

Lab 5.2.7: Configuring a pfSense Security Appliance

From TestOut CompTIA Security+ Course

In this lab I will be setting up and configuring a pfSense security appliance within a hypothetical organization.

The scenario for this lab is as follows:

“You are an IT security administrator for a small corporate network. To increase security for the corporate network, you have installed the pfSense network security appliance in your network. Now you need to configure the device.

In this lab, your task is to configure pfSense as follows:

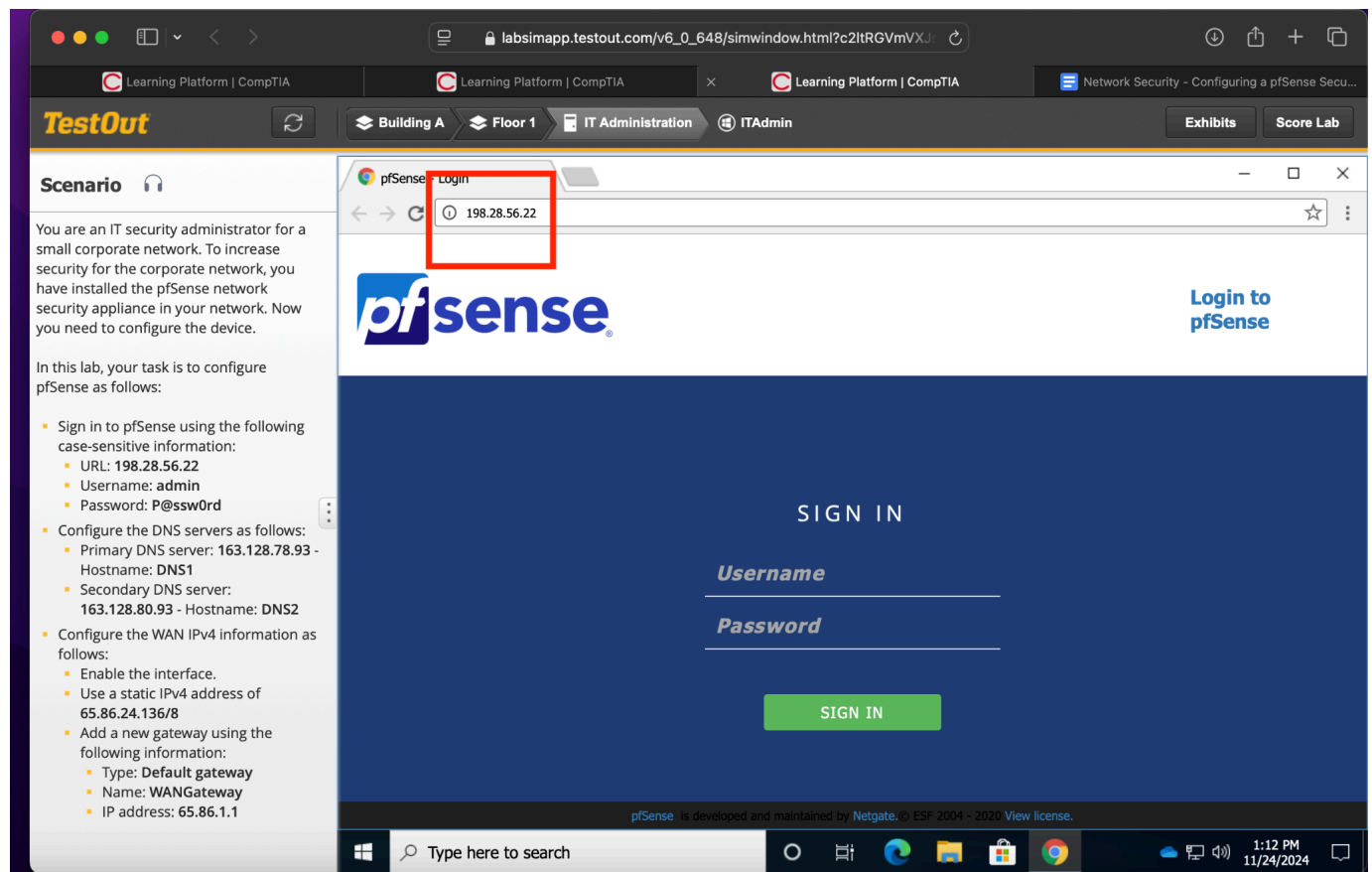
1. Sign in to pfSense using the following case-sensitive information:
 - a. URL: 198.28.56.22
 - b. Username: admin
 - c. Password: P@ssw0rd
2. Configure the DNS servers as follows:
 - a. Primary DNS server: 163.128.78.93 - Hostname: DNS1
 - b. Secondary DNS server: 163.128.80.93 - Hostname: DNS2
3. Configure the WAN IPv4 information as follows:
 - a. Enable the interface.
 - b. Use a static IPv4 address of 65.86.24.136/8
 - c. Add a new gateway using the following information:
 - i. Type: Default gateway
 - ii. Name: WANGateway
 - iii. IP address: 65.86.1.1 “

