Laboratory Report

# Network Attack and Defense Using OPNSense

Author: Vlassov Vladislav

Date: September 23. 2025

# Introduction

The purpose of this lab work is to demonstrate network attacks using Kali Linux and analyze the effectiveness of security mechanisms implemented on the OPNSense firewall/router. The defense involves configuring firewall rules and enabling the Suricata intrusion detection system (IDS). We also evaluate the success rate of the protection measures against different types of network threats.

# Infrastructure Overview

Three virtual machines were used in this lab environment:

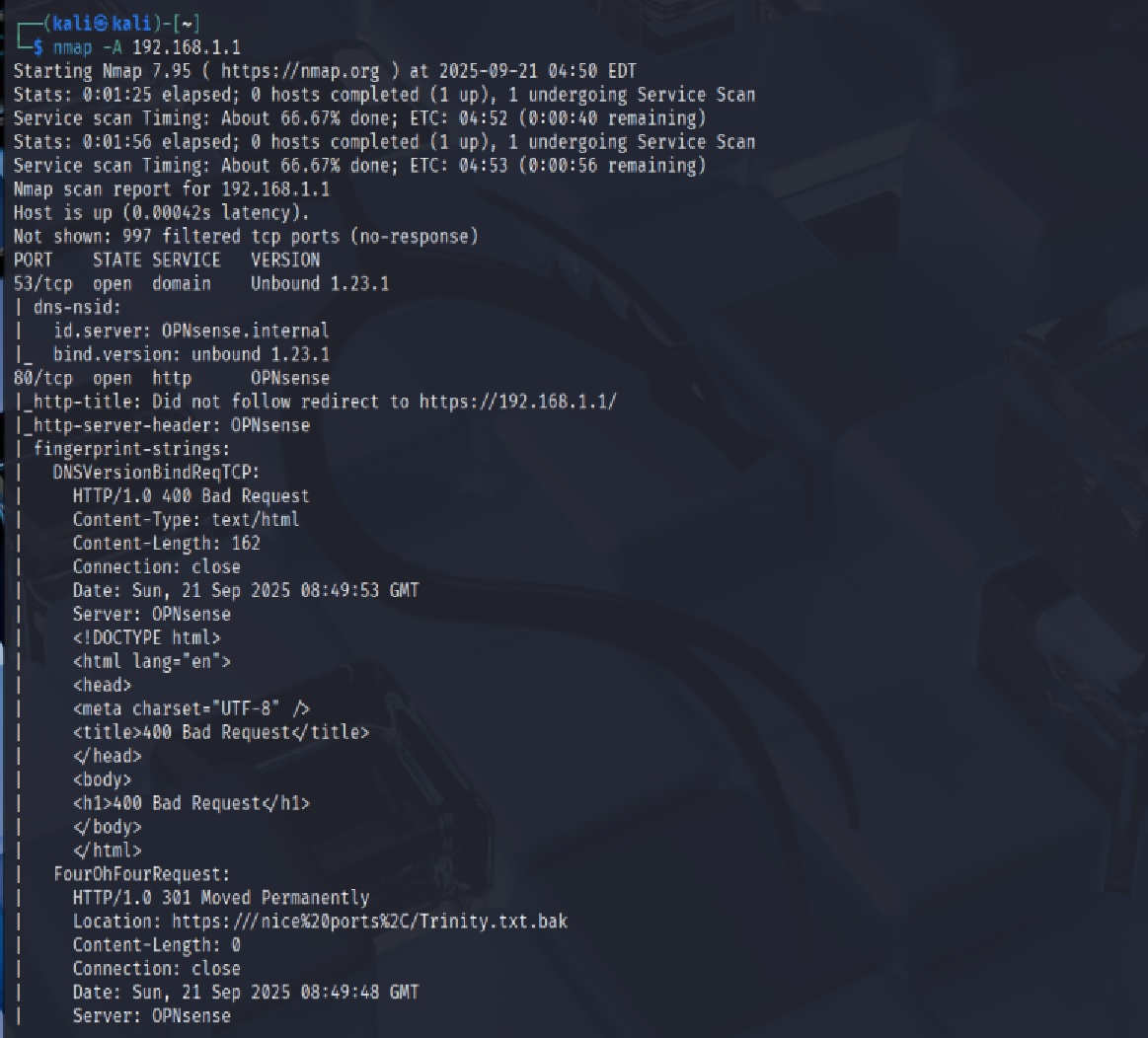
- Kali Linux — attacker machine (external network)

