IT Technology 2. sem

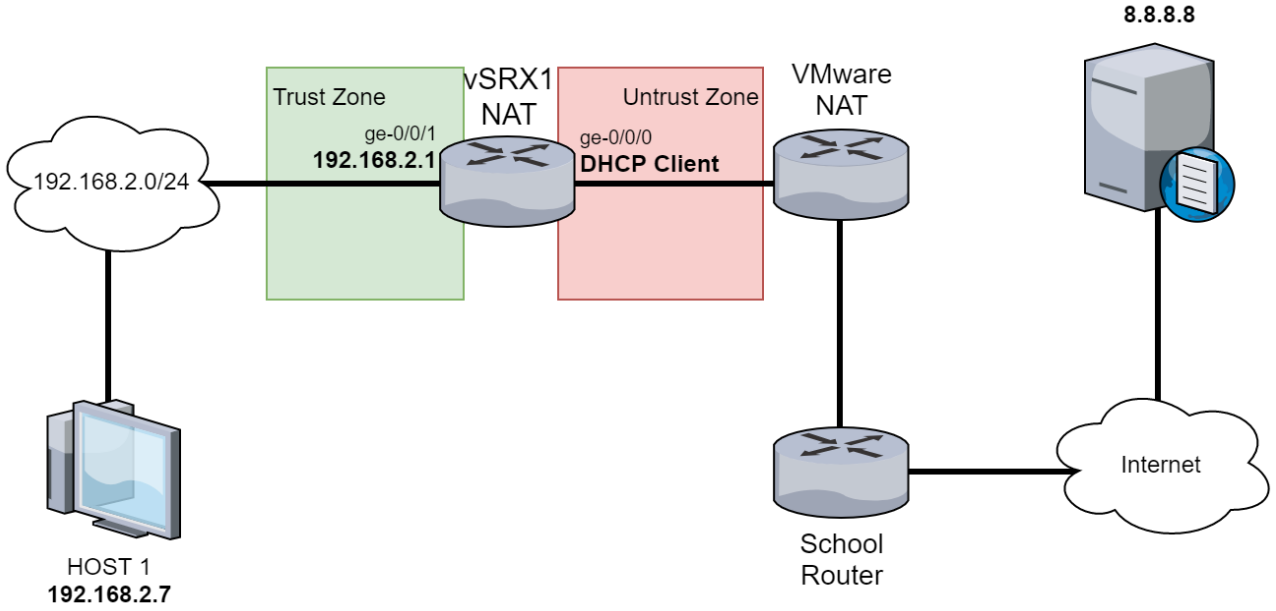
Assignment 01
Source Nat

Authors
Tihamer Biliboc
tiha0006@edu.eal.dk
Sebastian Thomle Mason
seba7286@edu.eal.dk
Anthony James Peak
anth0662@edu.eal.dk

