pfSense Firewall Project: Securing My Home Lab

Implementing Firewall Rules for Effective Network Traffic Control

Project Overview: Firewall Implementation

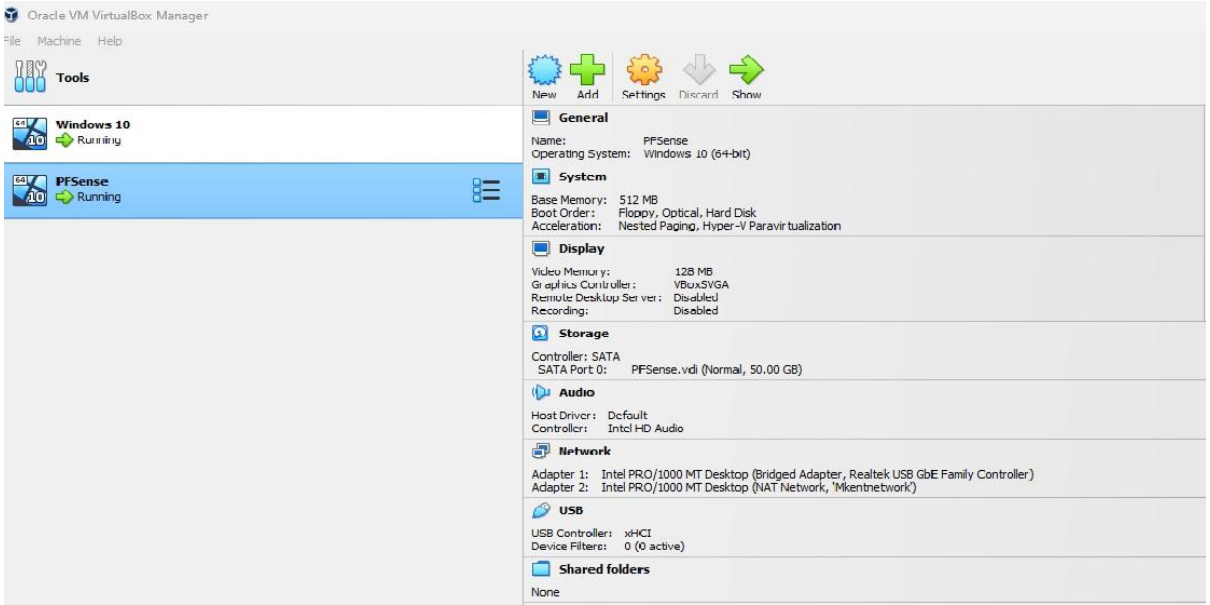
In this project, I used pfSense to set up a virtual machine (VM) alongside a Windows VM to enhance my home lab network security. I configured both machines to operate within the same subnet and created a firewall rule to block access to a specific website using an alias.

Additionally, I demonstrated how to block traffic based on IP addresses. This hands-on experience deepened my understanding of firewall management and strengthened my existing knowledge of network security practices.

Virtual Machine Setup

In this project, I utilized Oracle VirtualBox to set up two virtual machines (VMs). I downloaded and configured a pfSense firewall as one of the VMs to manage network traffic securely.

For the second VM, I deployed Windows 10 using the Windows Media Creation Tool, allowing me to create a testing and development environment.

