

## Lab 5.3.3: Configuring a DMZ / Screened Subnet on a Security Appliance (pfSense)

*From TestOut CompTIA Security+ Course*

In this lab I will be setting up and configuring a Screened Subnet / DMZ (DeMilitarized Zone) on a pfSense Security Appliance.

### **The scenario for this lab is as follows:**

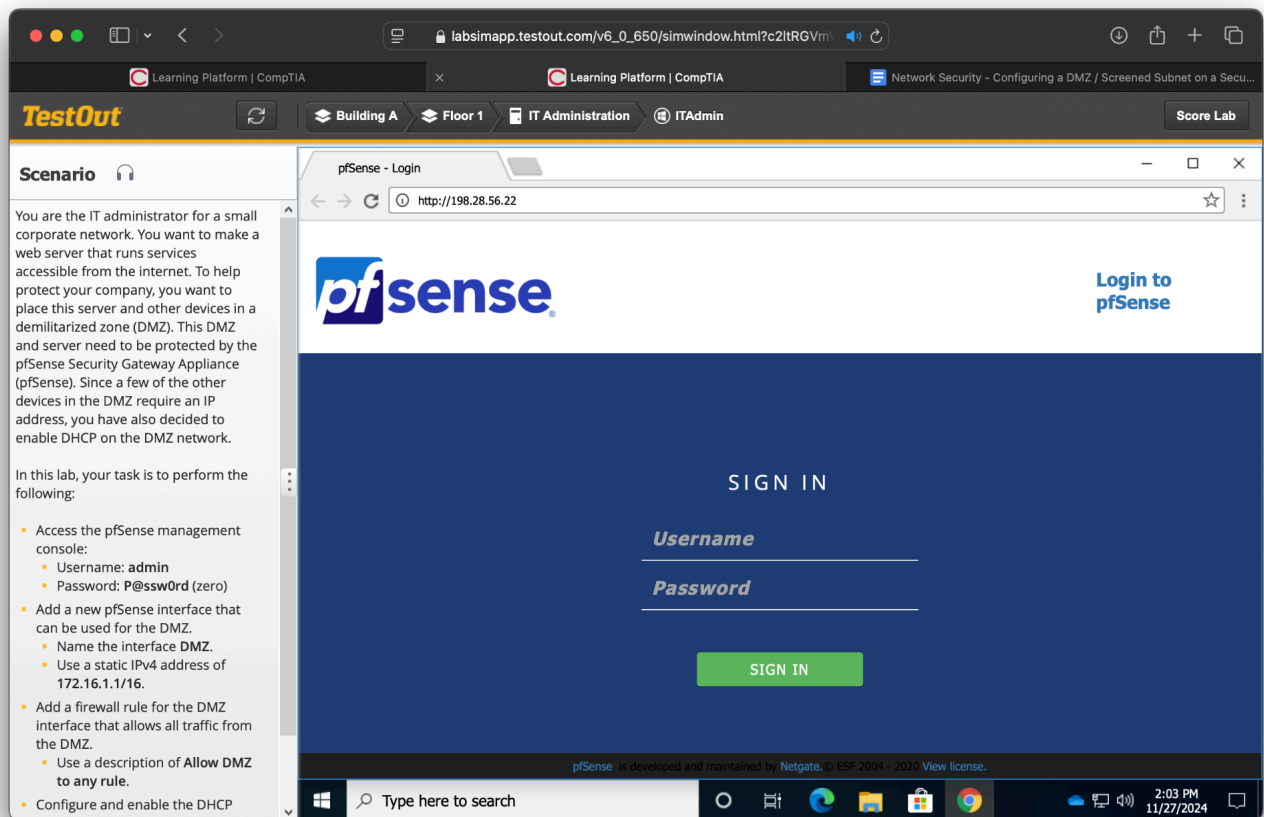
“You are the IT administrator for a small corporate network. You want to make a web server that runs services accessible from the internet. To help protect your company, you want to place this server and other devices in a demilitarized zone (DMZ). This DMZ and server need to be protected by the pfSense Security Gateway Appliance (pfSense). Since a few of the other devices in the DMZ require an IP address, you have also decided to enable DHCP on the DMZ network.

