-------------PC1-------------

```
ip 10.2.2.100/24 10.2.2.10
save
```

-------------PC2-------------

```
ip 200.2.2.100/24 200.2.2.10
save
```

-------------ROUTER INSIDE-------------

```
conf t
interface f0/1
ip address 10.2.2.10 255.255.255.0
no shutdown
interface f0/0
ip address 10.1.1.10 255.255.255.0
no shutdown
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 0.0.0.0 0.0.0.0 10.1.1.2

end
write
```

-------------ROUTER OUTSIDE-------------

```
conf t
interface f0/1
ip address 200.2.2.10 255.255.255.0
no shutdown
interface f0/0
ip address 200.1.1.10 255.255.255.0
no shutdown
ip route 192.1.0.0 255.255.254.0 200.1.1.1
ip route 192.1.0.0 255.255.254.0 200.1.1.2

end
write
```

-------------LB1A-------------

```
sudo cp /opt/vyatta/etc/config.boot.default /config/config.boot
reboot

configure
```

```
set system host-name LB1A
set interfaces ethernet eth0 address 10.1.1.1/24
set interfaces ethernet eth1 address 10.1.2.1/24
set interfaces ethernet eth2 address 10.1.3.1/24
set interfaces ethernet eth3 address 10.1.4.1/24

set high-availability vrrp group LB1Cluster vrid 1
set high-availability vrrp group LB1Cluster interface eth1
set high-availability vrrp group LB1Cluster virtual-address 10.1.2.1/24
set high-availability vrrp sync-group LB1Cluster member LB1Cluster
set high-availability vrrp group LB1Cluster rfc3768-compatibility
```

(para as firewalls)

```
set load-balancing wan interface-health eth2 nexthop 10.1.3.2
set load-balancing wan interface-health eth3 nexthop 10.1.4.2

set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 protocol all
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat

set protocols static route 10.2.2.0/24 next-hop 10.1.1.10

set service conntrack-sync accept-protocol tcp,udp,icmp
set service conntrack-sync failover-mechanism vrrp sync-group LB1Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache

commit
save
exit
```

-------------LB1B-------------

```
set system host-name LB1B
set interfaces ethernet eth0 address 10.1.1.2/24
set interfaces ethernet eth1 address 10.1.2.2/24
set interfaces ethernet eth2 address 10.2.0.1/24
set interfaces ethernet eth3 address 10.2.1.1/24

set protocols static route 10.2.2.0/24 next-hop 10.1.1.10
set high-availability vrrp group LB1Cluster vrid 1
set high-availability vrrp group LB1Cluster interface eth1
set high-availability vrrp group LB1Cluster virtual-address 10.1.2.1/24
set high-availability vrrp sync-group LB1Cluster member LB1Cluster
set high-availability vrrp group LB1Cluster rfc3768-compatibility

(para as firewalls)
set load-balancing wan interface-health eth2 nexthop 10.2.0.2
set load-balancing wan interface-health eth3 nexthop 10.2.1.2

set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 protocol all
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat


set service conntrack-sync accept-protocol tcp,udp,icmp
set service conntrack-sync failover-mechanism vrrp sync-group LB1Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache

commit
save
exit
```

-------------LB2A-------------

```
set system host-name LB2A
set interfaces ethernet eth0 address 200.1.1.1/24
set interfaces ethernet eth1 address 10.5.0.1/24
set interfaces ethernet eth2 address 10.3.0.2/24
set interfaces ethernet eth3 address 10.4.1.2/24

set protocols static route 200.2.2.0/24 next-hop 200.1.1.10

set high-availability vrrp group LB2Cluster vrid 2
set high-availability vrrp group LB2Cluster interface eth1
set high-availability vrrp group LB2Cluster virtual-address 192.168.100.1/24
set high-availability vrrp sync-group LB2Cluster member LB2Cluster
set high-availability vrrp group LB2Cluster rfc3768-compatibility

set load-balancing wan interface-health eth2 nexthop 10.3.0.1
set load-balancing wan interface-health eth3 nexthop 10.4.1.1

set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 protocol all
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat


set service conntrack-sync accept-protocol tcp,udp,icmp
set service conntrack-sync failover-mechanism vrrp sync-group LB2Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache

commit
save
exit
```

