Firewall and IDS Configuration with pfSense

By: Michael Emil Santos

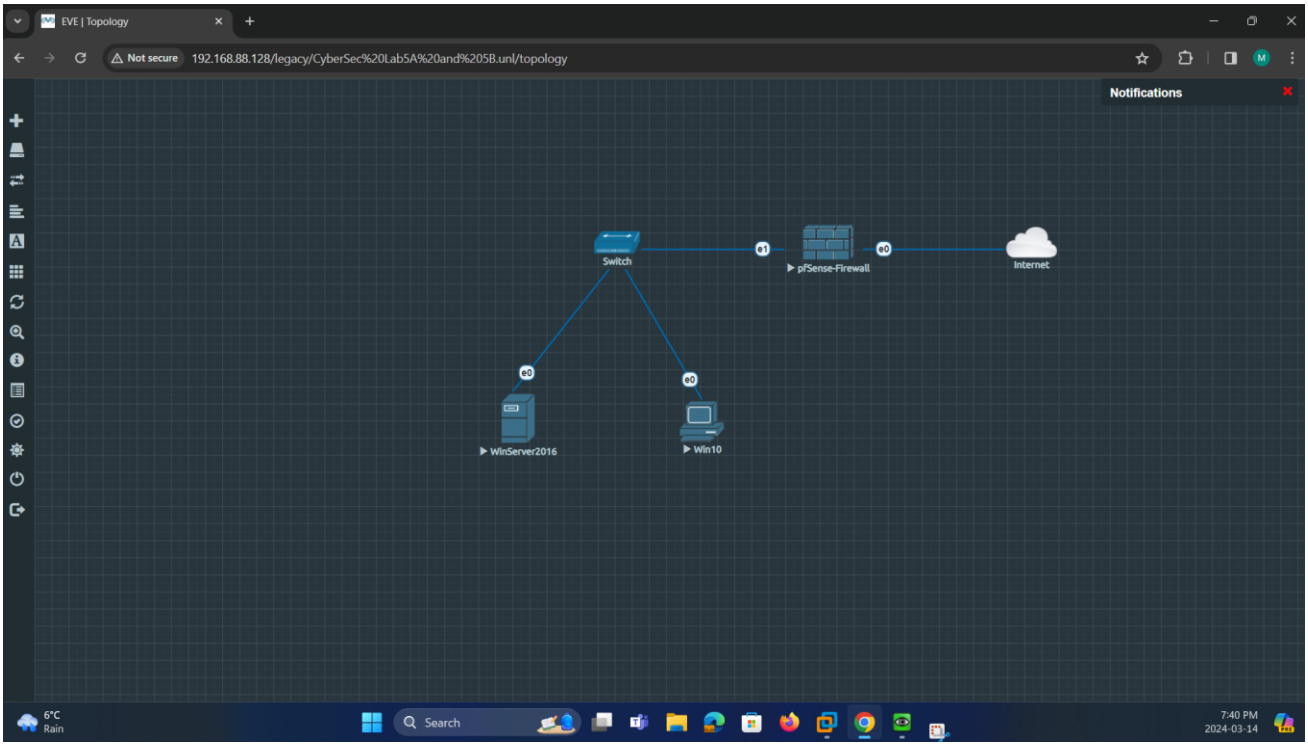
Introduction

This project involves setting up and configuring the pfSense firewall to secure a network environment. Using pfSense, I implemented firewall rules to block specific websites and deployed Snort as an Intrusion Detection System (IDS), adding a proactive layer of security. This hands-on experience in network protection highlights key skills in traffic management, content filtering, and intrusion detection.

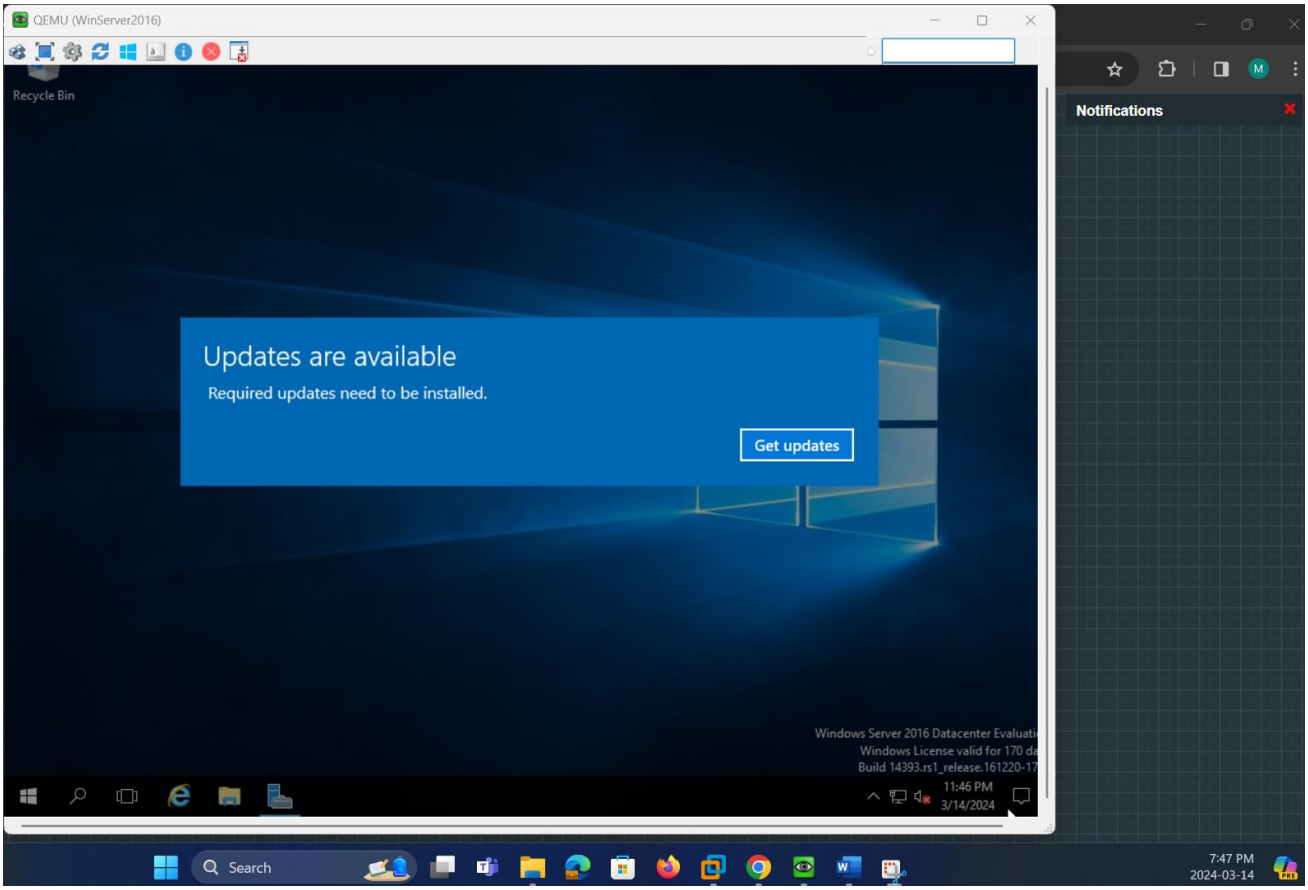
Pfsense is a free and open-source Unix-like operating system that powers existing servers, desktops, and embedded platforms. To create a dedicated firewall/router for a network, it is installed on a physical computer or a virtual machine. It can be upgraded and managed using a web-based interface, and managing it does not need understanding the underlying FreeBSD system.

Project Objectives and Setup

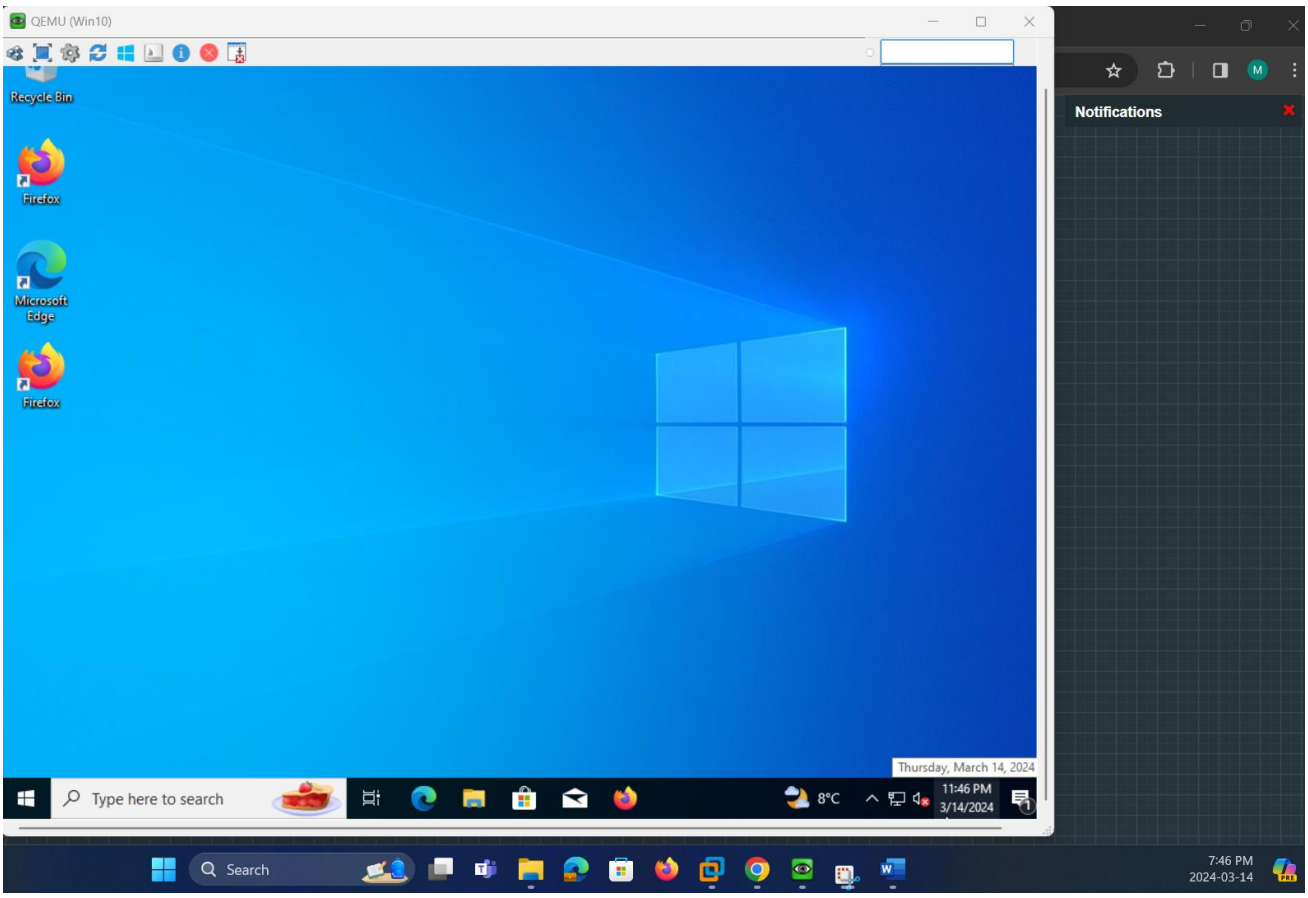
1. **pfSense Installation and Initial Setup**
    - **Objective**: Deploy pfSense on a virtual machine and configure the network for secure connectivity.
    - **Steps**: Installed pfSense in VirtualBox, set up WAN and LAN interfaces, and assigned IP addresses for the firewall, server, and workstation to create a controlled network environment.
2. **Firewall Rules for Content Filtering**
    - **Objective**: Restrict access to social media sites by creating firewall rules.
    - **Steps**: Configured pfSense to block domains (e.g., Facebook, Instagram) by setting up aliases and firewall rules on the LAN network, ensuring compliance with acceptable use policies.
3. **Snort IDS Installation and Configuration**
    - **Objective**: Enhance network security by deploying Snort to monitor for suspicious activities.
    - **Steps**: Installed Snort on pfSense, set up rule sets for intrusion detection, and monitored traffic for malicious patterns. This proactive approach provided an additional security layer, helping to detect potential threats.
4. **Lab Topology Requirements:** Creating the Topology of the Lab Environment composed of the following nodes:
    - WinServer 2016 (Active Directory and DNS)
    - Win 10 Client
    - Switch
    - PF Sense Firewall
    - Cloud (Internet)