In this lab, your task is to perform the following:

- **Access the pfSense management console:**
  - Username: admin
  - Password: P@ssw0rd (zero)
- **Add a new pfSense interface that can be used for the DMZ.**
  - Name the interface DMZ.
  - Use a static IPv4 address of 172.16.1.1/16.
- **Add a firewall rule for the DMZ interface that allows all traffic from the DMZ.**
  - Use a description of Allow DMZ to any rule.
- **Configure and enable the DHCP server for the DMZ interface.**
  - Use a range of 172.16.1.100 to 172.16.1.200.”

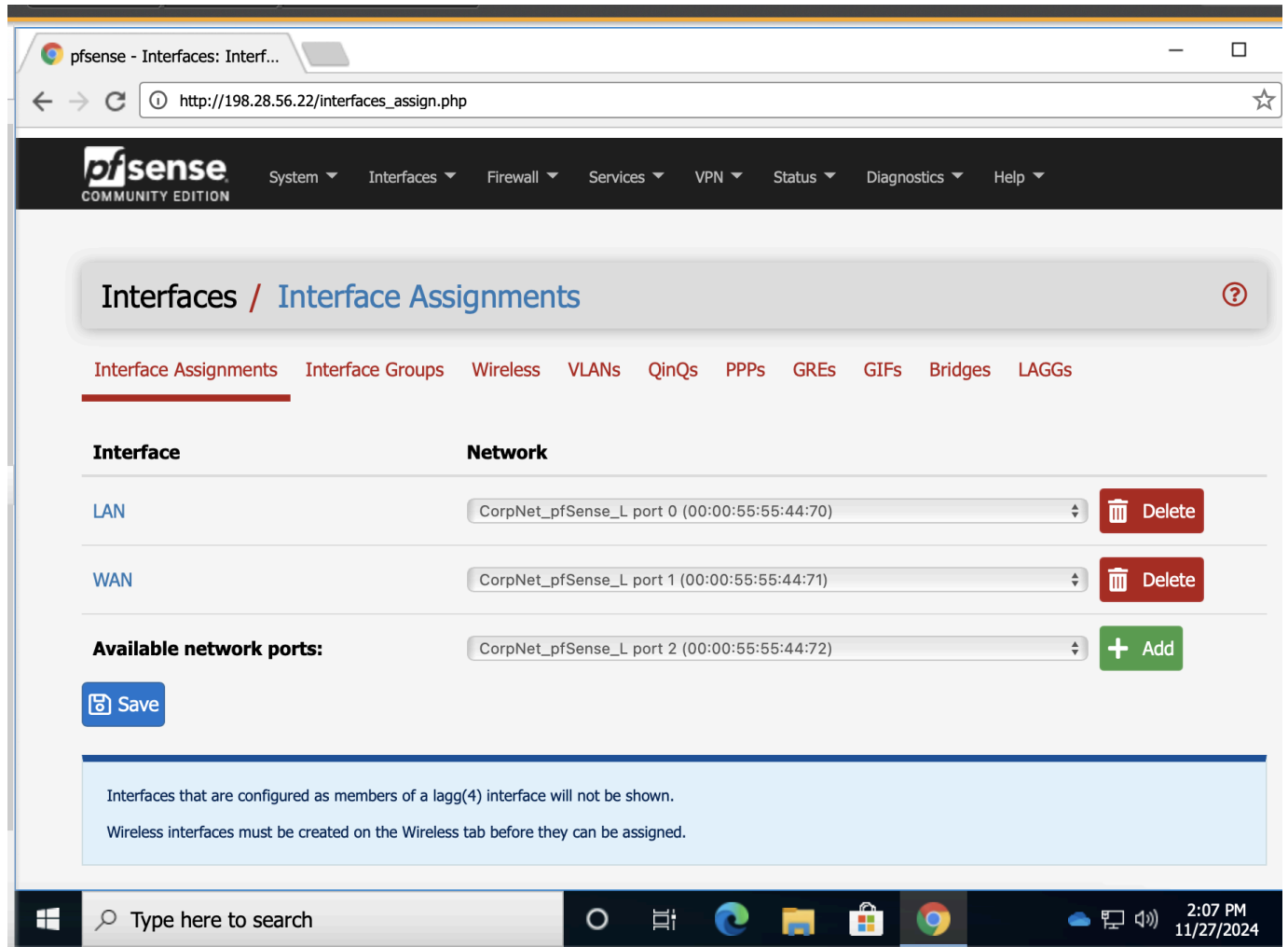
First , I'll navigate to the pfsense console and login with the credentials provided.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sun November 24th 2024



