Quentin Baker

CS 332

Firewall Lab

2017-12-08

1) Users in a 192.168.x.x network cannot directly access internet resources because the 192.168.x.x block is a reserved address for systems behind a NAT. Even if the local network didn't translate the IPs, any router would discard the packet as required by protocol.

2) The LAN PC is visible to the outside world as 153.106.116.115. This is because the LAN PC is set up to send all its data behind the NAT to the WAN PC, who is then sending out the data on behalf of the LAN PC. Therefore, to the outside world, all the information is coming from the IP we chose.

3) Yes, the Management interface appeared on the LAN (NAT address) for the LAN PC, and the WAN address for the WAN PC.

4) The firewall rule added will automatically send an "ICMP Host Unreachable" response to anything coming in with on port 80. This will prevent any further TCP setup, effectively denying any outside attempt to connect to the management interface.

5) Neither the LAN nor the WAN PC could reach the interface. This is because the firewall is IP agnostic, monitoring ports and interfaces, not the addresses, so no which end we try to connect to we will be rejected.

6) Port 22 for SSH, and Port 23 for Telnet

7) Add new firewall rules by adding two new filter rules:

a. One rule to listen for connections coming in to 192.168.115.1 on port 80 (http)
b. Another rule to listen for connections coming in on 192.168.115.1 on port 22 (ssh)

These rules will be set to "accept" and placed above our previous rules, meaning anything matching the criteria will be allowed through. Since the rules are before the reject rules, they supersede the rejection.

8) Windows RDP listens on TCP port 3389 for internal (LAN) connections.

9) Svchost.exe (NetworkService) is listening on TCP 3389.

10) We can setup any port in a NAT port forward. The ports do not have to be the same; we could have a listening port forward to a different port on the forwarded machine.

11) The firewall rule we added will reject ANYTHING coming in to interface ether2. Since our LAN PC is behind a NAT running on the WAN PC, all traffic is attempting to go through this interface, and therefore denied.

12) I added rules on the **forward** chain to accept requests on TCP and UDP port 53 for DNS.

13) 66.35.59.249 (isc.sans.edu), 104.192.190.195 (howsmyssl.com)

14) I added a rule for http and https on the 66.35.59.249 IP:

a. Port 80, chain forward, Dst. Address = 66.35.59.249, Action = Accept
b. Port 443, chain forward, Dst. Address = 66.35.59.249, Action = Accept

Both rules were placed in front of the forward reject all rule.