手把手教你一步一步配置 Juniper SRX 防火墙基于 IP POOL 的目的地址转换（Dst-NAT）

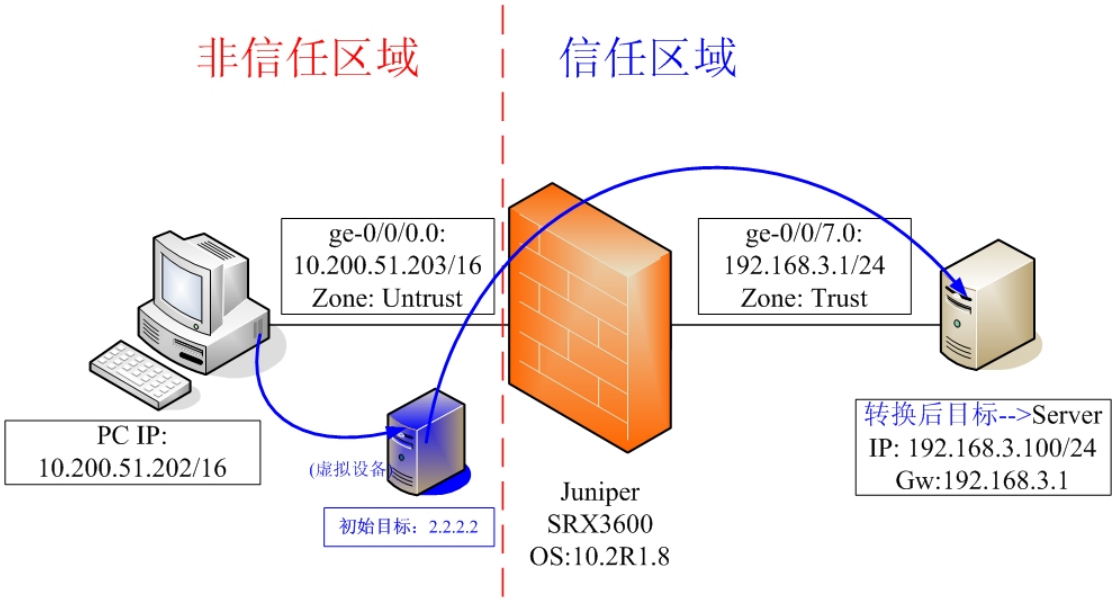
由 wzknet@hotmail.com 原创

Juniper ID：JPR29525 JNCIS-FWV/JNCIS-ER/JNSS-S

SRX 防火墙型号/JUNOS 版本

```
netscreen@SRX3600B> show version
Hostname: SRX3600B
Model: srx3600
JUNOS Software Release [10.2R1.8]
```