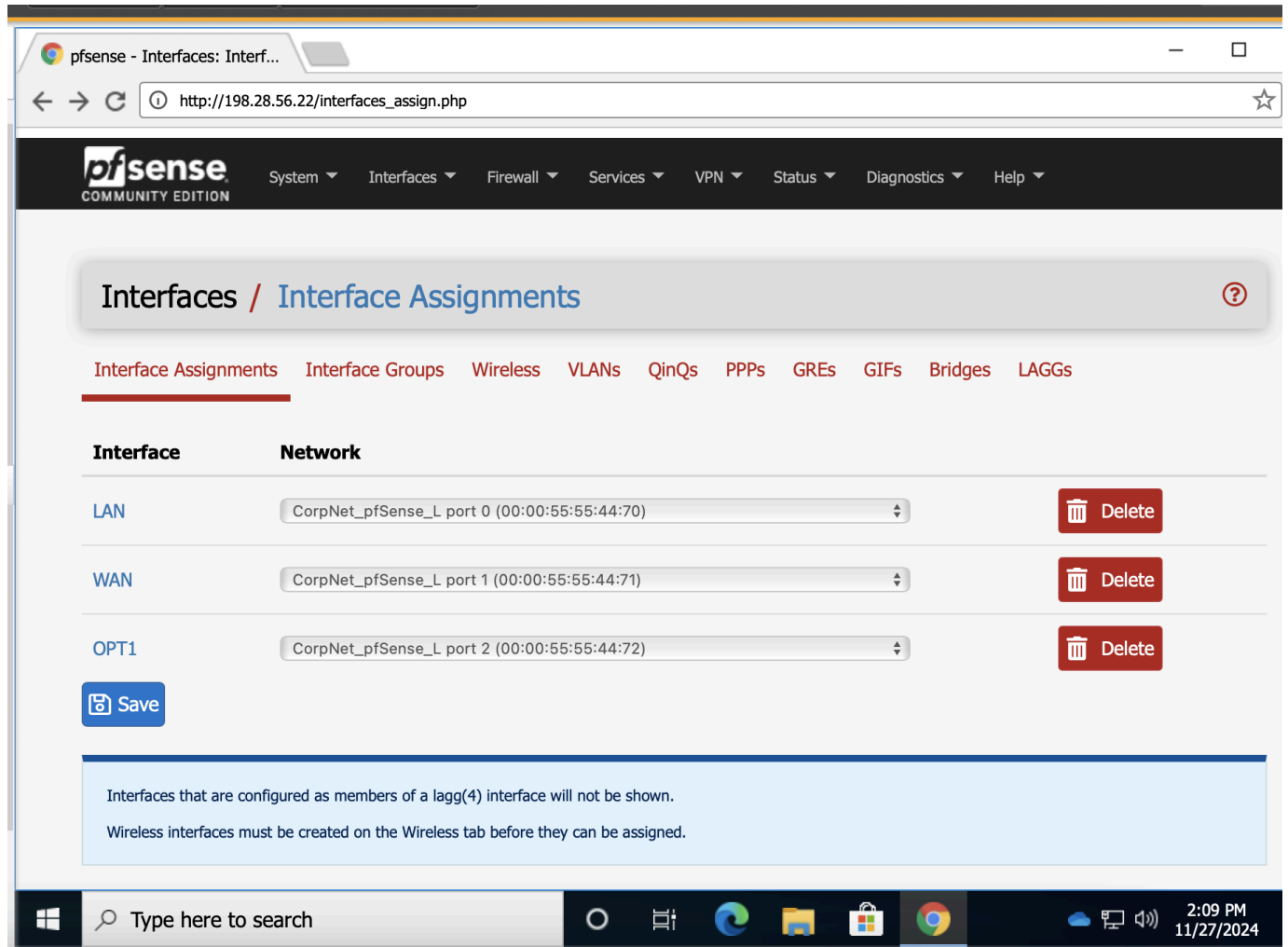
Our first task is to add a screened subnet. In order to do that, we'll need to create a new interface on the pfSense appliance that way we're able to route traffic to it. To add an interface I'll navigate to menu bar at the top of pfSense and go to **Interfaces > Assignments**.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sun November 24th 2024



From here, I'll click the Add button. A new interface called **OPT1** appears. To edit the properties and rename it, we'll need to click the **OPT1** interface to bring up the configuration settings for it.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sun November 24th 2024