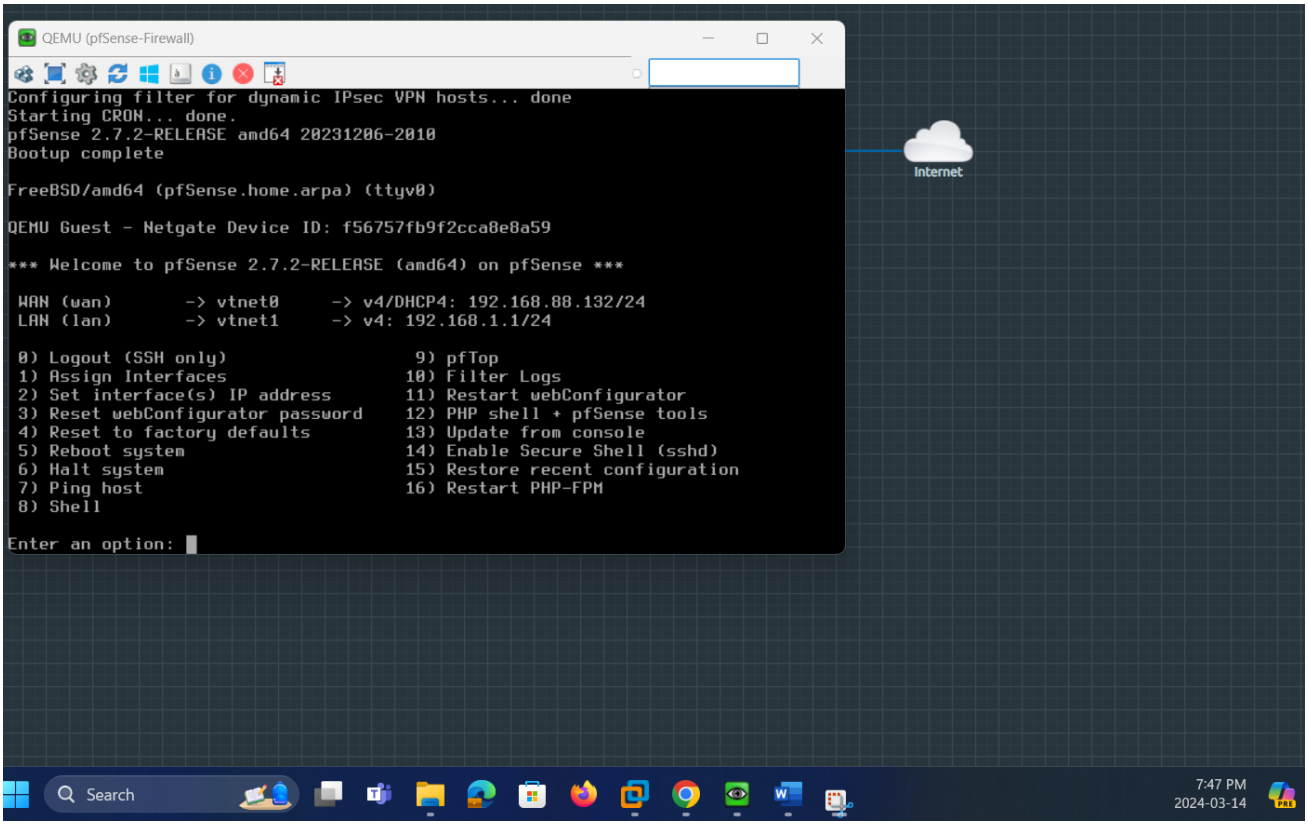
EVE-NG Lab Scenario Topology



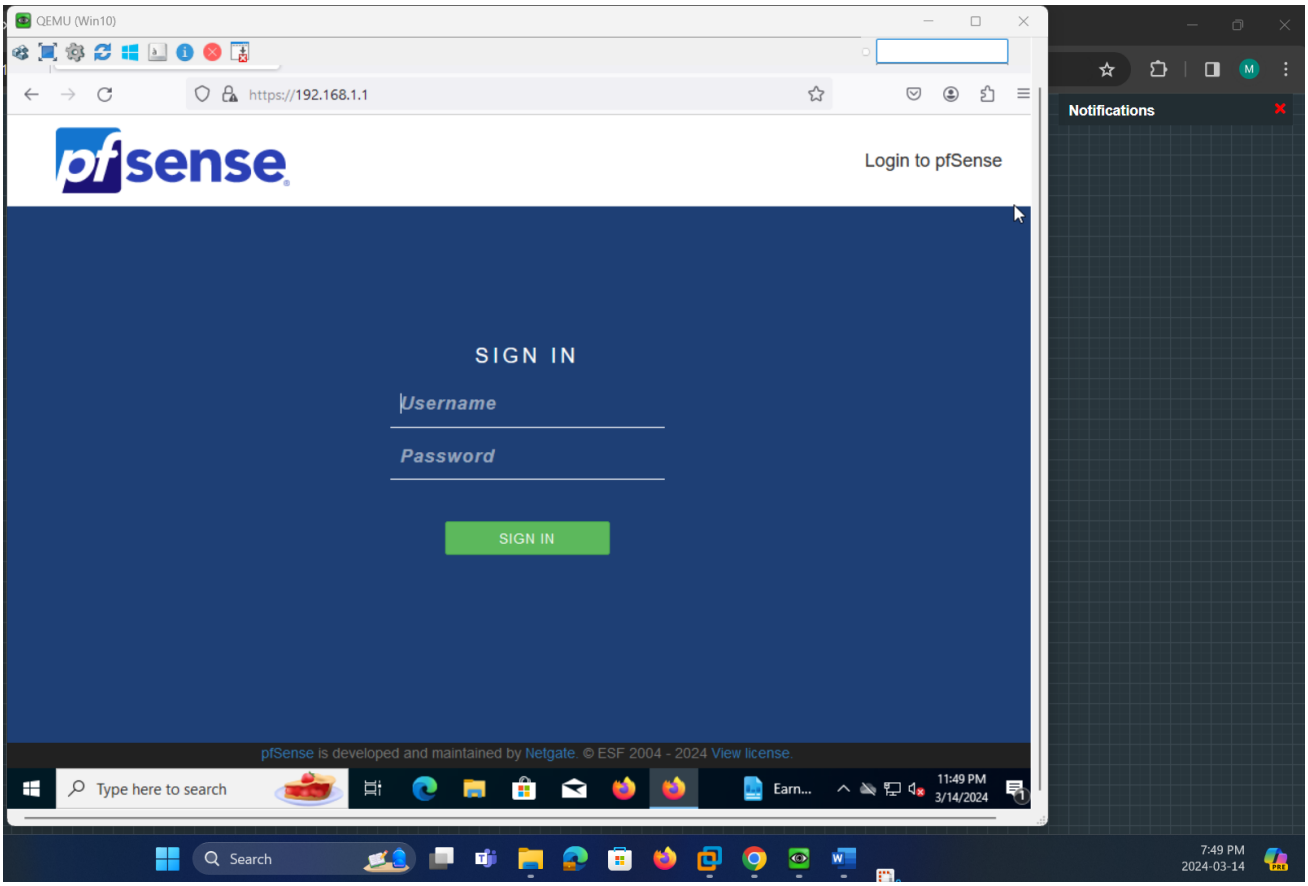
Win2016 Server

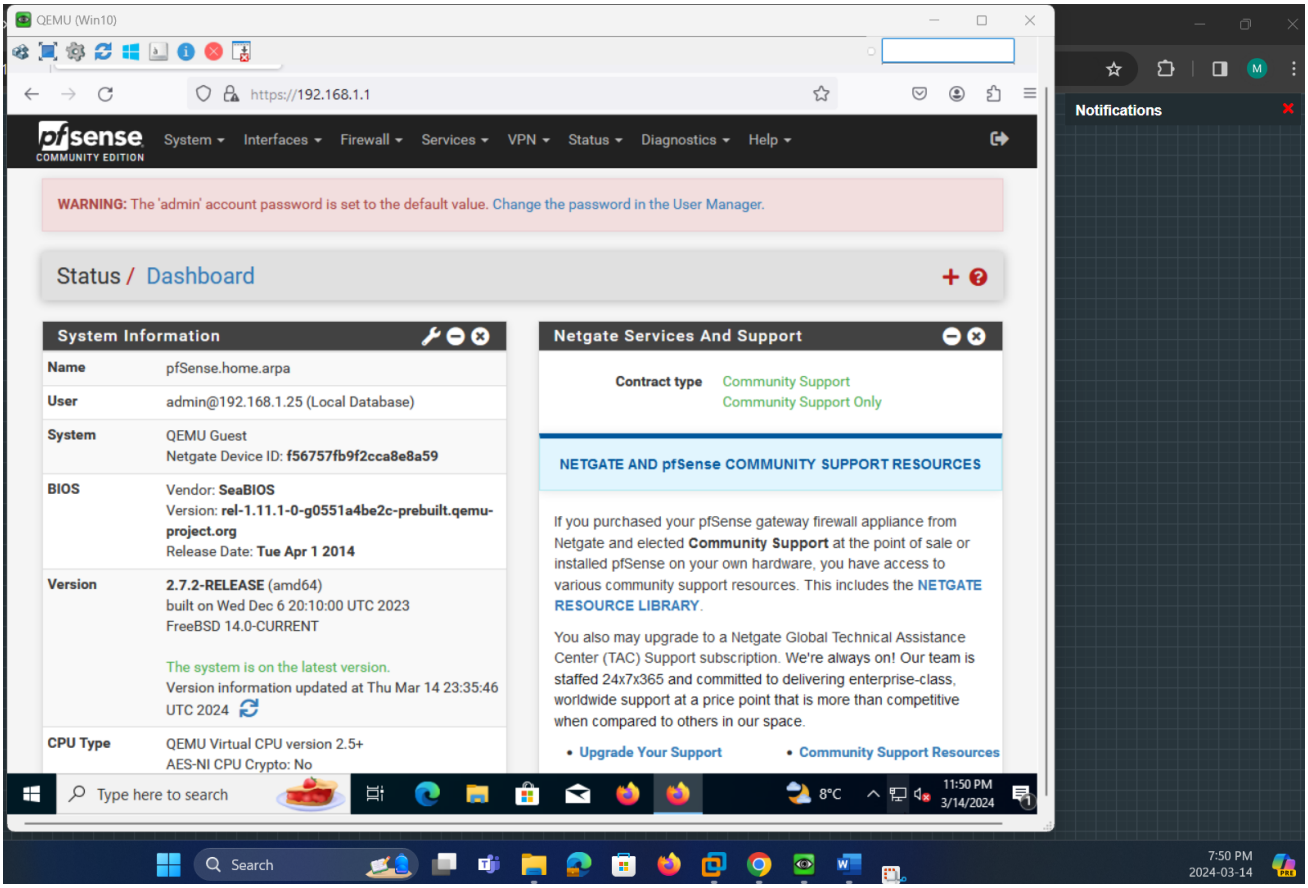


Win10 Client


QEMU (pfSense-Firewall)
Configuring filter for dynamic IPsec VPN hosts... done
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: f56757fb9f2cca8e8a59
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> vtnet0 -> v4/DHCP4: 192.168.88.132/24
LAN (lan) -> vtnet1 -> v4: 192.168.1.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:
Internet
Search
7:47 PM
2024-03-14

