Prerequisites

- Lab 7-- passed all tests and got all the points

Machine-A/Router

1. Allow the appropriate DHCP traffic to/from 100.64.N.0/24 & 10.21.32.0/24 (So your other machines can get their configs).
   - Done in previous lab

2. 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.
   - Done in previous lab

3. Deny your users access to icanhas.cheezburger.com and cheezburger.com. Again, you need not block all such IP addresses, just the ones you receive from a one-time resolve.
   - Done in previous lab

   ens192 internet facing, ens224 DMZ , ens256 internal files

4. Only forward packets to/from machines behind the router, based on the intended purpose of that specific machine. In other words, there should be rules on Machine A that mimic the rules for Machines B-F. This is an added layer of security in case the firewall on one of the other machines is inadvertently dropped.
   - iptables -N FORWARD && iptables -A FORWARD -d 157.240.28.35 -j DROP && iptables -A FORWARD -s 157.240.28.35 -j DROP && iptables -A FORWARD -d 216.176.186.210 -j DROP && iptables -A FORWARD -s 216.176.186.210 -j DROP && service iptables save
   - iptables -N ITODMZ && iptables -N DMZTOI && iptables -N ITOLOC && iptables -N LOCTOI && iptables -N LOCTODMZ && iptables -N DMZTOLOC
   - iptables -A FORWARD -p icmp -j ICMP-ALLOW
   - iptables -A FORWARD -i ens192 -o ens224 -j ITODMZ && iptables -A FORWARD -i ens192 -o ens256 -j ITOLOC && iptables -A FORWARD -o ens192 -i ens224 -j DMZTOI && iptables -A FORWARD -o ens192 -i ens256 -j LOCTOI && iptables -A FORWARD -o ens256 -i ens224 -j DMZTOLOC && iptables -A FORWARD -o ens224 -i ens256 -j LOCTODMZ
   - iptables -A LOCTODMZ -p tcp --dport=22 -j SSH-ALLOW && iptables -A ITODMZ -p tcp --dport=22 -j SSH-ALLOW
   - iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
   - service iptables save
   - iptables -A DMZTOI -p tcp -m multiport --dport 21,22 -s 100.64.12.3 -j ACCEPT
   - iptables -A ITODMZ -p tcp -m multiport --dport 80,443 -d 100.64.12.2,100.64.12.5 -j ACCEPT && iptables -A LOCTODMZ -p tcp -m multiport --dport 80,443 -d 100.64.12.2,100.64.12.5 -j ACCEPT
   - iptables -A DMZTOI -p udp --dport=53 -s 100.64.12.0/24 -j ACCEPT
   - iptables -A LOCTOI -s 10.21.32.0/24 -j ACCEPT
   - iptables -A ITODMZ -p udp --dport=53 -d 100.64.12.4 -j ACCEPT && iptables -A LOCTODMZ -p udp --dport=53 -d 100.64.12.4 -j ACCEPT && service iptables save
   - SET EVERYTHING ELSE TO DROP:
     - iptables -A ITODMZ -j DROP && iptables -A ITOLOC -j DROP && iptables -A LOCTODMZ -j DROP && iptables -A LOCTOI -j DROP && iptables -A DMZTOI -j DROP && iptables -A DMZTOLOC -j DROP && service iptables save

- ○ Tested with nmap, dig, ssh, and ping many different pathways from different machines, turning off machine firewalls, and watched packets rebooted and repeated checking and everything seemed to be working correctly.