

Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

3 hours, 45 minutes

Progress:

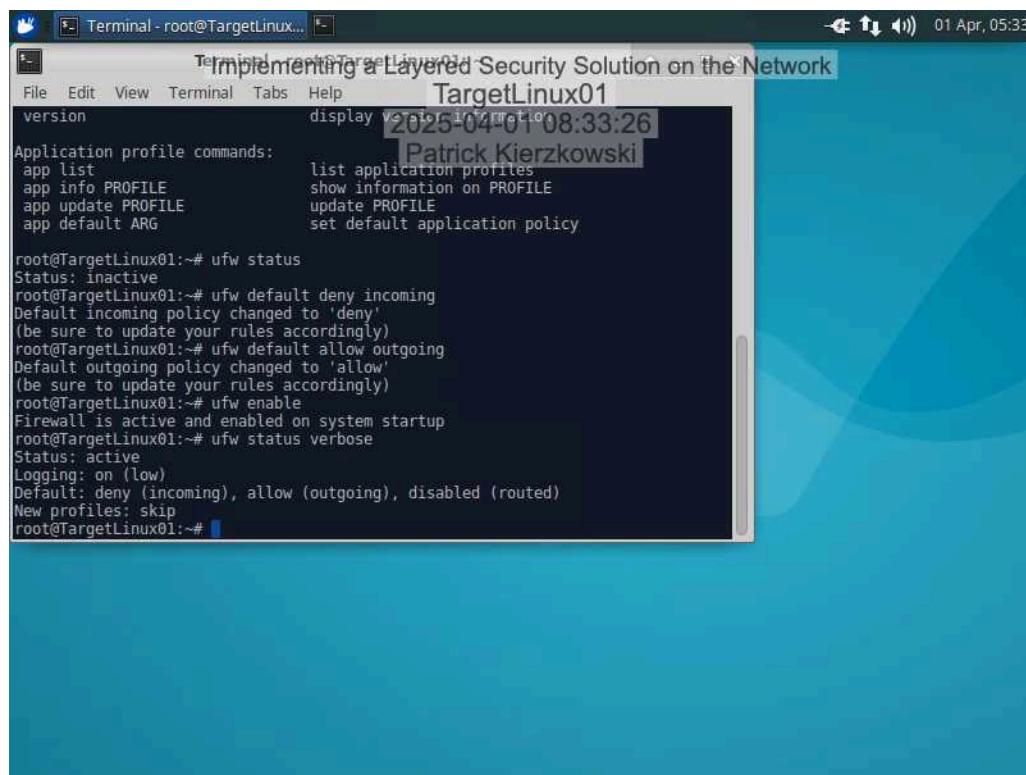
100%

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.



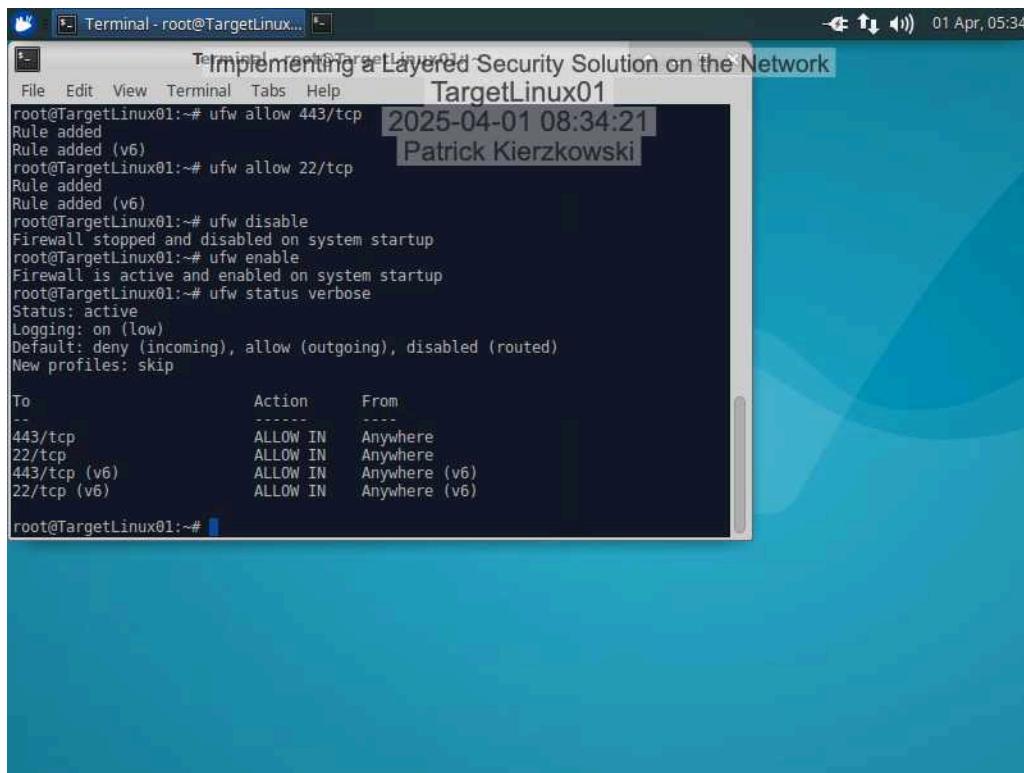
```
Terminal - root@TargetLinux...
File Edit View Terminal Tabs Help TargetLinux01
version display 2025-04-01 08:33:26
Application profile commands:
app list list application profiles
app info PROFILE show information on PROFILE
app update PROFILE update PROFILE
app default ARG set default application policy

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:~#
```

Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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



