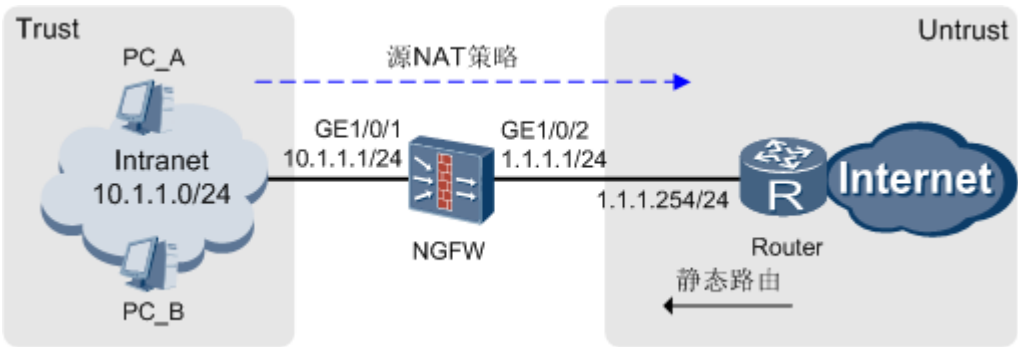
举例：私网用户通过地址池方式的源 NAT 策略访问 Internet

本例通过地址池方式的源 NAT 策略，将大量私网 IP 转换为少量公网 IP，使私网用户可以正常访问 Internet。

组网需求

某公司在网络边界处部署了 NGFW 作为安全网关。为了使私网中 10.1.1.0/24 网段的用户可以正常访问 Internet，需要在 NGFW 上配置源 NAT 策略。除了公网接口的 IP 地址外，公司还向 ISP 申请了 6 个 IP 地址（1.1.1.10~1.1.1.15）作为私网地址转换后的公网地址。网络环境如图 1 所示，其中 Router 是 ISP 提供的接入网关。

图 1 源 NAT 策略组网图



数据规划

项目		数据	说明
GigabitEthernet 1/0/1		IP 地址：10.1.1.1/24 安全区域：Trust	私网主机需要将 10.1.1.1 配置为默认网关。
GigabitEthernet 1/0/2		IP 地址：1.1.1.1/24 安全区域：Untrust	实际配置时需要按照 ISP 的要求进行配置。
允许访问 Internet 的私网网段		10.1.1.0/24	-
转换后的公网地址		1.1.1.10~1.1.1.15	由于私网地址比公网地址多，无法做到地址一一映射，所以需要开启允许端口转换，通过端口转换实现公网地址复用。
路由	NGFW 缺省路由	目的地址：0.0.0.0 下一跳：1.1.1.254	为了使私网流量可以正常转发至 ISP 的路由器，可以在 NGFW 上配置去往 Internet 的缺省路由。
	NGFW 黑洞路由	目的地址：1.1.1.10~1.1.1.15 下一跳：NULL 0	为了避免 Internet 用户主动访问转换后的公网地址时，NGFW 和 Router 之间形成路由环路。
	Router 静态路由	目的地址：1.1.1.10~1.1.1.15 下一跳：1.1.1.1	由于转换后的公网地址不存在实际接口，通过路由协议无法直接发现，所以需要在 Router 上手工配置静态路由。通常需要联系 ISP 的网络管理员配置。

配置思路

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
2. 配置安全策略，允许私网指定网段与 Internet 进行报文交互。
3. 配置 NAT 地址池，配置时开启允许端口转换，以实现公网地址复用。
4. 配置源 NAT 策略，实现私网指定网段访问 Internet 时自动进行源地址转换。
5. 在 NGFW 上配置缺省路由，使私网流量可以正常转发至 ISP 的路由器。
6. 在 NGFW 上配置黑洞路由，避免 NGFW 与 Router 之间产生路由环路。
7. 在私网主机上配置缺省网关，使私网主机访问 Internet 时，将流量发往 NGFW。
8. 在 Router 上配置静态路由，使从 Internet 返回的流量可以被正常转发至 NGFW。

操作步骤

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
 - a. 选择“网络 > 接口”。
 - b. 单击 GE1/0/1，按如下参数配置。

安全区域	trust
IPv4	
IP 地址	10.1.1.1/24

- c. 单击“确定”。
- d. 参考上述步骤按如下参数配置 GE1/0/2 接口。

安全区域	untrust
IPv4	
IP 地址	1.1.1.1/24

2. 配置安全策略，允许私网指定网段与 Internet 进行报文交互。
 - a. 选择“策略 > 安全策略”。
 - b. 单击“新建”，按如下参数配置。关于安全策略的更多信息，请参见[安全策略](#)。

名称	policy1
源安全区域	trust

目的安全区域	untrust
源地址/地区	10.1.1.0/24
目的地址/地区	any
动作	允许

c. 单击“确定”。

3. 配置 NAT 地址池，配置时开启允许端口地址转换，实现公网地址复用。

a. 选择“策略 > NAT 策略 > 源 NAT > NAT 地址池”。

b. 单击“新建”，按如下参数配置。

c. 单击“确定”。

4. 配置源 NAT 策略，实现私网指定网段访问 Internet 时自动进行源地址转换。

a. 选择“策略 > NAT 策略 > 源 NAT 策略”。

b. 单击“新建”，按如下参数配置。

c. 单击“确定”。

5. 在 NGFW 上配置缺省路由，使私网流量可以正常转发至 ISP 的路由器。

a. 选择“网路 > 路由 > 静态路由”。

b. 单击“新建”，按如下参数配置。

目的地址/掩码	0.0.0.0/0.0.0.0
下一跳	1.1.1.254

c. 单击“确定”。

6. 在 NGFW 上配置黑洞路由，避免 NGFW 与 Router 之间产生路由环路。

a. 在“静态路由”页面继续单击“新建”，按如下参数配置。

目的地址	1.1.1.10
掩码	255.255.255.255
出接口	Null0

b. 单击“应用”。参考上述步骤为 1.1.1.11~1.1.1.15 分别配置五条黑洞路由。

7. 在私网主机上配置缺省网关，使私网主机访问 Internet 时，将流量发往 NGFW。

以 WinXP 系统为例。

a. 在“控制面板”中找到对应的“网络连接”，右键单击“网络连接”，选择“属性”。

b. 在“常规”页签中选择“Internet 协议（TCP/IP）”，单击“属性”。

c. 选择“使用下面的 IP 地址”，按如下参数配置。

IP 地址	10.1.1.0/24 网段范围内的 IP 地址，由网络管理员分配。
子网掩码	255.255.255.0
默认网关	10.1.1.1

d. 单击“确定”。

8. 在 Router 上配置到 NAT 地址池地址（1.1.1.10~1.1.1.15）的静态路由，下一跳为 1.1.1.1，使从 Internet 返回的流量可以被正常转发至 NGFW。

通常需要联系 ISP 的网络管理员来配置此静态路由。

结果验证

1. 在内网中的 PC_A 上完成私网地址及缺省网关配置后，使用 IE 浏览器访问 <http://3.3.3.3>，可以正常访问即表示 NAT 策略配置成功。



说明：

此处仅以 3.3.3.3 为例进行说明，如果使用域名方式来访问 Web 服务器，还需要在 PC_A 上正确配置 DNS 以解析域名。

2. 如果想查看命中 NAT 策略的命中情况，可以选择“策略 > NAT 策略 > 源 NAT”，在源 NAT 策略列表中查看 NAT 策略的命中次数。
3. 如果想查看本次 NAT 转换的详细信息，可以选择“监控 > 会话表”，通过搜索找到源地址为 PC_A 私网地址（10.1.1.5）的表项，查看详细的转换信息。

