Building and Configuring a Basic Multi-Subnet Network and Firewall Part 2

Continue from part 1 Roozah Khan

Initial Functionality Testing

Ping the server via both its IP address and its URL from each of the two clients:

ping 5.5.5.5

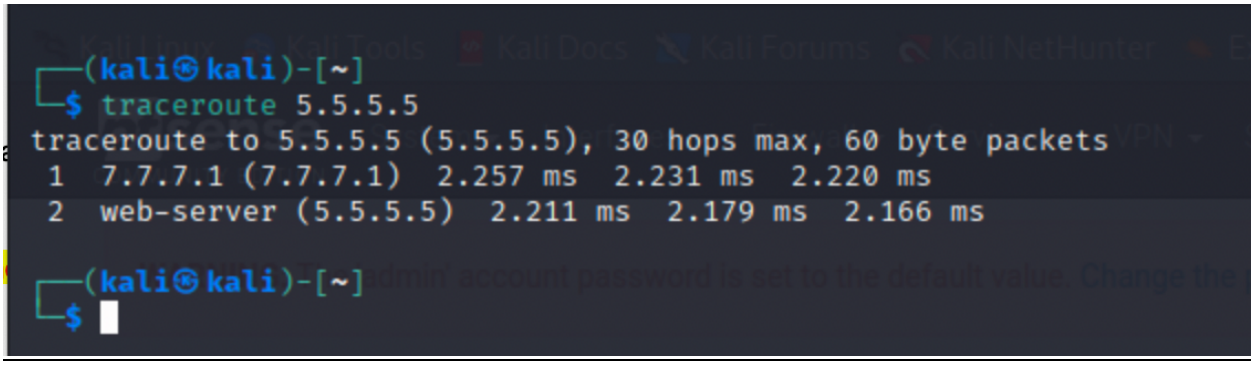
ping web-server

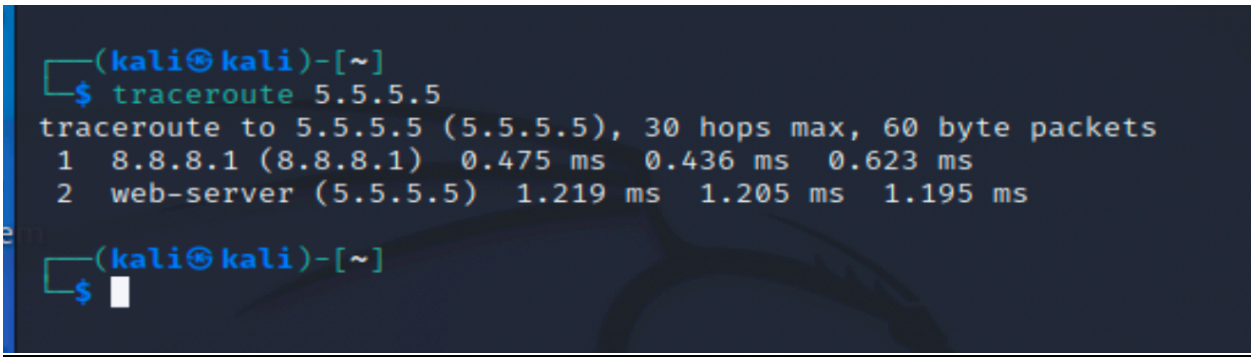
All of these must work or you need to troubleshoot the issue before proceeding.

Just because, do a traceroute from each client to the server:

traceroute 5.5.5.5

Provide the output from the ***LANnet client's*** traceroute command from both clients as **Screenshot 9.**





Basic Firewall Rules

The pfSense webconfigurator (webpage) can only be accessed from the LAN interface.

In order to establish basic network connectivity, you started with "ALLOW ALL" (or PASS ALL) rules in pfSense for the LAN net and OPT1 net. Now you must remedy this significant security issue prior to permitting other users on the network. You must remove the "ALLOW ALL" rules and create appropriate rules for specific protocols to allow the functionality specified by corporate policy. It is not up to you to decide what should be allowed – it is your duty to implement the policy.