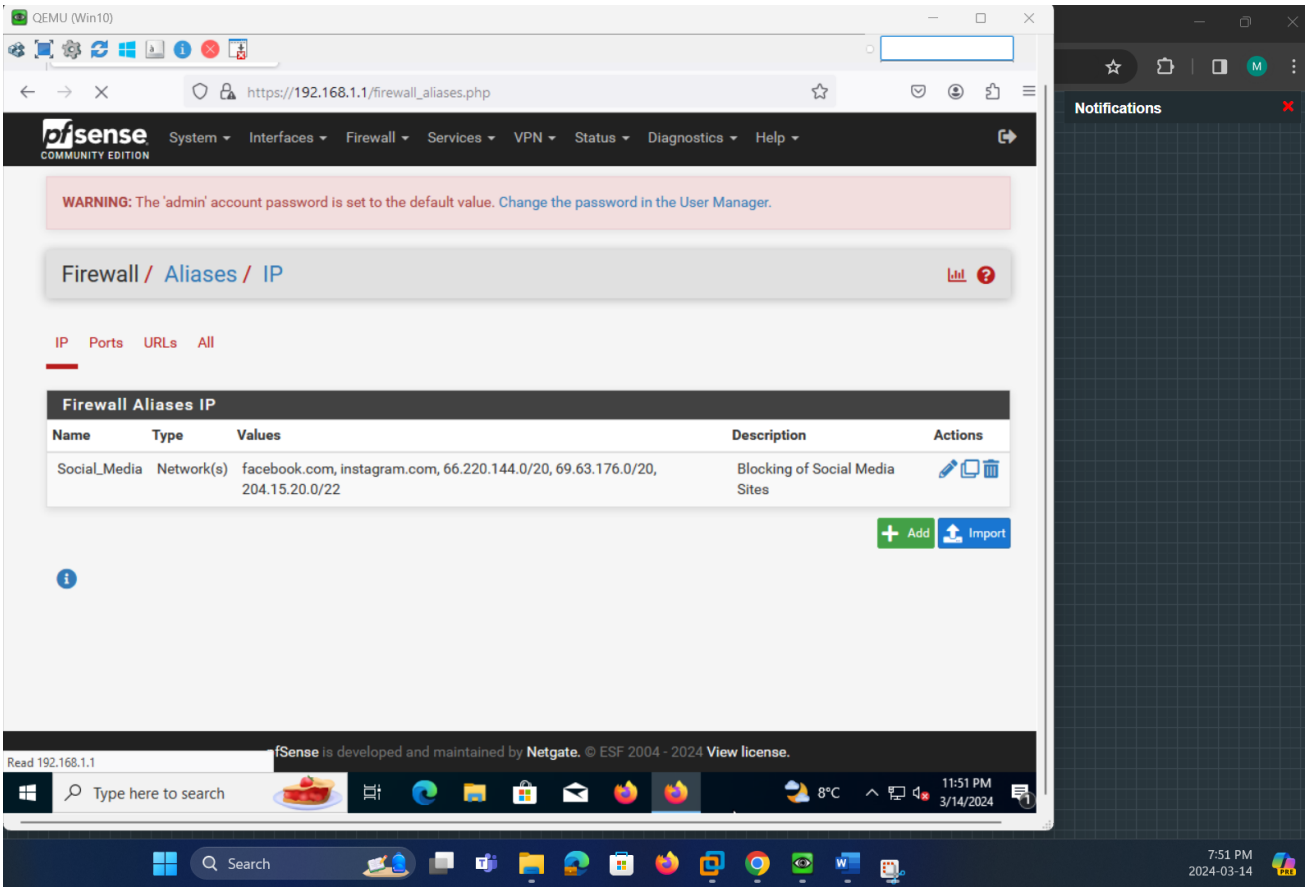
PF Sense CLI

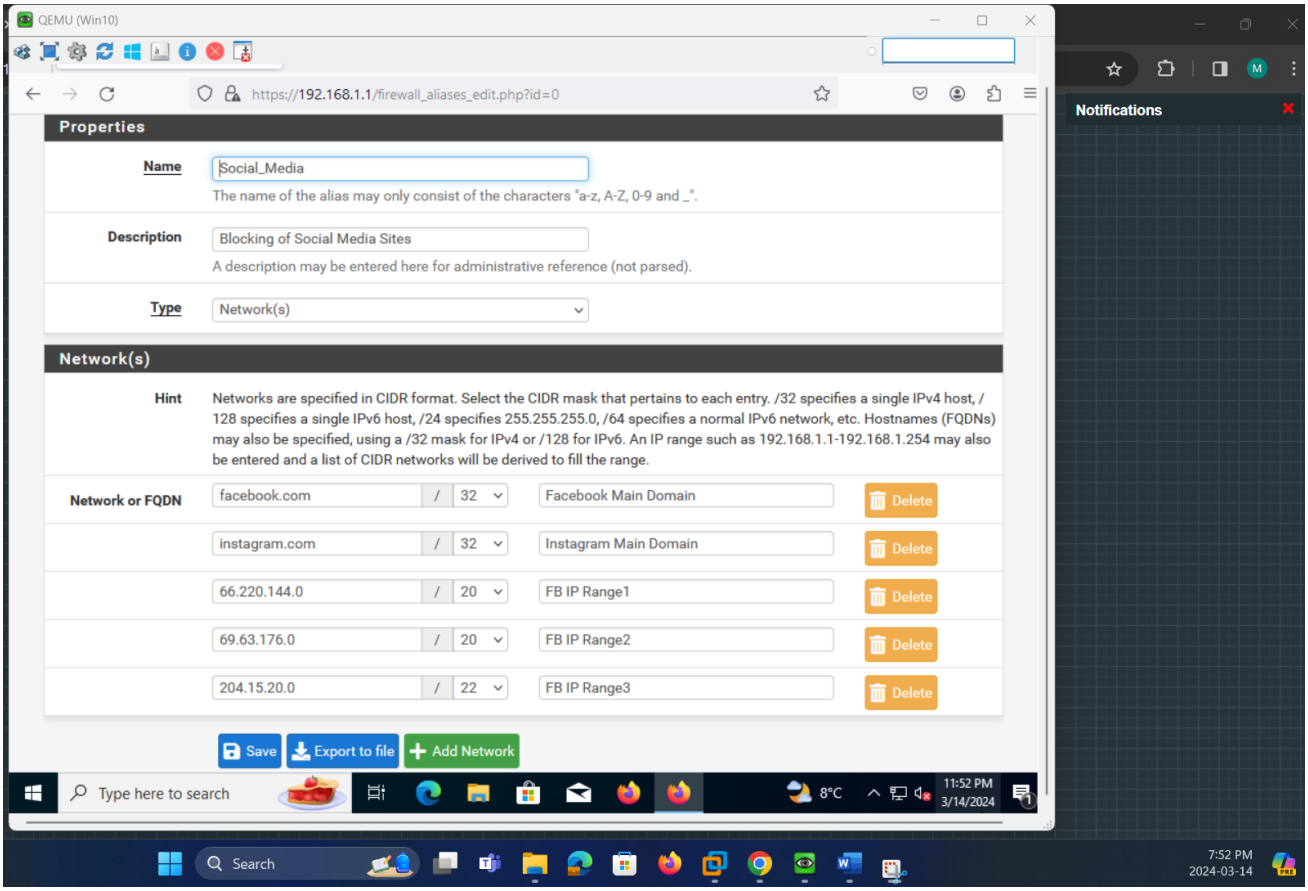

QEMU (Win10)
https://192.168.1.1
pfsense
Login to pfSense
SIGN IN
Username
Password
SIGN IN
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Type here to search
Earn...
11:49 PM
3/14/2024
Notifications
Search
7:49 PM
2024-03-14



PF Sense Web GUI

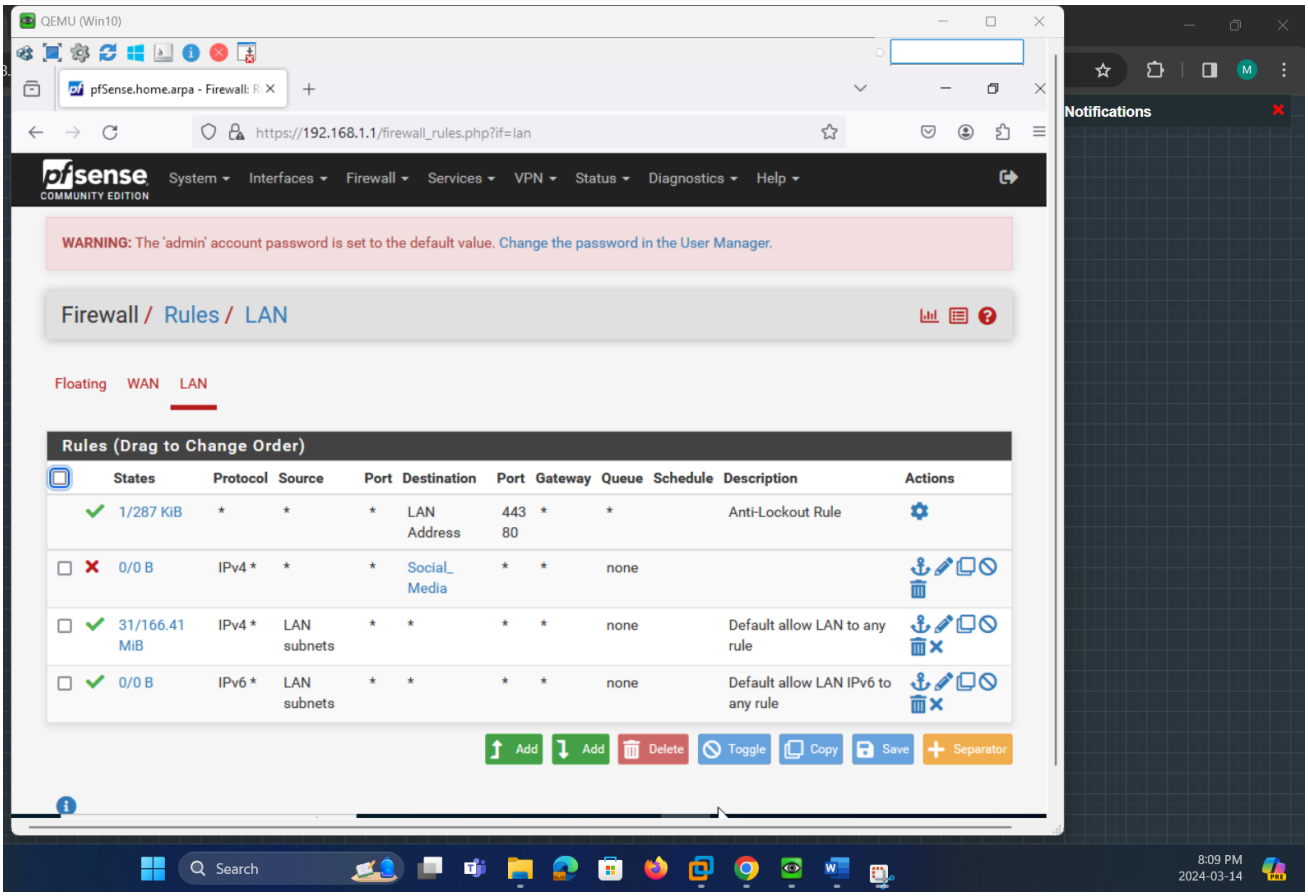
1. Defining Firewall Rules – Adding Alias for Group of Social Media Sites