Sunday 10 Feb 2019

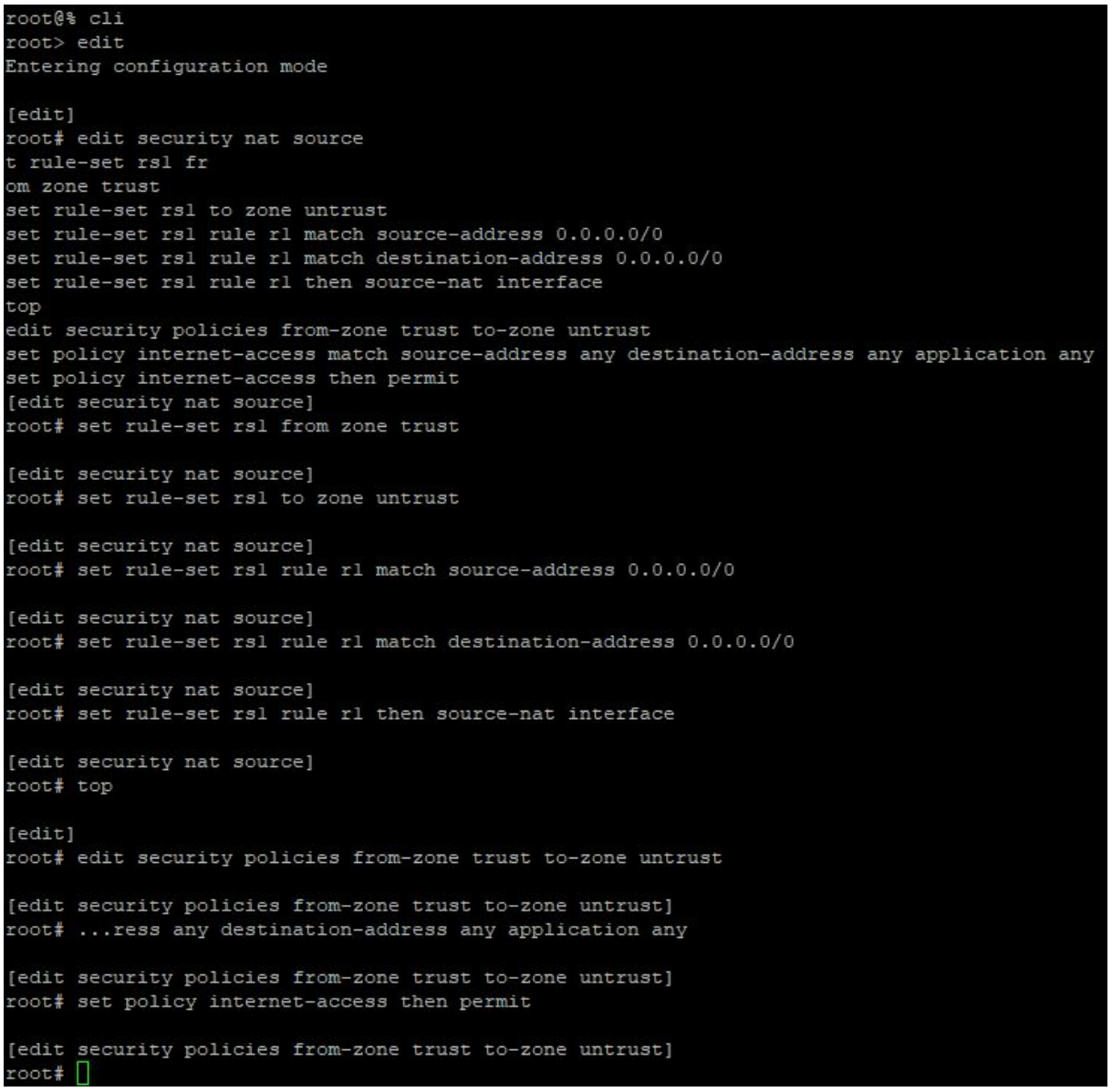
Table of Contents

A topology diagram with explanation.



