## Prerequisites

- root@machineX# yum install nc tcpdump nmap

# All Machines

1. Allow all traffic to and from the local loopback adapter lo, so each machine can talk to itself.
   - iptables -A INPUT -i lo -j ACCEPT && iptables -A OUTPUT -o lo -j ACCEPT
   - Setup conntrack (to be second rule)
     - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

2. Allow inbound icmp traffic for echo-request, echo-reply (ping), time-exceeded (traceroute), or destination-unreachable.
   - iptables -N ICMP-ALLOW && iptables -A ICMP-ALLOW -p icmp --icmp-type echo-request -j ACCEPT && iptables -A ICMP-ALLOW -p icmp --icmp-type echo-reply -j ACCEPT && iptables -A ICMP-ALLOW -p icmp --icmp-type destination-unreachable -j ACCEPT && iptables -A ICMP-ALLOW -p icmp --icmp-type time-exceeded -j ACCEPT && iptables -A INPUT -p icmp -j ICMP-ALLOW && iptables -A ICMP-ALLOW -p icmp -j DROP && echo $?
   - tested with ---- tracepath 100.64.0.254 --- got 2 hops back

3. On all machines, except Machine E, allow inbound ssh connections from the 100.64.0.0/16, 10.21.32.0/24, and 198.18.0.0/16 subnets.
   - iptables -N SSH-ALLOW && iptables -A INPUT -p tcp --dport=22 -j SSH-ALLOW && iptables -A SSH-ALLOW -p tcp -s 100.64.0.0/16 -j ACCEPT && iptables -A SSH-ALLOW -p tcp -s 10.21.32.0/24 -j ACCEPT && iptables -A SSH-ALLOW -p tcp -s 198.18.0.0/16 -j ACCEPT && iptables -A SSH-ALLOW -p tcp -j DROP && echo $?
   - service iptables save---on all machines as a checkpoint
   - checked with nmap to see what ports were open

4. All machines should implement a default deny policy for inbound traffic.
   - iptables -P INPUT DROP && service iptables save

5. Machines should also prevent bad actors from "bouncing" or forwarding packets through them if they're not intended as routers. This should be done both with ip forwarding disabled in the kernel and through the forward chain.
   - On all except router (machineA)
   - iptables -P FORWARD DROP && iptables -P OUTPUT ACCEPT && service iptables save
   - checked all machines-- echo 0 > /proc/sys/net/ipv4/ip_forward
     - make persistent
       1. touch /etc/sysctl.d/01_noForward.conf && echo “net.ipv4.ip_forward=0” > /etc/sysctl.d/01_noForward.conf

6. Deny your users access to Facebook, icanhas.cheezburger.com, and cheezburger.com. You need not block all such IP addresses, just the ones you receive from a one-time resolve.
   - nslookup [domain] --- on machineD(DNS-chase) for the ip addresses
   - F: 157.240.28.35, C: 216.176.186.210, I: 216.176.186.210
   - All: iptables -A OUTPUT -d 157.240.28.35 -j DROP && iptables -A INPUT -s 157.240.28.35 -j DROP && iptables -A OUTPUT -d 216.176.186.210 -j DROP && iptables -A INPUT -s 216.176.186.210 -j DROP && service iptables save

- Router: iptables -A FORWARD -d 157.240.28.35 -j DROP && iptables -A FORWARD -s 216.176.186.210 -j DROP && service iptables save

## Machine A/Router

1. Allow the appropriate DHCP traffic to/from 100.64.N.0/24 & 10.21.32.0/24 (configs).
   - iptables -A OUTPUT -p udp -d 100.64.12.0/24 --dport=68 -j ACCEPT && iptables -A INPUT -p udp -s 100.64.12.0/24 --dport=67 -j ACCEPT && iptables -A OUTPUT -p udp -d 10.21.32.0/24 --dport=68 -j ACCEPT && iptables -A INPUT -p udp -s 10.21.32.0/24 --dport=67 -j ACCEPT && service iptables save
   - restarted network & dhcpd and network on one machine to check it's working

## Machines B (Carriage) & F (Saddle)

1. Allow inbound http and https requests from any source IP.
   - iptables -A INPUT -p tcp --dport=80 -j ACCEPT && iptables -A INPUT -p tcp --dport=443 -j ACCEPT && service iptables save
   - tested with nc -l 443 and nmap on another machine

## Machine C/Platen

1. Allow outbound ftp, http, https, and **ssh** connections to any host. (gotta keep ssh first)
   - iptables -A OUTPUT -p tcp --dport=22 -j SSH-ALLOW && service iptables save
   - iptables -I OUTPUT 2 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
   - iptables -A OUTPUT -p tcp --dport=80 -j ACCEPT && iptables -A OUTPUT -p tcp --dport=443 -j ACCEPT
   - tested with yum to install ftp
1. Unlike the other machines, the default outbound policy for Machine C should be deny.
   - Iptables -P OUTPUT DROP
2. Allow ftp connections only from 100.64.0.0/16.
   - iptables -A INPUT -p tcp --dport=21 -s 100.64.0.0/16 -j ACCEPT
3. Allow dns requests to 100.64.N.4 (chase).
   - iptables -I OUTPUT 3 -p udp -d 100.64.12.4 --dport 53 -j ACCEPT
4. Allow outbound icmp traffic only for icmp-types echo-request, echo-reply (ping), time-exceeded (traceroute), or destination-unreachable.
   - iptables -A OUTPUT -p icmp -j ICMP-ALLOW

✓ tested with nmap, ssh, ping, wget --- service iptables save

## Machine D/Chase

1. Unlike the other machines, the default outbound policy for Machine C should be deny.
   - iptables -A INPUT -p udp --dport=53 -j ACCEPT && iptables -A OUTPUT -p udp --sport=53 -j ACCEPT && iptables -A INPUT -p tcp --dport=53 -j ACCEPT && iptables -A OUTPUT -p tcp --sport=53 -j ACCEPT && iptables -A INPUT -p tcp --sport=53 -j ACCEPT && service iptables save

Machine E/Roller

1.Restrict connections to the file sharing services (CIFS and SMB) from the 10.21.32.0/24 network only. CIFS and SMB use port numbers: 135/tcp, 137-139/udp, and 445/tcp.

- iptables -N FILES-ALLOW && iptables -A FILES-ALLOW -p tcp --dport=135 -j ACCEPT && iptables -A FILES-ALLOW -p tcp --dport=445 -j ACCEPT && iptables -A FILES-ALLOW -p udp --dport=137:139 -j ACCEPT && iptables -A FILES-ALLOW -j DROP && iptables -A INPUT -s 10.21.32.0/24 -j FILES-ALLOW
- tested with nmap ---- service iptables save

2.Allow SSH connections only from hosts in the 10.21.32.0/24 subnet.

- Lost access because of setting policy for INPUT to drop before setting this, now it works
- iptables -N SSH-ALLOW && iptables -A INPUT -p tcp --dport=22 -j SSH-ALLOW && iptables -A SSH-ALLOW -p tcp -s 10.21.32.0/24 -j ACCEPT && service iptables save

Machine F/Saddle

- Found that after reboot my settings did not persist
- so checked that iptables was enabled and it wasn't
- so made sure the firewalld was disabled and enabled and started iptables

✓ all seems to be working on all machines now