

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

3 hours, 45 minutes

Progress:

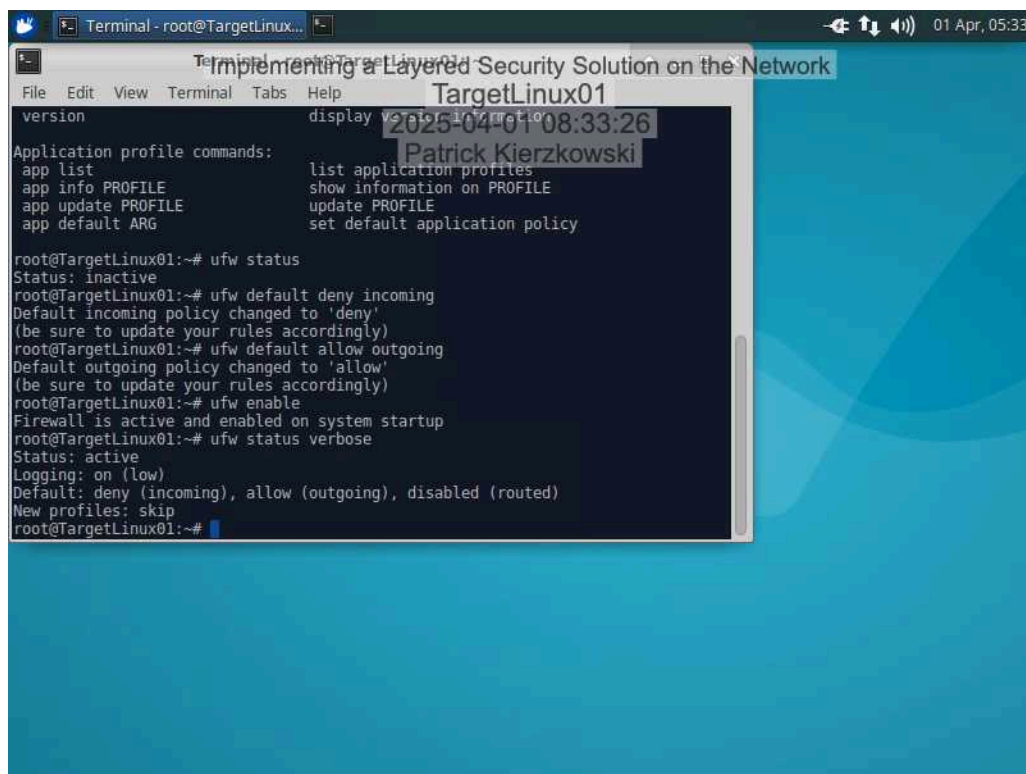
100%

Report Generated: Monday, July 7, 2025 at 9:47 PM

Section 1: Hands-On Demonstration

Part 1: Configure an Endpoint Firewall

10. **Make a capture** showing the **current status and ruleset for your running UFW configuration**.

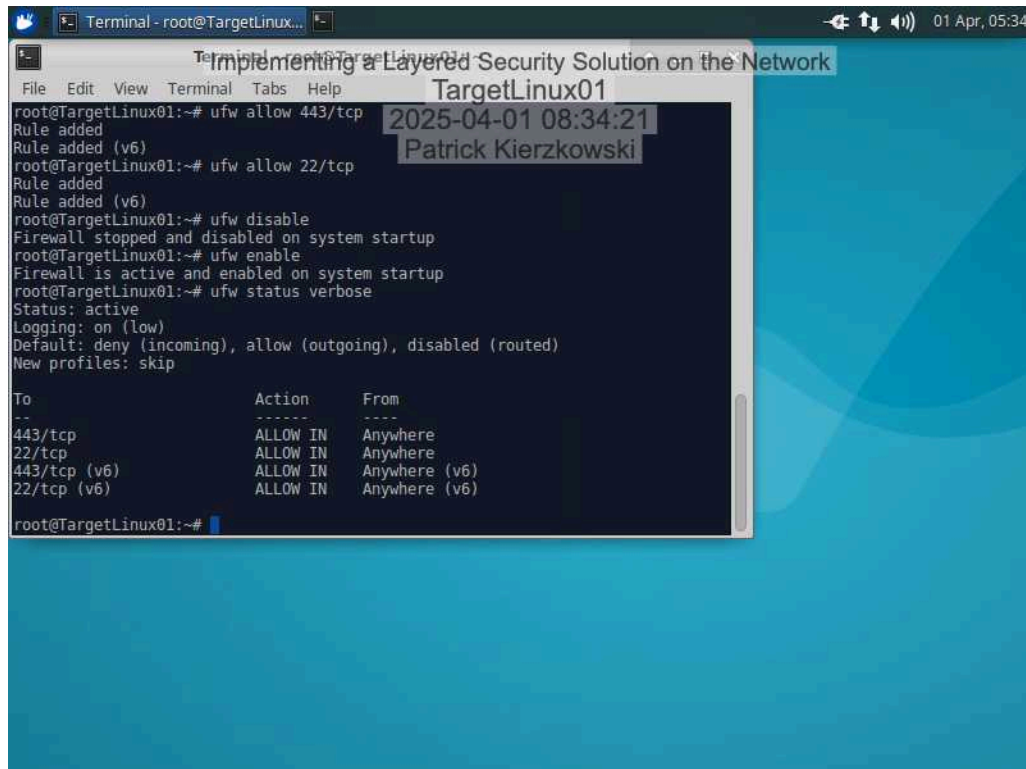


The screenshot shows a terminal window titled "Terminal - root@TargetLinux01" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output shows the following commands and their results:

```
root@TargetLinux01:~# ufw status
Status: inactive
root@TargetLinux01:~# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@TargetLinux01:~# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@TargetLinux01:~# ufw enable
Firewall is active and enabled on system startup
root@TargetLinux01:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
root@TargetLinux01:~#
```

Overlaid on the terminal is a semi-transparent box containing the text: "Implementing a Layered Security Solution on the Network", "TargetLinux01", "2025-04-01 08:33:26", and "Patrick Kierzkowski".