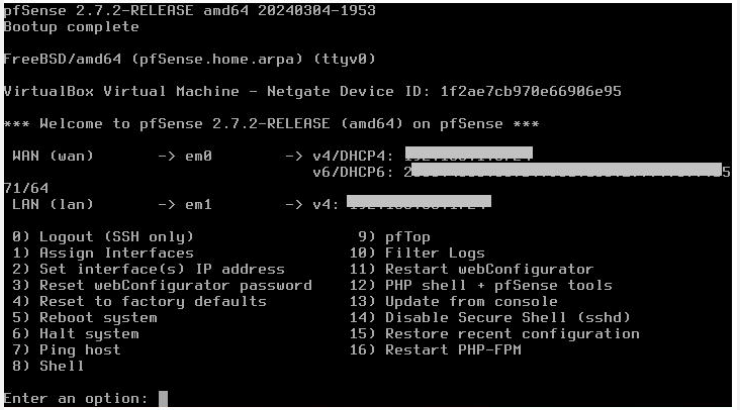


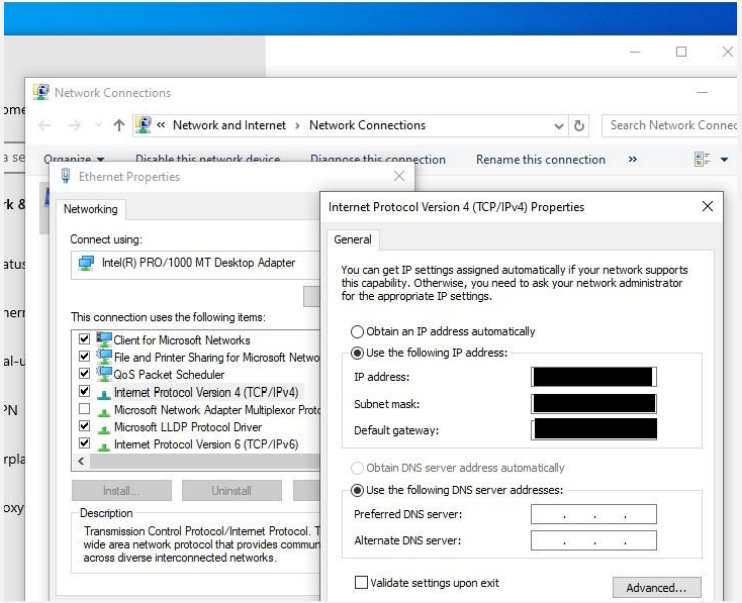
pfSense Network Configuration

I configured a bridged network adapter for the WAN interface, allowing pfSense to act as the gateway by connecting directly to my physical network.

For the LAN, I used a NAT network. I then set the pfSense LAN IP as the default gateway for the Windows VM, assigning it an IP within the same subnet.

This configuration ensured that all traffic from the VM passed through the pfSense firewall. To confirm that the VM's IP address was aligned with pfSense's network configuration, I utilized the 'ipconfig' command.

