Cybersecurity Homelab Documentation

Network Security and SOC Monitoring Platform

Author: Ahmed Ashraf GitHub: github.com/CSCOD3X Date: May 2026 Status: Active — Under Continuous Development

Table of Contents

1. Executive Summary
2. Physical Infrastructure
3. Network Architecture
4. Security Zones and Segmentation
5. Component Deep Dive
6. Firewall Configuration — pfSense
7. IDS/IPS Architecture — Suricata and Snort
8. SIEM — ELK Stack
9. XDR — Wazuh
10. SOAR — Shuffle and n8n
11. Threat Intelligence — OpenCTI
12. Digital Forensics — SANS SIFT and REMnux
13. Secondary SIEM — Splunk
14. Honeypot — T-Pot on Linode
15. Cloud Identity — Microsoft Entra ID
16. Remote Access — Tailscale VPN
17. DNS Security — Pi-hole
18. Storage — TerraMaster F4-425 NAS
19. Service Monitoring — Uptime Kuma
20. Attack Simulations and Validation
21. Detection Capabilities and MITRE ATT&CK
22. Log Flow Architecture
23. Kibana Dashboards
24. Maintenance and Troubleshooting
25. Planned Improvements
26. Port Reference
27. Quick Reference Commands

1. Executive Summary

Project Overview

This project implements a complete enterprise-grade Security Operations Center environment distributed across three physical machines, a dedicated NAS appliance, a cloud VPS, and a Raspberry Pi 5. The lab simulates a realistic multi-site enterprise network with dual firewalls, multiple isolated network segments, multi-layer intrusion detection and prevention, centralized log management, endpoint detection, automated incident response, cyber threat intelligence management, and digital forensics capability.

The environment provides hands-on experience with the exact tools, workflows, and architectures used in professional SOC, threat intelligence, and incident response roles.

Key Capabilities

- Edge IDS/IPS
  - Tool: Suricata on Raspberry Pi 5
  - Status: Running
- Internal IDS/IPS
  - Tool: Snort on pfSense-1 and pfSense-2
  - Status: Running
- Network Firewall
  - Tool: Dual pfSense CE with IPsec VPN
  - Status: Running
- Endpoint Detection
  - Tool: Wazuh XDR across 6+ agents
  - Status: Troubleshooting
- Primary SIEM
  - Tool: ELK Stack — 300,000+ events
  - Status: Running
- Secondary SIEM
  - Tool: Splunk — comparative enterprise SIEM
  - Status: In Progress
- SOAR
  - Tool: Shuffle + n8n automation
  - Status: In Progress
- Threat Intelligence
  - Tool: OpenCTI platform
  - Status: In Progress
- Honeypot
  - Tool: T-Pot on Linode — real attacker data
  - Status: In Progress
- DNS Security
  - Tool: Pi-hole with log forwarding
  - Status: Running
- Remote Access
  - Tool: Tailscale VPN
  - Status: Running
- Service Monitoring

    - Tool: Uptime Kuma
    - Status: Running
- Digital Forensics
    - Tool: SANS SIFT Workstation
    - Status: In Progress
- Malware Analysis
    - Tool: REMnux Workstation
    - Status: In Progress
- Cloud Identity
    - Tool: Microsoft Entra ID Connect
    - Status: In Progress
- Enterprise Storage
    - Tool: TerraMaster F4-425 iSCSI SAN
    - Status: In Progress

Key Achievements

- Suricata detection rules: 65,796 — daily updated
- Snort rule sets: ET Open + Snort VRT
- Suricata events indexed: 300,000+
- Firewall logs indexed: 140,000+
- Wazuh enrolled agents: 6+ endpoints
- Kibana dashboards: 3 professional dashboards
- Attack types validated: 4 simulated and detected
- Physical machines: 3 + 1 NAS + 1 cloud VPS
- Network segments: 6 isolated segments
- IDS/IPS layers: 3 layers of detection
- SIEM platforms: 2 — ELK and Splunk
- CTI platform: OpenCTI
- DFIR workstations: 2 — SIFT and REMnux

2. Physical Infrastructure

Hardware

- ThinkPad Laptop
    - Specs: 32GB RAM
    - Role: SOC controller, pfSense-1, Kali
- Desktop PC
    - Specs: 16GB RAM
    - Role: pfSense-2, Windows VMs via VirtualBox
- Dell Optiplex 7090
    - Specs: Dedicated
    - Role: Proxmox hypervisor — SIFT, REMnux, CTI VM
- TerraMaster F4-425
    - Specs: 4-bay, 10GbE
    - Role: iSCSI SAN, file storage

- Raspberry Pi 5
  - Specs: 8GB RAM
  - Role: Suricata edge sensor, Pi-hole, NAS, Tailscale
- Linode VPS
  - Specs: Cloud
  - Role: T-Pot honeypot — public internet exposure

Network Hardware

- Core Switch
  - Model: Cisco Catalyst 3560CX
  - Role: Layer 3 routing, inter-VLAN
- Access Switch
  - Model: Cisco Catalyst 2960CX
  - Role: Layer 2 access, SPAN port
- Link
  - Model: LACP EtherChannel
  - Role: Aggregated uplink between switches
- SPAN Port
  - Model: Cisco hardware
  - Role: Mirrors all traffic to Raspberry Pi eth0

Hypervisors

- ThinkPad Laptop
  - Hypervisor: VirtualBox
  - Hosts: Ubuntu NOC VM, pfSense-1, Kali Linux
- Desktop PC
  - Hypervisor: VirtualBox
  - Hosts: pfSense-2, Windows DC, PC-1, PC-2
- Dell Optiplex 7090
  - Hypervisor: Proxmox
  - Hosts: SANS SIFT VM, REMnux VM, Monitoring and CTI VM

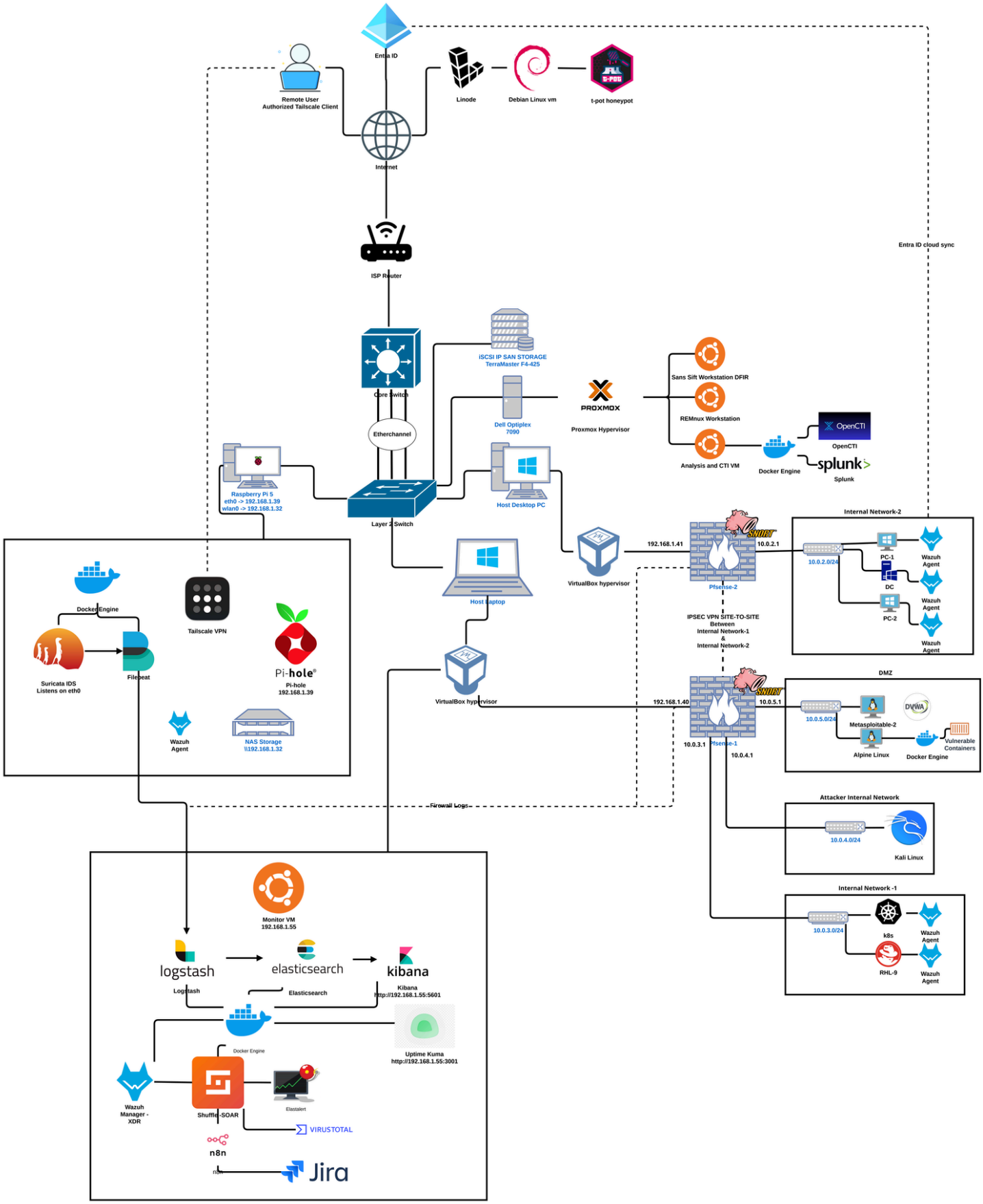
Proxmox VM Allocation — Dell Optiplex 7090

- SANS SIFT Workstation
  - Purpose: Digital forensics and IR
  - Key Tools: Volatility, Autopsy, Plaso, RegRipper
- REMnux Workstation
  - Purpose: Malware analysis
  - Key Tools: Remnux tools, YARA, binary analysis
- Monitoring and CTI VM
  - Purpose: Threat intelligence and secondary SIEM
  - Key Tools: Splunk, OpenCTI via Docker

Resource Allocation

- ThinkPad Laptop
  - Total RAM: 32GB
  - Allocated: ~28GB
  - Buffer: ~4GB
- Desktop PC
  - Total RAM: 16GB
  - Allocated: ~14GB
  - Buffer: ~2GB
- Dell Optiplex 7090
  - Total RAM: Dedicated
  - Allocated: Proxmox managed
  - Buffer: Per VM
- Raspberry Pi 5
  - Total RAM: 8GB
  - Allocated: ~3GB
  - Buffer: ~5GB

3. Network Architecture



Network Segments

Network	Subnet	Gateway	Protected By	Purpose
Home LAN	192.168.1.0/24	192.168.1.1	Router	Management, SOC tools
Internal Network 1	10.0.3.0/24	10.0.3.1	pfSense-1 + Snort	Linux workloads
Internal Network 2	10.0.2.0/24	10.0.2.1	pfSense-2 + Snort	Windows workloads
DMZ	10.0.5.0/24	10.0.5.1	pfSense-1 + Snort	Vulnerable targets
Attacker Network	10.0.4.0/24	10.0.4.1	pfSense-1 + Snort	Isolated Kali Linux
Tailscale Mesh	100.x.x.x/32	Tailscale	WireGuard	Secure remote access
Storage VLAN	VLAN 88	N/A	Isolated	iSCSI SAN fabric
Management VLAN	VLAN 99	192.168.1.1	Router	Device management

Complete Device IP Reference

Home LAN — 192.168.1.0/24

Device	IP	Role
ISP Router	192.168.1.1	Default gateway
Raspberry Pi wlan0	192.168.1.32	Wireless interface
Raspberry Pi eth0	192.168.1.39	Wired — Suricata listens here
Ubuntu NOC VM	192.168.1.55	SOC controller
pfSense-1 WAN	192.168.1.40	Site A firewall external
pfSense-2 WAN	192.168.1.41	Site B firewall external
Kali Linux	192.168.1.112	Attack machine

Internal Network 1 — 10.0.3.0/24

Device	IP	Role
pfSense-1 LAN	10.0.3.1	Gateway — Snort IPS inline
k8s Node	10.0.3.17	Kubernetes container host
Red Hat Linux	10.0.3.13	Linux production server

Internal Network 2 — 10.0.2.0/24

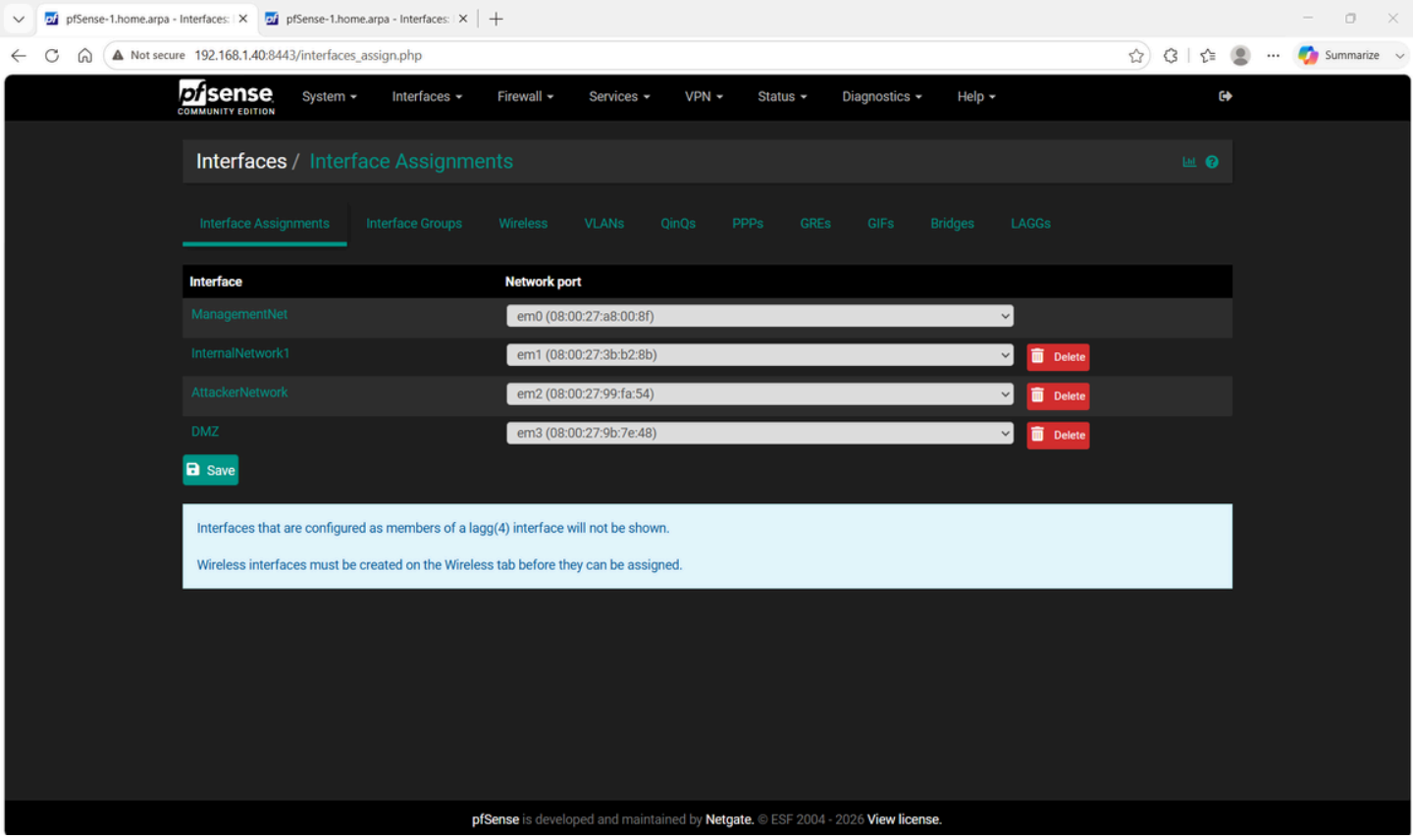
Device	IP	Role
pfSense-2 LAN	10.0.2.1	Gateway — Snort IPS inline
Domain Controller	10.0.2.100	Active Directory, DNS, DHCP
PC-1	10.0.2.5	Windows 10 endpoint
PC-2	10.0.2.6	Windows 10 endpoint