16. Make a capture showing the **current status** and **ufw ruleset** in the output.

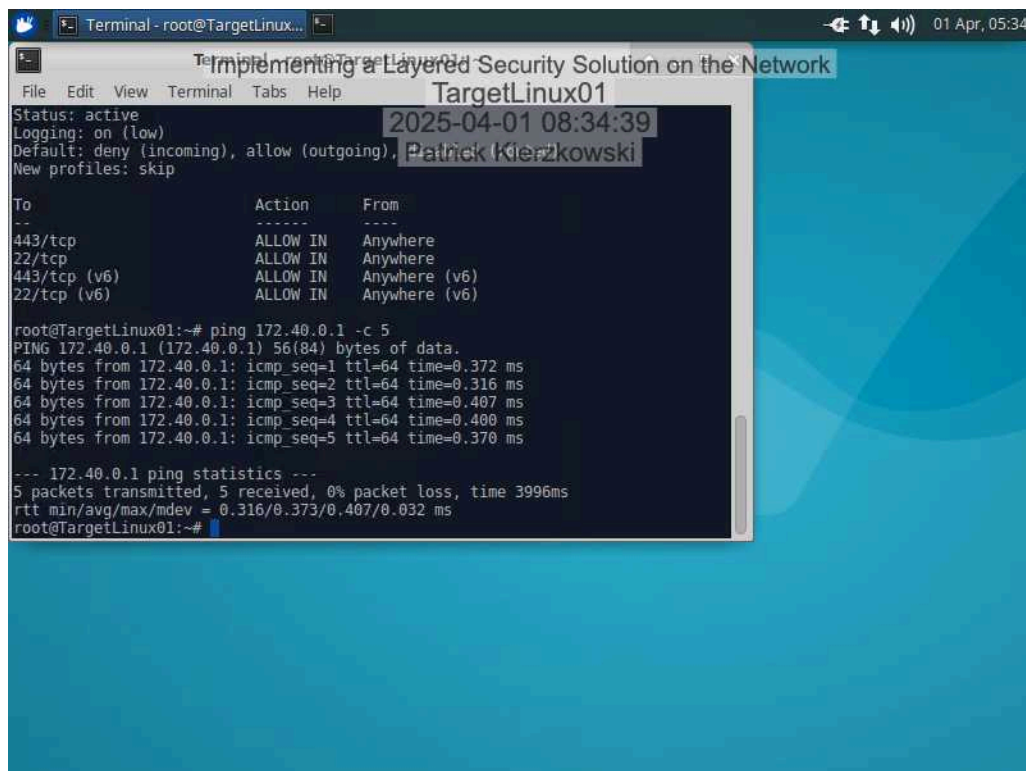


A terminal window titled "Terminal - root@TargetLinux01" showing the configuration and status of the UFW firewall. The user has added rules for 443/tcp and 22/tcp for both IPv4 and IPv6, disabled the firewall, and then re-enabled it. The status is active, and the ruleset is displayed as follows:

```
root@TargetLinux01:~# ufw allow 443/tcp
Rule added
root@TargetLinux01:~# ufw allow 22/tcp
Rule added
root@TargetLinux01:~# ufw disable
Firewall stopped and disabled on system startup
root@TargetLinux01:~# ufw enable
Firewall is active and enabled on system startup
root@TargetLinux01:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
443/tcp ALLOW IN Anywhere
22/tcp ALLOW IN Anywhere
443/tcp (v6) ALLOW IN Anywhere (v6)
22/tcp (v6) ALLOW IN Anywhere (v6)
```

18. Make a screen capture showing the **successful ping** to the DMZ interface.

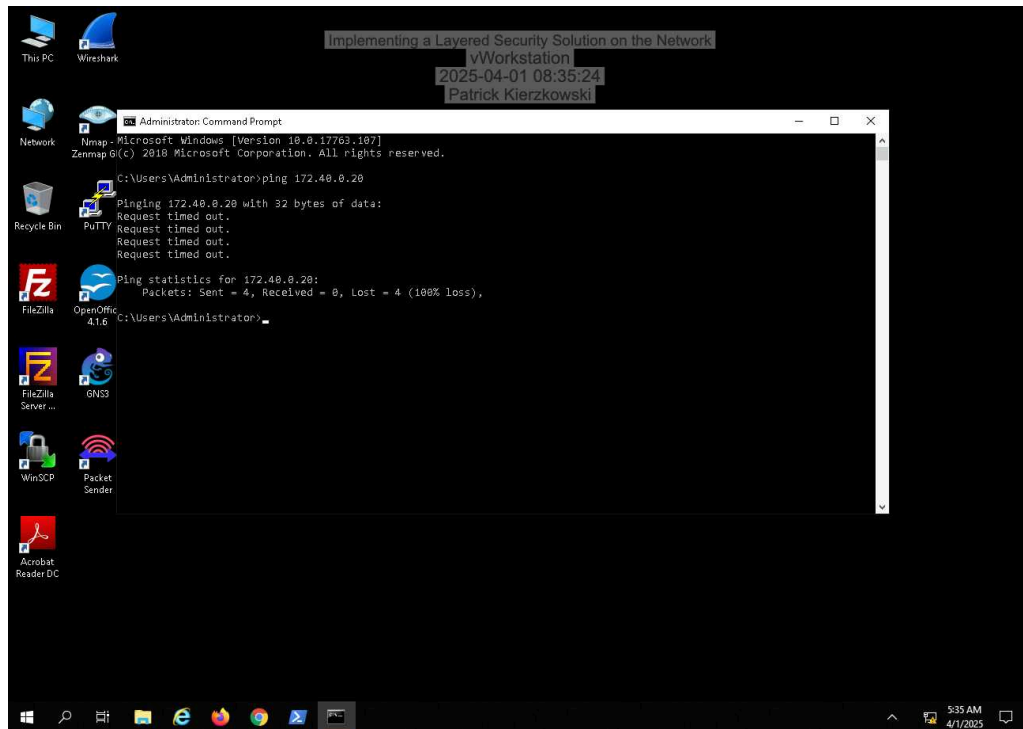


A terminal window titled "Terminal - root@TargetLinux01" showing the output of a ping command to 172.40.0.1. The firewall status is active, and the ruleset is the same as in the previous screenshot. The ping command is successful, showing 5 packets transmitted with 0% packet loss.

