IT357 Tools and Techniques in Defensive Security
Assignment 5 – Firewall Configuration
15questions – 50 Points

Save this as PDF and submit on ReggieNet

Objective: To implement firewall rules and policies that make sense for a small organization.

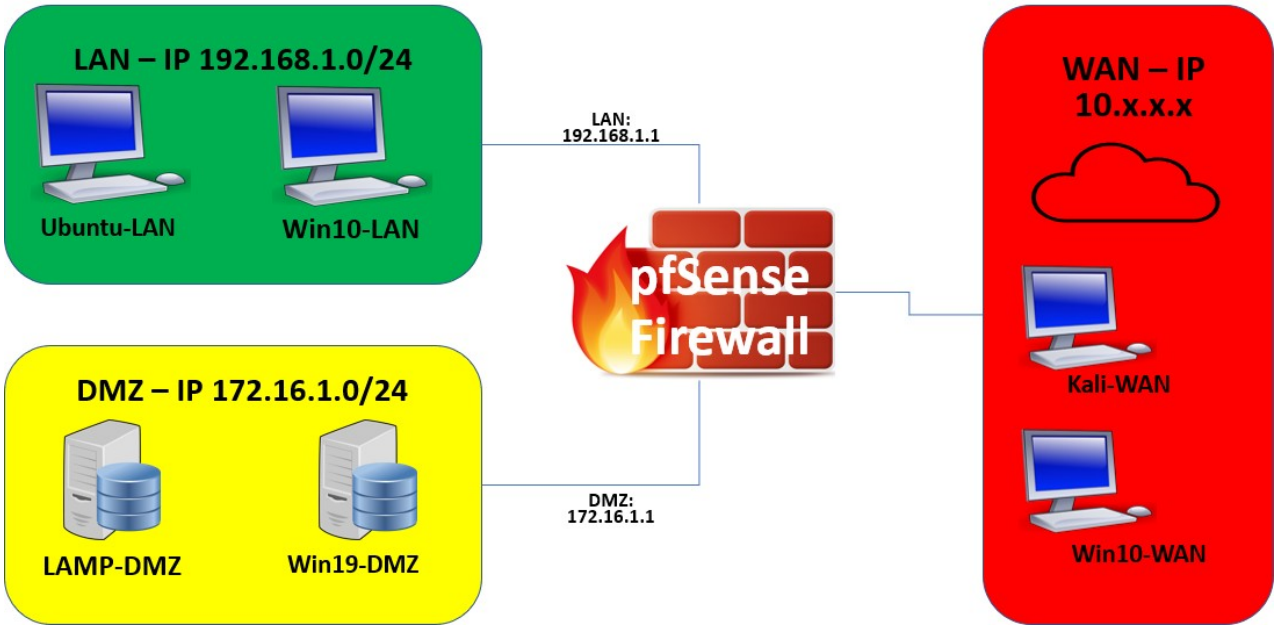
Preparation:

In the ProxMox environment, use the Ubuntu-LAN, LAMP-DMZ, Win10-WAN,and the pfSense Console.

Scenario:

You are administering a small network that looks like the diagram below. The small office network consists of a private network (LAN: Windows 10 user desktop and Ubuntu Desktop), a demilitarized zone (DMZ: Ubuntu LAMP Server), all protected by a pfSense Firewall. The Internet is represented by the red WAN zone. An attacker/eavesdropper is represented by a Windows 10 desktop connected to the public Internet as well.

ProxMox VM Environment and Network Config



Currently, the pfSensefirewall is set to its default state, that is, it blocks all ingress traffic to the private network and DMZ, while allowing all egress traffic from the private network and the DMZ. Thus, all application traffic out of the internal network and DMZ is allowed while the web server running on the LAMP-D machine cannot be seen from the outside world. The firewall must be configured to allow HTTP traffic to theLAMP-D server.

The LAMP-D serverhas its host firewall turned OFF, which will need to be enabled and then exceptions allowed for the server to be able to serve web requests. Then, the LAMP-D server canbe

accessed from the Win10-WANhost on the outside (on the Internet, WAN).

The Win10-WANhostwillhave default Windows firewall rules; these will remain unchanged.

Firewall Status			
OS	**Current**	**Target Ingress Rule**	**Target Egress Rule**
pfSense	**Internal and DMZ:** -Everything blocked in and everything allowed out	**DMZ**: -Allow HTTP -Allow HTTPS -Deny everything else **LAN - Internal Network**: -Deny everything	**DMZ**: -Deny everything **LAN - Internal Network**: -Allow HTTP -Allow HTTPS -Allow ICMP -Allow DNS (UDP) -Deny everything else
LAMP-DMZ Host Firewall	-Firewall turned OFF -Everything allowed	-Default policy change to DENY -Allow HTTP -Allow HTTPS	-Default policy change to DENY

NOTE: All screenshots must be large enough to see the details being asked to show in the screenshot. Use the Windows snipping tool to crop out relevant part of the screen instead of inserting the entire screen in your report.

