

IT Technology 2. sem

Assignment 01 **Source Nat**



.....

University College

Authors

Tihamer Biliboc

tiha0006@edu.eal.dk

Sebastian Thomle Mason

seba7286@edu.eal.dk

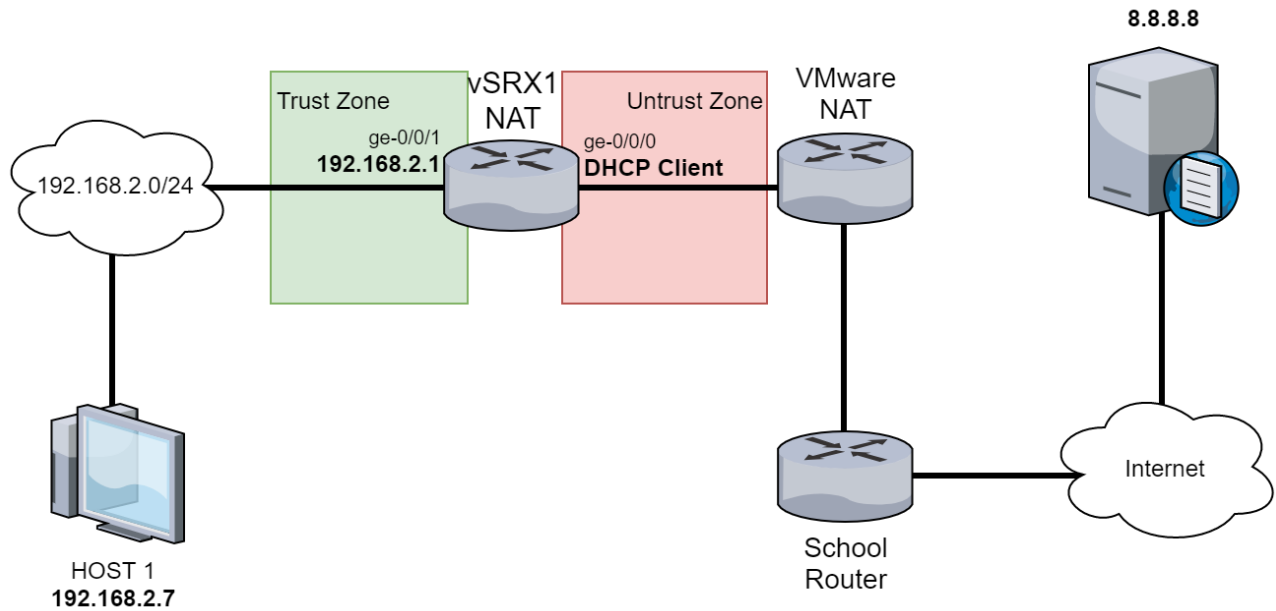
Anthony James Peak

anth0662@edu.eal.dk

Table of Contents

A topology diagram with explanation.	2
One screenshots and descriptions of how to set up the SRX router(s) in VMware.	3
One screenshot and description of how to configure the used PCs.	4
One screenshot, description, and commands on how to configure the SRX router(s) with PAT for relevant subnet(s).	5
Show how ping was used for troubleshooting.	6
Show how traceroute was used for troubleshooting.	7
Run Wireshark and show one screenshot/description that proves that the NATTING for all subnets is working.	8

A topology diagram with explanation.



The vSRX1 router is configured to use Port Address Translation (PAT), allowing the private network infrastructure behind the “Trust Zone” to be hidden from the network infrastructure beyond the untrust zone. The Google DNS server (8.8.8.8) is added as a target for test pings.

One screenshots and descriptions of how to set up the SRX router(s) in VMware.

```
root@% cli
root> edit
Entering configuration mode

[edit]
root# edit security nat source
t rule-set rs1 fr
om zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat interface
top
edit security policies from-zone trust to-zone untrust
set policy internet-access match source-address any destination-address any application any
set policy internet-access then permit
[edit security nat source]
root# set rule-set rs1 from zone trust

[edit security nat source]
root# set rule-set rs1 to zone untrust

[edit security nat source]
root# set rule-set rs1 rule r1 match source-address 0.0.0.0/0

[edit security nat source]
root# set rule-set rs1 rule r1 match destination-address 0.0.0.0/0

[edit security nat source]
root# set rule-set rs1 rule r1 then source-nat interface

[edit security nat source]
root# top

[edit]
root# edit security policies from-zone trust to-zone untrust

[edit security policies from-zone trust to-zone untrust]
root# ...ress any destination-address any application any

[edit security policies from-zone trust to-zone untrust]
root# set policy internet-access then permit

[edit security policies from-zone trust to-zone untrust]
root#
```

```
[edit]
edit security nat source
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat interface
top
edit security policies from-zone trust to-zone untrust
set policy internet-access match source-address any destination-address any
application any
set policy internet-access then permit
```

One screenshot and description of how to configure the used PCs.