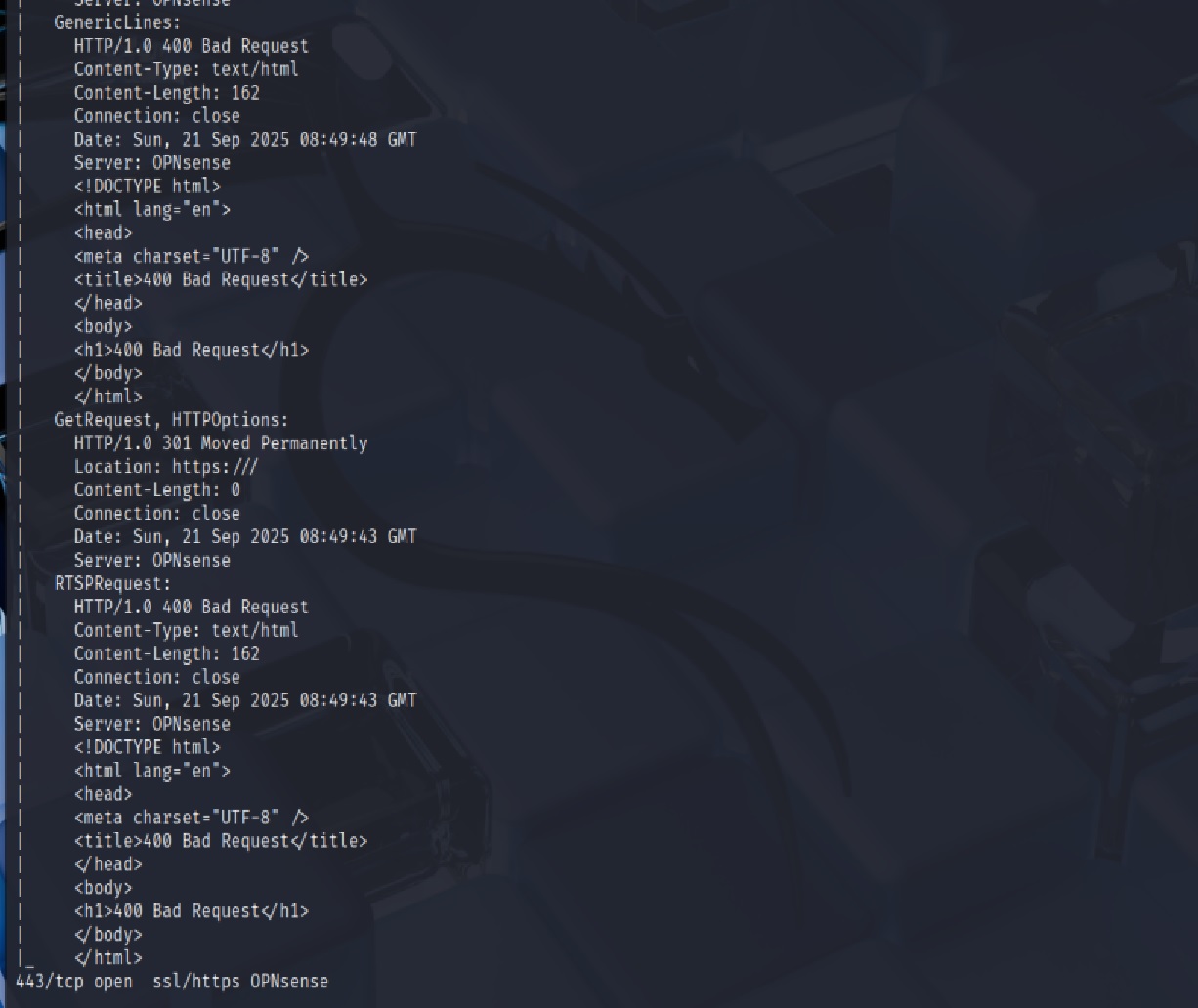
- Ubuntu — target machine in the DMZ segment

- OPNSense — router and traffic filtering system

# Attack #1 — Network Access Attempt from Kali Linux

In the first stage, the attacker initiated a connection attempt from Kali Linux to a service hosted in the DMZ. This involved scanning and direct service requests to test access control boundaries.