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

Based off what I've learned so far about pfSense, I know that you must access the GUI through http. We'll fire up a web browser and navigate to the IP address of our pfSense Security Appliance. I see that in the Windows 10 machine the lab gives us, Google Chrome is installed. Also, in the lab scenario the IP address for the pfSense appliance is 198.28.56.22.

(Note to self: It looks like a Private IP address on first glance but remember that Class C Private IP address range is 192.168.0.0 to 192.168.255.255)

In my web browser I'll type 198.28.56.22 and then login with the credentials provided.



Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

The screenshot shows the pfSense Status Dashboard in a web browser. The browser's address bar shows the URL 198.28.56.22. The pfSense header includes the logo and navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Status / Dashboard' and features two primary sections: 'System Information' and 'Netgate Services And Support'.

System Information

Name	pfSense.localdomain
User	admin@198.28.56.22 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: b7af12f074cedc817e9d
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Thu Apr 28 2016
Version	2.4.5-RELEASE (amd64) built on Tue Mar 24 15:25:50 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHZ AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled

Netgate Services And Support

Contract Type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class., worldwide

The Windows taskbar at the bottom shows the search bar, task view button, and several application icons including Edge, File Explorer, and Chrome. The system clock indicates 1:13 PM on 11/24/2024.

Now that I'm logged into the Administrator account we can proceed to configure our DNS servers setting them to the corresponding hostnames and IPs. I'll navigate to System > General Setup > DNS Server settings.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

The screenshot shows the pfSense web interface. The browser address bar indicates the URL is 198.28.56.22. The pfSense logo and 'COMMUNITY EDITION' are visible. The 'System' menu is expanded, showing various configuration options. The 'System Information' table provides details about the system, including the version (2.4.5-RELEASE) and hardware specifications. The 'Netgate Services And Support' section highlights the 'Community Support' contract type and provides links to resources.

System Information	
Name	
User	
System	f074cedc817e9d
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Thu Apr 28 2016
Version	2.4.5-RELEASE (amd64) built on Tue Mar 24 15:25:50 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHZ AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled

Netgate Services And Support

Contract Type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide

After clicking that and scrolling down the page a bit more, I see the DNS server setting field. I'll go ahead and enter **DNS1** as the hostname and **163.128.78.93** as the IP address. This will be our primary DNS server. After , I'll click "add" and set the secondary DNS server as **163.128.80.93** with a hostname of **DNS2**.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

Do not use '.local' as the final part of the domain (TLD). The '.local' domain is widely used by mDNS (including Avahi and Apple OS X's Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the router uses '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

DNS Server Settings

DNS Servers			
163.128.78.93	DNS1	none	Delete
163.128.80	DNS2	none	Delete

Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

Hostname
Enter the DNS server Hostname for TLS Verification (optional).

Gateway
Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

Add DNS Server + Add DNS Server

DNS Server Override ☐ Allow DNS server list to be overridden by DHCP/PPP on WAN
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