The following are the firewall ***policies*** that must be implemented. Remember that it is the security architect's duty to create *rules that enforce the policy* **IN THE MOST RESTRICTIVE WAY POSSIBLE!** Another way of saying that is that the policy must pass the least number of packets possible while meeting the policy objective. If it's not done in the most restrictive way possible, it will not survive a vulnerability test.

Policy 1:

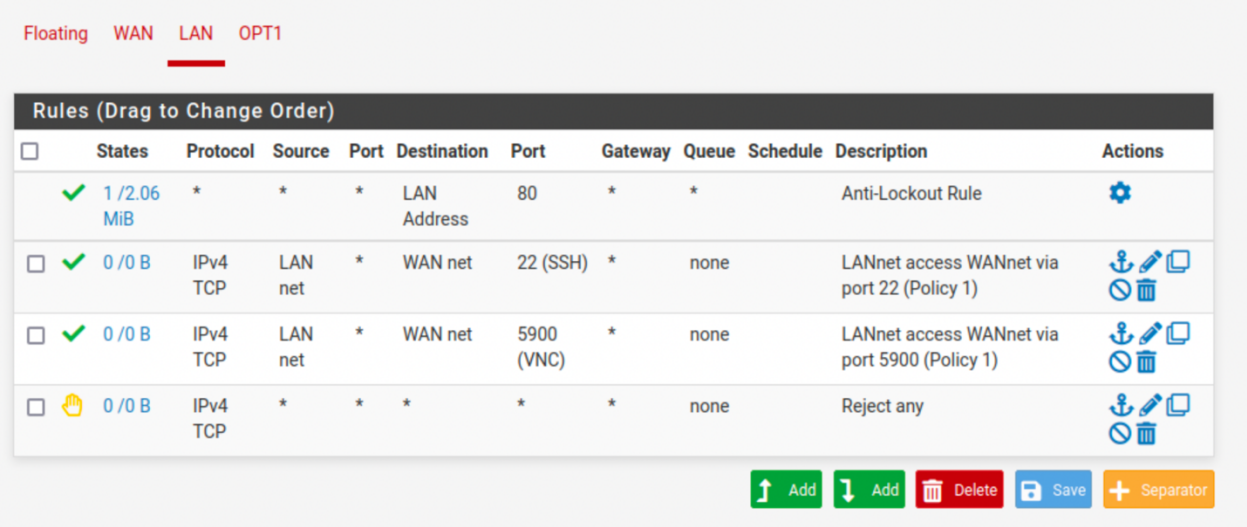
- The IT department (LANnet) will have access to all systems in the server subnet (WANnet) via VNC (port 5900) & SSH (port 22) only. That is, only ports 5900 and 22 should be allowed as the destination port from the LANnet to the WANnet.

- Note that that LANnet has access to ports 443 and 80 by default, as the "anti-lockout rule". This rule can not be removed to prevent the case where you accidentally "lock yourself out".

- Remember, after you specified all the "allow" rules, the last rule in the Firewall should always be "reject any", which essentially denies all the other possibilities that has not been explicitly allowed.

1 Create pfSense firewall rules that implement policy 1.

Record the rule setup screen for VNC and SSH as **Screenshot 10**. Be sure you enter a description for the rule that indicates which policy it is implementing.



