10
OPTION

安全技术— NAT 配置

讲师：顾荣
Tel：13826101853(微信同号)
Mail： mygurong@126.com

2020.05

NAT 的基本原理

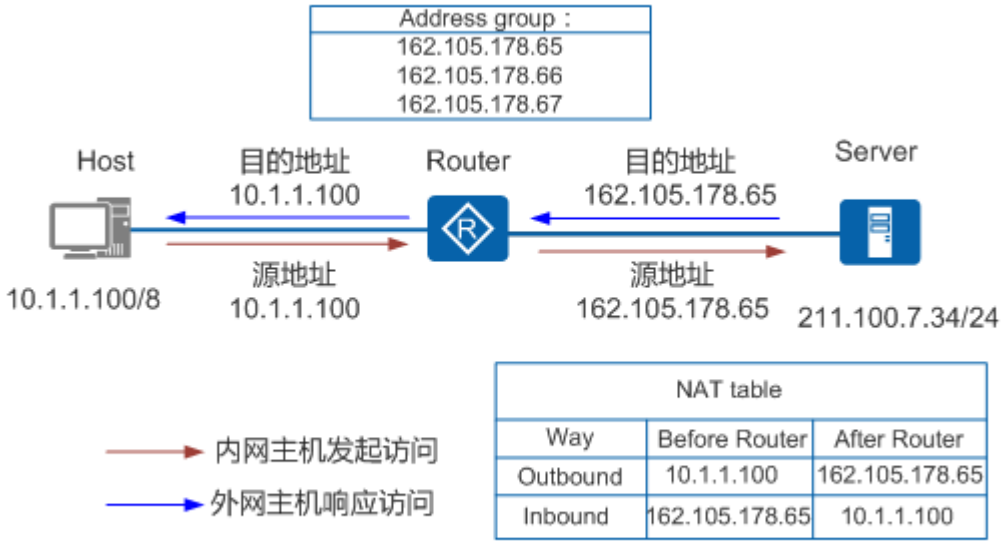
- 网络地址转换 NAT （ Network Address Translation ）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。
- 作用
- 作为减缓 IP 地址枯竭的一种过渡方案， NAT 通过地址重用的方法来满足 IP 地址的需要，可以在一定程度上缓解 IP 地址空间枯竭的压力。 NAT 除了解决 IP 地址短缺的问题，还带来了两个好处：
  - 有效避免来自外网的攻击，可以很大程度上提高网络安全性。
  - 控制内网主机访问外网，同时也可以控制外网主机访问内网，解决了内网和外网不能互通的问题。

NAT 概述

- **Basic NAT**
- Basic NAT 方式属于一对一的地址转换，在这种方式下只转换 IP 地址，而不处理 TCP/UDP 协议的端口号，一个公网 IP 地址不能同时被多个私网用户使用。

- Router 收到内网侧 Host 发送的访问公网侧 Server 的报文，其源 IP 地址为 10.1.1.100 。
- Router 从地址池中选取一个空闲的公网 IP 地址，建立与内网侧报文源 IP 地址间的 NAT 转换表项（正反向），并依据查找正向 NAT 表项的结果将报文转换后向公网侧发送，其源 IP 地址是 162.105.178.65 ，目的 IP 地址是 211.100.7.34 。
- Router 收到公网侧的回应报文后，根据其目的 IP 地址查找反向送，其源 IP 地址是 211.100.7.34 ，目的 IP 地址是 10.1.1.100

图1 Basic NAT示意图



NAT table		
Way	Before Router	After Router
Outbound	10.1.1.100	162.105.178.65
Inbound	162.105.178.65	10.1.1.100