网络拓朴如下：



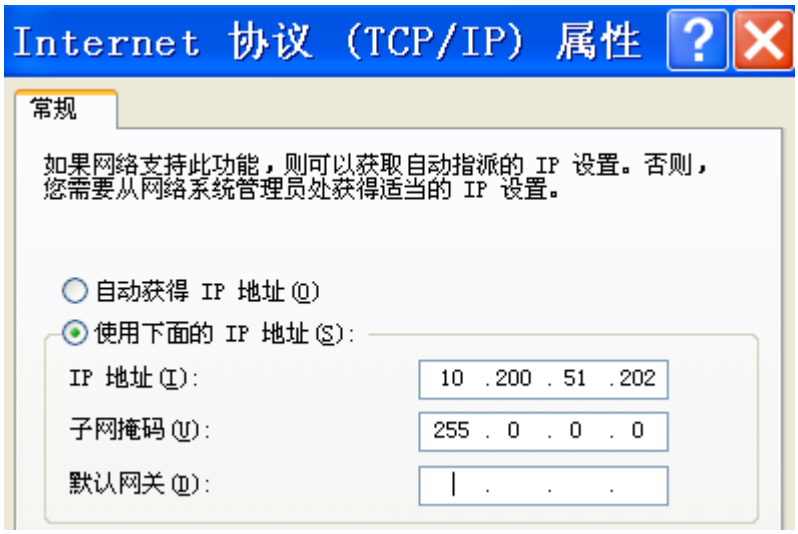
案例说明：

1. Server 操作系统为 Novell SuSe Linux，接在 Juniper SRX3600 防火墙 ge-0/0/7 物理接口上，Server IP：192.168.3.100，网关指向 192.168.3.1。

2. PC 操作系统为 Windows XP，接在 Juniper SRX3600 防火墙 ge-0/0/0 物理接口上，PC IP：10.200.51.202，不设置网关。

3、通过配置基于 IP POOL 的目的地址转换，实现 Pc 访问(ping /telnet)2.2.2.2 时，SRX3600 防火墙自动执行到 192.168.3.100 的目的地址转换。

Pc 设置



C:\>route add 2.2.2.2 mask 255.255.255.255 10.200.51.203

Server IP 和路由设置

```
suse9db:~ # ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:14:2A:33:64:EA
          inet addr:192.168.3.100  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::214:2aff:fe33:64ea/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10061 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30633 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:701245 (684.8 Kb)  TX bytes:2413850 (2.3 Mb)
          Interrupt:11 Memory:fdff8000-0
```

```
suse9db:~ # netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.3.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
0.0.0.0         192.168.3.1     0.0.0.0         UG        0 0          0 eth0
```

SRX 防火墙配置步骤

一、配置 Zones

```
netscreen@SRX3600B# set security zones security-zone trust
netscreen@SRX3600B# set security zones security-zone untrust
```

二、配置接口 IP

```
netscreen@SRX3600B# set interfaces ge-0/0/0 unit 0 family inet address 10.200.51.203/16
netscreen@SRX3600B# set interfaces ge-0/0/7 unit 0 family inet address 192.168.3.1/24
```

三、把接口绑定到 Zones

```
netscreen@SRX3600B# set security zones security-zone untrust interfaces ge-0/0/0.0
netscreen@SRX3600B# set security zones security-zone trust interfaces ge-0/0/7.0
```

四、配置地址本

```
netscreen@SRX3600B# set security zones security-zone trust address-book address Server 192.168.3.100/32
netscreen@SRX3600B# set security zones security-zone untrust address-book address Pc 10.200.51.202/32
```

五、配置基于 IP POOL 的 Dst-NAT

下面配置将 Untrust 10.200.51.202 访问 2.2.2.2 地址映射到内网 192.168.3.100 地址，**注意：定义的 Dst Pool 是内网真实 IP 地址**，而不是映射前的公网地址。这点和 Src-NAT Pool 有所区别。

```
netscreen@SRX3600B# set security nat destination pool testpool address 192.168.3.100/32
netscreen@SRX3600B# set security nat destination rule-set 1 from zone untrust
netscreen@SRX3600B# set security nat destination rule-set 1 rule testrule match source-address 10.200.51.202/32
netscreen@SRX3600B# set security nat destination rule-set 1 rule testrule match destination-address 2.2.2.2/32
netscreen@SRX3600B# set security nat destination rule-set 1 rule testrule then destination-nat pool testpool
```

六、配置策略

```
netscreen@SRX3600B# set security policies from-zone untrust to-zone trust policy 1 match source-address Pc
netscreen@SRX3600B# set security policies from-zone untrust to-zone trust policy 1 match destination-address Server
netscreen@SRX3600B# set security policies from-zone untrust to-zone trust policy 1 match application junos-icmp-ping
netscreen@SRX3600B# set security policies from-zone untrust to-zone trust policy 1 match application junos-telnet
netscreen@SRX3600B# set security policies from-zone untrust to-zone trust policy 1 then permit
```

验证测试

分别在 Pc 上 ping/telnet 2.2.2.2，如下所示：

```
C:\>ping 2.2.2.2  -t

Pinging 2.2.2.2 with 32 bytes of data:

Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
Reply from 2.2.2.2: bytes=32 time<1ms TTL=63
```

```
Telnet 2.2.2.2
Welcome to SUSE LINUX Enterprise Server 9 (i586) - Kernel 2.6.5-7.97-default (3)
.

suse9db login: root
Password:
Last login: Thu Jul 29 18:45:51 from 192.168.3.1
suse9db:~ #
```