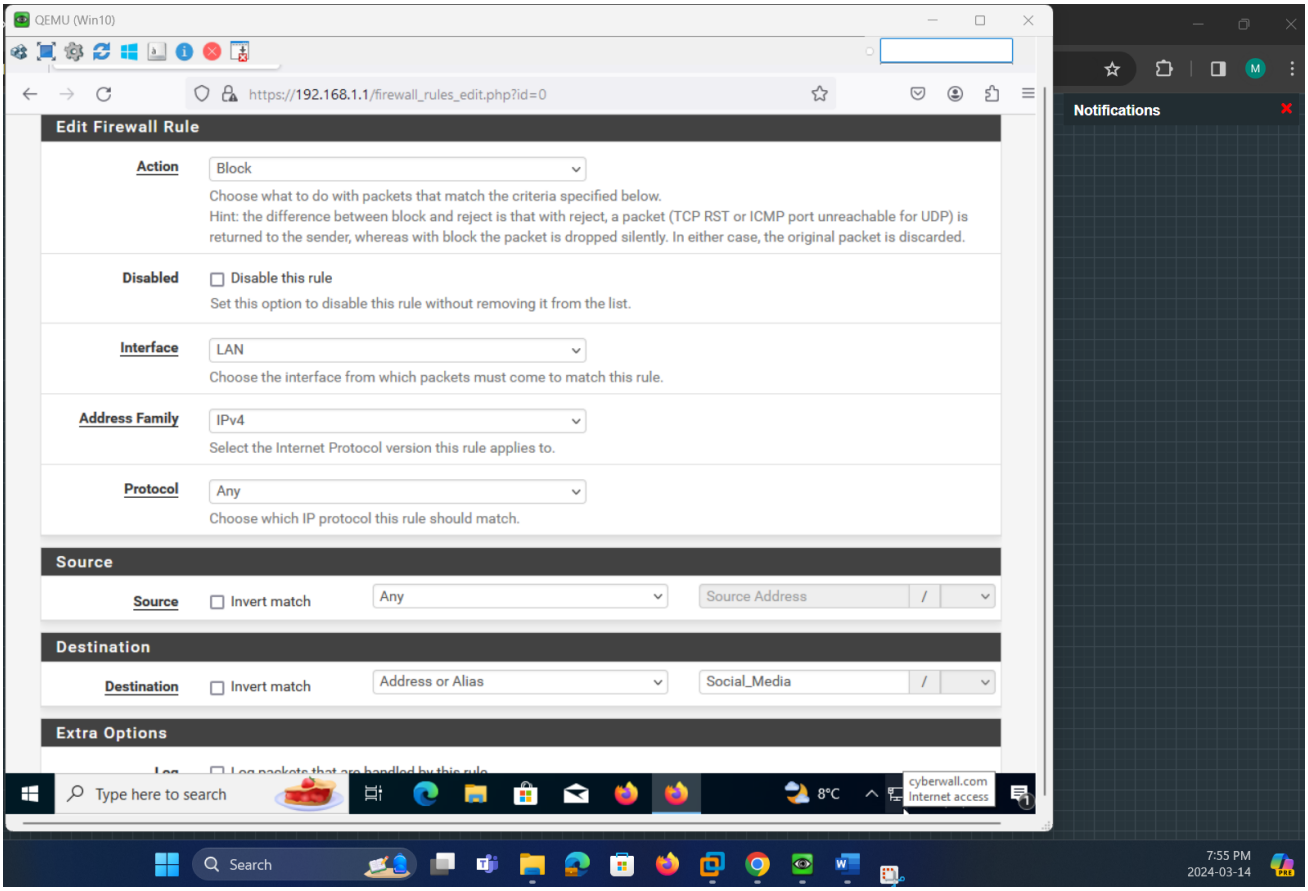

QEMU (Win10)
https://192.168.1.1/firewall_aliases.php
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Aliases / IP
IP Ports URLs All
Firewall Aliases IP
Name Type Values Description Actions
Social_Media Network(s) facebook.com, instagram.com, 66.220.144.0/20, 69.63.176.0/20, 204.15.20.0/22 Blocking of Social Media Sites
Add Import
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Read 192.168.1.1
Type here to search
8°C
11:51 PM
3/14/2024
Notifications
Search
7:51 PM
2024-03-14

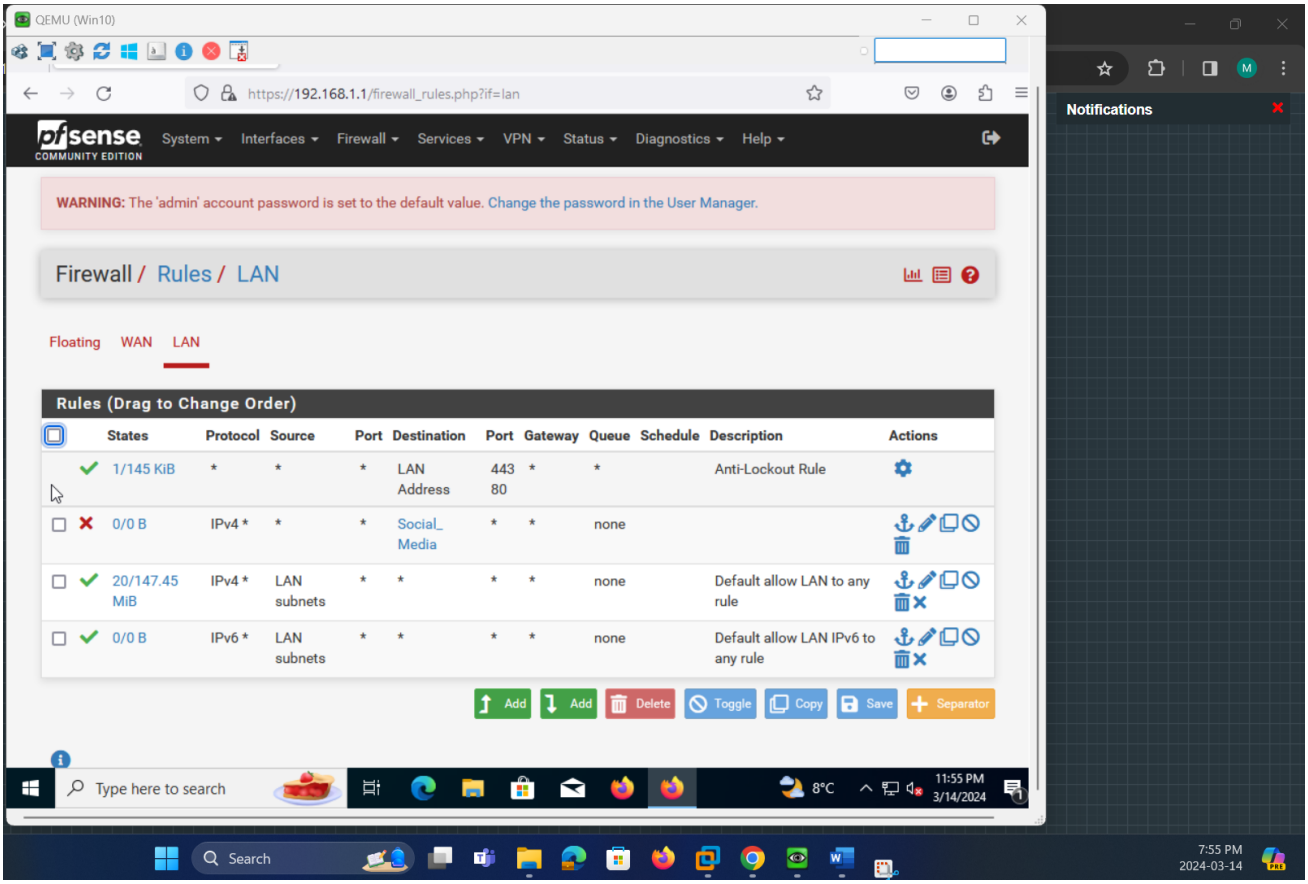


Added hostname/FQDN of facebook.com and Instagram.com, as well as IP ranges (CIDR network) of facebook.com.

2. Adding Firewall Rules for LAN Implementation Blocking

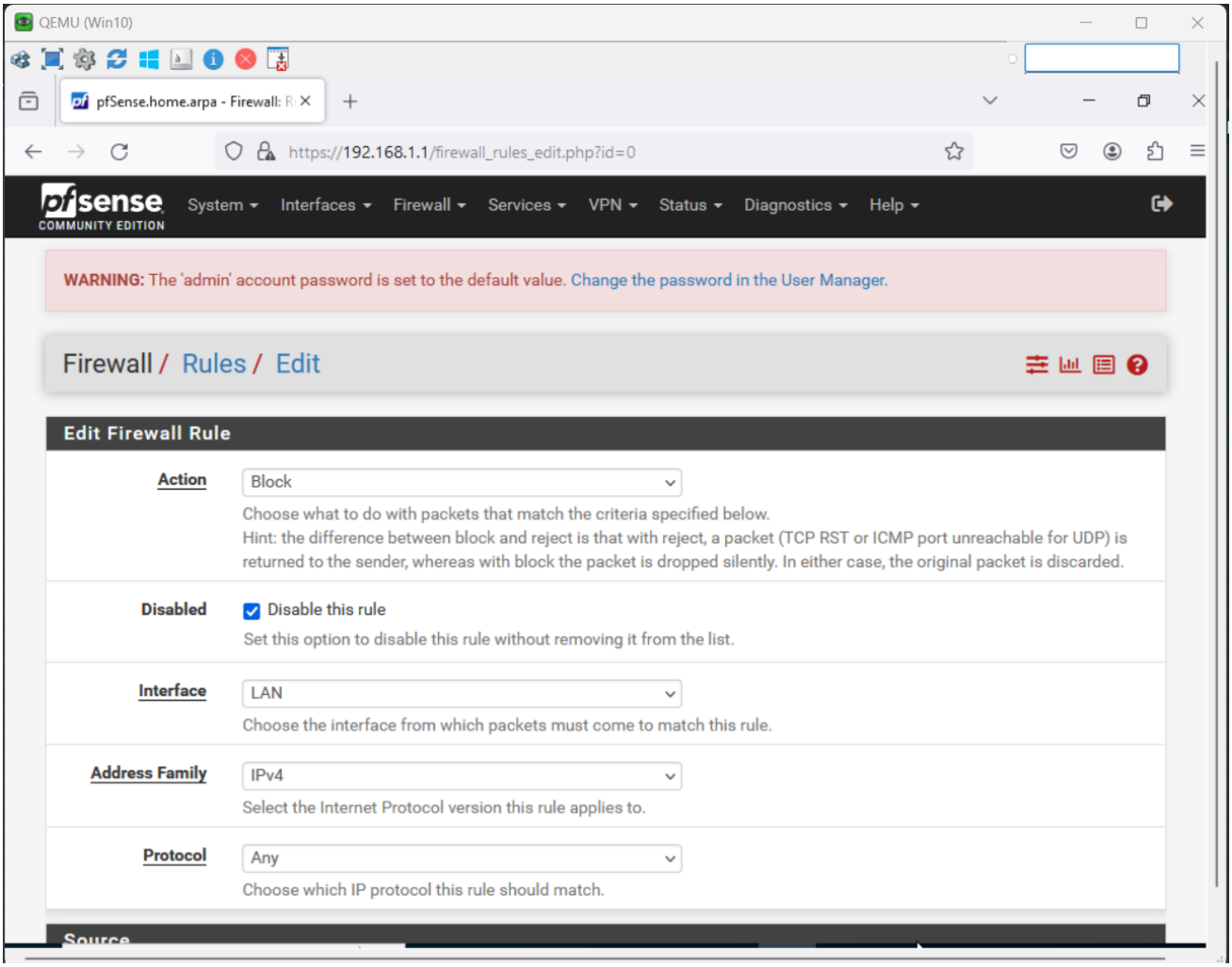

QEMU (Win10)
pfSense.home.arpa - Firewall: R
https://192.168.1.1/firewall_rules.php?if=lan
Notifications
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / LAN
Floating WAN LAN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
1/287 KiB * * * LAN Address 443 80 * * Anti-Lockout Rule
0/0 B IPv4 * * * * Social_ Media * * none
31/166.41 MiB IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
Add Add Delete Toggle Copy Save Separator
Search
8:09 PM
2024-03-14

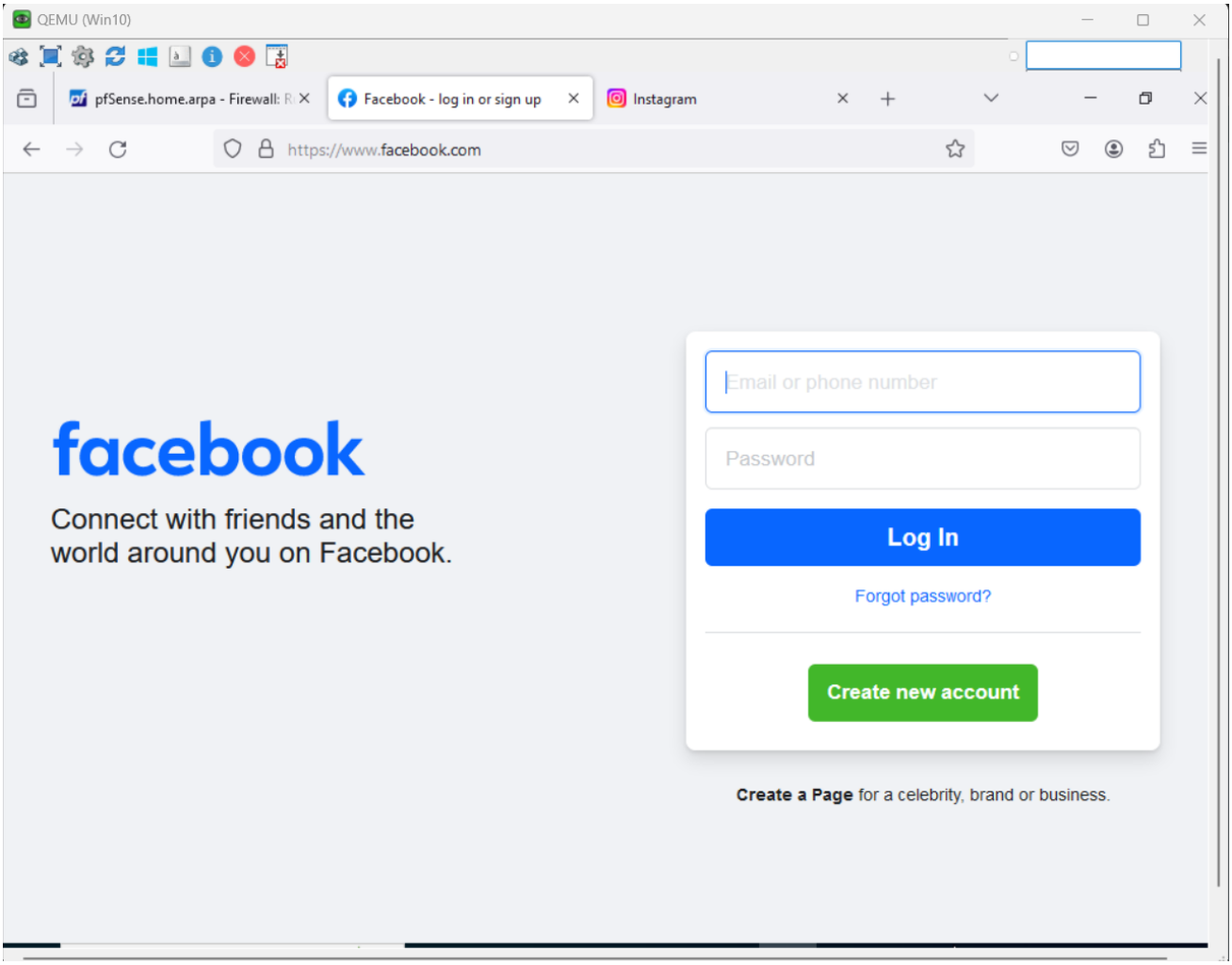

QEMU (Win10)
https://192.168.1.1/firewall_rules_edit.php?id=0
Edit Firewall Rule
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
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
Any
Source Address
Destination
Destination
Invert match
Address or Alias
Social_Media
Extra Options
Type here to search
8°C
cyberwall.com
Internet access
Notifications
Search
7:55 PM
2024-03-14