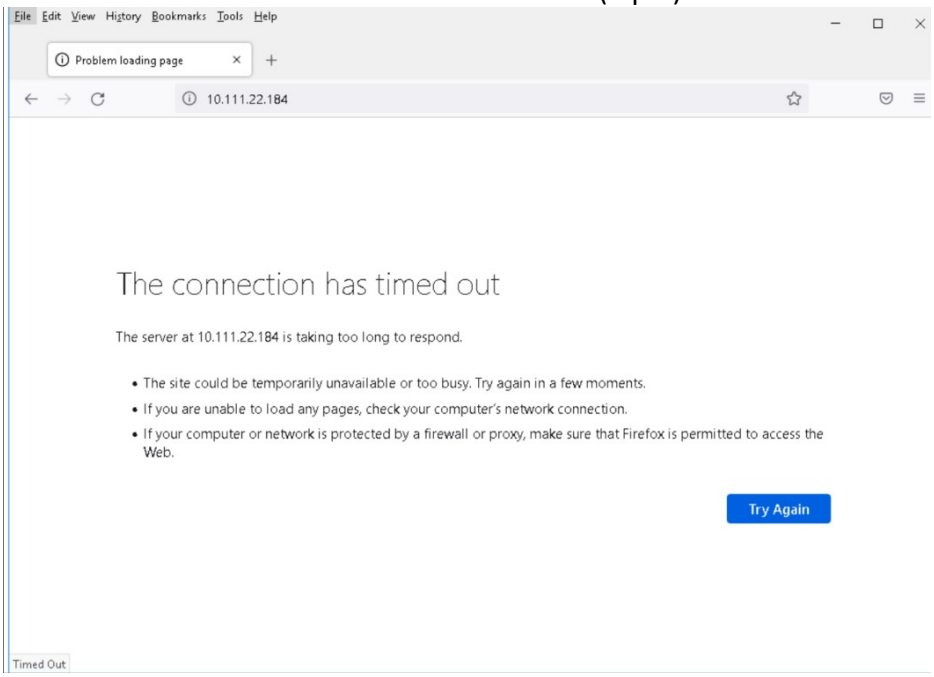
NOTE: To simplify the implementation and testing of the firewall rules, it will be necessary to remove the HTTP to HTTPS redirectionfrom our SSL/TLS assignment. To do this, on the LAMP-D VM, simply add a # in front of the "Redirect" line of the /etc/apache2/sites-available/000-default.conf file.

Part 1: pfSense

Q1) First, find the IP addresses of all your VMs, and record them here. Log in to each VM, including theconsole of the pfSense VMand use the appropriate command-line tool to find the IP addresses, and record them in the table below (5 pts).

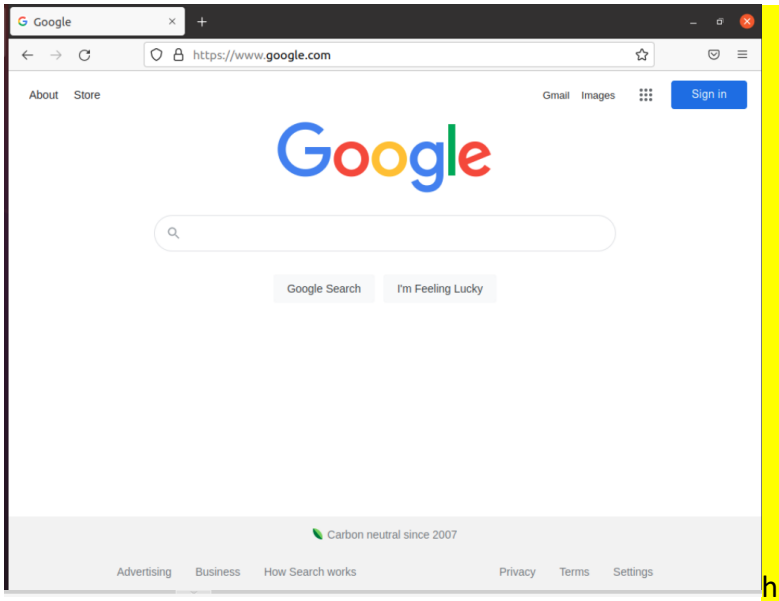
Win10-WAN:	10.111.16.85
LAMP-D:	172.16.1.21
Ubuntu-LAN:	192.168.1.106
pfSenseWAN interface:	10.111.22.184
pfSenseLANinterface:	192.168.1.1
pfSenseDMZ interface:	172.16.1.1

Q2) Verify that you CANNOT access the web server running on LAMP-D from the Win10-WAN host. On the Win10-WAN desktop, open a browser, and go to http://<IP_OF_pfSense_WAN_PORT>, replacing the text in brackets with the real IP address for the WAN port found above. Your browser should show a timeout or unreachable error. (3 pts)

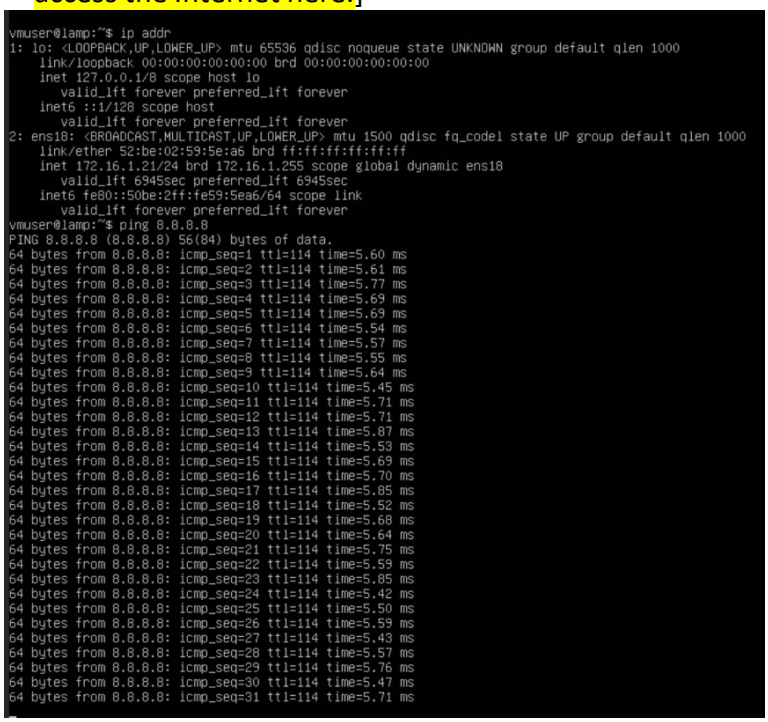


Q3) Verify that the Internet is accessible from both the Ubuntu-LAN machine and the LAMP-D server. Ping to 8.8.8.8 from the LAMP server to verify connectivity. (4 pts)

[Insert screens



hots for both the machines showing that they can access the Internet here.]



