LAB 03 – Firewalls

By :- Faraz Ahmed

Contents

1. Allow Only Approved Protocols Inbound to AdminNet 3

a. WinRM protocol 3

2. Allow Additional Approved Protocols Outbound to AdminNet 5

a. FTP protocol 5

3. Designate Only One Machine to Manage our Firewall 7

a. Disabling "Anti-Lookout Rule" 7

4. Submitting Summary Screenshots of Firewall Rules 9

a. External Interface 9

Figure 8: Screenshot of all firewall rules in "External Interface". 9

b. AdminNet Interface 9

c. ServerNet 10

5. Update the Topology 11

6. Testing 12

A. Testing the AdminNet outbound protocols 12

B. Testing the AdminNet outbound protocols 14

- Test the only one machine where we manage the firewall 16
  - For OutsideDevice 16
  - For UbuntuClient 18
  - Testing for one allowed device (Windows 10 Client) 19

7. Additional Task of Memo Page 21

1. Allow Only Approved Protocols Inbound to AdminNet

All the approved inbound protocols allow to AdminNet are as follows :-

a. WinRM protocol

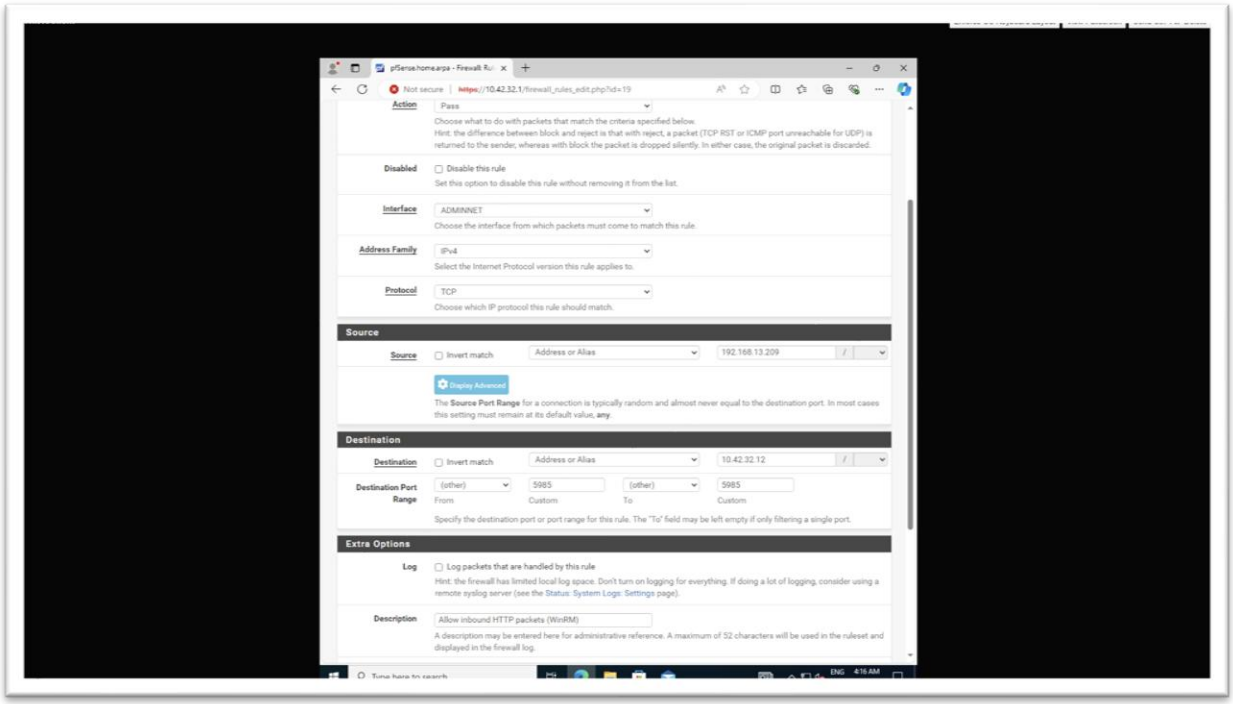

Figure 1: Screenshot of WinRM firewall rule to allow inbound HTTP packets from Outside Device to Win10Client.

- As we can see in the above Figure 1, basic configuration for setting up rule for allowing to inbound HTTPS packets by WinRM. WinRM is a protocol that allows Windows to communicate with other servers remotely through HTTP/HTTPS to communicate. So for HTTP, we have to use 5985 as a port and for HTTPS, we have to use 5986 as a port. Then, in source we have to enter ip address for OutsideDevice and in destination we have to enter ip address for Windows 10 client. Then lastly add description and click save.

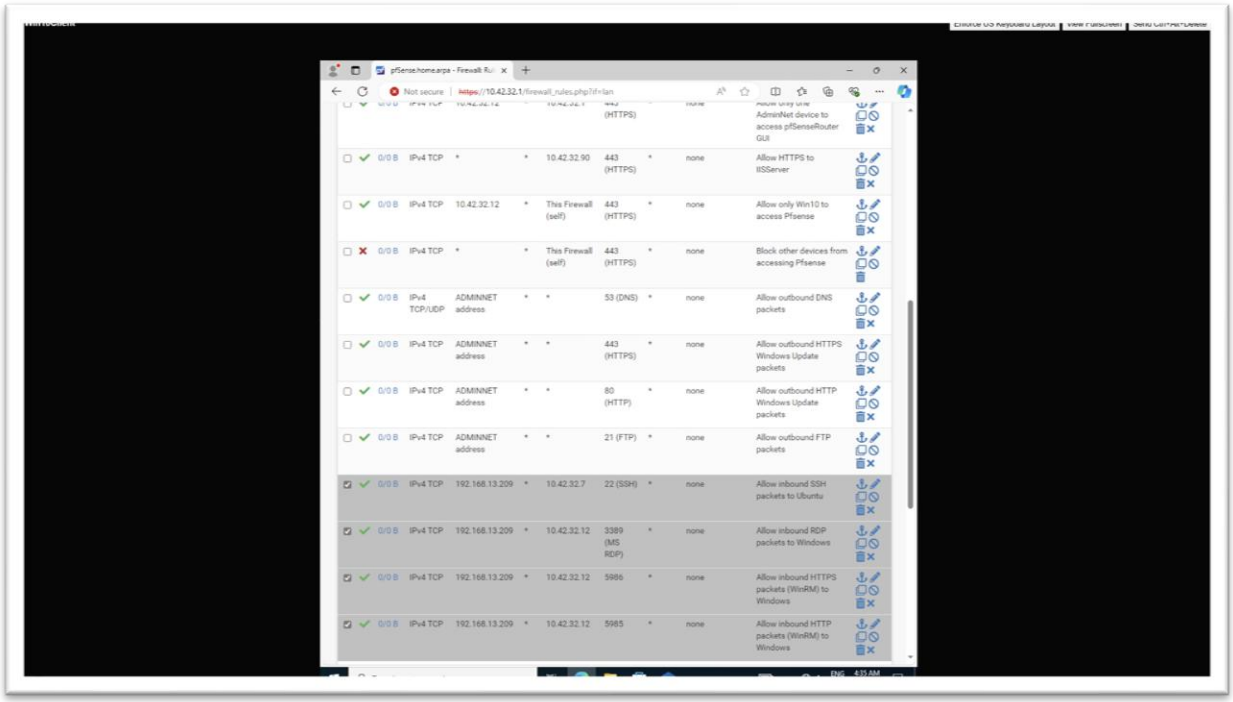

Figure 2: Screenshot of Highlighted firewall rules of WinRM, RDP and SSH in AdminNet.

- So, from above figure 2, we can note that four rules are created for inbound in AdminNet and their description state's purpose of each rule.

2. Allow Additional Approved Protocols Outbound to AdminNet

All the approved outbound protocols allow to AdminNet are as follows :-

a. FTP protocol

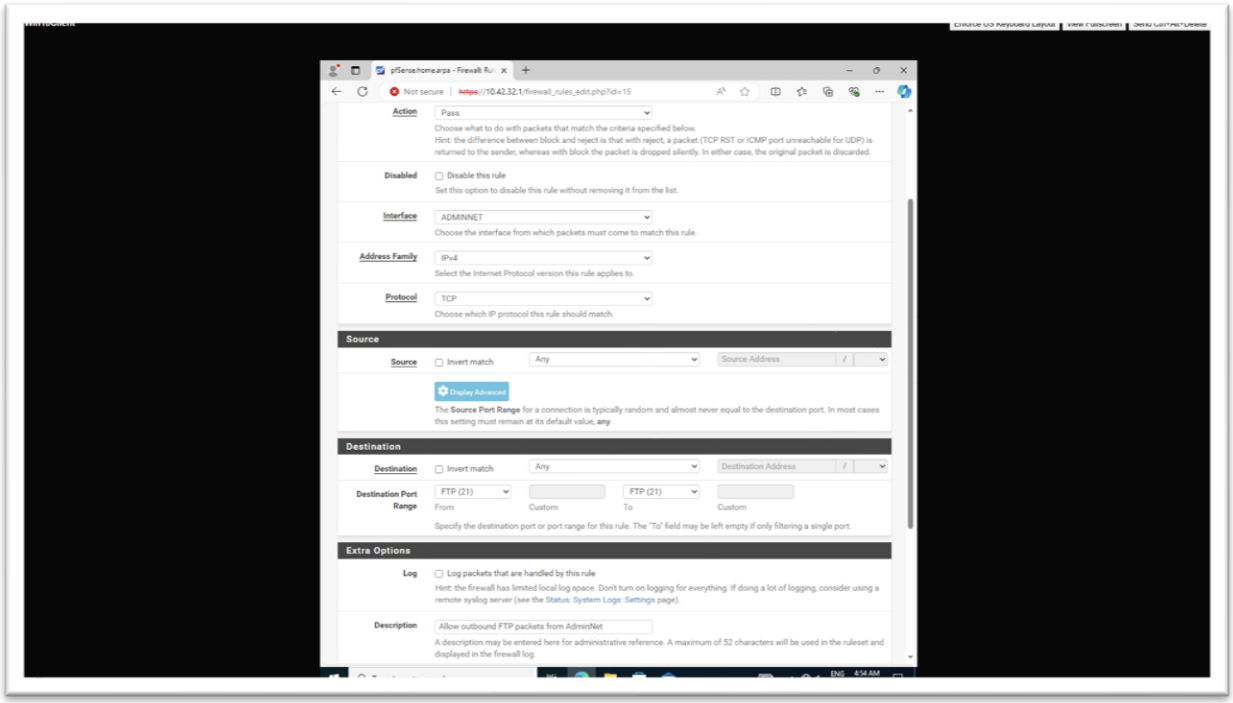

Figure 3: Screenshot of FTP firewall rule to allow outbound from AdminNet.

- As we can see in the above figure 3, basic configuration for setting up rule for allowing to outbound FTP packets. FTP contains the text data from a previous session of the File Transfer Protocol. FTP is a network protocol that enables the transfer of files between the hosts over the internet. So for source, we will use AdminNet address and in port we have to select FTP(21) and lastly add the description and click save.