协议	源地址	目的地址	NAT源地址	NAT目的地址	详细信息
http	10.1.1.5:2474	3.3.3.3:80	1.1.1.10:3761		

上图中红框部分为经过转换后的源地址和源端口，源地址为地址池中的地址。

配置脚本

NGFW 的配置脚本：

```
#
sysname NGFW
#
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface NULL0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
```

```
set priority 5
add interface GigabitEthernet1/0/2
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
ip route-static 1.1.1.10 255.255.255.255 NULL0
ip route-static 1.1.1.11 255.255.255.255 NULL0
ip route-static 1.1.1.12 255.255.255.255 NULL0
ip route-static 1.1.1.13 255.255.255.255 NULL0
ip route-static 1.1.1.14 255.255.255.255 NULL0
ip route-static 1.1.1.15 255.255.255.255 NULL0
#
nat address-group addressgroup1
section 0 1.1.1.10 1.1.1.15
#
security-policy
rule name policy1
source-zone trust
destination-zone untrust
source-address 10.1.1.0 24
action permit
#
nat-policy
rule name policy_nat1
source-zone trust
destination-zone untrust
source-address 10.1.1.0 24
action nat address-group addressgroup1
#
return
```

配置服务器静态映射

当内网部署了一台服务器，其真实 IP 是私网地址，但是希望公网用户可以通过一个公网地址来访问该服务器，这时可以配置服务器静态映射（NAT Server），使设备将公网用户访问该公网地址的报文转发给内网服务器。

操作步骤

1. 在系统视图下配置服务器静态映射。

- 对所有安全区域发布相同的公网 IP，即这些安全区域的用户通过访问相同的公网 IP 来访问内部服务器。

- 配置不指定协议类型的静态映射。

```
nat server name [ vpn-instance vpn-instance-name1 ] global { global-address
[ global-address-end ] | interface interface-type interface-number } inside
host-address [ host-address-end ] [ no-reverse ] [ vpn-instance vpn-instance-
name2 ]
```

- 配置指定协议类型的静态映射。

```
nat server name [ vpn-instance vpn-instance-name1 ] protocol protocol-type
global { global-address [ global-address-end ] | interface interface-type
interface-number } [ global-port ] [ global-port-end ] inside host-address
[ host-address-end ] [ host-port ] [ no-reverse ] [ vpn-instance vpn-instance-
name2 ]
```

- 针对不同的安全区域发布不同的公网 IP，即不同安全区域的用户可以通过访问不同的公网 IP 来访问内部服务器。

- 配置不指定协议类型的静态映射。

```
nat server name [ vpn-instance vpn-instance-name1 ] zone zone-name global
{ global-address [ global-address-end ] | interface interface-type interface-
number } inside host-address [ host-address-end ] [ no-reverse ] [ vpn-instance
vpn-instance-name2 ]
```

- 配置指定协议类型的静态映射。

```
nat server name [ vpn-instance vpn-instance-name1 ] zone zone-name protocol
protocol-type global { global-address [ global-address-end ] | interface
interface-type interface-number } [ global-port ] [ global-port-end ] inside
host-address [ host-address-end ] [ host-port ] [ no-reverse ] [ vpn-instance
vpn-instance-name2 ]
```

2. 以上两条命令中的参数解释如下：

- **global** 地址为服务器对外提供的公网地址，**inside** 地址为服务器的私网地址。**global** 地址可以为静态的 IP 地址 *global-address*，也可以借用动态的接口，即 **interface** 对应的接口，以实现当公网 IP 发生变化时能进行正常的地址转换。
- 对于同一个内部服务器发布多个公网 IP 供外部网络访问的场景，如果不同公网 IP 所在的链路规划在不同的安全区域，可以通过配置针对不同的安全区域发布不同的公网 IP 的 NAT Server 来实现。如果不同公网 IP 所在的链路规划在同一个安全区域，可以通过配置指定 **no-reverse** 参数的 NAT Server 来实现。指定 **no-reverse** 参数后，可以配置多个 **global** 地址和同一个 **inside** 地址建立映射关系。例如：

```
[NGFW] nat server global 1.1.1.1 inside 10.1.1.1 no-reverse
```

```
[NGFW] nat server global 2.2.2.2 inside 10.1.1.1 no-reverse
```

另外，指定 **no-reverse** 参数后，设备生成的 [Server-map 表](#) 只有正方向，内部服务器主动访问外部网络时，设备无法将内部服务器的私网地址转换成公网地址，内部服务器也就无法主动向外发起连接。因此，通过指定 **no-reverse** 参数可以禁止内部服务器主动访问外部网络。



说明：

配置指定 **no-reverse** 参数的 NAT Server 来实现同一个内部服务器发布多个公网 IP 供外部网络访问的需求时，由于配置了 **no-reverse** 参数，内部服务器将无法主动访问外部网络。此时，如果内部服务器想要访问外部网络，需要在内部服务器所在区域和外部网络所在区域的域间配置源 NAT 策略，将服务器的私网地址转换为公网地址。源 NAT 策略中引用的地址池可以是 **global** 地址也可以是其他的公网地址。

- 指定协议类型后，只有指定的端口才会被进行转换。这样可以只对外开放内部服务器的一部分端口，更加安全，但是有可能会影响一些端口不固定的协议的转发。这种情况下必须配置 NAT ALG 来进行解决。

配置指定协议的内部服务器地址到外部端口的映射时，可以配置为单个端口值，也可以配置为端口范围。当配置外部端口为一个范围时，内部地址也为一个范围，且一一对应，范围不可超过 128。

一个内部服务器使用一个公网 IP 地址对外发布，且需将多个内部端口转换成对应的多个外部端口时，需要多次使用 **nat server** 命令对其进行配置。例如，针对将真实 IP 地址为 10.1.1.1 的内部服务器的 1000 到 2000 端口映射成公网 IP 地址 1.1.1.1 的 1000 到 2000 的情况，不能配置端口的批量映射，需多次执行 **nat server** 命令才能实现。

- *vpn-instance-name1* 为需要访问服务器的客户端所在的 VPN 实例，*vpn-instance-name2* 为服务器本身所在的 VPN 实例。

如果使用 **vpn-instance** 参数，表示进行基于 VPN 实例的静态映射。此时应当注意客户端和服务端所在的 VPN 实例的关系，否则会导致业务不通。对 **vpn-instance** 参数的配置方法请参见[表 1](#)。

表 1 <i>vpn-instance-name1</i> 和 <i>vpn-instance-name2</i> 的配置说明			
VPN 实例 ID	配置说明	路由配置	示例
服务器 VID: 0 客户端 VID: 0	<i>vpn-instance-name1</i> 和 <i>vpn-instance-name2</i> 均不配置。	-	<ul style="list-style-type: none"> nat server global 1.1.1.1 inside 10.1.1.1 nat server zone untrust global 1.1.1.1 inside 10.1.1.1
服务器 VID: 非 0 客户端 VID: 0	配置 <i>vpn-instance-name2</i> ，不配置 <i>vpn-instance-name1</i> 。	必须配置一条静态路由，该静态路由的目的地址是服务器的私网地址，下一跳地址为设备去往服务器的下一跳地址。下一跳地址需要与 <i>vpn-instance-name2</i> 绑定。	假设设备去往服务器的下一跳地址为 2.2.2.2，静态映射和路由的配置如下： <ul style="list-style-type: none"> nat server global 1.1.1.1 inside 10.1.1.1 vpn-instance vpn1 ip route-static 10.1.1.1 32 vpn-instance vpn1 2.2.2.2 nat server zone untrust global 1.1.1.1 inside 10.1.1.1 vpn-instance vpn1 ip route-static 10.1.1.1 32 vpn-instance vpn1 2.2.2.2
服务器 VID: 0 客户端 VID: 非 0	配置 <i>vpn-instance-name1</i> ，不配置 <i>vpn-instance-name2</i> 。	必须配置一条静态路由，该静态路由的目的地址是服务器的私网地址，下一跳地址为设备去往服务器的下一跳地址。这条路由本身需要与 <i>vpn-instance-name1</i> 绑定。	假设设备去往服务器的下一跳地址为 2.2.2.2，静态映射和路由的配置如下： <pre>nat server zone vpn-instance vpn1 untrust global 1.1.1.1 inside 10.1.1.1 ip route-static vpn-instance vpn1 10.1.1.1 32 2.2.2.2</pre>
服务器 VID: 非 0 客户端 VID: 非 0 服务器和客户端在相同的 VPN 实例。	配置 <i>vpn-instance-name1</i> 和 <i>vpn-instance-name2</i> 为 VPN 实例名。	-	<pre>nat server zone vpn-instance vpn1 untrust global 1.1.1.1 inside 10.1.1.1 vpn-instance vpn1</pre>
服务器 VID: 非 0	暂不支持，即两个 <i>vpn-instance</i>	-	-