Editing Wired connection 2

Connection name: **Wired connection 2**

General | Ethernet | 802.1X Security | DCB | Proxy | IPv4 Settings | IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.2.7	24	192.168.2.1

Add
Delete

DNS servers: 8.8.8.8

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

Open network settings and edit the connection to match the above.

One screenshot, description, and commands on how to configure the SRX router(s) with PAT for relevant subnet(s).

```
nat {
  source {
    rule-set rs1 {
      from zone trust;
      to zone untrust;
      rule r1 {
        match {
          source-address 0.0.0.0/0;
          destination-address 0.0.0.0/0;
        }
        then {
          source-nat {
            interface;
          }
        }
      }
    }
  }
}
```

```
[edit]
edit security nat source
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat interface
top
edit security policies from-zone trust to-zone untrust
set policy internet-access match source-address any destination-address any
application any
set policy internet-access then permit
```

Show how ping was used for troubleshooting.

```
Terminal - root1@ubuntu: ~
File Edit View Terminal Tabs Help
root1@ubuntu:~$ ping google.com -c 10
PING google.com (172.217.17.142) 56(84) bytes of data.
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=1 ttl=127 time=40.1 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=2 ttl=127 time=31.5 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=3 ttl=127 time=27.5 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=4 ttl=127 time=31.3 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=5 ttl=127 time=31.3 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=6 ttl=127 time=31.2 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=7 ttl=127 time=30.7 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=8 ttl=127 time=39.2 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=9 ttl=127 time=27.5 ms
64 bytes from ams15s30-in-f14.1e100.net (172.217.17.142): icmp_seq=10 ttl=127 time=27.6 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9028ms
rtt min/avg/max/mdev = 27.550/31.841/40.165/4.247 ms
```

Ping was used for verifying connections in the network as well as testing connections at the end.

Show how traceroute was used for troubleshooting.

```
root1@ubuntu:~$ traceroute google.com
traceroute to google.com (172.217.17.110), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  3.095 ms  3.069 ms  3.030 ms
 2  192.168.248.2 (192.168.248.2)  3.342 ms  3.308 ms  3.391 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  *^C
```

Traceroute was not used during this assignment.

After the assignment was done, traceroute showed the above when tracerouting outside the local network. Most likely a problem with the untrust-to-trust security policy.

Run Wireshark and show one screenshot/description that proves that the NATTING for all subnets is working.

1	0.000000	192.168.2.7	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=1/256, ttl=64 (reply in 2)
2	0.037242	8.8.8.8	192.168.2.7	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=1/256, ttl=127 (request in 1)
3	1.006235	192.168.2.7	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=2/512, ttl=64 (reply in 4)
4	1.037665	8.8.8.8	192.168.2.7	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=2/512, ttl=127 (request in 3)
5	2.010518	192.168.2.7	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=3/768, ttl=64 (reply in 6)
6	2.041816	8.8.8.8	192.168.2.7	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=3/768, ttl=127 (request in 5)
7	3.017672	192.168.2.7	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=4/1024, ttl=64 (reply in 8)
8	3.056875	8.8.8.8	192.168.2.7	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=4/1024, ttl=127 (request in 7)
9	4.023278	192.168.2.7	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=5/1280, ttl=64 (reply in 10)
10	4.054755	8.8.8.8	192.168.2.7	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=5/1280, ttl=127 (request in 9)

Img1: Between Host1 and vSRX1

3	9.887009	192.168.248.131	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=31854/28284, ttl=63 (reply in 4)
4	9.923066	8.8.8.8	192.168.248.131	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=31854/28284, ttl=128 (request in 3)
5	10.892421	192.168.248.131	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=21842/21077, ttl=63 (reply in 6)
6	10.917387	8.8.8.8	192.168.248.131	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=21842/21077, ttl=128 (request in 5)
7	11.900552	192.168.248.131	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=31994/64124, ttl=63 (reply in 8)
8	11.923947	8.8.8.8	192.168.248.131	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=31994/64124, ttl=128 (request in 7)
9	12.907793	192.168.248.131	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=21524/5204, ttl=63 (reply in 10)
10	12.935961	8.8.8.8	192.168.248.131	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=21524/5204, ttl=128 (request in 9)
11	13.909547	192.168.248.131	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0b7a, seq=24809/59744, ttl=63 (reply in 12)
12	13.936154	8.8.8.8	192.168.248.131	ICMP	98 Echo (ping) reply	id=0x0b7a, seq=24809/59744, ttl=128 (request in 11)

Img2: Between vSRX1 and internet

As seen above, when Host1(192.168.2.7) pings 8.8.8.8 in *Img1*, the router(vSRX1) changes the src-ip to the routers ip(192.168.248.131) in *Img2*.

When 8.8.8.8 then replies, it sends the reply to the router which then changes the dst-ip to Host1's ip.