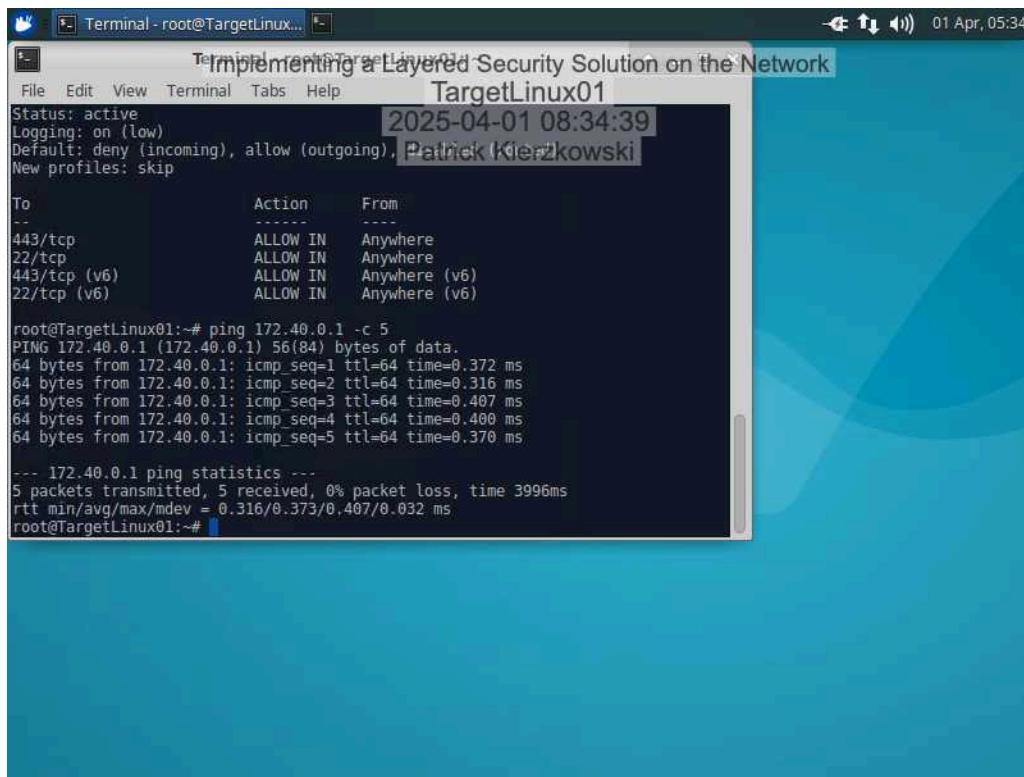
The screenshot shows a terminal window titled "Terminal - root@TargetLinux...". The window title bar also displays "Implementing a Layered Security Solution on the Network" and "TargetLinux01". The terminal shows the following command history:

```
root@TargetLinux01:~# ufw allow 443/tcp
Rule added
Rule added (v6)
root@TargetLinux01:~# ufw allow 22/tcp
Rule added
Rule added (v6)
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)

root@TargetLinux01:~#
```

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



The screenshot shows a terminal window titled "Terminal - root@TargetLinux...". The window title bar also displays "Implementing a Layered Security Solution on the Network" and "TargetLinux01". The terminal shows the following command history:

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), Patrick Kierzkowski
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)

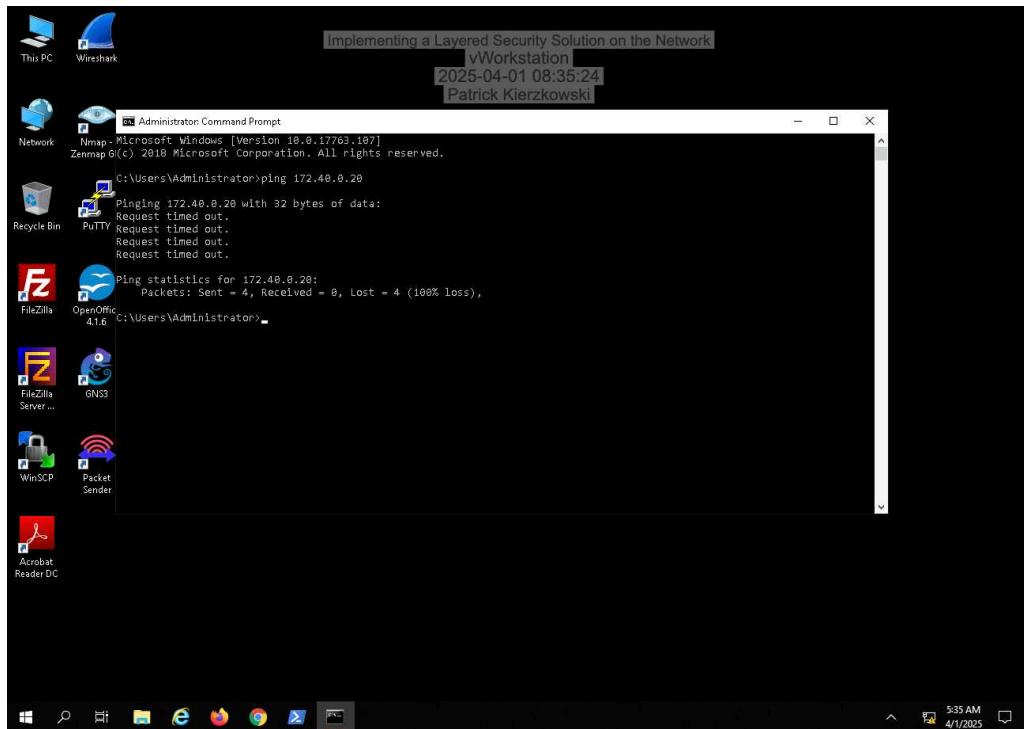
root@TargetLinux01:~# ping 172.40.0.1 -c 5
PING 172.40.0.1 (172.40.0.1) 56(84) bytes of data.
64 bytes from 172.40.0.1: icmp_seq=1 ttl=64 time=0.372 ms
64 bytes from 172.40.0.1: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 172.40.0.1: icmp_seq=3 ttl=64 time=0.407 ms
64 bytes from 172.40.0.1: icmp_seq=4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