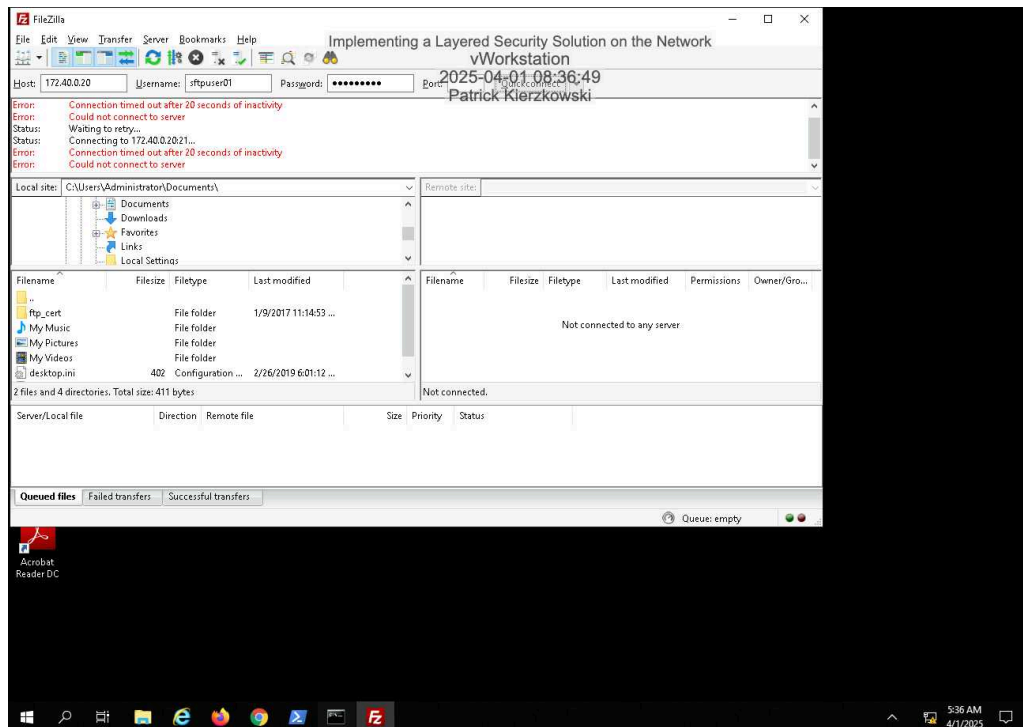
```
root@TargetLinux01:~# ping 172.40.0.1 -c 5
PING 172.40.0.1 (172.40.0.1) 56(84) bytes of data:
64 bytes from 172.40.0.1: icmp_seq=1 ttl=64 time=0.372 ms
64 bytes from 172.40.0.1: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 172.40.0.1: icmp_seq=3 ttl=64 time=0.407 ms
64 bytes from 172.40.0.1: icmp_seq=4 ttl=64 time=0.400 ms
64 bytes from 172.40.0.1: icmp_seq=5 ttl=64 time=0.370 ms

--- 172.40.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.316/0.373/0.407/0.032 ms
root@TargetLinux01:~#
```

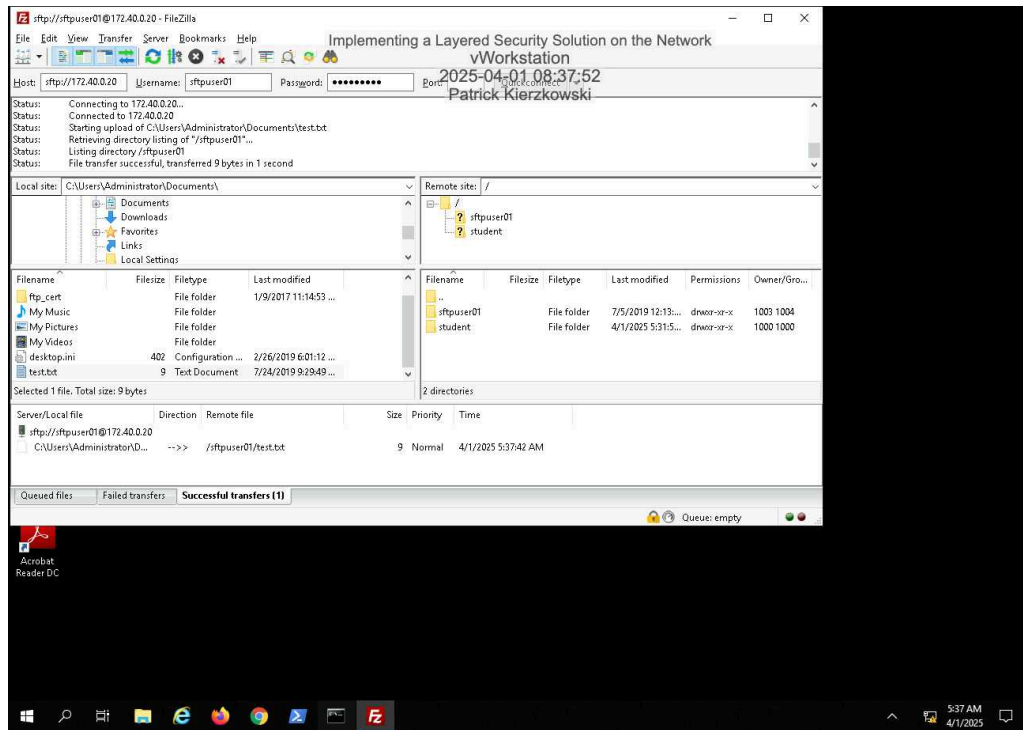
23. Make a screen capture showing the **timed-out ICMP** request to the **TargetLinux01** machine.



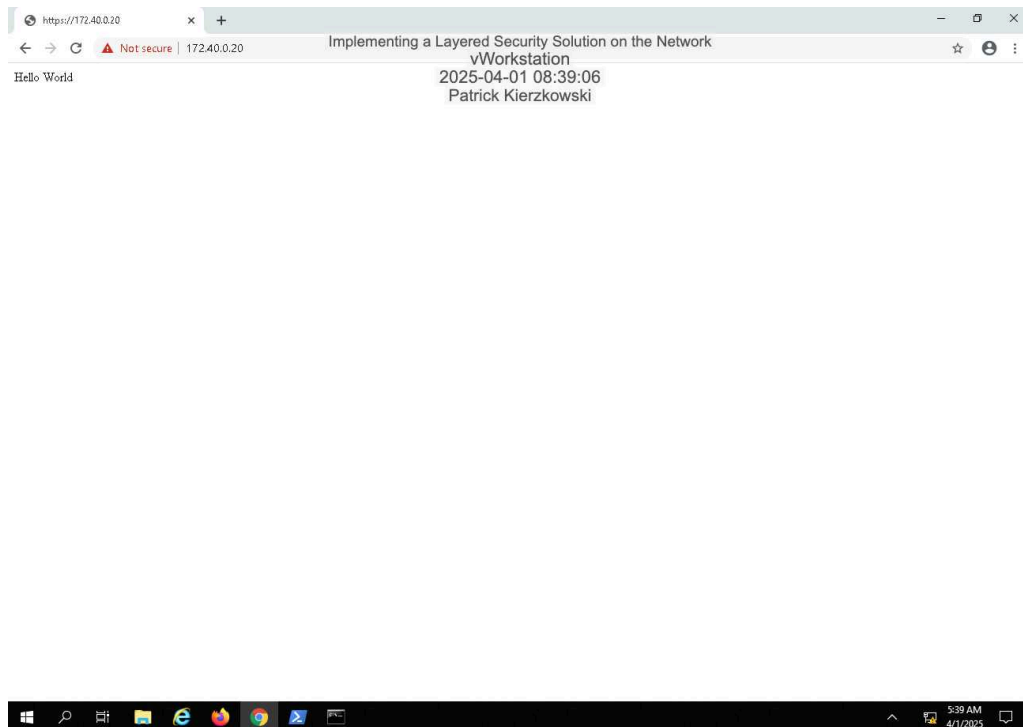
28. Make a screen capture showing the **connection timeout** to **172.40.0.20:21**.



