Student:	Email:
Enrique Mejia	enriquem2260@gmail.com

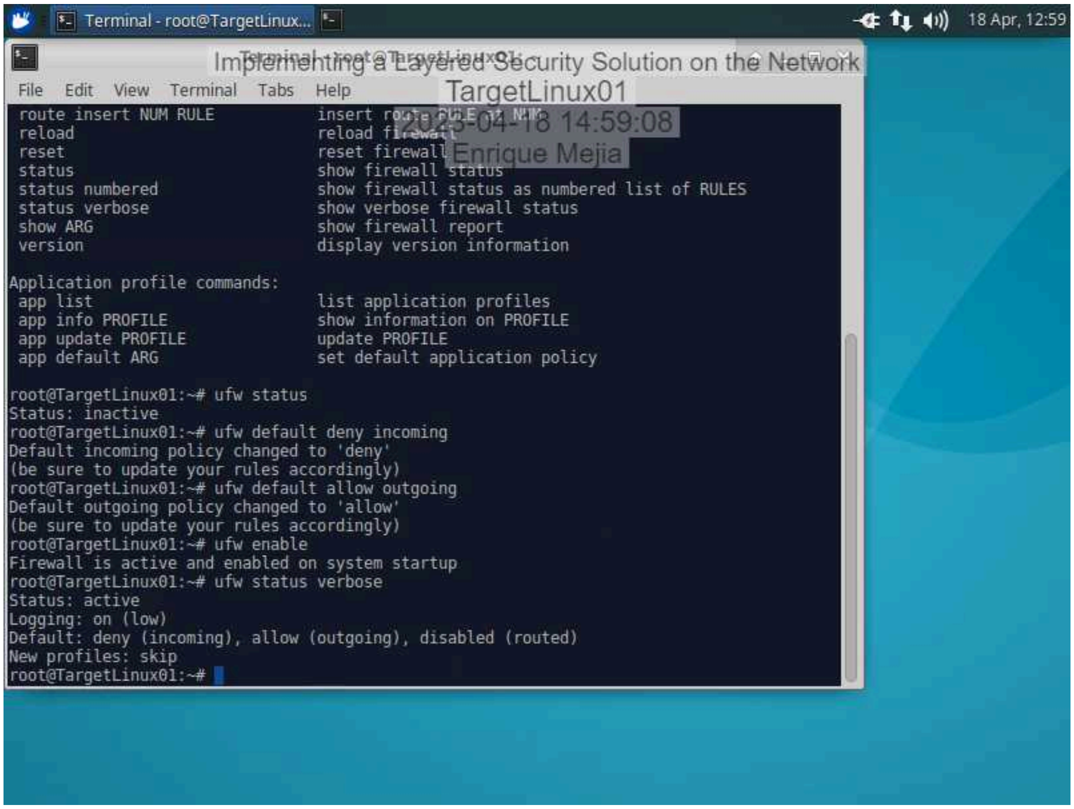
Time on Task:	Progress:
1 hour, 12 minutes	100%

Report Generated: Tuesday, April 18, 2023 at 5:01 PM

Section 1: Hands-On Demonstration

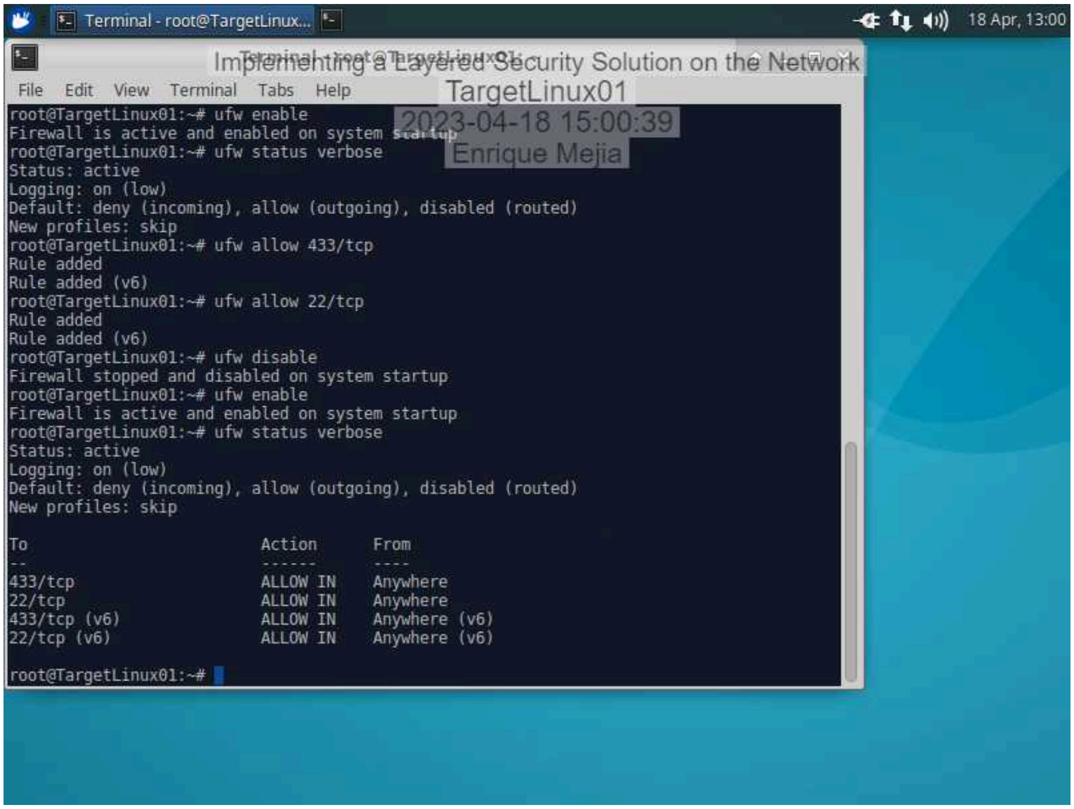
Part 1: Configure an Endpoint Firewall

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


Terminal - root@TargetLinux...
18 Apr, 12:59
Terminal - root@TargetLinux01:~
File
Edit
View
Terminal
Tabs
Help
Implementing a Layered Security Solution on the Network
TargetLinux01
2023-04-18 14:59:08
Enrique Mejia

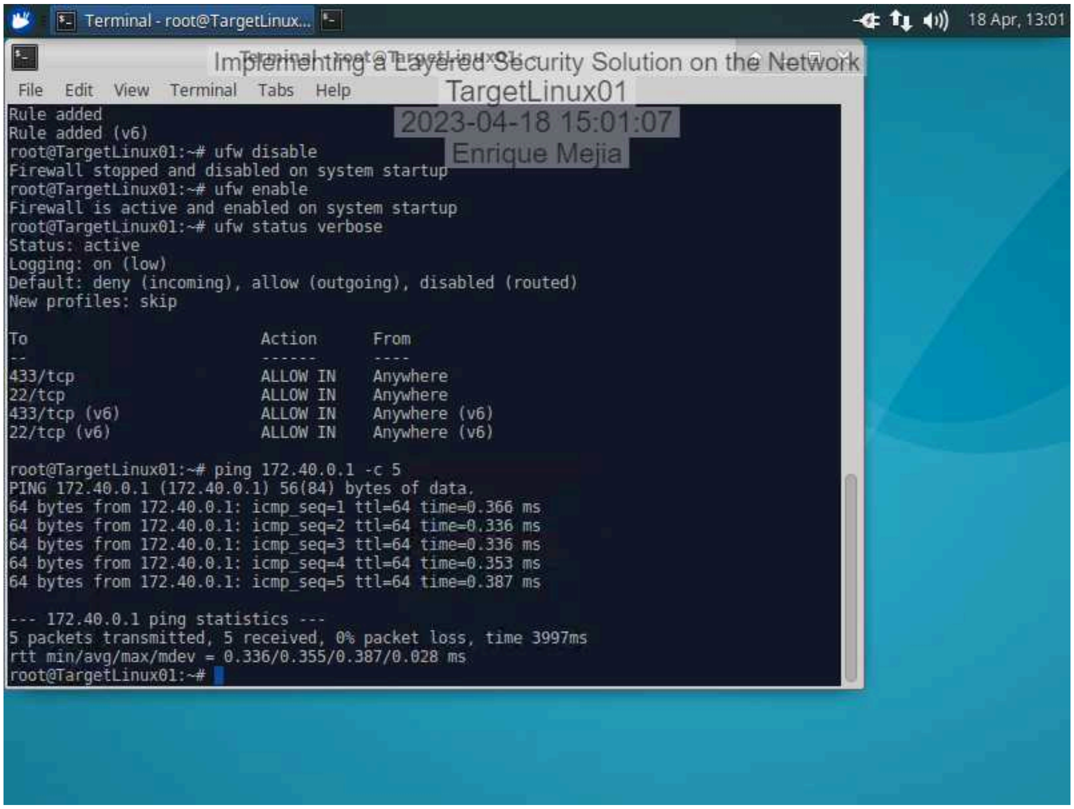
```
 route insert NUM RULE          insert route RULE at NUM
 reload                         reload firewall
 reset                          reset firewall
 status                         show firewall status
 status numbered                show firewall status as numbered list of RULES
 status verbose                 show verbose firewall status
 show ARG                       show firewall report
 version                        display version information

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:~#
```