表 1 vpn-instance-name1 和 vpn-instance-name2 的配置说明

VPN 实例 ID	配置说明	路由配置	示例
客户端 VID: 非 0 服务器和客户 端在不同的 VPN 实例。	参数配置为不 同 VPN 实例名 的话, 命令执行 后不会生效。		

3. 可选: 配置设备发送静态映射公网地址的免费 ARP。

如果用户是先配置静态映射公网地址, 后配置公网接口地址, 且公网接口地址与静态映射公网地址在同一网段, 则需要完成该步骤手动配置设备发送静态映射公网地址的免费 ARP;

如果用户是先配置公网接口地址, 后配置静态映射公网地址, 且静态映射公网地址与公网接口地址在同一网段, 设备会自动发送静态映射公网地址的免费 ARP, 用户不需要配置该步骤。

- a. 在系统视图下进入公网接口的接口视图。

`interface interface-type interface-number`

- b. 配置设备发送静态映射公网地址的免费 ARP。

`nat arp-gratuitous send`

4. 可选: 当内部服务器需要提供多通道协议 (如 FTP、QQ、MSN 等) 的服务时, 还需要配置 NAT ALG, 以对这些协议在通信过程中临时协商出来的随机端口进行 NAT 转换。



说明:

缺省情况下, ftp 协议已开启该功能。

5. 在内部服务器上配置到外网地址的路由信息, 或者将其缺省网关设置为 NGFW 与内部服务器相连的接口的 IP 地址, 使其缺省将报文返回给设备, 由设备转发给相应的外网用户。

任务示例

配置名称为 policy1 的一对一静态映射, 把公网地址为 1.1.1.1、公网端口号为 21 的服务器映射为私网地址为 10.0.0.2、私网端口号为 21 的服务器, 并配置 `no-reverse` 参数不允许服务器主动访问外网。

```
[sysname] nat server policy1 protocol tcp global 1.1.1.1 21 inside 10.0.0.2 21 no-reverse
```

配置名称为 policy2 的一对一静态映射，把公网地址采用 GigabitEthernet 1/0/2 接口 IP 地址、公网端口号为 8080 的服务器映射为私网地址为 10.0.0.2、私网端口号为 80 的服务器，并配置 **no-reverse** 参数不允许服务器主动访问外网。

```
[sysname] nat server policy2 protocol udp global interface GigabitEthernet 1/0/2 8080 inside 10.0.0.2 80 no-reverse
```

配置名称为 policy3 的批量静态映射，把公网地址为 1.1.1.1~1.1.1.5、公网端口号为 3000 的服务器分别映射为私网地址为 10.0.0.1~10.0.0.5、私网端口号为 3000 的服务器，并配置 **no-reverse** 参数不允许服务器主动访问外网。

```
[sysname] nat server policy3 protocol tcp global 1.1.1.1 1.1.1.5 3000 inside 10.0.0.1 10.0.0.5 3000 no-reverse
```

配置名称为 policy4 的批量静态映射，把公网地址为 1.1.1.1、公网端口号为 2000~2005 的服务器分别映射为私网地址为 10.0.0.1~10.0.0.5、私网端口号为 80 的服务器，并配置 **no-reverse** 参数不允许服务器主动访问外网。

```
[sysname] nat server policy4 protocol tcp global 1.1.1.1 2000 2005 inside 10.0.0.1 10.0.0.5 80 no-reverse
```

后续处理

如果希望查看静态映射的配置情况，可以执行命令 [display nat server](#)，如下。

```
[sysname] display nat server
Server in private network information:
id           : 0
zone         : ---
interface    : ---
globaladdr   : 1.1.1.2
inside-start-addr : 10.1.1.2      inside-end-addr : 10.1.1.2
global-start-port : 21(ftp)      global-end-port  : 21(ftp)
insideport    : 21(ftp)
globalvpn     : public      insidevpn        : public
protocol      : tcp         vrrp              : ---
no-reverse    : no

Total    1 NAT servers
```

在本例中，根据屏显信息可以看出存在一个内部服务器的映射关系，是将私网 10.1.1.2 的服务器的 IP 地址映射为 1.1.1.1。

当外网用户访问服务器公网地址后，使用 [display firewall session table nat](#) 命令，查询目的地址为公网地址的表项，存在该表项，且该表项的 NAT 目的地址应为内网服务器的真实地址，则表示服务器映射部分的配置成功。

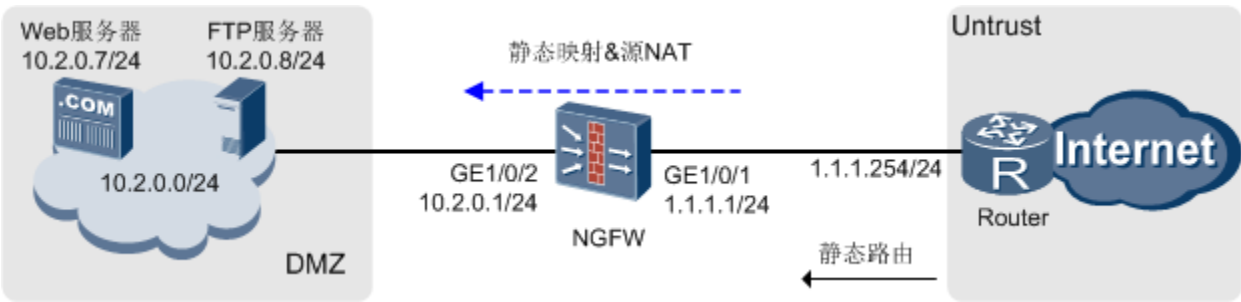
举例：外部网络用户通过服务器静态映射功能访问内部服务器（双向 NAT）

本例通过服务器静态映射功能（NAT Server），实现公网地址到内部私网服务器的映射，使私网服务器能够对外提供服务。同时为了简化内部服务器的回程路由配置，配置源 NAT 功能将公网访问内部服务器报文的源地址转换为私网地址。

组网需求

某公司在网络边界处部署了 NGFW 作为安全网关。为了使私网 Web 服务器和 FTP 服务器能够对外提供服务，需要在 NGFW 上配置服务器静态映射功能。除了公网接口的 IP 地址外，公司还向 ISP 申请了一个 IP 地址（1.1.1.10）作为内网服务器对外提供服务的地址。同时，为了简化内部服务器的回程路由配置，通过配置源 NAT 策略，使内部服务器缺省将回应报文发给 NGFW。网络环境如[图 1](#)所示，其中 Router 是 ISP 提供的接入网关。

图 1 静态映射+源 NAT 组网图



数据规划

项目	数据	说明
GigabitEthernet 1/0/1	IP 地址：1.1.1.1/24 安全区域：Untrust	实际配置时需要按照 ISP 的要求进行配置。
GigabitEthernet 1/0/2	IP 地址：10.2.0.1/24	内网服务器需要将 10.2.0.1 配置为默认网

HCIE-Security 备考指南 NAT 策略

项目		数据	说明
		安全区域: DMZ	关。
服务器映射		名称: policy_web 公网地址: 1.1.1.10 私网地址: 10.2.0.7 公网端口: 8080 私网端口: 80	通过该映射, 使用外网用户能够访问 1.1.1.10, 且端口号为 8080 的流量能够送给内网的 Web 服务器。 Web 服务器的私网地址为 10.2.0.7, 私网端口号为 80。
		名称: policy_ftp 公网地址: 1.1.1.10 私网地址: 10.2.0.8 公网端口: 21 私网端口: 21	通过该映射, 使用外网用户能够访问 1.1.1.10, 且端口号为 21 的流量能够送给内网的 FTP 服务器。 FTP 服务器的私网地址为 10.2.0.8, 私网端口号为 21。
NAT 地址池地址		10.2.0.10~10.2.0.15	-
路由	缺省路由	目的地址: 0.0.0.0 下一跳: 1.1.1.254	为了内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器, 可以在 NGFW 上配置去往 Internet 的缺省路由。
	黑洞路由	目的地址: 1.1.1.10 下一跳: NULL 0	为了避免外网用户访问 Global 地址但没有匹配到 Server-Map 的报文, 在 NGFW 和 Router 之间形成路由环路。