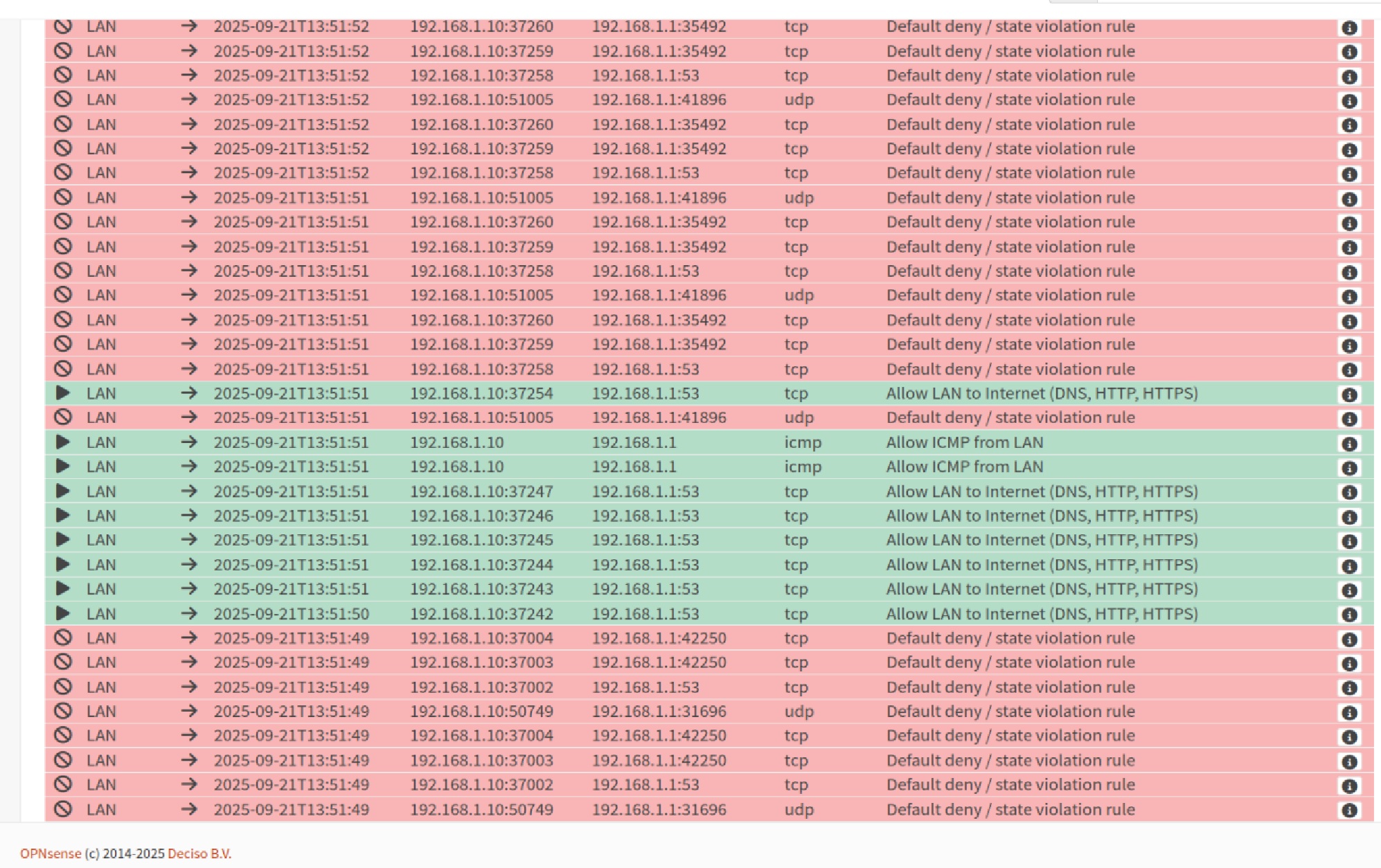
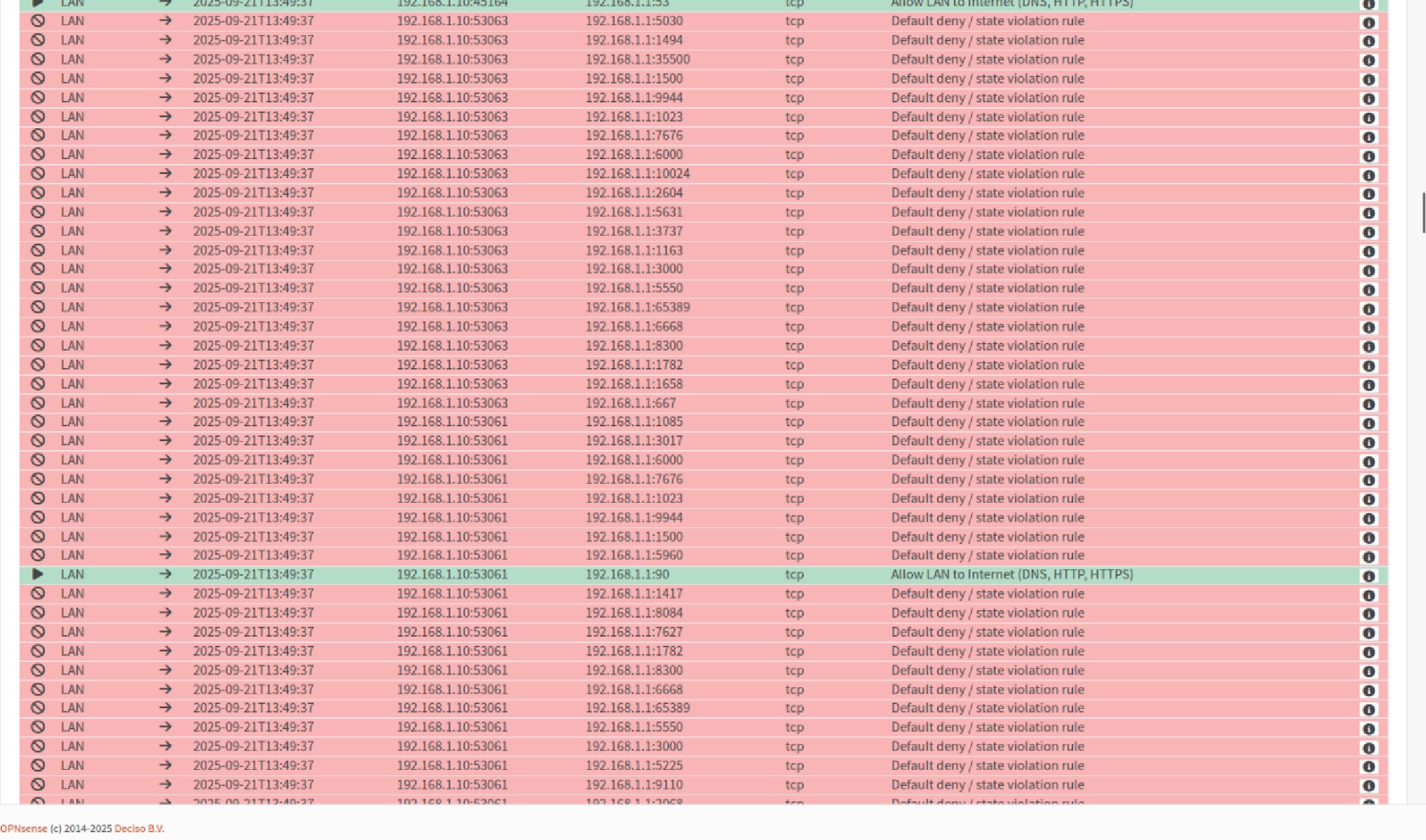