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


Terminal - root@TargetLinux...
18 Apr, 13:00
Terminal - root@TargetLinux01: ~
File Edit View Terminal Tabs Help
Implementing a Layered Security Solution on the Network
TargetLinux01
2023-04-18 15:00:39
Enrique Mejia

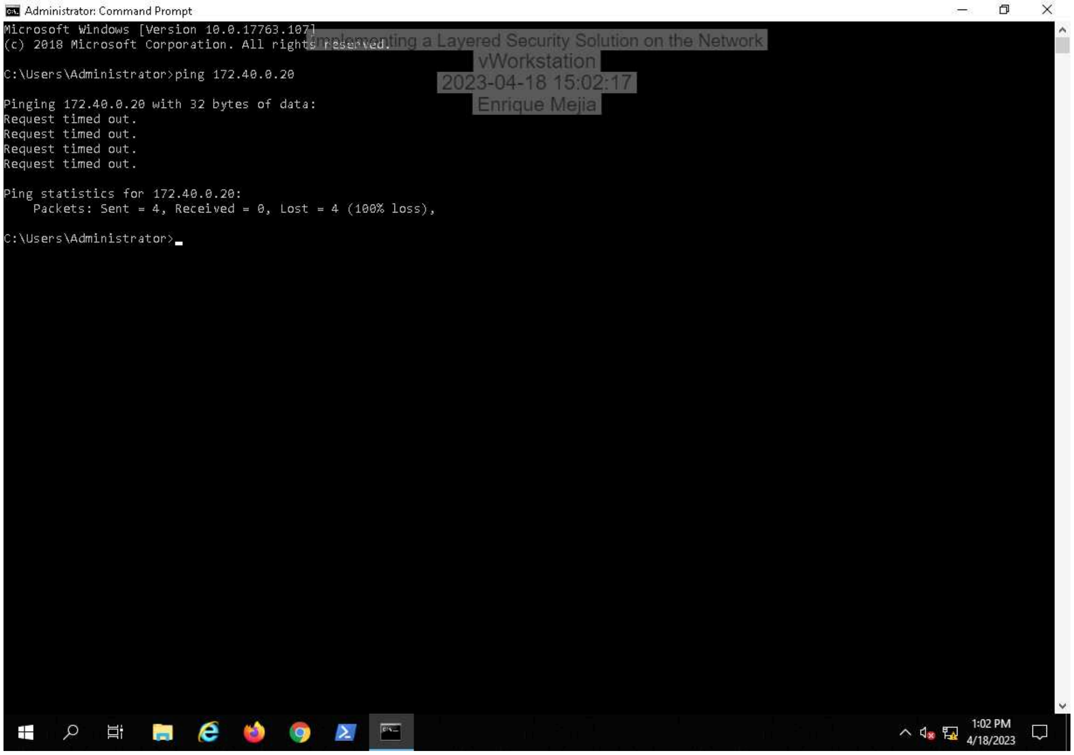
```
root@TargetLinux01:~# ufw enable
Firewall is active and enabled on system startup
root@TargetLinux01:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
root@TargetLinux01:~# ufw allow 433/tcp
Rule added
Rule added (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
--                         ------      ----
433/tcp                    ALLOW IN    Anywhere
22/tcp                     ALLOW IN    Anywhere
433/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**.


Terminal - root@TargetLinux...
18 Apr, 13:01
Terminal - root@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help
Implementing a Layered Security Solution on the Network
TargetLinux01
2023-04-18 15:01:07
Enrique Mejia

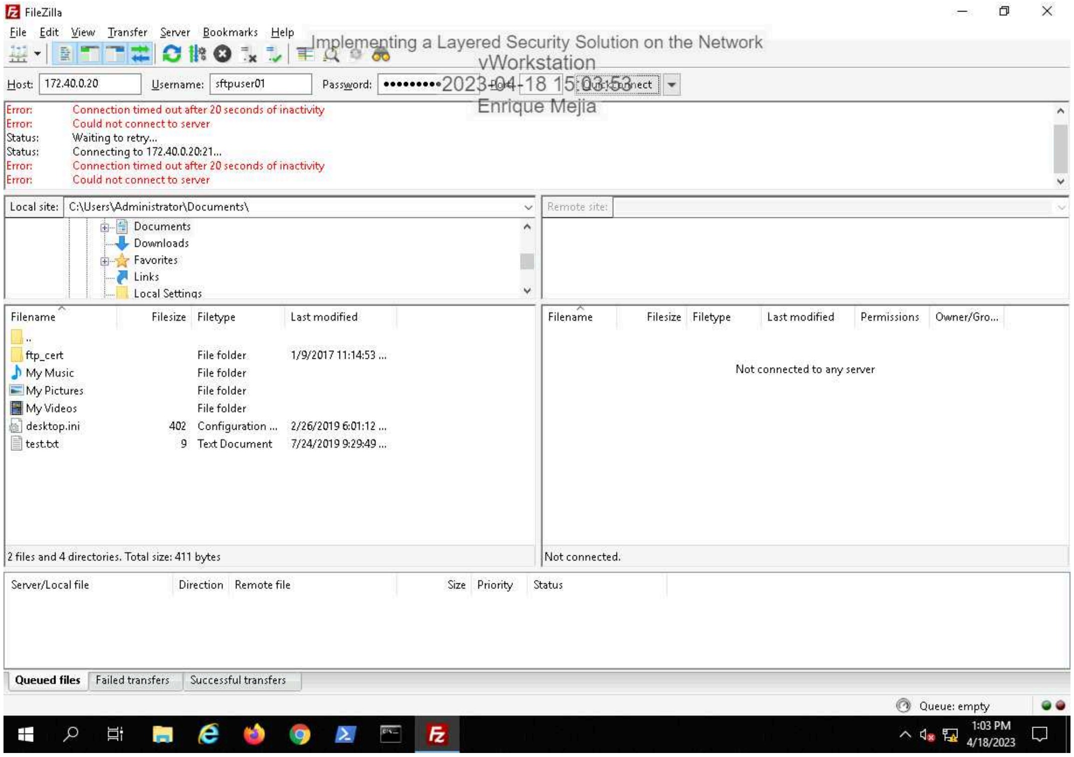
```
Rule added
Rule added (v6)
root@TargetLinux01:~# ufw disable
Firewall stopped and disabled on system startup
root@TargetLinux01:~# ufw enable
Firewall is active and enabled on system startup
root@TargetLinux01:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
433/tcp                    ALLOW IN    Anywhere
22/tcp                     ALLOW IN    Anywhere
433/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=0.366 ms
64 bytes from 172.40.0.1: icmp_seq=2 ttl=64 time=0.336 ms
64 bytes from 172.40.0.1: icmp_seq=3 ttl=64 time=0.336 ms
64 bytes from 172.40.0.1: icmp_seq=4 ttl=64 time=0.353 ms
64 bytes from 172.40.0.1: icmp_seq=5 ttl=64 time=0.387 ms

--- 172.40.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.336/0.355/0.387/0.028 ms
root@TargetLinux01:~#
```

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


Administrator: Command Prompt
Implementing a Layered Security Solution on the Network
vWorkstation
2023-04-18 15:02:17
Enrique Mejia
1:02 PM
4/18/2023

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.40.0.20

Pinging 172.40.0.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.40.0.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>_
```

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



Host: 172.40.0.20 Username: sftpuser01 Password: ••••••••••

```
Error:    Connection timed out after 20 seconds of inactivity
Error:    Could not connect to server
Status:   Waiting to retry...
Status:   Connecting to 172.40.0.20:21...
Error:    Connection timed out after 20 seconds of inactivity
Error:    Could not connect to server
```

Local site: C:\Users\Administrator\Documents\

Remote site:

Filename	Filesize	Filetype	Last modified
..			
ftp_cert		File folder	1/9/2017 11:14:53 ...
My Music		File folder	
My Pictures		File folder	
My Videos		File folder	
desktop.ini	402	Configuration ...	2/26/2019 6:01:12 ...
test.txt	9	Text Document	7/24/2019 9:29:49 ...