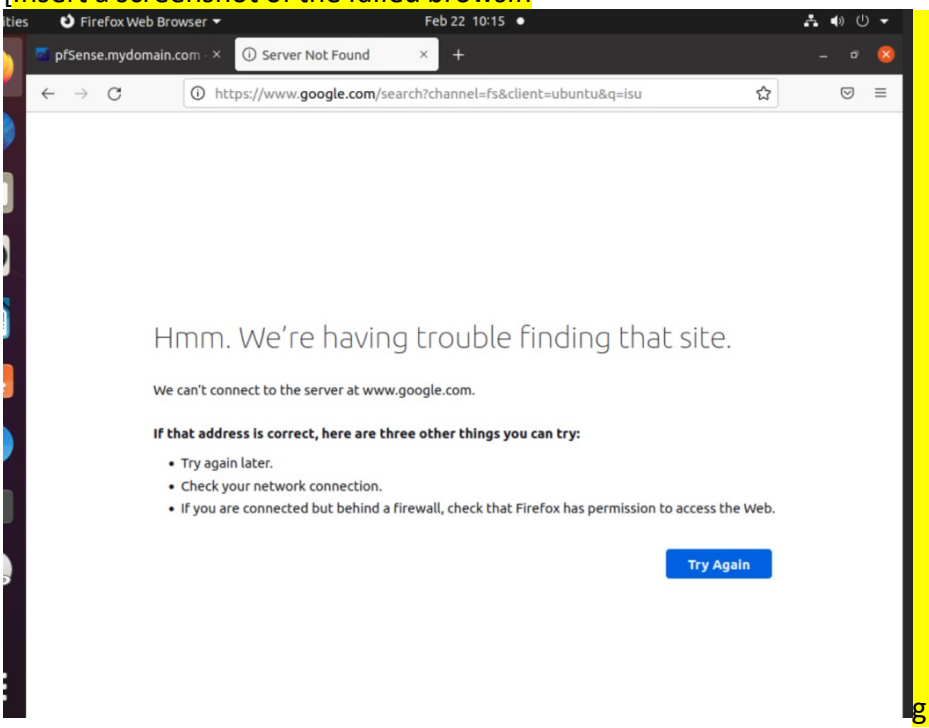
```
vmuser@lamp:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:be:02:59:5e:a6 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.21/24 brd 172.16.1.255 scope global dynamic ens18
       valid_lft 6945sec preferred_lft 6945sec
    inet6 fe80::50be:2ff:fe59:5ea6/64 scope link
       valid_lft forever preferred_lft forever
vmuser@lamp:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=5.60 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=5.61 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=5.77 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=5.69 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=5.69 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=5.54 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=5.57 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=114 time=5.55 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=114 time=5.64 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=114 time=5.45 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=114 time=5.71 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=114 time=5.71 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=114 time=5.87 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=114 time=5.53 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=114 time=5.69 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=114 time=5.70 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=114 time=5.85 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=114 time=5.52 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=114 time=5.68 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=114 time=5.64 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=114 time=5.75 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=114 time=5.59 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=114 time=5.85 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=114 time=5.42 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=114 time=5.50 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=114 time=5.59 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=114 time=5.43 ms
64 bytes from 8.8.8.8: icmp_seq=28 ttl=114 time=5.57 ms
64 bytes from 8.8.8.8: icmp_seq=29 ttl=114 time=5.76 ms
64 bytes from 8.8.8.8: icmp_seq=30 ttl=114 time=5.47 ms
64 bytes from 8.8.8.8: icmp_seq=31 ttl=114 time=5.71 ms
```

Reconfigure the pfSense firewall device to allow the Win10-WANhost (WAN/Internet) to connect to the LAMP-D web server in the DMZ. pfSense is a console-only distribution, and while you can create firewall rules that way, the web interface is MUCH easier to use. To get to it, open a browser on Ubuntu-LAN and browse to https:**//**<IP_OF_pfSense_LAN_PORT>. Use the credentials provided at the beginning of this document to login to the web interface.

1. Change the default policy of egress traffic from the internal network to deny by default by going to **Firewall→Rules** andthen selecting the **LAN** tab. Click on the pencil (edit) icon of the "Default allow LAN to any rule" to open the rule editing page. At the top of the page, change the **Action** to Block. Scroll down to near the bottom of the page and change the **Description** to "Default deny LAN to any rule" and then click the Save button at the bottom of the page.Now, back on the LAN firewall rules page, be sure to click the **Apply Changes** button at the top of the page.

   Q4) Test the change by trying to browse the Internet from the Ubuntu-LANmachine. This should now fail. (3 pts).