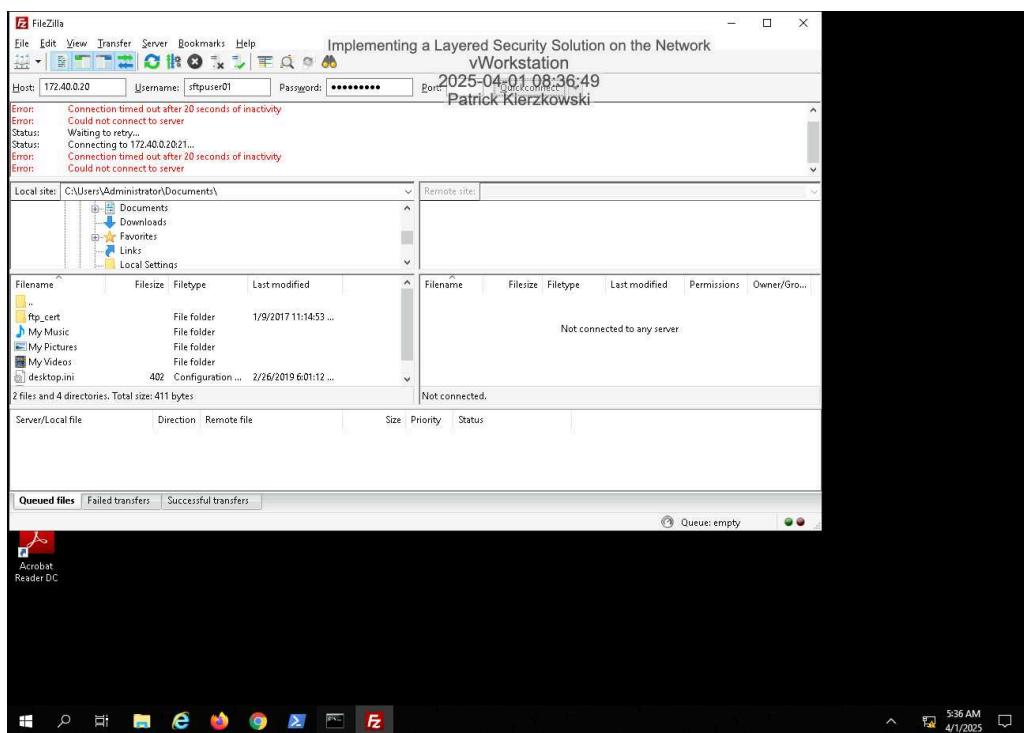
Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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



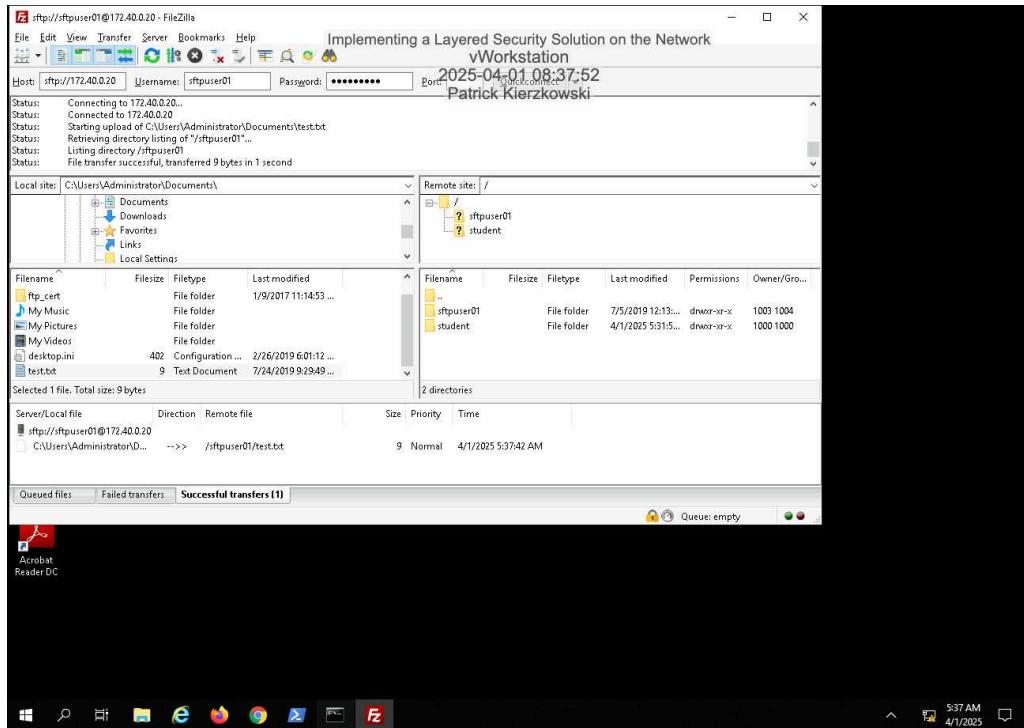
28. Make a screen capture showing the **connection timeout to 172.40.0.20:21**.