Since we would like this to be a static IP address I will select from the **IPv4 Configuration Type** drop-down menu the **"Static IPv4"** option.

pfSense - Interfaces: OPT1 ...

http://198.28.56.22/interfaces.php?if=opt1

### General Configuration

**Enable** ☐ Enable interface

**Description**

Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**

This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

**MTU**

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

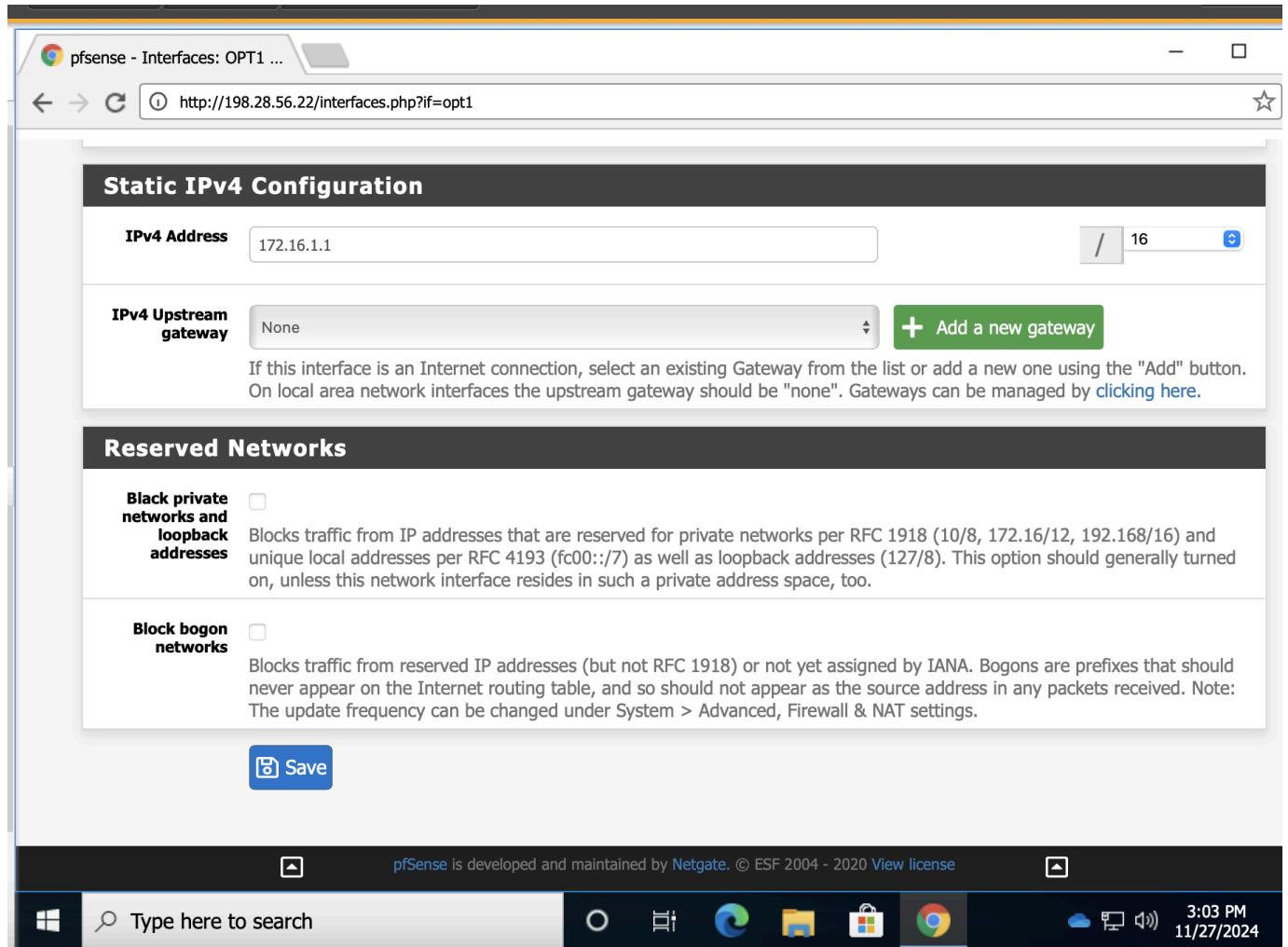
**MSS**

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

**Speed and Duplex**

Note that I've also renamed the interface to "**DMZ**" as requested from the lab instructions. We will also need to set the IP address and subnet mask for it. The lab would like us to use **172.16.1.1/16**. Note that the "/16" is **CIDR Notation** for the subnet mask, where 16 represents the number of bits that indicate the network portion. In this case since each IP address is 32 bits long we know that the first 2 octets indicate that this machine is part of the **172.16.x.x subnet**.