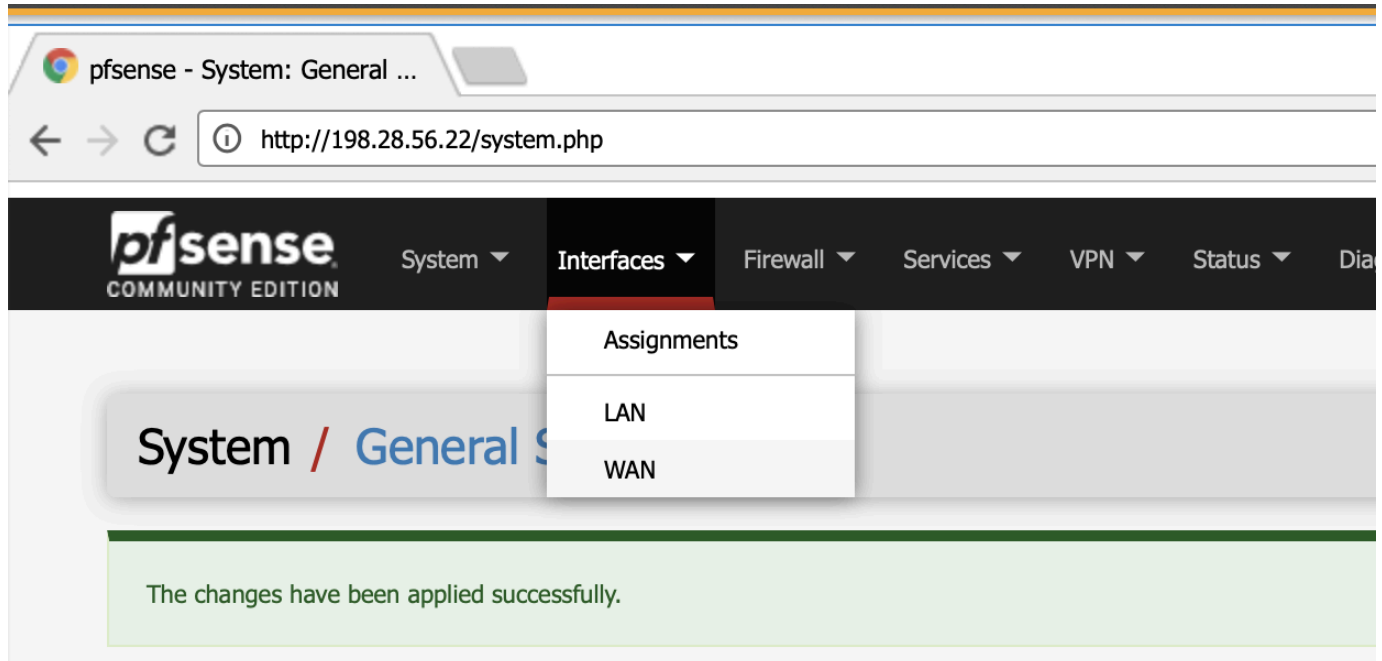
Everything looks good! To save our changes scroll to the bottom of the web page and click the blue “SAVE” button.