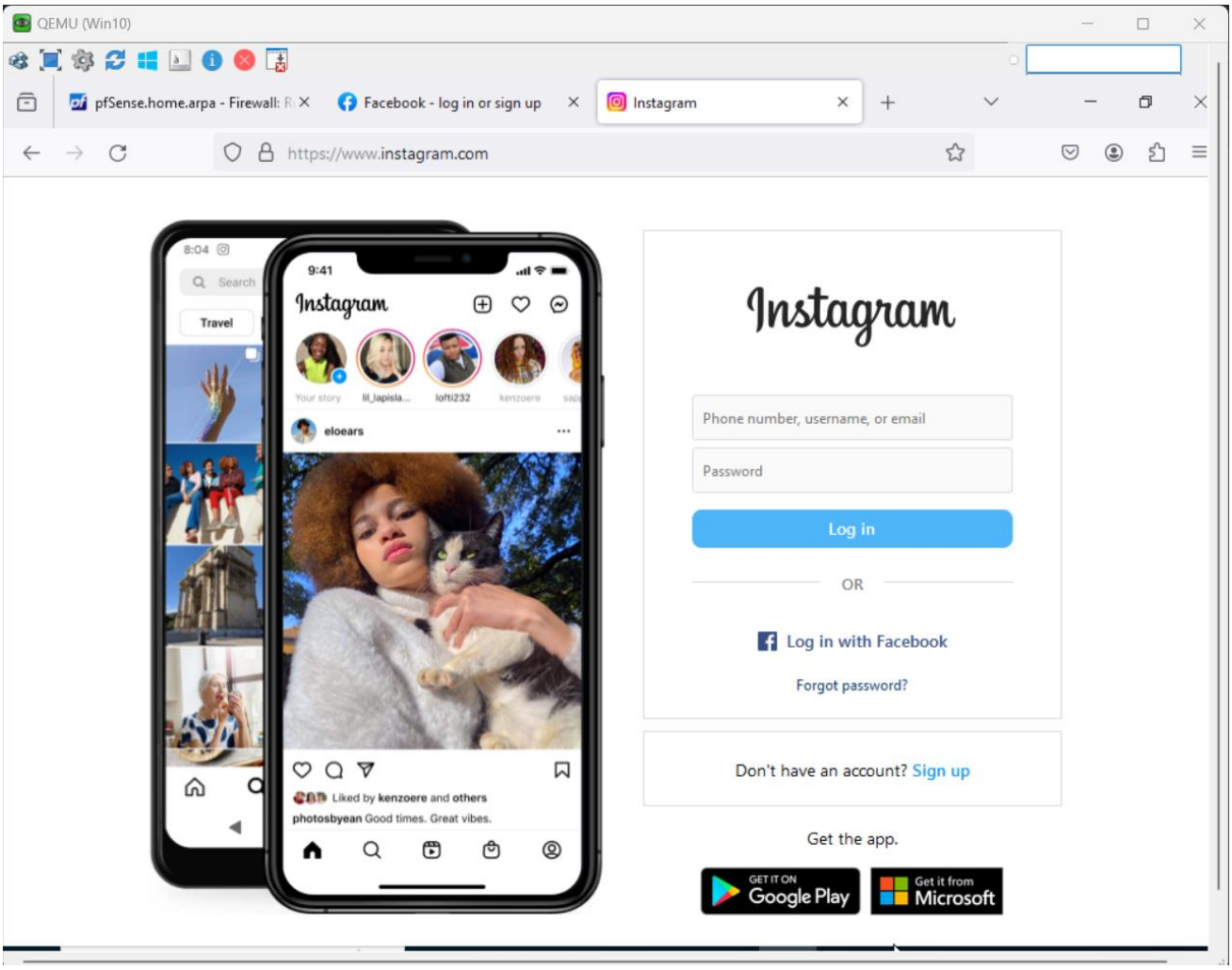


3. Testing the Firewall Rules – Blocking Social Media Blocking

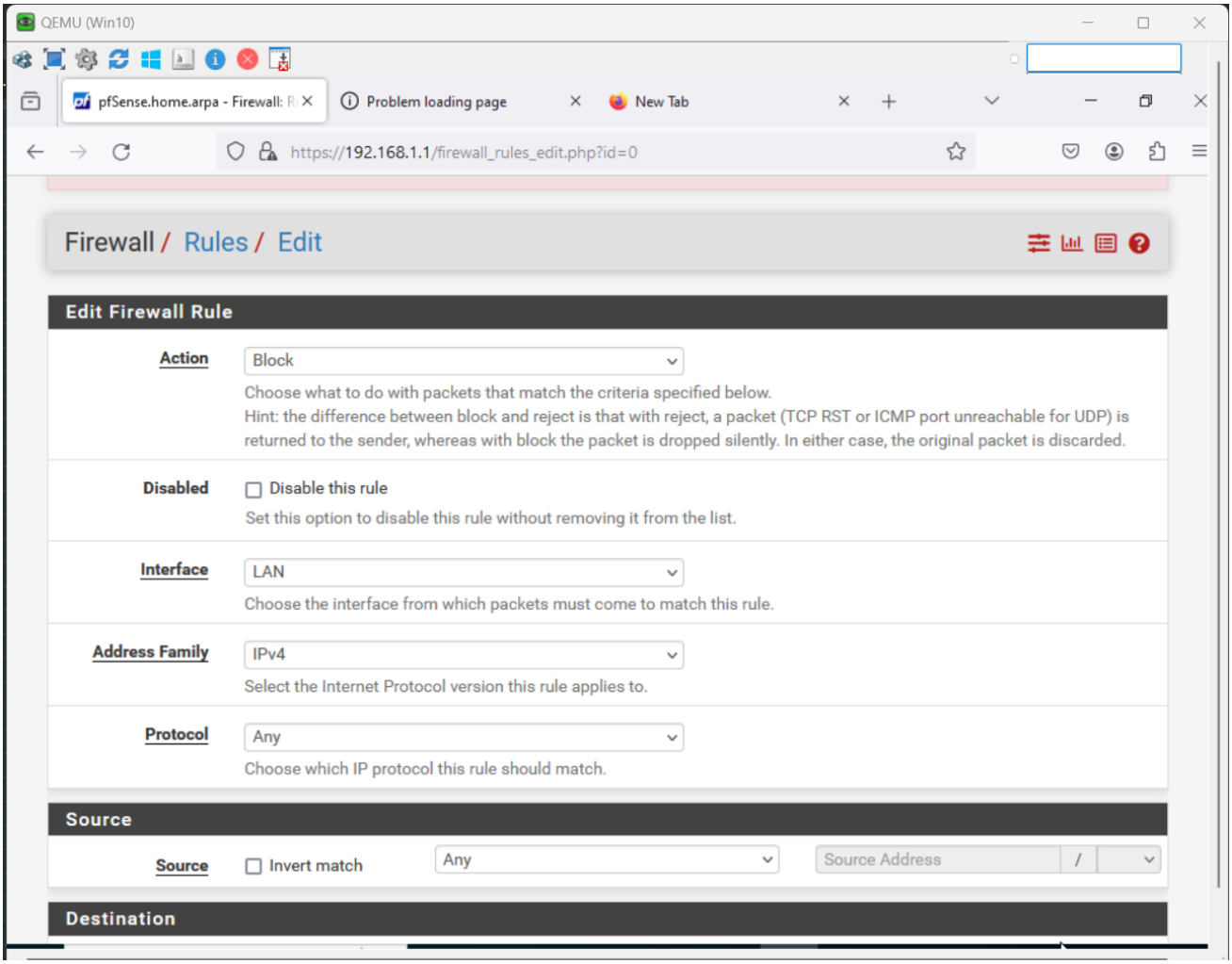
a. Firewall Rule Disabled

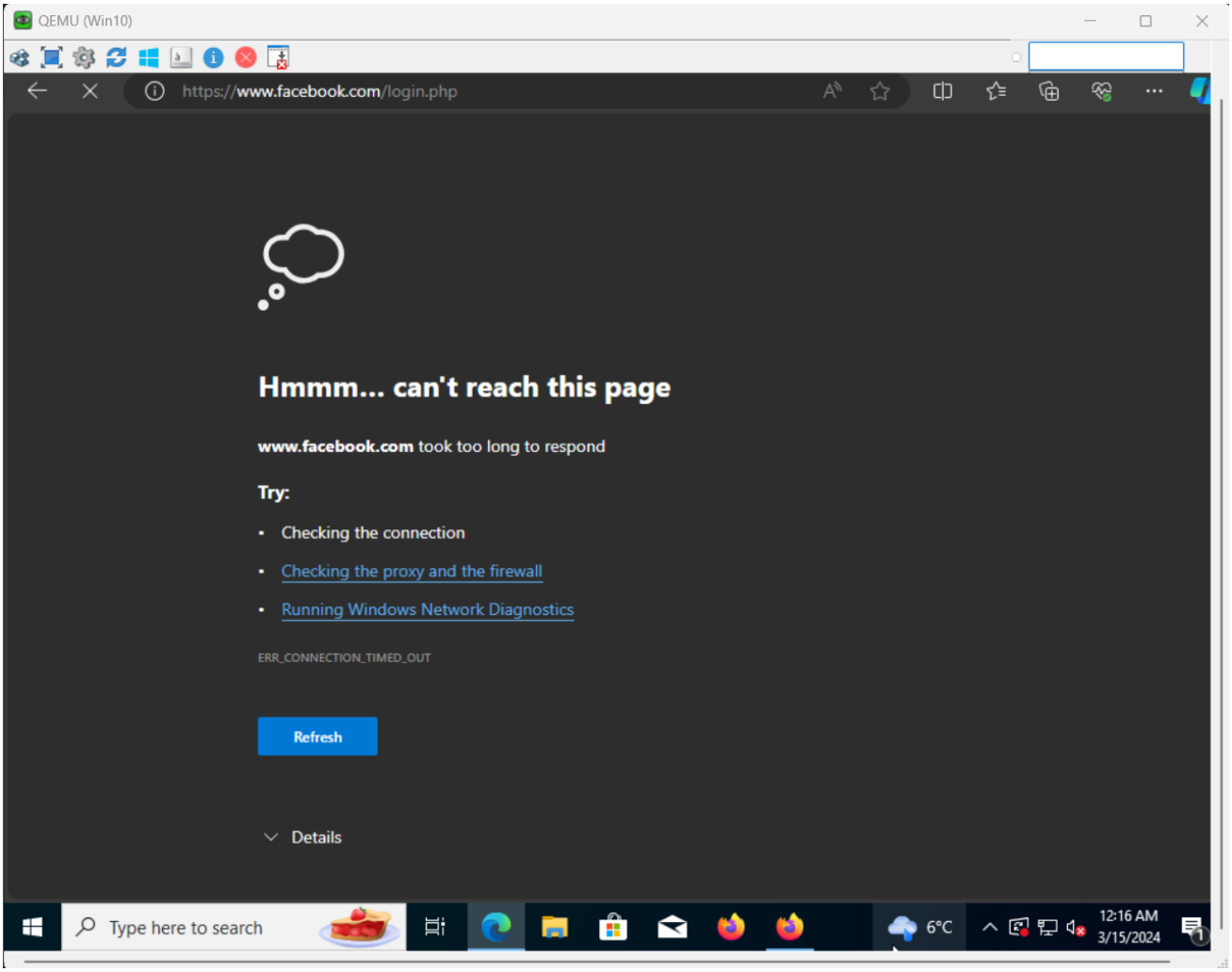

QEMU (Win10)
pfSense.home.arpa - Firewall:
https://192.168.1.1/firewall_rules_edit.php?id=0
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
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
Set this option to disable this rule without removing it from the list.
Interface
LAN
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