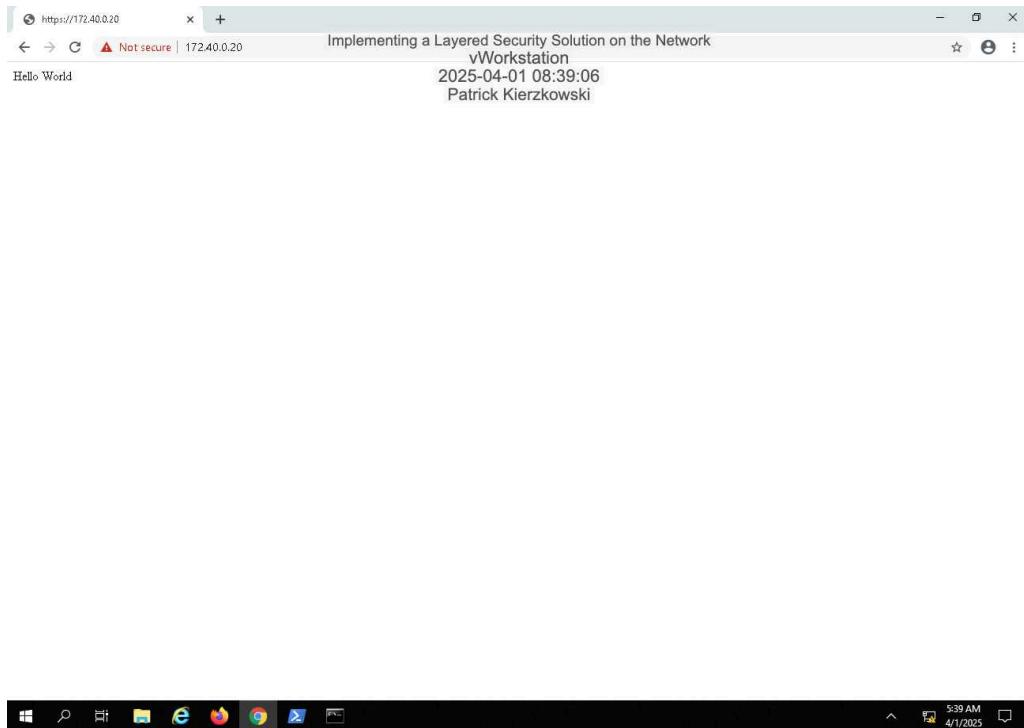
Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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.

The screenshot shows the pfSense Firewall Rules/WAN interface. The WAN tab is selected. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, a table lists the rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
0/0 B	IPv4 TCP	*	*	DMZ net	443 (HTTPS)	*	none						
0/0 B	IPv4 TCP	*	*	DMZ net	22 (SSH)	*	none						
0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none						
0/15 KiB	IPv4 *	*	*	*	*	*	none						

Buttons at the bottom include: Add, Add, Delete, Save, and Separator.

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

The screenshot shows the pfSense Firewall Rules/DMZ interface. The DMZ tab is selected. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, a table lists the rules:

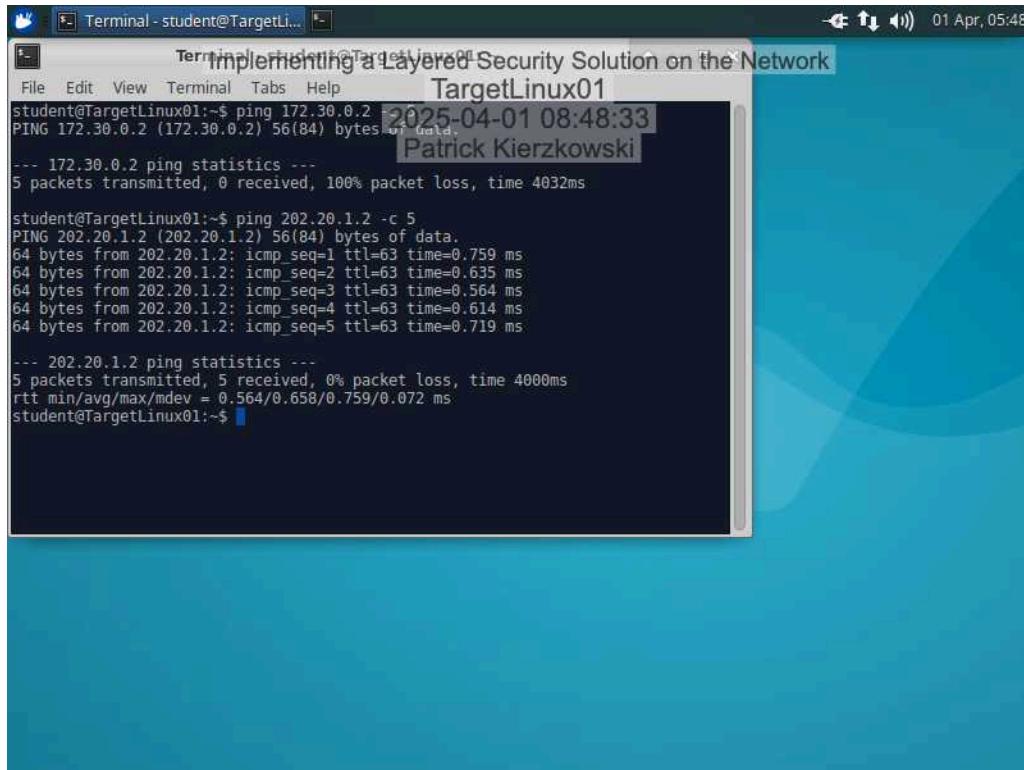
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
1/2 KiB	IPv4 *	*	*	LAN net	*	*	none						
0/0 B	IPv4 *	*	*	*	*	*	none						

Buttons at the bottom include: Add, Add, Delete, Save, and Separator.

Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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

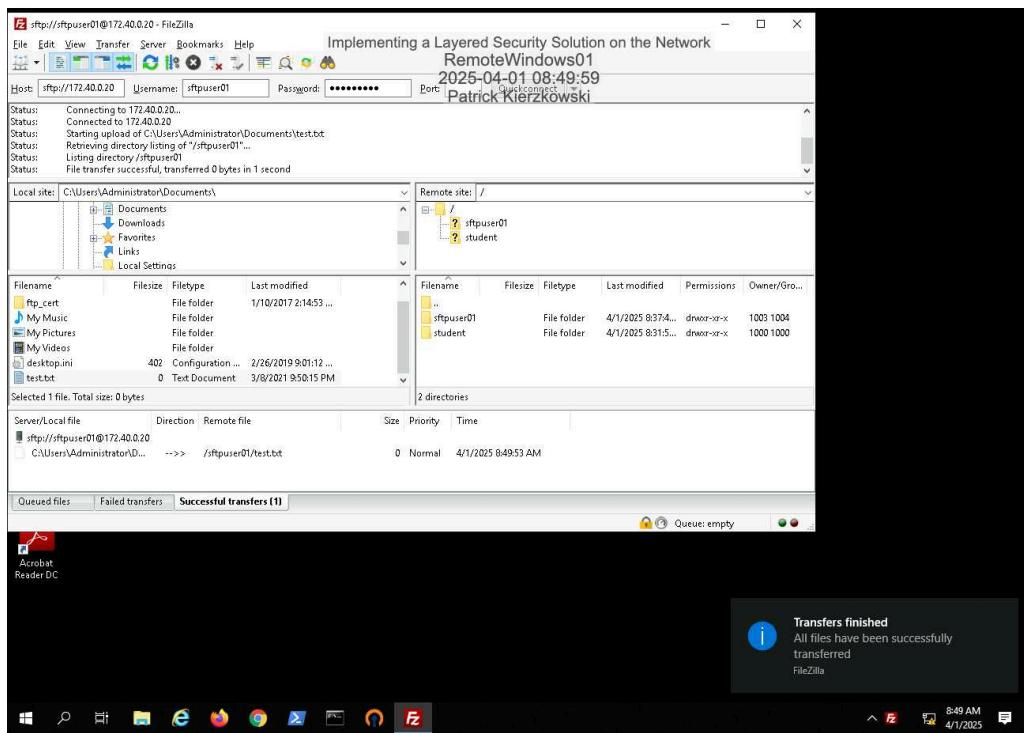


```
Terminal - student@TargetLinux01... 01 Apr, 05:48
Terminal - student@TargetLinux01... 01 Apr, 05:48
student@TargetLinux01:~$ ping 172.30.0.2 -c 5
PING 172.30.0.2 (172.30.0.2) 56(84) bytes of data.
--- 172.30.0.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4032ms

student@TargetLinux01:~$ ping 202.20.1.2 -c 5
PING 202.20.1.2 (202.20.1.2) 56(84) bytes of data.
64 bytes from 202.20.1.2: icmp_seq=1 ttl=63 time=0.759 ms
64 bytes from 202.20.1.2: icmp_seq=2 ttl=63 time=0.635 ms
64 bytes from 202.20.1.2: icmp_seq=3 ttl=63 time=0.564 ms
64 bytes from 202.20.1.2: icmp_seq=4 ttl=63 time=0.614 ms
64 bytes from 202.20.1.2: icmp_seq=5 ttl=63 time=0.719 ms

--- 202.20.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.564/0.658/0.759/0.072 ms
student@TargetLinux01:~$
```

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



Implementing a Layered Security Solution on the Network

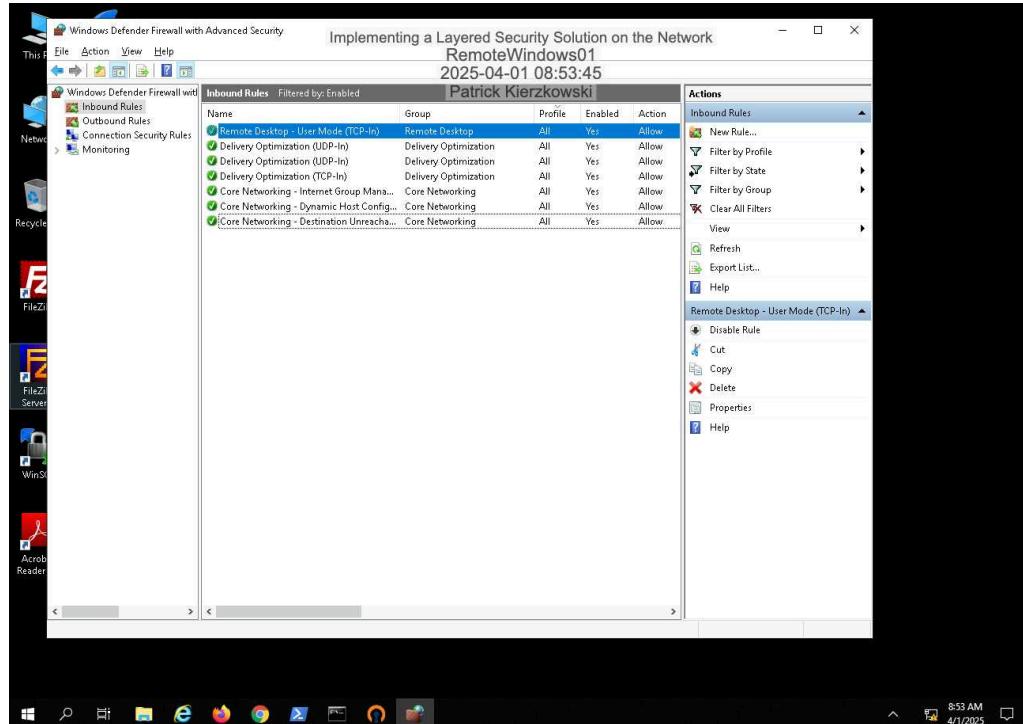
Fundamentals of Communications and Networking, Third Edition - Lab 09