32. Make a screen capture showing the **successfully transferred test.txt** file.

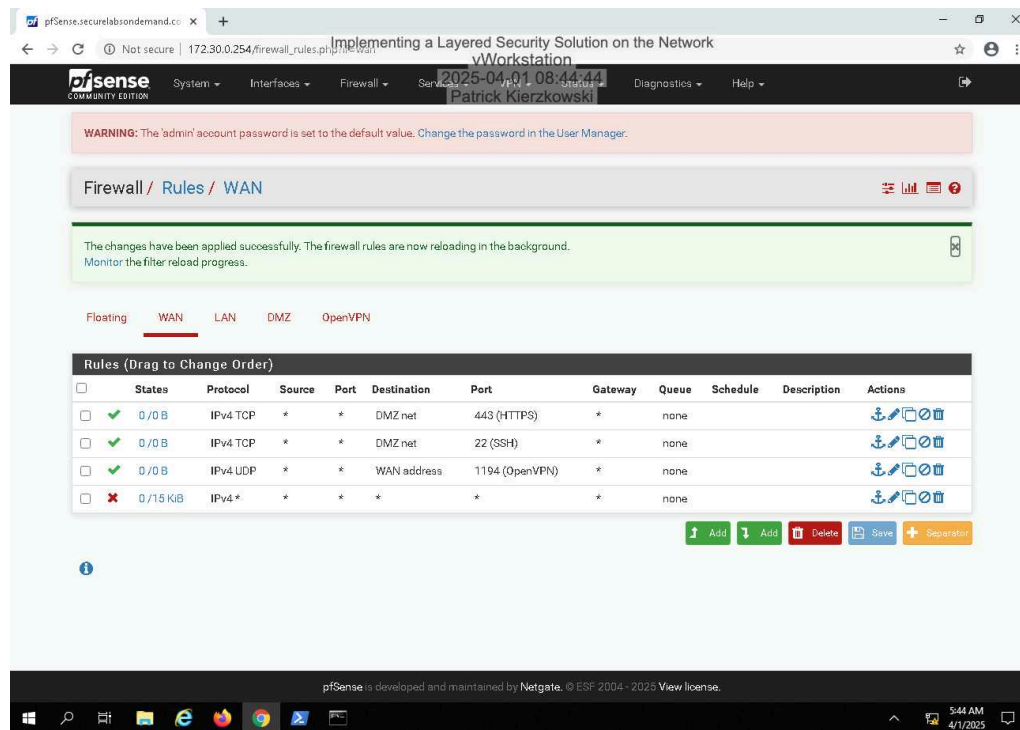


38. Make a screen capture showing the **successful HTTPS** connection from vWorkstation to the webpage on TargetLinux01.

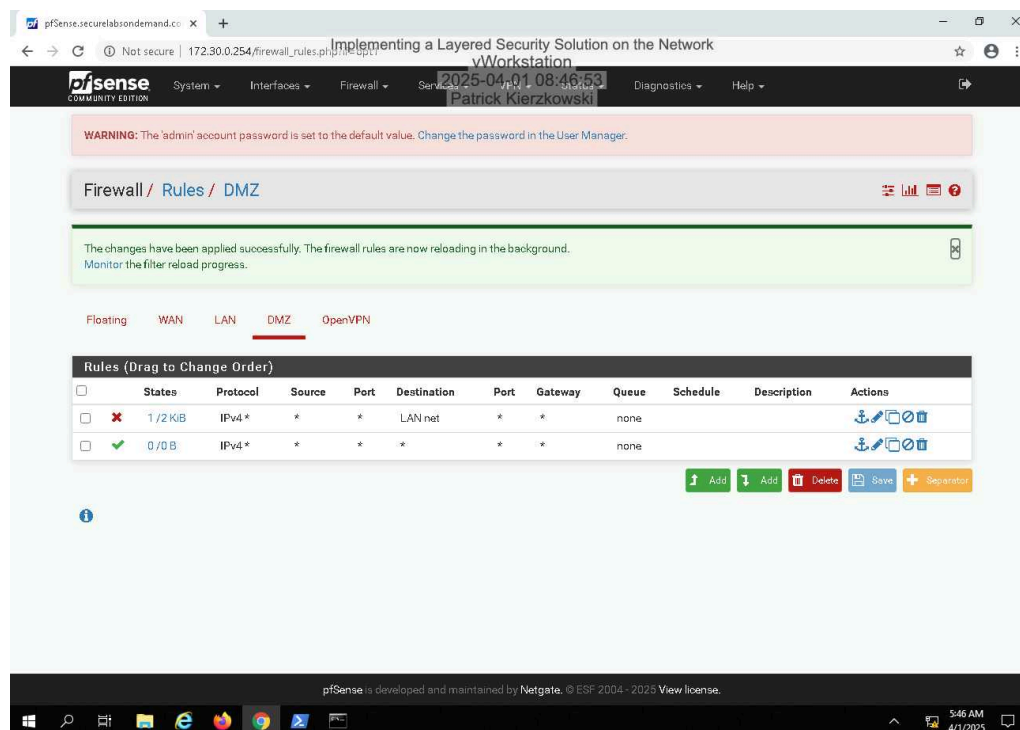


Part 2: Configure a Network Perimeter Firewall

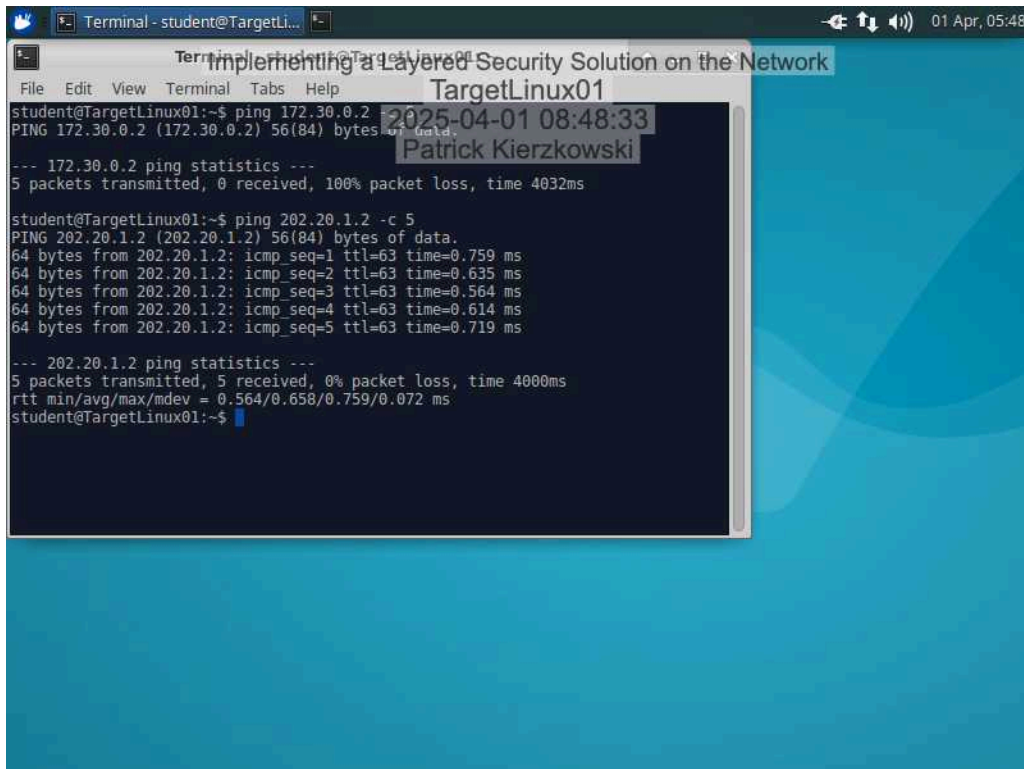
11. Make a screen capture showing the complete ruleset on the WAN interface.



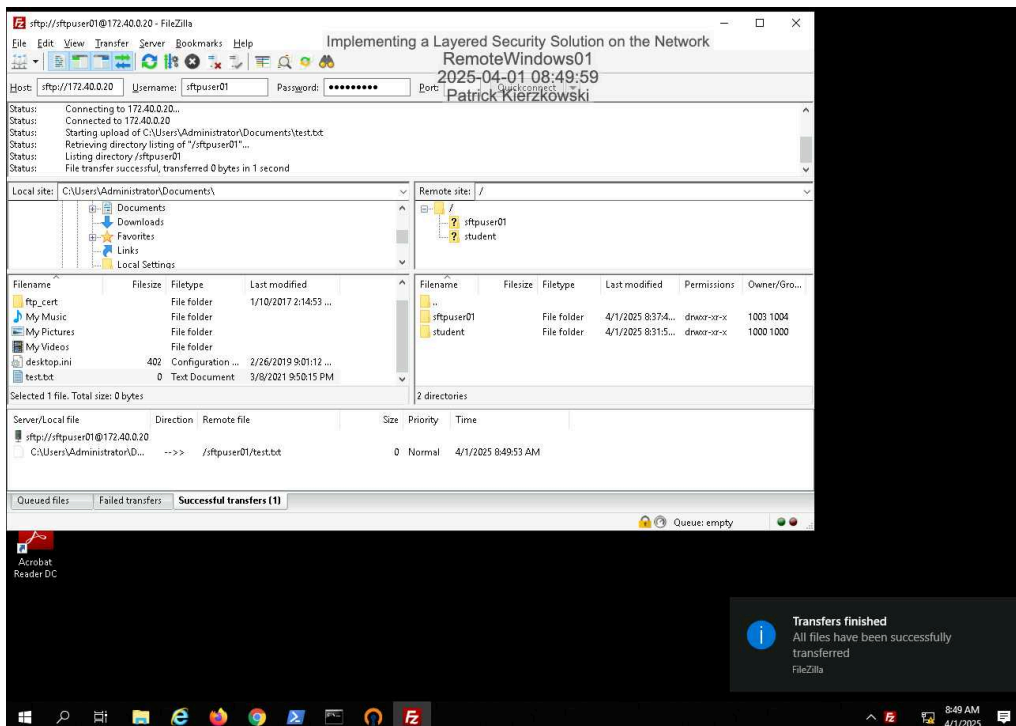
21. Make a screen capture showing the complete ruleset on the DMZ interface.