配置思路

1. 配置接口 IP 地址和安全区域, 完成网络基本参数配置。
2. 配置安全策略, 允许外部网络用户访问内部服务器。
3. 配置服务器映射功能, 创建两条静态映射, 分别映射内网 Web 服务器和 FTP 服务器。
4. 配置源 NAT 策略, 将公网访问内部服务器报文的源地址转换为 NAT 地址池中地址。
5. 在 NGFW 上配置缺省路由, 使内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器。
6. 在 NGFW 上配置黑洞路由, 避免 NGFW 与 Router 之间产生路由环路。
7. 在 Router 上配置到服务器映射的公网地址的静态路由。

操作步骤

1. 配置接口 IP 地址和安全区域, 完成网络基本参数配置。
 - a. 选择“网络 > 接口”。
 - b. 单击 GE1/0/1, 按如下参数配置。

安全区域	untrust
IPv4	
IP 地址	1.1.1.1/24

- c. 单击“确定”。
- d. 参考上述步骤按如下参数配置 GE1/0/2 接口。

安全区域	dmz
IPv4	
IP 地址	10.2.0.1/24

2. 配置安全策略，允许外部网络用户访问内部服务器。

- a. 选择“策略 > 安全策略”。
- b. 单击“新建”，按如下参数配置。

名称	policy1
源安全区域	untrust
目的安全区域	dmz
源地址/地区	any
目的地址/地区	10.2.0.0/24
动作	允许

- c. 单击“确定”。

3. 配置服务器映射功能，创建两条静态映射，分别映射内网 Web 服务器和 FTP 服务器。

- a. 选择“策略 > NAT 策略 > 服务器映射”。
- b. 单击“新建”，按如下参数创建名称为“policy_web”的静态映射策略，用于映射内网 Web 服务器。

- c. 单击“确定”。
- d. 参考上述步骤，按如下参数创建名称为“policy_ftp”的静态映射策略，用于映射内网 FTP 服务器。

4. 配置 NAT 地址池，配置时开启允许端口地址转换。
 - a. 选择“策略 > NAT 策略 > 源 NAT > NAT 地址池”。
 - b. 单击“新建”，按如下参数配置。

新建NAT地址池

名称: addressgroup1 *

描述:

IP地址范围: 10.2.0.10 * - 10.2.0.15

☒ 允许端口转换

c. 单击“确定”。

5. 配置源 NAT 策略，实现公网用户访问私网服务器时自动进行源地址转换。

a. 选择“策略 > NAT 策略 > 源 NAT 策略”。

b. 单击“新建”，按如下参数配置。

新建源NAT策略

[\[功能介绍\]](#)

名称: policy_nat1 *

描述:

源安全区域: untrust * [\[多选\]](#)

目的类型: ☒ 目的安全区域 ☐ 出接口

目的安全区域: dmz *

转换前

源地址: any

目的地址: 10.2.0.7-10.2.0.8

服务: ftp,http [\[多选\]](#)

动作: ☒ NAT转换 ☐ 不做NAT转换

转换后

源地址: ☒ 地址池中的地址 ☐ 出接口地址

地址池: addressgroup1 *



说明：

源 NAT 策略的目的地址要配置成服务器的私网地址。因为 NGFW 是先匹配服务器静态映射生成的 Server-map 表，将报文的目的地址转换为服务器私网地址，而后再匹配源 NAT 策略。

c. 单击“确定”。

6. 在 NGFW 上配置缺省路由，使内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器。

a. 选择“网路 > 路由 > 静态路由”。

b. 单击“新建”，按如下参数配置。

目的地址/掩码	0.0.0.0/0.0.0.0
下一跳	1.1.1.254

c. 单击“确定”。

7. 在 NGFW 上配置黑洞路由，避免 NGFW 与 Router 之间产生路由环路。

a. 在“静态路由”页面继续单击“新建”，按如下参数配置。

目的地址	1.1.1.10
掩码	255.255.255.255
出接口	Null0



b. 单击“确定”。

8. 在 Router 上配置到服务器映射的公网地址（1.1.1.10）的静态路由，下一跳为 1.1.1.1，使得去服务器的流量能够送往 NGFW。

通常需要联系 ISP 的网络管理员来配置此静态路由。

结果验证

- 配置完成后，外网用户能够正常访问内网服务器提供的服务，表示服务器映射配置成功。
- 如果想查看服务器映射过程中地址和端口的转换信息，可以选择“监控 > 会话表”，通过搜索找到目的地址为 1.1.1.10 的表项，查看详细的转换信息。

协议	源地址	目的地址	NAT源地址	NAT目的地址	详细信息
http	3.3.3.3:4182	1.1.1.10:8080	10.2.0.10:2182	10.2.0.7:80	
ftp	3.3.3.3:63485	1.1.1.10:21	10.2.0.10:2134	10.2.0.8:21	

上图中蓝框部分为经过转换后的源地址和源端口，源地址为地址池中的地址；红框部分为经过服务器映射后的目的地址和目的端口。

配置脚本

NGFW 的配置脚本：

```
#
sysname NGFW
#
nat server policy_web protocol tcp global 1.1.1.10 www inside 10.0.0.7 80 no-reverse
nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp no-reverse
```

```
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface NULL0
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/1
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet1/0/2
#
firewall interzone dmz untrust
 detect ftp
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
ip route-static 1.1.1.10 255.255.255.255 NULL0
#
nat address-group addressgroup1
 section 0 10.2.0.10 10.2.0.15
#
security-policy
 rule name policy1
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 24
  action permit
#
nat-policy
 rule name policy_nat1
  source-zone untrust
  destination-zone dmz
  destination-address range 10.2.0.7 10.2.0.8
  service http
  service ftp
  action nat address-group addressgroup1
#
```

```
return
```

配置服务器负载均衡

服务器负载均衡实现了将访问同一个 IP 地址的用户流量分配到不同服务器上的功能。

背景信息

当一台服务器无法处理多个用户的访问时，可使用多台服务器，分担网络流量。此时需要将 NGFW 部署在服务器所在网络的出口，然后在 NGFW 上配置服务器负载均衡功能，将访问同一个 IP 地址的用户流量分配到不同的服务器上。



说明：

在配置完负载均衡后，后续配置安全策略、NAT、路由等功能时，需针对真实服务器的地址来配置，而不是虚服务器地址。

操作步骤

1. 在系统视图下启用负载均衡功能。

[slb enable](#)

2. 配置内网真实服务器。

- a. 在系统视图下进入负载均衡配置视图。

[slb](#)

- b. 配置真实服务器。

```
rserver rserver-id [ to end-rserver-id ] rip ip-address [ active | inactive |  
healthchk ] [ weight weight ] [ description text ] [ vpn-instance vpn-instance  
name ]
```

- *rserver-id* 表示真实服务器的起始 ID。
- *end-rserver-id* 表示真实服务器的终止 ID。
- **rip** *ip-address* 表示真实服务器的起始 IP 地址。

真实服务器的 IP 地址为连续的 IP 地址时，可以通过指定真实服务器的起始 ID 和终止 ID 以及真实服务器的起始 IP 地址来进行批量配置。真实服务器的 ID 从起始 ID 开始加 1 递增，到终止 ID 结束。真实服务器的 IP 地址也从配置的起始 IP 地址开始加 1 递增，且与真实服务器 ID 一一对应。例如 3 个真实服务器 IP 地址分别为 10.100.1.1、10.100.1.2 和 10.100.1.3，则可以配置起始 `IDrserver-id` 为 1，终止 `IDend-rserver-id` 为 3，起始 IP 地址 `ip-address` 为 10.100.1.1。这样，ID 为 1、2、3 的真实服务器的 IP 地址分别为 10.100.1.1、10.100.1.2、10.100.1.3。