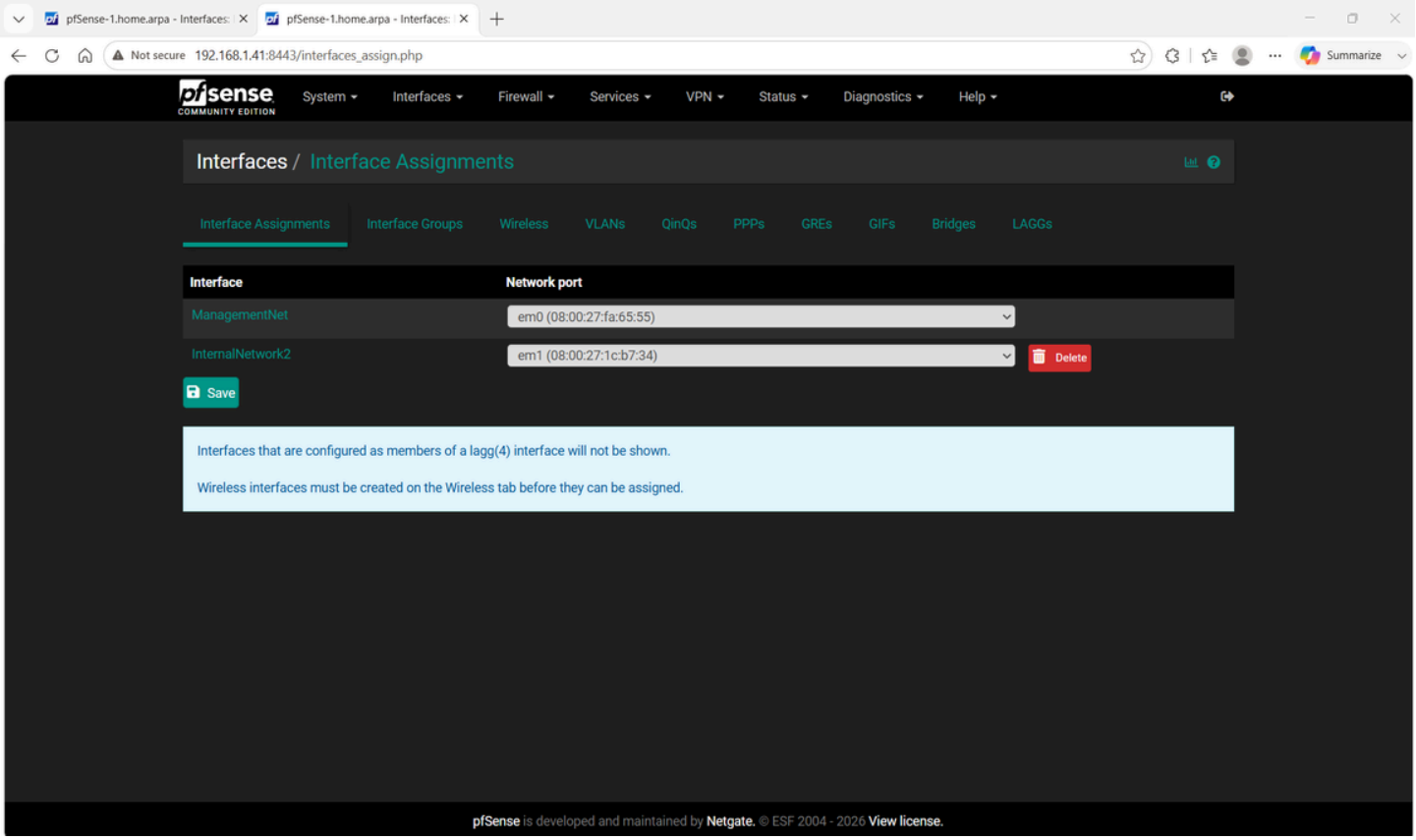
DMZ — 10.0.5.0/24

Device	IP	Role
pfSense-1 DMZ	10.0.5.1	DMZ gateway — Snort IPS inline
Metasploitable-2	10.0.5.x	Intentionally vulnerable Linux target
Alpine Linux	10.0.5.x	Lightweight Linux target
DVWA	10.0.5.x	Damn Vulnerable Web Application

Attacker Network — 10.0.4.0/24

Device	IP	Role
pfSense-1 ATK	10.0.4.1	Attacker network gateway
Kali Linux	10.0.4.4	Isolated attack machine





4. Security Zones and Segmentation

Zone Architecture

The environment is organized into the following trust zones:

- Home LAN / Management (192.168.1.0/24): SOC tools, sensors, pfSense WAN interfaces. Suricata monitors all traffic on this segment.
- Internal Network 1 (10.0.3.0/24): Linux workloads behind pfSense-1 with Snort IPS inline
- Internal Network 2 (10.0.2.0/24): Windows workloads behind pfSense-2 with Snort IPS inline
- DMZ (10.0.5.0/24): Vulnerable targets — no access to internal networks
- Attacker Network (10.0.4.0/24): Isolated Kali Linux — DMZ access only

Traffic Policy Matrix

Source	Destination	Policy	Notes
Internal Net 1	Internet	Allow web and DNS	Via NAT
Internal Net 1	Internal Net 2	Allow all	Via IPsec VPN
Internal Net 1	SOC Server	Wazuh and syslog only	Ports 1514, 5140
Internal Net 2	Internet	Allow web and DNS	Via NAT
Internal Net 2	Internal Net 1	Allow all	Via IPsec VPN
Internal Net 2	SOC Server	Wazuh and syslog only	Ports 1514, 5140
DMZ	Internet	Web only	Restricted
DMZ	Internal networks	Deny	Hard block
DMZ	SOC Server	Wazuh and syslog only	Monitoring only
Attacker Net	DMZ	Allow all	Lab testing
Attacker Net	Internal networks	Deny	Hard block
Attacker Net	Home LAN	Deny	Hard block
Home LAN	pfSense GUIs	HTTPS and SSH	Management only

5. Component Deep Dive

Software Stack

- Firewall
  - Technology: pfSense CE
  - Version: 2.7.2
  - Host: Laptop + Desktop
- Edge IDS/IPS
  - Technology: Suricata
  - Version: 7.0.5
  - Host: Raspberry Pi
- Internal IDS/IPS
  - Technology: Snort
  - Version: Latest
  - Host: pfSense-1 and pfSense-2
- XDR
  - Technology: Wazuh
  - Version: 4.9.0
  - Host: Ubuntu NOC VM
- Log Storage
  - Technology: Elasticsearch
  - Version: 7.17.15
  - Host: Ubuntu NOC VM
- Log Processing
  - Technology: Logstash
  - Version: 7.17.15
  - Host: Ubuntu NOC VM
- Visualization
  - Technology: Kibana
  - Version: 7.17.15
  - Host: Ubuntu NOC VM
- Log Shipping
  - Technology: Filebeat
  - Version: 7.17.15
  - Host: Wazuh container
- SOAR
  - Technology: Shuffle
  - Version: Latest
  - Host: Ubuntu NOC VM
- Workflow Automation
  - Technology: n8n
  - Version: Latest
  - Host: Ubuntu NOC VM

- Ticketing
  - Technology: Jira
  - Version: Cloud free
  - Host: External
- Threat Intel API
  - Technology: VirusTotal
  - Version: v3
  - Host: Via Shuffle
- Threat Intelligence
  - Technology: OpenCTI
  - Version: Latest
  - Host: Monitoring and CTI VM
- Secondary SIEM
  - Technology: Splunk
  - Version: Latest
  - Host: Monitoring and CTI VM
- Honeypot
  - Technology: T-Pot
  - Version: Latest
  - Host: Linode VPS
- DNS Security
  - Technology: Pi-hole
  - Version: Latest
  - Host: Raspberry Pi
- Remote VPN
  - Technology: Tailscale
  - Version: Latest
  - Host: All machines
- Service Monitoring
  - Technology: Uptime Kuma
  - Version: 1.23.0
  - Host: Ubuntu NOC VM
- DFIR
  - Technology: SANS SIFT
  - Version: Latest
  - Host: Dell Optiplex Proxmox
- Malware Analysis
  - Technology: REMnux
  - Version: Latest
  - Host: Dell Optiplex Proxmox
- Cloud Identity
  - Technology: Microsoft Entra ID
  - Version: Free tier
  - Host: Cloud
- Storage
  - Technology: TerraMaster F4-425

    - Version: TOS
    - Host: Standalone NAS
- Attack Machine
    - Technology: Kali Linux
    - Version: Latest
    - Host: Laptop VM

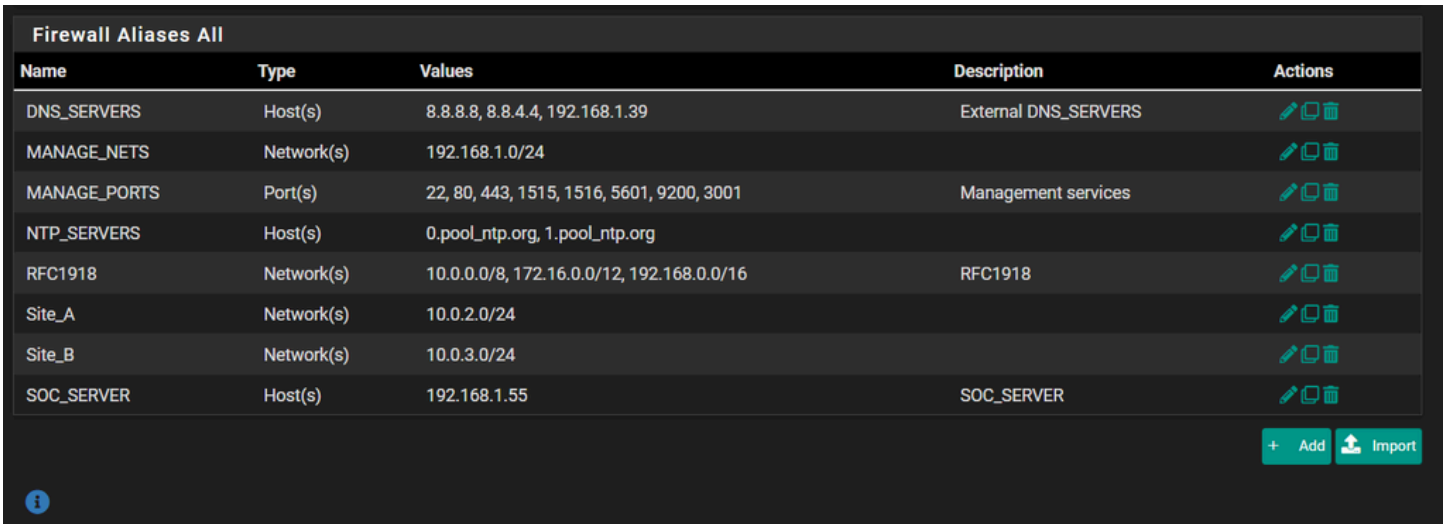
Service Endpoints

Service	URL	Purpose
Kibana	http://192.168.1.55:5601	Primary security dashboards
Uptime Kuma	http://192.168.1.55:3001	Service monitoring
Shuffle SOAR	http://192.168.1.55:3002	Automated response
n8n	http://192.168.1.55:5678	Workflow automation
Elasticsearch	http://192.168.1.55:9200	Log queries and API
Wazuh API	http://192.168.1.55:55000	XDR management
pfSense-1 GUI	https://192.168.1.40:8443	Site A firewall
pfSense-2 GUI	https://192.168.1.41:8443	Site B firewall
Pi-hole GUI	http://192.168.1.39:80	DNS management

6. Firewall Configuration — pfSense

pfSense-1 — Site A

Firewall Aliases:

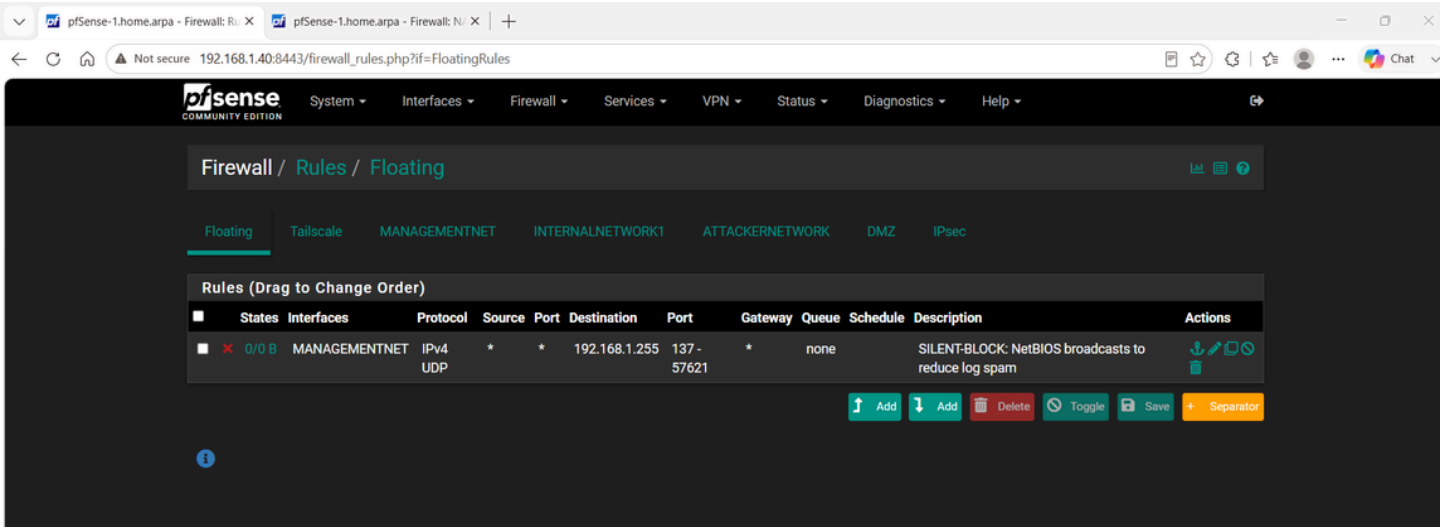


Firewall Aliases All

Name	Type	Values	Description	Actions
DNS_SERVERS	Host(s)	8.8.8.8, 8.8.4.4, 192.168.1.39	External DNS_SERVERS	
MANAGE_NETS	Network(s)	192.168.1.0/24		
MANAGE_PORTS	Port(s)	22, 80, 443, 1515, 1516, 5601, 9200, 3001	Management services	
NTP_SERVERS	Host(s)	0.pool_ntp.org, 1.pool_ntp.org		
RFC1918	Network(s)	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	RFC1918	
Site_A	Network(s)	10.0.2.0/24		
Site_B	Network(s)	10.0.3.0/24		
SOC_SERVER	Host(s)	192.168.1.55	SOC_SERVER	