26. Make a screen capture showing the result of both ping operations.



34. Make a screen capture showing the successfully transferred test.txt file.

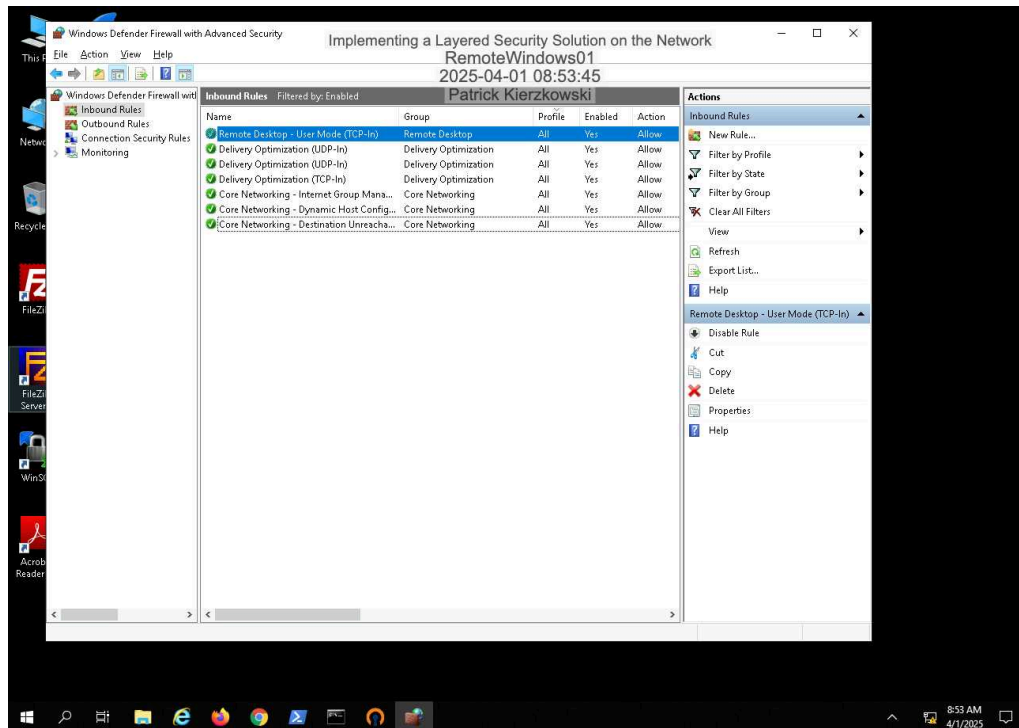


39. **Make a screen capture** showing the **successful HTTPS connection** from **RemoteWindows01** to the **webpage on TargetLinux01**.

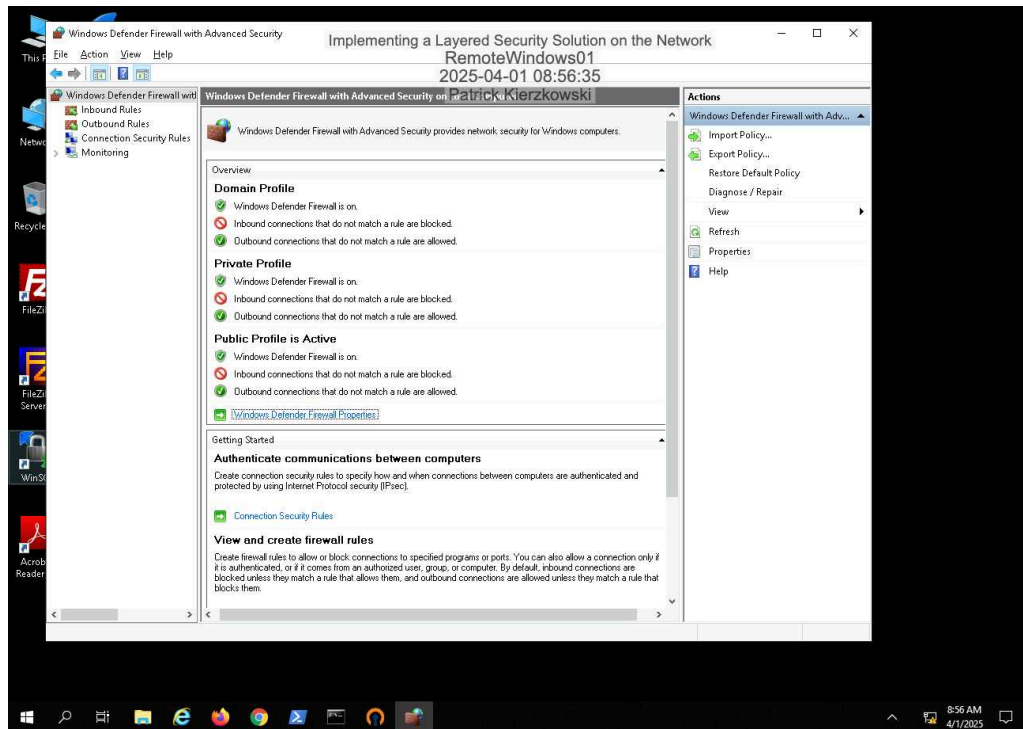
Section 2: Applied Learning

Part 1: Configure a Remote Access Solution on an Endpoint

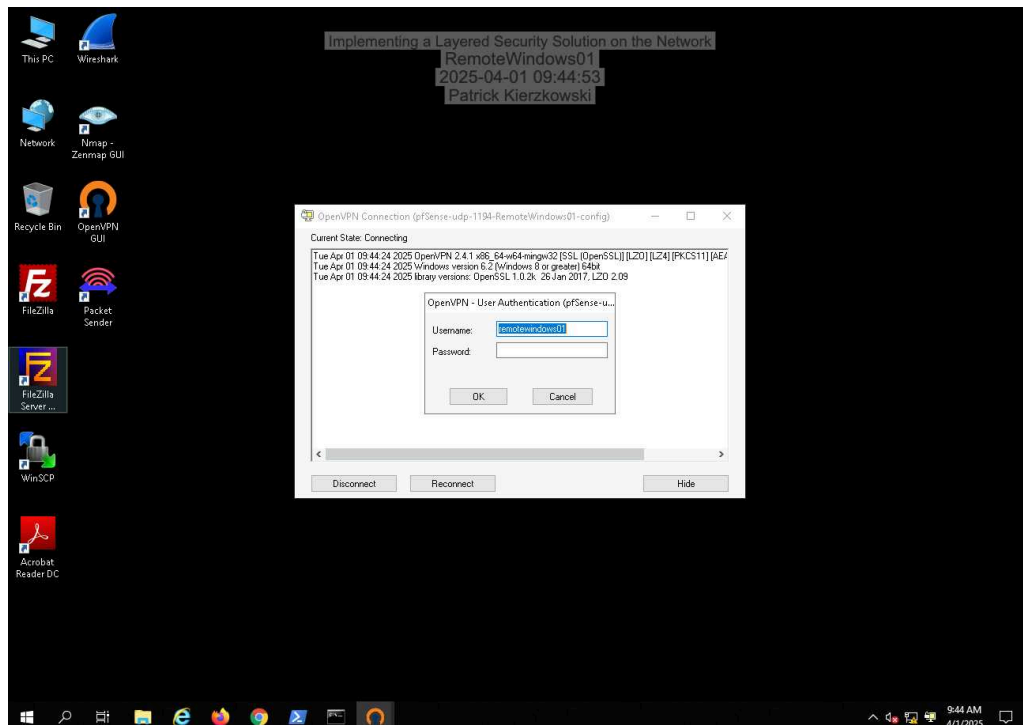
12. Make a screen capture showing the **current inbound ruleset for the RemoteWindows01 machine.**



