Firewall Lab. 12/5/2017 Professor Norman

Ben Kastner and Micah Bonewell

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

The LAN computer can reach out to the internet, but the internet resources cannot send back to them because we have not set up the NAT / masquarading yet.

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

153.106.116.112 The firewall is acting as a NAT, so the only IP address the outside world sees is the WAN side 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 prevents the device on the WAN from accessing the web management interface.

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? The firewall rule to deny tcp traffic to port 80 blocks the management site on all interfaces.

No, we can't get to the management page from either the LAN or WAN computer.

Question 6: What ports did you have to block?

Ports 22 and 23

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

I had to go to IP > Firewall add a rule that allowed access on the LAN side only to the ip address of the lan management computer and only using the ssh port.

Question 8: What port is it?

3389

Question 9: What process is listening on the port?

Svchost.ext

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

We can set any port to be forwarded. The ports do need to be 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.

Prevents the LAN computer from reaching any website. It simply blocks all traffic attempting to go in ether2.

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

We added a rule to allow TCP connections to ether2, on port 53. We added an identical rule for UDP.

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

66.35.59.249 isc.sans.edu

45.60.33.34 sans.org

45.60.31.34 sans.org