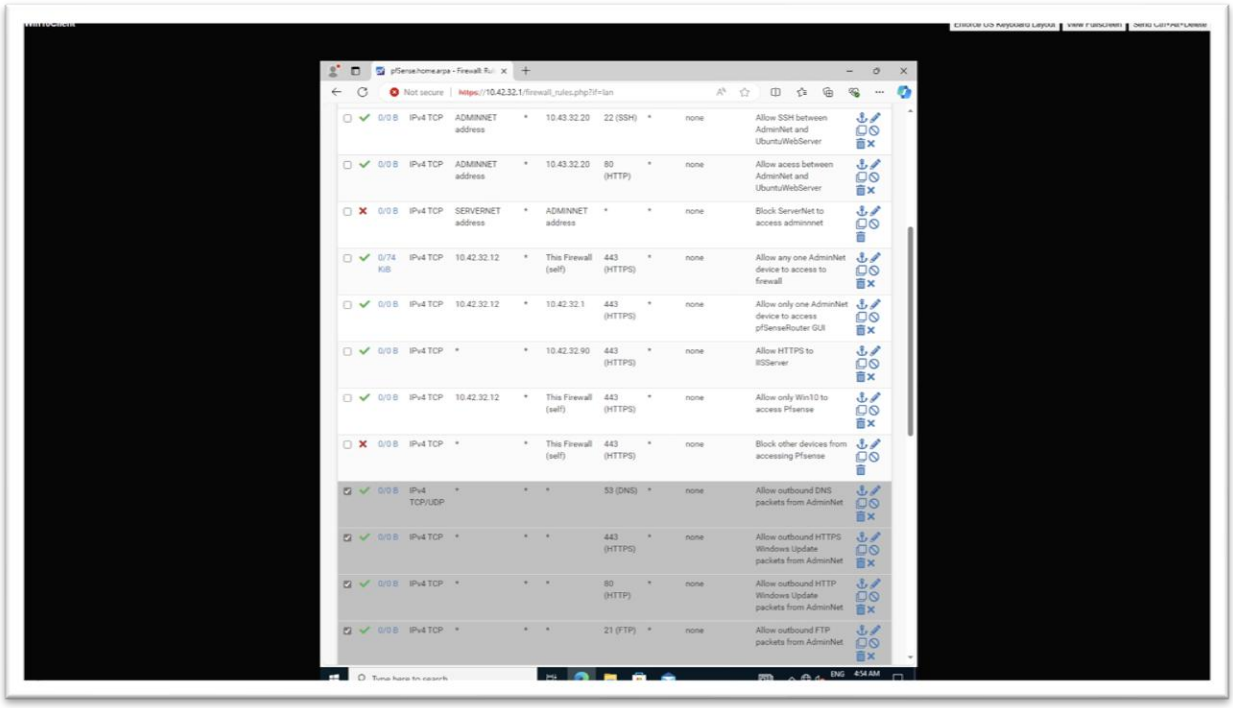

Figure 4: Screenshot of Highlighted firewall rules of FTP, Windows Update and DNS in AdminNet.

- So, from above figure 4, we can note that four rules are created for outbound in AdminNet and their description state's purpose of each rule.

3. Designate Only One Machine to Manage our Firewall

a. Disabling “Anti-Lookout Rule”

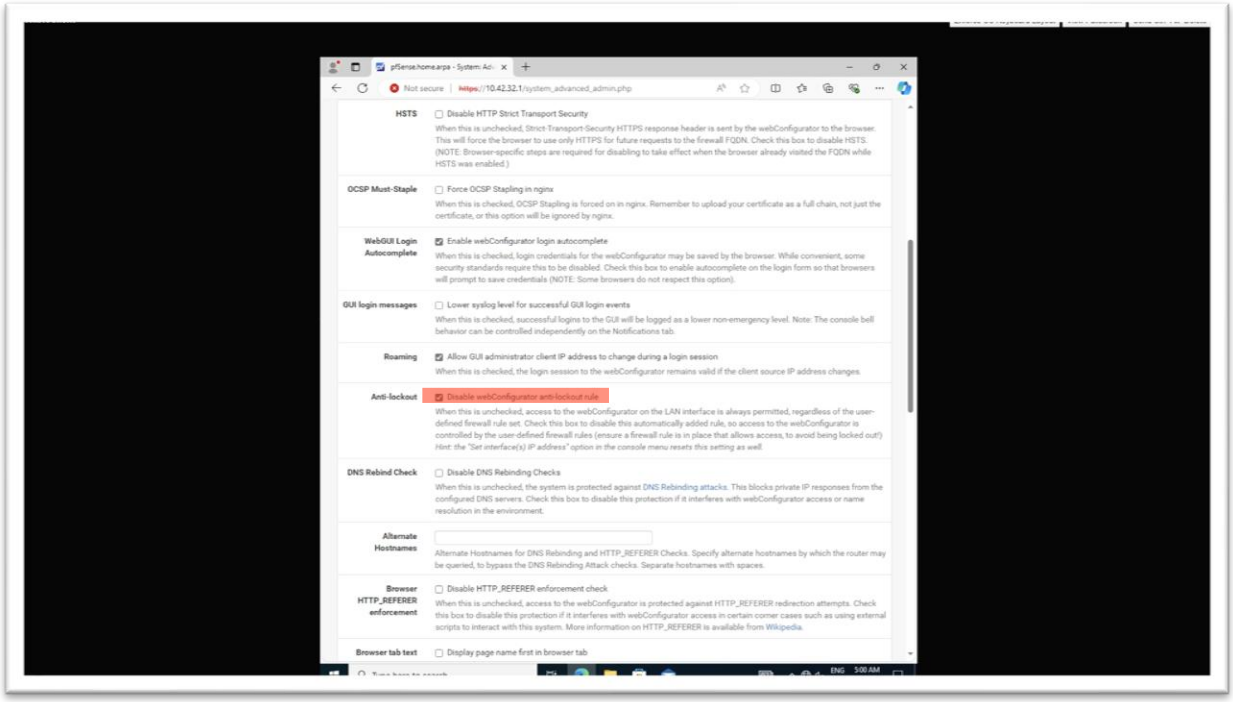

Figure 5: Screenshot of Enabling Anti-lockout rule.

- To enable Anti-Lockout rule, we navigate to “System>Advanced” and then scroll down to Anti-lockout option and select it as highlighted in Figure 5.

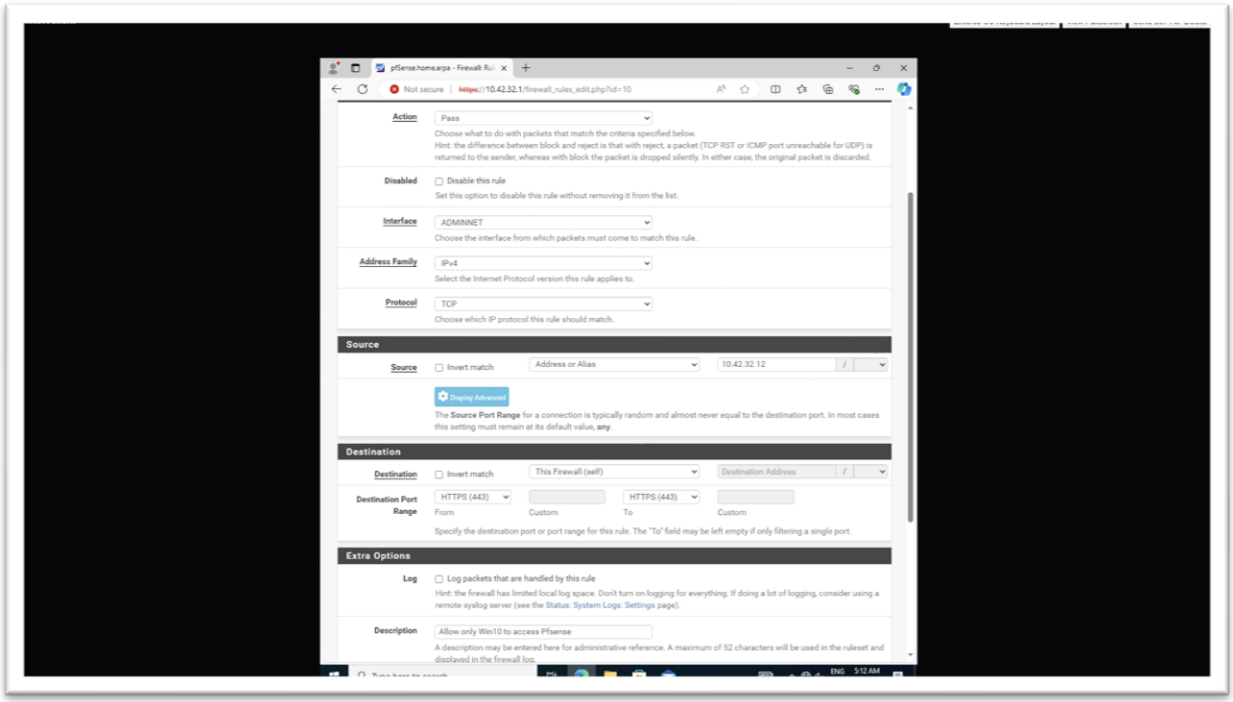

Figure 6: Screenshot of firewall rules to allow Win10 to access Pfsense.

- As we can see in the above figure 6, basic configuration for setting up rule for blocking other devices from accessing Pfsense. So, in the destination we have to select this firewall(self) and in port select HTTPS(443) as HTTPS is default connection for Pfsense. Then lastly add the description and click save.

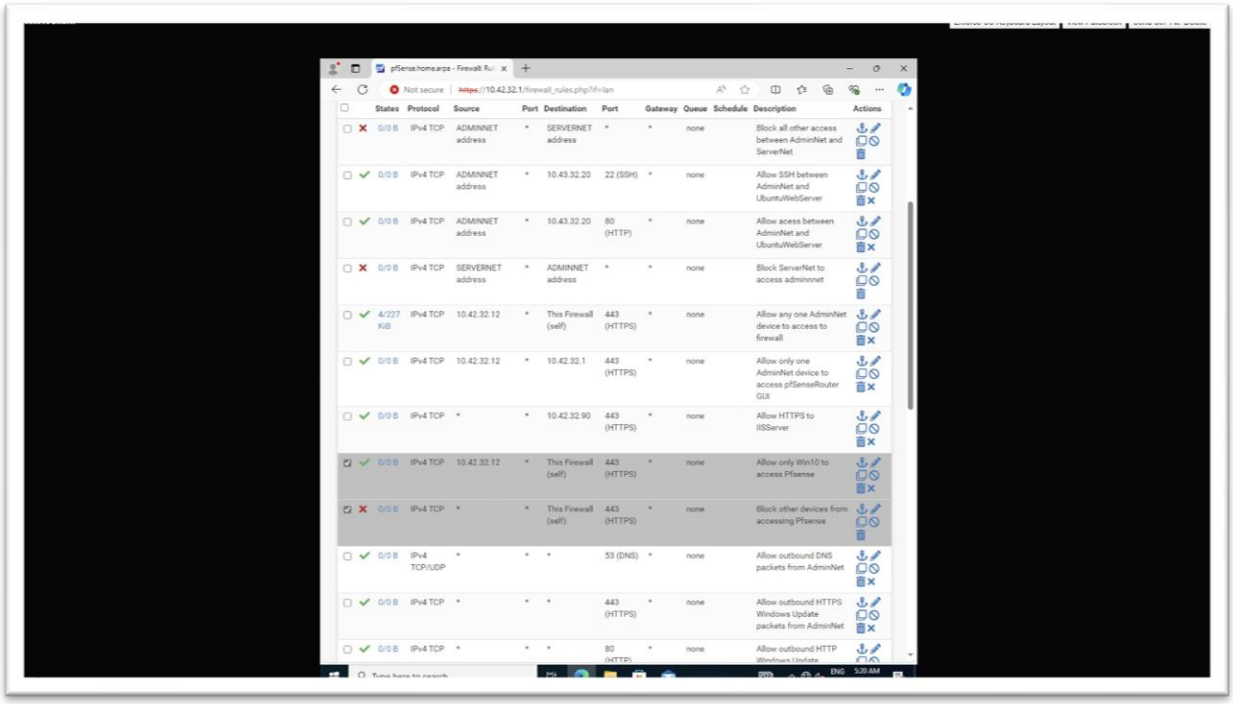

Figure 7: Screenshot of all Highlighted rules to allow one machine ot access Pfsense.