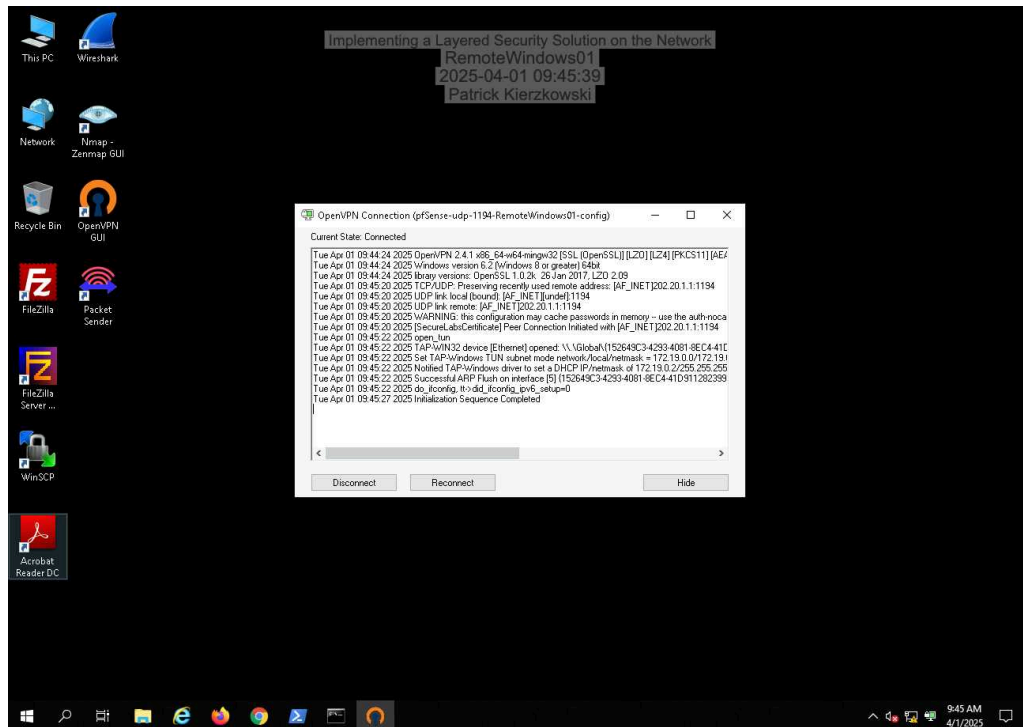
18. Make a screen capture showing the **firewall status** for all profiles as viewed in the main dashboard.