**Be sure to hit the save button after making the changes!**



Now we can move on to create the firewall rules. We need to allow all traffic from the DMZ interface. To configure this we'll go to the pfSense menu bar at the top and navigate to **Firewall > Rules**.

The screenshot shows the pfSense web interface in a browser window. The address bar shows the URL `http://198.28.56.22/firewall_rules.php`. The page title is "Firewall: Rules: WAN". The breadcrumb navigation shows "Firewall / Rules / WAN". The interface has a dark header with the pfSense logo and navigation menus for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the header, there's a sub-header "Firewall / Rules / WAN" with icons for list, chart, and help. A tab bar shows "Floating", "LAN", "WAN" (selected), "DMZ", and "OpenVPN". The main content area is titled "Rules (Drag to Change Order)" and contains a table with two rules. Both rules are disabled (indicated by a red 'X' and a gear icon), have "0 / 0 B" states, "IPv4" protocol, and "Block private networks" description. The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. Below the table are buttons for "Add", "Add", "Delete", "Save", and "Separator". A yellow warning box at the bottom states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." The footer of the browser window shows the Windows taskbar with the search bar and several application icons, and the system clock shows 3:07 PM on 11/27/2024.

Firewall: Rules: WAN

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / WAN

Floating LAN **WAN** DMZ OpenVPN

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	*		Block private networks	

Add Add Delete Save Separator

No rules are currently defined for this interface  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

Type here to search

3:07 PM 11/27/2024

Click the add button and open the rule to set the configuration. We will pass LAN traffic through the DMZ and apply our rules on the DMZ interface. I will select the LAN from the breadcrumb menu and copy the rules from the LAN.

**Edit Firewall Rule**

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule

**Interface** DMZ  
Choose the interface from which packets must come to match this rule

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** Any  
Choose which IP protocol this rule should match.

**Source**

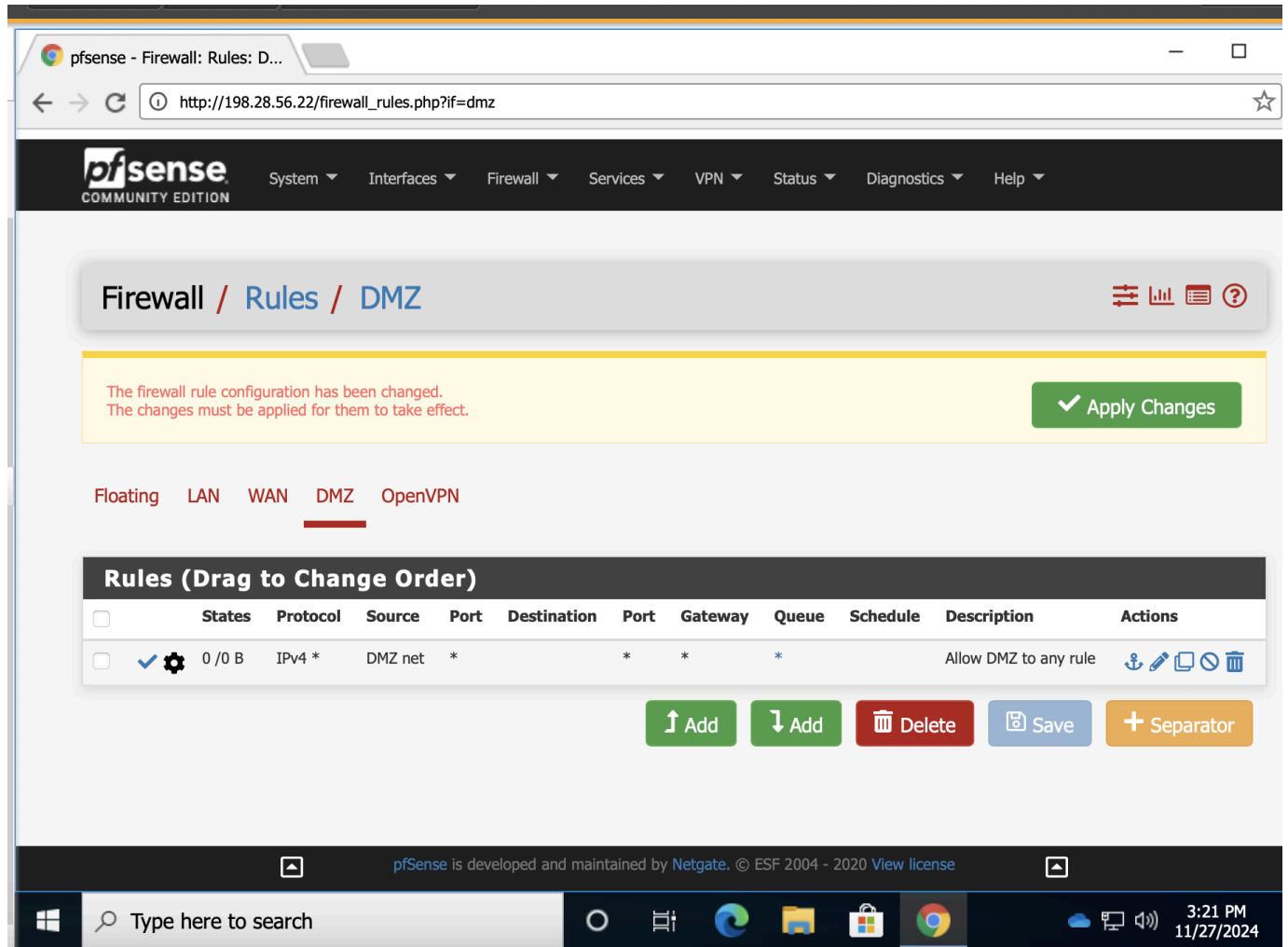
**Source** ☐ Invert match LAN net Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