- So, from above figure 7, we can note that two rules are created for allowing one machine to access Pfsense and their description state's purpose of each rule.

4. Submitting Summary Screenshots of Firewall Rules

a. External Interface

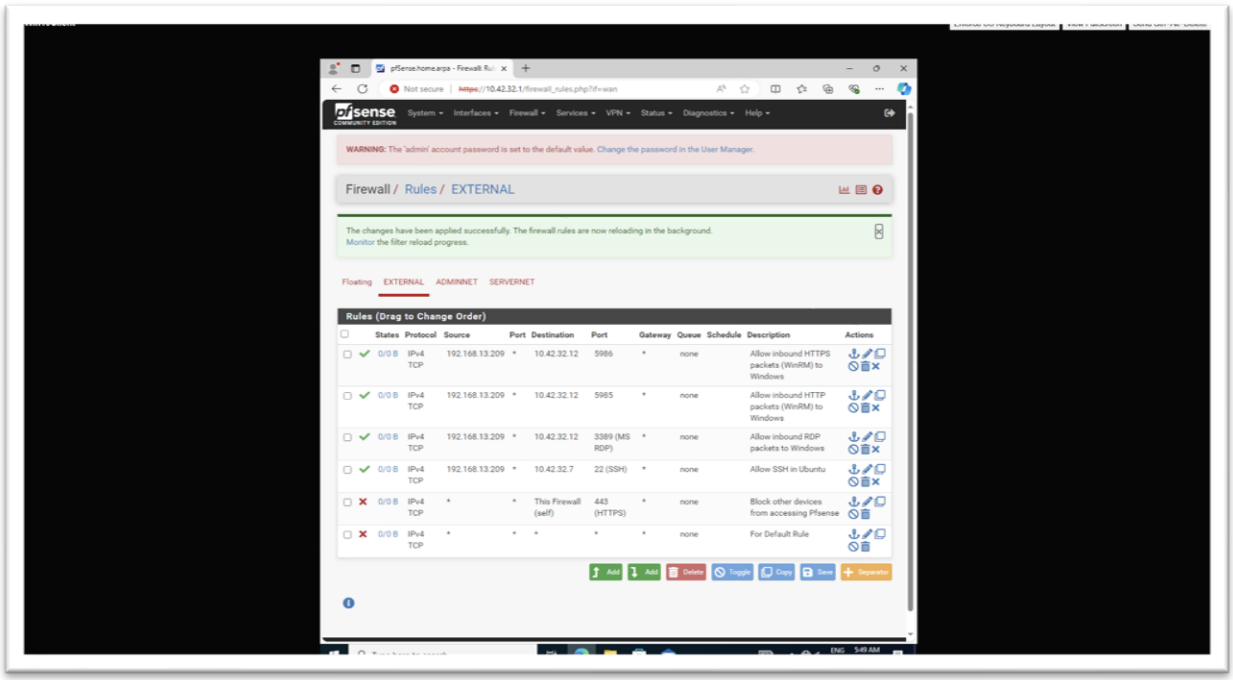

Figure 8: Screenshot of all firewall rules in "External Interface".

- Figure 8 shows all of the firewall rules in the "External Interface".

b. AdminNet Interface

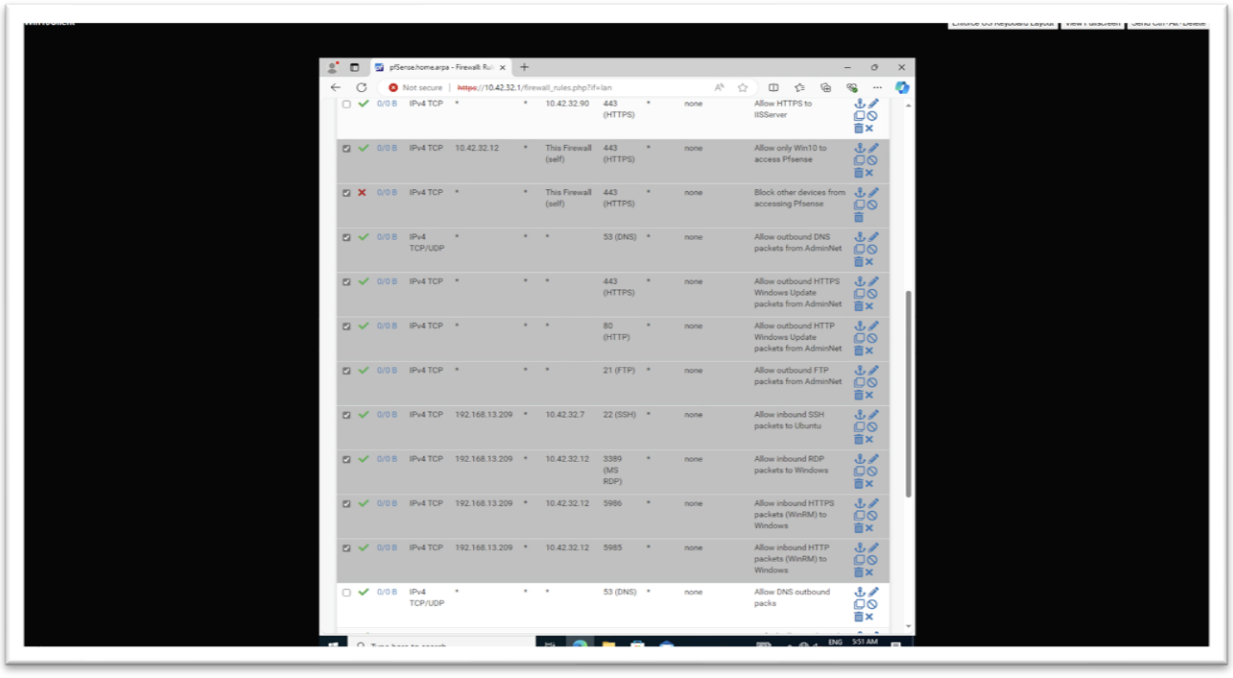

Figure 9: Screenshot of all firewall rules in "AdminNet Interface".

- Figure 9 shows all of the firewall rules in the "AdminNet Interface".

c. ServerNet

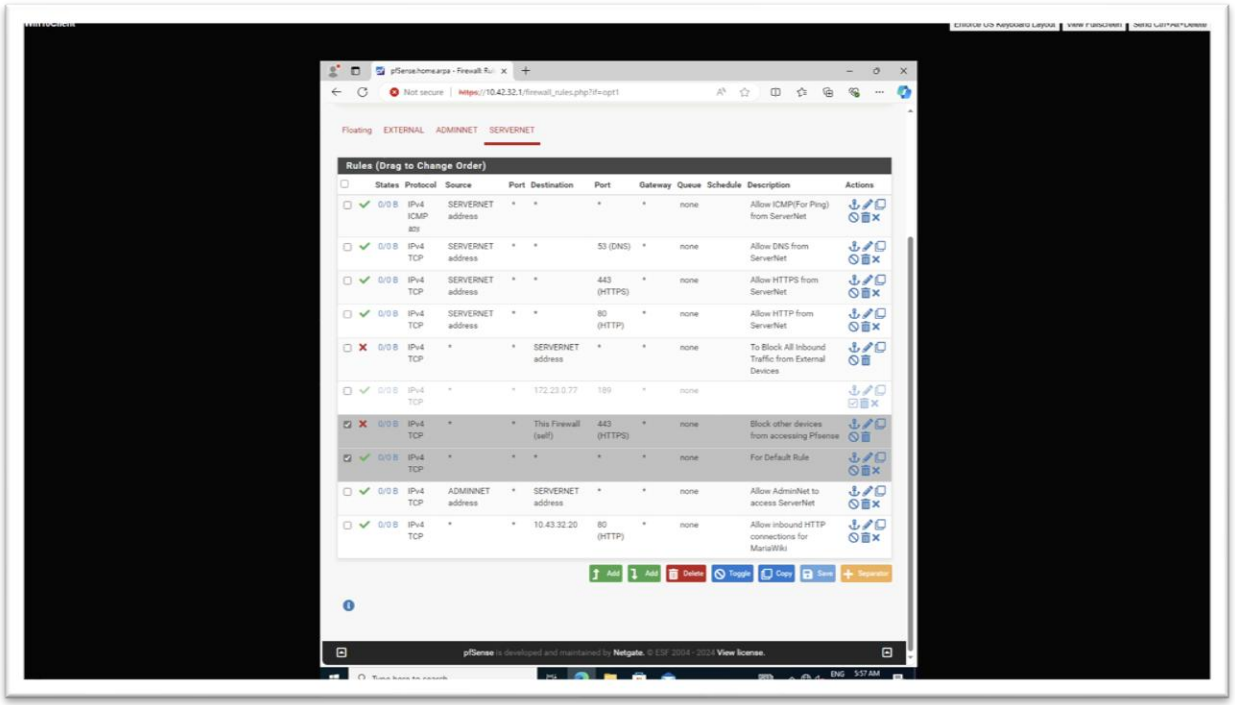

Figure 10: Screenshot of all firewall rules in "ServerNet Interface".

- Figure 10 shows all of the firewall rules in the "ServerNet Interface".