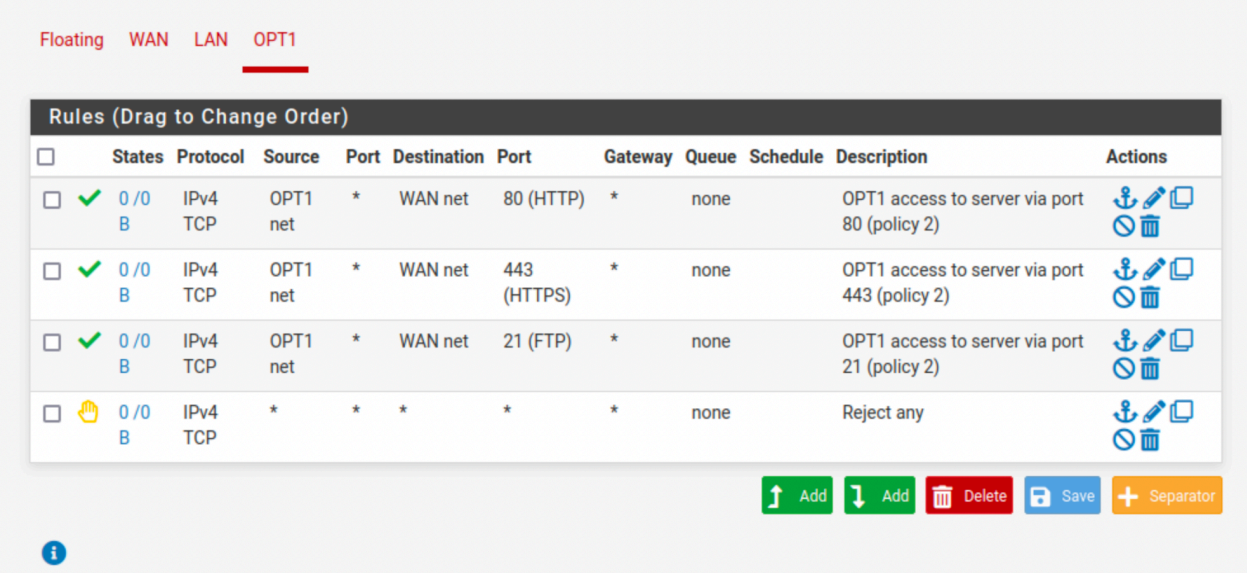
Policy 2:

- Corporate clients (OPT1net) will have access to the server via HTTP (port 80), HTTPS (port 443) and FTP (port 21) only. That is, only ports 80, 443, and 21 should be allowed as the destination port from OPT1net to WANnet.

- Don't forget to add a "reject any" rule at the end.

2 Create pfSense firewall rules that implement Policy 2.

Record the rule setup screen for HTTP and FTP traffic as **Screenshot 11**. Be sure you enter a description for the rule that indicates which policy it is implementing.