   [Insert a screenshot of the failed browsin

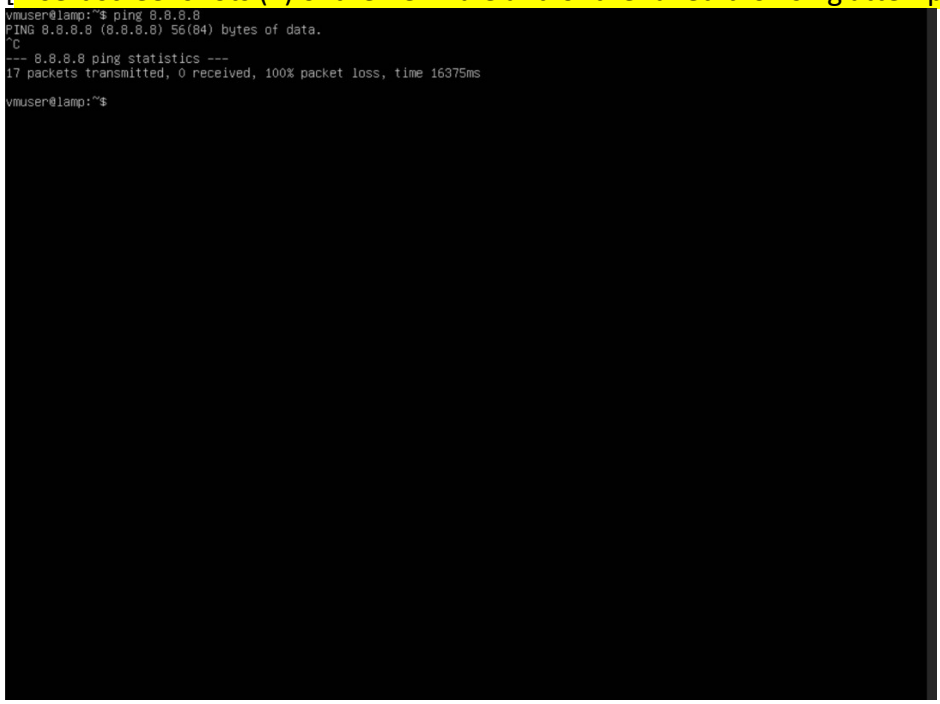


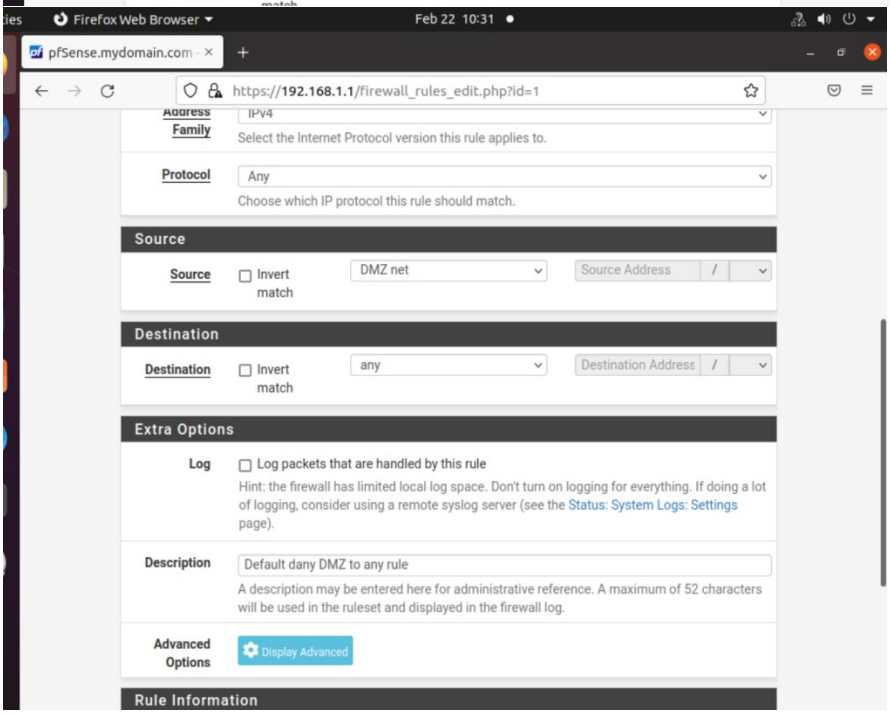
g attempt here]

2. Repeat the process for the DMZ by selecting the **DMZ** tab of the Firewall Rules page. Change the **Action**and **Description** of the “Default allowDMZ to any rule” the same as we did for the default LAN rule.Save and Applythe rule and test the settings by pinging 8.8.8.8 from the LAMP-D server.

   Q5) This should fail now. (4 pts).

   [Insert screenshots (2) of the new rule and of the failed browsing attempt here]





3. Create a set of NAT Port Forward rules (also known as Destination NAT) that allows ingress HTTP and HTTPS traffic on the WAN interface of pfSense, to the LAMP-D server. To do this, go to **Firewall→NAT**and then select the **Port Forward** tab. Key things to remember when creating port forward rules are the LAMP-D machine's IP as the redirect target, and to use HTTP(80) and HTTPS(443) as the destination port and redirect port.

   Q6) Show the NAT Port Forward rules and the relevant **descriptions** on each rule (3 pts)

   [Take a screenshot of the NAT Port Forward rules. There should be relevant **descriptions** on each rule]

Activities Firefox Web Browser Feb 24 15:39

pfSense.mydomain.com

https://192.168.1.1/firewall_nat_edit.php?id=0

Destination port range

HTTP (From port) | Custom | HTTP (To port) | Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Single host (Type) | 172.16.1.21 (Address)