35. Make a screen capture showing the **save password** checkbox is no longer present.

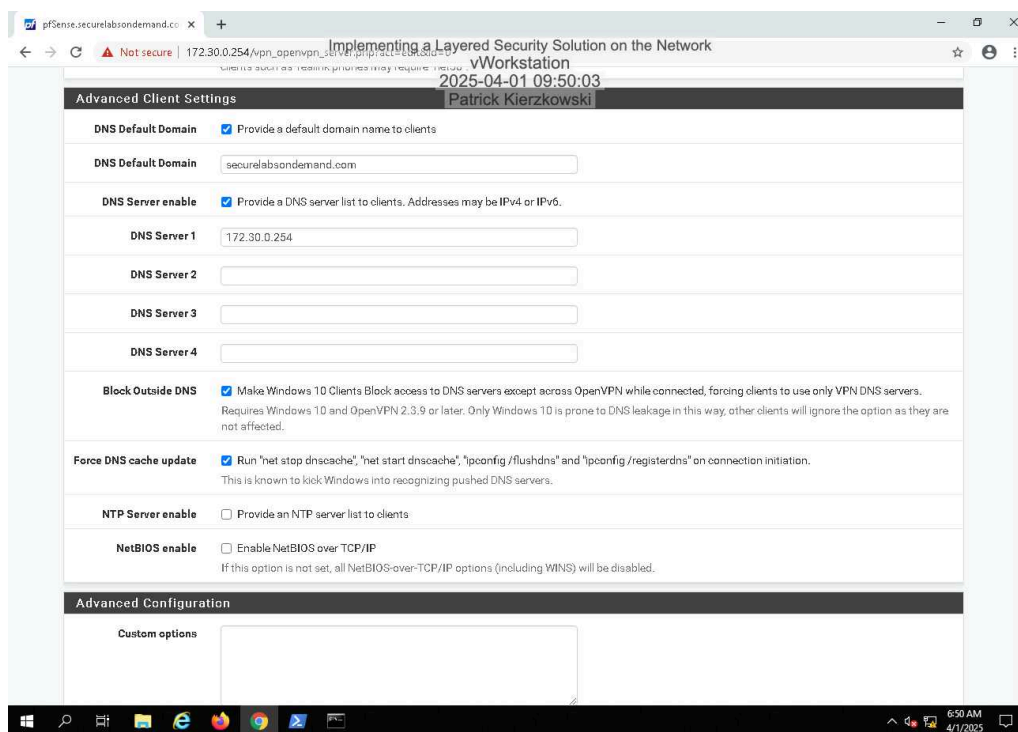


38. Make a screen capture showing the server validation warning is no longer present.

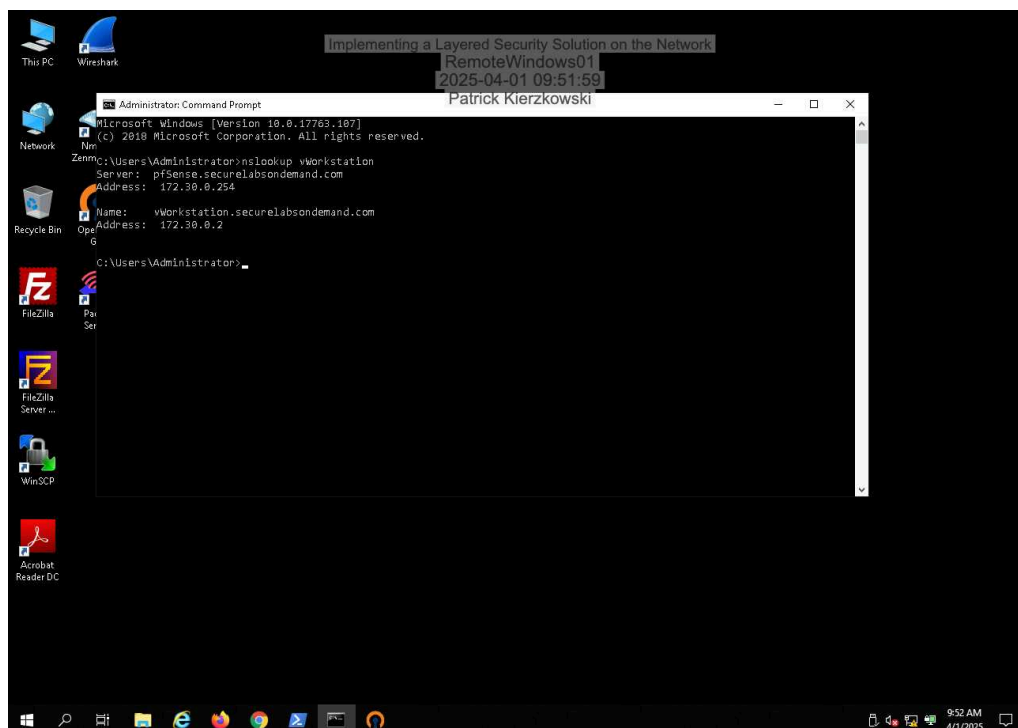


Part 2: Configure a Remote Access Solution on a Server

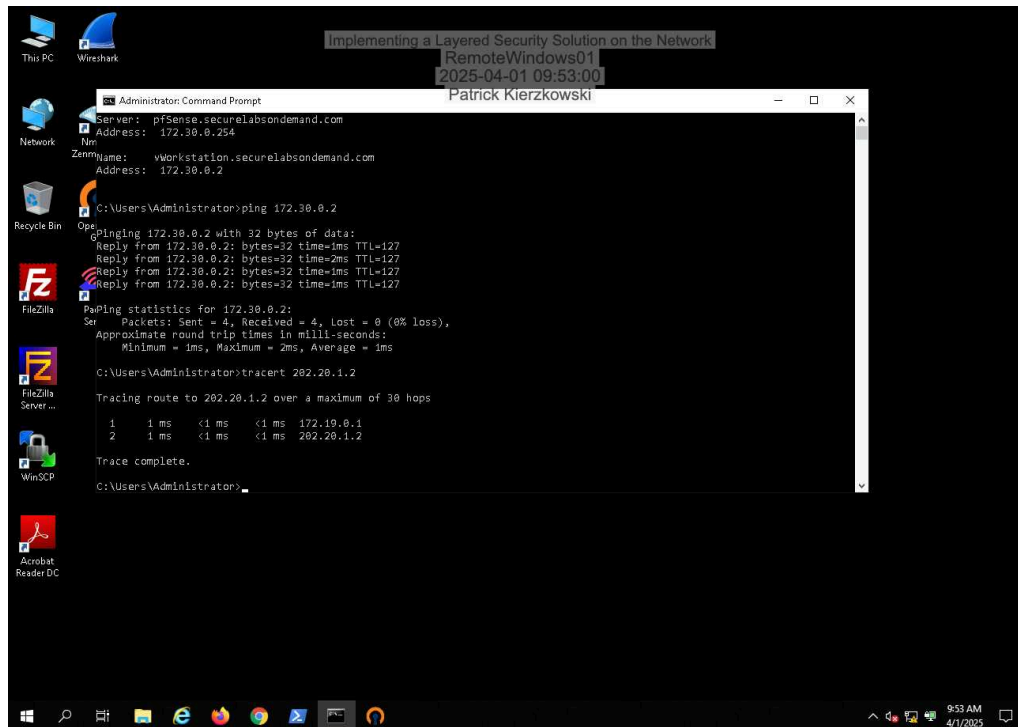
13. Make a screen capture showing the **DNS Server 1, Block Outside DNS and Force DNS Update** selections in the **Advanced Client Settings** section.



24. Make a screen capture showing the **output of your nslookup execution**.