pfSense COMMUNITY EDITION

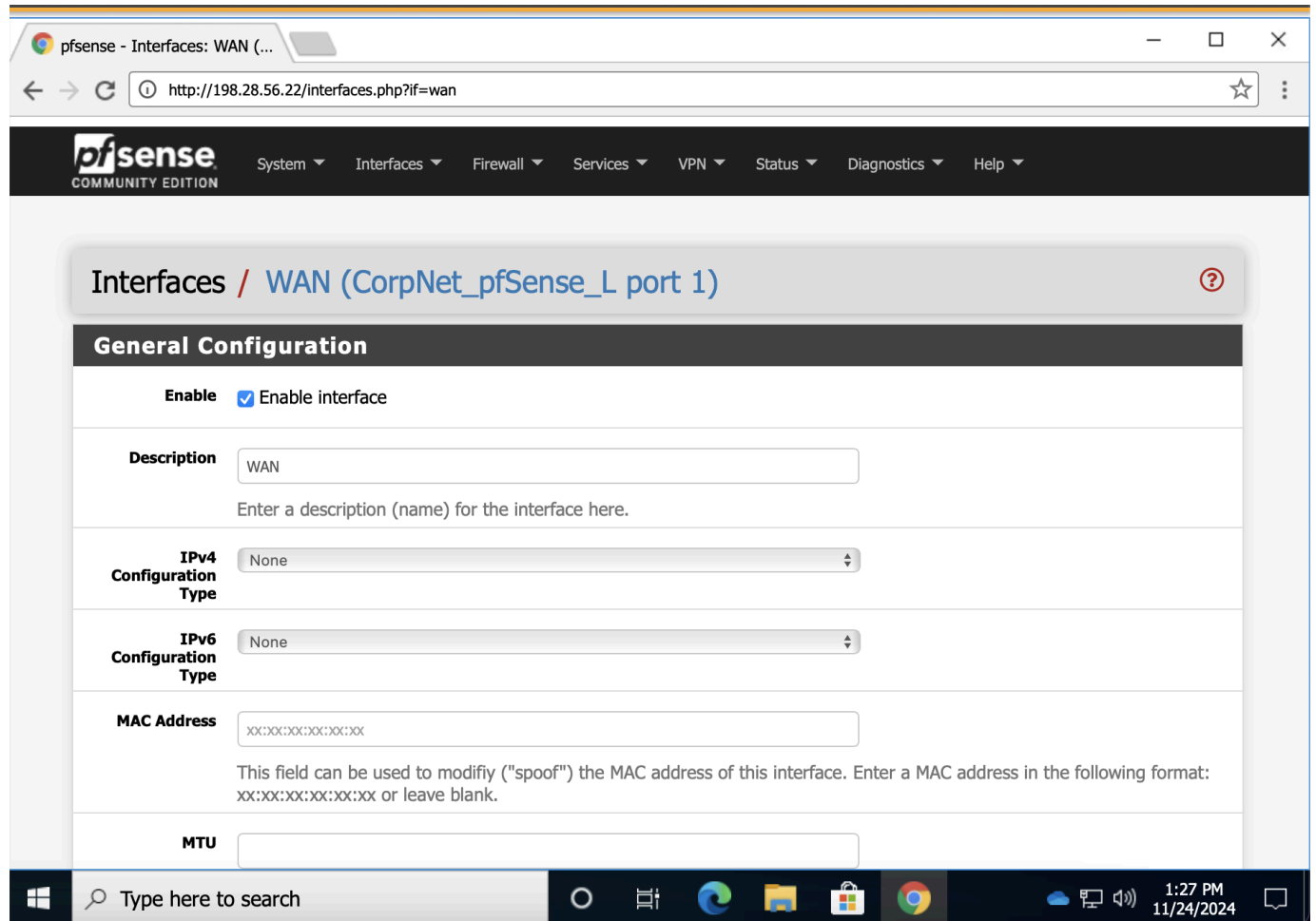
System / General Setup

The changes have been applied successfully.