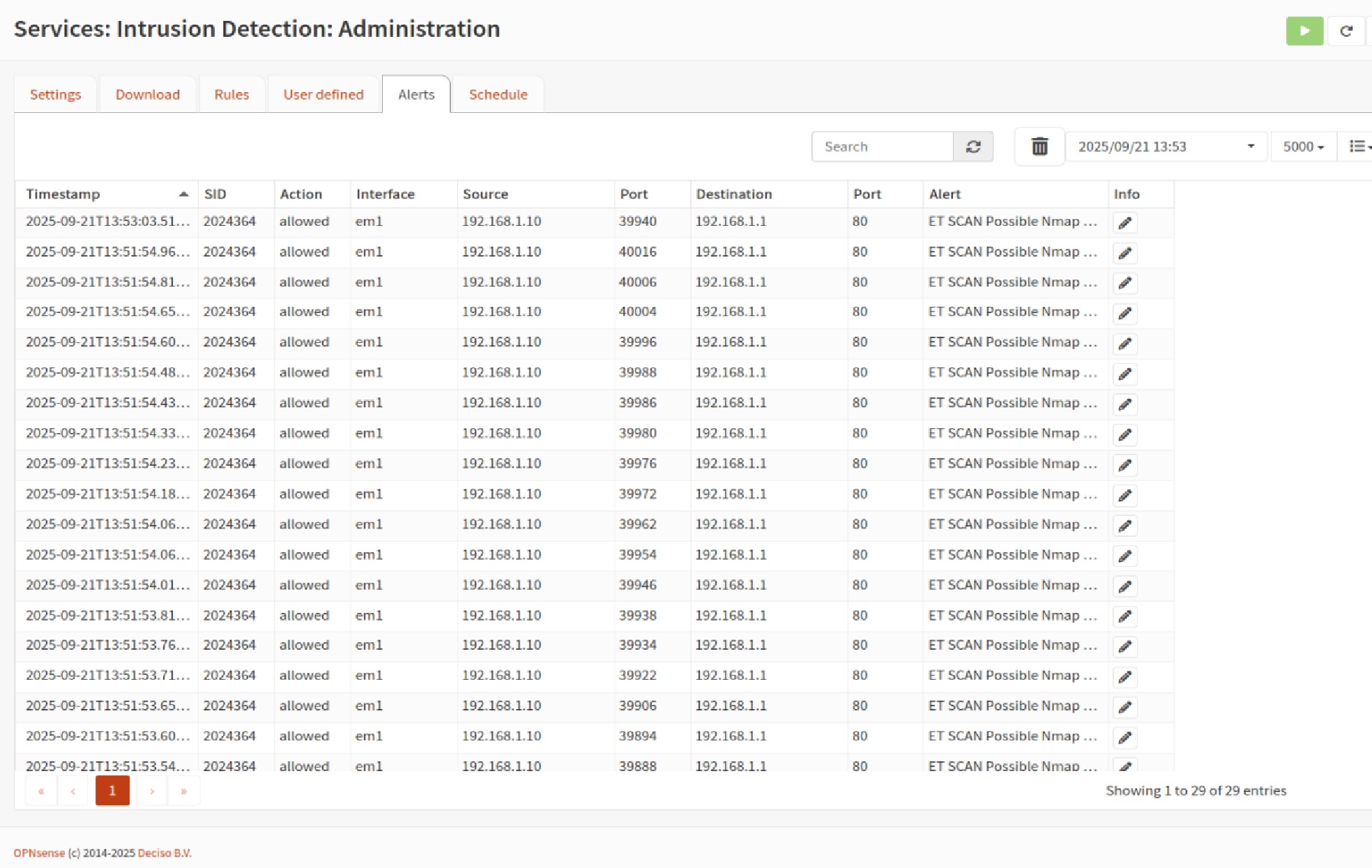
## Response and Mitigation

OPNSense Live View monitoring captured the attack activity. Additionally, the Ubuntu system showed no successful connection, confirming that the attack was blocked.

Live View



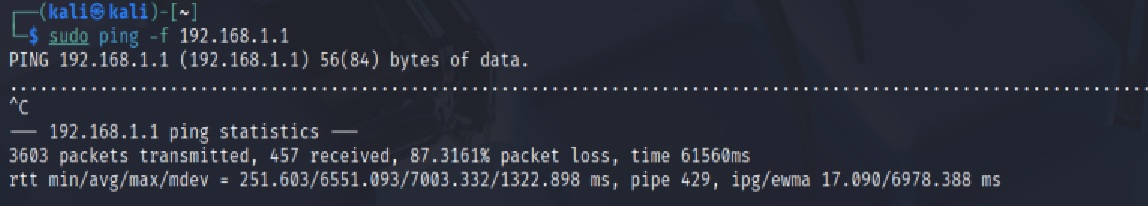
Victim Response -



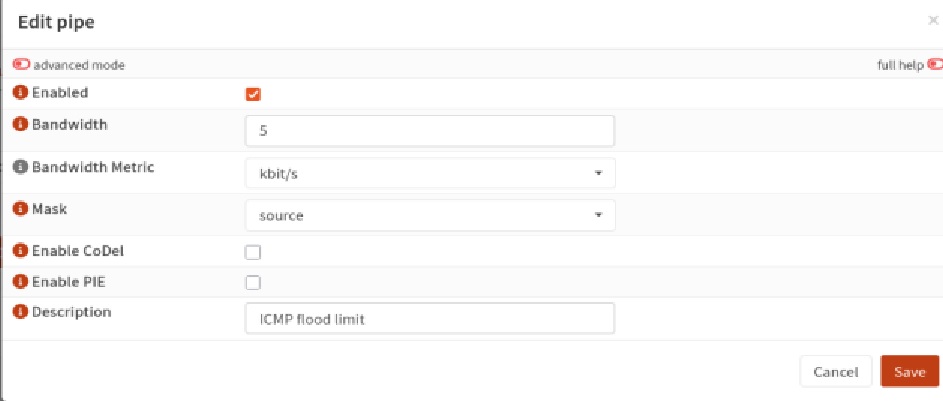
# Attack #2 — ICMP Flood (DDoS via Ping)

The second attack was an ICMP flood, where the attacker from Kali Linux generated thousands of ping requests in a short timeframe. This is a classic example of a Denial of Service (DoS) attack aimed at overwhelming the target with traffic.