27. Make a screen capture showing the results of your traceroute execution.



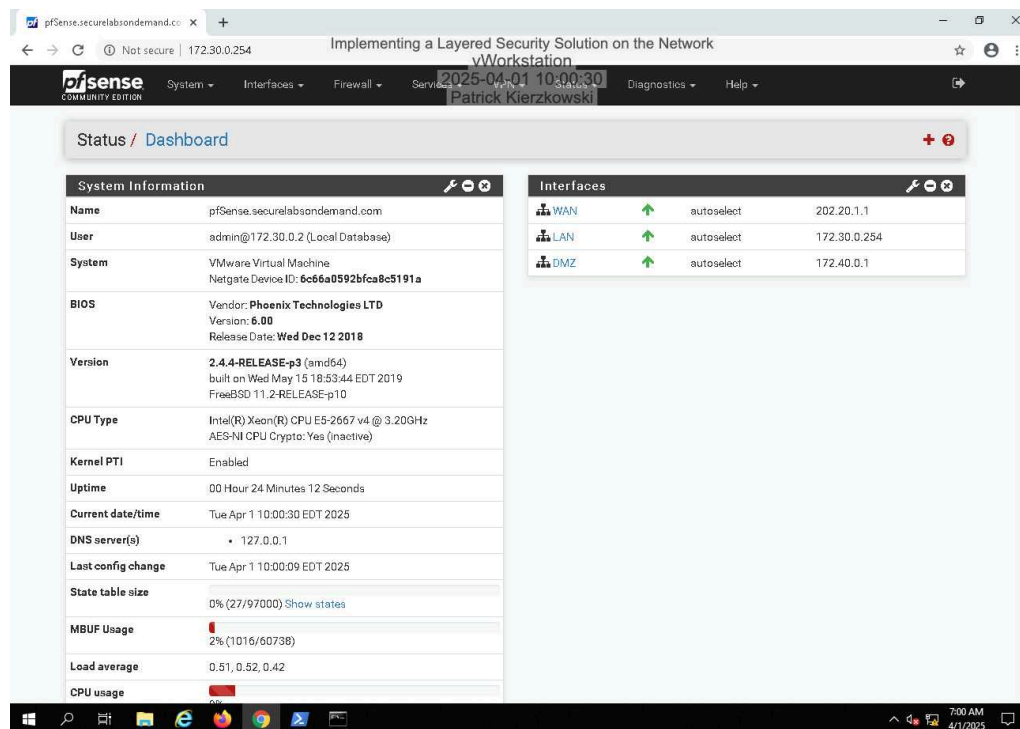
Section 3: Challenge and Analysis

Part 1: Improve User Account Security in pfSense

Document your new password for the admin account.

P@ssw0rd!

Make a screen capture showing the pfSense dashboard, after configuring your new password.



Part 2: Force Encrypted Access to the pfSense WebGUI

Make a screen capture showing the certificate warning displayed upon accessing the pfSense WebGUI.