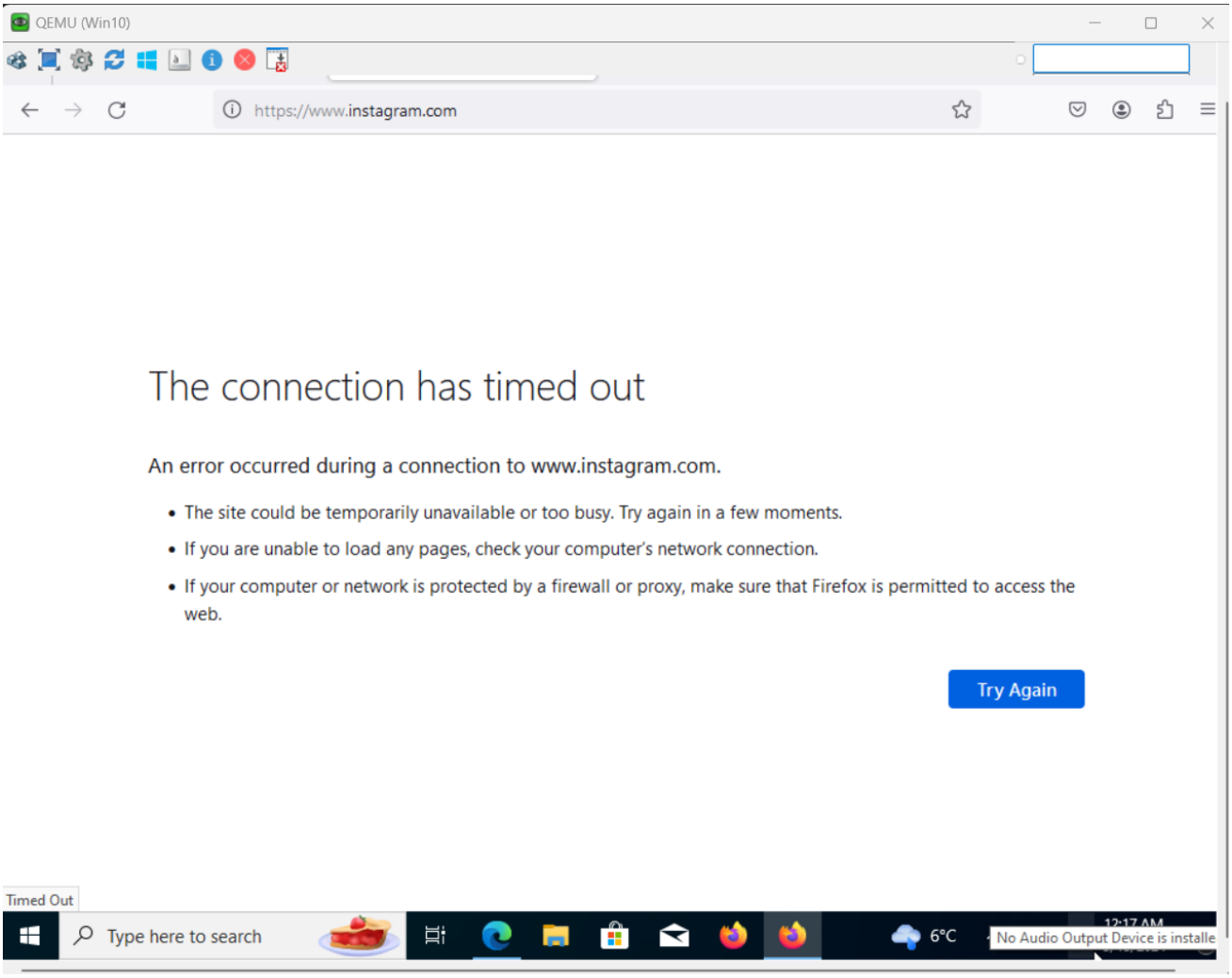

QEMU (Win10)
pfSense.home.arpa - Firewall: R
Facebook - log in or sign up
Instagram
https://www.facebook.com
facebook
Connect with friends and the world around you on Facebook.
Email or phone number
Password
Log In
Forgot password?
Create new account
Create a Page for a celebrity, brand or business.



b. Firewall Rules Enabled

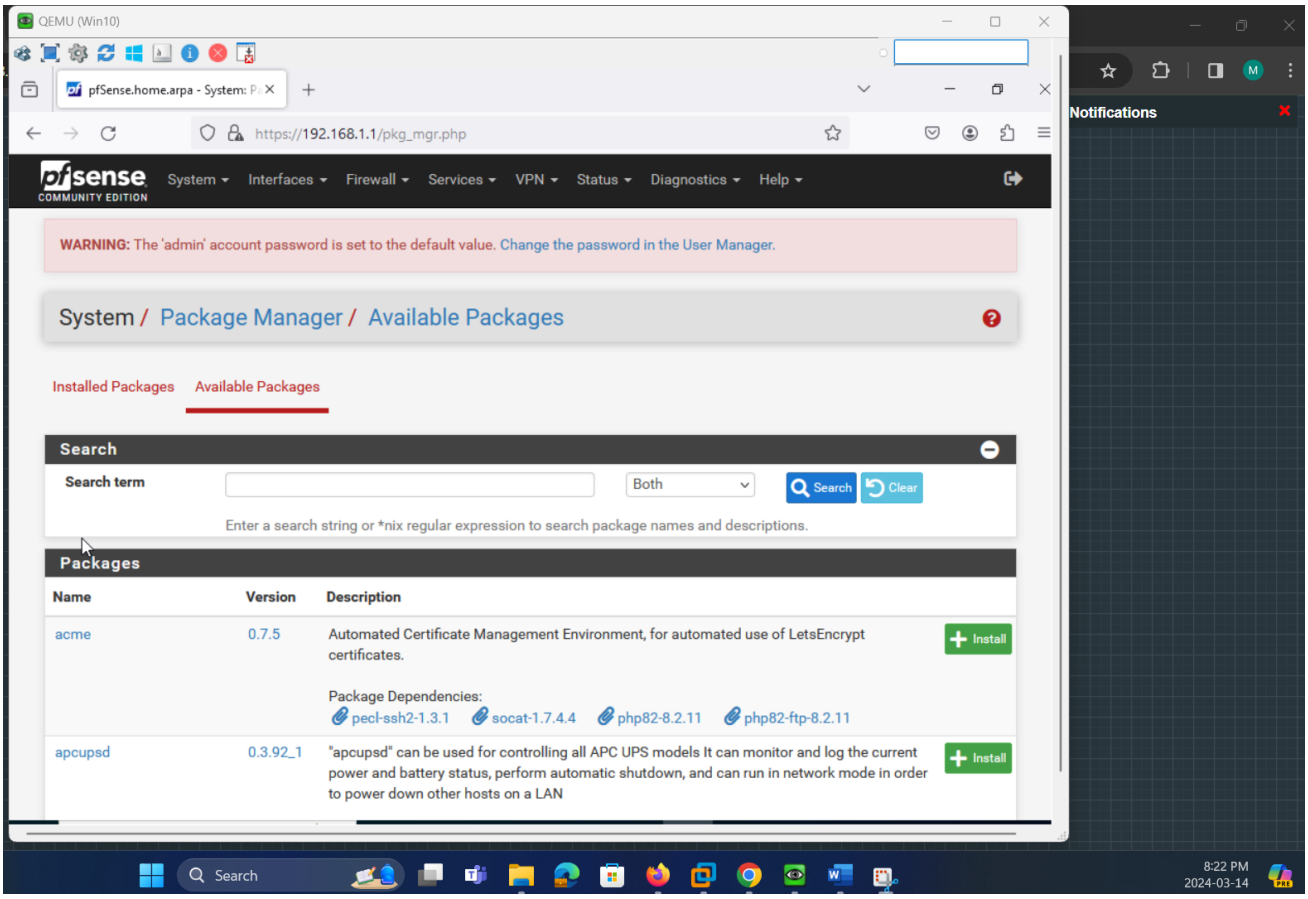

QEMU (Win10)
pfSense.home.arpa - Firewall: R
Problem loading page
New Tab
https://192.168.1.1/firewall_rules_edit.php?id=0
Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that 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
Set this option to disable this rule without removing it from the list.
Interface
LAN
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
Any
Source Address
/
Destination

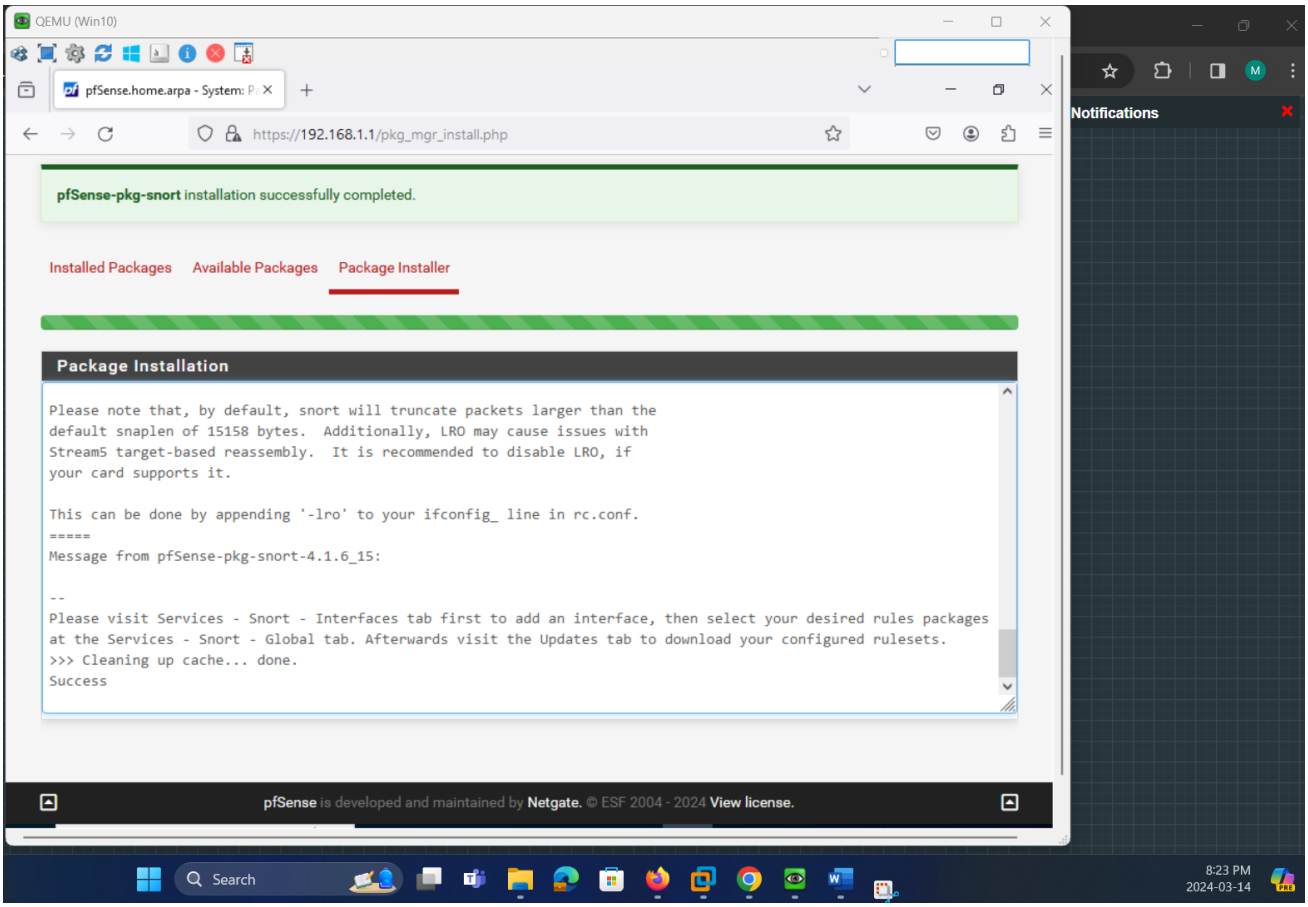

QEMU (Win10)
https://www.facebook.com/login.php
Hmmm... can't reach this page
www.facebook.com took too long to respond
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_TIMED_OUT
Refresh
Details
Type here to search
6°C
12:16 AM
3/15/2024