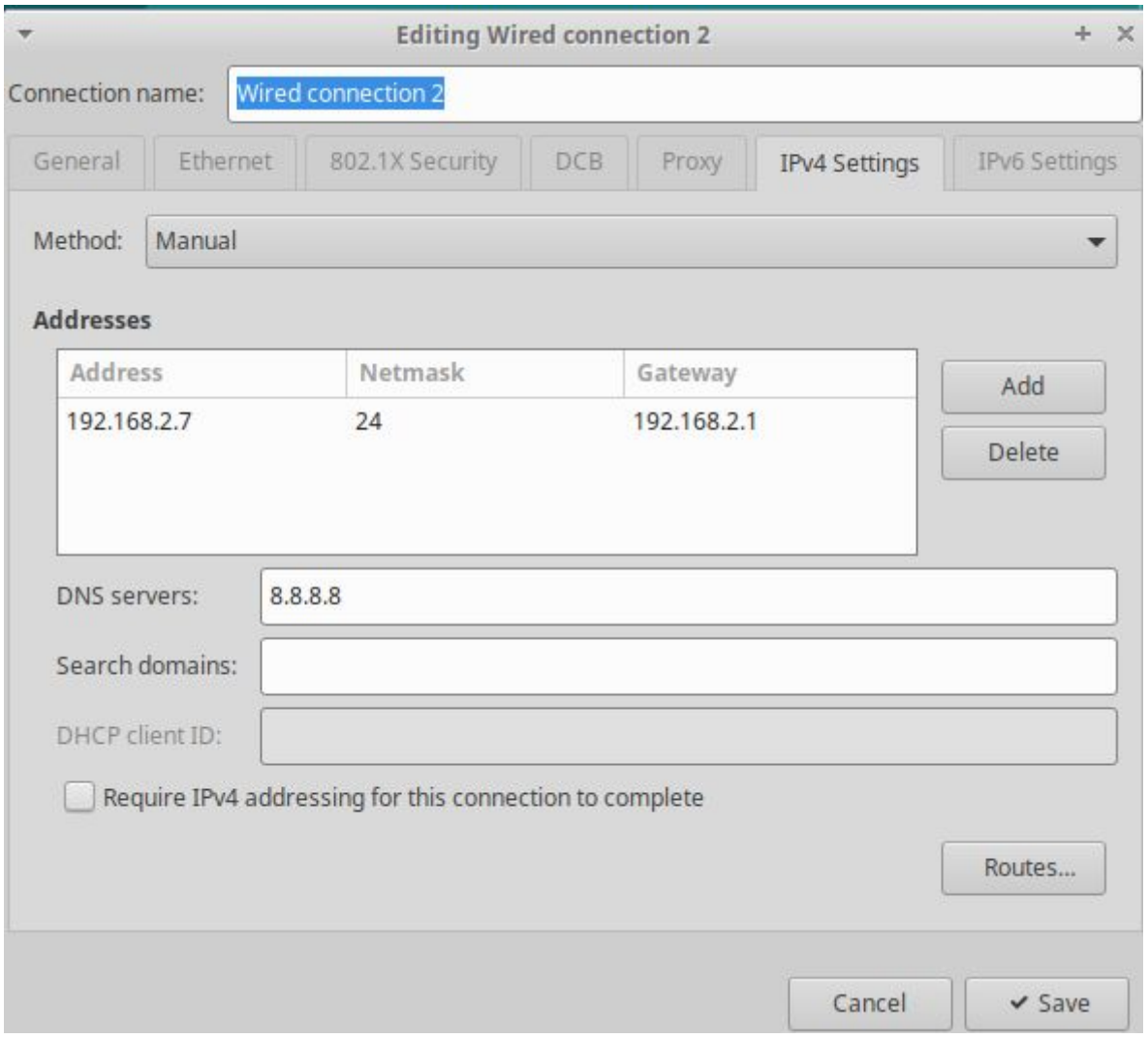
The vSRX1 router is configured to use Port Address Translation (PAT), allowing the private network infrastructure behind the “Trust Zone” to be hidden from the network infrastructure beyond the untrust zone. The Google DNS server (8.8.8.8) is added as a target for test pings.

