

## **Server Setup: Setting up the Firewall**

Branson Bailey

Home Lab Project

21 December 2024

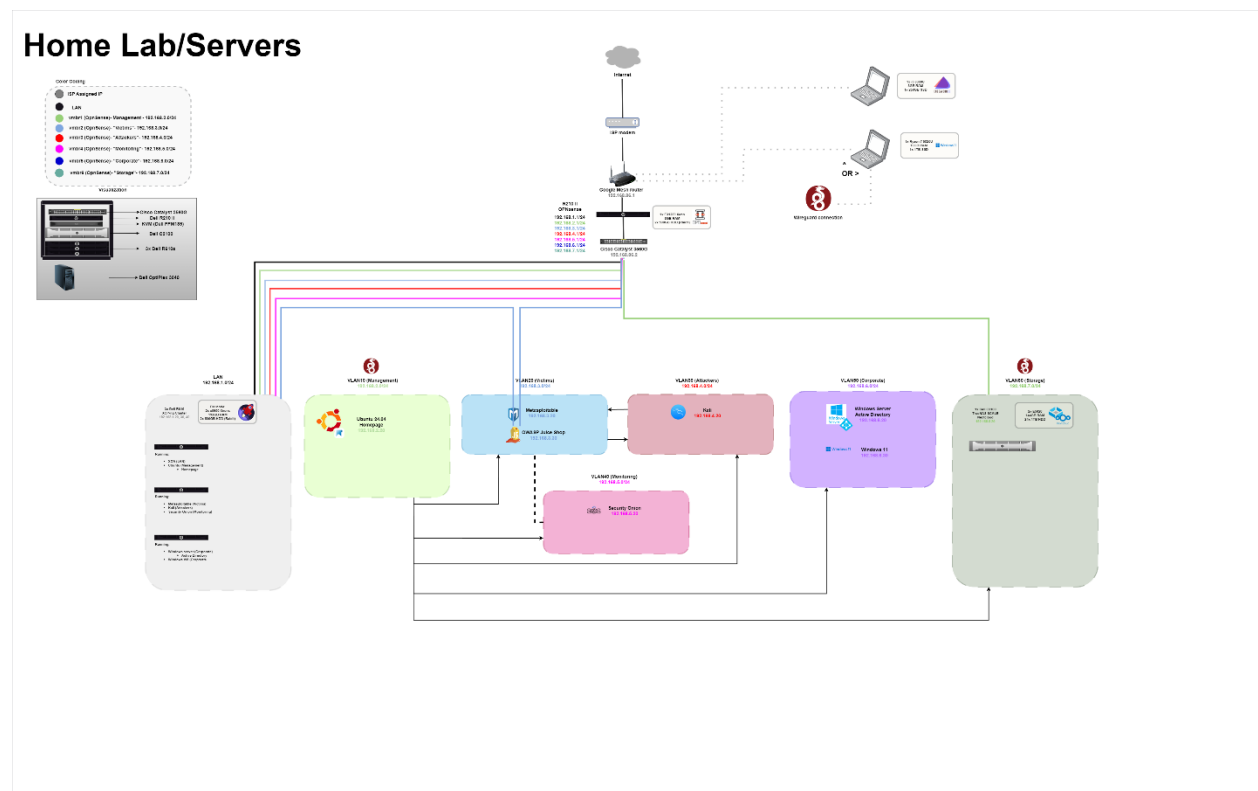
**Table of Contents**

<b>Content</b>	<b>Page</b>
Cover Page	1
Table of contents	2
Project Focus	3
Firewall Setup Process	4
Write-up	7
References	8

## Project Focus

The focus of this project is to setup the firewall rules on OPNsense (24.7) in my home lab environment. This will provide some simple network security for my setup. Please note that my entire home lab is in an internal network, so I don't face the same immediate risk that a setup with a public facing IP would