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

HTTP (Port) | Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description

NET port forwrding

A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync

☐ Do not automatically sync to other CARP members

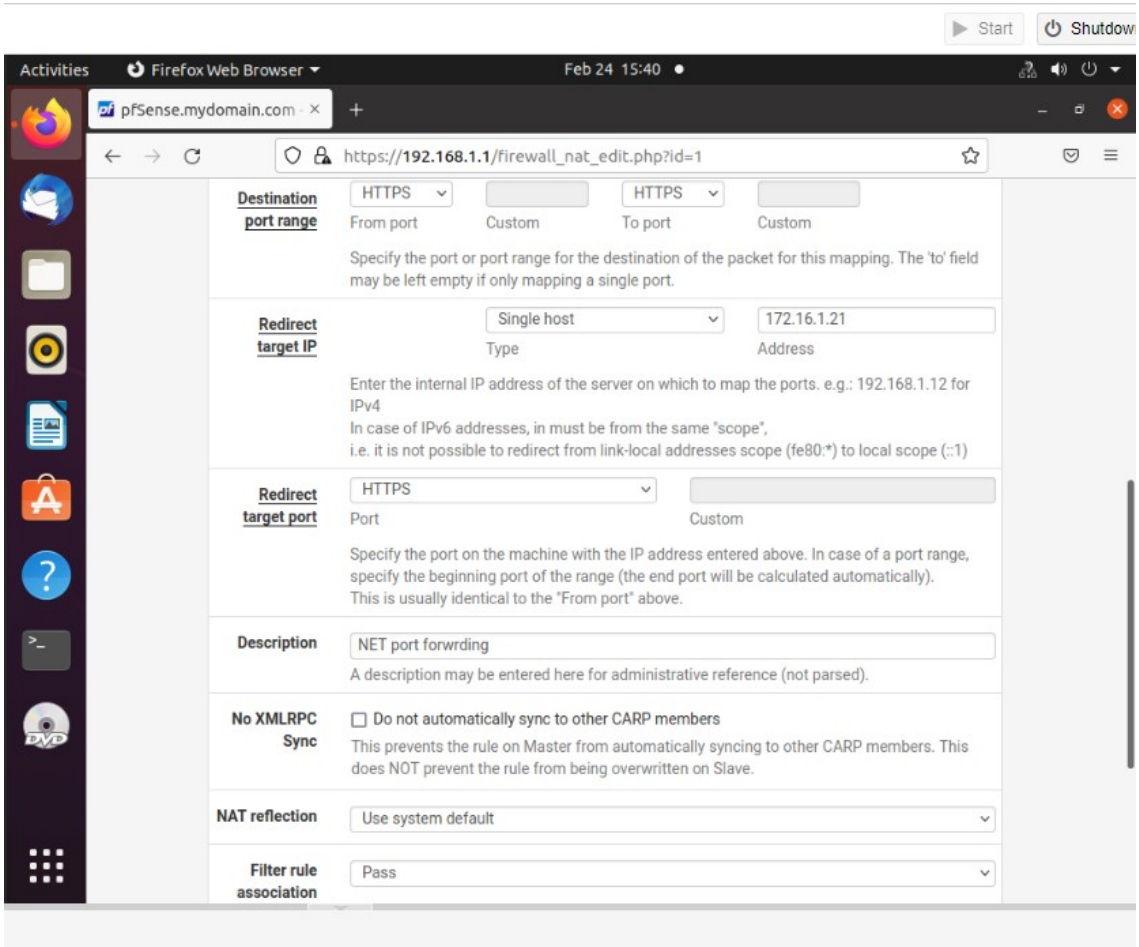
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Use system default