真实服务器的 IP 地址不是连续的 IP 地址时，则需要逐条进行配置。

- **active** 表示不对真实服务器进行健康状态检查，强制配置真实服务器为健康状态；
inactive 表示不对真实服务器进行健康状态检查，强制配置真实服务器为不健康状态；
healthchk 表示对真实服务器进行健康状态检查。缺省情况下，配置为 **healthchk**。
- **weight** 表示真实服务器的权重，NGFW 可根据服务器的权重判断数据流应该流向哪一台服务器。仅当设置负载均衡算法为 **weightrr** 时才需要配置权重。



说明：

需要根据真实服务器的处理能力配置权值 **weight**，处理能力弱的服务器应配置的权值较小。

真实服务器和服务器组 **group** 必须处在同一 VPN 实例下。真实服务器被加入到服务器组 **group** 后，不允许再修改真实服务器的权重 **weight**。

不同 VPN 实例下的实服务器 ID 可以相同，IP 可以相同。

3. 配置服务器组。

- 在负载均衡视图下，创建并进入服务器组视图。

```
group group-name [ vpn-instance vpn-instance name ]
```

根系统用户配置此命令时，最多可以配置 256 个服务器组。当指定 VPN 实例名称的时候，最多可以配置 4 个服务器组。不同 vpn 实例下的组名可以相同，虚拟系统用户可以通过 telnet 登录配置组，但是只能配置用户所属的虚拟系统的组。

- 将真实服务器添加到指定服务器组。

```
addrserver rserver-id [ to end-rserver-id ] [ vpn-instance vpn-instance name ]
```

c. 设置负载均衡算法。

```
metric { roundrobin | srchash | weightrr }
```

- **roundrobin** 表示简单轮询算法：根据流量的带宽均分到各个内网服务器上，使每台服务器的负载相同。
- **srchash** 表示源地址哈希算法：根据流量的源地址进行 Hash 算法计算，保证相同源地址的流量由同一台内网服务器处理。
- **weightrr** 表示加权轮询算法：根据每台内网服务器的权值比例（权重）来分配流量，使每台服务器的负载比例与权值比例相同。新增内网服务器时，重新计算权值比例，按新的权值比例来分配流量。



说明：

NGFW 采用简单轮询算法进行负载均衡时存在如下的使用限制：

客户端使用 FTP 方式和内网服务器传输文件时，与一台服务器建立控制通道后，文件的传输就在客户端与该服务器之间进行。但传输的文件较多时，客户端可能会重新发起控制连接，此时简单轮询算法会将流量分配到另一台服务器上，后续的文件传输将转由该服务器来处理。如果两台服务器上存放文件的路径不一致，就会导致文件传输失败。

使用 HTTP 方式传输文件时存在同样的问题，因为传输文件较多时，需要建立多条 HTTP 连接才能完成文件的传输。

对于上述的场景，建议采用源地址哈希算法，保证相同源地址的流量由同一台内网服务器处理。

4. 配置虚拟服务器地址，并和服务器组进行关联。

```
vserver vserver-name vip ip-address group group-name [ { tcp | udp } [ vport vport-number ] [ rport rport-number ] ] [ vpn-instance vpn-instance name ]
```

这里的 *ip-address* 为虚拟服务器的 IP 地址，配置完该项之后，用户可以通过访问该地址，达到对真实服务器流量负载均衡的目的。*group-name* 对应为上文中的服务器组。

可以通过配置 **tcp** 或者 **udp** 来限制服务器的会话协议类型；同时，可以通过配置 **vport** *vport-number* 和 **rport** *rport-number* 来严格控制真实服务器和虚服务器的访问端口。

配置完服务器负载均衡后 NGFW 会自动对外发布虚服务器 IP 地址的路由信息，故无需配置与虚服务器 IP 地址相关的路由。



说明：

虚拟服务器 IP 地址不允许和真实服务器或 NGFW 接口的 IP 地址相同。

不同 VPN 实例下的虚服务器 ID 可以相同，IP 可以相同。

5. 可选：配置设备发送虚拟服务器地址的免费 ARP。

如果用户是先配置虚拟服务器地址，后配置公网接口地址，且公网接口地址与虚拟服务器地址在同一网段，则需要完成该步骤手动配置设备发送虚拟服务器地址的免费 ARP；

如果用户是先配置公网接口地址，后配置虚拟服务器地址，且虚拟服务器地址与公网接口地址在同一网段，设备会自动发送虚拟服务器地址的免费 ARP，用户不需要配置该步骤。

- a. 在系统视图下进入公网接口的接口视图。

[interface](#) *interface-type interface-number*

- b. 配置设备发送虚拟服务器地址的免费 ARP。

[nat arp-gratuitous send](#)

后续处理

当外网用户访问服务器公网地址后，使用 [display firewall session table nat](#) 命令，查询目的地址为公网地址的表项，存在该表项，且该表项的 NAT 目的地址应为内网服务器的真实地址，则表示服务器映射部分的配置成功。

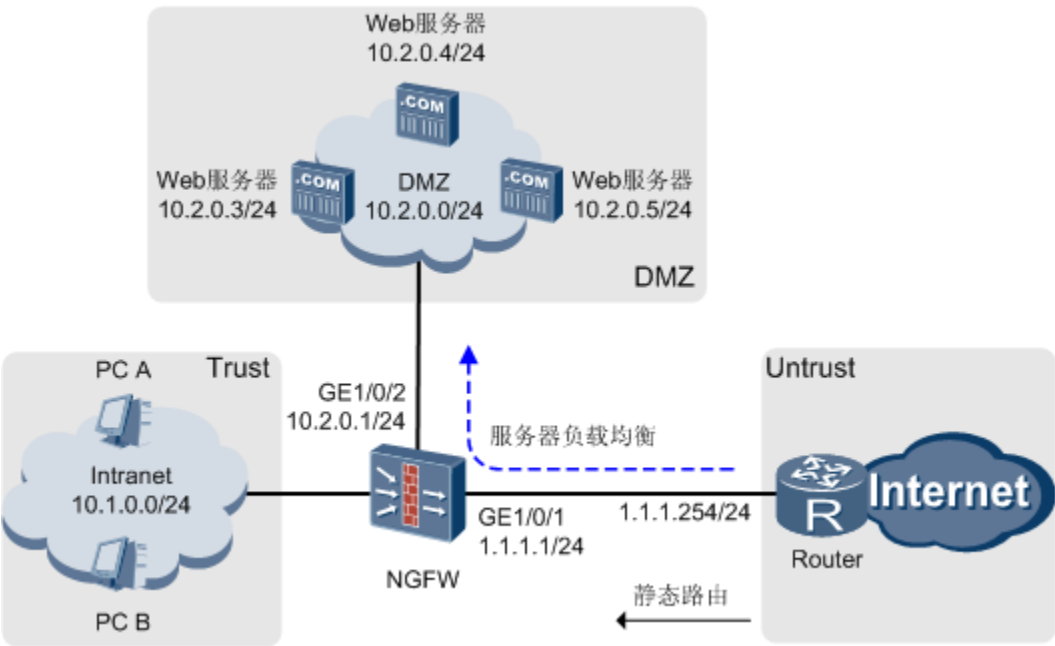
举例：服务器负载均衡

内部网络中存在三台真实服务器对外提供 Web 服务，通过在 NGFW 上配置负载均衡功能，保证三台服务器的流量负载均衡。

组网需求

某公司在网络边界处部署了 NGFW 作为安全网关，公司内部网络存在三台私网 Web 服务器对外提供 Web 访问功能。为了节约公网 IP 地址，同时出于可靠性的考虑，需要在 NGFW 上配置服务器负载均衡。除了公网接口的 IP 地址外，公司还向 ISP 申请了一个 IP 地址（1.1.1.10）作为三台私网 Web 服务器对外虚拟的服务器的公网地址。网络环境如图 1 所示，其中 Router 是 ISP 提供的接入网关。

