

配置NAT

2016年6月10日 15:26

Juniper SRX上实现NAT功能

只有一个公网IP: 20.1.1.1

服务器30.1.1.2

企业内部网络

10.0.0.10
10.0.0.20
10.0.0.30
10.0.0.40



ISP路由器

位于ISP的路由器没有私有地址条目



作为NAT的设备，会存在一个NAT转换表，记录了IP地址转换前后的一些条目

10.0.0.10:1010	-----	20.1.1.1:1010
10.0.0.20:1010	-----	20.1.1.1:1011

1、源地址转换

转换数据包的源地址，通常应用在内部主机需要访问互联网的时候
单向的，只能由内部主机主动发起访问
可以使得多个私有IP地址共享一个公网地址，节约公网IP地址

2、目标地址转换

转换数据包的目标地址，通常应用在向外发布服务器的时候



web1 TCP80



公网地址: 20.1.1.1

172.16.1.10



web2 TCP80

20.1.1.1:80 ---- 172.16.1.10:80

20.1.1.1:8080 --- 172.16.1.20:80

172.16.1.20

目标地址转换：单向，内部主机无法上网

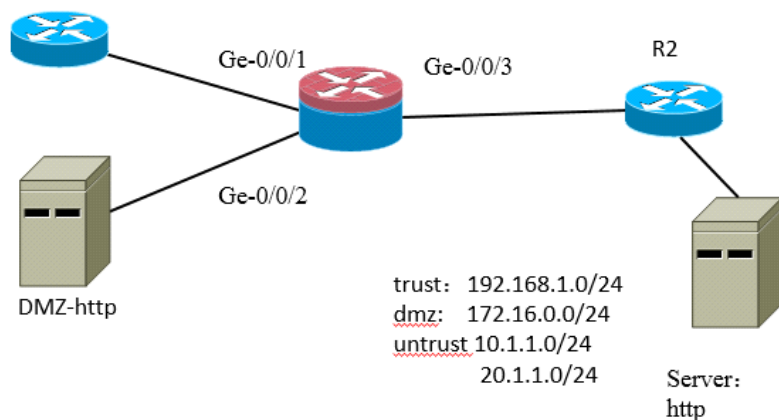
3、静态NAT

双向转换

必须要求内部地址和外部地址的数量是1: 1

在SRX上实现NAT有四种方式

- 1、基于接口的源地址转换
- 2、基于地址池的源地址转换
- 3、基于地址池的目标地址转换
- 4、静态NAT



1、防火墙初始化配置

```
set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 172.16.0.1/24
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
set security policies from-zone trust to-zone untrust policy T-to-U match source-address any
set security policies from-zone trust to-zone untrust policy T-to-U match destination-address any
set security policies from-zone trust to-zone untrust policy T-to-U match application any
set security policies from-zone trust to-zone untrust policy T-to-U then permit
set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic system-services ping
set security zones security-zone dmz interfaces ge-0/0/2.0 host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/3.0 host-inbound-traffic system-services ping
```

基于接口的源地址转换

把内部的私有地址，转换成NAT设备上连接互联网接口的地址

本案例连接互联网的接口是Ge-0/0/3，上面的地址是10.1.1.2

配置命令

```
set security nat source rule-set 1 from zone 转换前地址所属的zone
set security nat source rule-set 1 to zone 转换后地址所属的zone
set security nat source rule-set 1 rule RULE的名字 match source-address 指定转换前的地址段
destination-address 指定目标地址（通常是0.0.0.0/0）
set security nat source rule-set 1 rule RULE的名字 then source-nat interface
```

本案例的配置

```
set security nat source rule-set 1 from zone trust
set security nat source rule-set 1 to zone untrust
set security nat source rule-set 1 rule SNAT-IF match source-address 192.168.1.0/24
set security nat source rule-set 1 rule SNAT-IF match destination-address 0.0.0.0/0
set security nat source rule-set 1 rule SNAT-IF then source-nat interface
```

基于地址池的源地址转换

定义地址池，地址池不能和ISP路由器的直连网段冲突

set security nat source pool POOL的名称 address 起始地址 终止地址

```
set security nat source rule-set 1 from zone 转换前地址所属的zone
set security nat source rule-set 1 to zone 转换后地址所属的zone
set security nat source rule-set 1 rule RULE的名字 match source-address 指定转换前的地址段
destination-address 指定目标地址（通常是0.0.0.0/0）
set security nat source rule-set 1 rule RULE的名字 then source-nat pool POOL的名称
```

配置一个ARP代理

set security nat proxy-arp interface Untrust接口 address 地址池里的起始地址和终止地址

本案例的配置i

```
set security nat source pool POOL30 address 30.1.1.11/32 to 30.1.1.20/32
set security nat source rule-set 1 from zone trust
set security nat source rule-set 1 to zone untrust
set security nat source rule-set 1 rule SNAT-POOL match source-address 192.168.1.0/24
set security nat source rule-set 1 rule SNAT-POOL match destination-address 0.0.0.0/0
set security nat source rule-set 1 rule SNAT-POOL then source-nat pool POOL30
set security nat proxy-arp interface ge-0/0/3.0 address 30.1.1.11/32 to 30.1.1.20/32
```

基于地址池的目标地址转换

```
set security nat destination pool POOL的名称 address 需要发布的内网服务器的地址
set security nat destination rule-set 2 from zone 流量从哪里来
set security nat destination rule-set 2 rule DNAT-POOL match source-address 0.0.0.0/0
set security nat destination rule-set 2 rule DNAT-POOL match destination-address 外网访问的IP地址
set security nat destination rule-set 2 rule DNAT-POOL then destination-nat pool POOL的名称
```

首先放行untrust到dmz的流量，只允许访问TCP-80和TCP-22

```
set security policies from-zone untrust to-zone dmz policy U-to-D match source-address any
set security policies from-zone untrust to-zone dmz policy U-to-D match destination-address 172.16.0.0/24
set security policies from-zone untrust to-zone dmz policy U-to-D match application TCP-80
set security policies from-zone untrust to-zone dmz policy U-to-D match application TCP-22
set security policies from-zone untrust to-zone dmz policy U-to-D then permit
```

配置DNAT，把172.16.1.2映射到30.1.1.2上

```
set security nat destination pool DMZ-POOL address 172.16.0.2/32
set security nat destination rule-set 2 from zone untrust
set security nat destination rule-set 2 rule DNAT-POOL match source-address 0.0.0.0/0
set security nat destination rule-set 2 rule DNAT-POOL match destination-address 30.1.1.2/32
set security nat destination rule-set 2 rule DNAT-POOL then destination-nat pool DMZ-POOL
```

配置静态NAT（建立172.16.1.2和10.1.1.2的双向转换）

```
set security nat static rule-set STATIC-NAT from zone untrust
set security nat static rule-set STATIC-NAT rule RULE1 match destination-address 10.1.1.2/32
set security nat static rule-set STATIC-NAT rule RULE1 then static-nat prefix 172.16.1.2/32
```