Filter rule association

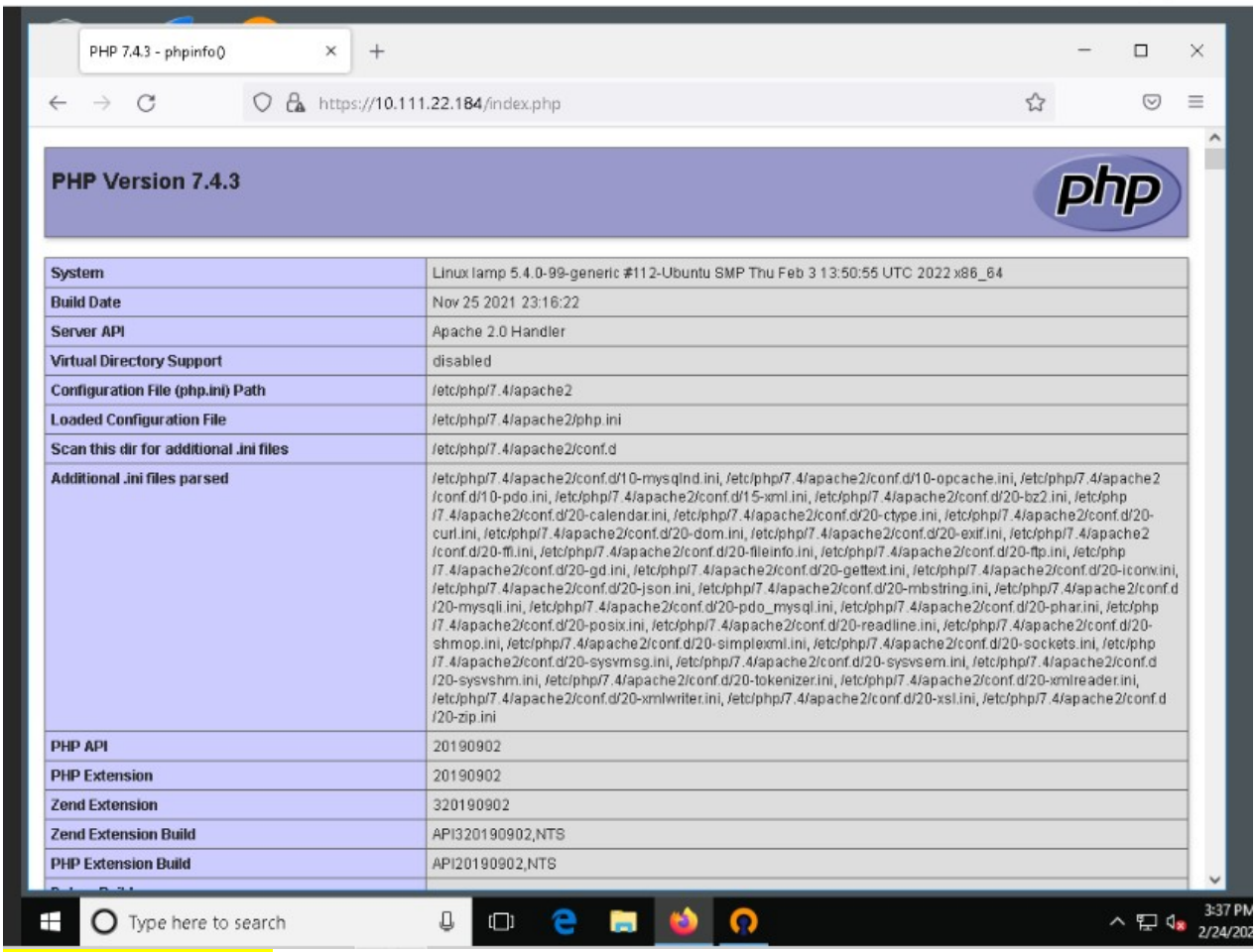
Pass


Start
Shutdow
Activities
Firefox Web Browser
Feb 24 15:40
pfSense.mydomain.com
https://192.168.1.1/firewall_nat_edit.php?id=1
Destination port range
HTTPS
From port
Custom
HTTPS
To port
Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP
Single host
Type
172.16.1.21
Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)
Redirect target port
HTTPS
Port
Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.
Description
NET port forwrding
A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync
Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection
Use system default
Filter rule association
Pass

Now, test the rule, by going to the browser in your Win10-WAN, and entering **https://**<IP_OF_pfSense_WAN_PORT>.

Q7) If everything is working properly, you should see the default PHP page of the Apache web server running on LAMP-D. (3 pts)

[Insert a screenshot of that page. THE URL BAR SHOWING THE IP ADDRESS OF pfSense firewall MUST BE VISIBLE

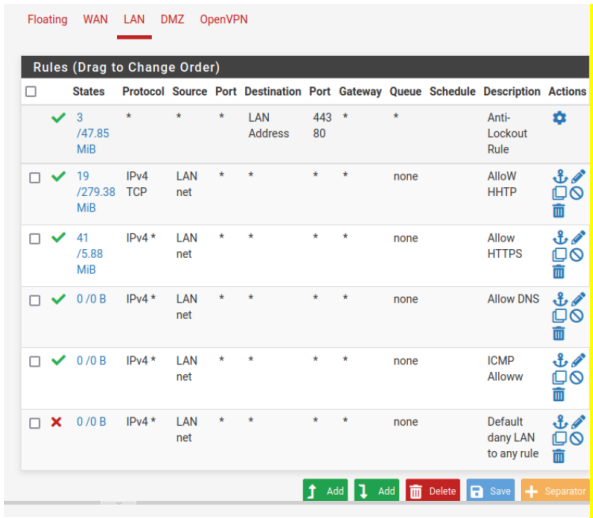


IN THE SCREENSHOT]

4. Create a set of firewall rules that allows egress traffic according to the table above. These rules apply to the**LAN** Interface of pfSense, in other words, allowing traffic out to the WAN-Internet. Refer to https://docs.netgate.com/pfsense/en/latest/firewall/configure.htmlfor details of how to create a firewall rule.
    a. Notes:
        i. You should make 4 rules
        ii. The **source** for all the rules should be “LAN net”
        iii. The **destination** for all the rules should be “Any”
        iv. Only the **destination port** for the protocol needs to be set (or choose from the predefinedports instead)
        v. **Be careful** to choose TCP, ICMP, or UDP, depending on what the protocol listed in the table above actually uses
        vi. **Be careful** to consider the order of the firewall rules

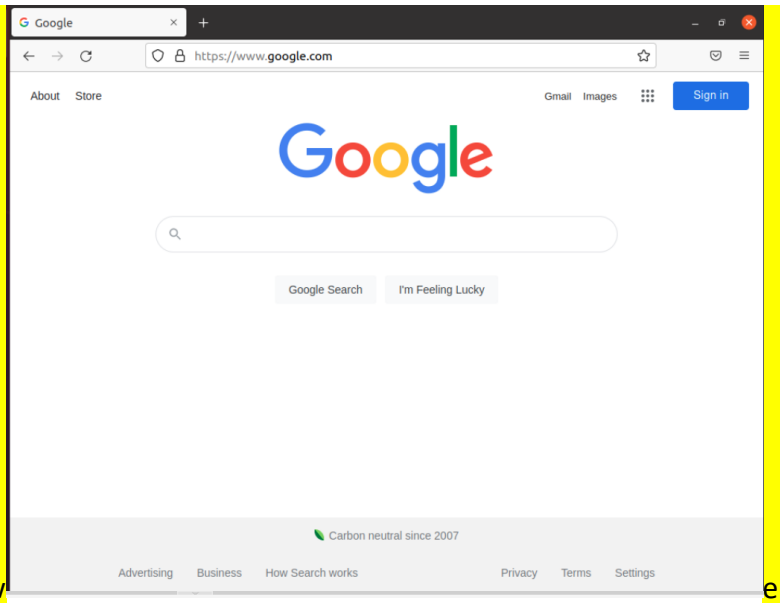
Q8) Show the created LAN rules. There should be meaningful descriptionsfor each rule. (3 pts)