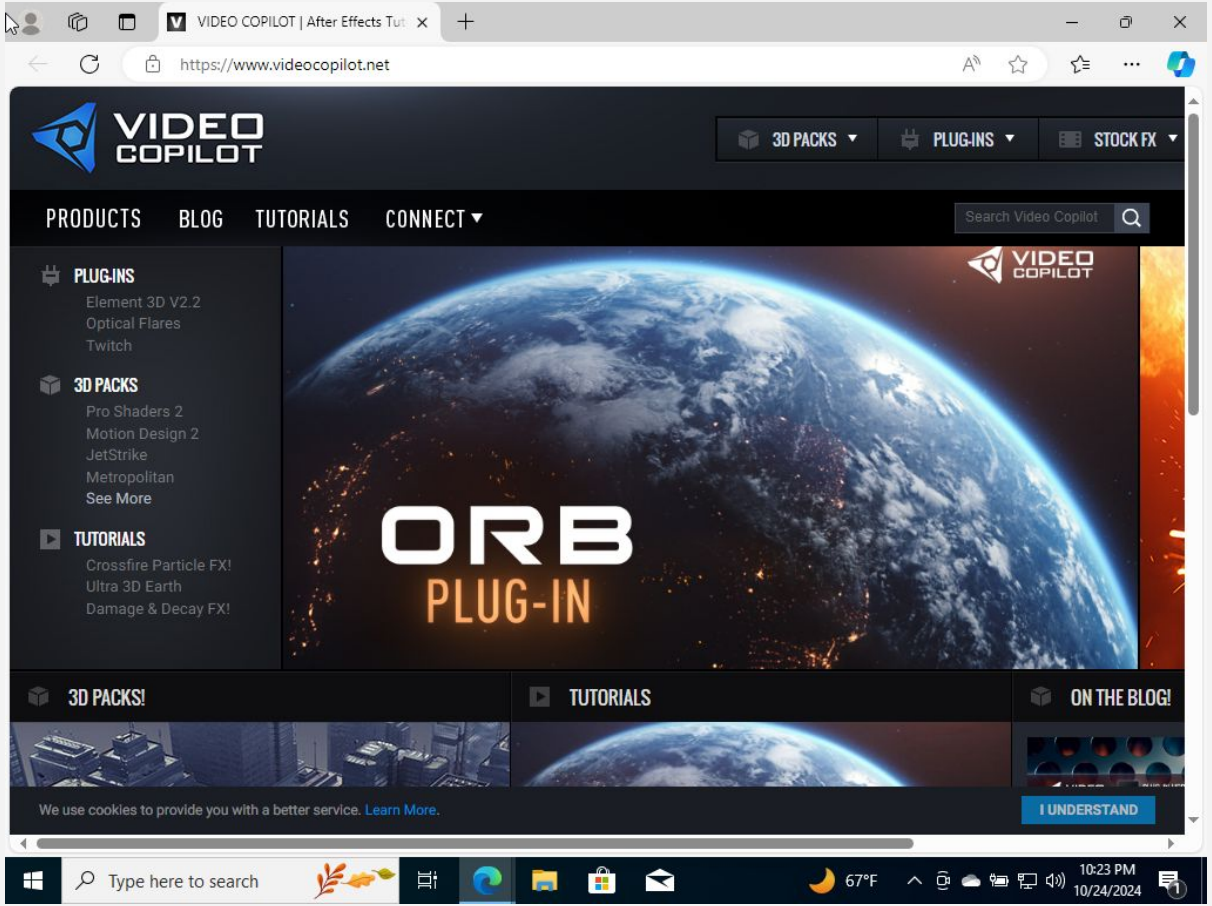




Blocking Website Traffic

This slide features the website videocopilot.net, which is currently accessible, as shown in the image.

Next I will demonstrate how to configure the firewall to block traffic from our network to this site, illustrating how firewall rules can be used to manage network traffic and enforce security policies effectively.

