NAT网络地址转换

使用NAT的原因

- 内外网的隔离
- IPv4地址的短缺
- 内网安全

私网地址范围

- 10.0.0.0~10.255.255.255
- 172.16.0.0~172.31.255.255
- 192.168.0.0~192.168.255.255
- 运营商级私网地址
  - 100.64.0.0 ~100.127.255.255　运营商NAT地址

NAT装换的类型

1、静态NAT

一对一进行地址映射

- 一个私网地址对应一个公网地址
- 使用场景　公司内网一台服务器需要对外网提供某个特定服务
- 实现内外网映射

配置静态NAT

思科

- ip nat　inside　source　static　192.168.1.1　100.1.1.2　静态192.168.1.1地址映射为100.1.1.2
- R2(config)#int　f0/0
  R2(config-if)#ip nat　inside　内网接口配置inside
- R2(config-if)#int　f0/1
  R2(config-if)#ip nat　outside　外网接口配置outside
- ip nat　inside　source　static　tcp　192.168.1.1 3389　100.1.1.3 11111
  外网中如果有一台设备通过远程桌面 100.1.1.3的11111端口，远程的设备其实是192.168.1.1的3389端口

华为

- nat　static　global　100.1.1.99　inside　192.168.1.1
  - 公网接口的IP不能使用静态NAT
  - 如果该命令直接配置在出接口则不需要再在端口下调用
- [R2-GigabitEthernet0/0/1]nat　static enable　出接口开启静态NAT
- nat　static　protocol　tcp　global　100.1.1.3　telnet　inside　192.168.1.1　telnet
  外网中如果有一台设备telnet 100.1.1.3，telnet的设备其实是192.168.1.1　内外网端口映射

缺陷

- 公网IP要求多
- 只能一对一映射
- 配置量大　优化方式　动态NAT

2、动态NAT

使用类似于DHCP的地址池，让NAT自动调用

筛选　acl筛选能够进行NAT的流量

配置

思科

- NAT的地址池　ip nat pool NATPOOL 100.1.1.10 100.1.1.12 netmask 255.255.255.0
- ACL筛选需要NAT的流量　access-list　1　permit　192.168.0.0　0.0.255.255
- 地址池和ACL互相协同工作　ip nat　inside　source　list 1 pool　NATPOOL
- NAT接口调用
  - R2(config)#int　f0/0
    R2(config-if)#ip nat　inside　内网接口配置inside
  - R2(config-if)#int　f0/1
    R2(config-if)#ip nat　outside　外网接口配置outside

华为

- 地址池　nat address-group　1　100.1.1.10　100.1.1.12　地址池只能使用数字
- ACL筛选流量
  acl number 2000
  rule 10 permit source 192.168.0.0 0.0.0.255　华为默认允许所有需要加deny　any
  rule 20　deny　source any
- NAT地址池+ACL调用+不使用端口复用
  interface GigabitEthernet0/0/1
  nat outbound 2000 address-group 1 no-pat　华为默认启用端口复用

缺陷

- 用户数量有限
- 成本高

3、PAT端口复用

PAT　在动态NAT的基础上使用传输层端口号标识不同PC的数据

配置

思科

- NAT的地址池　ip nat pool NATPOOL 100.1.1.10 100.1.1.12 netmask 255.255.255.0
- ACL筛选需要NAT的流量　access-list　1　permit　192.168.0.0　0.0.255.255
- 地址池和ACL互相协同工作+端口复用　ip nat inside source list 1 pool NATPOOL overload
- NAT接口调用
  - R2(config)#int　f0/0
    R2(config-if)#ip nat　inside　内网接口配置inside
  - R2(config-if)#int　f0/1
    R2(config-if)#ip nat　outside　外网接口配置outside

华为

- 地址池　nat address-group　1　100.1.1.10　100.1.1.12　地址池只能使用数字
- ACL筛选流量
  acl number 2000
  rule 10 permit source 192.168.0.0 0.0.0.255　华为默认允许所有需要加deny　any
  rule 20　deny　source any
- NAT地址池+ACL调用+不使用端口复用
  interface GigabitEthernet0/0/1
  nat outbound 2000 address-group 1　华为默认启用端口复用

只使用一个地址

思科

- ACL筛选需要NAT的流量　access-list　1　permit　192.168.0.0　0.0.255.255
- 接口地址和ACL互相协同工作+端口复用　ip nat inside source list 1 pool interface f0/1 overload
- NAT接口调用
  - R2(config)#int　f0/0
    R2(config-if)#ip nat　inside　内网接口配置inside
  - R2(config-if)#int　f0/1
    R2(config-if)#ip nat　outside　外网接口配置outside

华为easy nat

- ACL筛选流量
  acl number 2000
  rule 10 permit source 192.168.0.0 0.0.255.255
  rule 20　deny　source any
- 接口下调用接口IP+ACL+端口复用
  nat outbound 2000
  直接使用该端口的地址NAT