2 files and 4 directories. Total size: 411 bytes

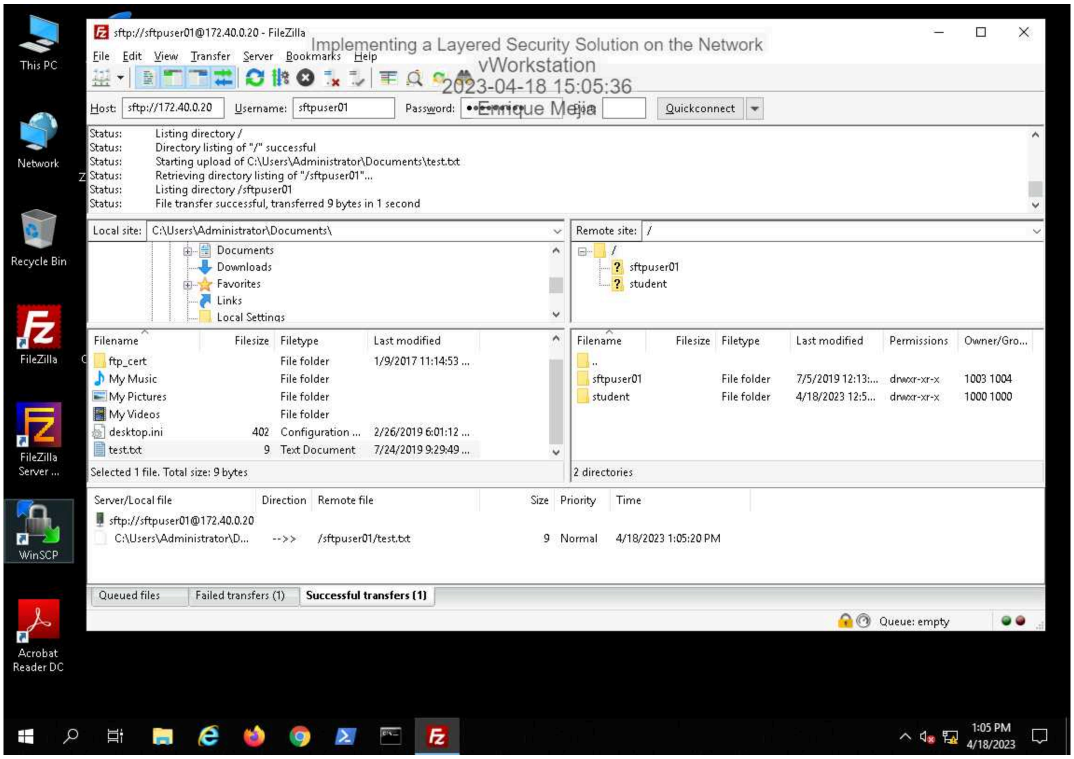
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...

Not connected to any server

Not connected.

Server/Local file	Direction	Remote file	Size	Priority	Status

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



Host: sftp://172.40.0.20 Username: sftpuser01 Password: ••••••••• Port:

```
Status:     Listing directory /
Status:     Directory listing of "/" successful
Status:     Starting upload of C:\Users\Administrator\Documents\test.txt
Status:     Retrieving directory listing of "/sftpuser01"...
Status:     Listing directory /sftpuser01
Status:     File transfer successful, transferred 9 bytes in 1 second
```

Local site: C:\Users\Administrator\Documents\

```
Documents
Downloads
Favorites
Links
Local Settings
```

Remote site: /

```
/
  sftpuser01
  student
```

Filename	Filesize	Filetype	Last modified
ftp_cert		File folder	1/9/2017 11:14:53 ...
My Music		File folder	
My Pictures		File folder	
My Videos		File folder	
desktop.ini	402	Configuration ...	2/26/2019 6:01:12 ...
test.txt	9	Text Document	7/24/2019 9:29:49 ...

Selected 1 file. Total size: 9 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
sftpuser01		File folder	7/5/2019 12:13:...	drwxr-xr-x	1003 1004
student		File folder	4/18/2023 12:5...	drwxr-xr-x	1000 1000

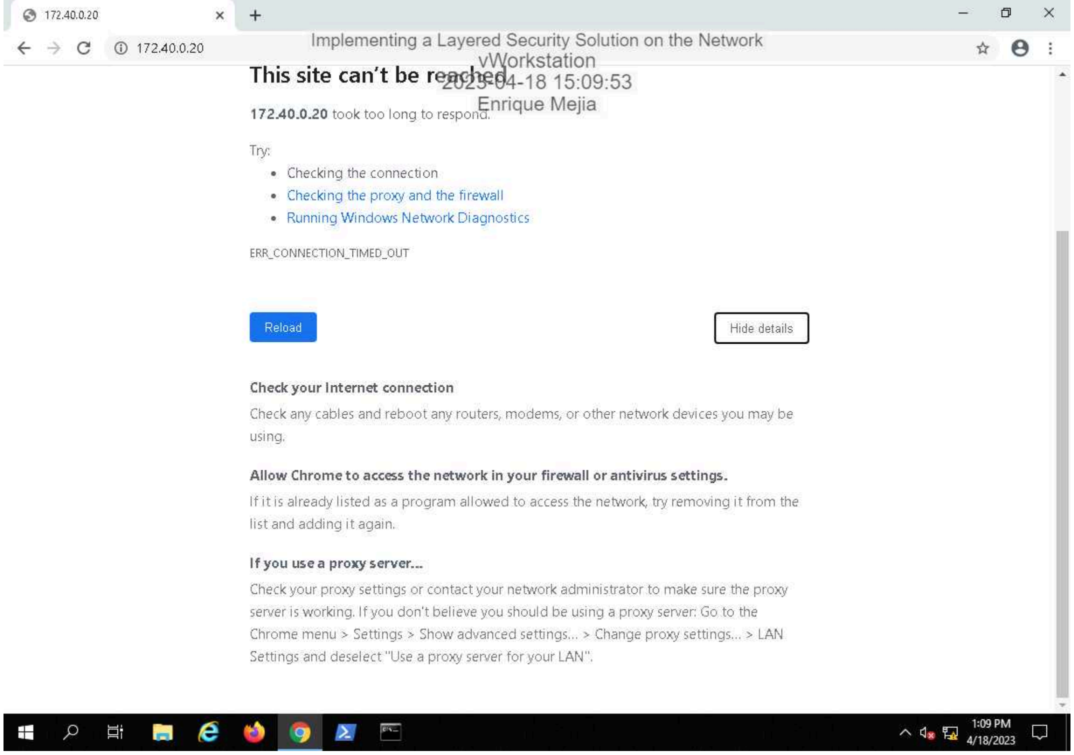
2 directories

Server/Local file	Direction	Remote file	Size	Priority	Time
sftp://sftpuser01@172.40.0.20					
C:\Users\Administrator\D...	-->>	/sftpuser01/test.txt	9	Normal	4/18/2023 1:05:20 PM

Queued files | Failed transfers (1) | **Successful transfers (1)**

Queue: empty

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



This site can’t be reached

172.40.0.20 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Check your Internet connection

Check any cables and reboot any routers, modems, or other network devices you may be using.

Allow Chrome to access the network in your firewall or antivirus settings.

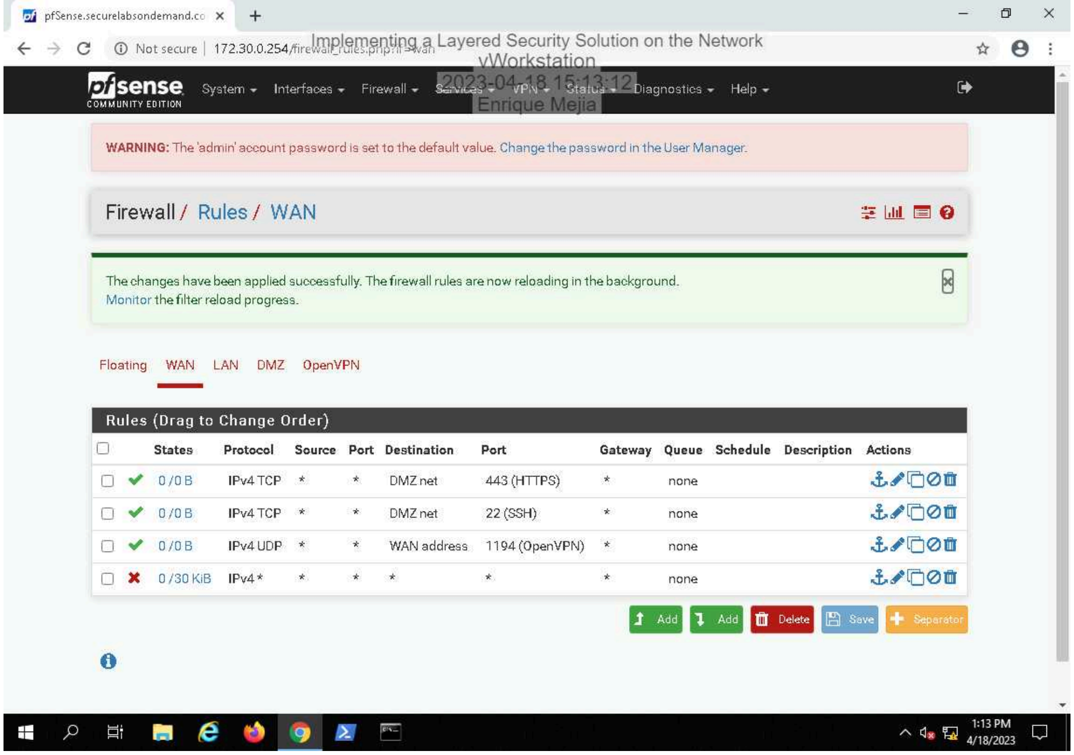
If it is already listed as a program allowed to access the network, try removing it from the list and adding it again.