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



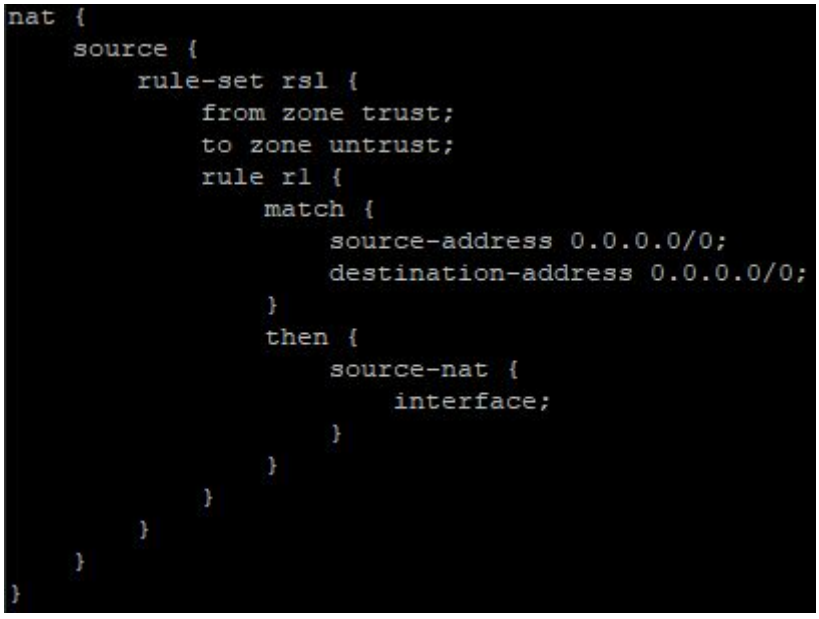

```
[edit]
edit security nat source
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat interface
top
edit security policies from-zone 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.



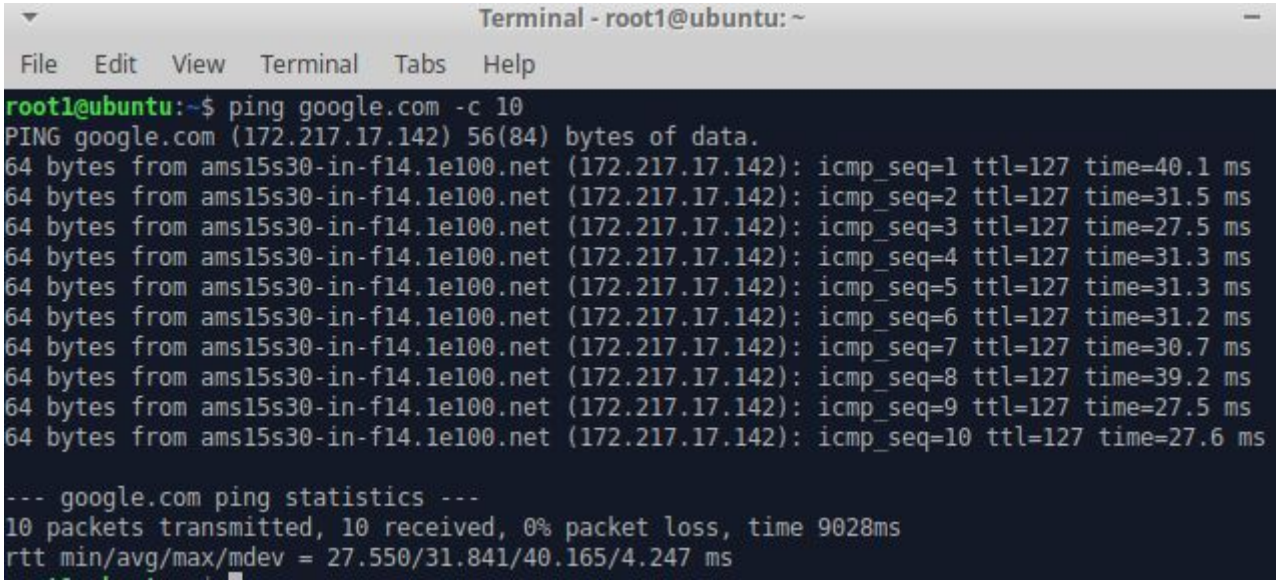
Open network settings and edit the connection to match the above.

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



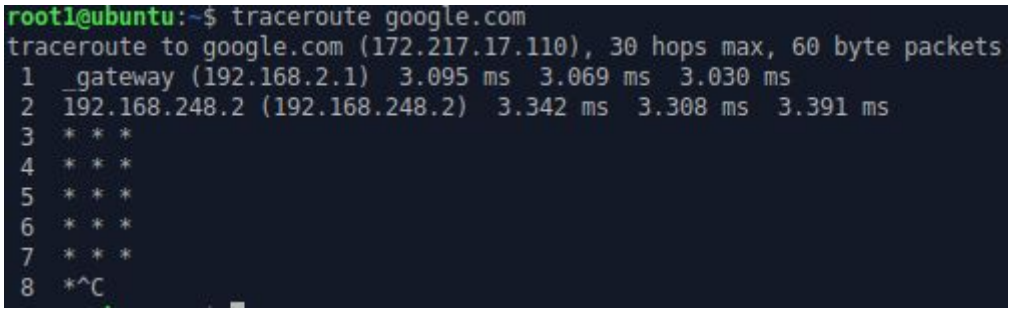

```
[edit]
edit security nat source
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat interface
top
edit security policies from-zone 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.



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

Show how traceroute was used for troubleshooting.



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.