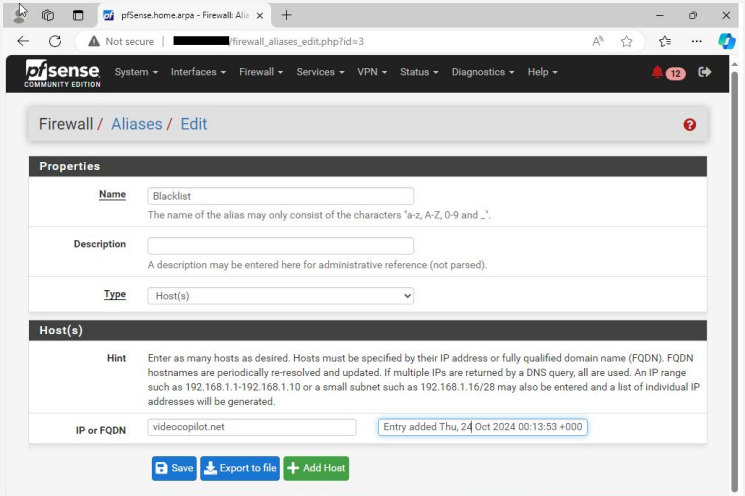


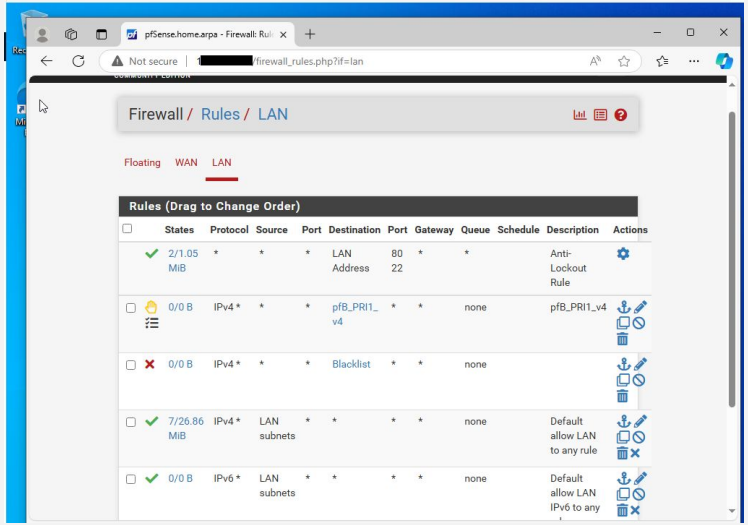
Firewall Blocking Videopilot.net

This slide shows the steps taken to block access to *videopilot.net* by creating an alias labeled Blocked_Sites.

Using this alias allows centralized control over restricted domains, simplifying rule management.

To ensure that the rule remains effective and isn't overridden by other rules, it was positioned near the top of the rule list. This placement prioritizes the block and ensures consistent enforcement across all associated domains.

