Katelynn Johnson

November 19th, 2019

Firewall lab

In our lab environment, we have been using pfSense as our firewall. Configuring firewall rules for pfSense is easy because pfSense provides the user with a web interface to create and submit firewall rules. The web console provides the user with “form-like” formatting for all configurations. This makes configuring the firewall rules uniform and fast. The two main categories of firewall rules are “WAN” and “LAN”. As the name suggests, a user can choose which “side” to configure rules for simply by choosing a category.

Choosing which “side” to configure for firewall rules can be tricky. When deciding which side to configure, think about where the source of the packet is coming from. If the source address is within the local network this is a LAN firewall rule. And respectively, if the source of a packet comes from outside the network, this is a WAN firewall rule.

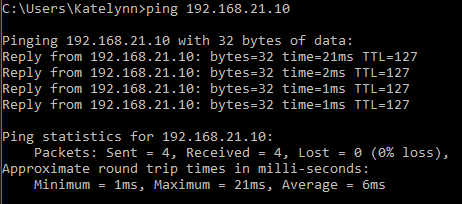
There are many ways to customize a firewall rule, these options include: protocol type, IPv4/IPv6/both, source IP and port, destination IP and port. Once all of these choices are selected for the rule, the final step is to decide what to do with the rule: pass/block/reject. Once the rule is created be sure that the order in which the firewall rules are in is correct. The firewall rules read from top to bottom. Meaning, the first rule a packet matches, will be what happens to the packet.

Firewall rules are highly customizable. Therefore, they can be used to allow or deny very specific traffic. This allows for a network administrator to be very specific about what they do and do not want to pass into and out of their network. It is best practice to implement an “implicit deny” at the bottom of the firewall rule list. This allows for a “catch all” by applying that if a packet is not explicitly allowed by any of the previous firewall rules, then do not allow the packet to pass. It is much easier (time wise and effort wise) to state what is allowed on a network than to allow everything and then make a rule for everything you want to deny.

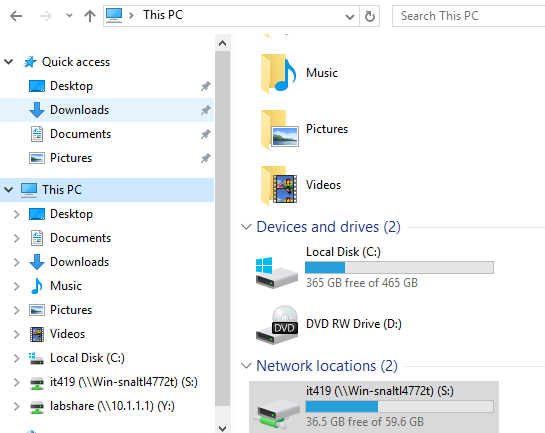
**Steps in the lab:**

* **Clients not on your private network can only access the windows server on your private network via port 80 and port 443 (the sites on the web server). This also includes not allowing ping messages and file sharing**

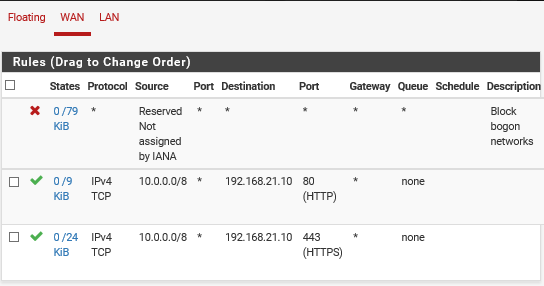
1. Ping being allowed from host machine (10.1.1.58) to server (192.168.21.10)



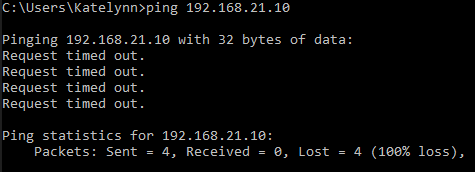
1. File sharing allowed from host machine(10.1.1.58) to server (192.168.21.10)



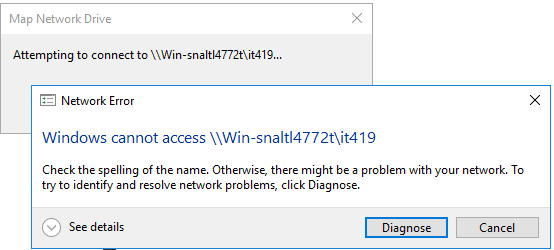
1. A change in my WAN firewall rules to remove allowing ICMP and remove allowing 445 SMB



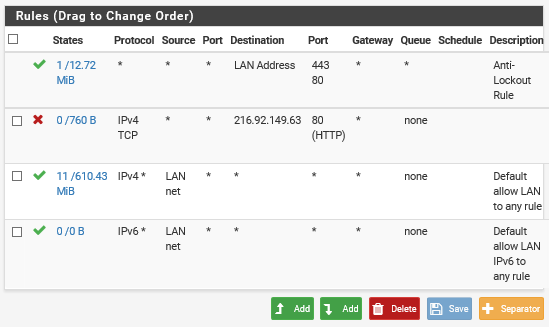
1. Ping denied from host machine(10.1.1.58) to server (192.168.21.10)



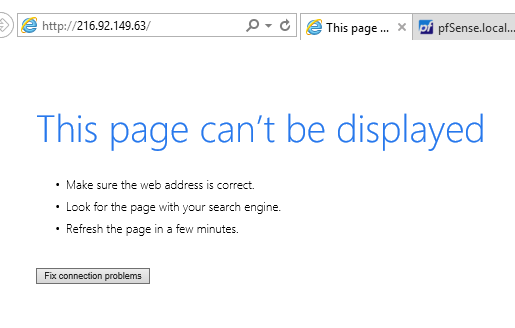
1. File sharing denied from host machine(10.1.1.58) to server (192.168.21.10)



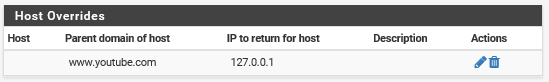
* **Machines on the trusted network cannot access the website “stopfakenews.net”. Use pfSense DNS resolver to block a popular web site like YouTube.com**
  1. In order to block “stopfakenews.net” I needed the IP address of the website. I did this by using nslookup. After I obtained the IP address, I added it to a LAN firewall rule to block all local network traffic from going to that site.
     + LAN rules blocking “stopfakenews.com” by IP address



* + - Site being blocked when attempted connection from browser



* 1. In order for a site like YouTube to be blocked, extra steps had to be taken. A site that generates a lot of traffic will have many servers and many IP addresses assigned to that domain in order to be able to handle all the traffic coming to it. So blocking a single IP address would not work in this case. It is possible to look up the IP address ranges for the site and then block all of those ranges, but a way that takes less steps and is more likely to work is to block the site by DNS name.
     + An entry in the “Host Overrides” section of the DNS resolver in pfSense to block “www.youtube.com”



* + - An attempt to browse to “www.youtube.com”