If you use a proxy server...

Check your proxy settings or contact your network administrator to make sure the proxy server is working. If you don't believe you should be using a proxy server: Go to the Chrome menu > Settings > Show advanced settings... > Change proxy settings... > LAN Settings and deselect "Use a proxy server for your LAN".

Part 2: Configure a Network Perimeter Firewall

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



pfSense.securelabsondemand.co
Not secure | 172.30.0.254/firewall_rules.php?if=wan
Implementing a Layered Security Solution on the Network
vWorkstation
2023-04-18 15:13:12
Enrique Mejia
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

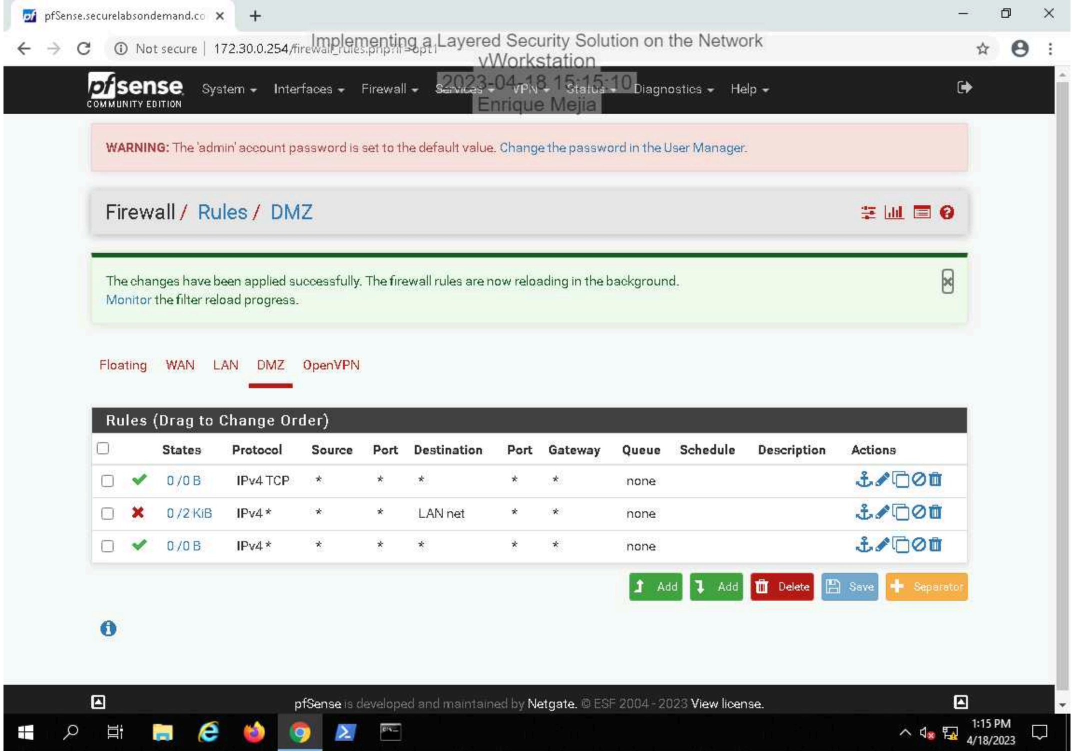
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating
WAN
LAN
DMZ
OpenVPN

Rules (Drag to Change Order)

□		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 / 30 KiB	IPv4 *	*	*	*	*	*	none			

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



pfSense.securelabsondemand.co
Not secure | 172.30.0.254/firewall_rules.php?if=opt1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Implementing a Layered Security Solution on the Network
vWorkstation
2023-04-18 15:15:10
Enrique Mejia

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

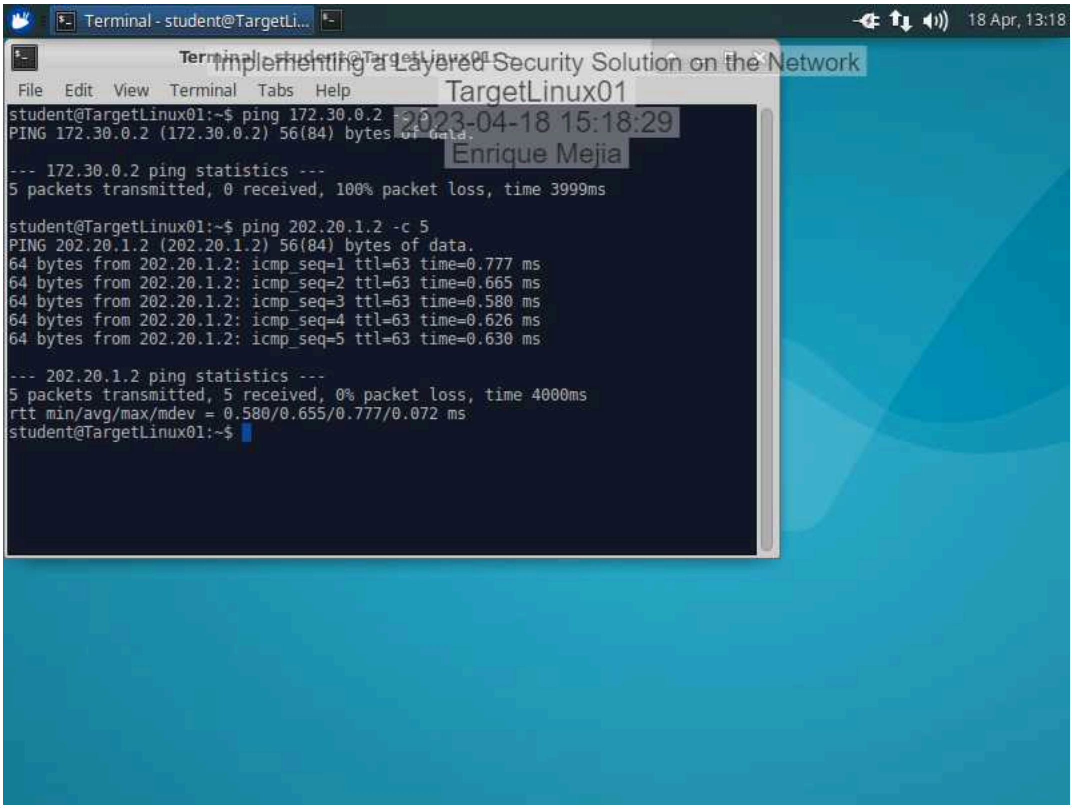
Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