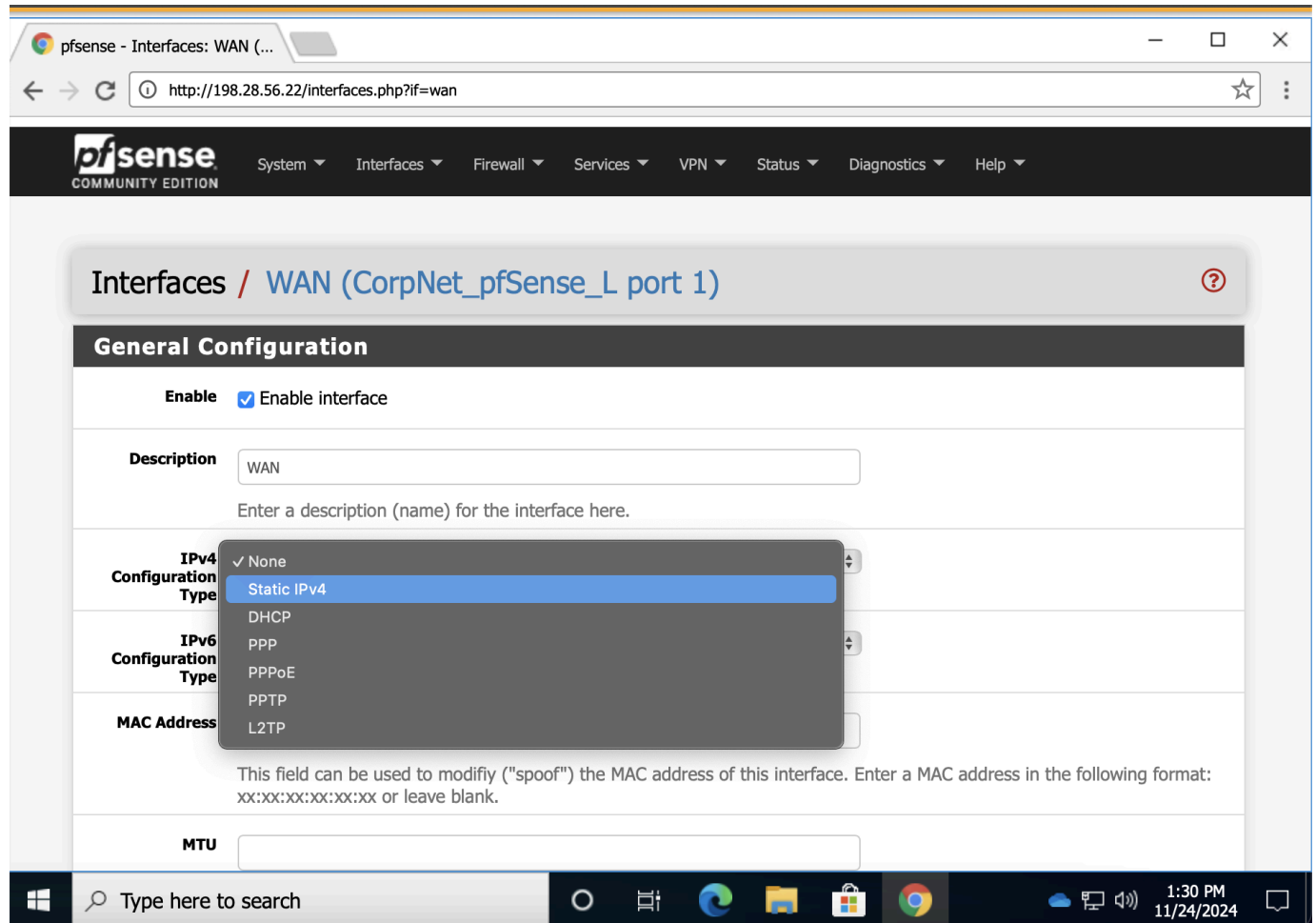
After I get the confirmation message shown above that the changes have been successfully applied. Now we can move on to the next part of the lab which is to configure our WAN. WAN is very important because it serves as a way to connect all the LANs together within the organization. We will want to set it to be static that way DHCP doesn't hand out the IP address to another user on the network. Navigate to the menu bar at the top and go to **Interfaces > WAN**



Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

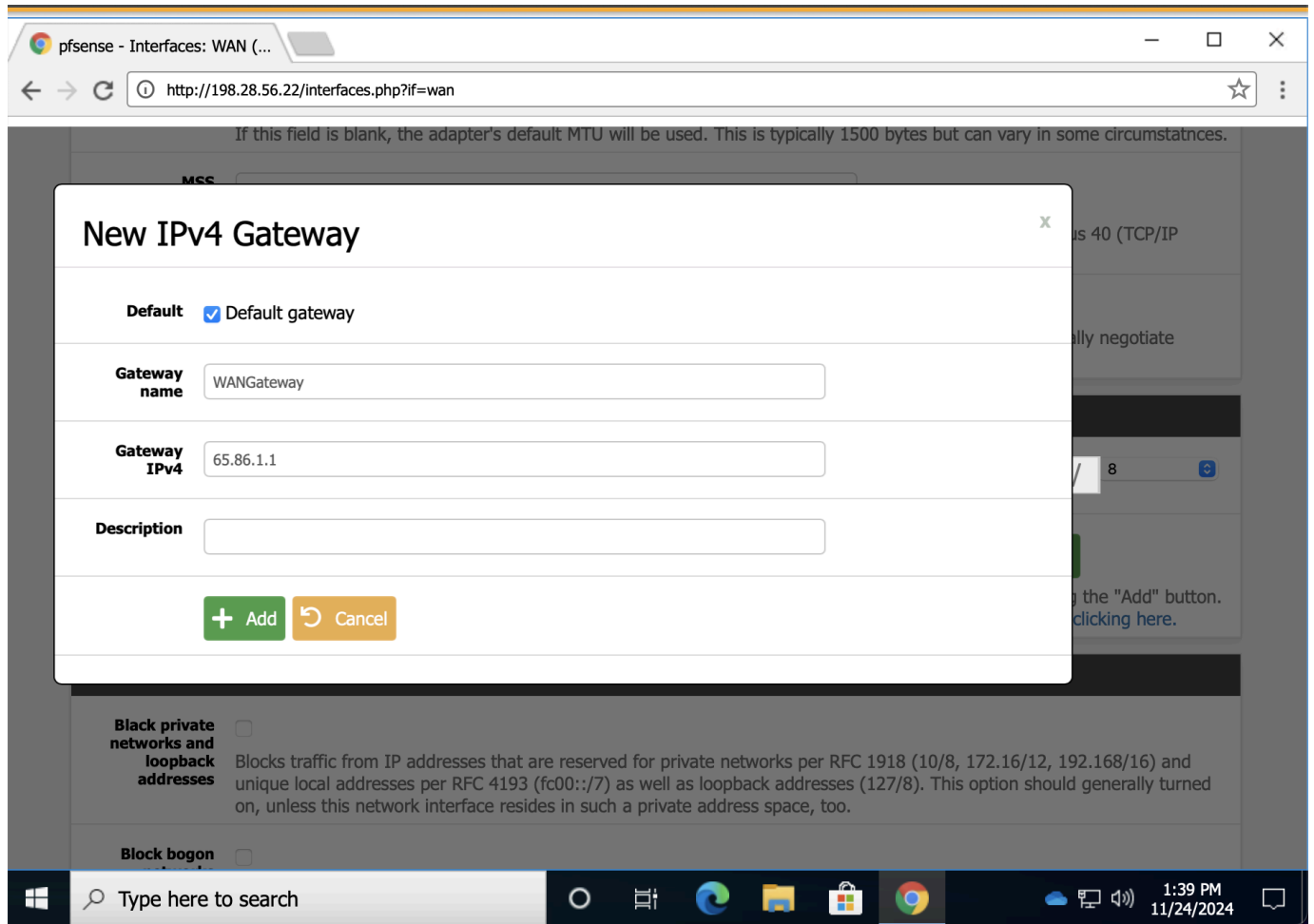


Now that we are in the WAN settings let's configure what we are asked to do in the lab. First, I see that “**Enable Interface**” is checked already. This means our WAN port is working and can communicate on the network. Next, we need to set a static **IPv4** address. On the dropdown menu we can see varying options like **DHCP** but that's not what we want in this case. Select the “**Static IPv4**” option.



Scroll down more on the page to get to the **Static IP Address** fields. Then, enter in the given IP address of **65.86.24.136/8**. Note that the **/8** is a **CIDR** notation for the subnet mask. This means that our IP address is **65.86.24.136** and our subnet mask is **255.0.0.0** because **/8** means that only the first 8 binary bits of the IPv4 are the network portion. After entering that, we need to add a gateway that way our users are still able to access the internet. We'll set the gateway by clicking "**Add a new gateway**" and entering the settings we are given.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Now that we've applied all the settings we hit the Save button then hit "Apply Changes."

This now concludes this lab!

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

The screenshot displays a web browser window with a 'Lab Report' modal open. The modal is titled 'Lab Report' and shows a score of 3/3 (100%) and a time spent of 36:55. Below the score is a 'TASK SUMMARY' section with 'Required Actions' listed as follows:

- ✓ Configure DNS servers [Show Details](#)
- ✓ Configure the WAN settings [Show Details](#)
- ✓ Add and configure a new gateway [Show Details](#)

The background shows the 'Scenario' page for the lab. It contains the following instructions:

You are an IT security administrator for a small corporate network. To increase security for the corporate network, you have installed the pfSense network security appliance in your network. Now you need to configure the device.

In this lab, your task is to configure pfSense as follows:

- Sign in to pfSense using the following case-sensitive information:
 - URL: 198.28.56.22
 - Username: admin
 - Password: P@ssw0rd
- Configure the DNS servers as follows:
 - Primary DNS server: 163.128.78.93 - Hostname: DNS1
 - Secondary DNS server: 163.128.80.93 - Hostname: DNS2
- Configure the WAN IPv4 information as follows:
 - Enable the interface.
 - Use a static IPv4 address of 65.86.24.136/8
 - Add a new gateway using the following information:
 - Type: Default gateway
 - Name: WANGateway
 - IP address: 65.86.1.1