+ Add Import

Floating Rules:



pfSense-1.home.arpa - Firewall: Ru pfSense-1.home.arpa - Firewall: Nu

Not secure 192.168.1.40:8443/firewall_rules.php?if=FloatingRules

pfsense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / Floating

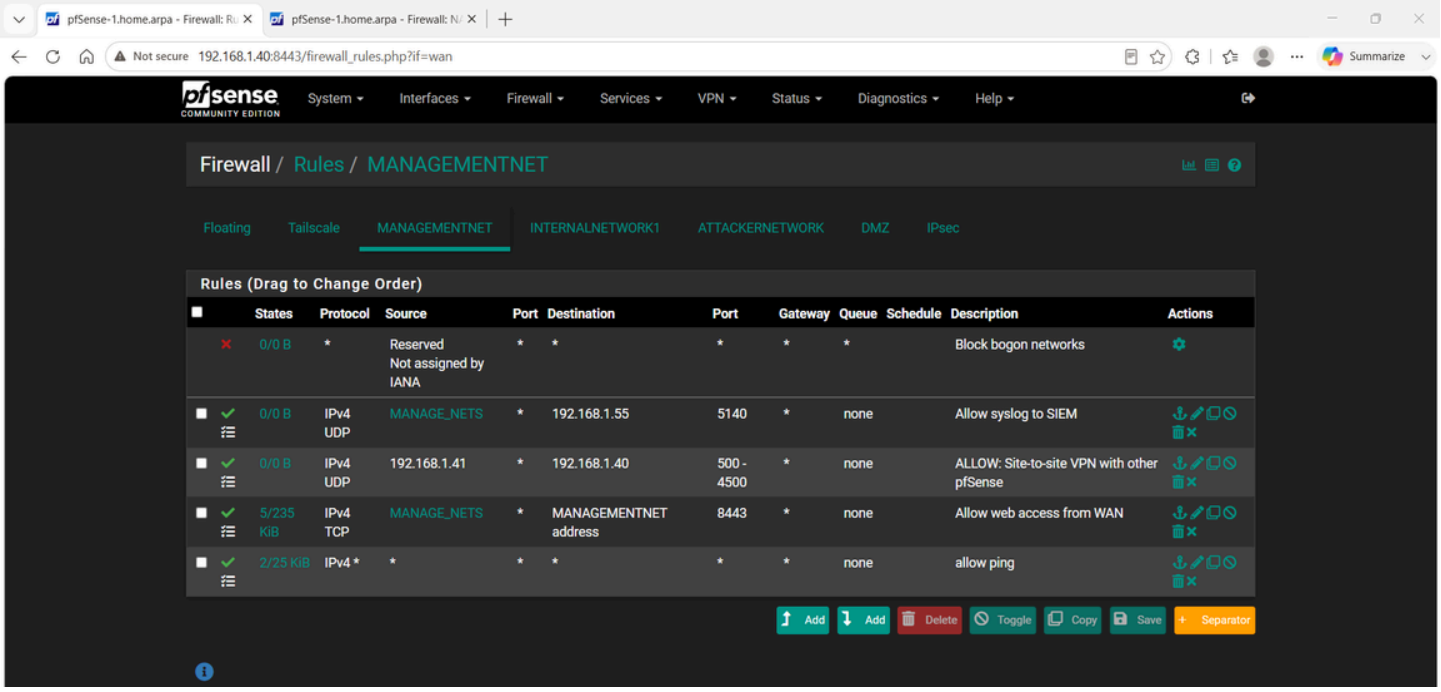
Floating Tailscale MANAGEMENTNET INTERNALNETWORK1 ATTACKERNETWORK DMZ IPsec

Rules (Drag to Change Order)

States	Interfaces	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	MANAGEMENTNET	IPv4 UDP	*	*	192.168.1.255	137 - 57621	*	none		SILENT-BLOCK: NetBIOS broadcasts to reduce log spam	

Add Add Delete Toggle Save + Separator

Management Network Rules:



pfSense-1.home.arpa - Firewall: Ru pfSense-1.home.arpa - Firewall: Nu

Not secure 192.168.1.40:8443/firewall_rules.php?if=wan

pfsense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / MANAGEMENTNET

Floating Tailscale MANAGEMENTNET INTERNALNETWORK1 ATTACKERNETWORK DMZ IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
0/0 B	IPv4 UDP	MANAGE_NETS	*	192.168.1.55	5140	*	none		Allow syslog to SIEM	
0/0 B	IPv4 UDP	192.168.1.41	*	192.168.1.40	500 - 4500	*	none		ALLOW: Site-to-site VPN with other pfSense	
5/235 KiB	IPv4 TCP	MANAGE_NETS	*	MANAGEMENTNET address	8443	*	none		Allow web access from WAN	
2/25 KiB	IPv4 *	*	*	*	*	*	none		allow ping	

Add Add Delete Toggle Copy Save + Separator

Internal Network 1 Rules:

Not secure 192.168.1.40:8443/firewall_rules.php?if=lan

Floating | Tailscale | MANAGEMENTNET | INTERNALNETWORK1 | ATTACKERNETWORK | DMZ | IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	*	*	INTERNALNETWORK1 Address	8443	*	*		Anti-Lockout Rule	
0/0 B	IPv4 *	10.0.3.0/24	*	10.0.3.0/24	*	*	none		Allow Full Internal Network Access	
0/0 B	IPv4 TCP/UDP	10.0.3.0/24	*	DNS_SERVERS	53 (DNS)	*	none		ALLOW: DNS resolution	
0/0 B	IPv4 TCP	10.0.3.0/24	*	*	80 - 443	*	none		ALLOW: Web browsing	
0/0 B	IPv4 TCP	*	*	*	853 (DNS over TLS)	*	none		Block DNS-over-TLS to prevent bypassing Pi-hole	
0/0 B	IPv4 TCP/UDP	192.168.1.39	*	*	53 (DNS)	*	none		Bypass Pi-hole DNS Redirect to allow Pi-hole to work	
0/0 B	IPv4 TCP	MANAGE_NETS	*	This Firewall (self)	22 (SSH)	*	none		ALLOW: SSH management	
0/0 B	IPv4 TCP	10.0.3.0/24	*	SOC_SERVER	1515 - 1516	*	none		ALLOW: Wazuh agent communication	
0/0 B	IPv4 TCP/UDP	10.0.3.0/24	*	SOC_SERVER	5140	*	none		ALLOW: pfSense syslog to SIEM	
0/0 B	IPv4 *	10.0.3.0/24	*	! RFC1918	*	*	none		ALLOW: General internet access	
0/0 B	IPv4 *	10.0.3.0/24	*	10.0.2.0/24	*	*	none		Allow to Internal 2 via VPN	
0/0 B	IPv4 TCP/UDP	INTERNALNETWORK1 subnets	*	192.168.1.55	1514 - 55000	*	none		wazuh agent to manager	
0/0 B	IPv4 *	10.0.3.0/24	*	*	*	*	none		Block Everything else	
0/0 B	IPv4 *	INTERNALNETWORK1 subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	INTERNALNETWORK1 subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Attacker Network Rules:

Firewall / Rules / ATTACKERNETWORK

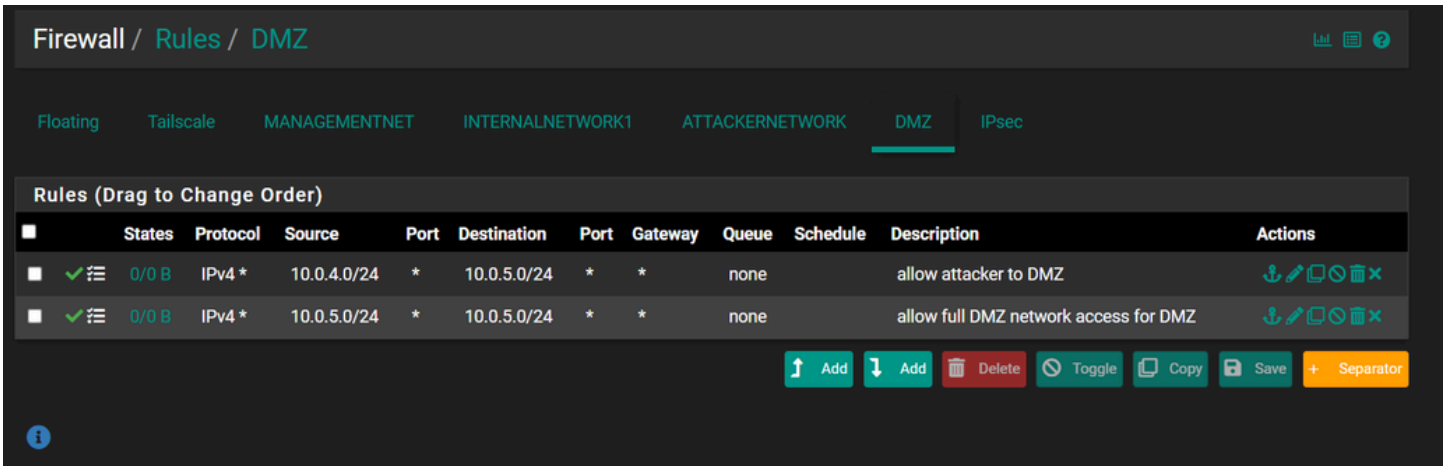
Floating | Tailscale | MANAGEMENTNET | INTERNALNETWORK1 | ATTACKERNETWORK | DMZ | IPsec

Rules (Drag to Change Order)

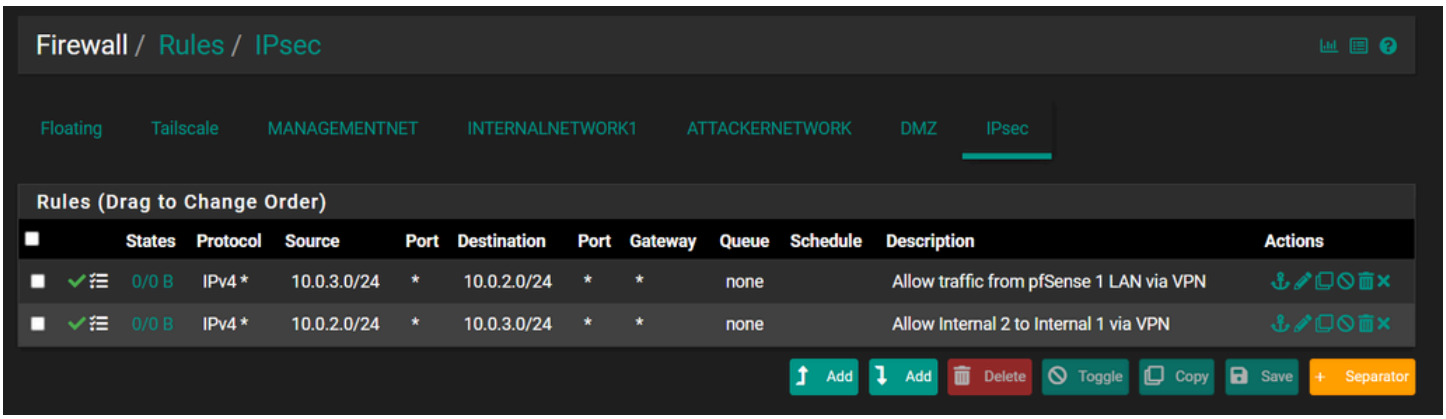
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	10.0.4.0/24	*	! RFC1918	*	*	none		allow internet access for attacker	
0/0 B	IPv4 *	10.0.4.0/24	*	10.0.5.0/24	*	*	none		allow attacker to DMZ	
0/0 B	IPv4 *	10.0.4.0/24	*	10.0.4.0/24	*	*	none		allow full attacker network access for attacker	
0/0 B	IPv4 *	10.0.4.0/24	*	*	*	*	none			

Add | Add | Delete | Toggle | Copy | Save | + Separator

DMZ Rules:

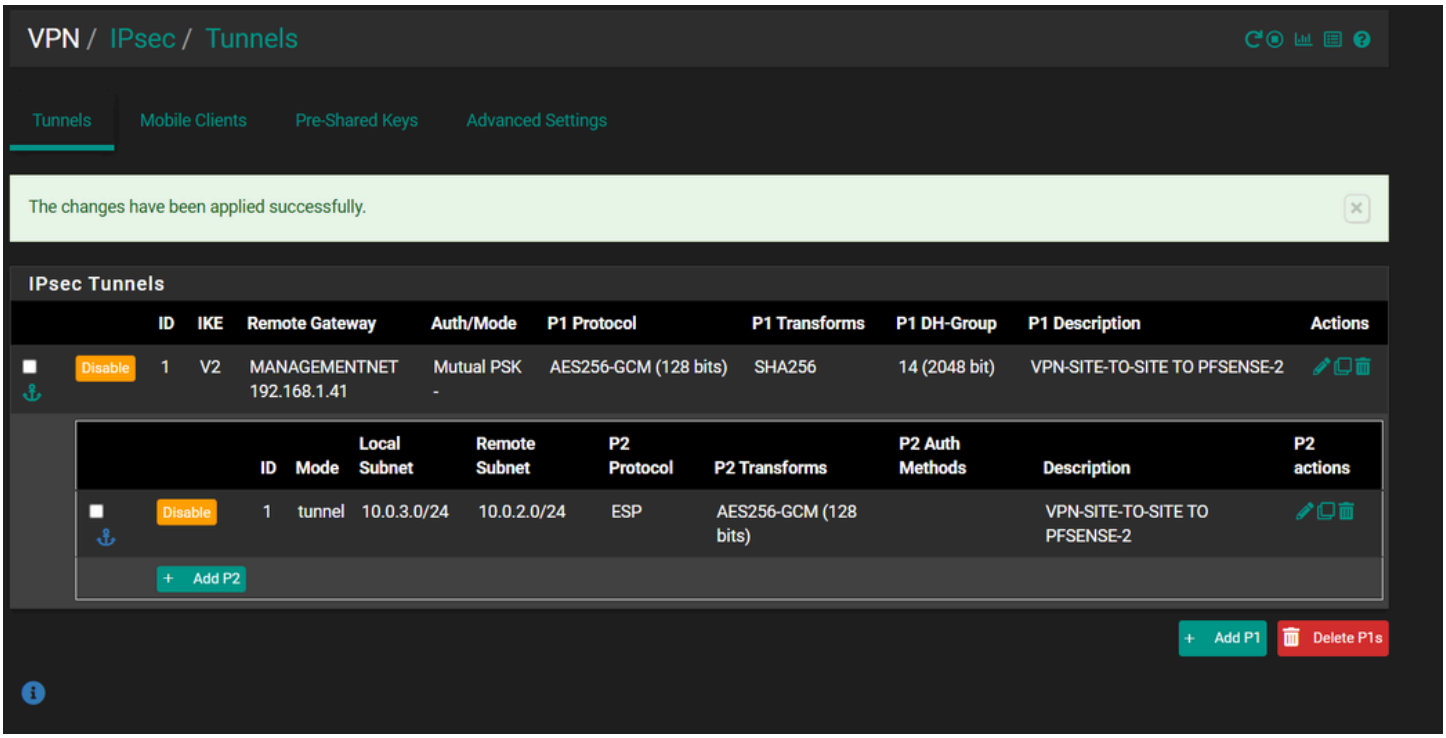


IPSEC Rules:

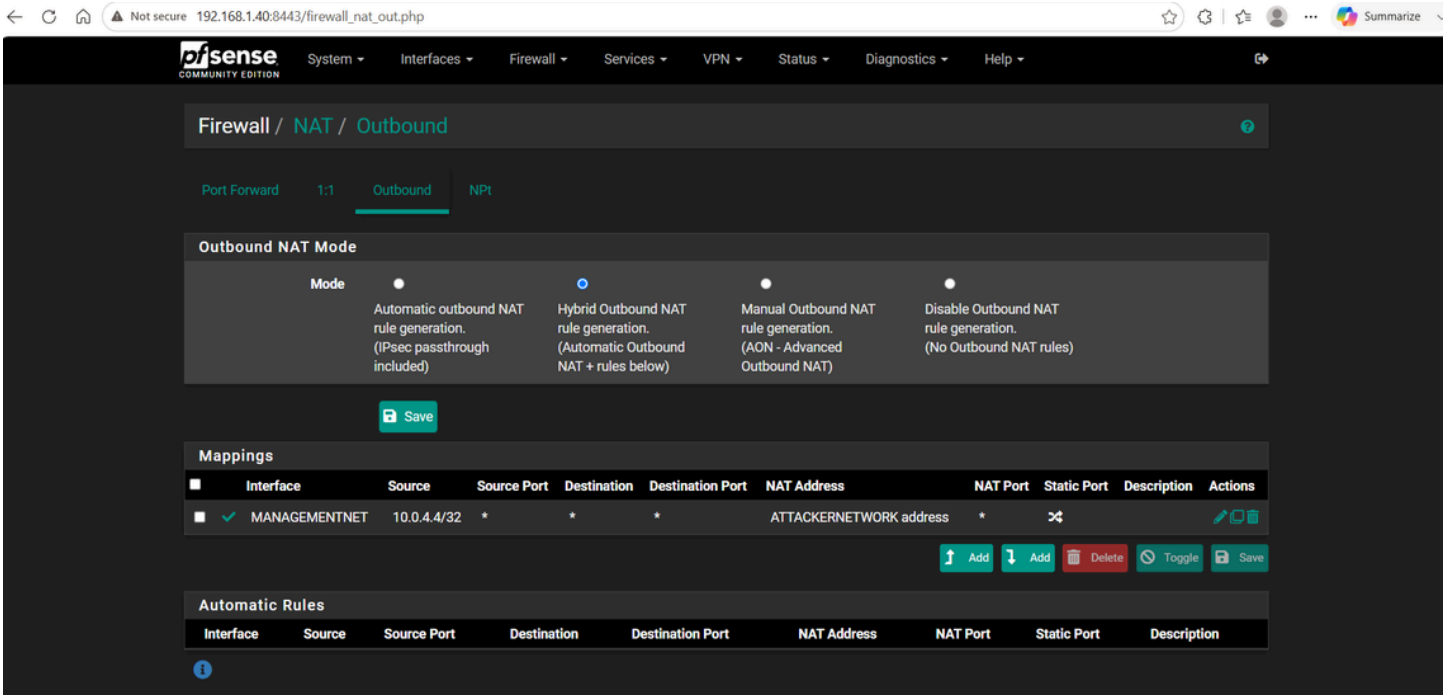


IPsec VPN Configuration:

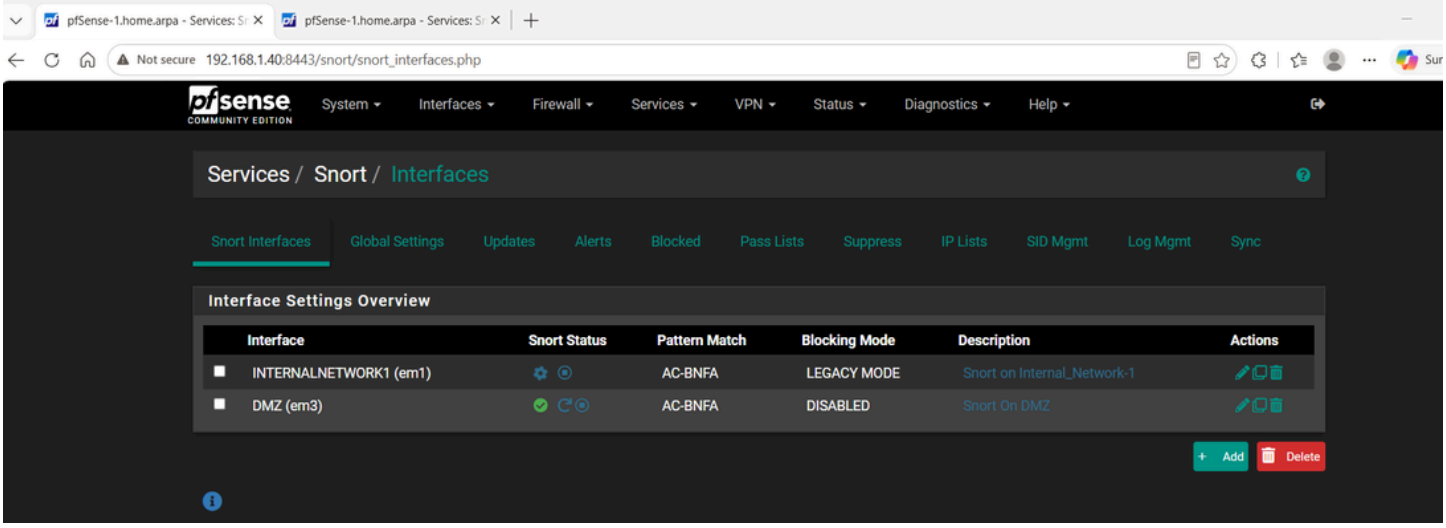
- Protocol: IKEv2
- Local subnet: 10.0.3.0/24
- Remote subnet: 10.0.2.0/24
- Remote gateway: 192.168.1.41
- Authentication: Pre-shared key
- Encryption: AES-256
- Hash: SHA-256
- DH Group: 14
- Phase 1 lifetime: 28800 seconds
- Phase 2 lifetime: 3600 seconds



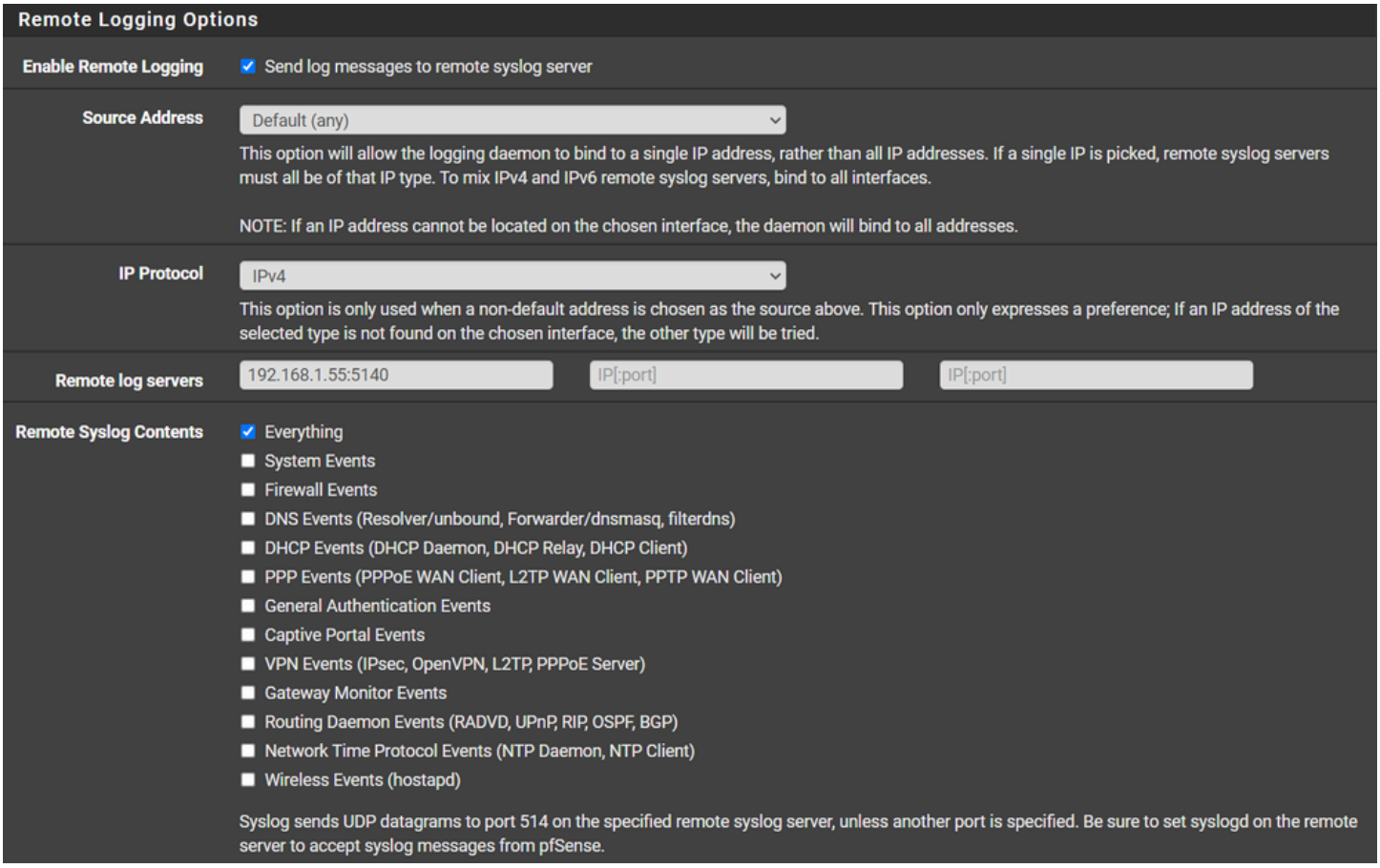
NAT Outbound Rules:



Snort:

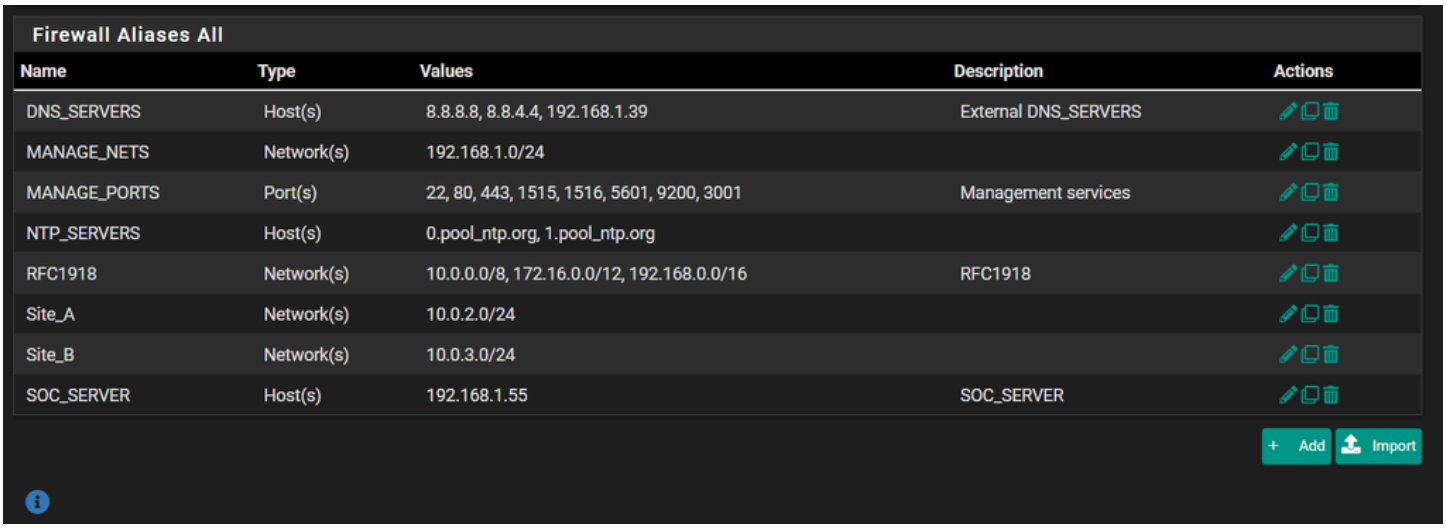


Remote Syslog to Logstash:



pfSense-2 — Site B

Aliases:

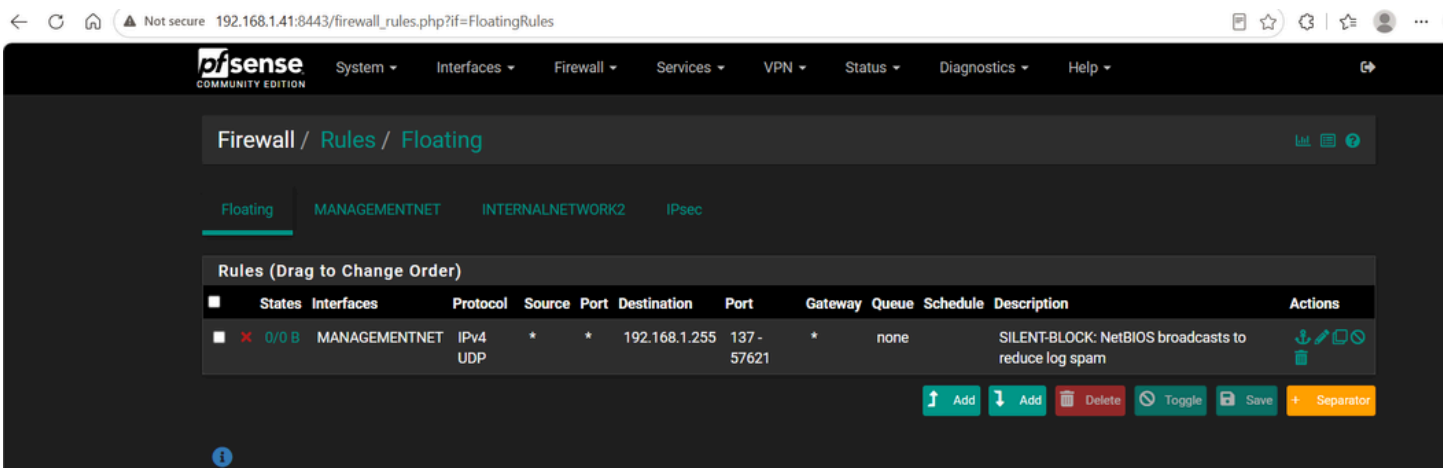


Firewall Aliases All

Name	Type	Values	Description	Actions
DNS_SERVERS	Host(s)	8.8.8.8, 8.8.4.4, 192.168.1.39	External DNS_SERVERS	
MANAGE_NETS	Network(s)	192.168.1.0/24		
MANAGE_PORTS	Port(s)	22, 80, 443, 1515, 1516, 5601, 9200, 3001	Management services	
NTP_SERVERS	Host(s)	0.pool_ntp.org, 1.pool_ntp.org		
RFC1918	Network(s)	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	RFC1918	
Site_A	Network(s)	10.0.2.0/24		
Site_B	Network(s)	10.0.3.0/24		
SOC_SERVER	Host(s)	192.168.1.55	SOC_SERVER	

+ Add Import

Floating Rules:



Not secure 192.168.1.41:8443/firewall_rules.php?if=FloatingRules

pfsense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / Floating

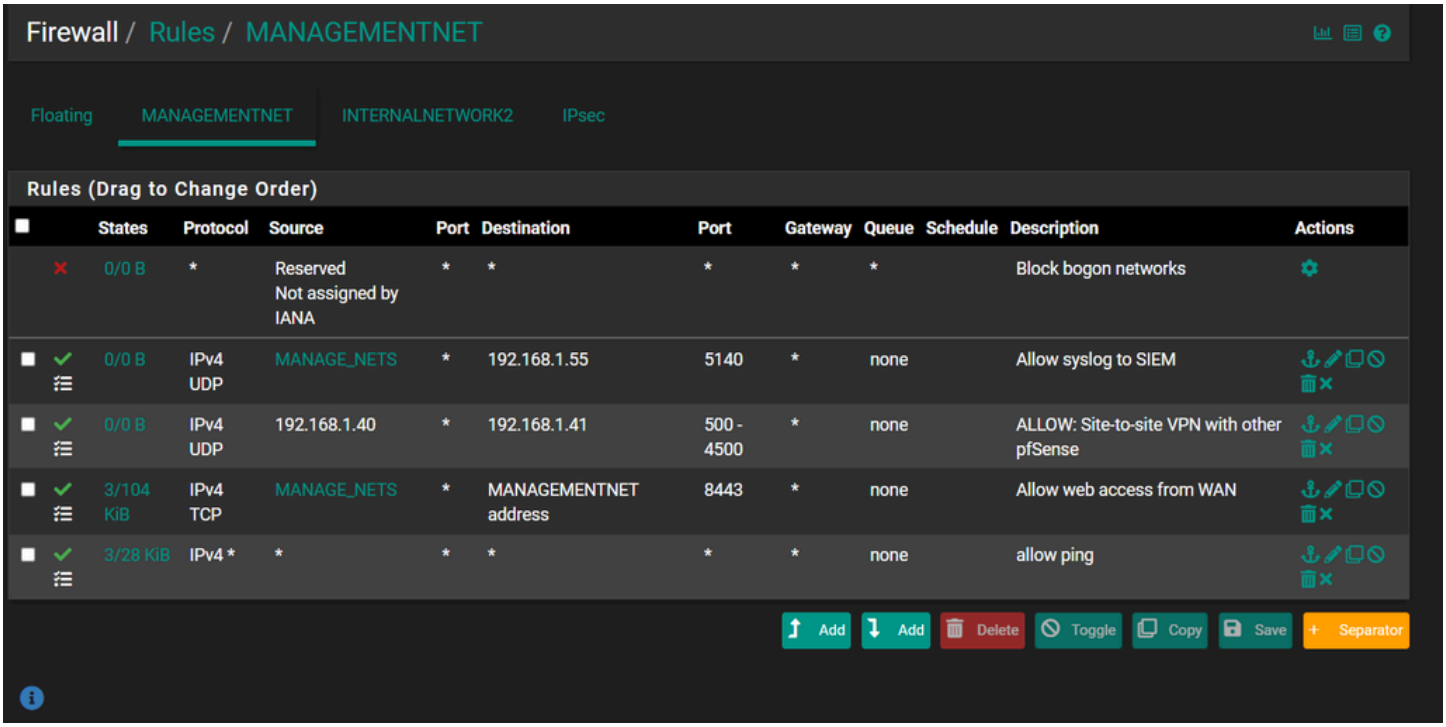
Floating MANAGEMENTNET INTERNALNETWORK2 IPsec