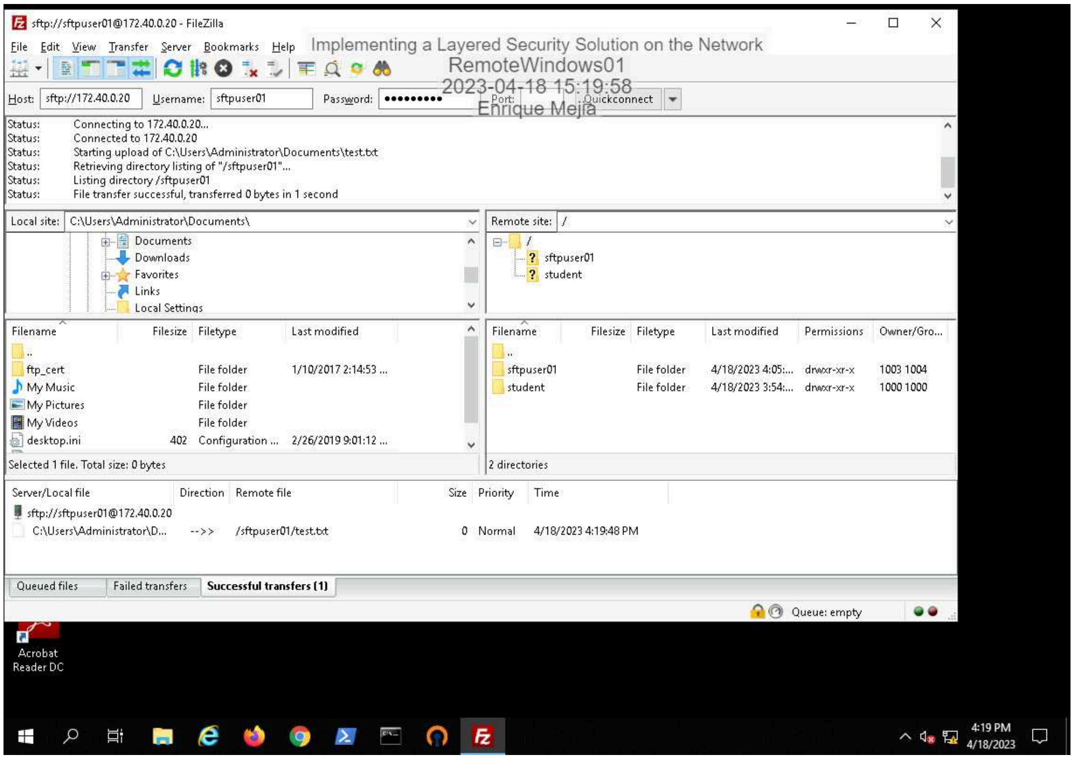
26. **Make a screen capture** showing the **result of both ping operations**.



Terminal - student@TargetLi...
18 Apr, 13:18
Terminal - student@TargetLinux01:~
File
Edit
View
Terminal
Tabs
Help
Implementing a Layered Security Solution on the Network
TargetLinux01
2023-04-18 15:18:29
Enrique Mejia

```
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 3999ms

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=0.777 ms
64 bytes from 202.20.1.2: icmp_seq=2 ttl=63 time=0.665 ms
64 bytes from 202.20.1.2: icmp_seq=3 ttl=63 time=0.580 ms
64 bytes from 202.20.1.2: icmp_seq=4 ttl=63 time=0.626 ms
64 bytes from 202.20.1.2: icmp_seq=5 ttl=63 time=0.630 ms

--- 202.20.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.580/0.655/0.777/0.072 ms
student@TargetLinux01:~$
```

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



sftp://sftpuser01@172.40.0.20 - FileZilla

Implementing a Layered Security Solution on the Network
RemoteWindows01
2023-04-18 15:19:58
Enrique Mejia

Host: sftp://172.40.0.20 Username: sftpuser01 Password: ●●●●●●●●● Port:

```
Status:     Connecting to 172.40.0.20...
Status:     Connected to 172.40.0.20
Status:     Starting upload of C:\Users\Administrator\Documents\test.txt
Status:     Retrieving directory listing of "/sftpuser01"...
Status:     Listing directory /sftpuser01
Status:     File transfer successful, transferred 0 bytes in 1 second
```

Local site: C:\Users\Administrator\Documents\

Remote site: /

Filename	Filesize	Filetype	Last modified
..			
ftp_cert		File folder	1/10/2017 2:14:53 ...
My Music		File folder	
My Pictures		File folder	
My Videos		File folder	
desktop.ini	402	Configuration ...	2/26/2019 9:01:12 ...

Selected 1 file. Total size: 0 bytes

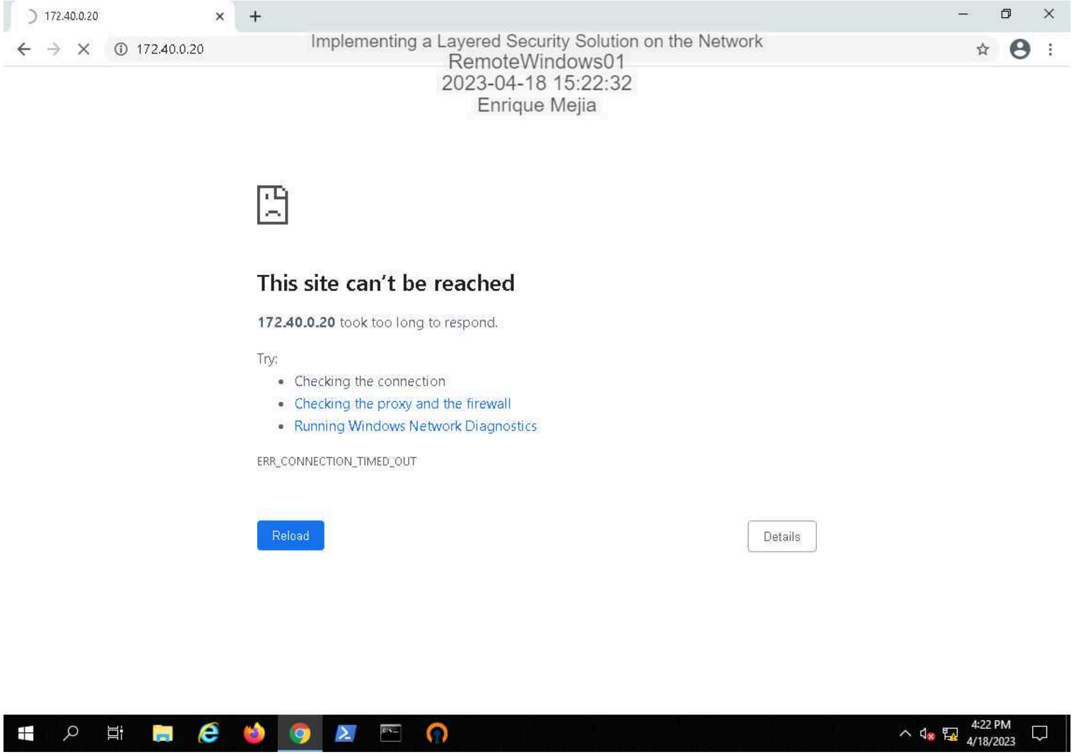
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
sftpuser01		File folder	4/18/2023 4:05:...	drwxr-xr-x	1003 1004
student		File folder	4/18/2023 3:54:...	drwxr-xr-x	1000 1000

2 directories

Server/Local file	Direction	Remote file	Size	Priority	Time
sftp://sftpuser01@172.40.0.20					
C:\Users\Administrator\D...	-->>	/sftpuser01/test.txt	0	Normal	4/18/2023 4:19:48 PM

Queue: empty

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



172.40.0.20

Implementing a Layered Security Solution on the Network
RemoteWindows01
2023-04-18 15:22:32
Enrique Mejia

This site can't be reached

172.40.0.20 took too long to respond.

Try:

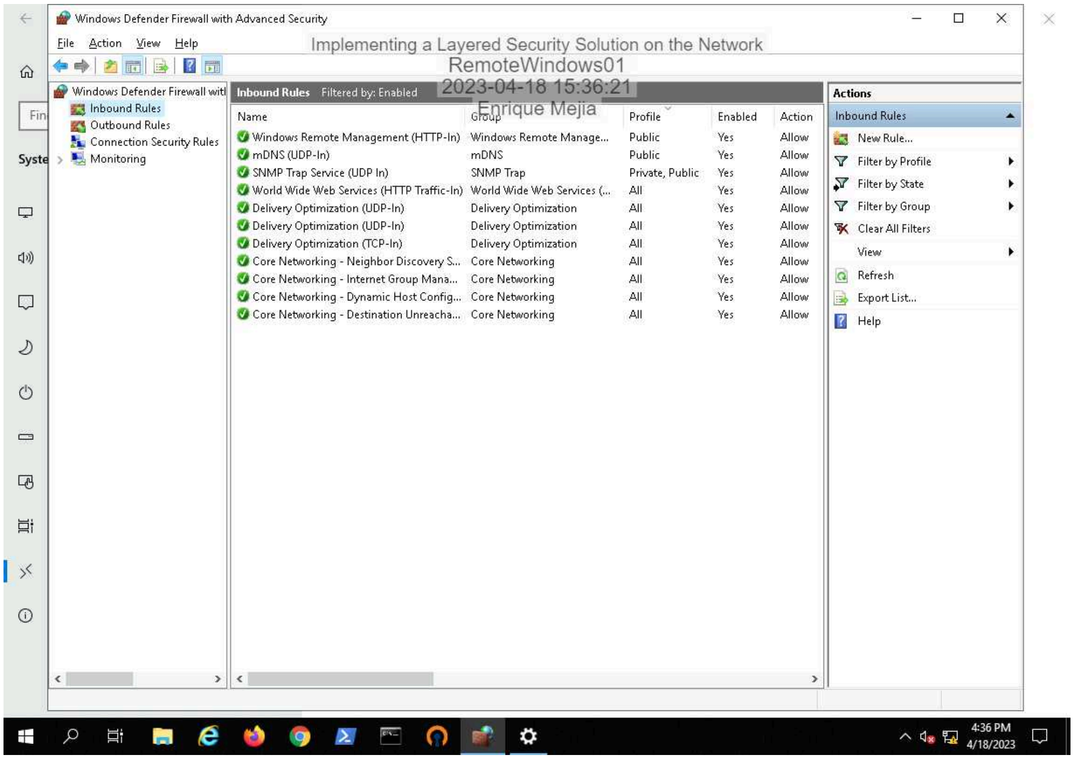
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

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**.