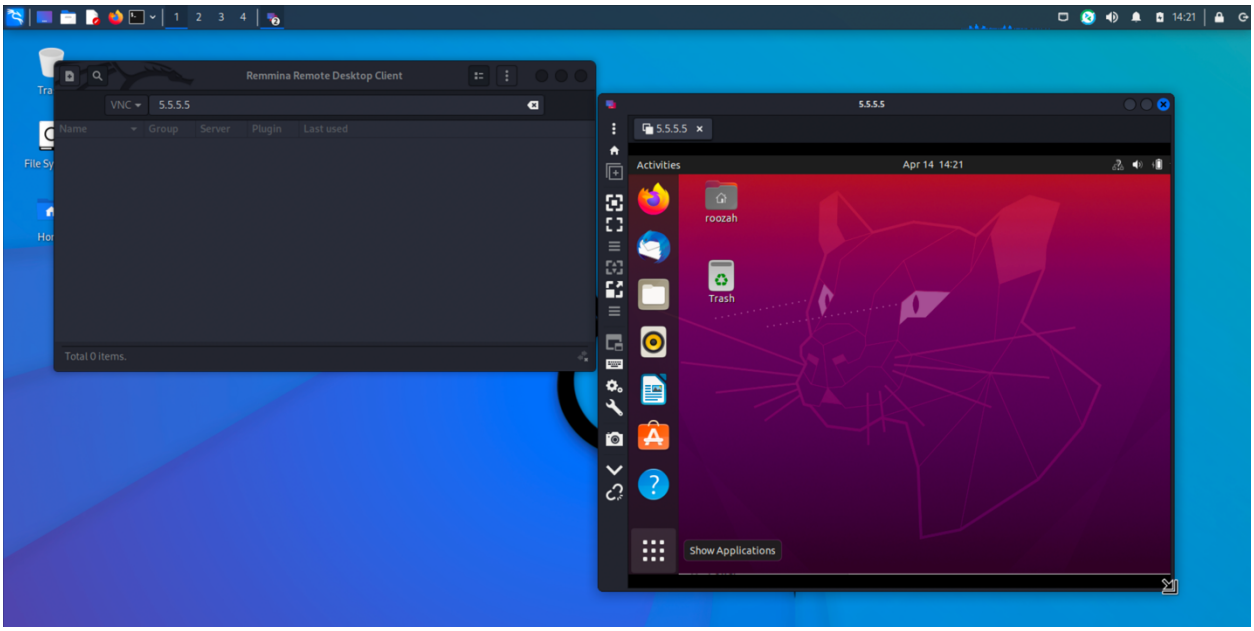


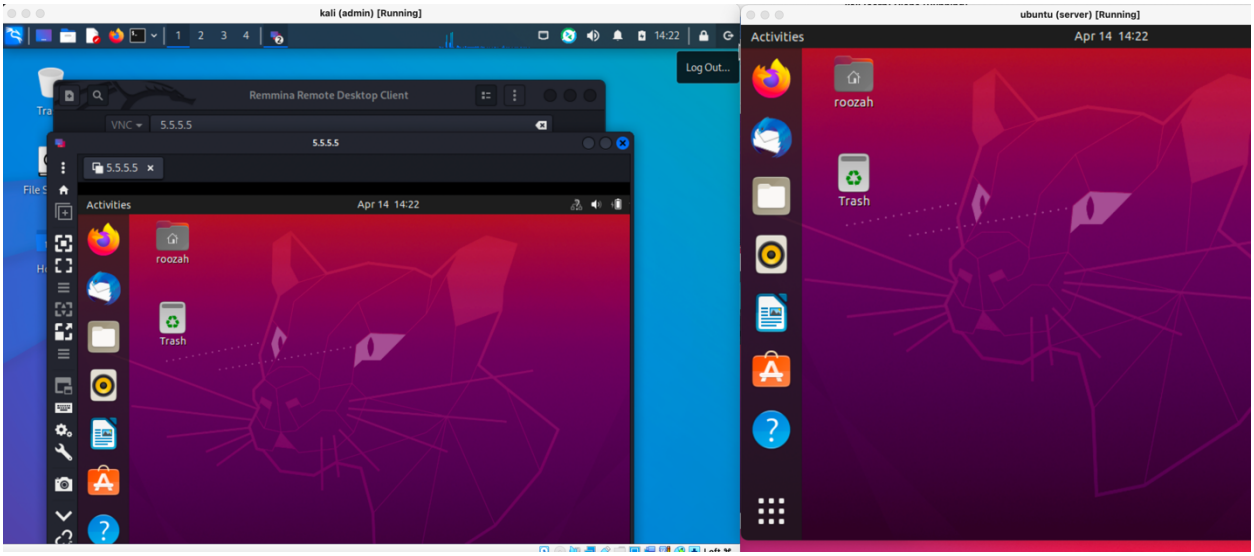
At this point, if you have not, delete the "ALLOW ALL" rules in both the LAN and OPT1 rule tables to ensure that no unauthorized traffic is passed through the firewall. And add a "REJECT ANY" at the bottom after all the "allow" rules. You must do this before testing, otherwise all traffic will pass and the more restrictive "pass" rules will appear to be working even if they really aren't.

---

3 Demonstrate that the rules you created for Policy 1 actually work. On the Admin Client, provide screenshots showing:

a An active VNC connection to the server (VNC session window in Remmina). Please use one screenshot to show the three essential components: the desktop of the Admin client (Kali), the application window of Remmina, and the window in which the Server (Ubuntu) desktop is running. **Screenshot 12**.