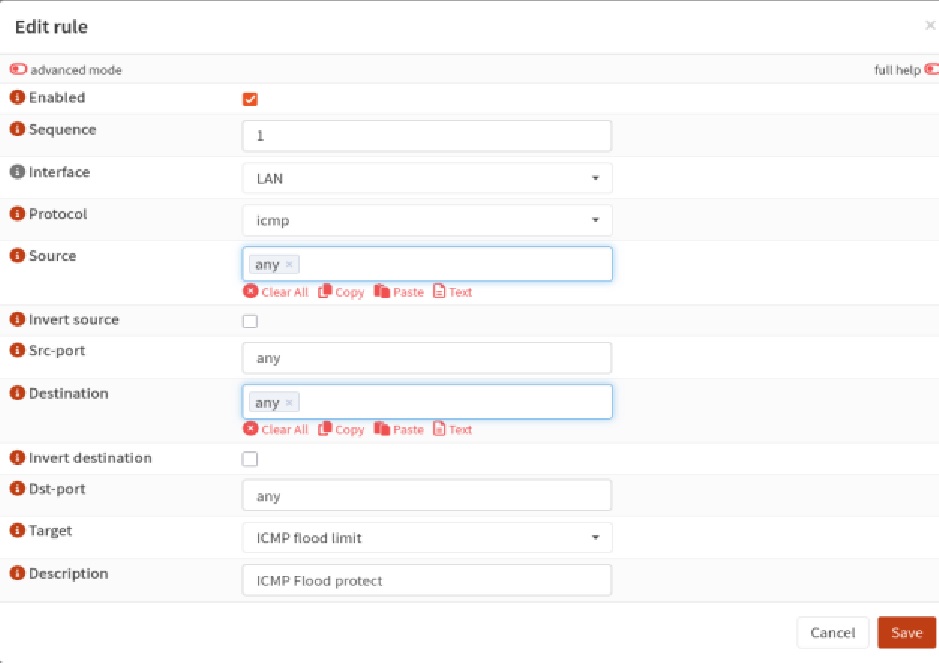
Kali -



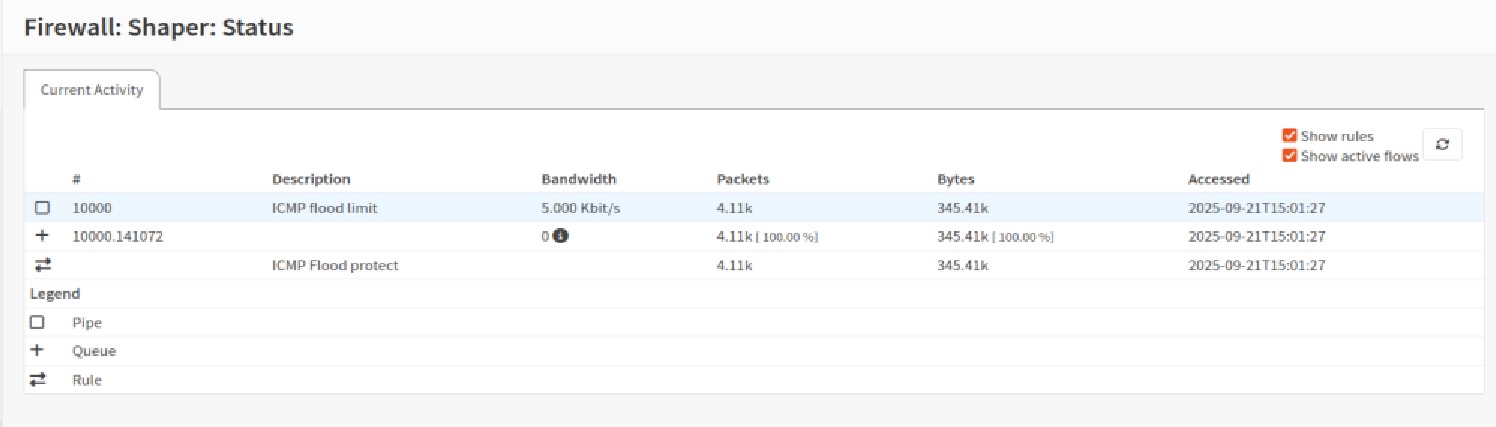
Pipes -



Rules -



Status -



## Attack Result and Defense

After configuring ICMP filtering rules in OPNSense, most packets were dropped. Although some initial ping requests were allowed, the majority of the attack traffic was blocked. This demonstrates the effectiveness of the implemented firewall policies in mitigating a DoS attack.