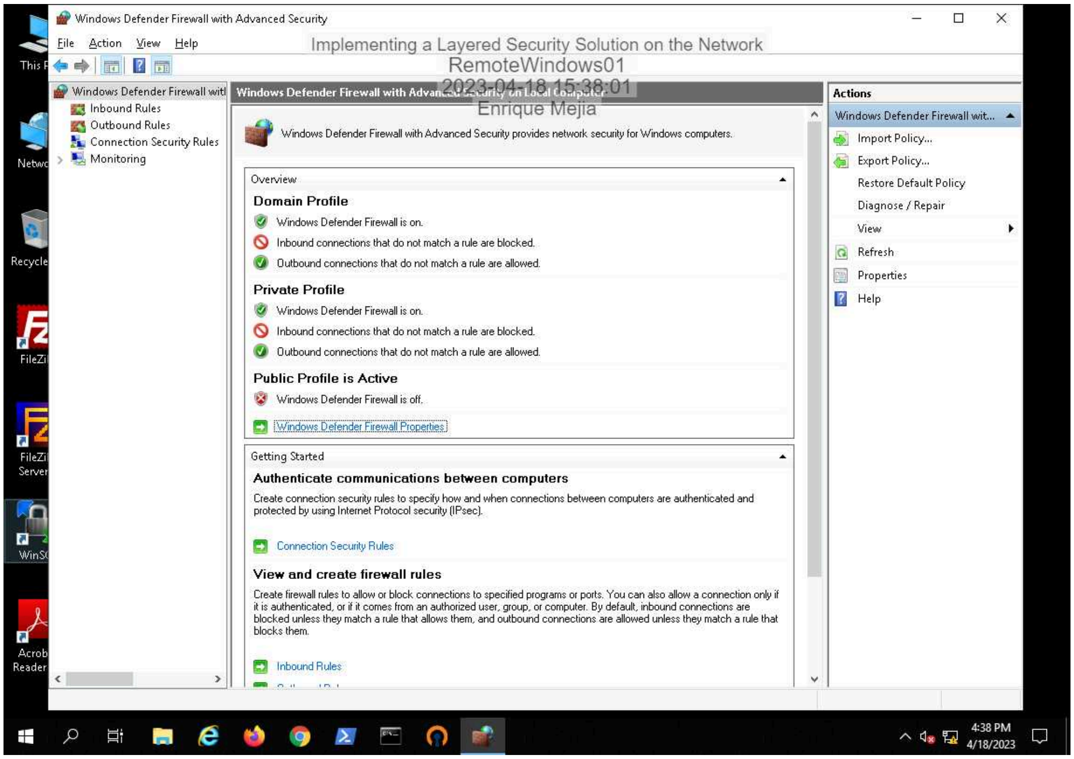
Windows Defender Firewall with Advanced Security

Implementing a Layered Security Solution on the Network
RemoteWindows01
2023-04-18 15:36:21
Enrique Mejia

Inbound Rules Filtered by: Enabled

Name	Group	Profile	Enabled	Action
Windows Remote Management (HTTP-In)	Windows Remote Manage...	Public	Yes	Allow
mDNS (UDP-In)	mDNS	Public	Yes	Allow
SNMP Trap Service (UDP In)	SNMP Trap	Private, Public	Yes	Allow
World Wide Web Services (HTTP Traffic-In)	World Wide Web Services (...	All	Yes	Allow
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes	Allow
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes	Allow
Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow

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



Implementing a Layered Security Solution on the Network
RemoteWindows01
2023-04-18 15:38:01
Enrique Mejia

Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active
- Windows Defender Firewall is off.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

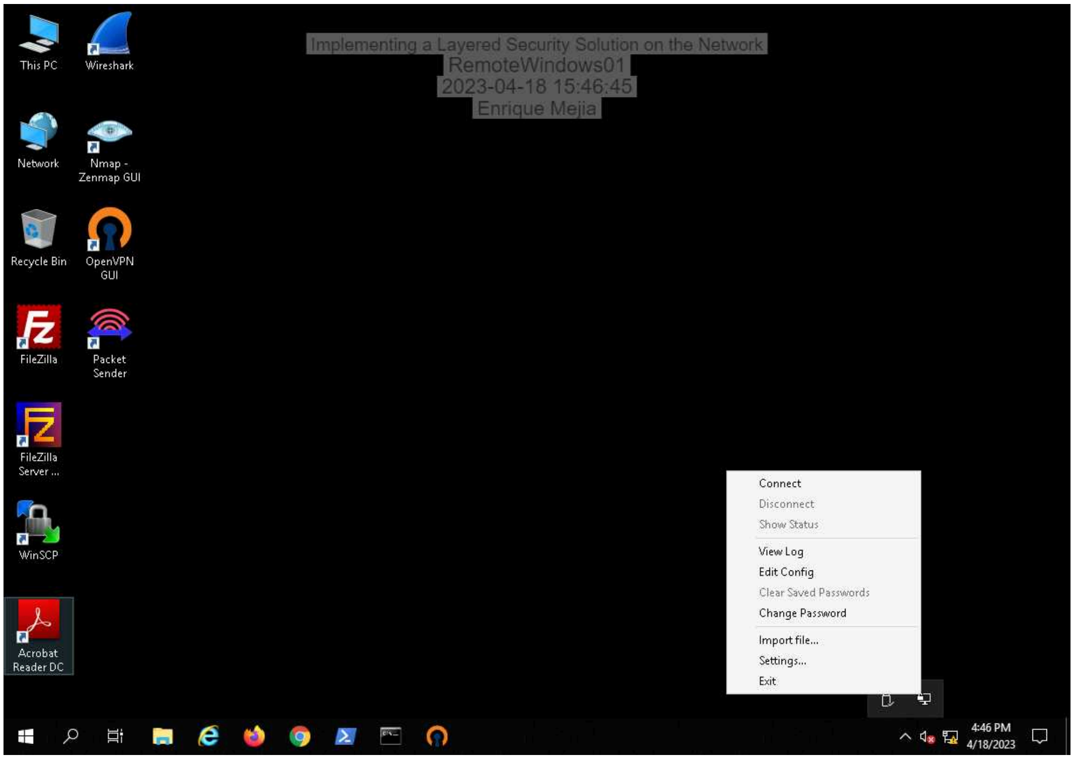
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

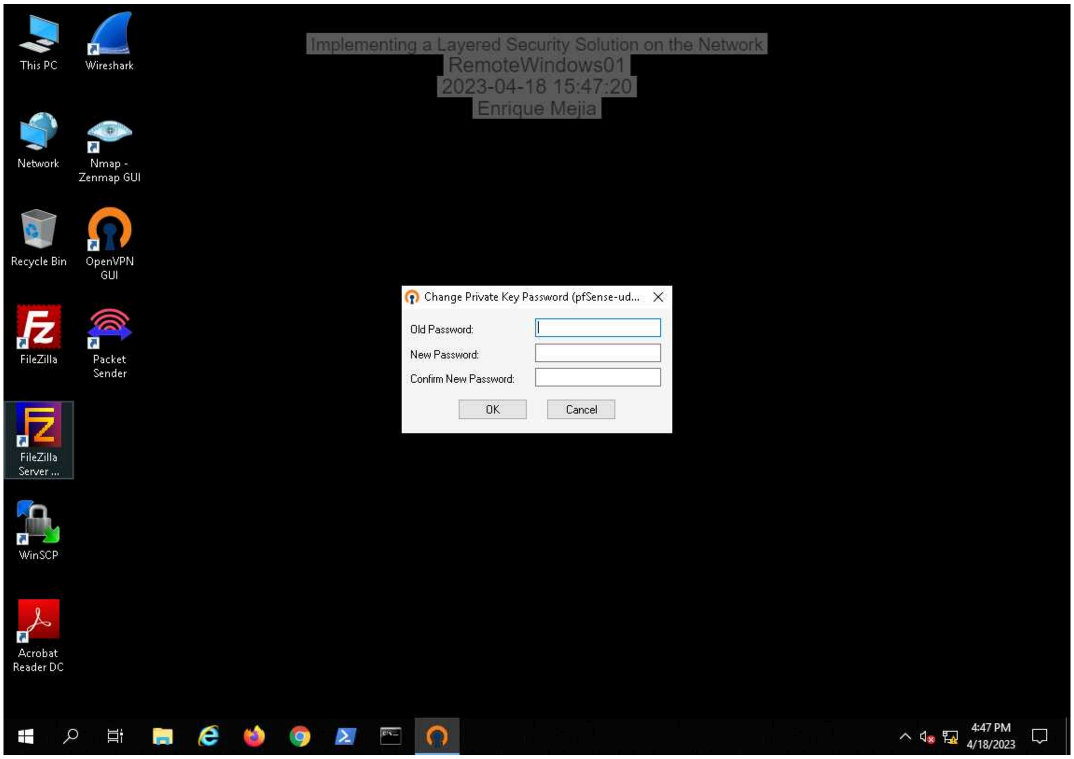
Inbound Rules

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



Implementing a Layered Security Solution on the Network
RemoteWindows01
2023-04-18 15:46:45
Enrique Mejia