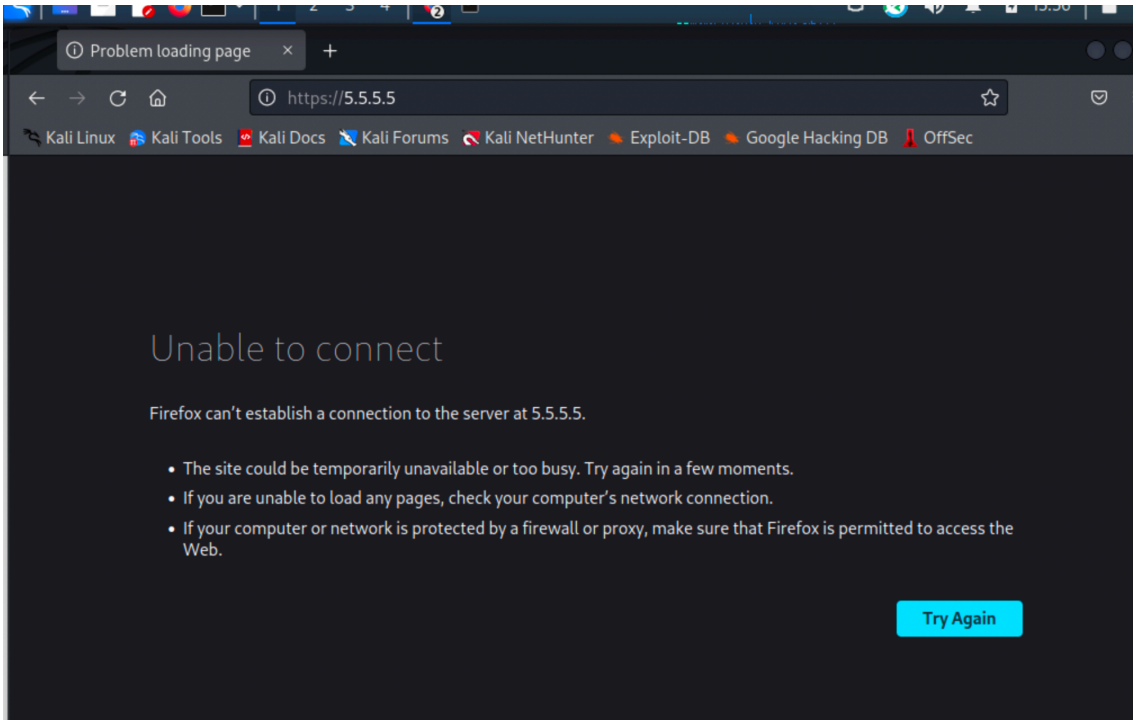


b A successful SSH session log in to the server (5.5.5.5) using a terminal (you do not need to login, but you need to show that the ssh command has been successfully connected to the Ubuntu server)– **Screenshot 13**.

Note: before the next test you'll need to clear your browser cache. In Firefox, go to the 3 lines on the top-right of the browser, select HISTORY > CLEAR RECENT HISTORY > CLEAR NOW. Otherwise, the cached data makes it appear that you can still access the web server.