-------------LB2B-------------

```
set system host-name LB2B
set interfaces ethernet eth0 address 200.1.1.2/24
set interfaces ethernet eth1 address 10.5.0.2/24
set interfaces ethernet eth2 address 10.3.1.2/24
set interfaces ethernet eth3 address 10.4.0.2/24

set protocols static route 200.2.2.0/24 next-hop 200.1.1.10

set high-availability vrrp group LB2Cluster vrid 2
set high-availability vrrp group LB2Cluster interface eth1
set high-availability vrrp group LB2Cluster virtual-address 192.168.100.1/24
set high-availability vrrp sync-group LB2Cluster member LB2Cluster
set high-availability vrrp group LB2Cluster rfc3768-compatibility

set load-balancing wan interface-health eth2 nexthop 10.3.1.1
set load-balancing wan interface-health eth3 nexthop 10.4.0.1

set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 protocol all
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat

set service conntrack-sync accept-protocol tcp,udp,icmp
set service conntrack-sync failover-mechanism vrrp sync-group LB2Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache
```

```
commit
save
exit
```

-------------FW1-------------

```
configure
set system host-name FW1
set interfaces ethernet eth0 address 10.1.3.2/24
set interfaces ethernet eth1 address 10.2.0.2/24
set interfaces ethernet eth2 address 10.3.0.1/24
set interfaces ethernet eth3 address 10.3.1.1/24
set int eth eth4 add 192.1.1.200/24

***** Configurar NAT *****
set nat source rule 10 outbound-interface eth2
set nat source rule 10 source address 10.0.0.0/8
set nat source rule 10 translation address 192.1.0.1-192.1.0.10

set nat source rule 20 outbound-interface eth3
set nat source rule 20 source address 10.0.0.0/8
set nat source rule 20 translation address 192.1.0.11-192.1.0.20

***** Definir Static routes *****
set protocols static route 0.0.0.0/0 next-hop 10.3.0.2
set protocols static route 0.0.0.0/0 next-hop 10.3.1.2
set protocols static route 10.2.2.0/24 next-hop 10.1.3.1
set protocols static route 10.2.2.0/24 next-hop 10.2.0.1

set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth0
set zone-policy zone INSIDE interface eth1
set zone-policy zone DMZ description "DMZ (Server Farm)"
set zone-policy zone DMZ interface eth4
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth2
set zone-policy zone OUTSIDE interface eth3


set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 description "streaming ports access 5000-6000"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol udp
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 destination port 5000-6000

set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 description "Inside network access for HTTP and HTTPS through TCP"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 protocol tcp
set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 destination port 80,443

set firewall name FROM-DMZ-TO-INSIDE rule 10 action accept
set firewall name FROM-DMZ-TO-INSIDE rule 10 description "Accept established-related connections"
set firewall name FROM-DMZ-TO-INSIDE rule 10 state established enable
set firewall name FROM-DMZ-TO-INSIDE rule 10 state related enable

set firewall name FROM-DMZ-TO-OUTSIDE rule 10 action accept
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 description "Accept Established-related connections"
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state established enable
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state related enable

set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 action accept
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 description "Accept Established-related connections"
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state established enable
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state related enable

set firewall name FROM-INSIDE-TO-DMZ rule 10 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 10 description "Accept ICMP packets to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 10 icmp type 8
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol icmp

set firewall name FROM-INSIDE-TO-DMZ rule 12 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 12 description "Accept HTTP and HTTPS from INSIDE to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 12 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 12 destination port 80,443
set firewall name FROM-INSIDE-TO-DMZ rule 12 protocol tcp


set firewall name FROM-INSIDE-TO-DMZ rule 30 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 30 description "Allow DNS access to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination port 53
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol udp

set firewall name FROM-INSIDE-TO-DMZ rule 15 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 15 description "Accept HTTP, HTTPS and SSH from INSIDE to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 15 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 15 destination port 22,80,443
set firewall name FROM-INSIDE-TO-DMZ rule 15 protocol tcp
set firewall name FROM-INSIDE-TO-DMZ rule 15 source address 10.2.2.0/2



set zone-policy zone OUTSIDE from INSIDE firewall name FROM-INSIDE-TO-OUTSIDE
set zone-policy zone INSIDE from OUTSIDE firewall name FROM-OUTSIDE-TO-INSIDE
set zone-policy zone DMZ from INSIDE firewall name FROM-INSIDE-TO-DMZ
set zone-policy zone INSIDE from DMZ firewall name FROM-DMZ-TO-INSIDE
set zone-policy zone OUTSIDE from DMZ firewall name FROM-DMZ-TO-OUTSIDE
set zone-policy zone DMZ from OUTSIDE firewall name FROM-OUTSIDE-TO-DMZ


set service ssh port 22


commit
exit
```