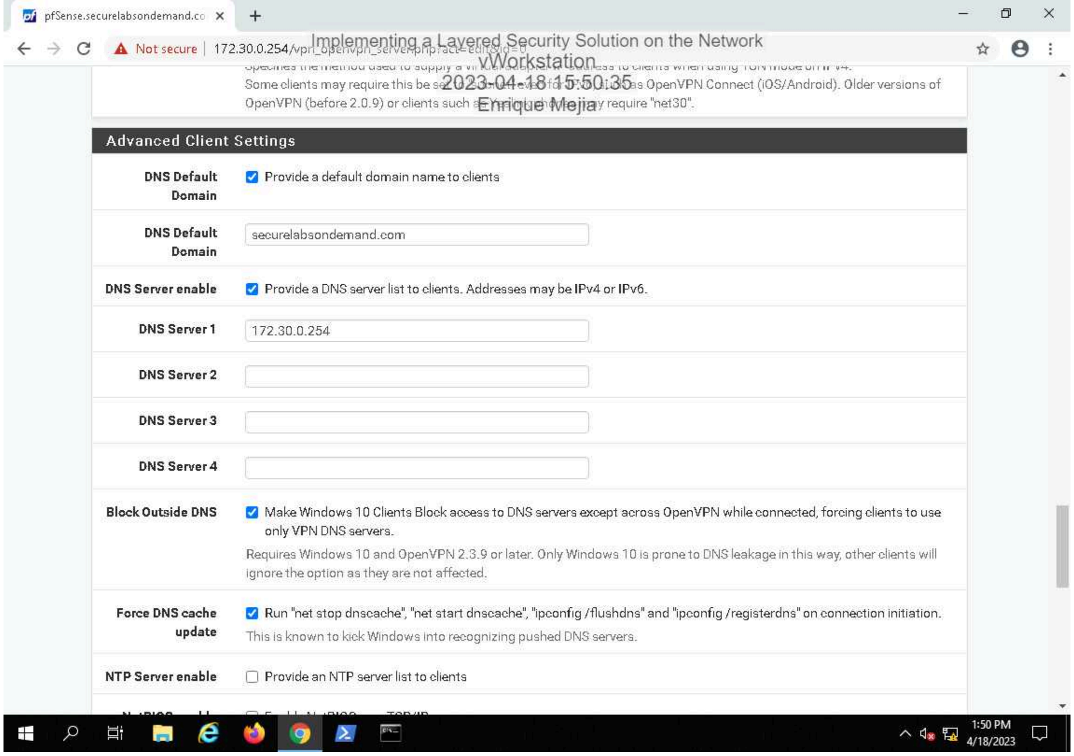
38. **Make a screen capture** showing the **server validation warning is no longer present**.



Implementing a Layered Security Solution on the Network
RemoteWindows01
2023-04-18 15:47:20
Enrique Mejia

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**.


pfSense.securelabsondemand.co
Not secure
172.30.0.254/vpn_openvpn_server.php?act=edit&id=0

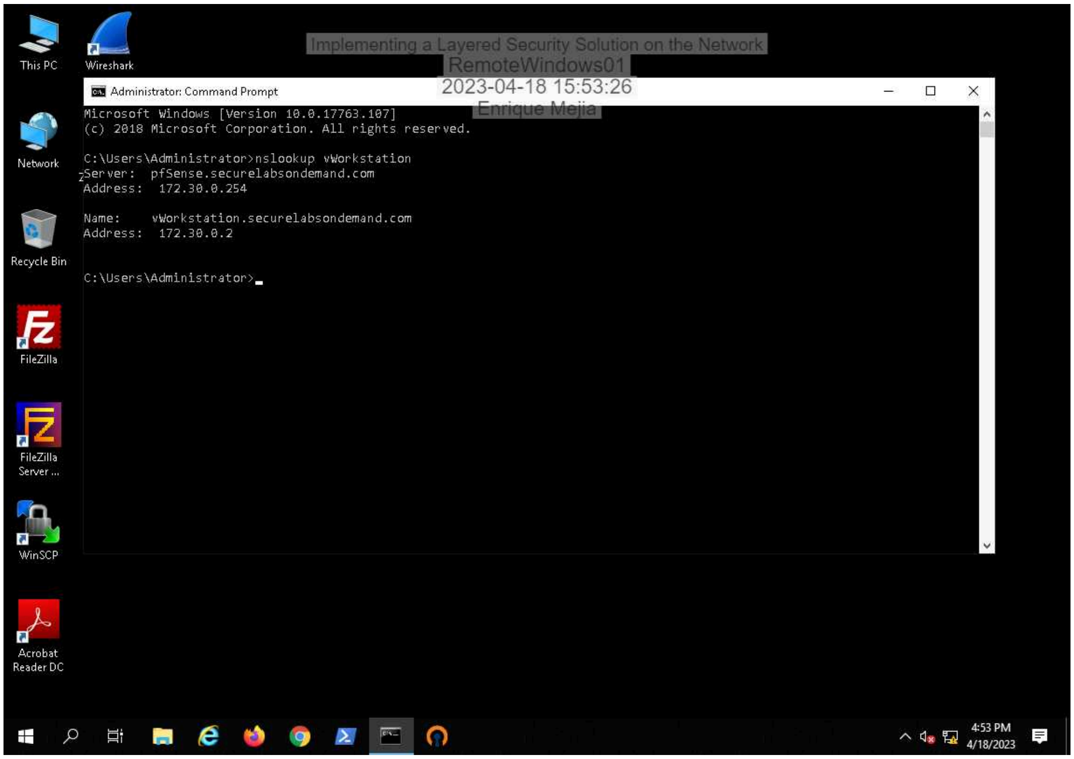
Implementing a Layered Security Solution on the Network
vWorkstation
2023-04-18 15:50:35
Enrique Mejia

Specifies the method used to supply a vi... adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be s... as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such a... y require "net30".

Advanced Client Settings

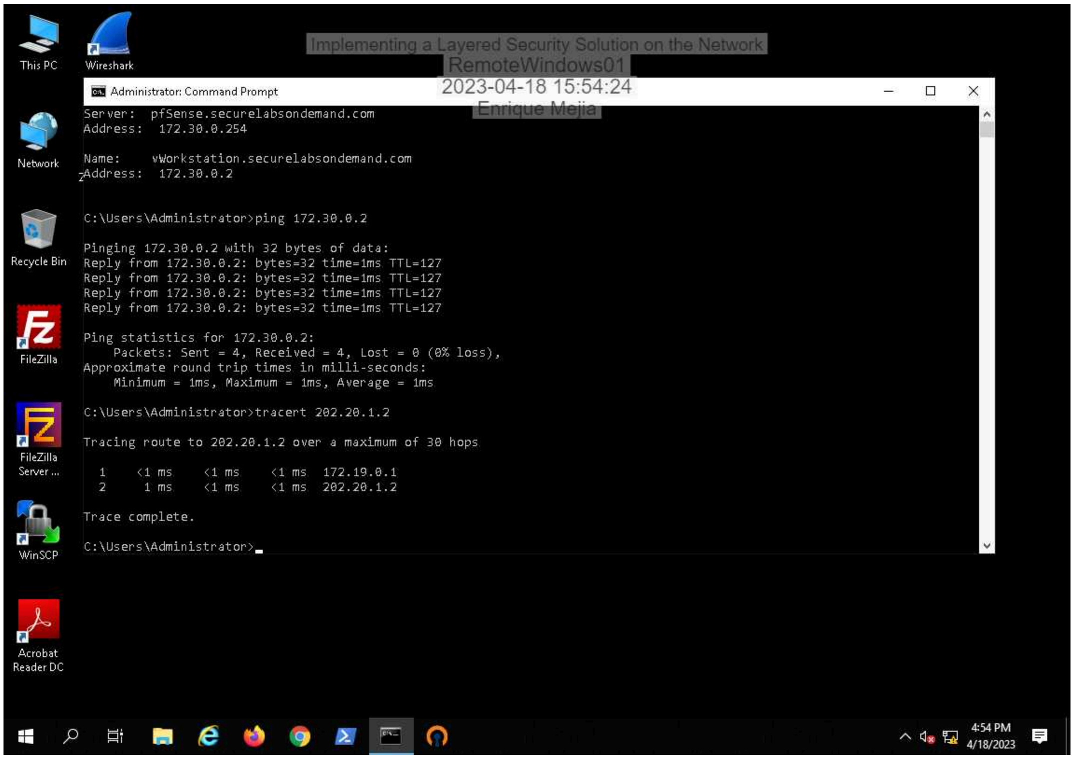
DNS Default Domain	☑ Provide a default domain name to clients
DNS Default Domain	securelabsondemand.com
DNS Server enable	☑ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	172.30.0.254
DNS Server 2	
DNS Server 3	
DNS Server 4	
Block Outside DNS	☑ Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Force DNS cache update	☑ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	☐ Provide an NTP server list to clients