图 1 服务器负载均衡组网图



数据规划

项目		数据	说明
GigabitEthernet 1/0/1		IP 地址：1.1.1.1/24 安全区域：Untrust	实际配置时需要按照 ISP 的要求进行配置。
GigabitEthernet 1/0/2		IP 地址：10.2.0.1/24 安全区域：DMZ	私网服务器需要将 10.2.0.1 配置为默认网关。
服务器负载均衡		名称：policy_web 公网地址：1.1.1.10 流量分配方式：源地址哈希 私网地址：10.2.0.3/10.2.0.4/10.2.0.5 公网端口：8080 私网端口：80	通过服务器负载均衡功能，对外虚拟服务器 1.1.1.10，对外端口号为 8080。真实服务器为 10.2.0.3、10.2.0.4 和 10.2.0.5，内部端口号为 80，三台服务器采用流量均分的方式对外提供服务。
路由	NGFW 缺省路由	目的地址：0.0.0.0 下一跳：1.1.1.254	使内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器。

项目		数据	说明
	Router 静态路由	目的地址：1.1.1.10 下一跳：1.1.1.1	使访问服务器的流量可以被正常转发至 NGFW，通常需要联系 ISP 的网络管理员配置。

配置思路

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
2. 配置服务器负载均衡。
3. 配置安全策略，允许外部网络用户访问内部服务器，允许 Local 区域发出报文对 DMZ 区域的服务器进行健康状态检查。
4. 在 NGFW 上配置缺省路由，使内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器。
5. 在 Router 上配置静态路由，使访问服务器的流量可以被正常转发至 NGFW。

操作步骤

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
 - a. 选择“网络 > 接口”。
 - b. 单击 GE1/0/1，按如下参数配置。

安全区域	untrust
IPv4	
IP 地址	1.1.1.1/24

- c. 单击“确定”。
- d. 参考上述步骤按如下参数配置 GE1/0/2 接口。

安全区域	dmz
IPv4	
IP 地址	10.2.0.1/24

2. 配置服务器负载均衡。
 - a. 选择“策略 > NAT 策略 > 服务器映射”。
 - b. 单击“新建”，按如下参数配置。

新建服务器映射

[\[功能介绍\]](#)

名称

policy_web

类型

静态映射

服务器负载均衡

公网地址

1.1.1.10

流量分配方式

源地址哈希

内部服务器列表

新建

删除

私网地址

健康状态检查

10.2.0.5

10.2.0.4

10.2.0.3

共 3 条

允许端口转换

协议

TCP

UDP

公网端口

8080

<1-65535>

私网端口

80

<1-65535>

c. 单击“确定”。

3. 配置安全策略，允许外部网络用户访问内部服务器，允许 Local 区域发出报文对 DMZ 区域的服务器进行健康状态检查。

a. 选择“策略 > 安全策略”。

b. 单击“新建”，按如下参数配置。关于安全策略的更多信息，请参见[安全策略](#)。

名称	policy_1
源安全区域	untrust、local
目的安全区域	dmz
源地址/地区	any
目的地址/地区	10.2.0.0/24
动作	允许

c. 单击“确定”。

4. 在 NGFW 上配置缺省路由，使内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器。

a. 选择“网路 > 路由 > 静态路由”。

b. 单击“新建”，按如下参数配置。

47

目的地址/掩码	0.0.0.0/0.0.0.0
下一跳	1.1.1.254




c. 单击“确定”。

5. 在 Router 上配置到服务器的公网地址（1.1.1.10）的静态路由，下一跳为 1.1.1.1，使得去服务器的流量能够送往 NGFW。

通常需要联系 ISP 的网络管理员来配置此静态路由。

结果验证

1. 配置完成后，外网用户能够通过虚拟服务器的 IP 地址和端口（1.1.1.10:8080）正常访问内网服务器提供的服务。
2. 当多个（大于或等于三个）外网用户同时访问内网服务器或者一个外网用户同时对内网服务器发起多个（大于或等于三个）连接时，三台服务器上均有流量。
3. 如果想查看服务器负载均衡过程中地址和端口的转换信息，可以选择“监控 > 会话表”，通过搜索找到目的地址为 1.1.1.10 的表项，查看详细的转换信息。

协议	源地址	目的地址	NAT源地址	NAT目的地址	详细信息
http	3.3.3.3:4182	1.1.1.10:8080		10.2.0.3:80	
http	3.3.3.3:3060	1.1.1.10:8080		10.2.0.4:80	
http	3.3.3.3:4424	1.1.1.10:8080		10.2.0.5:80	

从上图可以看出，服务器的公网地址 1.1.1.10 经过服务器映射后转换为三个私网服务器的地址：10.2.0.3、10.2.0.4 和 10.2.0.5，端口也由 8080 转换为 80 端口。

配置脚本

NGFW 的配置脚本：

```
#
sysname NGFW
#
slb enable
#
interface GigabitEthernet1/0/1
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```

ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet1/0/1
#
firewall zone dmz
    set priority 50
    add interface GigabitEthernet1/0/2
#
slb
    rserver 1 rip 10.2.0.4 weight 32 healthchk
    rserver 2 rip 10.2.0.4 weight 32 healthchk
    rserver 3 rip 10.2.0.5 weight 32 healthchk
    group policy_web
    metric srchash
    addrserver 1
    addrserver 2
    addrserver 3
    vserver policy_web vip 1.1.1.10 group policy_web tcp vport 8080 rport 80
#
security-policy
    rule name policy1
        source-zone local
        source-zone untrust
        destination-zone dmz
        destination-address 10.2.0.0 24
        action permit
#
return

```

配置目的 NAT

目的 NAT 主要用于手机用户上网时需要修改目的网关地址的场景。

背景信息

手机用户需要通过登录 WAP（Wireless Application Protocol）网关来实现上网的功能。目前，大量用户使用直接从国外购买的手机，这些手机出厂时，缺省设置的 WAP 网关地址与本国 WAP 网关地址不符，且无法自行修改，从而导致用户不能移动上网。

为解决这一问题，无线网络中，在 WAP 网关与用户之间部署 NGFW。通过在设备上配置目的 NAT 功能，使这部分手机用户能够正常获取网络资源。

如图 1 所示，当手机用户上网时，目的 NAT 处理过程如下：

1. 当手机用户上网时，请求报文经过基站及其他中间设备到达 NGFW。
2. 到达 NGFW 的报文如果匹配 NGFW 上所配置的目的 NAT 策略，则将此数据报文的目的 IP 地址转换为已配置好的 WAP 网关的 IP 地址，并送往 WAP 网关。
3. WAP 网关对手机客户端提供相应的业务服务（如视频服务、网页服务等），并将回应报文发往 NGFW。
4. 回应报文在 NGFW 上命中会话，NGFW 转换该报文的源 IP 地址，并将该报文发往手机用户，完成一次通信。

图 1 手机用户上网目的 NAT 组网图



说明：

- 如果报文在到达 NGFW 前已经在其他设备上做了允许端口转换的 NAT 策略，则不能再在 NGFW 上启用目的 NAT。
- 目的 NAT 不支持与 NAT ALG 同时使用。

操作步骤

1. 在系统视图下进入安全区域视图。

```
firewall zone [ name ] zone-name
```

这里应当进入的是移动终端所在安全区域，不支持对从 Local 域发出的报文做目的 NAT。

2. 配置目的 NAT。

```
destination-nat acl-number address ip-address [ port port-number ]
```

acl-number 用来将高级 ACL 与正确的 WAP 网关地址进行绑定。设备将命中 ACL 的报文目的 IP 地址更换为已正确的 WAP 网关的 IP 地址 *ip-address*，并转发给 WAP 网关。