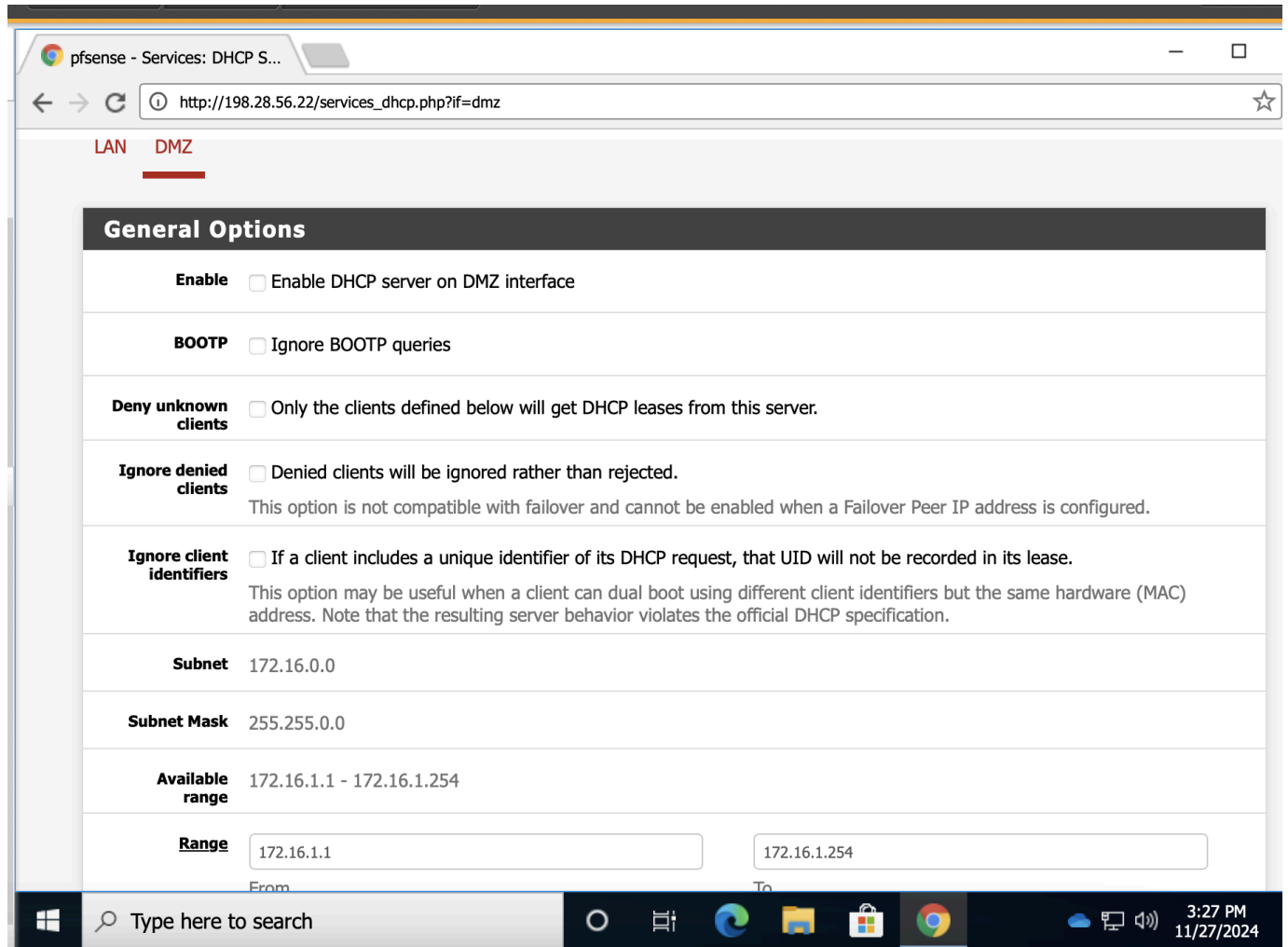
After setting all the configuration settings and hitting the “SAVE” button I can see that a new rule has appeared in the DMZ interface breadcrumb menu:





Awesome! With that configured we can move on to the last part of the lab which is the configure our DHCP server with a reserved range. When devices connect to the DMZ subnet we want our DHCP server to hand out leases for the IP range of **172.16.1.100 to 172.16.1.200**. This will make managing the DMZ easier because we'll know that if a device has an IP in that range , we know that the DHCP server handed out that IP.

To get to the DHCP configuration settings navigate from the top pfSense menu to **Services > DHCP Server**.

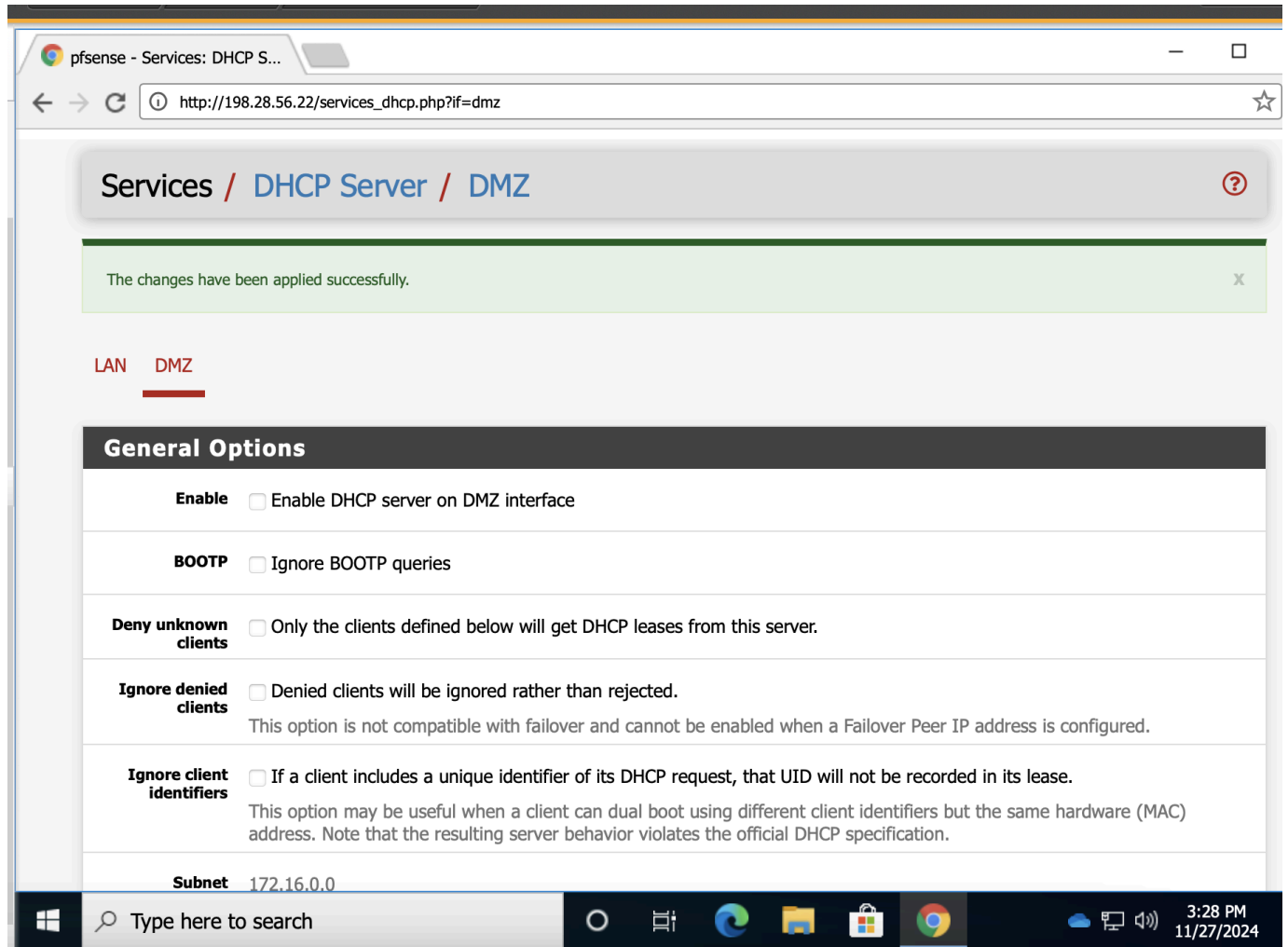


See the default range ? Let's change that!

The screenshot shows a web browser window with the address bar displaying `http://198.28.56.22/services_dhcp.php?if=dmz`. The page title is "pfsense - Services: DHCP S...". The interface has two tabs: "LAN" and "DMZ", with "DMZ" being the active tab. Below the tabs is a "General Options" section with several configuration options:

- Enable**: ☐ Enable DHCP server on DMZ interface
- BOOTP**: ☐ Ignore BOOTP queries
- Deny unknown clients**: ☐ Only the clients defined below will get DHCP leases from this server.
- Ignore denied clients**: ☐ Denied clients will be ignored rather than rejected.  
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore client identifiers**: ☐ If a client includes a unique identifier of its DHCP request, that UID will not be recorded in its lease.  
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
- Subnet**: 172.16.0.0
- Subnet Mask**: 255.255.0.0
- Available range**: 172.16.1.1 - 172.16.1.254
- Range**: Two input fields are shown. The first field contains "172.16.1.100" and the second field contains "172.16.1.200".

The bottom of the image shows a Windows taskbar with the search bar, task view button, and several application icons (Edge, File Explorer, Store, Chrome). The system clock in the bottom right corner shows "3:28 PM 11/27/2024".



