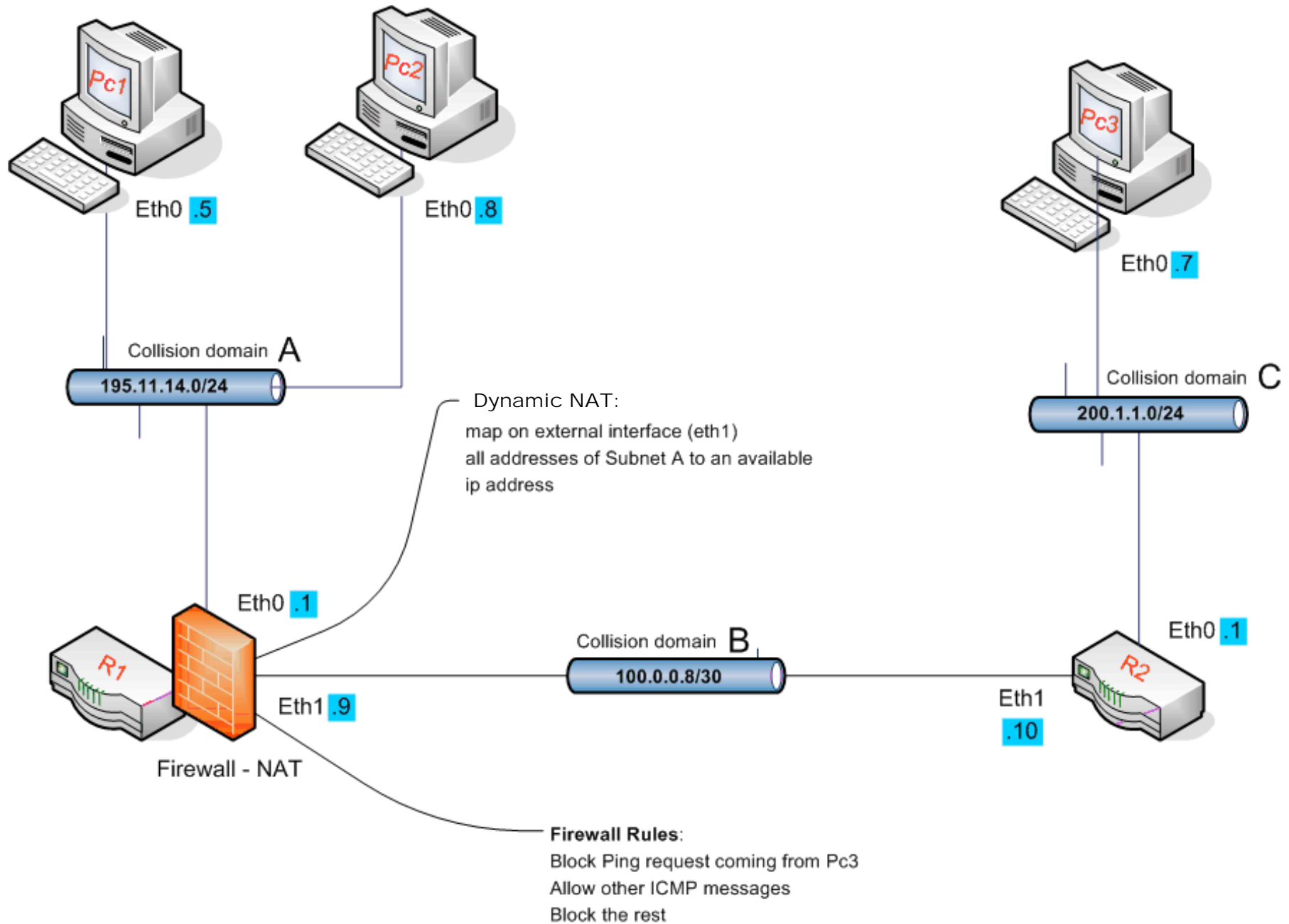


Static routing featuring firewall  
and NAT functions

# Network Configuration



# Firewall configuration

```
<FwallConf>
  <link>r_1</link>    [machine mounting this firewall]
  <acl>
    <name>static_demo</name>
    <effect>demonstration of firewall rules and
              Nat</effect>
    <policy>deny</policy>  [Block everything by default]

    <construct description=".." name="icmp">
      ... [Filtering rules]
    </construct>

    <Nat>
      ... [Nat functions]
    </Nat>

  </acl>
</FwallConf>
```