# Implemented Defense Mechanisms

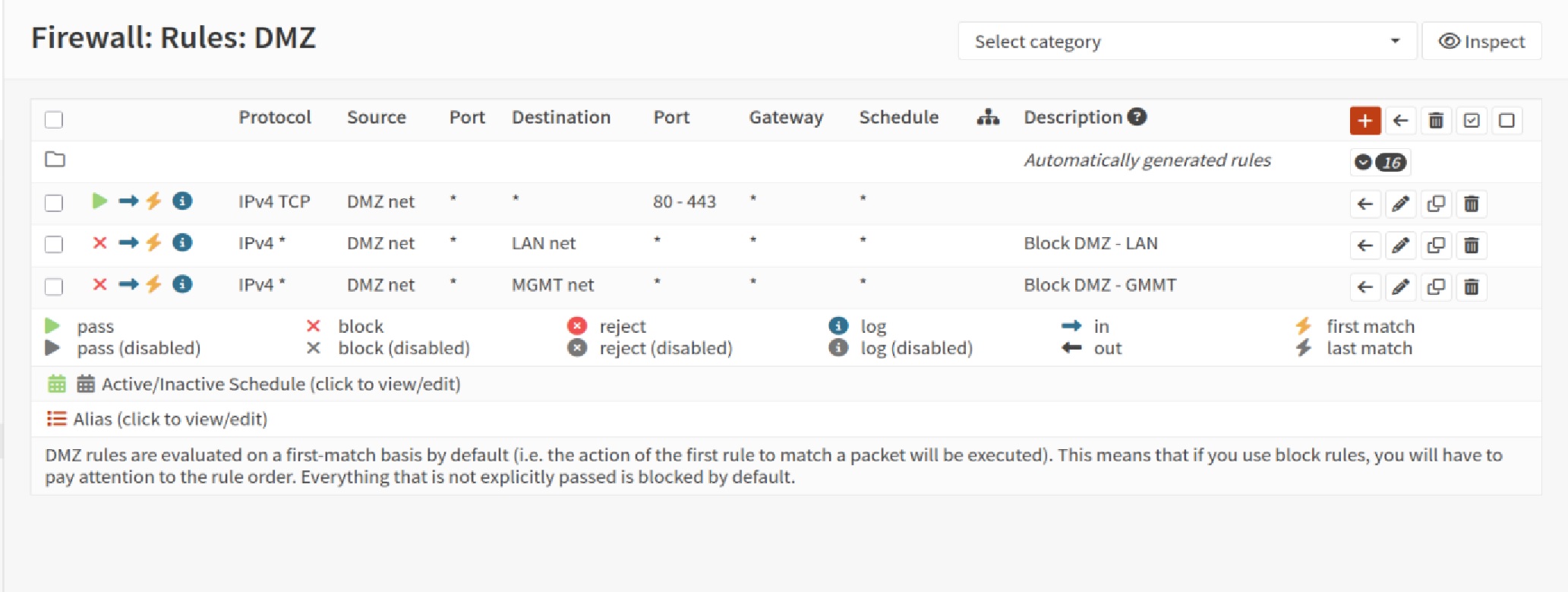
To block and detect the attacks, the following configurations were applied:

- OPNSense firewall rules (LAN → DMZ, WAN → LAN, etc.)

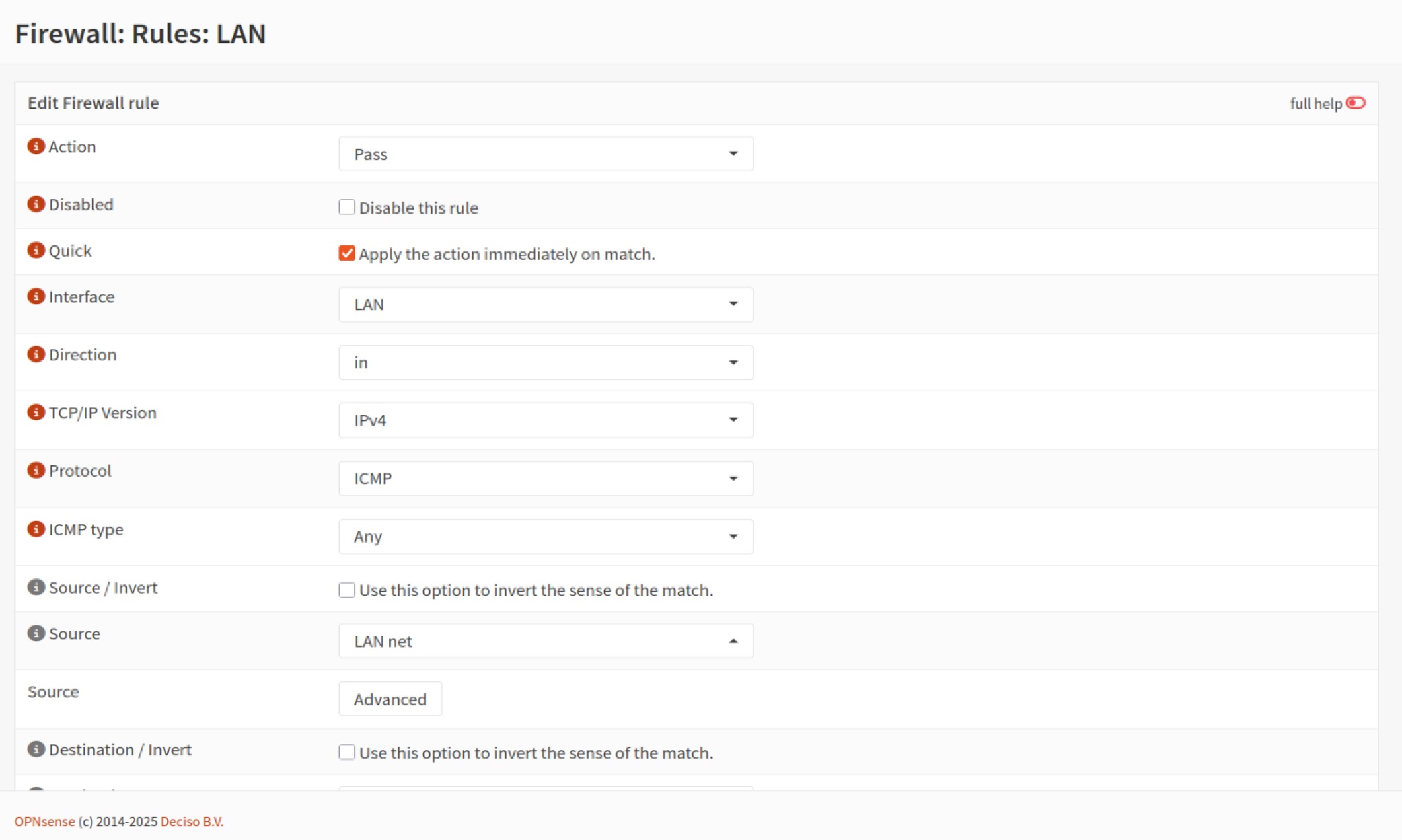
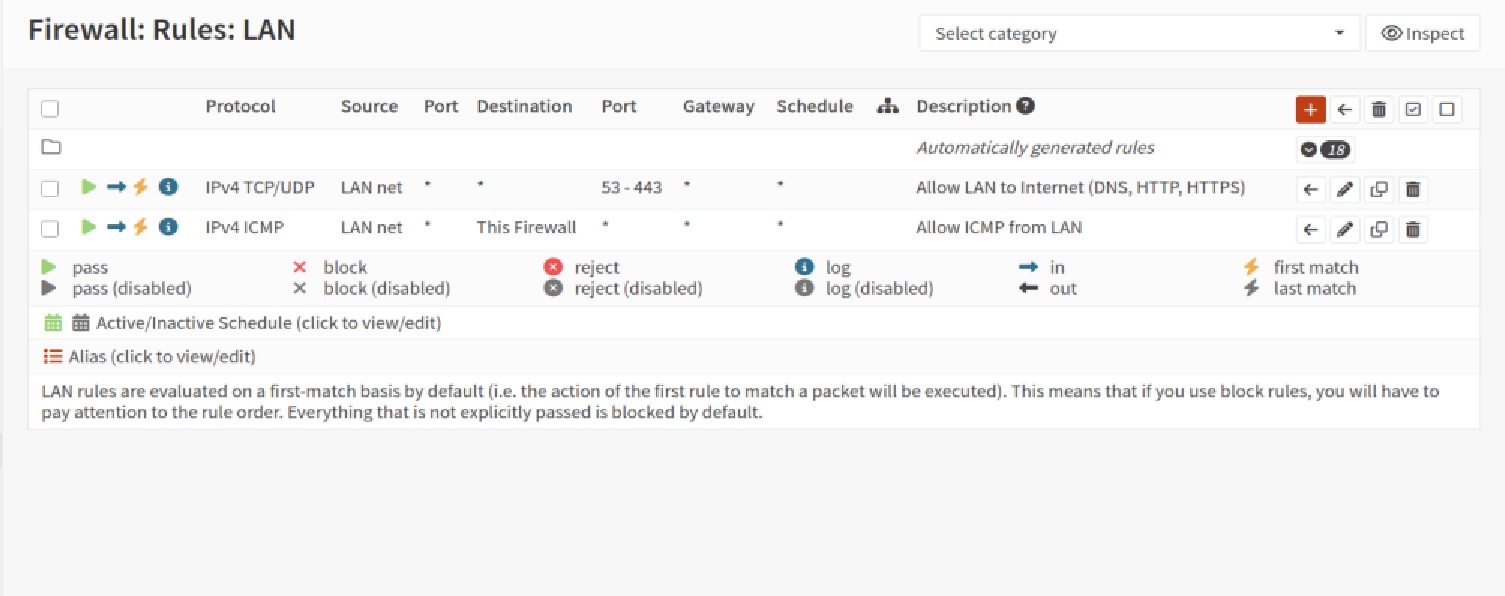
- Suricata IDS for attack detection