5. Update the Topology

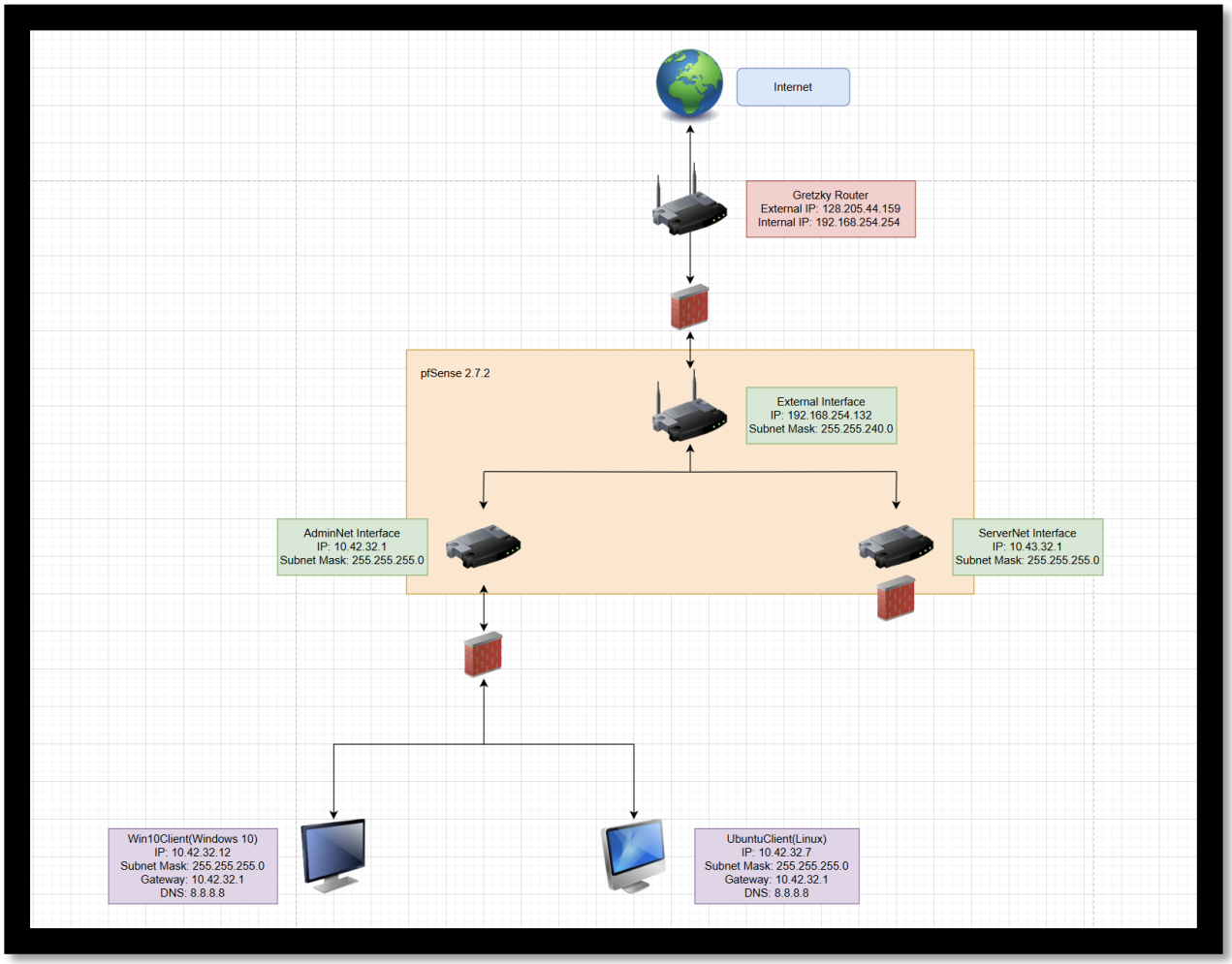

Figure 11: Screenshot of Updated Topology.

6. Testing

A. Testing the AdminNet outbound protocols

a. ICMP

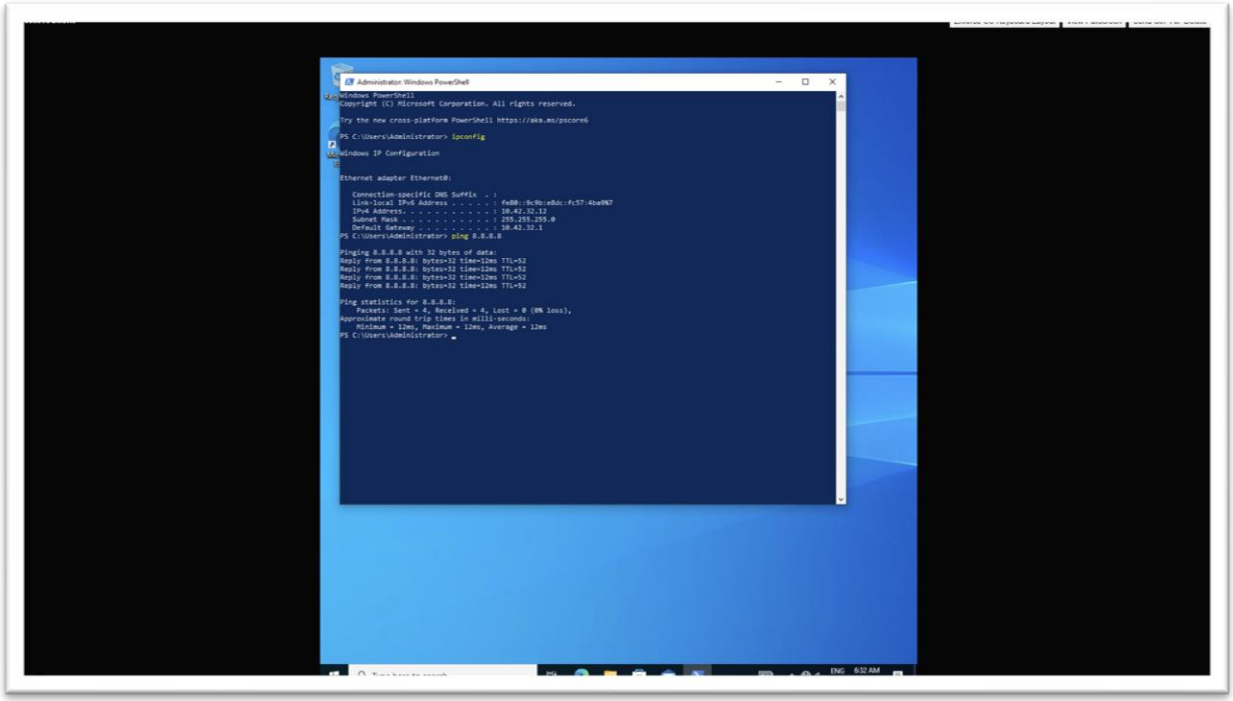

Figure 12: Screenshot of "ping 8.8.8.8" to test ICMP.

- Figure 12 shows the test for ICMP by pinging DNS of Google site by entering "ping 8.8.8.8" as highlighted.

b. HTTPS/DNS

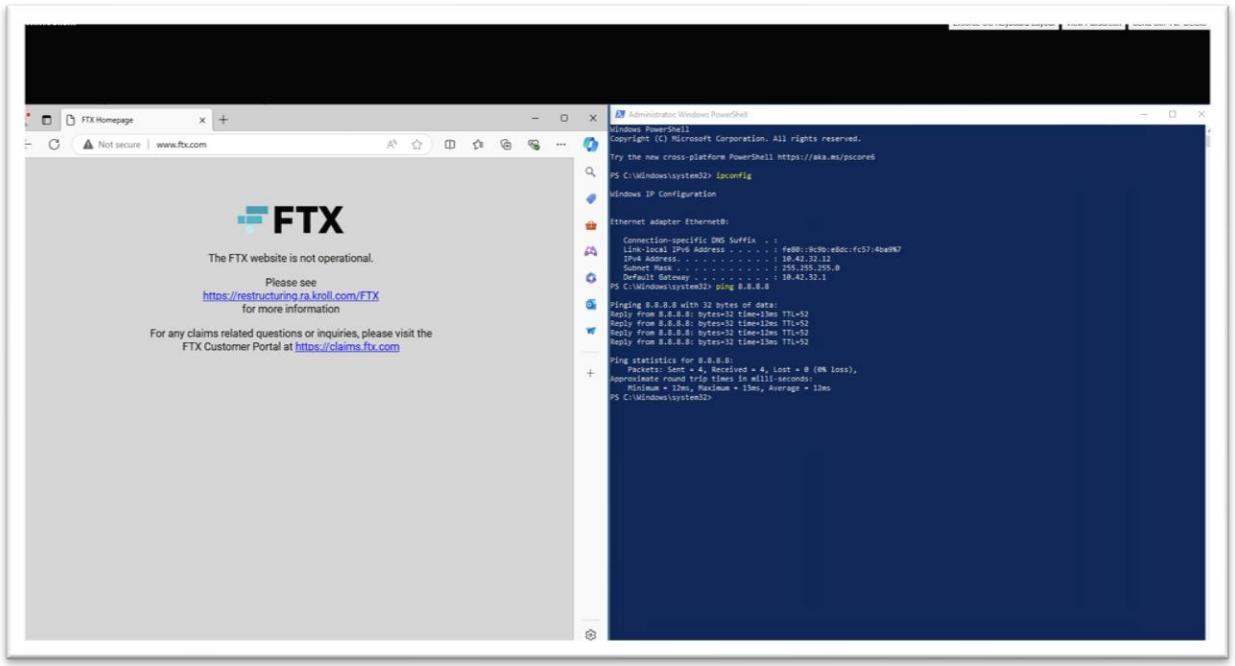

Figure 13: Screenshot of website "www.ftx.com" to check HTTP/DNS connection.

- Figure 13 shows the test for HTTPS/DNS by entering “www.ftx.com”.

c. HTTP/DNS

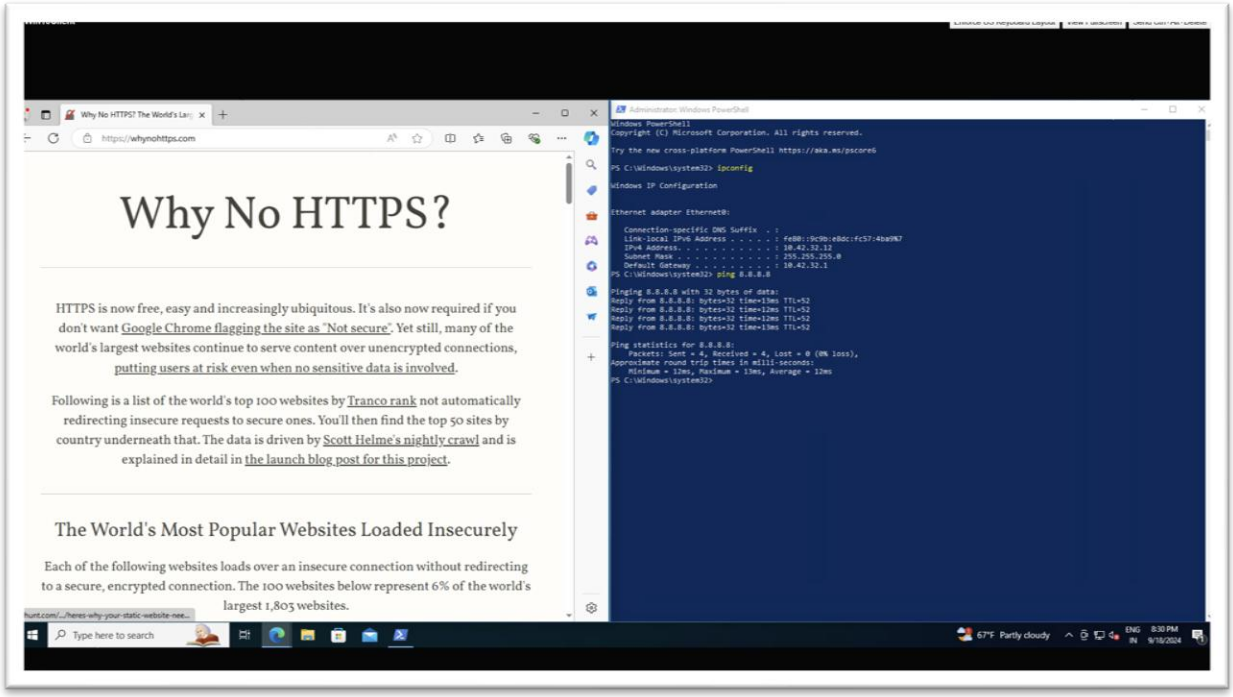

Figure 14: Screenshot of website “www.whynohttps.com” to check HTTP/DNS connections.

