Approx time to complete this assignment: 12 hours

Common configuration for all machines:

1. Allow all traffic to and from the local loopback adapter lo, so each machine can talk to itself.
2. The default policy for inbound connections should be to drop packets not explicitly permitted.
3. Allow inbound icmp traffic for echo-request, echo-reply (ping), time-exceeded (traceroute), or destination-unreachable. (This lets ping and traceroute work but drops other commonly abused icmp packets.)
4. Allow an incoming connection to tcp dport 4113 for the grading script.
5. Deny your users access to Facebook from any machine on your network. You need not block all Facebook IP addresses, just the one you receive from a one-time resolve of facebook.com.
6. Allow ssh from the LAN, DMZ, WAN subnet and VPN.

```
  chain incoming {
        #  Default drop
        type filter hook input priority 0; policy drop;
        #  accept loopback
        iifname lo accept
        #  established connections
        ct state invalid drop
        ct state related,established accept
        #  saclass grader and proxy
        tcp dport {4113,4114} accept
        #  ping
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
        #  ssh from LAN, WAN, DMZ and VPN
        ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
  }

  chain outgoing {
        #  Block facebook
        ip daddr 157.240.28.35 drop
```

Machine A configuration (/etc/sysconfig/nftables.conf):

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.26.0/24

#  Machine A
table ip saclass {
  #  Incoming chain
  chain incoming {
        #  Default drop
        type filter hook input priority 0; policy drop;
        #  accept loopback
        iifname lo accept
        #  established connections
        ct state invalid drop
        ct state related,established accept
        #  saclass grader and proxy
        tcp dport {4113,4114} accept
        #  ping
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
        #  ssh from LAN, WAN, DMZ and VPN
        ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
        #  Incoming DHCP and NTP
        udp dport {67,123} accept
  }
  #  Outgoing chain
  chain outgoing {
        #  Default accept
        type filter hook output priority 0; policy accept;
        #  Block facebook
        ip daddr 157.240.28.35 drop;
  }
```

```
  #  Forward chain
  chain forwarding {
          # Default drop
          type filter hook forward priority 0; policy drop;
          #  established connections
          ct state invalid drop
          ct state related,established accept
          #  interface based chains
          iifname "ens192" oifname "ens224" jump WAN2DMZ
          iifname "ens192" oifname "ens256" jump WAN2LAN
          iifname "ens224" oifname "ens192" jump DMZ2WAN
          iifname "ens224" oifname "ens256" jump DMZ2LAN
          iifname "ens256" oifname "ens192" jump LAN2WAN
          iifname "ens256" oifname "ens224" jump LAN2DMZ
  }
  #  WAN to DMZ chain
  chain WAN2DMZ {
          #  ping
          icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
          #  DNS
          udp dport 53 accept
          #  ssh, dns, html, grader
          tcp dport {22,53,80,443,4113,4114} accept;
  }
  #  WAN to LAN chain
  chain WAN2LAN {
          # only return traffic
  }
  #  DMZ to WAN
  chain DMZ2WAN {
          #  ping
          icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
          #  DNS
          udp dport 53 accept
          #  DNS, http, https
          tcp dport {53,80,443} accept
          #  Block facebook
```

```
        ip daddr 157.240.28.35 drop;
  }

  #  DMZ to LAN
  chain DMZ2LAN {
        #  ping
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
        #  ssh and NFS
        tcp dport {22,111,2049} accept
  }
  #  LAN to DMZ
  chain LAN2DMZ {
        #  Allow everything
        ip saddr {10.21.32.0/24} accept;
  }
  #  LAN to WAN
  chain LAN2WAN {
        #  Block facebook
        ip daddr 157.240.28.35 drop
        #  Allow everything else
        ip saddr {10.21.32.0/24} accept;
  }
}
#  NAT LAN to WAN
table ip nat {
  chain POSTROUTING {
        type nat hook postrouting priority srcnat; policy accept;
        oifname "ens192" ip saddr 10.21.32.0/24 masquerade
  }
}
```

Machine B configuration (/etc/sysconfig/nftables.conf)

```
#!/usr/sbin/nft -f
```

```
flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.26.0/24

#  Machine B
table ip saclass {
  #  Incoming chain
  chain incoming {
        #  Default drop
        type filter hook input priority 0; policy drop;
        #  accept loopback
        iifname lo accept
        #  Incoming DNS request
        udp dport 53 accept
        tcp dport 53 accept
        #  established connections
        ct state invalid drop
        ct state related,established accept
        #  saclass grader and proxy
        tcp dport {4113,4114} accept
        #  ping
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
        #  ssh from LAN, WAN, DMZ and VPN
        ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
  }

  #  Outgoing chain
  chain outgoing {
        #  Default accept
        type filter hook output priority 0; policy accept;
        #  Block facebook
        ip daddr 157.240.28.35 drop
  }
}
```

Machine C configuration (/etc/nftables.conf):

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.26.0/24

#  Machine C
table ip saclass {
  #  Incoming chain
  chain incoming {
        #  Default drop
        type filter hook input priority 0; policy drop;
        #  accept loopback
        iifname lo accept
        #  established connections
        ct state invalid drop
        ct state related,established accept
        #  saclass grader and proxy
        tcp dport {4113,4114} accept
        #  http and https
        tcp dport {80,443} accept
        #  ping
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
        #  ssh from LAN, WAN, DMZ and VPN
        ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
  }

  #  Outgoing chain
  chain outgoing {
        #  Default accept
        type filter hook output priority 0; policy drop;
        #  Block facebook
        ip daddr 157.240.28.35 drop
        #  established connections
        ct state invalid drop
```

```
        ct state related,established accept
        #  Allow DNS, DHCP, NTP traffic
        udp dport {53,67,123} oifname "ens192" accept
        #  Allow DNS to Machine B and F only
        ip daddr {100.64.26.2,100.64.26.6} udp dport 53 accept
        #  Allow NFS to Machine E only
        ip daddr 10.21.32.2 tcp dport {111,2049} accept
        #  Allow ssh to DMZ subnet
        ip daddr $DMZ tcp dport 22 accept
        #  Allow ping to all except LAN
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} ip
daddr != 10.21.32.0/24 accept
        # Allow http, http, grader and proxy
        tcp dport {80,443,4113,4114} accept
  }
}
```

Machine D's configuration would be the same as Machine C.

Machine E configuration (/etc/sysconfig/nftables.conf):

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.26.0/24

#  Machine E
table ip saclass {
  #  Incoming chain
  chain incoming {
        # allow NFS traffic from DMZ
        tcp dport {111,2049} iifname "ens192" accept
        #  Default drop
        type filter hook input priority 0; policy drop;
        #  accept loopback
```

```
        iifname lo accept
        #  established connections
        ct state invalid drop
        ct state related,established accept
        #  saclass grader and proxy
        tcp dport {4113,4114} accept
        #  ping
        icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded}
accept
        #  ssh from LAN, WAN, DMZ and VPN
        ip saddr {10.21.32.0/24,100.64.0.0/24,$DMZ,198.11.0.0/16} tcp dport 22 accept
        # allow NFS traffic from DMZ
        #ip saddr $DMZ tcp dport {111,2049} accept
  }

  #  Outgoing chain
  chain outgoing {
        #  Default accept

        type filter hook output priority 0; policy accept;

        #  Block facebook

        ip daddr 157.240.28.35 drop

  }
}
```