Rules (Drag to Change Order)

States	Interfaces	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	MANAGEMENTNET	IPv4 UDP	*	*	192.168.1.255	137 - 57621	*	none		SILENT-BLOCK: NetBIOS broadcasts to reduce log spam	

Add Add Delete Toggle Save + Separator

Mangement Network Rules:



Firewall / Rules / MANAGEMENTNET

Floating MANAGEMENTNET INTERNALNETWORK2 IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
0/0 B	IPv4 UDP	MANAGE_NETS	*	192.168.1.55	5140	*	none		Allow syslog to SIEM	
0/0 B	IPv4 UDP	192.168.1.40	*	192.168.1.41	500 - 4500	*	none		ALLOW: Site-to-site VPN with other pfSense	
3/104 KiB	IPv4 TCP	MANAGE_NETS	*	MANAGEMENTNET address	8443	*	none		Allow web access from WAN	
3/28 KiB	IPv4 *	*	*	*	*	*	none		allow ping	

Add Add Delete Toggle Copy Save + Separator

Internal Network-2 Rules:

Not secure 192.168.1.41:8443/firewall_rules.php?if=lan

Floating | MANAGEMENTNET | INTERNALNETWORK2 | IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	*	*	INTERNALNETWORK2 Address	8443	*	*		Anti-Lockout Rule	
0/0 B	IPv4 *	10.0.2.0/24	*	10.0.2.0/24	*	*	none		Allow Full Internal Network Access	
0/0 B	IPv4 TCP/UDP	10.0.2.0/24	*	DNS_SERVERS	53 (DNS)	*	none		ALLOW: DNS resolution	
0/0 B	IPv4 TCP	10.0.2.0/24	*	! RFC1918	80 - 443	*	none		ALLOW: Web browsing	
0/0 B	IPv4 *	10.0.2.0/24	*	! RFC1918	*	*	none		ALLOW: General internet access	
0/0 B	IPv4 TCP	*	*	*	853 (DNS over TLS)	*	none		Block DNS-over-TLS to prevent bypassing Pi-hole	
0/0 B	IPv4 TCP/UDP	192.168.1.39	*	*	53 (DNS)	*	none		Bypass Pi-hole DNS Redirect to allow Pi-hole to work	
0/0 B	IPv4 TCP	MANAGE_NETS	*	This Firewall (self)	22 (SSH)	*	none		ALLOW: SSH management	
0/0 B	IPv4 TCP	10.0.2.0/24	*	SOC_SERVER	1515 - 1516	*	none		ALLOW: Wazuh agent communication	
0/0 B	IPv4 TCP/UDP	10.0.2.0/24	*	SOC_SERVER	5140	*	none		ALLOW: pfSense syslog to SIEM	
0/0 B	IPv4 *	10.0.2.0/24	*	10.0.3.0/24	*	*	none		Allow to Internal 2 via VPN	
0/0 B	IPv4 TCP/UDP	INTERNALNETWORK2 subnets	*	192.168.1.55	1514 - 55000	*	none		wazuh agent to manager	
0/0 B	IPv4 *	10.0.2.0/24	*	*	*	*	none		Block Everything else	
0/0 B	IPv4 *	INTERNALNETWORK2 subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	INTERNALNETWORK2 subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

IPsec Rules:

Firewall / Rules / IPsec

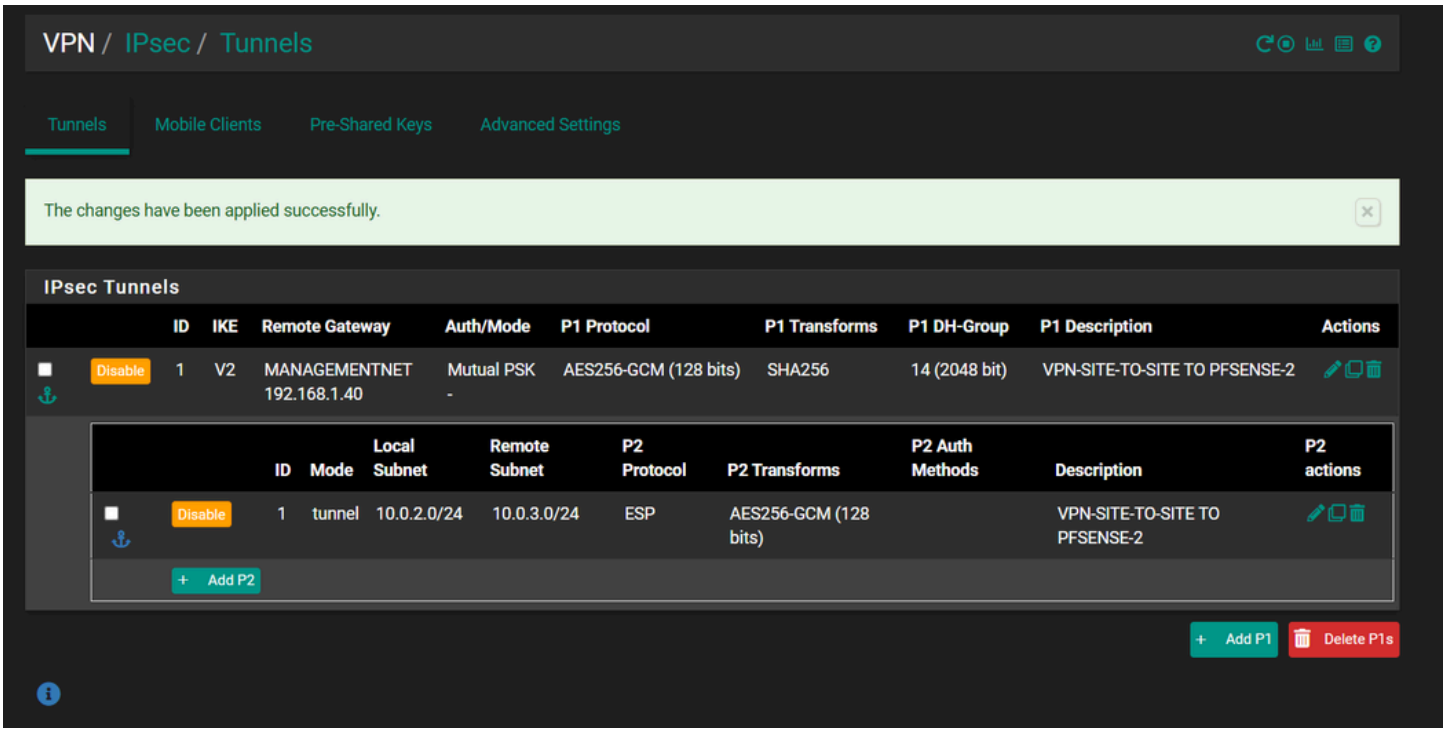
Floating | MANAGEMENTNET | INTERNALNETWORK2 | IPsec

Rules (Drag to Change Order)

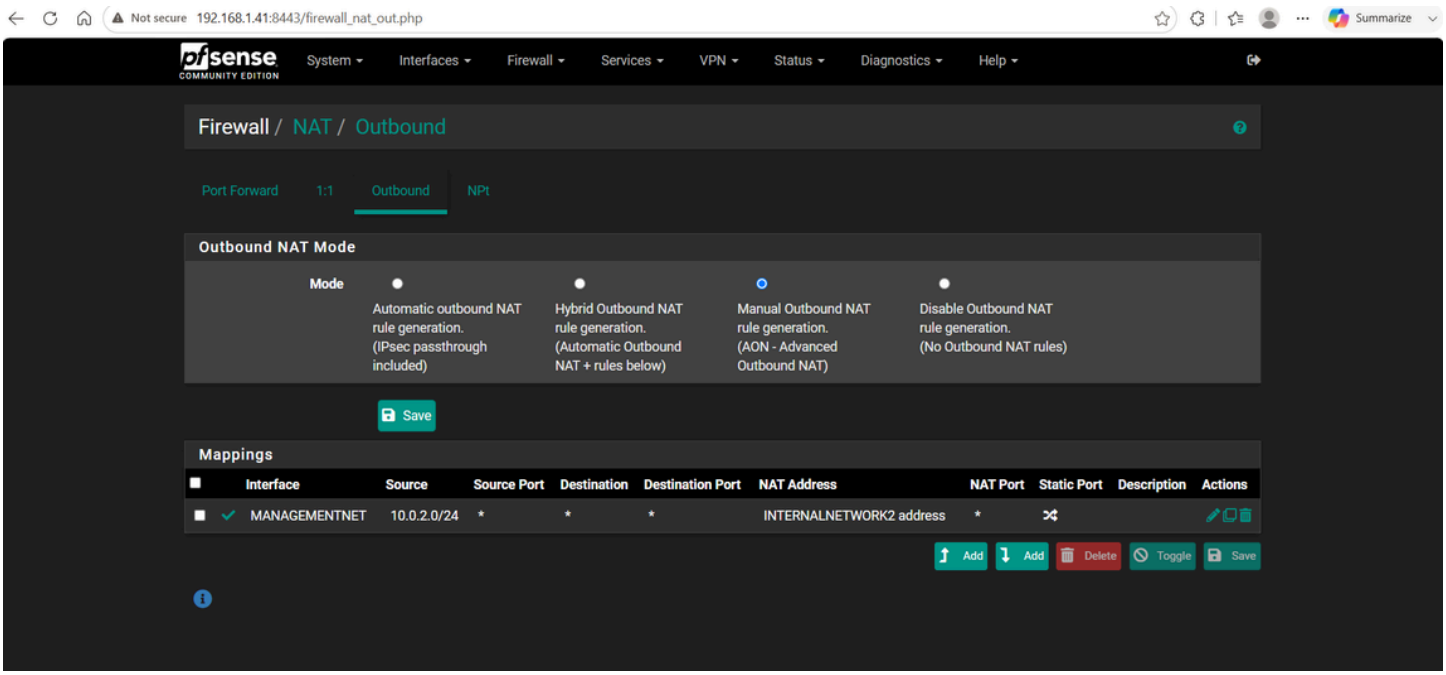
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	10.0.2.0/24	*	10.0.3.0/24	*	*	none		Allow traffic from pfSense 1 LAN via VPN	
0/0 B	IPv4 *	10.0.3.0/24	*	10.0.2.0/24	*	*	none		Allow Internal 2 to Internal 1 via VPN	

Add | Add | Delete | Toggle | Copy | Save | + Separator

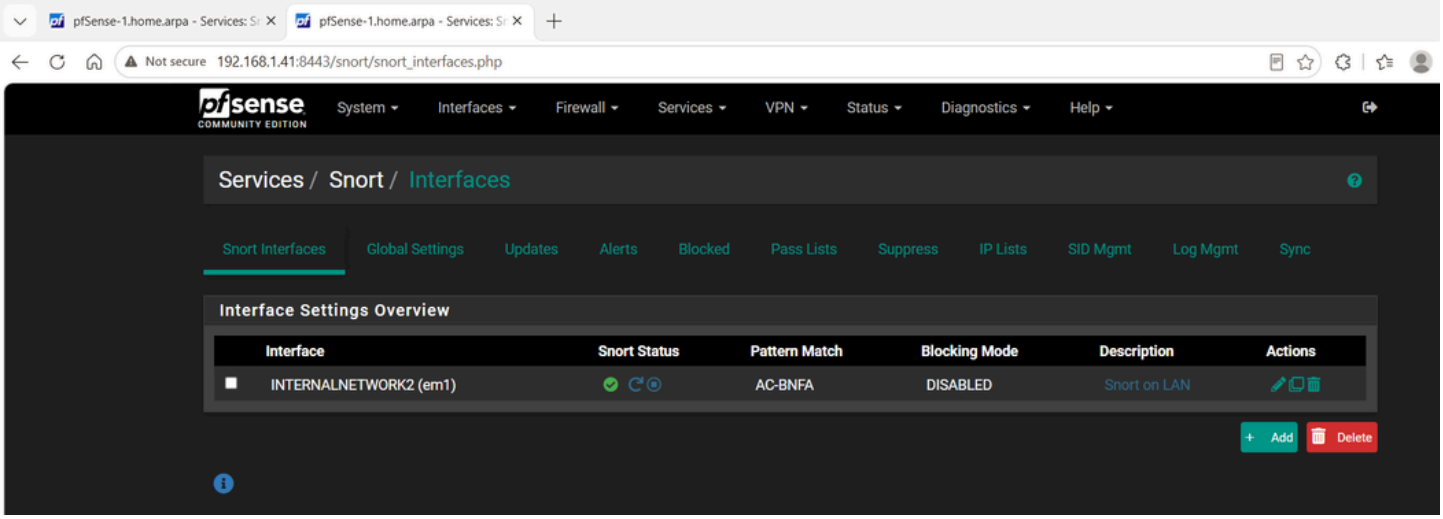
IPsec Configs:



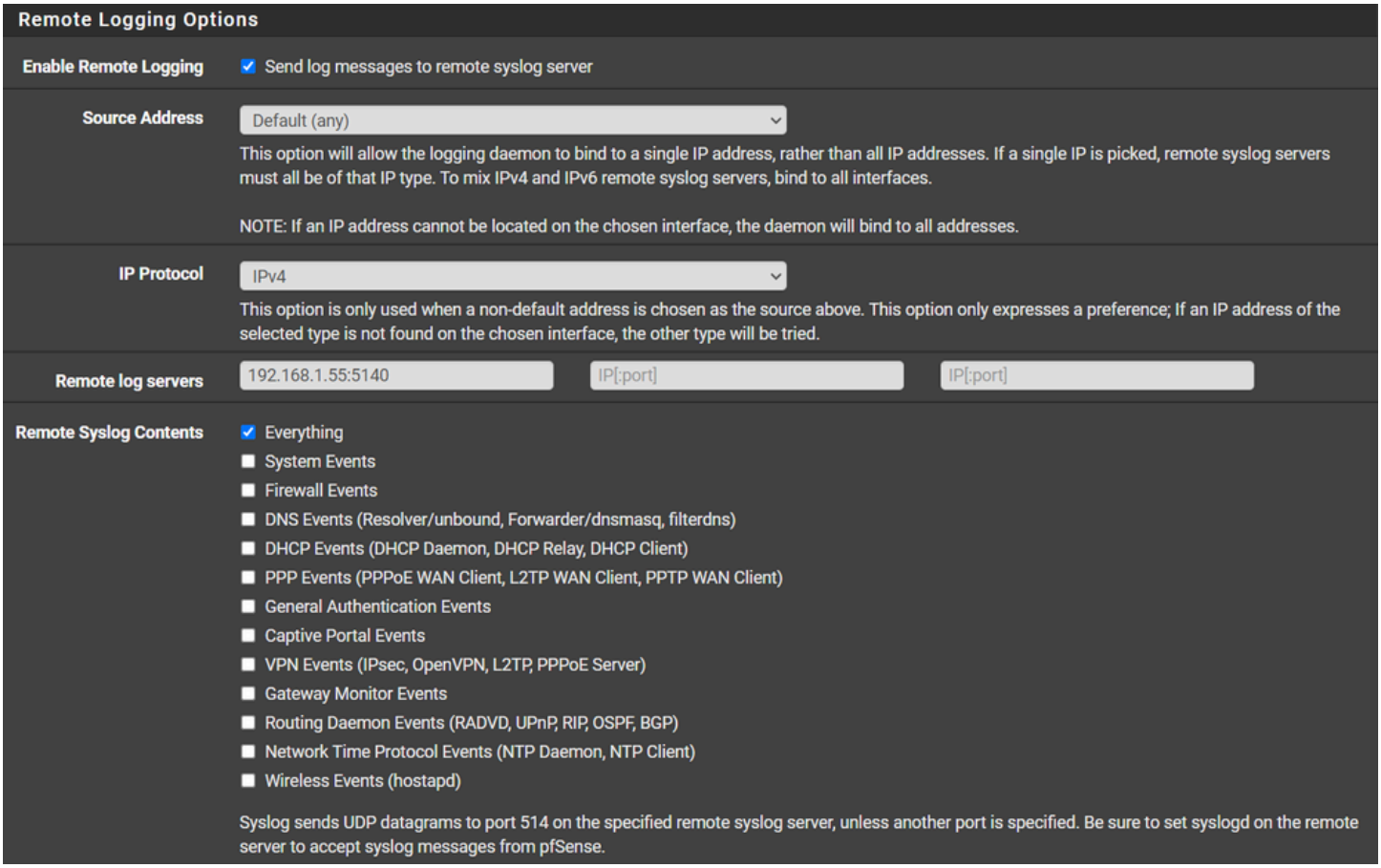
NAT Outbound Rules:



Snort:



Remote Syslog to Logstash:



7. IDS/IPS Architecture

Overview — Three Layer Detection

- Layer 1: Suricata on Raspberry Pi 5 — edge IDS monitoring all home LAN traffic via hardware SPAN port — passive detection only
- Layer 2: Snort on pfSense-1 and pfSense-2 — internal IPS inline on all internal segments — active blocking, drops malicious packets
- Layer 3: T-Pot on Linode — cloud honeypot capturing real attacker traffic from the public internet

Layer 1 — Suricata on Raspberry Pi 5

Role: Passive edge sensor monitoring all home LAN traffic captured directly from the Cisco switch SPAN port.