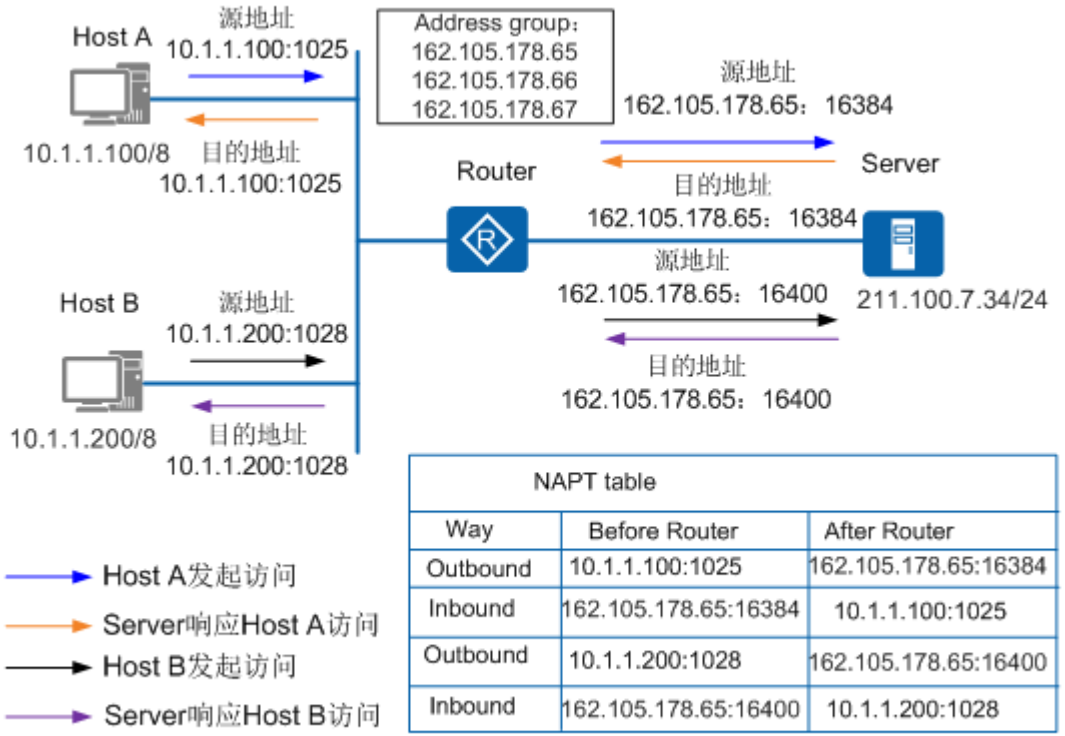
图1描述了Basic NAT的基本原理，实现过程如下：

NAT 概述

- **NAPT**
- 除了一对一的 NAT 转换方式外，网络地址端口转换
  NAPT （ Network Address Port Translation ）可以实现并发的地址转换。它允许多个内部地址映射到同一个公有地址上，因此也可以称为“多对一地址转换”或地址复用。
- NAPT 方式属于多对一的地址转换，它通过使用“ IP 地址＋端口号”的形式进行转换，使多个私网用户可共用一个公网 IP 地址访问外网。

- Router 收到内网侧 Host 发送的访问公网侧 Server 的报文。比如收到 Host A 报文的源地址是 10.1.1.100 ，端口号 1025 。
- Router 从地址池中选取一对空闲的“公网 IP 地址＋端口号”，建立与内网侧报文“源 IP 地址＋源端口号”间的 NAPT 转换表项（正反向），并依据查找正向 NAPT 表项的结果将报文转换后向公网侧发送。比如 Host A 的报文经 Router 转换后的报文源地址为 162.105.178.65 ，端口号 16384 。
- Router 收到公网侧的回应报文后，根据其“目的 IP 地址＋目的端口号”查找反向 NAPT 表项，并依据查表结果将报文转换后向私网侧发送。比如 Server 回应 Host A 的报文经 Router 转换后，目的地址为 10.1.1.100 ，端口号 1025 。

图2 NAPT示意图



NAPT table

Way	Before Router	After Router
Outbound	10.1.1.100:1025	162.105.178.65:16384
Inbound	162.105.178.65:16384	10.1.1.100:1025
Outbound	10.1.1.200:1028	162.105.178.65:16400
Inbound	162.105.178.65:16400	10.1.1.200:1028

图2描述了NAPT的基本原理，实现过程如下：

NAT 实现

- Basic NAT 和 NAPT 是私网 IP 地址通过 NAT 设备转换成公网 IP 地址的过程，分别实现一对一和多对一的地址转换功能。在现网环境下， NAT 功能的实现还得依据 Basic NAT 和 NAPT 的原理， NAT 实现主要包括：

- **Easy IP**

- **地址池 NAT: NAPT/No-PAT**

- **NAT Server**

- **静态 NAT/NAPT**

配置动态地址转换

- **配置地址转换的 ACL 规则**
- **操作步骤**
- 执行命令 **system-view**，进入系统视图。
- 执行命令 **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号创建一个 ACL，并进入 ACL 视图。
- 根据实际情况配置基本 ACL 规则或者高级 ACL 规则。