- 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

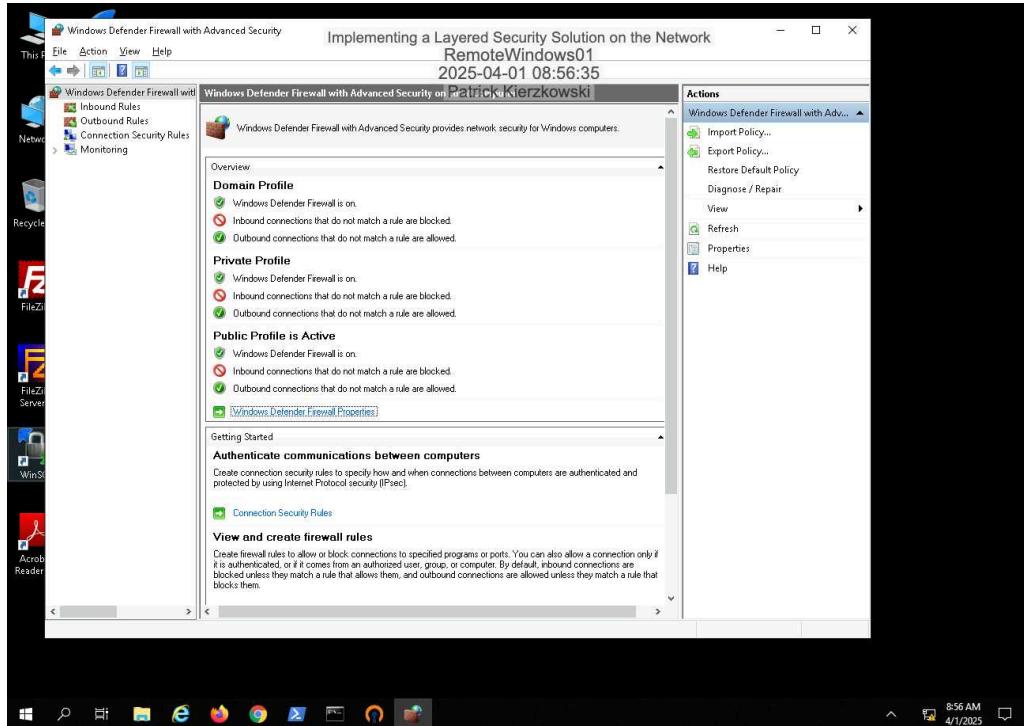
12. Make a screen capture showing the current inbound ruleset for the **RemoteWindows01** machine.



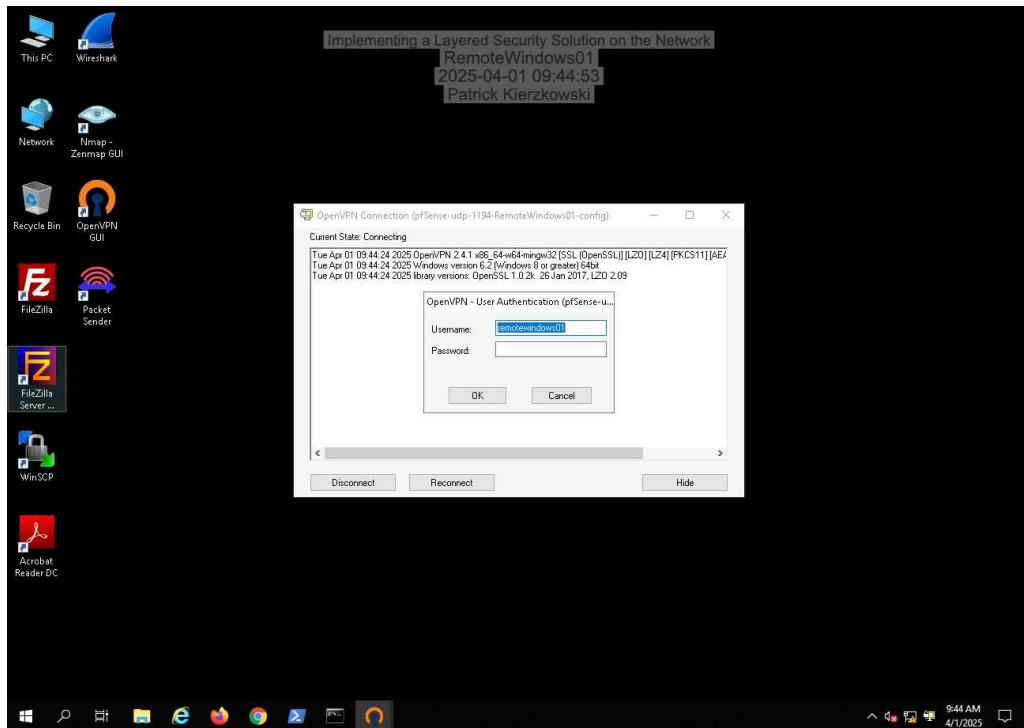
Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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