- Figure 14 shows the test for HTTP/DNS by entering “www.whynohttps.com”.

d. FTP

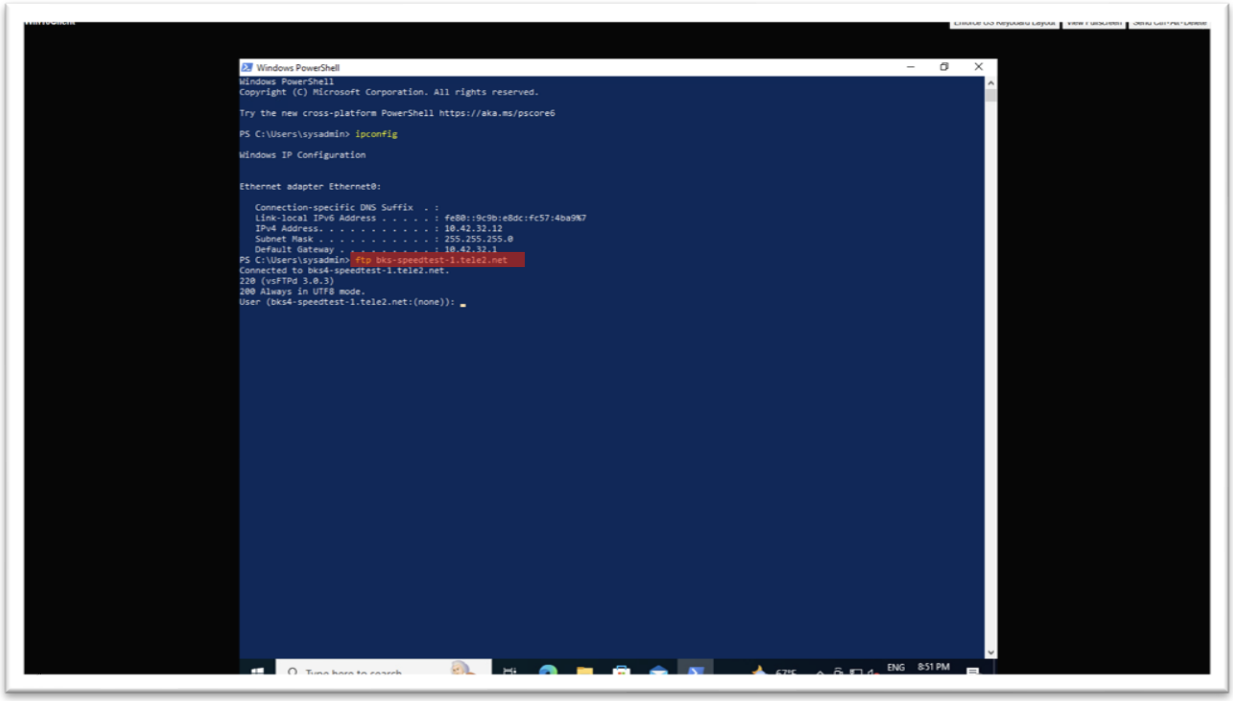

Figure 15: Screenshot of FTP command by entering “ftp bks-speedtest-1.tele2.net”

- Figure 15 shows the test for FTP by entering “ftp bks-speedtest-1.tele2.net” as highlighted above.

e. Windows Update

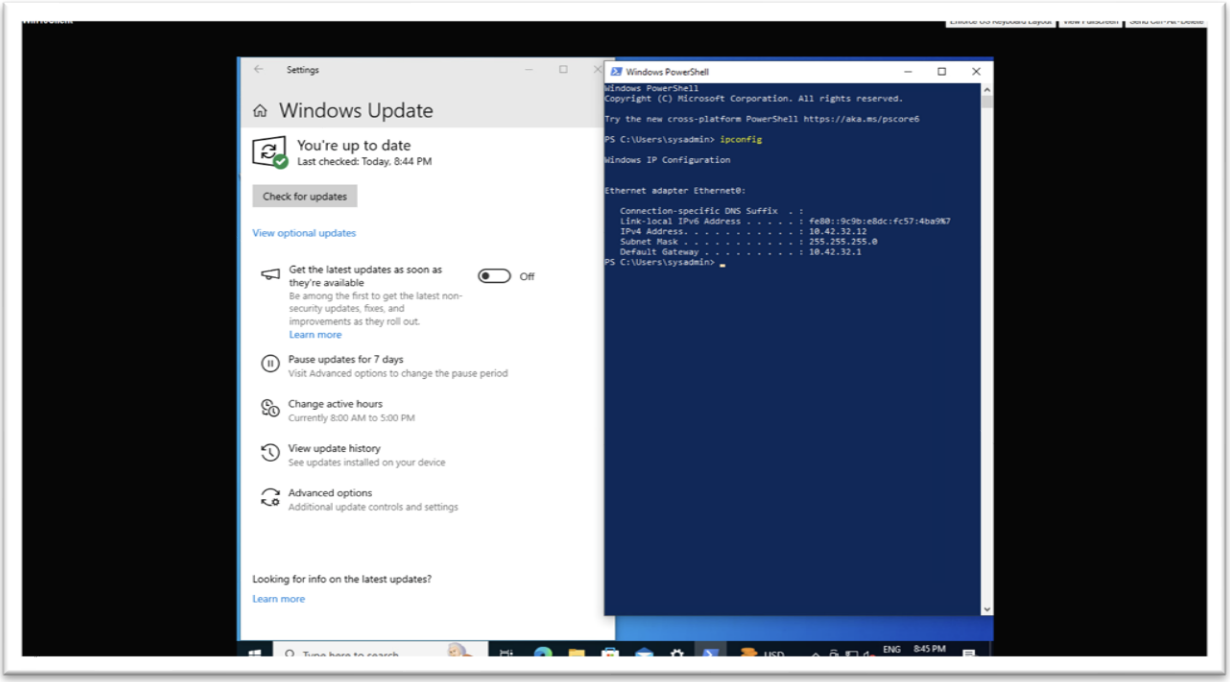

Figure 16: Screenshot for checking of Windows Update is working.

- To check that Windows Update is working or not, one can navigate to Settings>Windows Update then if it shows no error then Update is working properly as shown in figure 16.

B. Testing the AdminNet outbound protocols

a. Running test command

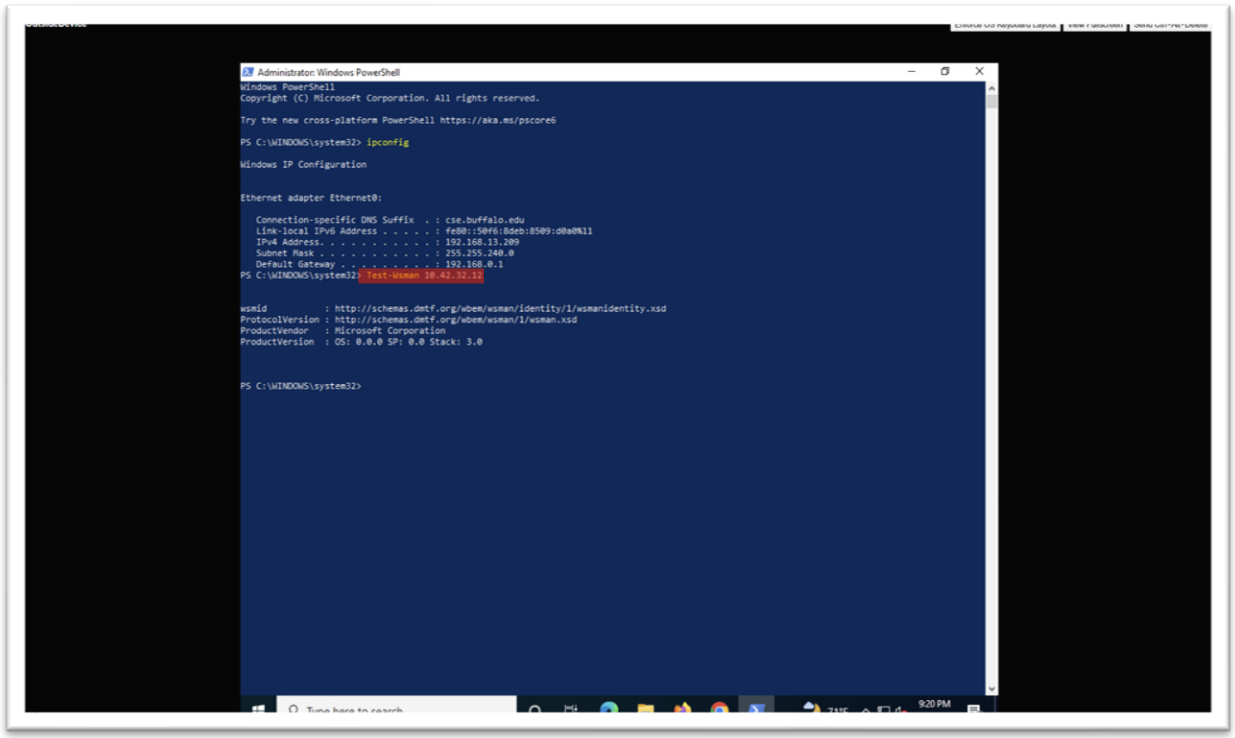

Figure 17: Screenshot of command “test-wsman 10.42.32.12" to check AdminNet outbound.

- To test that the outbound to AdminNet protocol works, enter “test-wsman 10.42.32.12” and we can get the result as shown in figure 17.

b. Remote Desktop Connection Tool

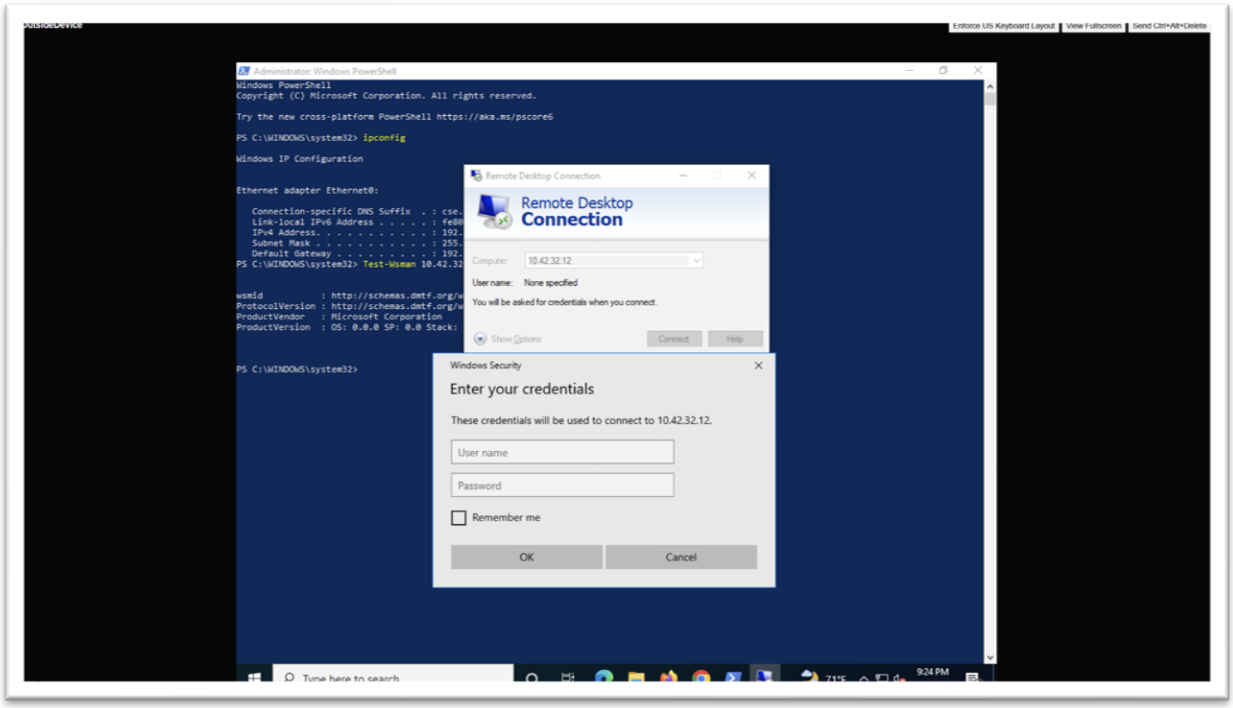

Figure 18: Screenshot of a functional Remote Desktop Connection Tool.