## Firewall Rule Configuration

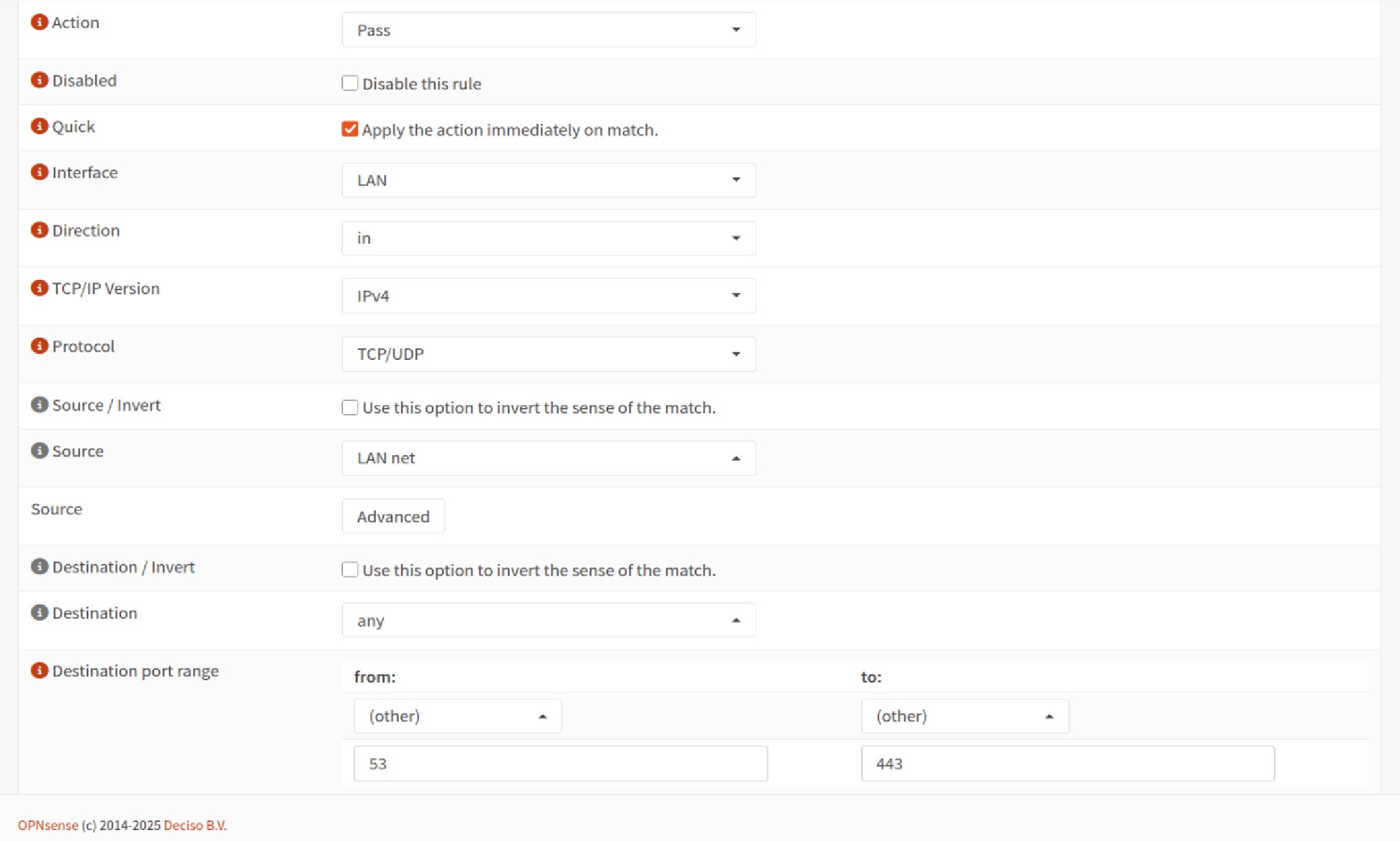
Firewall Rule -



Firewall Rule -

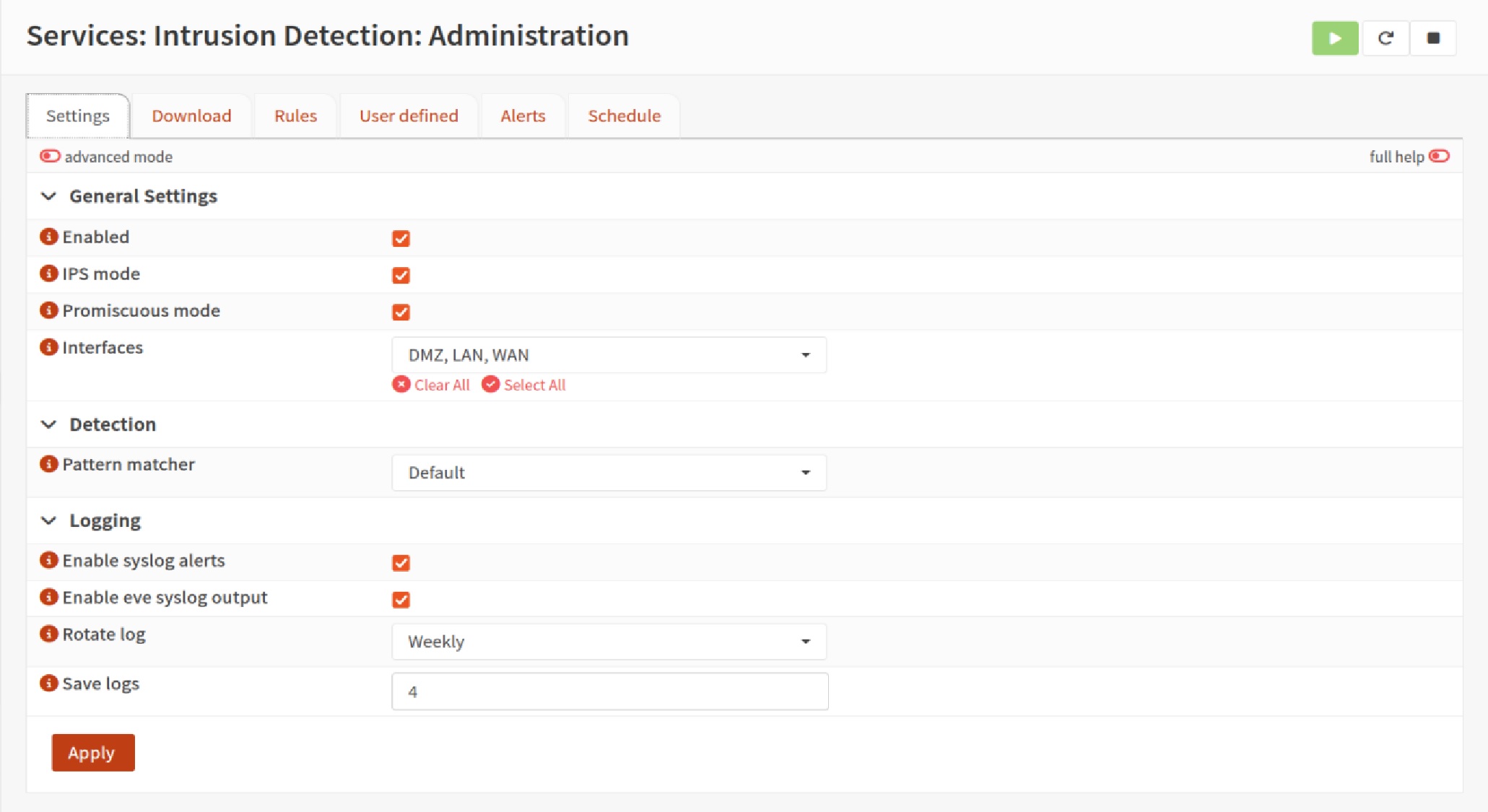


Firewall Rule - setting



## Suricata — Intrusion Detection System

Suricata Configuration - setting.jpg



# Conclusion

This lab demonstrated two network attacks: targeted service access and an ICMP flood. Both attacks were successfully detected and mitigated using OPNSense firewall rules and Suricata IDS. Notably, the ICMP flood was effectively suppressed by limiting and filtering the massive influx of ping requests, showing OPNSense’s strong protection capabilities.