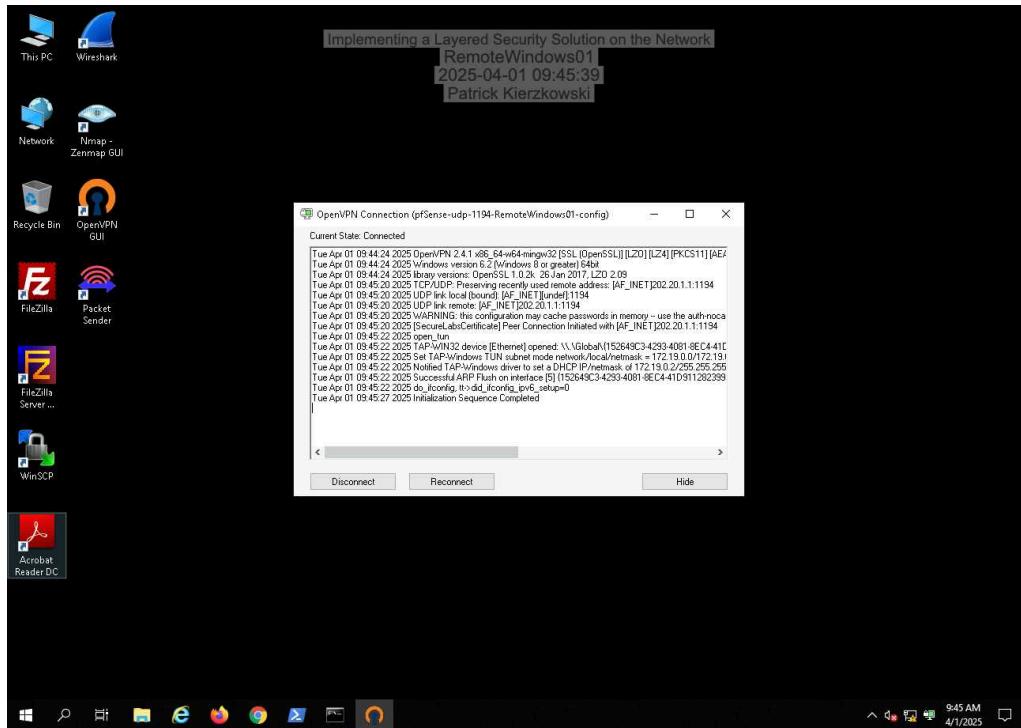
35. Make a screen capture showing the save password checkbox is no longer present.



Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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