[Screenshot of rules and



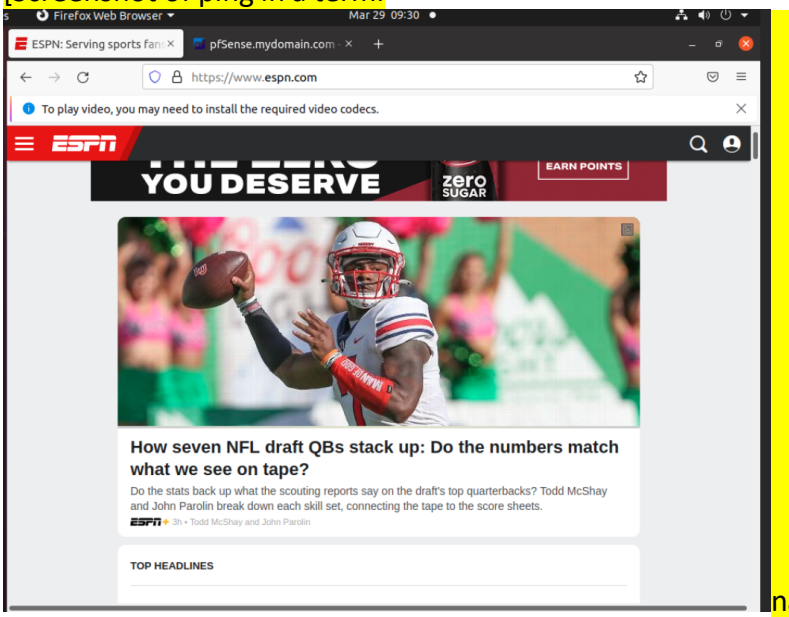
descriptions]

Q9) From the Ubuntu-LAN, verify that you can browse the web. (3 pts)

[Screenshot of the w 

eb browser accessing an Internet site]

Q10) From the Ubuntu-LAN, verify that you can ping the outside world, like espn.com or 8.8.8.8. (3 pts)

[Screenshot of ping in a termi 

nal pinging an Internet site]

HINT: Several commands need administrator privilege. If you get "permission denied" errors, use *sudo*.

Part 2: iptables – Linux host-based firewall

1. Configure the host firewall of the Ubuntu LAMP server. Since the server is a console only distribution, you will need to use iptables to configure the firewall. *ufw* is aneasyto use front end for iptables, so you can use it instead of iptables to configure the host firewall. To

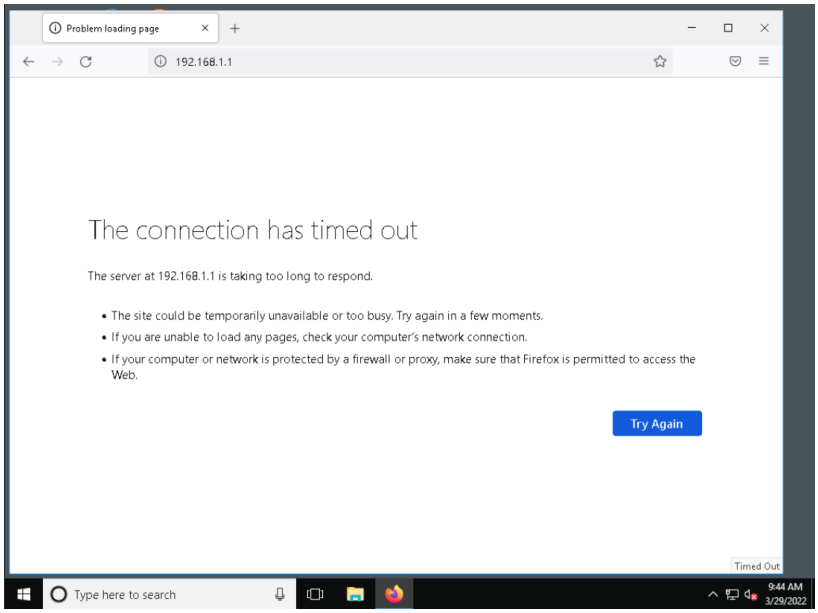
get an overview of *ufw* and basic configuration commands, see https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-18-04

2. First, enable the firewall and change the default policy for both ingress and egress traffic to "DENY".

   After changing the default policy to DENY, try to browse from the Windows 10 VM to the Ubuntu web server. This should fail. In other words, even though we just opened the pfSense firewall ports, and could successfully browse to the server on Ubuntu, setting a host-based firewall rule blocks the traffic at that machine, even though our border firewall allows it.

   Q11) Screenshot of Win10-WAN, showing that it is not able to access the LAMP-D web server. THE URL BAR SHOWING THE IP ADDRESS OF THE pfSense firewall MUST BE VISIBLE IN THE SCREENSHOT:(3 pts)

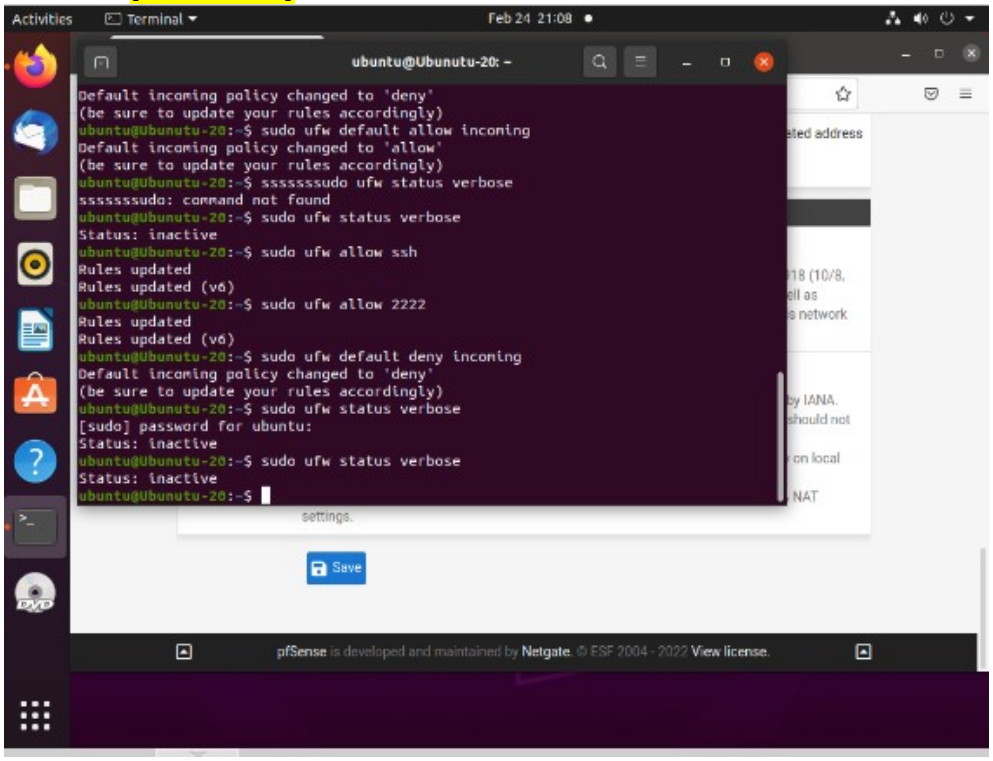
   [Screenshot]