Docker Deployment:

```
docker run -d \
  --name suricata \
  --restart always \
  --network host \
  --cap-add=NET_ADMIN \
  --cap-add=NET_RAW \
  -v /var/log/suricata:/var/log/suricata \
  jasonish/suricata:latest \
  -i eth0
```

Rule Statistics:

- Total rules: 65,796
- Alert rules: 49,920
- Update frequency: Daily via suricata-update

Key Detection Categories:

- Port Scanning — ET SCAN Nmap
- Malware C2 — ET MALWARE C2 Channel
- Exploit Detection — ET EXPLOIT EternalBlue
- Suspicious Protocols — ET INFO Suspicious UserAgent
- Web Attacks — SQL injection, XSS
- DDoS — DOS Slowloris Attack
- DNS Anomalies — ET DNS suspicious queries

Log Flow:

```
Suricata -> /var/log/suricata/eve.json
        -> Filebeat -> Elasticsearch (suricata-*)
```

```
192.168.1.32
cs-cod3x@raspberrypi:~ $ docker ps | grep suricata
70c593badd69   jasonish/suricata:latest                  "/docker-entrypoint.…"   5 weeks ago   Up 6 days            su
ricata
cda2759933b3   jasonish/suricata:latest                  "/docker-entrypoint.…"   6 weeks ago   Up 6 days            su
ricata-sensor
cs-cod3x@raspberrypi:~ $
```

Layer 2 — Snort on pfSense (Internal IPS)

Role: Inline IPS on both pfSense firewalls. Actively inspects and blocks malicious traffic within and between all internal segments.

Installation:

System -> Package Manager -> Available Packages -> Snort -> Install

Interface Configuration — repeat for each internal interface:

Services -> Snort -> Add Interface

Enable: yes

Block offenders: yes

Which IP to block: SRC

Kill states: yes

Log to syslog: yes

Alert log retention: 7 days

HOME_NET per interface:

- pfSense-1 LAN: 10.0.3.0/24
- pfSense-1 DMZ: 10.0.5.0/24
- pfSense-1 ATK: 10.0.4.0/24
- pfSense-2 LAN: 10.0.2.0/24

Enabled Rule Categories:

- emerging-attack_response
- emerging-exploit
- emerging-malware
- emerging-scan

- emerging-web_server
- snort_community

Alert Severity Mapping:

- Priority 1: Critical
- Priority 2: High
- Priority 3: Medium
- Priority 4+: Low

Log Flow:

Snort alert -> pfSense syslog -> Logstash:5140

-> Elasticsearch (snort-*)

Layer 3 — T-Pot on Linode

Role: Internet-facing cloud honeypot capturing real attacker traffic from the public internet entirely separate from home infrastructure.

Active Honeypot Services:

- Cowrie — simulates SSH and Telnet server — captures credentials, commands, sessions
- Dionaea — simulates Windows SMB services — captures malware samples
- Elasticpot — simulates Elasticsearch instance — captures exploit attempts
- Honeytrap — simulates generic services — captures attack patterns
- Mailoney — simulates SMTP server — captures spam, phishing payloads

Log Flow:

T-Pot -> Filebeat -> TLS encrypted tunnel

-> Logstash on 192.168.1.55

-> Elasticsearch (tpot-*)

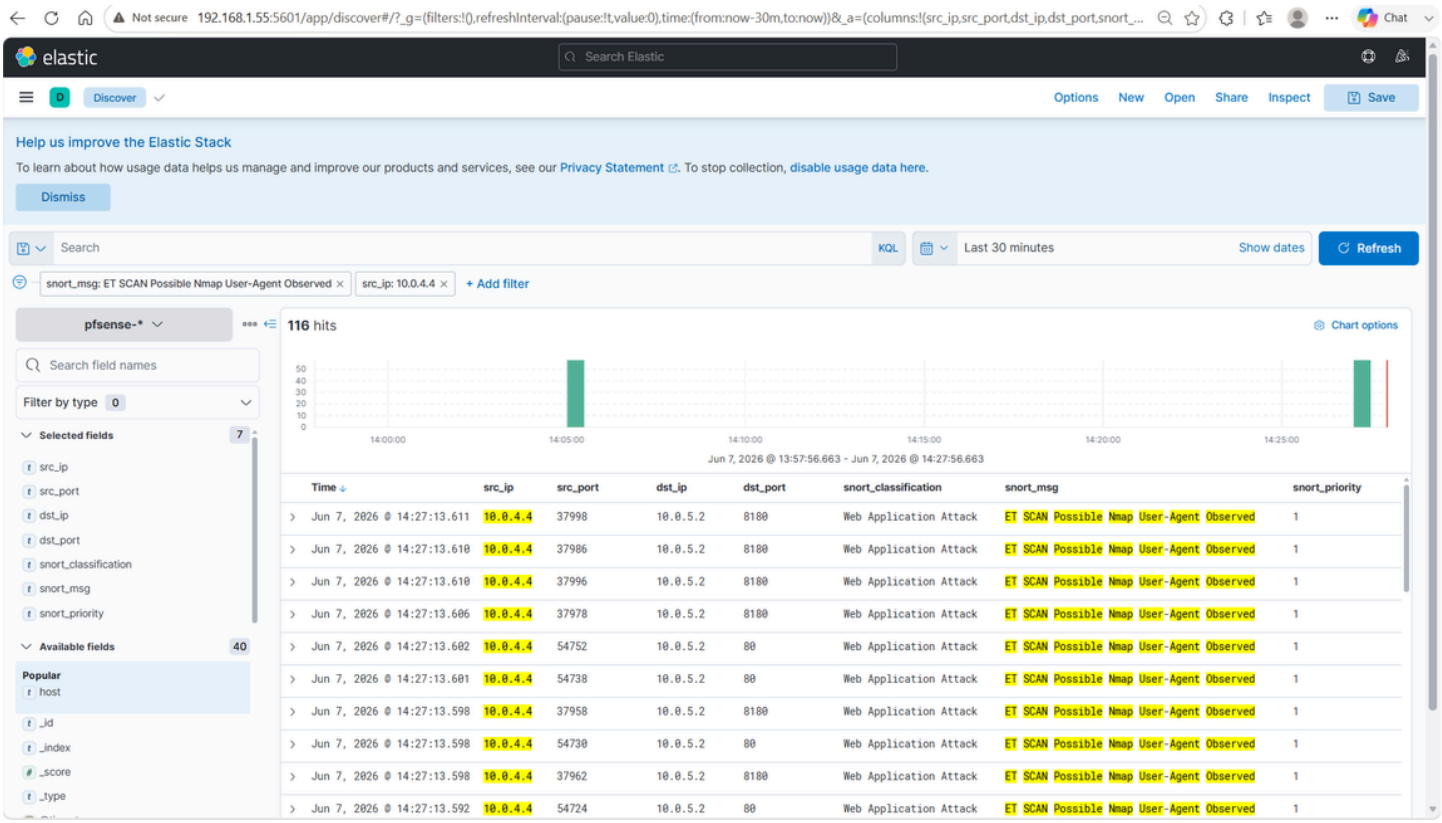
-> OpenCTI (IOC enrichment)

Value: T-Pot captures real attacker behavior from the internet — actual malware samples, real credential stuffing wordlists, and genuine exploitation techniques used against live infrastructure worldwide.

IDS/IPS Complete Coverage Map

Segment	Tool	Mode	Elasticsearch Index
Home LAN (192.168.1.x)	Suricata	IDS passive	suricata-*
Internal Network 1	Snort	IPS inline	snort-*
DMZ	Snort	IPS inline	snort-*
Attacker Network	Snort	IPS inline	snort-*
Internal Network 2	Snort	IPS inline	snort-*
Public Internet	T-Pot	IDS honeypot	tpot-*

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.5.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-06-07 07:26 EDT
Nmap scan report for 10.0.5.2
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.4.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2026-06-07T11:27:48+00:00; +3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```



8. SIEM — ELK Stack

Architecture

Data Sources -> Logstash (parsing) -> Elasticsearch (storage) -> Kibana (visualization)

Log Ingestion Sources

Source	Method	Port	Index
pfSense-1	Syslog UDP/TCP	5140	pfsense-*
pfSense-2	Syslog UDP/TCP	5140	pfsense-*
Suricata	Filebeat	Direct	suricata-*
Snort	Syslog via pfSense	5140	snort-*
Wazuh agents	TCP via Wazuh Manager	1514	wazuh-alerts-*
Pi-hole	Filebeat	Direct	pihole-*
T-Pot	Filebeat TLS	5140	tpot-*

Logstash Pipeline — pfSense and Snort

```
cat ~/logstash-pipeline/logstash.conf

input {

  udp {

    port => 5140

  }

}


filter {

  # Parse existing pfSense filterlog messages

  if [message] =~ /filterlog/ {

    dissect {

      mapping => { "message" => "<%{pri}>%{timestamp} filterlog[%{pid}]: %{csv}" }

    }
```

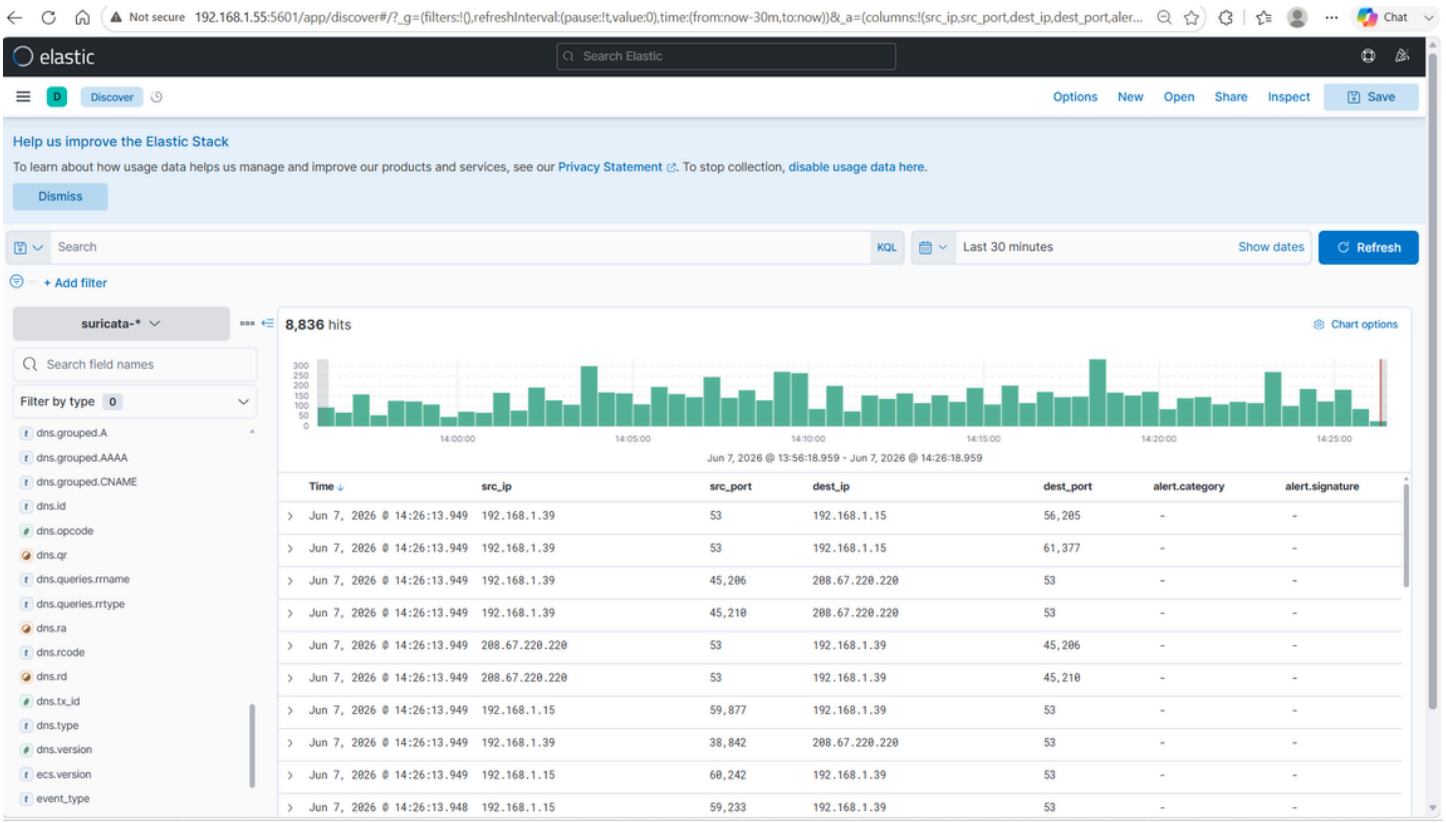
```
    csv {
      source => "csv"
      columns =>
["rule","sub","anchor","tracker","iface","action","dir","ver","tos","ecn","ttl","len","id","offset","flags","
proto_id","proto","len2","src_ip","dst_ip","src_port","dst_port","dlen"]
      separator => ","
    }
  }


  # Parse Snort alerts
  if [message] =~ /snort\[/ {
    grok {
      match => { "message" => "<%{POSINT:priority}>%{SYSLOGTIMESTAMP:timestamp} snort\
[%{NUMBER:snort_pid}\]: \[%{NUMBER:snort_gid}:%{NUMBER:snort_sid}:%
{NUMBER:snort_rev}\] %{GREEDYDATA:snort_msg} \[Classification: %
{DATA:snort_classification}\] \[Priority: %{NUMBER:snort_priority}\] \{%{WORD:protocol}\} %
{IP:src_ip}:%{NUMBER:src_port} -> %{IP:dst_ip}:%{NUMBER:dst_port}" }
    }
  }
}


output {
  elasticsearch {
    hosts => ["http://192.168.1.55:9200"]
    index => "pfsense-%{+YYYY.MM.dd}"
  }
}
```

Elasticsearch Indices

Index Pattern	Documents	Retention	Purpose
suricata-*	300,000+	30 days	Edge IDS alerts
snort-*	Active	30 days	Internal IPS alerts
pfsense-*	140,000+	30 days	Firewall logs
wazuh-alerts-*	500+	90 days	Endpoint alerts



Wazuh Alert to Elasticsearch Flow

Wazuh Agent -> TCP 1514 -> Wazuh Manager (192.168.1.55)

-> /var/ossec/logs/alerts/alerts.json

-> Filebeat inside Wazuh container

-> http://192.168.1.55:9200

-> wazuh-alerts-YYYY.MM.dd

9. XDR — Wazuh

Manager Deployment

```
services:
  wazuh.manager:
    image: wazuh/wazuh-manager:4.9.0
    ports:
      - "1515:1515"
      - "1516:1516"
      - "55000:55000"
    volumes:
      - wazuh-manager-data:/var/ossec
```

Enrolled Agents

Agent Name	OS	IP	Purpose
PC-1	Windows 10	10.0.2.5	Endpoint monitoring
PC-2	Windows 10	10.0.2.6	Endpoint monitoring
Domain Controller	Windows Server	10.0.2.100	Active Directory security
Red Hat Linux	RHEL 9	10.0.3.13	Linux server monitoring
k8s Node	Linux	10.0.3.17	Container host monitoring
Raspberry Pi	Ubuntu	192.168.1.39	Sensor self-monitoring

Active Detection Capabilities

- Windows Event Channel monitoring — Event IDs 4624, 4625, 4688, 4720, 4672
- Linux auditd monitoring — privilege escalation and suspicious commands
- File Integrity Monitoring across all enrolled endpoints
- Malware detection signatures
- Rootkit detection
- MITRE ATT&CK automatic tactic and technique mapping
- Security Configuration Assessment
- Vulnerability detection

10. SOAR — Shuffle and n8n

Shuffle SOAR

Purpose: Security-specific automated incident response triggered by Wazuh high-severity alerts.