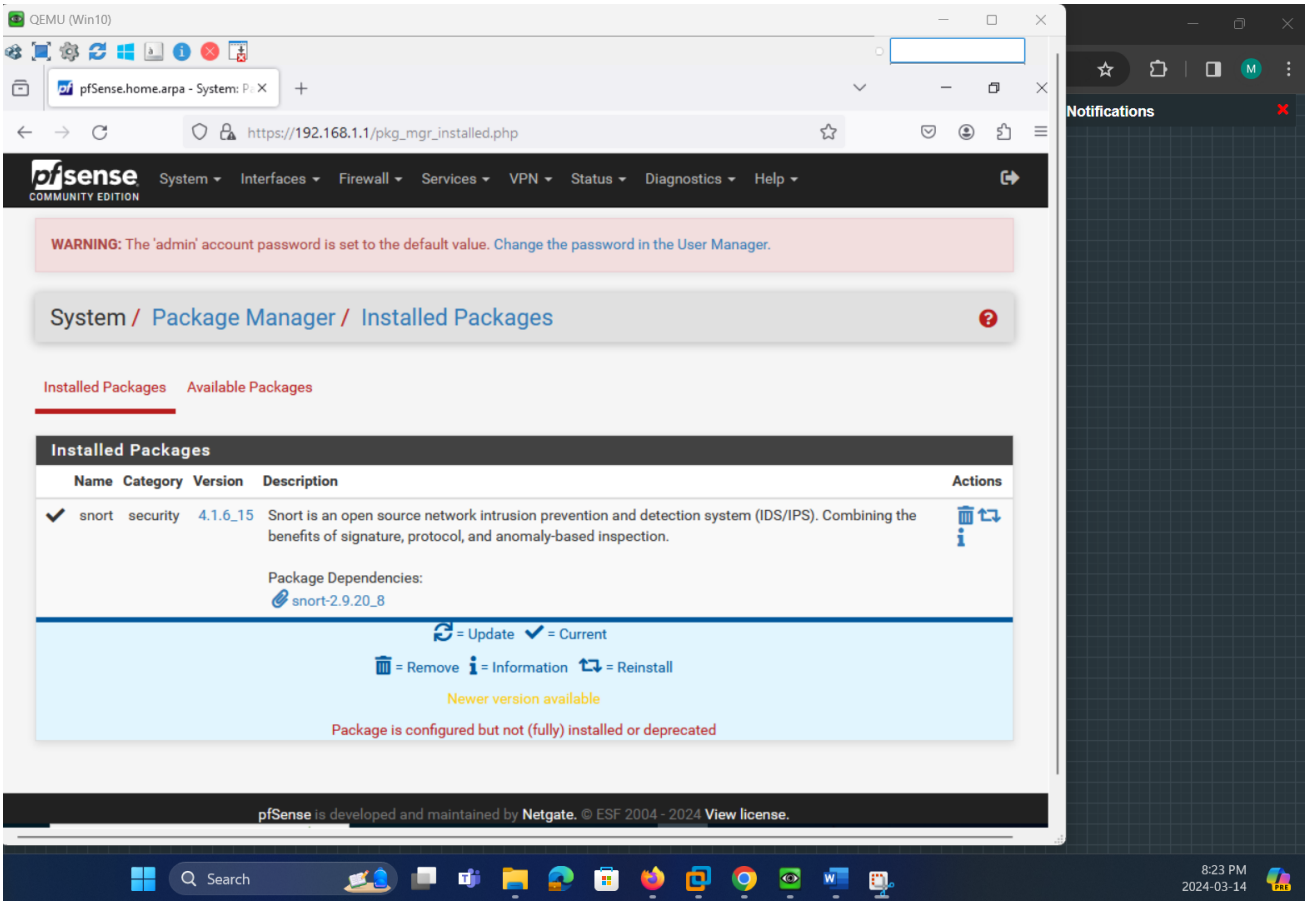


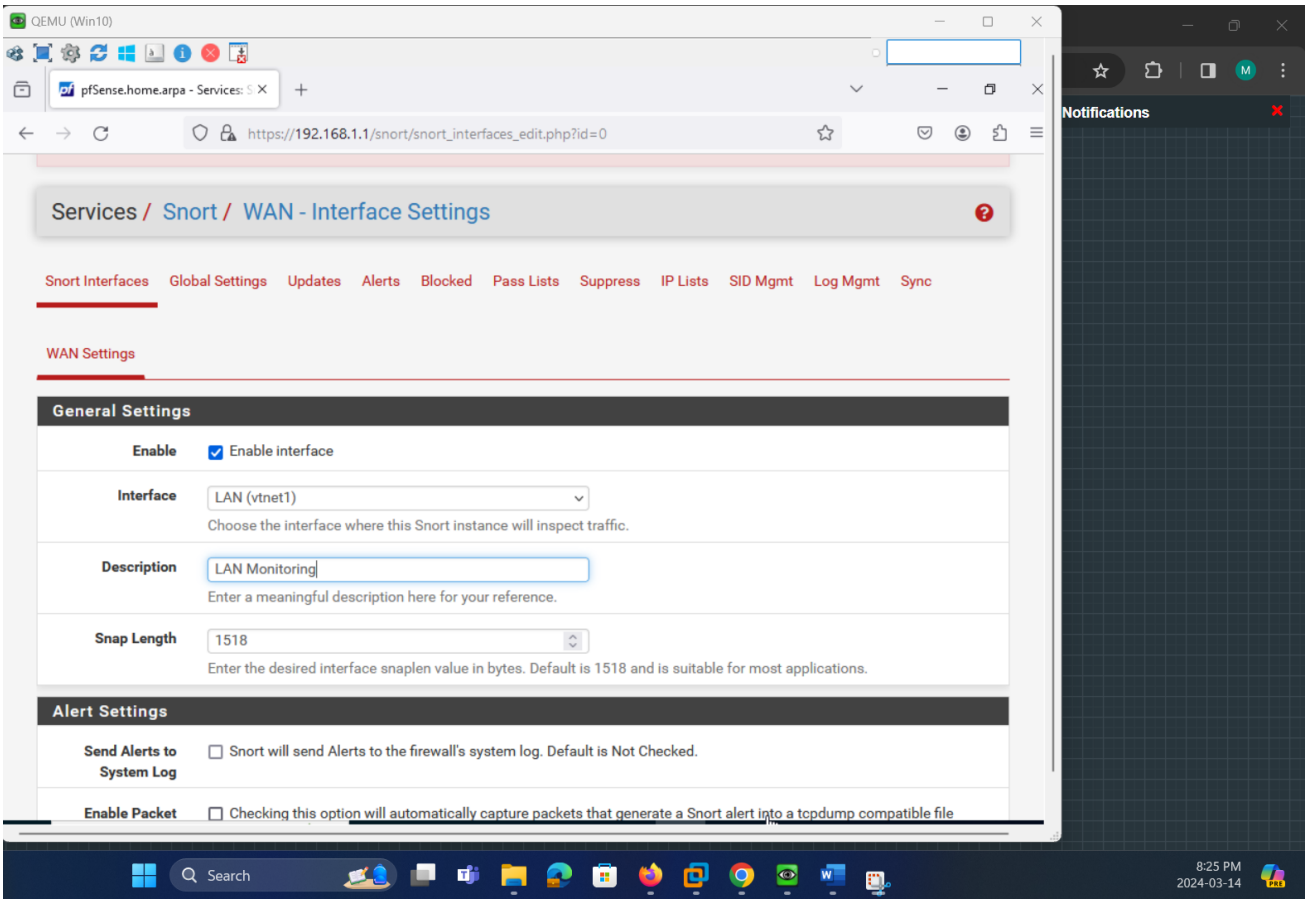
Tested both on Firefox and EDGE browser, both facebook and Instagram cannot be accessed when firewall rule is enabled.

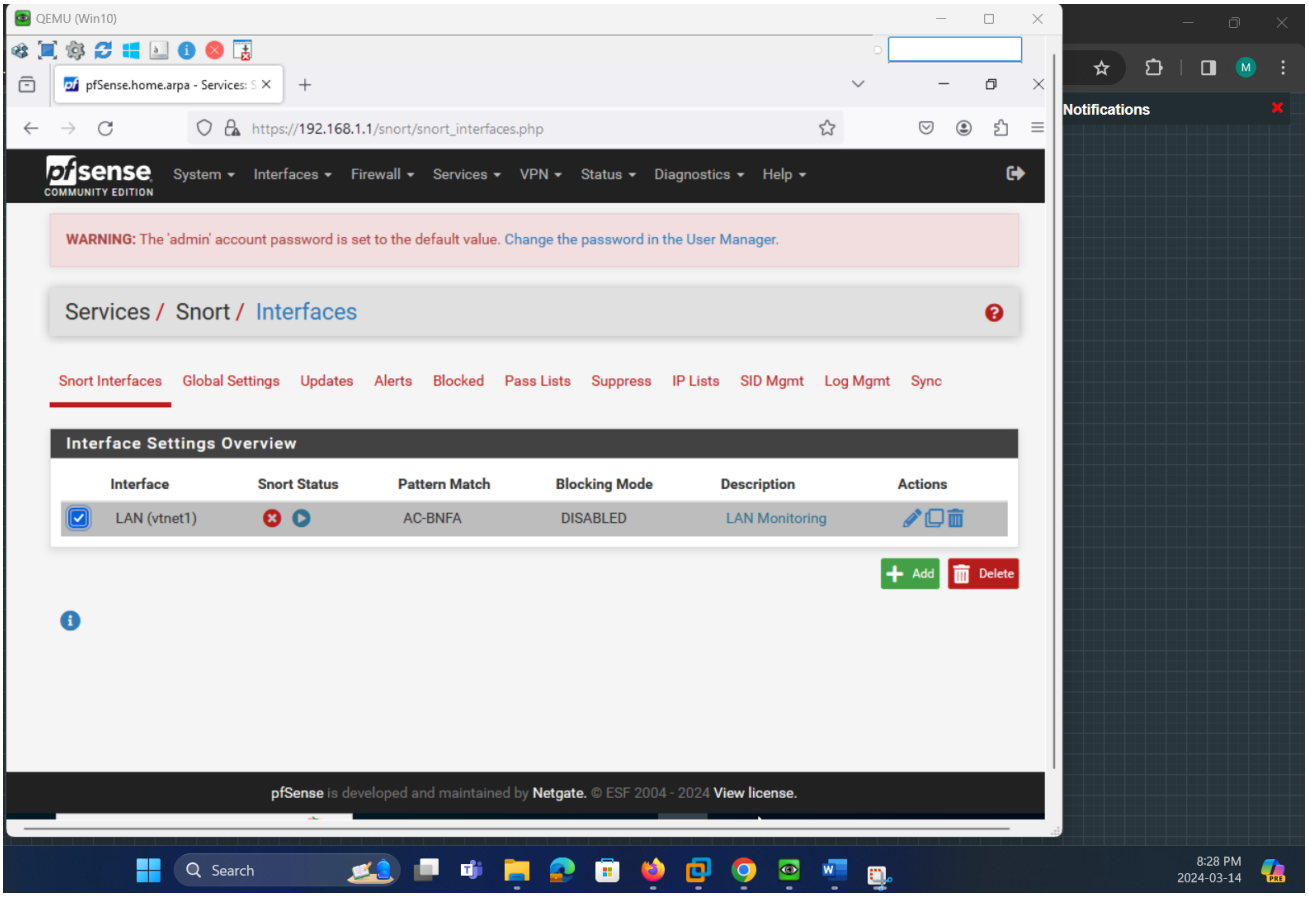
4. Installing IDS (Snort Package)