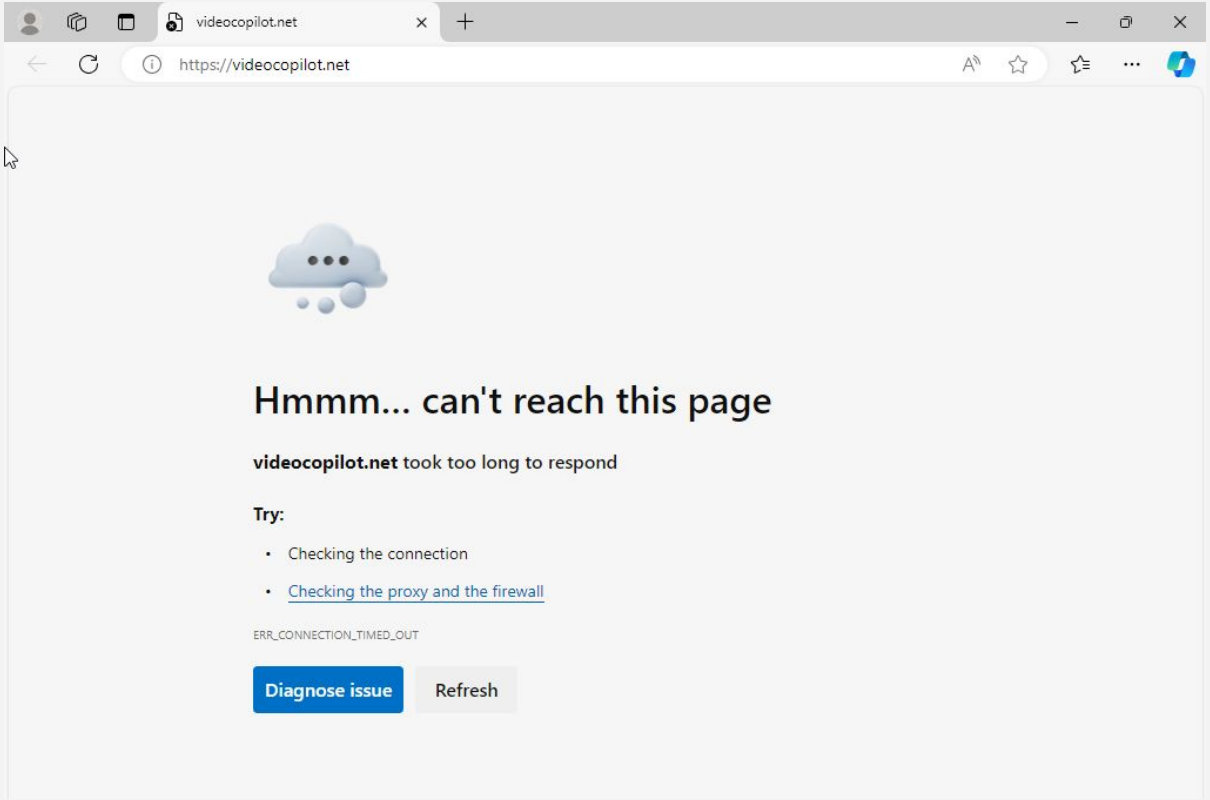




Firewall Block Success

This slide confirms that the firewall rule was effective, showing *videopilot.net* as inaccessible.

The displayed image demonstrates that attempts to access the site are blocked, verifying the functionality of the Blocked_Sites alias and firewall rule configuration.

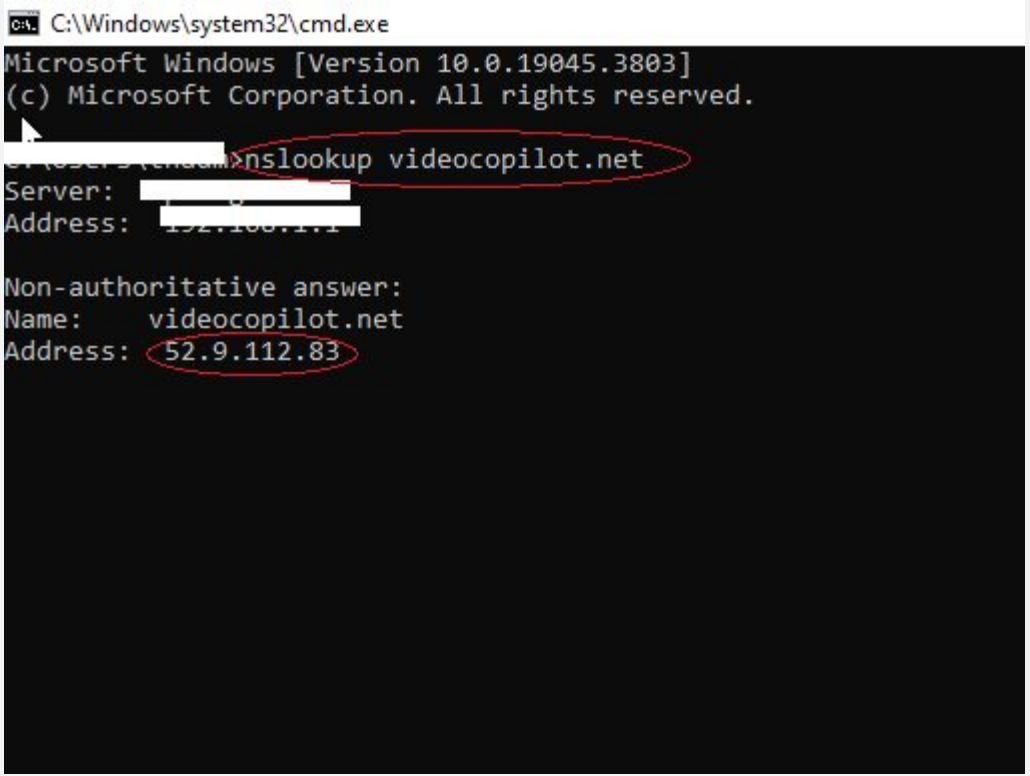


nslookup for IP Resolution

In this slide, I demonstrate the use of the `nslookup` command to query DNS for the IP address associated with a domain name.

By entering `nslookup videocopilot.net` on the command line, I retrieve the resolved IP address, 52.9.112.83.

This technique is useful for creating effective firewall rules to block unwanted traffic.