Primary Playbook — Automated Alert Triage:

1. Trigger: Wazuh alert severity >= 10
2. Extract source IP from alert
3. Query VirusTotal API for IP reputation
4. If malicious score > 5: send enriched notification
5. Update Elasticsearch with verdict
6. Trigger n8n webhook for ticket creation
7. Feed IOC to OpenCTI

Integrations:

- Wazuh webhook — alert trigger source
- VirusTotal API — IP and hash enrichment
- n8n webhook — handoff to workflow automation
- Elasticsearch — update alert with enrichment verdict
- OpenCTI API — submit new IOCs from alerts

n8n Workflow Automation

Purpose: Broader workflow automation — ticket creation, notifications, and reporting pipelines.

Primary Workflow — Incident to Jira Ticket:

1. Trigger: Shuffle webhook (high severity)
2. Format alert data into Jira structure
3. Create Jira ticket with alert description and severity, source IP with VirusTotal verdict, affected agent name and OS, MITRE ATT&CK tactic and technique
4. Send Discord notification with ticket link

5. Log incident to audit trail

Complete Automation Pipeline

Wazuh alert fires

-> Shuffle receives via webhook

-> VirusTotal IP enrichment

-> IOC submitted to OpenCTI

-> n8n receives enriched payload

-> Jira ticket created automatically

-> Analyst notification sent

-> Analyst investigates in Kibana

-> Deep forensics in SIFT if needed

-> Malware samples to REMnux if needed

11. Threat Intelligence — OpenCTI

Host: Monitoring and CTI VM (192.168.1.115) Access: http://192.168.1.115:8080 Deployment: Docker container on Proxmox VM

Purpose

OpenCTI is an enterprise-grade Cyber Threat Intelligence platform used by government agencies, MSSPs, and large enterprise SOC teams. It provides structured management of threat intelligence including IOCs, TTPs, threat actor profiles, and campaign tracking with native MITRE ATT&CK integration.

Integrations

- T-Pot honeypot — attacker IPs, malware hashes — inbound
- VirusTotal via Shuffle — IP and hash reputation — inbound
- MITRE ATT&CK — TTP framework — inbound
- Wazuh via Shuffle — new IOCs from endpoint alerts — inbound
- Elasticsearch — enriched alert context — bidirectional
- REMnux findings — malware analysis IOCs — inbound

Intelligence Workflow

T-Pot captures attacker IP

-> OpenCTI ingests as IOC

-> Correlated against MITRE ATT&CK

-> Wazuh rule created for that IP

-> Next appearance triggers alert automatically

-> Kibana dashboard updated

Key Features Used

- IOC management — IPs, hashes, domains, URLs
- Threat actor tracking and attribution
- Campaign and intrusion set modeling
- MITRE ATT&CK matrix visualization
- Automated feed ingestion
- Connector framework for external integrations

12. Digital Forensics — SANS SIFT and REMnux

SANS SIFT Workstation

Host: Dell Optiplex 7090 — Proxmox VM IP: 192.168.1.113 Purpose: Digital forensics and incident response analysis

Forensic Workflow:

Alert detected in Kibana

-> Analyst pivots to SIFT workstation

-> Mount disk image or memory dump

-> Timeline analysis with Plaso

-> Artifact extraction

-> Evidence stored on TerraMaster NAS

-> Forensic report documented

Key Tools:

- Volatility — memory forensics and analysis
- Autopsy — disk image forensics
- Plaso — super timeline creation
- NetworkMiner — PCAP file analysis
- YARA — malware pattern identification

- RegRipper — Windows registry analysis
- Log2timeline — timeline correlation

Evidence Storage: All forensic evidence, disk images, and investigation artifacts stored on TerraMaster NAS via Samba share for integrity, persistence, and access from other workstations.

REMnux Workstation

Host: Dell Optiplex 7090 — Proxmox VM IP: 192.168.1.114 Purpose: Malware analysis and reverse engineering

Malware Analysis Workflow:

Malware sample identified by Wazuh FIM

or recovered from T-Pot honeypot

-> Sample staged in isolated REMnux VM

-> Static analysis — strings, hashes, headers

-> Dynamic behavioral analysis

-> Network traffic analysis

-> IOCs extracted — IPs, domains, hashes, mutexes

-> IOCs submitted to OpenCTI

-> Detection rules updated in Wazuh and Snort

Key Tools:

- YARA — malware signature identification
- Capa — malware capability detection
- PEiD — PE file analysis
- Strings — string extraction from binaries
- Wireshark — network capture analysis
- Ghidra — binary reverse engineering
- Floss — obfuscated string extraction
- Oledump — Office document analysis

Integration with SOC Pipeline: REMnux operates as the malware analysis stage in the post-incident pipeline. Artifacts recovered by Wazuh File Integrity Monitoring or captured by T-Pot are submitted to REMnux for analysis. Findings feed back into OpenCTI as structured IOCs and into Wazuh and Snort as new detection rules — closing the loop between detection and defense improvement.

13. Secondary SIEM — Splunk

Host: Monitoring and CTI VM (192.168.1.115) Access: http://192.168.1.115:8000 Deployment: Docker container on Proxmox VM

Purpose

Splunk is deployed alongside the primary ELK Stack for two reasons. First, Splunk is the dominant enterprise SIEM in production SOC environments — the majority of enterprise SOC job postings list Splunk as a required skill. Second, running both platforms provides a direct comparison of query languages, dashboard capabilities, and data ingestion approaches.

Log Sources

Logs are forwarded from Logstash to Splunk using the Splunk Universal Forwarder or HTTP Event Collector:

- pfSense logs — index: pfsense — firewall analysis
- Suricata alerts — index: suricata — IDS correlation
- Snort alerts — index: snort — internal IPS
- Wazuh alerts — index: wazuh — endpoint events

Skills Practiced

- Splunk Processing Language (SPL) queries
- Splunk dashboard and visualization building
- Saved searches and alert configuration
- Splunk data model and CIM compliance
- Correlation searches across multiple data sources

14. Honeypot — T-Pot on Linode

Platform: Linode cloud VPS OS: Debian Linux VM WebUI: https://linode-ip:64295

Active Honeypot Services

- Cowrie — simulates SSH and Telnet server — captures credentials, session commands
- Dionaea — simulates Windows SMB and FTP — captures malware binaries
- Elasticpot — simulates Elasticsearch — captures exploit payloads
- Honeytrap — simulates generic TCP services — captures raw attack patterns
- Mailoney — simulates SMTP server — captures phishing content

Log Shipping to SIEM

T-Pot containers -> Filebeat

-> TLS encrypted connection

-> Logstash on 192.168.1.55

-> Elasticsearch (tpot-*)

-> Kibana honeypot dashboard

-> OpenCTI IOC enrichment

Intelligence Value

T-Pot provides something no internal lab simulation can replicate — real attacker data from the public internet. Every credential attempt, every malware sample, every exploitation attempt comes from actual threat actors. This data feeds directly into OpenCTI to enrich the threat intelligence picture and back into Wazuh and Snort as detection rules based on observed real-world attack patterns.

15. Cloud Identity — Microsoft Entra ID

Status: In Progress

Architecture

On-premises Active Directory (10.0.2.100)

-> Entra Connect Sync agent installed on DC

Microsoft Entra ID (cloud tenant — free tier)

-> Password Hash Synchronization

Hybrid identity — users exist in both locations

-> Remote user authentication via Tailscale + Entra ID

Purpose

Simulates the hybrid identity environment used by the vast majority of enterprise organizations. Enables cloud-based authentication event monitoring, user identity context in firewall and SIEM logs, and conditional access policy practice — all skills directly relevant to enterprise SOC roles.

16. Remote Access — Tailscale

Tailscale VPN installed on: ThinkPad Laptop, Desktop PC, Raspberry Pi 5

When the laptop is taken to a workspace, Tailscale automatically maintains connectivity between all three physical machines. The pfSense site-to-site VPN, Wazuh agent

communication, and Filebeat log shipping all continue operating as if the laptop never left the home network.

Subnet routing configured:

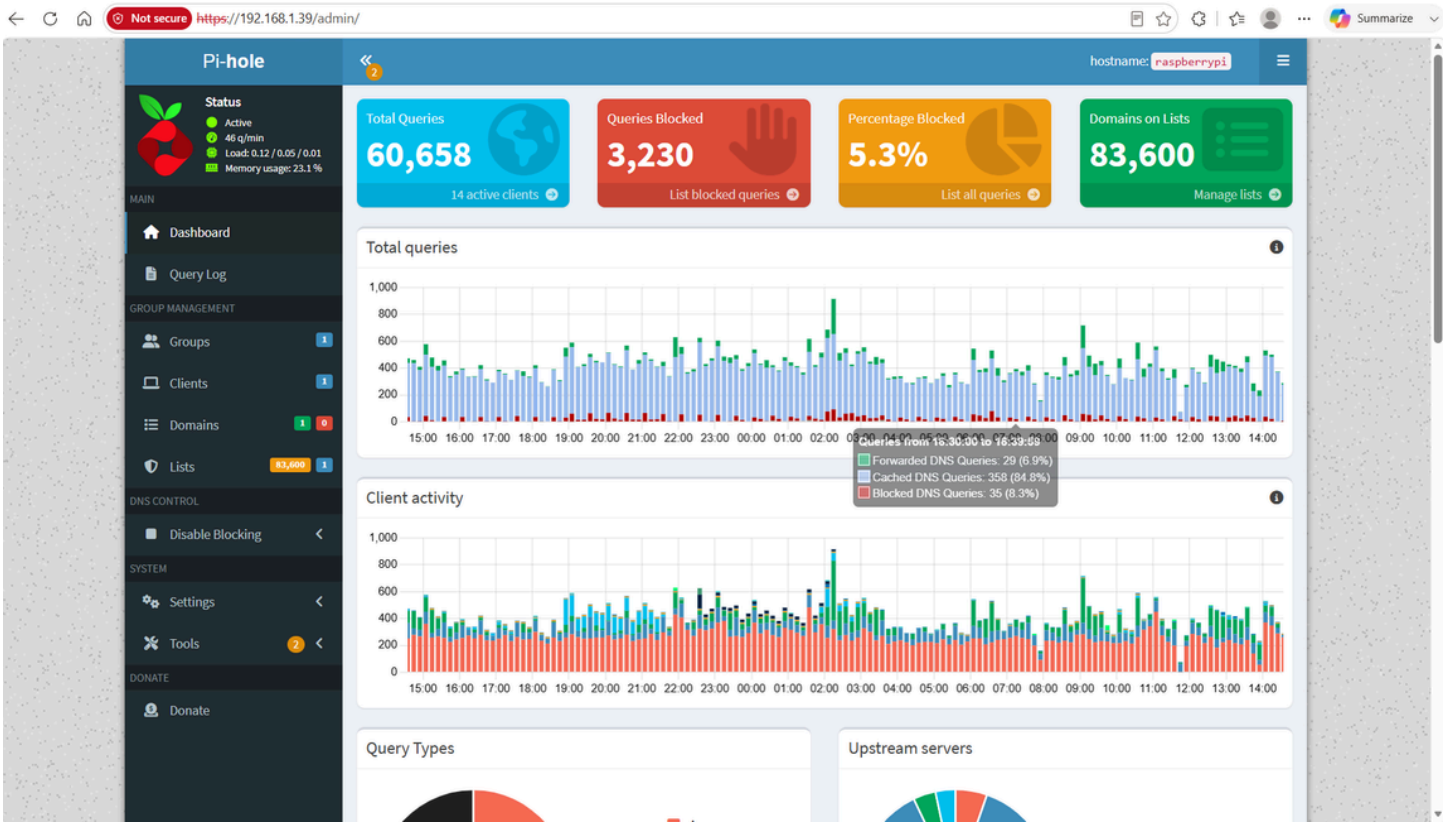
- Laptop — advertises 10.0.3.0/24 — enables access to Internal Network 1
- Desktop PC — advertises 10.0.2.0/24 — enables access to Internal Network 2
- Raspberry Pi — advertises 192.168.1.0/24 — enables access to Home LAN

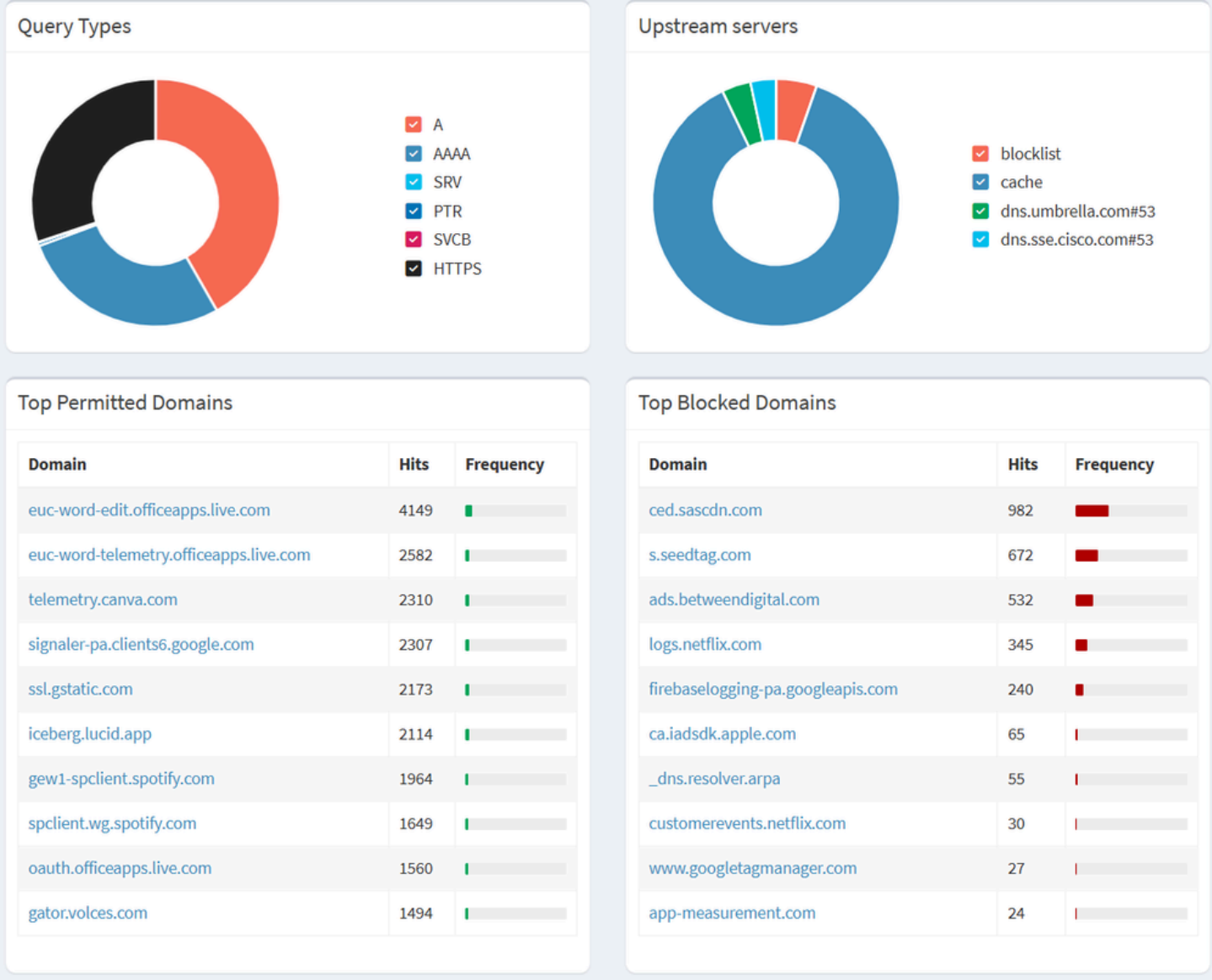
17. DNS Security — Pi-hole

IP: 192.168.1.39 GUI: http://192.168.1.39:80

Functions

- Network-wide DNS filtering blocking malware and C2 domains
- DNS query logging for threat correlation
- Ad blocking across all connected devices
- Upstream DNS forwarded to 8.8.8.8 and 8.8.4.4





Security Layering with Suricata

Pi-hole and Suricata provide complementary coverage at the DNS layer. Pi-hole blocks the DNS lookup before any connection is established. Suricata alerts on the network connection attempt even if DNS was blocked. Two independent tools catching the same C2 communication at different points in the kill chain.