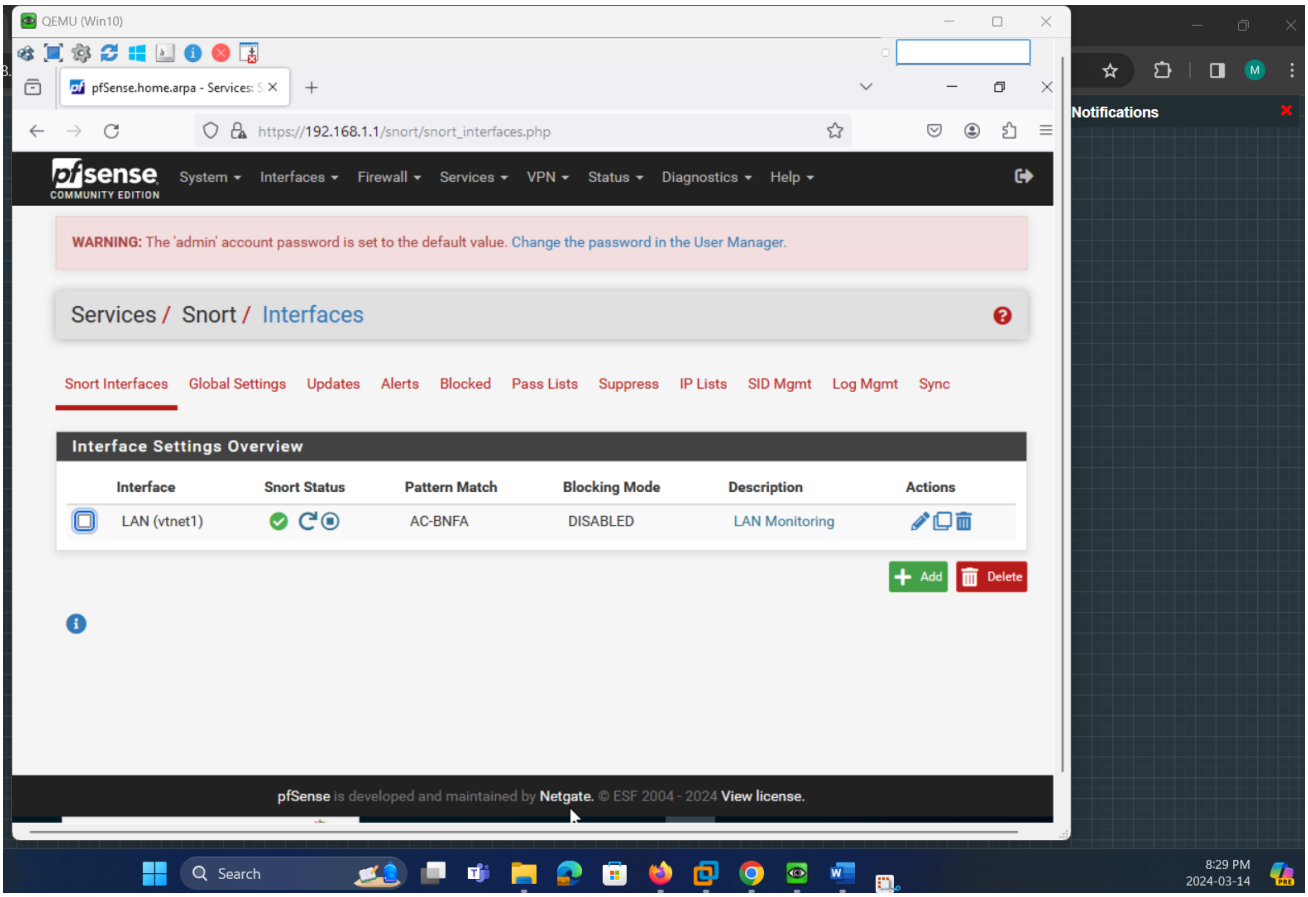

QEMU (Win10)
pfSense.home.arpa - System:
https://192.168.1.1/pkg_mgr.php
Notifications
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Package Manager / Available Packages
Installed Packages
Available Packages
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search package names and descriptions.
Packages
Name
Version
Description
acme
0.7.5
Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.
Package Dependencies:
pecl-ssh2-1.3.1
socat-1.7.4.4
php82-8.2.11
php82-ftp-8.2.11
Install
apcupsd
0.3.92_1
"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN
Install
Search
8:22 PM
2024-03-14

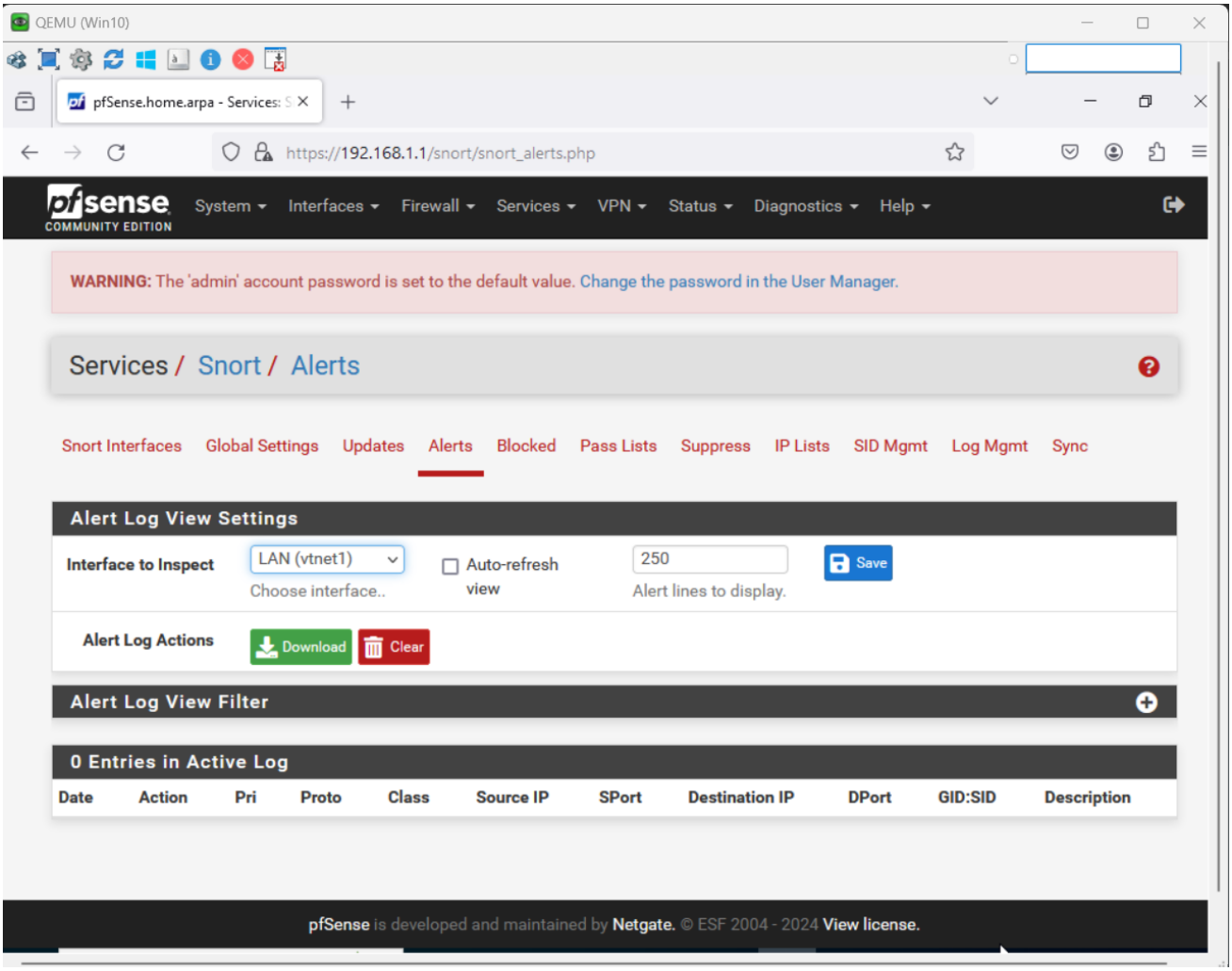

QEMU (Win10)
pfSense.home.arpa - System: P
https://192.168.1.1/pkg_mgr_install.php
Notifications
pfSense-pkg-snort installation successfully completed.
Installed Packages
Available Packages
Package Installer
Package Installation
Please note that, by default, snort will truncate packets larger than the
default snaplen of 15158 bytes. Additionally, LRO may cause issues with
Stream5 target-based reassembly. It is recommended to disable LRO, if
your card supports it.
This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
=====
Message from pfSense-pkg-snort-4.1.6_15:
--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages
at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Success
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Search
8:23 PM
2024-03-14


QEMU (Win10)
pfSense.home.arpa - System:
https://192.168.1.1/pkg_mgr_installed.php
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.
System / Package Manager / Installed Packages
Installed Packages
Available Packages
Installed Packages
Name Category Version Description Actions
snort security 4.1.6_15 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
Package Dependencies:
snort-2.9.20_8
= Update = Current
= Remove = Information = Reinstall
Newer version available
Package is configured but not (fully) installed or deprecated
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Notifications
Search
8:23 PM
2024-03-14


QEMU (Win10)
pfSense.home.arpa - Services: S
https://192.168.1.1/snort/snort_interfaces_edit.php?id=0
Notifications
Services / Snort / WAN - Interface Settings
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
WAN Settings
General Settings
Enable
Enable interface
Interface
LAN (vtnet1)
Choose the interface where this Snort instance will inspect traffic.
Description
LAN Monitoring
Enter a meaningful description here for your reference.
Snap Length
1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings
Send Alerts to System Log
Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet
Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Search
8:25 PM
2024-03-14


QEMU (Win10)
pfSense.home.arpa - Services: S
https://192.168.1.1/snort/snort_interfaces.php
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.
Services / Snort / Interfaces
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
Interface Settings Overview
Interface Snort Status Pattern Match Blocking Mode Description Actions
LAN (vtnet1) AC-BNFA DISABLED LAN Monitoring
Add Delete
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Notifications
Search
8:28 PM
2024-03-14


QEMU (Win10)
pfSense.home.arpa - Services:
https://192.168.1.1/snort/snort_interfaces.php
Notifications
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.
Services / Snort / Interfaces
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Interface Settings Overview
Interface
Snort Status
Pattern Match
Blocking Mode
Description
Actions
LAN (vtnet1)
AC-BNFA
DISABLED
LAN Monitoring
Add
Delete
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Search
8:29 PM
2024-03-14



Conclusion

Throughout this lab assignment, we successfully established a controlled network environment that included a Windows Server 2016 configured as an Active Directory and DNS server, a Windows 10 client, and a pfSense firewall to manage network traffic and enforce security policies. We leveraged the capabilities of pfSense to restrict access to specific social media websites, demonstrating the firewall's utility in content filtering. Additionally, the integration of Snort as an Intrusion Detection System (IDS) provided an extra layer of security by monitoring network traffic for signs of malicious activity and potential threats.

This hands-on experience highlighted the importance of layered security measures and the implementation of a defense-in-depth strategy. We saw firsthand how various components of a network can be configured and managed to protect organizational assets while also accommodating user requirements and accessibility.

Recommendations

- **Policy and Planning**: Before implementing network changes and security measures, it is crucial to establish clear policies that define acceptable use, access controls, and security protocols. These policies should align with the organization's overall security strategy and compliance requirements.
- **Regular Updates and Maintenance**: Keep all systems, including the Windows Server, Windows 10 client, and pfSense firewall, updated with the latest security patches and updates. This helps to mitigate vulnerabilities that could be exploited by attackers.
- **Continuous Monitoring and Improvement**: Utilize Snort IDS to continuously monitor network traffic and analyze logs for suspicious activity. Regularly update Snort's rulesets and review its configuration to adapt to evolving threats.
- **User Education**: Educate users about security best practices and the rationale behind blocking certain internet resources, such as social media sites. This helps to foster an organizational culture that values security.
- **Scalability and Performance**: As the network grows, consider the scalability of the current solutions. It may be necessary to upgrade hardware or optimize configurations to maintain performance and security levels.
- **Incident Response Plan**: Develop and maintain an incident response plan that includes procedures for addressing security breaches, including the role of IDS and network infrastructure in identifying and mitigating attacks.
- **Testing and Drills**: Regularly test the security infrastructure through drills and simulated attacks to ensure that all systems function as expected and to identify areas for improvement.

The objective of this lab was to provide practical skills in deploying and configuring network services and security measures, which are critical for any cybersecurity professional. The hands-on approach enhances understanding and prepares one to address real-world challenges.