------------FW2------------

```
configure
set system host-name FW2
set interfaces ethernet eth0 address 10.1.4.2/24
set interfaces ethernet eth1 address 10.2.1.2/24
set interfaces ethernet eth2 address 10.4.0.1/24
set interfaces ethernet eth3 address 10.4.1.1/24
set interfaces ethernet eth4 address 192.1.1.2/24

***** Configurar NAT *****
set nat source rule 10 outbound-interface eth3
set nat source rule 10 source address 10.0.0.0/8
set nat source rule 10 translation address 192.1.0.21-192.1.0.30

set nat source rule 20 outbound-interface eth2
set nat source rule 20 source address 10.0.0.0/8
set nat source rule 20 translation address 192.1.0.31-192.1.0.40

***** Definir Static routes *****
set protocols static route 0.0.0.0/0 next-hop 10.4.1.2 (ip eth3 LB2A)
set protocols static route 0.0.0.0/0 next-hop 10.4.0.2 (ip eth3 LB2B)
set protocols static route 10.2.2.0/24 next-hop 10.1.4.1 (ip eth3 LB1A)
set protocols static route 10.2.2.0/24 next-hop 10.2.1.1 (ip eth3 LB1B)


set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth0
set zone-policy zone INSIDE interface eth1
set zone-policy zone DMZ description "DMZ (Server Farm)"
set zone-policy zone DMZ interface eth4
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth2
set zone-policy zone OUTSIDE interface eth3


set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 description "streaming ports access
5000-6000"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol udp
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 destination port 5000-6000

set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 description "Inside network access
for HTTP and HTTPS through TCP"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 protocol tcp
set firewall name FROM-INSIDE-TO-OUTSIDE rule 11 destination port 80,443

set firewall name FROM-DMZ-TO-INSIDE rule 10 action accept
set firewall name FROM-DMZ-TO-INSIDE rule 10 description "Accept established-related
connections"
set firewall name FROM-DMZ-TO-INSIDE rule 10 state established enable
set firewall name FROM-DMZ-TO-INSIDE rule 10 state related enable

set firewall name FROM-DMZ-TO-OUTSIDE rule 10 action accept
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 description "Accept Established-related
connections"
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state established enable
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state related enable

set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 action accept
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 description "Accept
Established-related connections"
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state established enable
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state related enable

set firewall name FROM-INSIDE-TO-DMZ rule 10 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 10 description "Accept ICMP packets to
DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 10 icmp type 8
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol icmp

set firewall name FROM-INSIDE-TO-DMZ rule 12 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 12 description "Accept HTTP and HTTPS
from INSIDE to DMZ"
```

```
set firewall name FROM-INSIDE-TO-DMZ rule 12 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 12 destination port 80,443
set firewall name FROM-INSIDE-TO-DMZ rule 12 protocol tcp


set firewall name FROM-INSIDE-TO-DMZ rule 30 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 30 description "Allow DNS access to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination port 53
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol udp

set firewall name FROM-INSIDE-TO-DMZ rule 15 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 15 description "Accept HTTP, HTTPS and SSH from INSIDE to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 15 destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 15 destination port 22,80,443
set firewall name FROM-INSIDE-TO-DMZ rule 15 protocol tcp
set firewall name FROM-INSIDE-TO-DMZ rule 15 source address 10.2.2.0/2

set zone-policy zone OUTSIDE from INSIDE firewall name FROM-INSIDE-TO-OUTSIDE
set zone-policy zone INSIDE from OUTSIDE firewall name FROM-OUTSIDE-TO-INSIDE
set zone-policy zone DMZ from INSIDE firewall name FROM-INSIDE-TO-DMZ
set zone-policy zone INSIDE from DMZ firewall name FROM-DMZ-TO-INSIDE
set zone-policy zone OUTSIDE from DMZ firewall name FROM-DMZ-TO-OUTSIDE
set zone-policy zone DMZ from OUTSIDE firewall name FROM-OUTSIDE-TO-DMZ


set service ssh port 22

commit
exit
```

-------------DMZ-------------

```
ip 192.1.1.100/24 192.1.1.1
save

ip 192.1.1.200/24 192.1.1.1
```

—-------------IP’s—-----------------

pcs:
pc1: 10.2.2.100/24
pc2: 200.2.2.100/24

LB1A:
eth0: 10.1.1.1
eth1: 10.1.2.1
eth2: 10.1.3.1
eth3: 10.1.4.1

LB1B:
eth0: 10.1.1.2
eth1: 10.1.2.2
eth2: 10.2.0.1
eth3: 10.2.1.1

LB2A
eth0: 200.1.1.1
eth1: 10.5.0.1
eth2: 10.3.0.2
eth3: 10.4.1.2

LB2B
eth0: 200.1.1.2
eth1: 10.5.0.2
eth2: 10.3.1.1
eth3: 10.4.0.2

FW1
eth0: 10.1.3.2
eth1: 10.2.0.2
eth2: 10.3.0.1
eth3: 10.3.1.1
eth4: 192.1.1.1

FW2
eth0: 10.1.4.2
eth1: 10.2.1.2
eth2: 10.4.0.1
eth3: 10.4.1.1
eth4: 192.1.1.2