After hitting save we are now finished! This now concludes this lab!

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sun November 24th 2024

The screenshot shows a web browser window with a 'Lab Report' modal open. The modal displays the following information:

- Lab Report**
- Time Spent: 02:57
- Score: 3/3 (100%)
- TASK SUMMARY
- Required Actions
  - ✓ Configure an interface for the DMZ [Show Details](#)
  - ✓ Add a firewall rule to the DMZ interface
  - ✓ Configure pfSense's DHCP server for the DMZ interface [Show Details](#)

The background shows the 'TestOut' learning platform interface with a scenario titled 'pfSense - Services: DHCP S...'. The scenario text describes the task: 'protect your company, you want to place this server and other devices in a demilitarized zone (DMZ). This DMZ and server need to be protected by the pfSense Security Gateway Appliance (pfSense). Since a few of the other devices in the DMZ require an IP address, you have also decided to enable DHCP on the DMZ network. In this lab, your task is to perform the following:'

- Access the pfSense management console:
  - Username: admin
  - Password: P@ssw0rd (zero)
- Add a new pfSense interface that can be used for the DMZ.
  - Name the interface DMZ.
  - Use a static IPv4 address of 172.16.1.1/16.
- Add a firewall rule for the DMZ interface that allows all traffic from the DMZ.
  - Use a description of Allow DMZ to any rule.
- Configure and enable the DHCP server for the DMZ interface.
  - Use a range of 172.16.1.100 to 172.16.1.200.

The browser window also shows a 'Score Lab' button and a 'Network Security - Configuring a DMZ / Screened Subnet on a Secu...' tab. The Windows taskbar at the bottom shows the time as 3:36 PM on 11/27/2024.