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



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup vWorkstation
Server:  pfSense.securelabsondemand.com
Address:  172.30.0.254

Name:    vWorkstation.securelabsondemand.com
Address:  172.30.0.2


C:\Users\Administrator>_
```

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



```
Server:  pfSense.securelabsondemand.com
Address:  172.30.0.254

Name:    vWorkstation.securelabsondemand.com
Address:  172.30.0.2


C:\Users\Administrator>ping 172.30.0.2

Pinging 172.30.0.2 with 32 bytes of data:
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>tracert 202.20.1.2

Tracing route to 202.20.1.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  172.19.0.1
  2     1 ms    <1 ms    <1 ms  202.20.1.2

Trace complete.

C:\Users\Administrator>_
```

Section 3: Challenge and Analysis

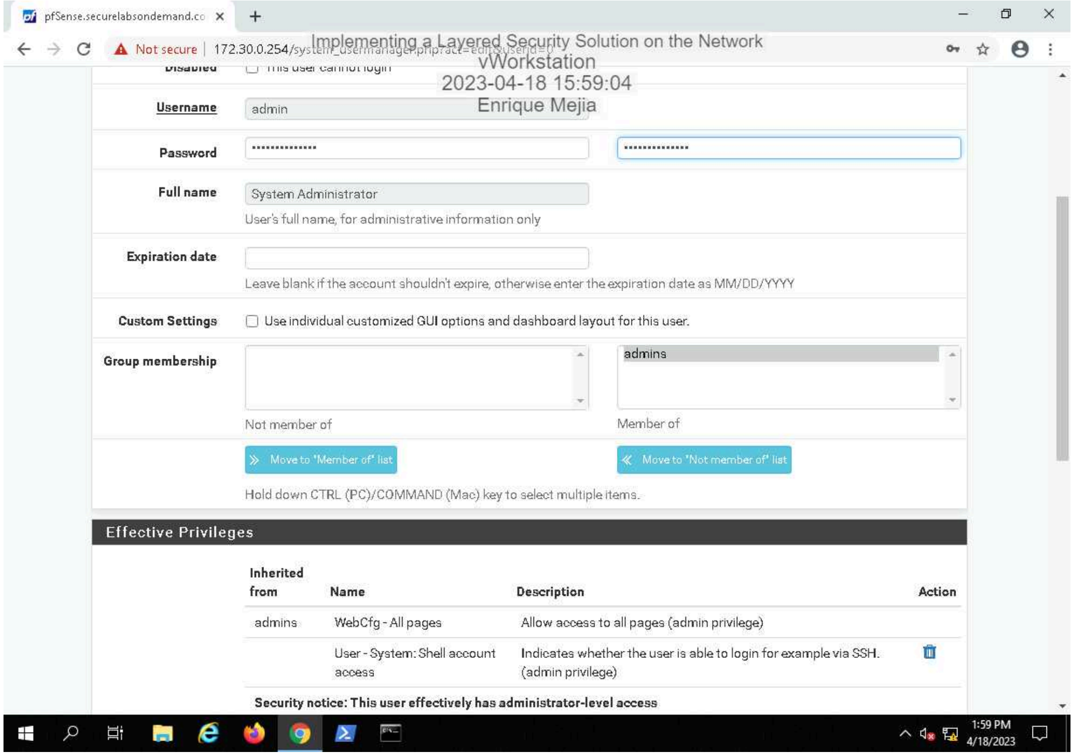
Part 1: Improve User Account Security in pfSense

Document your new password for the admin account.

DallasCowboys2260$!

would be the new password

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



pfSense.securelabsondemand.co

Not secure | 172.30.0.254/system_usermanager.php?act=edit&userid=0

Implementing a Layered Security Solution on the Network
vWorkstation
2023-04-18 15:59:04
Enrique Mejia

Disabled	□ This user cannot login	
Username	admin	
Password	•••••••••••••••	•••••••••••••••
Full name	System Administrator User's full name, for administrative information only	
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY	
Custom Settings	□ Use individual customized GUI options and dashboard layout for this user.	
Group membership	Not member of	admins Member of
	» Move to "Member of" list	« Move to "Not member of" list
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	

Effective Privileges

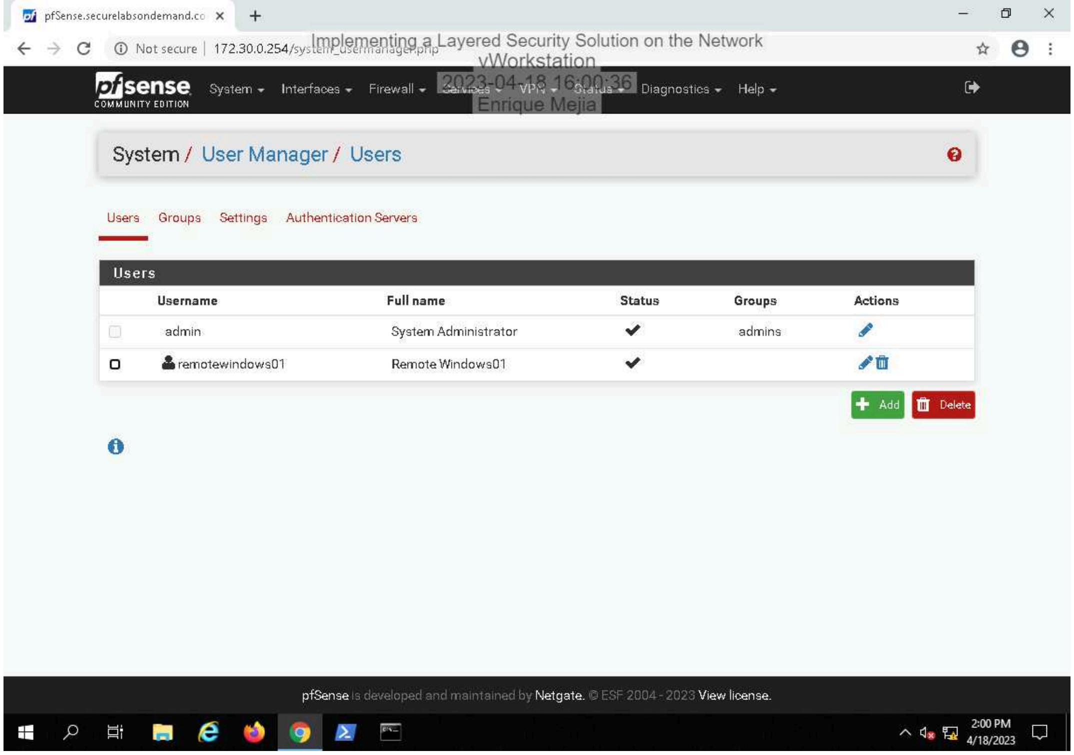
Inherited from	Name	Description	Action
admins	WebCfg - All pages	Allow access to all pages (admin privilege)	
	User - System: Shell account access	Indicates whether the user is able to login for example via SSH. (admin privilege)	🗑

Security notice: This user effectively has administrator-level access

1:59 PM
4/18/2023

Part 2: Force Encrypted Access to the pfSense WebGUI

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


pfSense.securelabsondemand.co
Not secure | 172.30.0.254/system_usermanager.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Implementing a Layered Security Solution on the Network
vWorkstation
2023-04-18 16:00:36
Enrique Mejia

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
□	admin	System Administrator	✓	admins	✎
□	remotewindows01	Remote Windows01	✓		✎ 🗑

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.