##### **Matt Kotva and Ye Joo Oh**

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

That is part of the private address subnet. In order to get to the internet, the private address needs to be changed to the public address.

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

153.106.116.114. That is our public IP address.

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

Yes.

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

It rejects machines from connecting to Mikrotik using a browser.

##### **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 just set up a rule to prevent that.

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

22 and 23

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

We set a rule before the rejection rule that says that if there is a SSH or HTTP request from the client IP, it should accept it.

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

Port 3389

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

Svchost

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

Any open port can be set up for a NAT port forward. Public and private ports can be different. Both sides in our case were the same.

##### 

##### 

##### **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.**

This rule rejects all ethernet requests. It works because it just rejects anything coming from ethernet2.

##### **Question 12: Describe the rule(s) you added, including the protocol and ports you used.**

We had two rules. They allowed forwarding from my computer to DNS server using TCP and UDP. They used port 53 as the destination. The input interface is ethernet2.

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

104.196.190.195

66.35.59.249

45.60.31.34

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

These rules allowed requests to a destination address to the IP addresses above. They are all TCP. There were two rules for each address--one for HTTP, and one for HTTPS. For HTTP the destination port is 80 and for HTTPS the destination port is 43. The input interface was ethernet2.