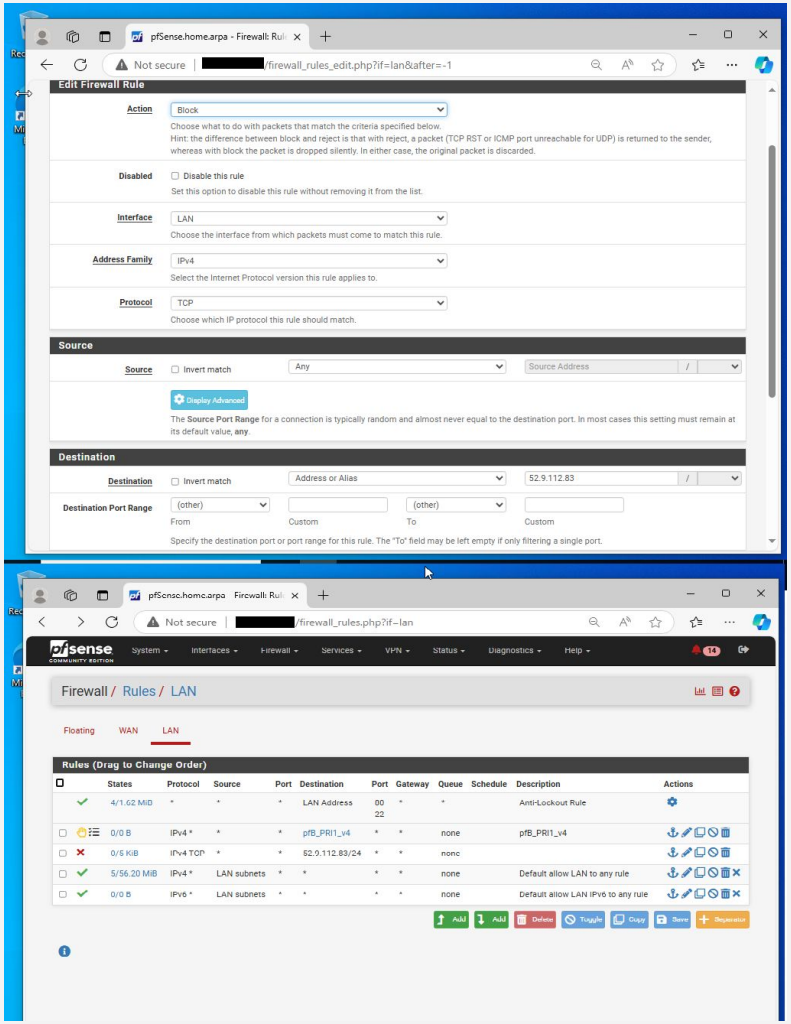


IP Blocking Insights

In this slide, I attempted to block *videopilot.net* using the IP address 52.9.112.83, but this approach proved ineffective. This could be due to the site using a content delivery network (CDN) or a load balancer, which distributes incoming requests across multiple IP addresses. As a result, blocking a single IP may not fully prevent access to the site. To improve the blocking strategy, I then blocked the CIDR range 52.9.112.83/24, which successfully restricted access.

Pros of blocking by CIDR range include a more comprehensive approach to preventing access, as it covers multiple associated IP addresses. However, downsides include the potential for inadvertently blocking legitimate traffic from other services hosted within that range.

To better understand why the single IP blocking didn't work, analyzing the logs can provide insights into the traffic patterns and reveal whether a load balancer or other factors are at play.



Closing Remarks

In this project, I utilized pfSense within Oracle VirtualBox to enhance my home lab network security by setting up two virtual machines: a pfSense firewall and a Windows 10 VM. I configured a bridged network adapter for the WAN interface, allowing pfSense to act as the gateway, while employing a NAT network for the LAN. This configuration ensured that all traffic from the Windows VM passed through the firewall.

This hands-on experience gave me valuable insights into creating firewall rules to manage network traffic effectively. Firewalls play a crucial role in protecting networks by filtering incoming and outgoing traffic, preventing unauthorized access, and enforcing security policies. Overall, this project deepened my understanding of firewall management and reinforced key network security practices.