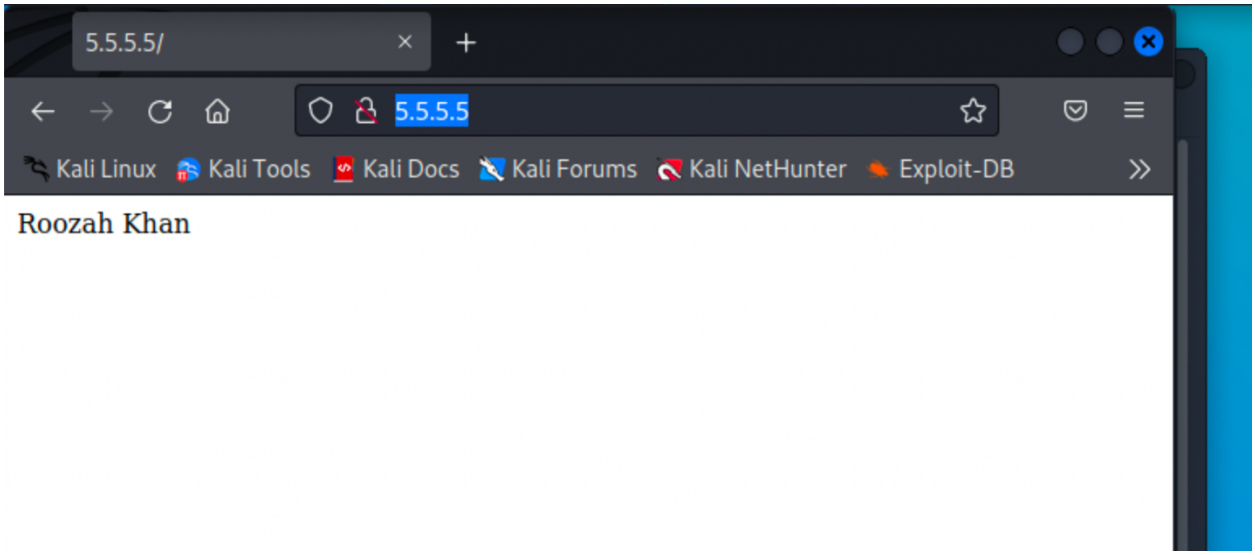
```
┌──(kali㉿kali)-[~]
└─$ ssh roozah@5.5.5.5
roozah@5.5.5.5's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-39-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

115 updates can be applied immediately.
88 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

roozah@roozah-VirtualBox:~$
```

c An attempt to access the web server from a web browser (http://5.5.5.5) (the page shouldn't load) - **Screenshot 14**.