- **配置出接口的地址关联**
- **背景信息**
- NAT Outbound 所用地址池是用来存放动态 NAT 使用到的 IP 地址的集合，在做动态 NAT 时会选择地址池中的某个地址用做地址转换。
- 如果用户想通过动态 NAT 访问外网时，可以根据自己公网 IP 的规划情况选择以下其中一种方式：
- 用户在配置了 NAT 设备出接口的 IP 和其他应用之后，还有空闲公网 IP 地址，可以选择带地址池的 NAT Outbound 。
- 用户在配置了 NAT 设备出接口的 IP 和其他应用之后，已没有其他可用公网 IP 地址，可以选择 Easy IP 方式， Easy IP 可以借用 NAT 设备出接口的 IP 地址完成动态 NAT 。
- **操作步骤**
- 执行命令 **system-view**，进入系统视图。
- 配置出接口的地址关联，用户根据实际情况选择其中一种配置方法。
  - 配置带地址池的 NAT Outbound:
    - 执行命令 **nat address-group** *group-index start-address end-address* ，配置公网地址池。
    - 执行命令 **interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。
    - 执行命令 **nat outbound** *acl-number* **address-group** *group-index* [**no-pat**]，配置带地址池的 NAT Outbound 。
  - 配置不带地址池的 Easy IP:
    - 执行命令 **interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。
    - 执行命令 **nat outbound** *acl-number* [**interface** *interface-type interface-number* [*.subnumber*]] [**vrrp** *vrrpid*]，配置 Easy IP 。

配置静态地址转换

- **配置静态地址映射**
- **操作步骤**
- 配置静态地址映射分以下两种方式：
- 方式一：在接口视图下配置静态映射：
  - 执行命令 **system-view**，进入系统视图。
  - 执行命令 **interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。
  - 用户根据实际情况选择下面的一条命令执行：
    - **nat static protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]
    - **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]

配置静态地址转换

- 方式二：在系统视图下配置静态映射：
  - 执行命令 **system-view**，进入系统视图。
  - 用户根据实际情况选择下面的一条命令执行：
    - **nat static protocol** { **tcp** | **udp** } **global** *global-address global-port* [*global-port2*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]
    - **nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]
    - **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]
  - 执行命令 **interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。
  - 执行命令 **nat static enable**，在接口下使能 nat static 功能。

检查配置结果

- 执行命令 **display nat alg**，查看 NAT ALG 的配置信息。
- 执行命令 **display nat dns-map** [*domain-name*]，查看 DNS Mapping 信息。
- 执行命令 **display nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }，查看 NAT 双向地址转换的相关信息。
- 执行命令 **display firewall-nat session aging-time**，查看 NAT 表项老化时间的相关信息。
- 执行命令 **display nat static** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-name* [*.subnumber*] | **acl** *acl-number*]，查看 NAT Static 的配置信息。
- 执行命令 **display nat sip cac bandwidth information** [**verbose**]，查看设备上的当前总带宽及被占用带宽。
- 执行命令 **display nat filter-mode**，查看当前的 NAT 过滤方式。
- 执行命令 **display nat mapping-mode**，查看 NAT 映射模式。
- 执行命令 **display nat mapping table** { **all** | **number** } 或者 **display nat mapping table inside-address** *ip-address* **protocol** *protocol-name* **port** *port-number* [**vpn-instance** *vpn-instance-name*]，查看 NAT 映射表所有表项信息或个数。
- 执行命令 **display nat static interface enable**，查看接口下静态 NAT 功能的使能情况。

配置内部服务器

- **操作步骤**
- 执行命令 **system-view**，进入系统视图。
- 执行命令 **interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。
- 根据实际情况，执行其中一条命令配置 NAT Server：
  - **nat server protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]
  - **nat server** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

维护

清除 NAT 映射表项

在确认需要清除 NAT 映射表项后，请在系统视图下执行命令 **reset nat session** { **all** | **transit interface** *interface-type interface-number* [*.subnumber*] } 。

监控 NAT 映射表项

执行命令 **display nat session** { **all** [**verbose**] | **number** } 、 **display nat session protocol** { *protocol-name* | *protocol-number* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**] 、 **display nat session source** *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**] 或 **display nat session destination** *destination-address* [*destination-port*] [**verbose**] ，查看 NAT 的映射表项信息。

THANK YOU

吃透原理 - 认真实践

http://exp.lnc.edu.cn