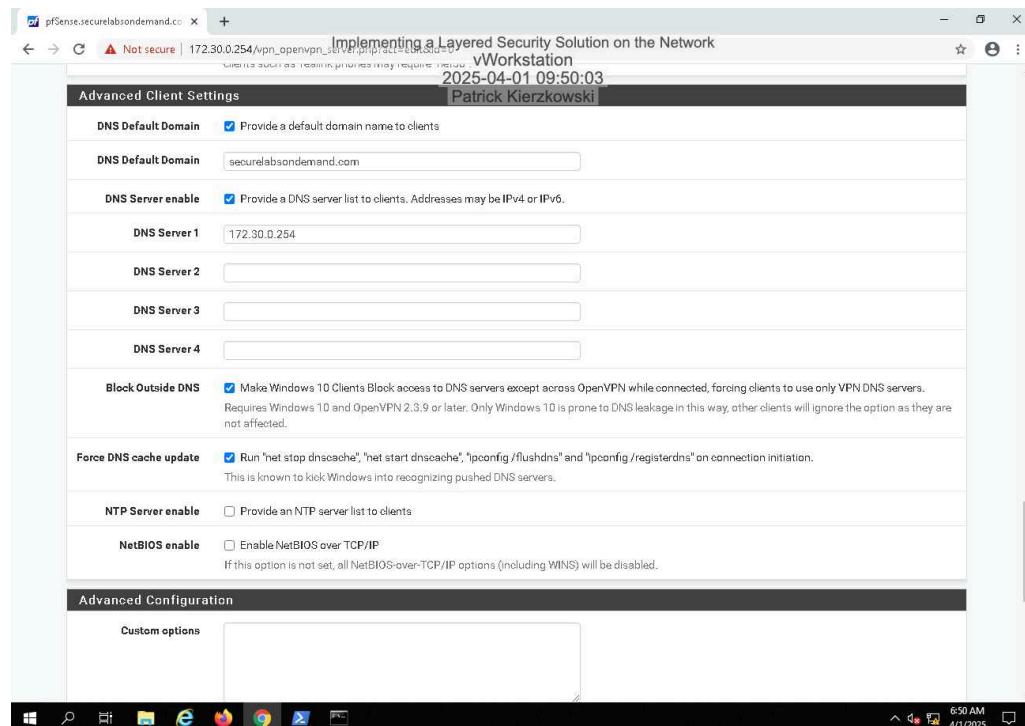


Part 2: Configure a Remote Access Solution on a Server

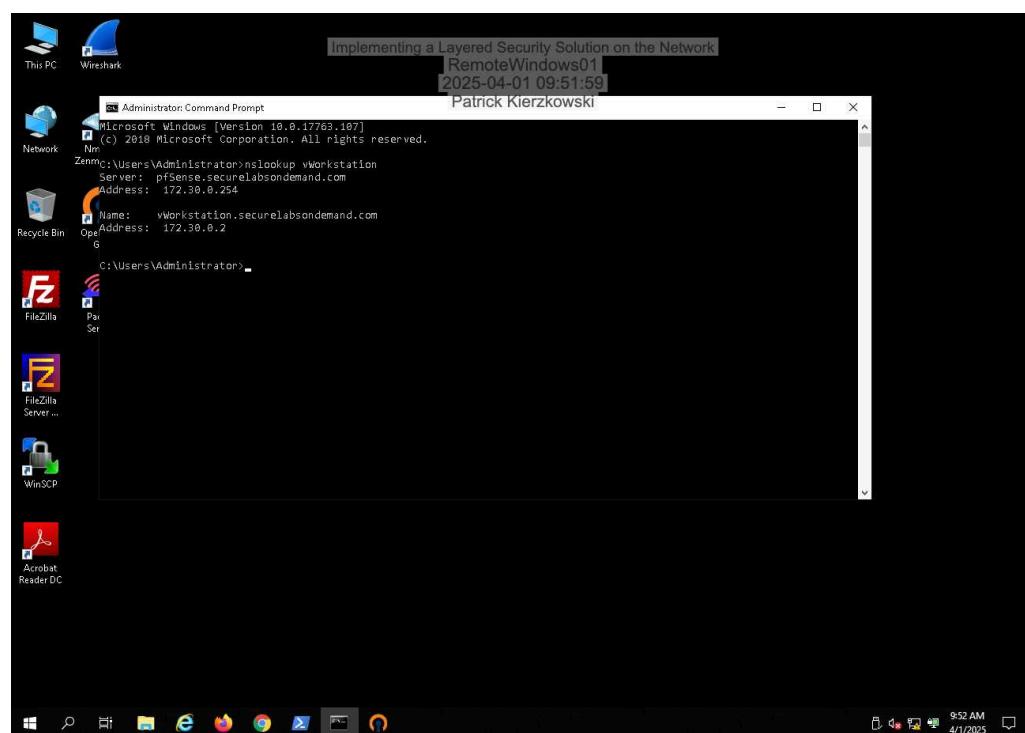
Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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



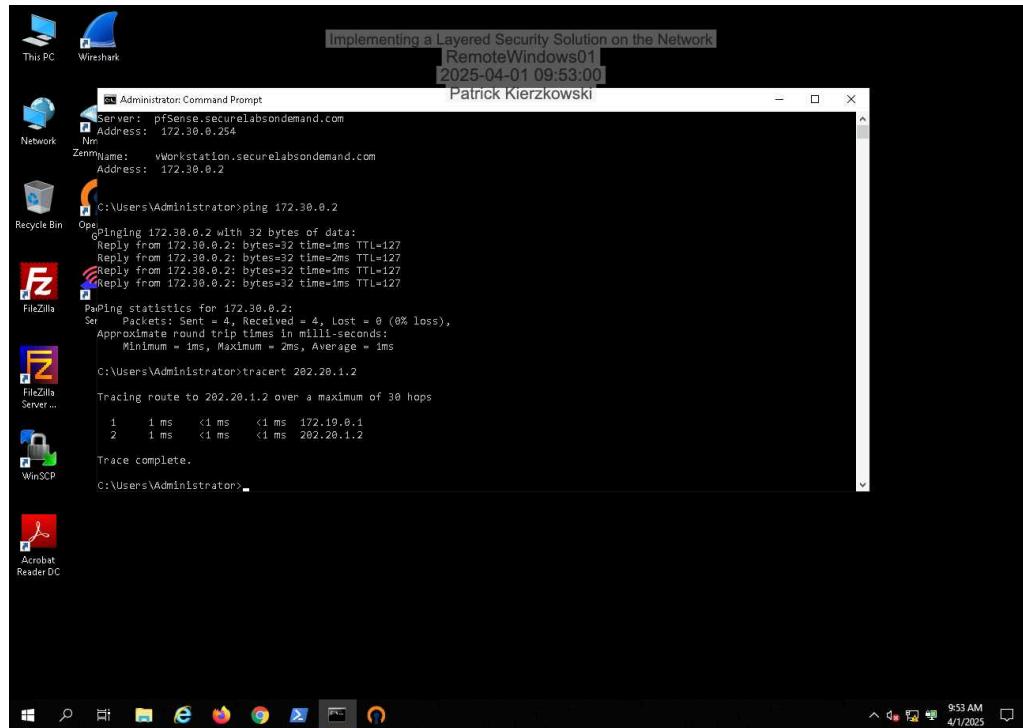
24. Make a screen capture showing the output of your nslookup execution.



Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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.

The screenshot shows the pfSense Status / Dashboard page. The top navigation bar includes links for System, Interfaces, Firewall, Services, Diagnostics, and Help. The main content area is divided into two sections: System Information and Interfaces.

System Information:

Name	Value
Name	pfSense.securelabsondemand.com
User	admin@172.30.0.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 6c66a0592bfcab5191a
BIOS	Vendor: Phoenix Technologies LTD Version: 8.00 Release Date: Wed Dec 12 2018
Version	2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10
CPU Type	Intel(R) Xeon(R) CPU E5-2667 v4 @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 24 Minutes 12 Seconds
Current date/time	Tue Apr 1 10:00:30 EDT 2025
DNS server(s)	• 127.0.0.1
Last config change	Tue Apr 1 10:00:09 EDT 2025
State table size	0% (27/97000) Show states
MBUF Usage	2% (1016/60738)
Load average	0.51, 0.52, 0.42
CPU usage	0%

Interfaces:

Interface	Status	IP Address
WAN	autoselect	202.20.1.1
LAN	autoselect	172.30.0.254
DMZ	autoselect	172.40.0.1

Part 2: Force Encrypted Access to the pfSense WebGUI

Implementing a Layered Security Solution on the Network

Fundamentals of Communications and Networking, Third Edition - Lab 09

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

