Firewall Lab for CS332 by Christiaan Hazlett and Isaac Chen

Question 1: The computer on the LAN cannot access the internet because there hasn't been a device setup on the network to forward requests to the outside world.

Question 2: We see the IP address of the NAT. The NAT translates addresses from inside the LAN to it's own, so that it receives the replies from the internet and can forward them back inside the network.

Question 3: Yes, we could access the config page

Question 4: This rule looks for incoming TCP connections to port 80 (the web port) on the NAT/firewall computer, and if it sees any coming in, blocks them.

Question 5: Once we had properly configured the rule, we were unable to access the web config from either computer.

Question 6: To block SSH, we needed to block port 22, and for telnet, port 23

Question 7: To allow the client to access the web config page, we actually just modified the rule from above to only take effect on the WAN interface. We could also have added a rule to allow the traffic from the LAN interface through the firewall, thus overriding the previous rule.

Question 8: Port 3389 is Windows' RDP port

Question 9: svchost.exe is listening on port 3389

Question 10: We can forward any port. Additionally, one port on the NAT can forward to another port on the LAN machine, so we could forward port 3000, for example, to port 22 on a LAN machine to make finding our publicly exposed SSH port slightly less easy for the jerks that are constantly trying to login to my server all the time. I'm not even mad. Well maybe just a little.

Question 11: This rule blocks the NAT from forwarding any information from the outside world (eth2) back to the inside network. So, when a website replies to the LAN computer's request, that reply is not allowed to get back inside the network to the LAN computer, and the site is effectively blocked.

Question 12: DNS operates on port 53. We added TCP and UDP allow rules to our firewall.

Question 13: isc.sans.edu uses 66.35.59.249, and references both www.howsmyssl.com (104.196.190.195) and www.sans.org (45.60.31.34)

Question 14: We needed to add rules to allow forwarding from the outside network (eth2) to the LAN on port 80 (http) and 443 (https). Then we were able to visit the site.