注意：

此处的 ACL，应该严格配置，避免非 WAP 业务数据流被 [destination-nat](#) 命令引用，从而导致非 WAP 业务中断。

此处只能引用范围为 3000~3999 的高级 ACL。

每个安全域上最多可以配置 256 个 WAP 网关地址。

后续处理

如果希望查看目的 NAT 的配置情况，可以执行命令 [display zone](#)，如下。

```
[sysname] display zone name trust
trust
priority is 85
destination-nat 3000 address 10.1.1.1
interface of the zone is (1):
GigabitEthernet1/0/2
```

在本例中，根据屏显信息可以看出 Trust 区域上配置了一个目的 NAT，将命中 ACL3000 的流量的目的地址转换为 10.1.1.1。

配置 NAT ALG

当设备既开启 NAT 功能，又需要转发多通道协议报文（例如 FTP 等）时，必须开启相应的 NAT ALG 功能。

前提条件

配置 NAT ALG 功能与 [ASPF](#) 功能使用的是同一条命令。所以如果已经在域间配置过 ASPF 功能的话，可以不需要再重复配置 NAT ALG 功能。

两者的区别在于：

- ASPF 功能的目的是识别多通道协议，并自动为其开放相应的安全策略。

- NAT ALG 功能的目的是识别多通道协议，并自动转换报文载荷中的 IP 地址和端口信息。

背景信息

为了简化配置，系统支持配置全局 NAT ALG 功能，开启全局 NAT ALG 功能相当于同时开启了域间 NAT ALG 功能和域内 NAT ALG 功能。

全局 NAT ALG 功能和域间/域内 NAT ALG 功能是“或”的关系，实际使用中选择其中一种方式进行配置即可。

操作步骤

1. 配置 NAT ALG 功能。

- 配置全局 NAT ALG 功能。

- a. 进入系统视图。

`system-view`

- b. 开启需要识别的协议。

`firewall detect protocol`

缺省情况下，FTP 协议已经开启该功能。

- 配置域间 NAT ALG 功能。

- a. 在系统视图下进入域间视图

`firewall interzone zone-name1 zone-name2`

- b. 开启需要识别的协议。

`detect (域间) protocol`

如果需要监控多种协议，重复执行该命令。

- 配置域内 NAT ALG 功能。

- a. 在系统视图下进入安全区域视图。

`firewall zone [name] zone-name`

- b. 开启需要识别的协议。

[detect \(域内\) protocol](#)

如果需要监控多种协议，重复执行该命令。

2. **可选：**配置在出现报文重传的情况下对 NAT 业务无影响。

[firewall alg-detect enable](#)

当 FTP ALG 应用下，如果网络环境不好，有 PORT 报文重传时，可能会导致业务不通。为避免这个情况，可以开启这个命令。

后续处理

如果希望查看已经配置的 NAT ALG 的情况，可以执行命令 [display interzone](#) 查看域间配置，或者执行命令 [display zone](#) 查看域内配置，如下。

```
[sysname] display interzone trust untrust
interzone trust untrust
    detect ftp
#
```

本例中，根据屏显信息可以看出在 trust 和 untrust 域间已经配置了对 FTP 协议的自动识别。

处理 NAT 故障

介绍了 NAT 策略使用中的常见故障。

- [配置了源 NAT 策略后，内部网络无法访问 Internet](#)

源 NAT 策略配置完成后，如果内部网络用户无法通过访问 Internet，可以参考本节的内容定位故障，调整配置。

- [配置了服务器静态映射后，外部网络无法访问内部服务器](#)

服务器静态映射（NAT Server）配置完成后，如果外部网络用户无法访问内部服务器，可以参考本节的内容定位故障，调整配置。

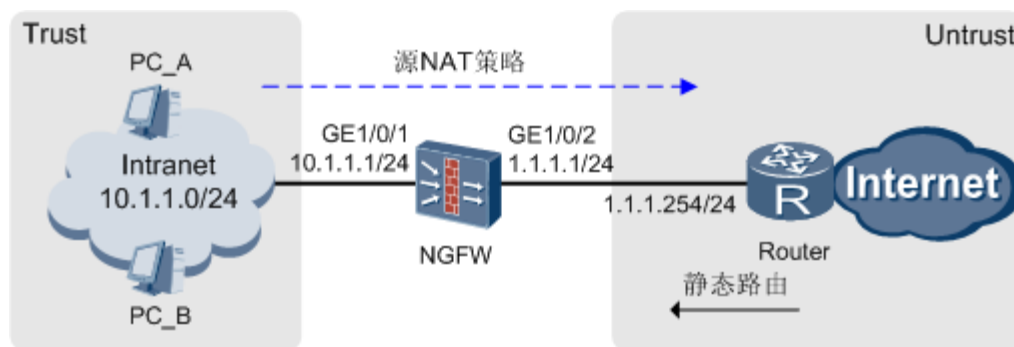
配置了源 NAT 策略后，内部网络无法访问 Internet

源 NAT 策略配置完成后，如果内部网络用户无法通过访问 Internet，可以参考本节的内容定位故障，调整配置。

现象描述

如图 1 所示，某公司在网络边界处部署了 NGFW 作为安全网关，通过在 NGFW 上配置源 NAT 策略，使内部网络中的 PC 能够访问 Internet 上的资源。

图 1 网络环境示意图



实际使用中，发现内部网络中的 PC_A（地址为 10.1.1.2）无法访问 Internet 上的 Web 服务器（地址为 3.3.3.3）。

定位思路

选择“监控 > 会话表”，查询源地址为 10.1.1.2 的表项。根据会话表显示结果可以缩小可能原因的范围，请分别按以下三种情况逐一排查可能原因：

- [没有找到源地址为 10.1.1.2 的会话表。](#)
- [存在会话表项，但是会话表项错误。例如：表项中没有 10.1.1.2 的转换记录、转换后源地址不正确。](#)
- [已经建立了正确的会话表项。](#)

处理步骤

没有找到源地址为 10.1.1.2 的会话表项。

可能原因及相应的处理步骤如下：

1. 内部网络中的 PC 上没有设置网关

检查 PC_A 的缺省网关地址是否为 10.1.1.1。是则此项配置正确，否则在私网主机上配置缺省网关进行配置。

2. 内部网络中的其他设备将报文丢弃

检查内部网络中 PC 和 NGFW 之间是否存在其他设备将 PC 发出的报文丢弃，如果存在，请检查并调整该设备的配置信息。

3. NGFW 的基础配置不正确

- a. 检查 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 是否配置了正确的 IP 地址并加入了安全区域。
- b. IP 地址和安全区域正确后，检查不需要进行 NAT 的流量是否可以正常访问 Internet。如果不需要 NAT 的流量也无法正常访问，则可能 NGFW 的其他网络配置有误，请网络检查排除。如果可以正常访问，请进行其他项目的检查。

4. NGFW 上配置了黑名单将报文丢弃

选择“策略 > 安全防护 > 黑名单”，搜索源地址为 10.1.1.2 的表项。如果找到则删除此表项，否则请进行其他项目的检查。

5. NGFW 上配置的安全策略不正确

选择“策略 > 安全策略 > 安全策略”，查找“源 IP 地址”包含 10.1.1.2 的表项，存在该条表项且“动作”为“允许”，则该项配置正确，否则请重新调整安全策略的配置。

6. NGFW 上没有配置去往 Internet 的路由

选择“网络 > 路由 > 路由表”，查找是否存在正确的公网路由表项。

存在会话表项，但是会话表项错误。例如：表项中没有 10.1.1.2 的转换记录、转换后源地址不正确。

可能原因及相应的处理步骤如下：

7. 源地址没有被转换

选择“策略 > NAT 策略 > 源 NAT 策略”，找到“源 IP 地址”包含 10.1.1.2 的表项。存在该条表项且“动作”为“允许”，则该项配置正确，否则请重新调整源 NAT 策略的配置。

8. 源地址转换错误

选择“策略 > NAT 策略 > 源 NAT 策略”，找到“源 IP 地址”包含 10.1.1.2 的表项，检查其“转换后的地址”是否配置正确，否则请重新调整源 NAT 策略的配置。