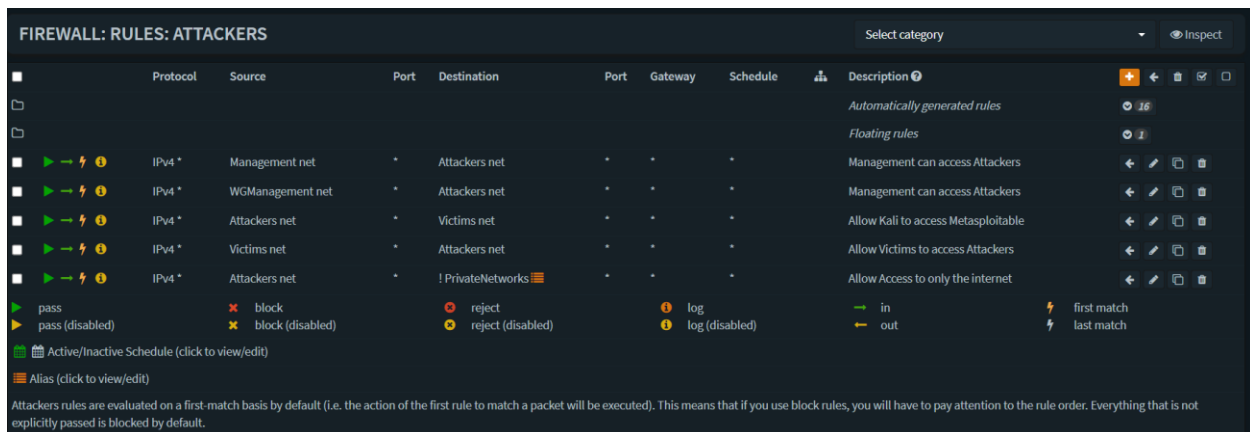
Attached below is a basic overview of the desired network topology for my home lab setup  
(After some consideration, it has changed a bit):



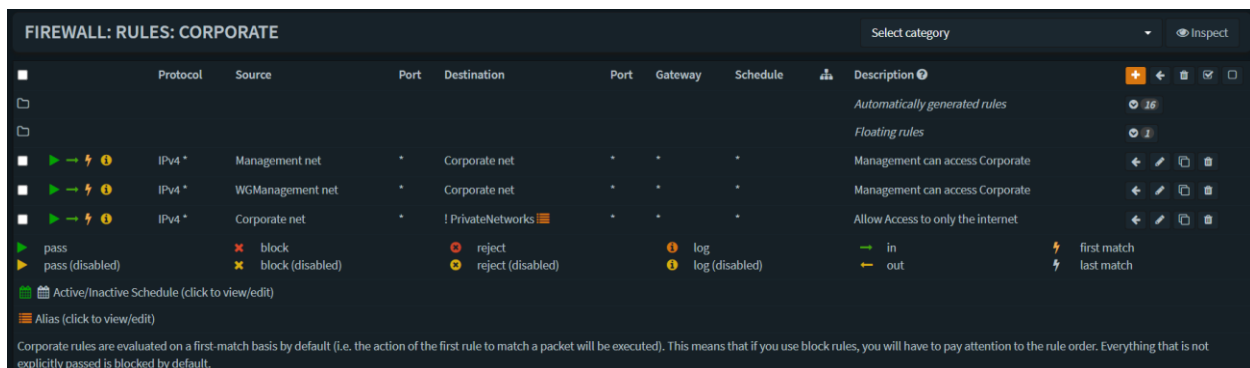
## End-Goal Network Topology

## Firewall Setup Process

In this part, I will display the process of setting up the firewall in OPNsense. This writeup will begin after my last addition to the project. Please note that there were some “behind-the-scenes” changes to my overall topology. I decided that instead of putting an Ubuntu server VM running a WireGuard instance in the desired networks, that I would instead simply make those instances in OPNsense. This part was extremely easy. In fact, all of these changes to the firewall were done through that VPN.



## Attackers firewall rules



## Corporate firewall rules

FIREWALL: RULES: LAN										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										25	
Floating rules										1	
	IPv4 TCP/UDP	Storage net	*	LAN net	445 - 2049	*	*		Allow access to TrueNas through SMB or NFS		
	IPv4+6 *	WGManagement net	*	LAN net	*	*	*		Management to LAN		
	IPv4+6 *	Management net	*	LAN net	*	*	*		Management to LAN		
	IPv4+6 *	LAN net	*	! PrivateNetworks	*	*	*		Give access to internet from LAN		
pass		block		reject			log		in	first match	
pass (disabled)		block (disabled)		reject (disabled)			log (disabled)		out	last match	
Active/Inactive Schedule (click to view/edit)											
Alias (click to view/edit)											