- Now we open “Remote Desktop Connection” and connect to the IP address of Win10Client. If you the “credentials windows” (as shown in figure 18) then it’s a success.

c. PuTTY

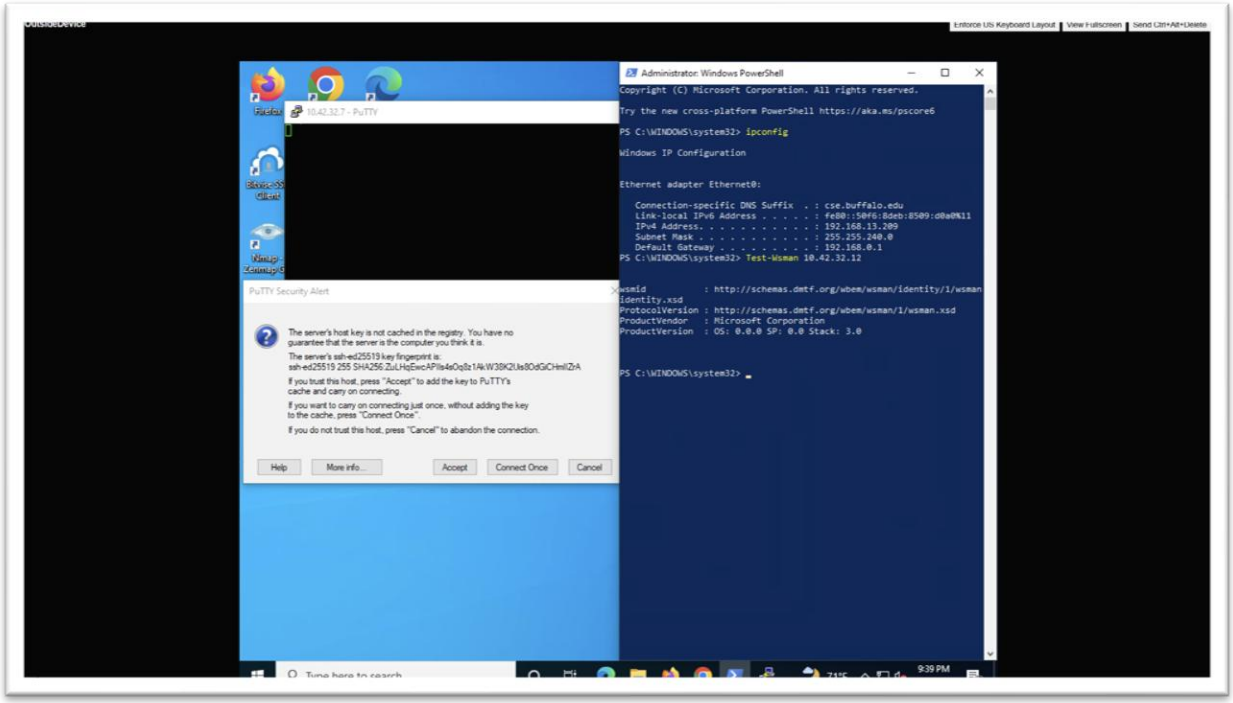

Figure 19: Screenshot of PuTTY security alert message.

- So now we download “PuTTY” to connect to UbuntuClient using SSH. After entering “Ubuntu IP address in Host Name” and if we get “PuTTY Security Alert” (as shown in figure 19) then it’s a success.

d. Ping “UbuntuClient”

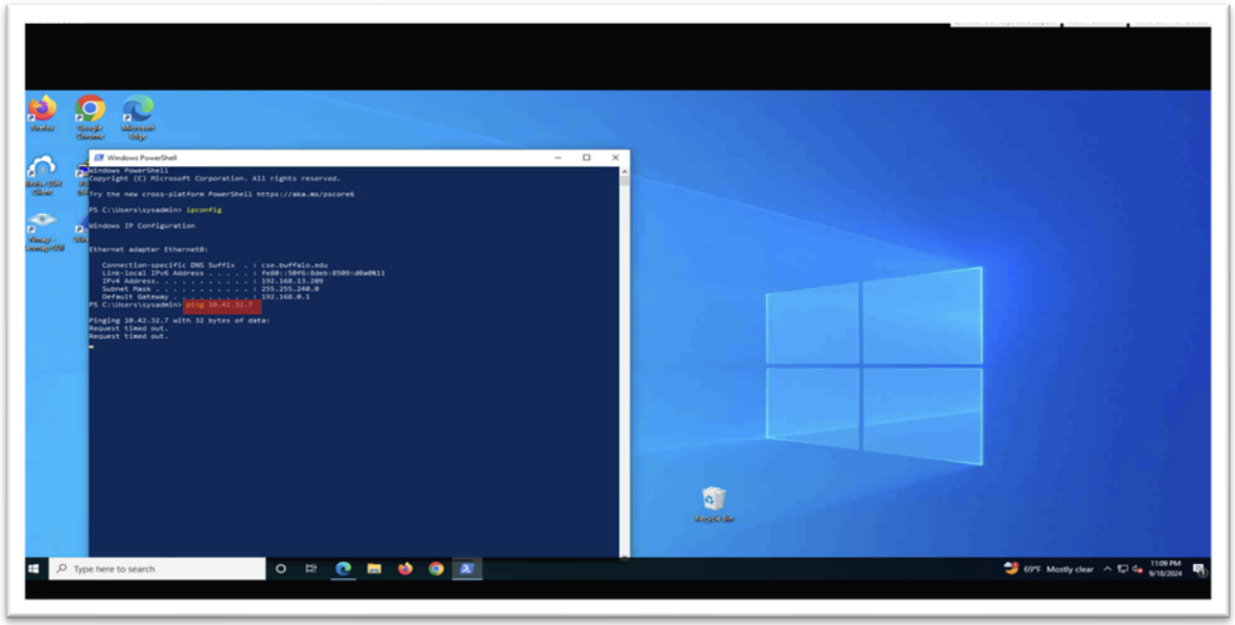

Figure 20: Screenshot of highlighted “ping 10.42.32.7” to communicate with Ubuntu Client.

- After that we can check if we can communicate with Ubuntu Client by pinging its IP Address by entering “ping 10.42.32.7 as highlighted in figure 20.

- Test the only one machine where we manage the firewall

➢ For OutsideDevice

a. HTTP

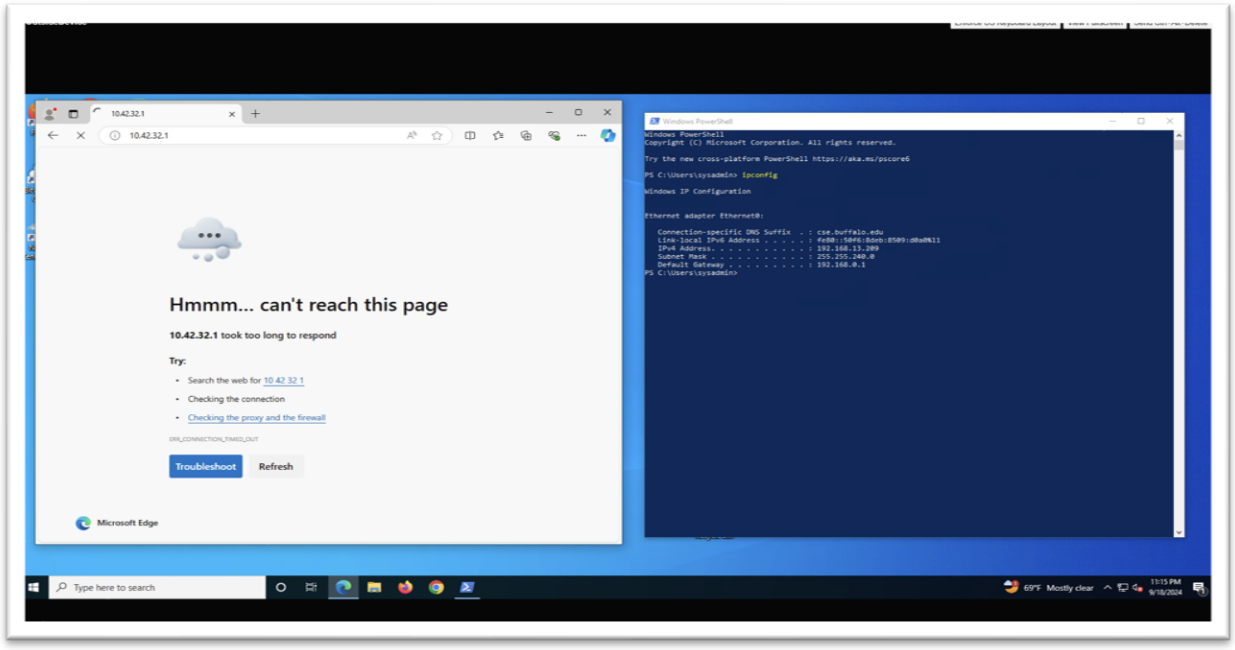

Figure 21: Screenshot of accessing HTTP for Pfsense from OutsideDevice.