3. Allow the exceptions for the ingress traffic to the LAMP-D server from the table at the start of the document (i.e., allow ingress HTTP and HTTPS).

   Q12) Take a screen shot of the rules that you created by using the command 'sudoufw status verbose' and insert it here (3 pts).

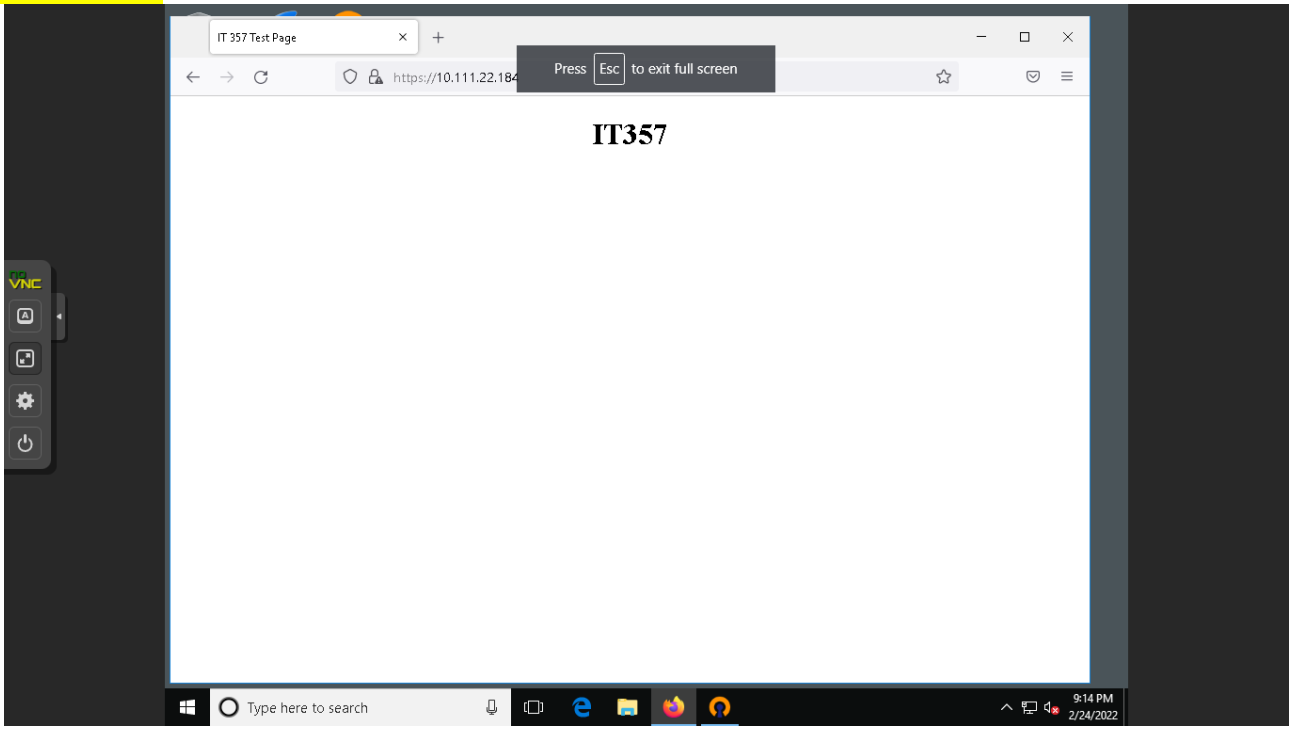
   [Screenshot]



4. Use the Win10-WAN to browse to the LAMP-D webserver. Remember to use the pfSenseWAN IP address. You should be able to view the Apache webpage.

   Q13) Screenshot of Win10-WAN accessing the LAMP-D web server. THE URL BAR SHOWING THE IP ADDRESS OF THE PFSENSE WAN PORT MUST BE VISIBLE IN THE SCREENSHOT: (3 pts)

   [screenshot]



Thought Questions:

14. In pfSense, under **Interfaces→WAN**and in the **Reserved Networks** section at the bottom of the page are two check boxes. One for blocking private network addresses and one for blocking bogon networks. These two settings automatically generate firewall rules that are applied to the WAN interface. During a normal perimeter firewall deployment, why would you want these two settings enabled?Why do we NOT want to block private addresses in our lab environment?(3 pts)

    Unless private IP space is in use on the WAN, enable this option. This only applies to traffic initiated on the WAN side. Local clients may still reach hosts on private networks form the inside of the firewall.
    We don't want to block private addresses in our lab environment because need to use them! Our LAN environment. resides inside of ISU's LAN environment; meaning, it would take considerable effort to. make our LAN environment work with public IPs-so we use private IPs.

15. DNS normally uses UDP port 53 for standard DNS lookups. Opening TCP port 53 for DNS creates a potential security vulnerability called a DNS zone transfer vulnerability. In your own words, explain this attack. (3 pts)

SAVE THIS AS A PDF&SUBMIT ON REGGIENET