# Firewall configuration

Sample filtering rule:

block echo-request messages from pc3

```
<rule id="block_echo_pc3">  
  <action> deny </action>  
  <protocol> icmp </protocol>  
  <source> 200.1.1.7 </source>  
  <destination> any </destination>  
  <options>  
    <IcmpType> echo-request </IcmpType>  
  </options>  
</rule>  
. . .
```

# Firewall configuration

Sample filtering rule:

translation for iptables firewall

```
sbin/iptables -A INPUT -s 200.1.1.7 -d 0/0 -p icmp  
-j DROP --icmp-type echo-request
```

```
/sbin/iptables -A FORWARD -s 200.1.1.7 -d 0/0 -p icmp  
-j DROP --icmp-type echo-request
```

```
/sbin/iptables -A OUTPUT -s 200.1.1.7 -d 0/0 -p icmp  
-j DROP --icmp-type echo-request
```

# Firewall configuration

## Dynamic NAT

```
<nat>  
  <translate interface="eth1"/>  
</nat>  
. . .
```

Or

## Static NAT

```
<nat>  
  <translate interface="eth1">  
    100.0.0.9  
  </translate>  
</nat>  
. . .
```

# Firewall configuration

## Dynamic NAT translation

```
# NAT
/sbin/iptables -t nat -A POSTROUTING -o eth1
-j MASQUERADE
# (Dynamic NAT)
```

## Static NAT translation

```
# NAT
/sbin/iptables -t nat -A POSTROUTING -o eth1
-j SNAT --to 100.0.0.9
# (Static NAT)
```

# Firewall configuration

## Checking iptables chains

```
r_1-r1:~# iptables -L
Chain INPUT (policy DROP)
target      prot opt source          destination
DROP        icmp -- 200.1.1.7       anywhere
icmp echo-request
ACCEPT      icmp -- anywhere        anywhere
icmp echo-request
ACCEPT      icmp -- anywhere        anywhere
icmp echo-reply
ACCEPT      icmp -- anywhere        anywhere
icmp time-exceeded

Chain FORWARD (policy DROP)
. . .
Chain OUTPUT (policy DROP)
. . .
```

# Test 1

## Ping pc3 from pc2

```
r_pc2-pc2:~# ping -c 3 200.1.1.7
PING 200.1.1.7 (200.1.1.7) 56(84) bytes of data.
64 bytes from 200.1.1.7: icmp_seq=1 ttl=62 time=3.58 ms
64 bytes from 200.1.1.7: icmp_seq=2 ttl=62 time=1.34 ms
64 bytes from 200.1.1.7: icmp_seq=3 ttl=62 time=1.80 ms

--- 200.1.1.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 1.346/2.246/3.586/0.966 ms
```

- Echo-request from pc2 and echo-reply from pc3 allowed by the firewall

# Test 1

## Sniffing traffic on r2

```
r_2-r2:~# tcpdump
16:08:21.569790 IP 100.0.0.9 > 200.1.1.7: icmp 64: echo request seq 1
16:08:21.570036 IP 200.1.1.7 > 100.0.0.9: icmp 64: echo reply seq 1
16:08:22.577808 IP 100.0.0.9 > 200.1.1.7: icmp 64: echo request seq 2
16:08:21.578169 IP 200.1.1.7 > 100.0.0.9: icmp 64: echo reply seq 2
16:08:23.589676 IP 100.0.0.9 > 200.1.1.7: icmp 64: echo request seq 3
16:08:21.590342 IP 200.1.1.7 > 100.0.0.9: icmp 64: echo reply seq 3
```

- The address showed outside the firewall is not pc1's, but it's the address of r1 (100.0.0.9)
- This is because NAT is active on interface eth1 of r1
- Pc1's address is hidden

# Test 2

## Ping pc1 from pc3

```
r_pc2-pc3:~# ping -c 3 195.11.14.5  
PING 195.11.14.5 (195.11.14.5) 56(84) bytes of data.  
--- 195.11.14.5 ping statistics ---  
3 packets transmitted, 0 received, 100% packet loss, time  
2015ms
```

- Echo-request from pc3 is not allowed by the firewall

# Test 2

## Sniffing traffic on r2

```
r_2-r2:~# tcpdump  
16:09:50.656701 IP 200.1.1.7 > 195.11.14.5: icmp 64: echo request seq 1  
16:09:51.671021 IP 200.1.1.7 > 195.11.14.5: icmp 64: echo request seq 2  
16:09:52.671809 IP 200.1.1.7 > 195.11.14.5: icmp 64: echo request seq 3
```

- No echo-reply answer is given