- So, we can check if OutsideDevice can access Pfsense for HTTP by entering the “URL of 10.42.32.1” (as shown in figure 21) which will not load which means that firewall is blocking it properly.

b. HTTPS

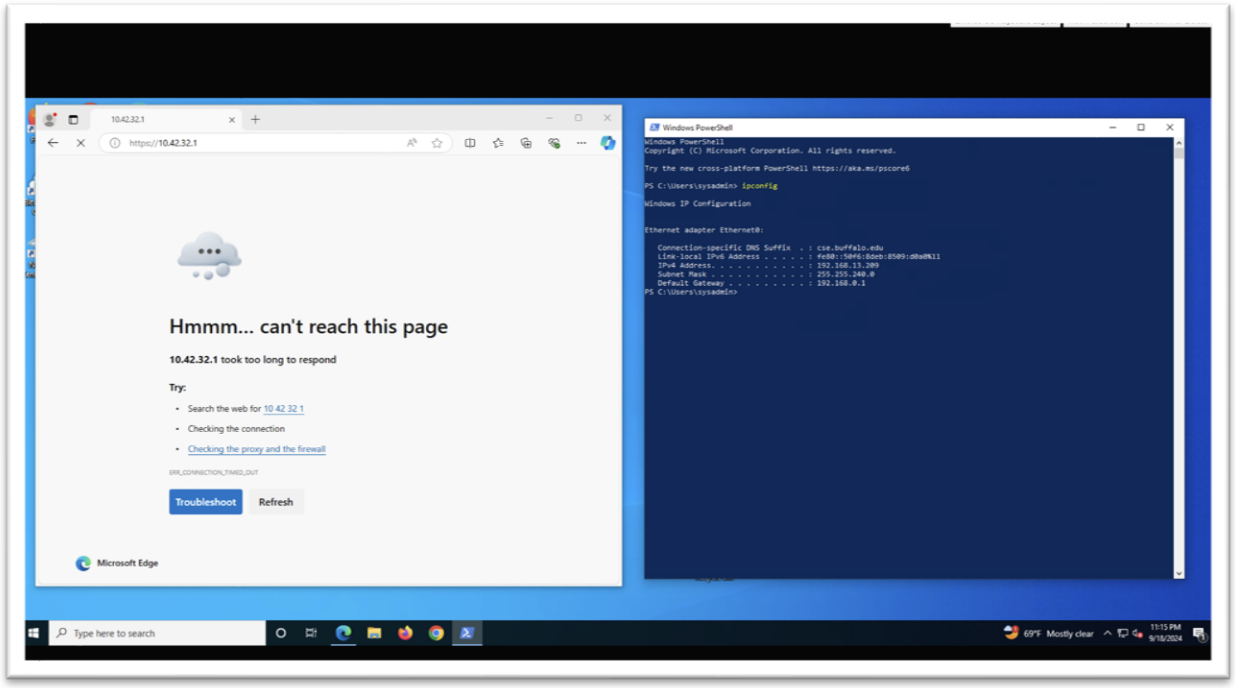

Figure 22: Screenshot of accessing HTTPS for Pfsense from OutsideDevice.

- So now we will do the same for HTTPS and we can observe the same result that the page is not loading.

c. SSH

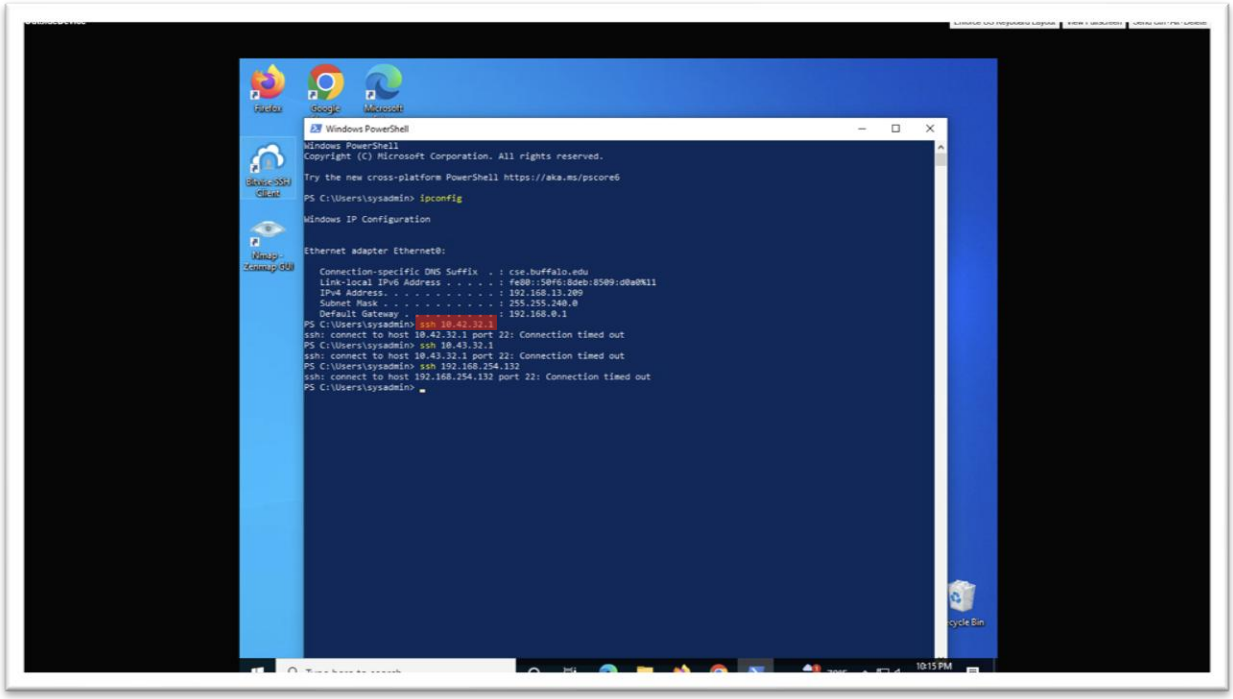

Figure 23: Screenshot of ssh commands using “ssh 10.42.32.1”.

- Now we will check for ssh connection by using “ssh 10.42.32.1” as highlighted in figure 23.

➢ For UbuntuClient

a. HTTP

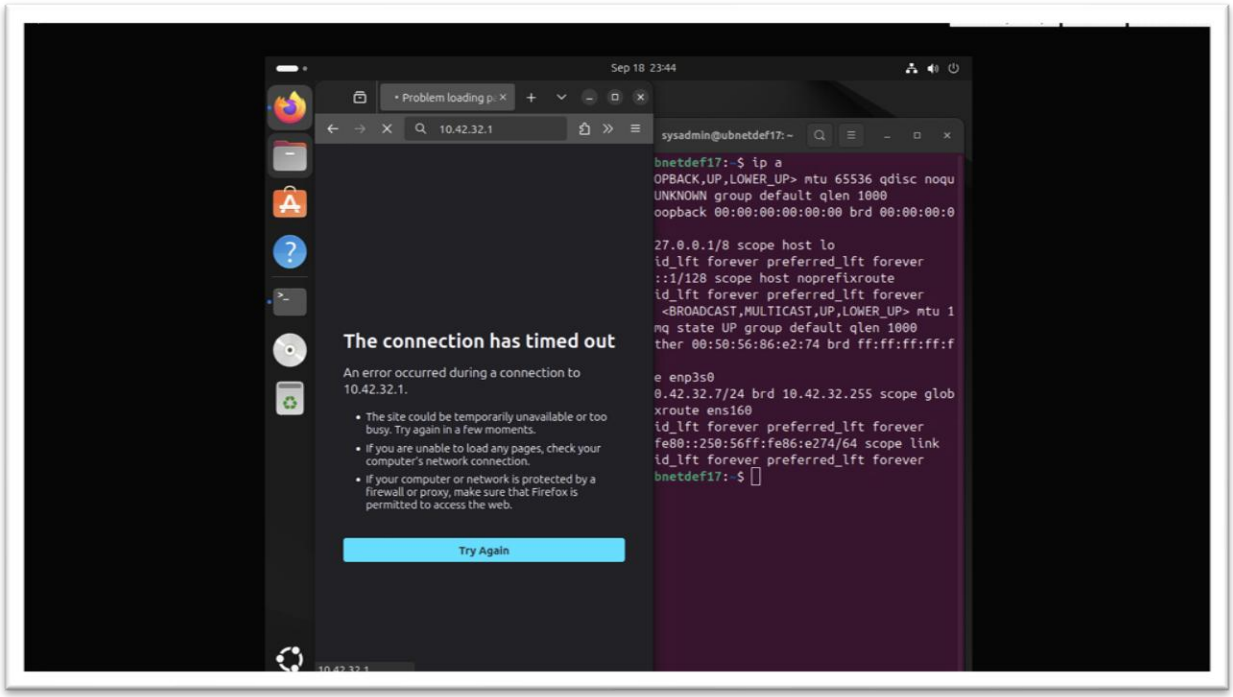

Figure 24: Screenshot of accessing HTTP for Pfsense from UbuntuClient.

- So, we can check if UbuntuClient can access Pfsense for HTTP by entering the “URL of 10.42.32.1” (as shown in figure 24) which will not load which means that firewall is blocking it properly.

b. HTTPS

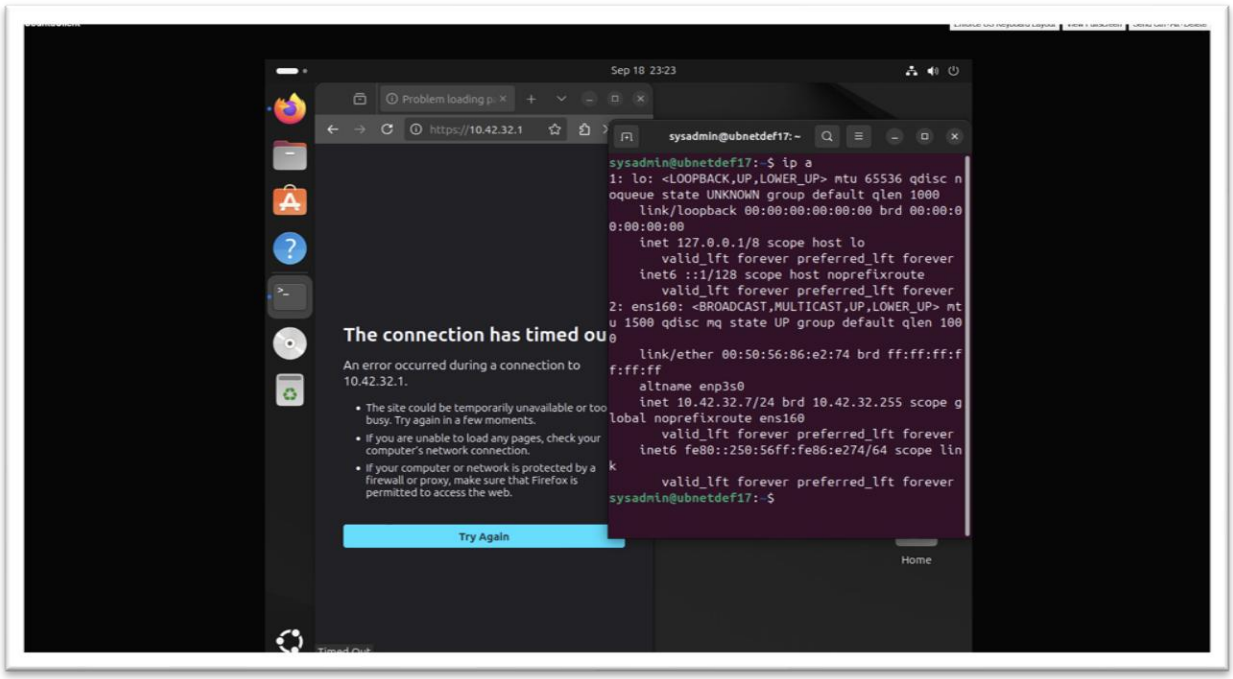

Figure 25: Screenshot of accessing HTTPS for Pfsense from UbuntuClient.

