**Russell clousing**

**Drew Vande Lune**

**Question 1:  Why can’t users in 192.168.x.x networks directly route and access internet resources?**

192.168.X.X are private non routable addresses.

**Question 2: What IP address did you get? Explain why you see the address you see.**

**153.106.116.110. Because I am hidden behind a NAT that has the IP address of 153.106.116.110.**

##### Question 3: Were you able to get to the management interface and login on both interfaces?

Yes we both could connect.

##### Question 4: Explain in "plain English" what the above rule does.

Rejects tcp requests with destination port 80.

**Question 5: On both your WAN and LAN computers, can you still browse to the web interface for controlling the Mikrotik?  Why or why not?**

**No we can not. The firewall rule that we set above does not allow anything to connect using tcp and port 80.**

##### Question 6:  What ports did you have to block?

To block telnet we blocked port 23. For SSH we blocked 22.

##### Question 7:  Describe (in plain english) how you had to add these rules?

Created two rules that allow connections to port 80 and port 22 from tcp requests, as long as the source address is 192.168.110.10, LAN client address.

##### Question 8: What port is it?

3389 tcp and udp

##### Question 9: What process is listening on the port?

Svchost.exe

##### Question 10: What ports can we setup in a NAT port forward? Do the ports on both sides have to be the same?

Any port can be port forwarded. No they do not.

**Question 11: Describe in plain English what this firewall rule is accomplishing and why it works with the little configuration we put in the rule.**

**Any connection that is not explicitly allowed by a firewall rule is denied.**

**Question 13: What IPv4 addresses are used by isc.sans.edu and dependent sites?**

**Isc.sans.edu ip:66.35.59.249**

**Sans.org ip: 45.60.33.34 and 45.60.31.34**

##### Question 14: Describe the rule(s) you added, in detail.

Added 6 rules, two rules for each of the three addresses that was needed. One for http and one for https. They allow traffic to 66.35.59.249 (isc.sans.edu) or 45.60.33.34 (sans.org) or 45.60.31.34 (sans.org).