查看防火墙会话表：

```
Session ID: 240710642, Policy name: 1/4, Timeout: 2, Valid
  In: 10.200.51.202/2063 --> 2.2.2.2/512;icmp, If: ge-0/0/0.0, Pkts: 1, Bytes: 60
  Out: 192.168.3.100/512 --> 10.200.51.202/2063;icmp, If: ge-0/0/7.0, Pkts: 1, Bytes: 60

Session ID: 240710646, Policy name: 1/4, Timeout: 2, Valid
  In: 10.200.51.202/2319 --> 2.2.2.2/512;icmp, If: ge-0/0/0.0, Pkts: 1, Bytes: 60
  Out: 192.168.3.100/512 --> 10.200.51.202/2319;icmp, If: ge-0/0/7.0, Pkts: 1, Bytes: 60

Session ID: 240710650, Policy name: 1/4, Timeout: 4, Valid
  In: 10.200.51.202/2831 --> 2.2.2.2/512;icmp, If: ge-0/0/0.0, Pkts: 1, Bytes: 60
  Out: 192.168.3.100/512 --> 10.200.51.202/2831;icmp, If: ge-0/0/7.0, Pkts: 1, Bytes: 60
```

```
Flow Sessions on FPC7 PIC0:

Session ID: 140522816, Policy name: 1/4, Timeout: 1744, Valid
  In: 10.200.51.202/5449 --> 2.2.2.2/23;tcp, If: ge-0/0/0.0, Pkts: 28, Bytes: 1198
  Out: 192.168.3.100/23 --> 10.200.51.202/5449;tcp, If: ge-0/0/7.0, Pkts: 28, Bytes: 1353
Total sessions: 1
```

查看基于 IP POOL 的 Dst-NAT Translation hits 数量

```
netscreen@SRX3600B> show security nat destination rule all
Total destination-nat rules: 1

Destination NAT rule: testrule                Rule-set: 1
  Rule-Id                      : 1
  Rule position                : 1
  From zone                    : untrust
  Match
    Source addresses           : 10.200.51.202    - 10.200.51.202
    Destination addresses      : 2.2.2.2          - 2.2.2.2
  Action                       : testpool
  Destination port             : 0
  Translation hits             : 19
```

```
netscreen@SRX3600B> show security nat destination pool all
Total destination-nat pools: 1

Pool name         : testpool
Pool id           : 1
Routing instance: default
Total address     : 1
Translation hits: 19
Address range                                 Port
  192.168.3.100 - 192.168.3.100                  0
```

```
netscreen@SRX3600B> show security nat destination summary
Total pools: 1
Pool name            Address                                 Routing        Port  Total
                     Range                                   Instance             Address
testpool             192.168.3.100   - 192.168.3.100         default        0     1

Total rules: 1
Rule name            Rule set        From                                  Action
testrule             1               untrust                               testpool
```

```
netscreen@SRX3600B> show security flow session session-identifier 140522816
Flow Sessions on FPC7 PIC0:

Session ID: 140522816, Status: Normal
Flag: 0x4000000
Policy name: 1/4
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1416
Session State: Valid
Start time: 1415383, Duration: 387
   In: 10.200.51.202/5449 --> 2.2.2.2/23;tcp,
    Interface: ge-0/0/0.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0xb0010, Gateway: 10.200.51.202, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 28, Bytes: 1198
   Out: 192.168.3.100/23 --> 10.200.51.202/5449;tcp,
    Interface: ge-0/0/7.0,
    Session token: 0x200, Flag: 0x0x20
    Route: 0x70010, Gateway: 192.168.3.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 28, Bytes: 1353
Total sessions: 1
```

版本申明

转载请注明原始出自 http://k968888.blog.sohu.com

2010 年 7 月 29 日　　广州