- So now we will do the same for HTTPS and we can observe the same result that the page is not loading.

c. SSH

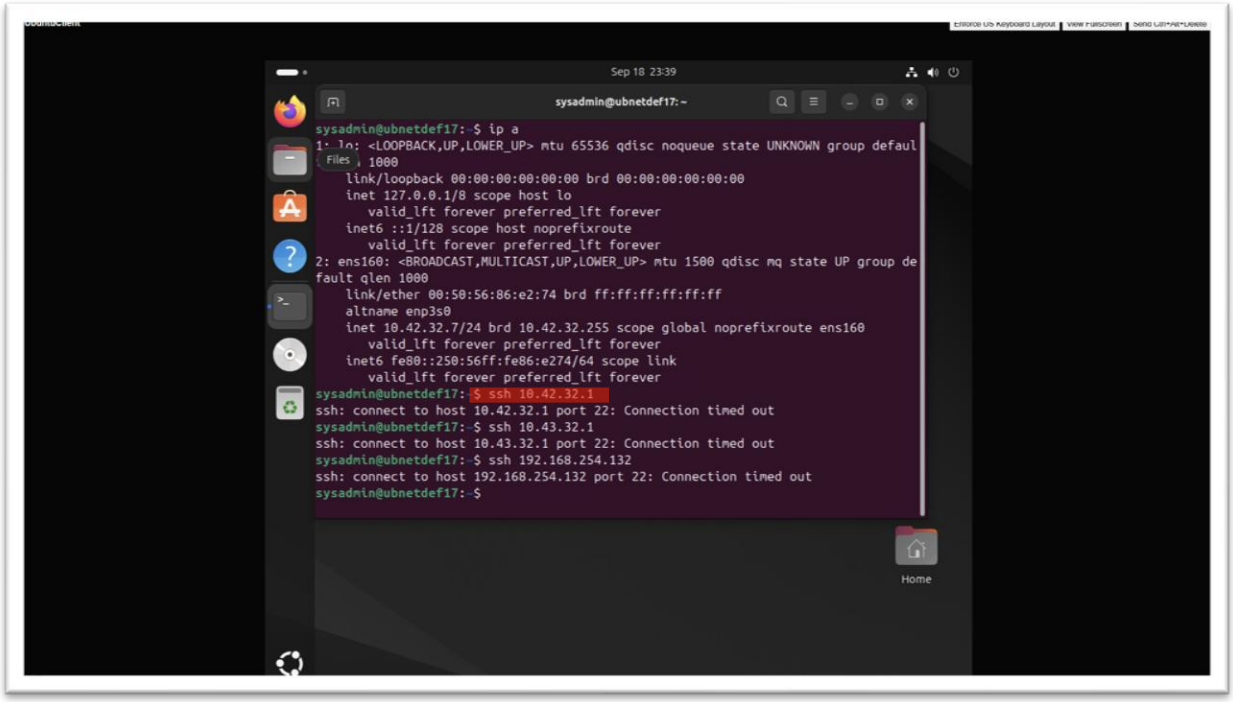

Figure 26: Screenshot of ssh commands to Pfsense from UbuntuClient.

- So to check the "ssh connections to Pfsense" from UbuntuClient as shown in figure 26.

➢ Testing for one allowed device (Windows 10 Client)

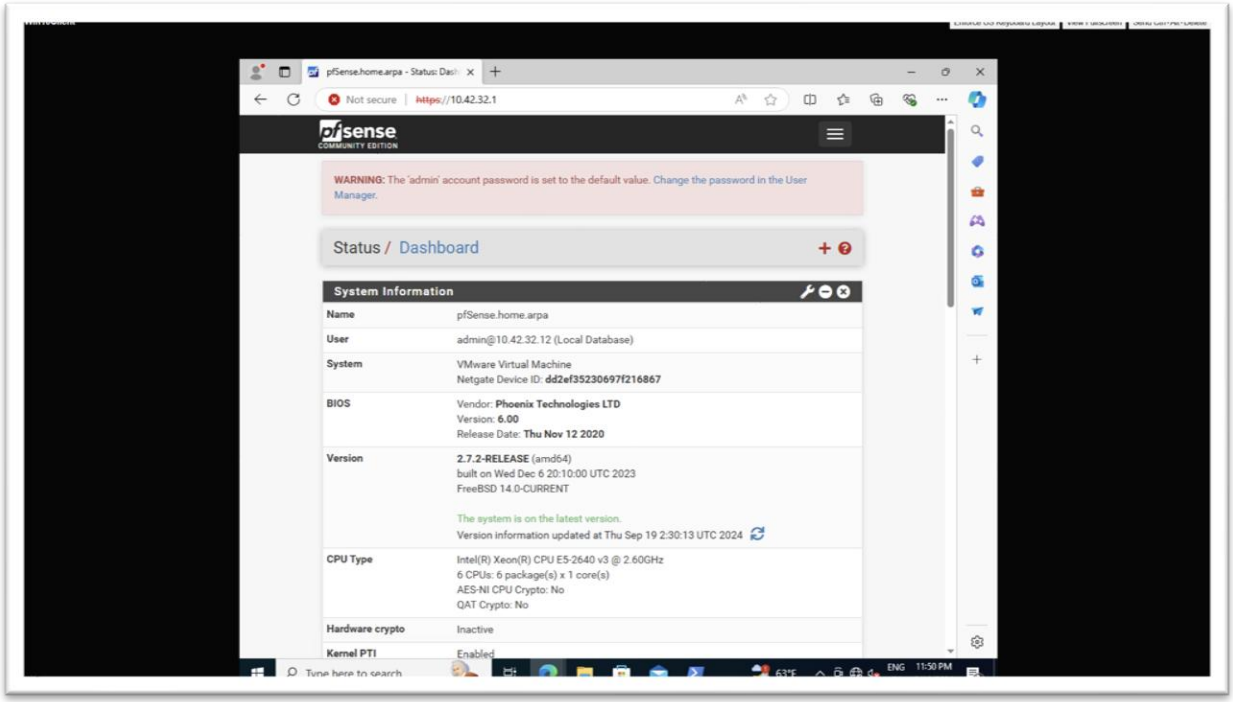

Figure 27: Screenshot of verifying if Pfsense can be accessed on Win10Client.

- Now as to check if we can access Pfsense through Win10Client. As shown in figure 27, we can access Pfsense.

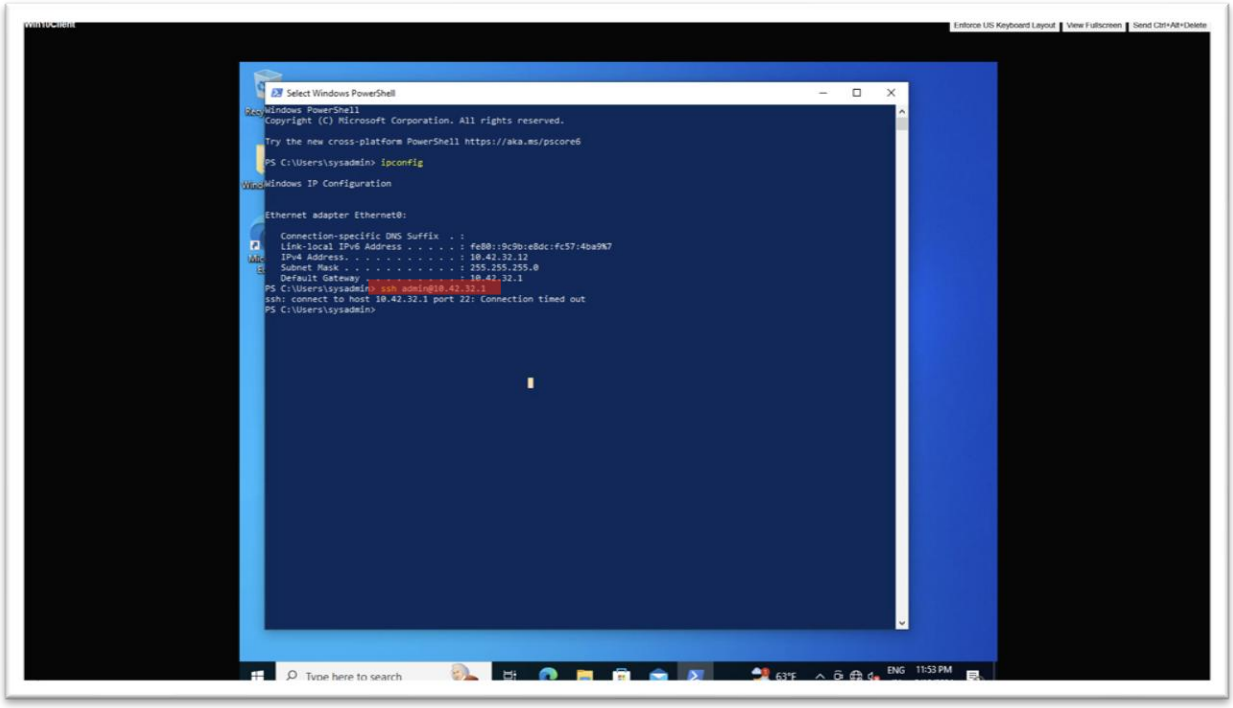

Figure 28: Screenshot of ssh to access Pfsense on Win10Client.

- Now we will check for ssh connection to Pfsense by using “ssh admin@10.42.32.1” as highlighted in figure 28.

7. Additional Task of Memo Page

To: CEO Kevin Cleary

From: Faraz Ahmed, Security Engineer

Date: September 18th 2024

Subject: To append changes to existing firewall rules by following firewall policy in place.

I am writing this memo to bring your attention to the need to update our existing firewall rules table by conducting a review of our current firewall policy. As we progress with time, so does the importance of cybersecurity so it's essential to update our existing firewall rules.

So, after reviewing and studying about the existing firewall rules, I updated the firewall table to follow new firewall policy in place and want your approval to attach this updated firewall table in real time. Now, I will showcase you the proposed firewall rules in tabular form as shown below :-

Rule	Protocol	Source	Port	Destination	Port	Gateway
Allow	IPv4 TCP	*	*	173.23.0.12	80	*
Allow	IPv4 TCP	*	*	173.23.0.12	443	*
Allow	IPv4 UDP	*	*	172.23.0.12	8080	*
Allow	IPv4 UDP	*	*	172.23.0.1	3306	*
Disallow	IPv4 TCP	*	*	*	3306	*
Disallow	IPv4 TCP	*	*	*	1234	*
Allow	IPv4 TCP	*	*	*	*	*
Allow	IPv4 TCP	*	*	172.23.0.68	119	*
Allow	IPv4 TCP	123.165.151.32	*	172.23.0.77	22	*
Allow	IPv4 TCP/UDP	*	*	172.23.0.8	189	*
Allow	IPv4 TCP	173.74.82.94	*	172.23.0.50	5432	*
Allow	IPv4 UDP	172.23.0.12	*	*	123	*
Allow	IPv4 TCP	*	*	172.23.0.12	80	*
Allow	IPv4 TCP	*	*	172.23.0.12	443	*

These modifications are critical in ensuring our network remains safe and secure while allowing necessary operations to continue smoothly. Please feel free to reach out if you have any questions or need any more changes in the table.

Thank You for your time.

Yours sincerely,

Faraz Ahmed

Security Engineer

UBNetDef SysSec

fahmed29@buffalo.edu