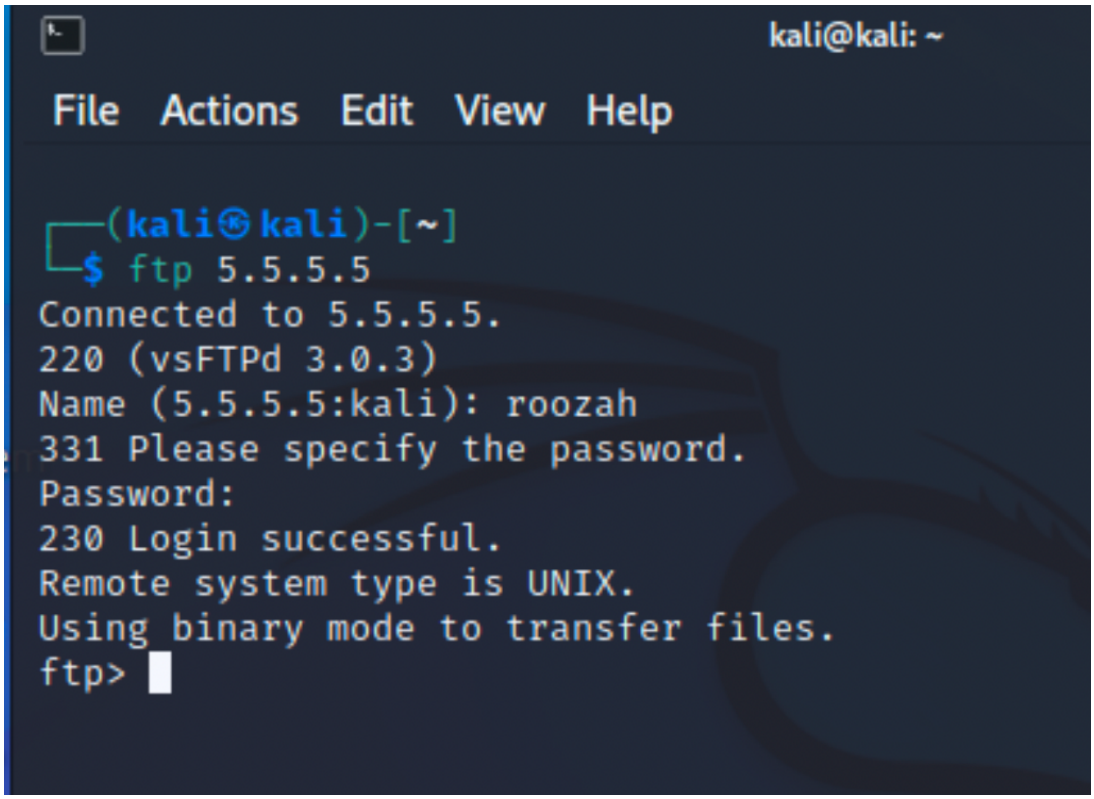


4 Demonstrate that the rules you created for Policy 2 on the OPT1 ACL actually work. From the Cooperate Client, provide screenshots showing:

a The server's default web page (index.html with your first name and last name in it) - **Screenshot 15**.

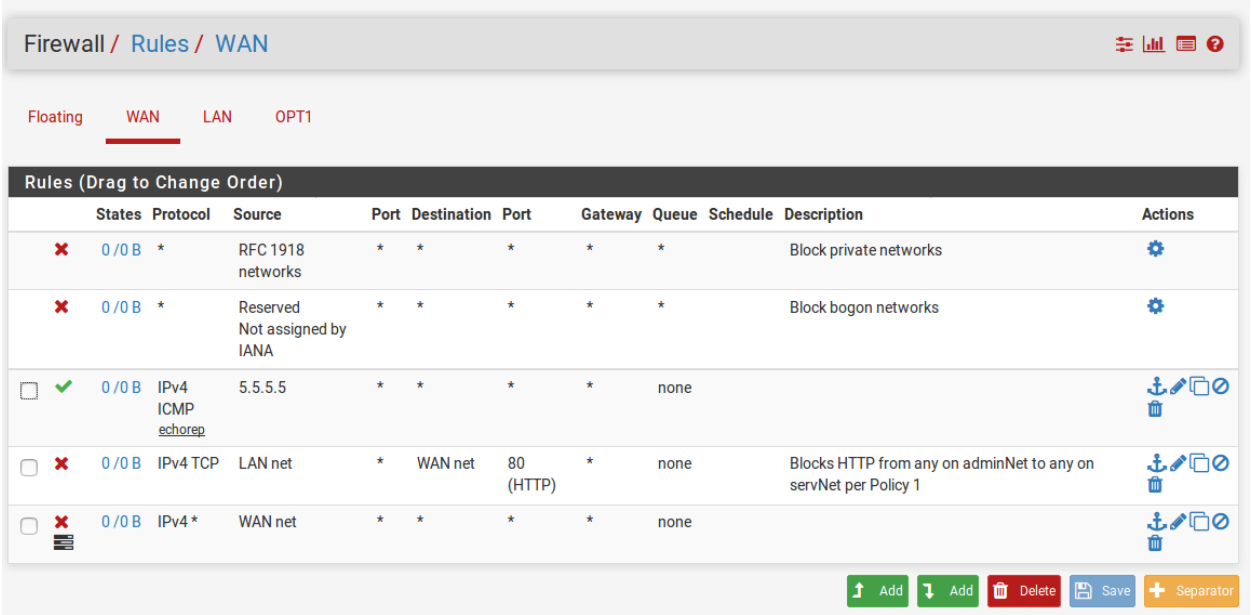


b A successful FTP connection screen (use ftp://5.5.5.5 or ftp://web-server from Firefox, you only need to display the prompt login dialog, and do not need to actually login) - **Screenshot 16**.



Additional Guidance on Screenshots

1. For screenshots 10 and 11, i.e., the firewall rules, please provide a screenshot like the following.



2. In general, you screenshot should include all information asked in the question, with all essential parts being legible.