已经建立了正确的会话表项。

可能原因及相应的处理步骤如下：

9. Internet 上没有达到地址池地址的路由

当 NAT 使用的公网地址不存在于实际接口上时，必须要 ISP 管理员在接入设备 Router 上手工配置达到这些公网地址的路由才能使 Internet 的回程报文被正确地转发至 NGFW。请联系 ISP 管理员确认此项配置。

如果希望通过动态路由协议让 NGFW 与 Router 之间自动发现路由，则需要在动态协议中发布目的地址为这些公网地址的黑洞路由。

10. Internet 中的设备将回程报文丢弃

检查 Internet 中是否存在其他设备将回程的报文丢弃，如果存在，请检查并调整该设备的配置信息。可能需要联系 ISP 管理员确认。

11. NGFW 上配置了黑名单将回程报文丢弃

请参考 [4](#) 检查处理。

12. NGFW 上没有去往 PC 的路由

本举例中，内部网络与 NGFW 直接相连，不涉及路由问题，因此不需要考虑本原因。如果内部网络与 NGFW 不是直连，而是跨越了其他网络，此时就需要在 NGFW 上配置去往内部网络的路由，否则 NGFW 会将回程报文丢弃。

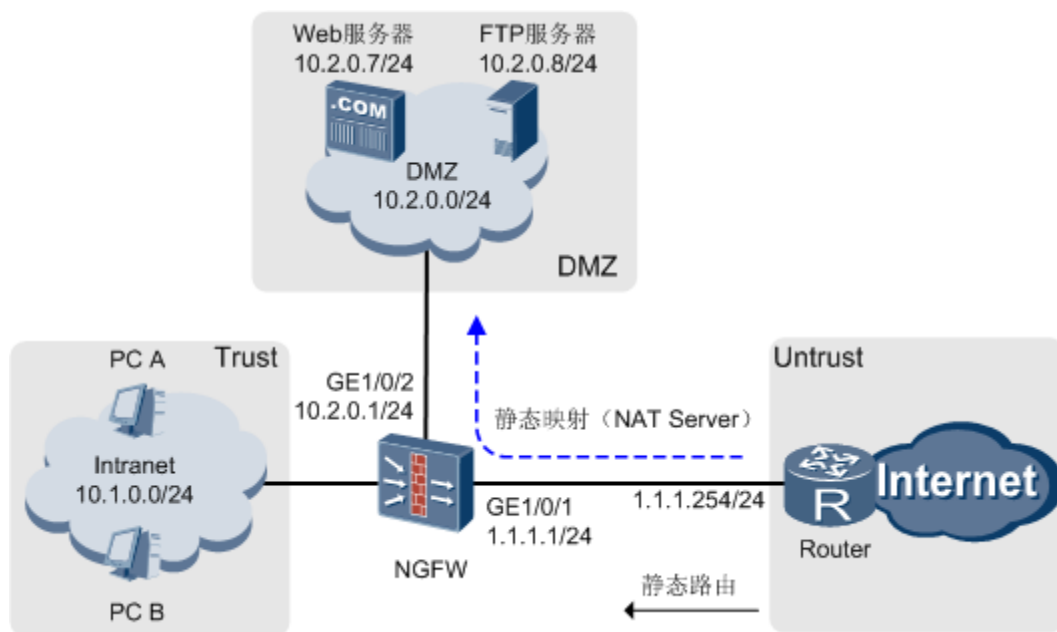
配置了服务器静态映射后，外部网络无法访问内部服务器

服务器静态映射（NAT Server）配置完成后，如果外部网络用户无法访问内部服务器，可以参考本节的内容定位故障，调整配置。

现象描述

如图 1 所示，某公司在网络边界处部署了 NGFW 作为安全网关，通过在 NGFW 上部署服务器静态映射功能，对外发布的 Global 地址为 1.1.1.10，使外部网络中的客户和出差员工可以访问公司的内部网络资源。

图 1 网络环境示意图



实际使用中，发现外部网络中的用户（地址为 3.3.3.3）无法访问内部 FTP 服务器 Server A（地址为 10.2.0.8）。

定位思路

选择“监控 > 会话表”，查询源地址为 3.3.3.3 的表项。根据会话表显示结果可以缩小可能原因的范围，请分别按以下三种情况逐一排查可能原因：

- [没有找到源地址为 3.3.3.3 的会话表。](#)
- [存在会话表项，但是会话表项错误。例如：表项中没有目的地址 1.1.1.10 的转换记录、转换后目的地址不正确。](#)
- [已经建立了正确的会话表项。](#)

处理步骤

没有找到源地址为 3.3.3.3 的会话表项。

可能原因及相应的处理步骤如下：

1. Internet 上没有达到 Global 地址 1.1.1.10 的路由

检查 Internet 中的路由设备是否存在到达 Global 地址的路由。可能需要联系 ISP 管理员确认。

2. Internet 上的其他设备将报文丢弃

检查 Internet 中是否存在设备将报文丢弃，如果存在，请检查并调整该设备的配置信息。

3. NGFW 的基础配置不正确

检查 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 是否配置了正确的 IP 地址并加入了安全区域。

4. NGFW 上配置了黑名单将报文丢弃

选择“策略 > 安全防护 > 黑名单”，搜索目的地址为 1.1.1.10 的表项以及和源地址为 3.3.3.3 的表项。如果找到则删除此表项，否则请进行其他项目的检查。

5. NGFW 上配置的安全策略不正确

选择“策略 > 安全策略 > 安全策略”，查找“源地址”包含 3.3.3.3，“目的地址”包含 1.1.1.10 的表项，存在该条表项且“动作”为“允许”，则该项配置正确，否则请重新调整安全策略的配置。

6. NGFW 上没有配置到达内部服务器的路由

本举例中，内部服务器与 NGFW 直接相连，不涉及路由问题，因此不需要考虑本原因。如果 NGFW 没有直接与内部服务器所在的网络相连，就需要在 NGFW 上配置到达内部服务器的路由。

选择“网络 > 路由 > 路由表”，查找是否存在正确的公网路由表项。

7. NGFW 上没有存在内部服务器的 ARP 表项

内部服务器与 NGFW 直接相连的情况下，如果 NGFW 无法获取内部服务器的 MAC 地址，在丢包统计信息中会出现 ARP miss 字段。此时请您检查内部服务器的 IP 地址设置或者内部服务器与 NGFW 的相连线路的问题。

存在会话表项，但是会话表项错误。例如：表项中没有目的地址 1.1.1.10 的转换记录、转换后目的地址不正确。

可能原因及相应的处理步骤如下：

8. 目的地址没有被转换

选择“策略 > NAT 策略 > 服务器映射”，找到“公网地址”包含 1.1.1.10 的表项。存在该条表项则该项配置正确，否则请重新调整静态映射的配置。

9. 目的地址转换错误

选择“策略 > NAT 策略 > 服务器映射”，找到“公网地址”包含 1.1.1.10 的表项，检查其“私网地址”是否配置正确，否则请重新调整静态映射的配置。

已经建立了正确的会话表项。

可能原因及相应的处理步骤如下：

10. 内部服务器故障

检查内部服务器是否故障，能否正常提供的服务。

检查内部服务器的网关设置是否正确，网关应设置为 NGFW 连接内部服务器所在网络接口的 IP 地址。

11. 内部网络中的其他设备将报文丢弃

检查内部网络中是否存在其他设备将回程的报文丢弃，如果存在，请检查并调整该设备的配置信息。

12. NGFW 上配置了黑名单将回程报文丢弃

请参考 [4](#) 检查处理。

13. NGFW 上没有去往 Internet 的路由

选择“网络 > 路由 > 路由表”，查找是否存在去往 Internet 的路由。

HCIE-Security 模拟面试问题及面试建议

1. 除了静态 NAT、端口 NAT、还有那些 NAT 技术，请说明。
2. 请详细描述各种 NAT 技术原理，画图解释流程。

每一章的 FAQ 都是面试考官喜欢追问的地方^_^

每一章的故障排除也是哦.....