## LAN firewall rules

FIREWALL: RULES: MANAGEMENT										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										16	
Floating rules										1	
	IPv4+6 *	Management net	*	*	*	*	*		Allow access to All		
	IPv4+6 *	WGManagement net	*	Management net	*	*	*				
	IPv4 *	LAN net	*	Management net	*	*	*		LAN network to Management		
	IPv4 *	Monitoring net	*	Management net	*	*	*		Block Monitoring network to Management		
	IPv4 *	Storage net	*	Management net	*	*	*		Block Storage network to Management		
	IPv4 *	Attackers net	*	Management net	*	*	*		Block Attackers from accessing management		
	IPv4 *	Victims net	*	Management net	*	*	*		Block Victims from accessing Management		
	IPv4 *	Corporate net	*	Management net	*	*	*		Block Corporate net from accessing Management		

## Management firewall rules

FIREWALL: RULES: MONITORING										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										16	
Floating rules										1	
	IPv4 *	WGManagement net	*	Monitoring net	*	*	*		Allow Management to monitoring		
	IPv4 *	Management net	*	Monitoring net	*	*	*		Allow Management to Monitoring		
	IPv4 *	Monitoring net	*	! PrivateNetworks	*	*	*		Allow Access to only the internet		
	IPv4 *	Victims net	*	Monitoring net	*	*	*		Block Victims from accessing Monitoring		
	IPv4 *	Corporate net	*	Monitoring net	*	*	*		Block Corporate from accessing Monitoring		
	IPv4 *	Attackers net	*	Monitoring net	*	*	*		Block Attackers from accessing Monitoring		

## Monitoring firewall rules

FIREWALL: RULES: STORAGE										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										19	
Floating rules										1	
	IPv4 *	LAN net	*	Storage net	*	*	*		Storage can access VPN		
	IPv4 *	WGStorage net	*	Storage net	*	*	*		VPN can access Storage		
	IPv4 *	WGManagement net	*	Storage net	*	*	*		Management to Storage		
	IPv4 *	Management net	*	Storage net	*	*	*		Management to Storage		
	IPv4 *	Storage net	*	! PrivateNetworks	*	*	*		Allow Access to only the internet		

## Storage firewall rules

FIREWALL: RULES: VICTIMS										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										16	
Floating rules										1	
	IPv4 *	Attackers net	*	Victims net	*	*	*		Allow Kali to access Metasploitable		
	IPv4 *	Victims net	*	Attackers net	*	*	*		Allow Kali to access Metasploitable		
	IPv4 *	Management net	*	Victims net	*	*	*		Management to Victims		
	IPv4 *	WGManagement net	*	Victims net	*	*	*		Management to Victims		
	IPv4 *	Victims net	*	! PrivateNetworks	*	*	*		Allow Access to only the internet		
pass		block		reject			log		in	first match	
pass (disabled)		block (disabled)		reject (disabled)			log (disabled)		out	last match	

### Victim firewall rules

FIREWALL: RULES: WGMANAGEMENT										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										16	
Floating rules										1	
	IPv4 *	WGManagement net	*	WGManagement address	*	*	*				
	IPv4 *	LAN net	*	WGManagement net	*	*	*		LAN network to Management		
	IPv4+6 *	WGManagement net	*	*	*	*	*		Allow access to All		
	IPv4+6 *	PrivateNetworks	*	WGManagement net	*	*	*		Block access from VLANs		
pass		block		reject			log		in	first match	
pass (disabled)		block (disabled)		reject (disabled)			log (disabled)		out	last match	

### WGManagement firewall rules

FIREWALL: RULES: WGSTORAGE										Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description		
Automatically generated rules										16	
Floating rules										1	
	IPv4 *	WGStorage net	*	WGStorage address	*	*	*				
	IPv4 *	WGStorage net	*	Storage net	*	*	*				
	IPv4 *	WGStorage net	*	! PrivateNetworks	*	*	*				
	IPv4 *	WGStorage net	*	PrivateNetworks	*	*	*				
pass		block		reject			log		in	first match	
pass (disabled)		block (disabled)		reject (disabled)			log (disabled)		out	last match	

### WGStorage firewall rules

### **Write-up & Summary**

In this project section, I focused on creating tailored firewall rules to enhance the security of this network architecture. These rules regulate traffic flow between subnets, allowing necessary communication while minimizing the attack surface and ensuring strict compliance with the principle of least privilege. This configuration establishes a robust foundation for a secure and scalable network environment.

## References

*Draw.io - free flowchart maker and diagrams online. Flowchart Maker & Online Diagram*

*Software. (n.d.). <https://app.diagrams.net/>*

*OPNsense® a true open source security platform and more - OPNsense® is a true open source*

*firewall and more. (2024, July 31). OPNsense® Is a True Open Source Firewall and More.*

*<https://opnsense.org/>*