



NGFW 源NAT原理咨询

NAT

王英凯 2023-09-11 发表

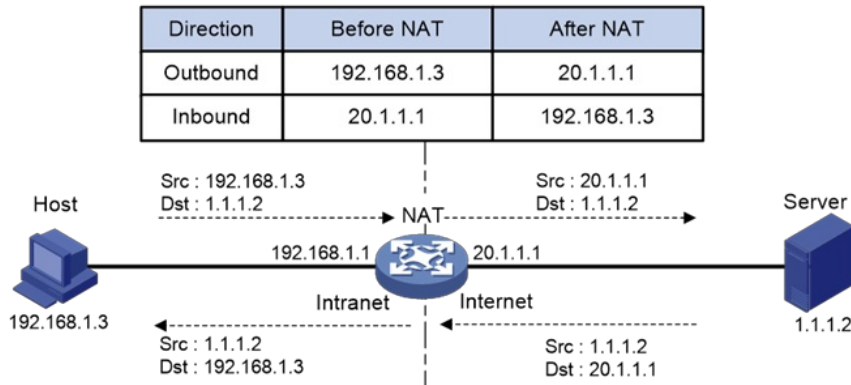
问题描述

NGFW防火墙如何实现源NAT转换?

解决方法

适用系列: 通用

NAT基本工作过程示意图:



如图所示, 一台NAT设备连接内网和外网, 当有报文经过NAT设备时, NAT的基本工作过程如下:

- (2) 当内网用户主机 (192.168.1.3) 向外网服务器 (1.1.1.2) 发送的IP报文通过NAT设备时, NAT设备查看报文的IP头内容, 发现该报文是发往外网的, 则将其源IP地址字段的内网地址192.168.1.3转换为一个可路由的外网地址20.1.1.1, 并将该报文发送给外网服务器, 同时在NAT设备上建立表项记录这一映射关系。
- (3) 外网服务器给内网用户发送的应答报文到达NAT设备后, NAT设备使用报文信息匹配建立的表项, 然后查找匹配到的表项记录, 用内网私有地址192.168.1.3替换初始的目的IP地址20.1.1.1。

上述的NAT过程对终端 (如图中的Host和Server) 来说是透明的。对外网服务器而言, 它认为内网用户主机的IP地址就是20.1.1.1, 并不知道存在192.168.1.3这个地址。因此, NAT“隐藏”了企业的私有网络。