18. Storage — TerraMaster F4-425 NAS

Model: TerraMaster F4-425 GUI: https://192.168.88.10 Network: VLAN 88 — MTU 9000 (iSCSI) and Home LAN (Samba)

Hardware Specifications

- Bays: 4
- Processor: Quad-core Intel
- Network: 10GbE capable
- OS: TOS — TerraMaster Operating System
- Protocol support: iSCSI, SMB, NFS, AFP

Three-Tier Storage Design

- Tier 1 — Hot: iSCSI LUN, VLAN 88, MTU 9000 — Elasticsearch active data, optimized IOPS
- Tier 2 — Warm: Samba share, Home LAN, MTU 1500 — PCAP dumps, config backups, forensic evidence
- Tier 3 — Cold: External HDD via USB, local — VM disaster recovery, cold archive

Storage Consumers

- Elasticsearch — iSCSI Tier 1 — all indexed log data
- SANS SIFT — Samba Tier 2 — forensic disk images, evidence
- REMnux — Samba Tier 2 — malware samples, analysis reports
- pfSense backup — Samba Tier 2 — configuration XML exports
- Kibana backup — Samba Tier 2 — saved objects and dashboard exports
- Suricata PCAP — Samba Tier 2 — packet capture archives

19. Service Monitoring — Uptime Kuma

URL: http://192.168.1.55:3001

Monitored Services

- Kibana — HTTP 200 — alert on failure or timeout
- Elasticsearch — HTTP cluster health — alert when not green
- Wazuh Manager — TCP port 1514 — alert when port closed
- Shuffle SOAR — HTTP 200 — alert on failure
- n8n — HTTP 200 — alert on failure
- OpenCTI — HTTP 200 — alert on failure
- Splunk — HTTP 200 — alert on failure
- pfSense-1 — Ping — alert on no response
- pfSense-2 — Ping — alert on no response
- Pi-hole — HTTP 200 — alert on failure
- TerraMaster NAS — Ping — alert on no response

Alerting: Discord webhook notification when any service becomes unavailable.

20. Attack Simulations and Validation

Simulation 1 — Port Scan

- Tool: Nmap stealth SYN scan
- Command: nmap -sS 192.168.1.40
- Source: Kali Linux 192.168.1.112
- Target: pfSense-1 WAN
- Detection: Suricata — ET SCAN Nmap
- Evidence: 4,180+ hits in suricata-* index
- Analyst conclusion: True positive — authorized internal scan

Simulation 2 — SSH Brute Force

- Tool: Hydra with rockyou.txt wordlist
- Command: hydra -l root -P rockyou.txt ssh://192.168.1.41:2222
- Source: Kali Linux
- Target: pfSense-2 NAT SSH
- Detection: Wazuh — multiple failed login correlation
- Evidence: wazuh-alerts-* — authentication failure pattern
- Analyst conclusion: True positive — authorized brute force test

Simulation 3 — Ping Flood DoS

- Tool: ping flood
- Command: sudo ping -f 192.168.1.40 -c 500
- Source: Kali Linux
- Target: pfSense-1 WAN
- Detection: pfSense rate-based ICMP detection
- Evidence: pfsense-* index — high ICMP volume confirmed
- Analyst conclusion: True positive — authorized DoS simulation

Simulation 4 — SMB Enumeration

- Tool: enum4linux
- Command: enum4linux 192.168.1.39
- Source: Kali Linux
- Target: Raspberry Pi NAS — Samba
- Detection: Suricata flow alerts — 8-12 alerted flows
- Evidence: suricata-* — SMB reconnaissance confirmed
- Analyst conclusion: True positive — Samba service info exposed

21. Detection Capabilities and MITRE ATT&CK

Detection Coverage by Layer

Edge Layer — Suricata:

- Port Scanning — threshold detection — ET SCAN Nmap scan
- Malware C2 — signature matching — ET MALWARE C2 Channel
- Exploit Attempts — vulnerability signatures — ET EXPLOIT EternalBlue
- DDoS Patterns — rate-based detection — DOS Slowloris Attack
- Suspicious Protocols — protocol anomaly — ET INFO Tor traffic

Internal Layer — Snort:

- Internal Scanning — threshold detection — scan rule triggers
- Lateral Movement — authentication anomaly — multiple auth failures
- Web Attacks — HTTP inspection — SQL injection pattern
- Exploit Attempts — vulnerability signatures — MS17-010 detection

- Malware Behavior — signature matching — known malware IOCs

Endpoint Layer — Wazuh:

- Malware Execution — FIM and signatures — malware detected
- Privilege Escalation — auditd monitoring — sudo abuse detected
- Persistence — registry monitoring — startup entry added
- Lateral Movement — auth log correlation — multiple failed logins
- Account Creation — Event ID 4720 — new user account created
- Admin Login — Event ID 4672 — privileged logon detected

DNS Layer — Pi-hole:

- Malware C2 Domains — blocklist matching — domain blocked
- DNS Tunneling — query frequency analysis — unusual DNS volume

Cloud Honeypot — T-Pot:

- SSH Brute Force — captures credentials, commands
- Malware Delivery — captures binary samples
- Exploitation — captures payload content
- Reconnaissance — captures scan patterns

MITRE ATT&CK Mapping

Detection	Tactic	Technique ID	Tool
Port scan detection	Reconnaissance	T1046 Network Service Scanning	Suricata
SSH brute force	Credential Access	T1110 Brute Force	Wazuh
SMB enumeration	Discovery	T1135 Network Share Discovery	Suricata
Malware C2 traffic	Command and Control	T1071 Application Layer Protocol	Suricata
New admin account	Privilege Escalation	T1078 Valid Accounts	Wazuh
Firewall rule bypass	Defense Evasion	T1562 Impair Defenses	pfSense
Public exploit attempt	Initial Access	T1190 Exploit Public-Facing App	Suricata
Registry modification	Persistence	T1547 Boot Autostart Execution	Wazuh
File modification	Impact	T1565 Data Manipulation	Wazuh FIM
Lateral movement	Lateral Movement	T1021 Remote Services	Wazuh

22. Log Flow Architecture

Wazuh Manager -(webhook)-> Shuffle SOAR -(VirusTotal)-> Enriched Alert

-> OpenCTI (new IOC)

-> n8n Webhook

-> Jira Ticket + Notification

23. Kibana Dashboards

Dashboard 1 — Main Security Dashboard

- Total Alerts count metric
- Blocked Connections count metric
- Unique Attacking IPs count metric
- Critical Alerts count metric
- Alerts over time — line chart by type
- Top attack sources — ranked table
- Protocol distribution — pie chart
- Most targeted ports — bar chart
- Recent security events — data table

Dashboard 2 — Network Security Dashboard

- pfSense allowed vs blocked traffic — stacked bar chart
- Suricata alert severity distribution
- Snort alerts by interface and severity
- VPN tunnel health indicators
- Top Suricata signatures fired
- Top Snort signatures fired
- Geographic attack origin map

Dashboard 3 — Endpoint Security Dashboard

- Wazuh active agent count and status
- Alerts by MITRE ATT&CK tactic — horizontal bar
- Top alert rules by frequency
- Recent endpoint alerts — data table
- FIM events timeline
- Agent health and last seen status

Kibana Index Patterns

Pattern	Time Field	Purpose
suricata-*	@timestamp	Edge IDS alerts
snort-*	@timestamp	Internal IPS alerts
pfsense-*	@timestamp	Firewall logs
wazuh-alerts-*	timestamp	Endpoint alerts
pihole-*	@timestamp	DNS queries
tpot-*	@timestamp	Honeypot data

24. Maintenance and Troubleshooting

Daily Health Checks

```
# Verify all containers running
docker ps

# Elasticsearch cluster health
curl -s "http://192.168.1.55:9200/_cluster/health" | jq .

# Recent Suricata alerts
docker exec suricata tail -5 /var/log/suricata/eve.json \
  | jq 'select(.event_type=="alert")'

# Recent Wazuh alerts timestamp
curl -s "http://192.168.1.55:9200/wazuh-alerts-*/_search\
?size=1&sort=timestamp:desc" | jq '.hits.hits[0]._source.timestamp'
```

Check Kibana — Discover -> last 15 minutes -> data present

Weekly Maintenance

- Update Suricata rules: docker exec suricata suricata-update
- Update Snort rules: pfSense -> Snort -> Updates -> Update Now
- Check disk space: df -h
- Clear old indices: curl -X DELETE http://192.168.1.55:9200/pfsense-YYYY.MM.*
- Backup pfSense-1 config: Diagnostics -> Backup/Restore -> Download
- Backup pfSense-2 config: Diagnostics -> Backup/Restore -> Download
- Backup Kibana dashboards: Stack Management -> Saved Objects -> Export
- Update T-Pot: SSH to Linode -> update containers

Common Issues and Solutions

- No pfsense-* logs — empty index — check pfSense remote syslog settings
- No suricata-* data — no alerts in Kibana — check docker logs suricata
- No wazuh-alerts-* — stale timestamp — check filebeat.yml hosts field
- Wazuh agent offline — agent disconnected — systemctl restart wazuh-agent
- Kibana shows no data — no results found — check time range and index pattern
- High Elasticsearch memory — slow queries — increase ES_JAVA_OPTS heap
- VPN tunnel down — sites unreachable — pfSense -> VPN -> IPsec -> Status
- Snort blocking legitimate traffic — false positive — Services -> Snort -> Suppress
- Tailscale disconnected — remote access lost — tailscale up on affected machine
- OpenCTI not starting — container error — docker logs opencti check dependencies
- Splunk license warning — data limit — Splunk free tier limited to 500MB/day

Log Retention Policy

Index	Retention	Reason
suricata-*	30 days	High volume, short investigation window
snort-*	30 days	High volume
pfsense-*	30 days	High volume, operational value
wazuh-alerts-*	90 days	Lower volume, longer investigation value
wazuh-archives-*	7 days	Very high volume, raw data
pihole-*	30 days	DNS reference
tpot-*	30 days	Threat intelligence value

25. Planned Improvements

- TerraMaster iSCSI activation — hot storage for Elasticsearch IOPS optimization — In Progress
- Entra ID Connect Sync — hybrid identity with on-prem AD — In Progress
- SANS SIFT full integration — DFIR pipeline with TerraMaster evidence storage — In Progress
- REMnux malware pipeline — automated sample staging from Wazuh and T-Pot — In Progress
- OpenCTI feed integration — T-Pot and VirusTotal IOC automation — In Progress
- Splunk log forwarding — forward from Logstash to Splunk via HEC — In Progress
- OpenCTI to ELK integration — bidirectional enrichment pipeline — Planned
- n8n + Jira ticketing — full SOC incident tracking automation — Planned
- Cisco SPAN port activation — hardware traffic mirroring to Raspberry Pi — Planned
- LACP EtherChannel activation — physical switch aggregation — Planned
- Custom Snort rules — lab-specific detection signatures — Planned
- PCAP long-term archive — Suricata captures to TerraMaster Tier 2 — Planned

26. Port Reference

Port	Service	Protocol	Purpose
22	SSH	TCP	Remote management
53	DNS / Pi-hole	TCP/UDP	Name resolution
80	HTTP / Pi-hole GUI	TCP	Web services
443	HTTPS	TCP	Secure web
500	IKE	UDP	IPsec key exchange
1514	Wazuh	TCP	Agent communication
1515	Wazuh	TCP	Agent enrollment
3001	Uptime Kuma	HTTP	Service monitoring
3002	Shuffle SOAR	HTTP	SOAR platform
4500	IPsec NAT-T	UDP	VPN through NAT
5140	Logstash / Syslog	UDP/TCP	All firewall log collection
5601	Kibana	HTTP	Primary SIEM dashboards
5678	n8n	HTTP	Workflow automation
8000	Splunk	HTTP	Secondary SIEM
8080	OpenCTI	HTTP	Threat intelligence platform
8443	pfSense GUI	HTTPS	Firewall management

9200	Elasticsearch	HTTP	Log queries and API
55000	Wazuh API	HTTP	XDR management
64295	T-Pot WebUI	HTTPS	Honeypot dashboard

27. Quick Reference Commands

Docker Management

```
# List all running containers with status

docker ps


# View container logs

docker logs [container_name] --tail 50


# Restart a container

docker restart [container_name]


# Live resource usage per container

docker stats


# Open shell inside a container

docker exec -it [container_name] /bin/bash


# View all container resource usage snapshot

docker stats --no-stream
```

Elasticsearch

```
# All indices with document counts and sizes
curl -s "http://192.168.1.55:9200/_cat/indices?v"

# Cluster health check
curl -s "http://192.168.1.55:9200/_cluster/health" | jq .

# Most recent Wazuh alert
curl -s "http://192.168.1.55:9200/wazuh-alerts-*/_search\
?size=1&sort=timestamp:desc" | jq \
'.hits.hits[0]._source | {timestamp, rule: .rule.description, agent: .agent.name}'

# Most recent Suricata alert
curl -s "http://192.168.1.55:9200/suricata-*/_search\
?size=1&sort=@timestamp:desc" | jq \
'.hits.hits[0]._source | {timestamp: ."@timestamp", alert: .alert.signature}'

# Delete old index
curl -X DELETE "http://192.168.1.55:9200/pfsense-2026.03.*"

# Index document count by pattern
curl -s "http://192.168.1.55:9200/_cat/indices/suricata-*?h=index,docs.count"
```

Suricata

```
# View recent alerts only
docker exec suricata tail -20 /var/log/suricata/eve.json \
  | jq 'select(.event_type=="alert")'
```

```
# Update detection rules
docker exec suricata suricata-update

# Verify Suricata process is running
docker exec suricata ps aux | grep suricata

# Check loaded rule count
docker exec suricata suricata --list-runmodes
```

Wazuh

```
# List all enrolled agents with status
docker exec wazuh-manager_wazuh.manager_1 \
  /var/ossec/bin/agent_control -lc

# Restart Wazuh agent on Windows endpoint
# Run in PowerShell as Administrator
Restart-Service WazuhSvc

# Check Wazuh agent logs on Windows
Get-Content "C:\Program Files (x86)\ossec-agent\ossec.log" -Tail 30

# Test agent connectivity from Windows
Test-NetConnection 192.168.1.55 -Port 1514
```

Snort

```
# View Snort alerts
# Services -> Snort -> [interface] -> Alerts tab in pfSense GUI
```

Check suppression list

Services -> Snort -> [interface] -> Suppress tab

Force rule update

Services -> Snort -> Updates -> Update Rules Now

Verify Snort running status per interface

Services -> Snort -> Snort Interfaces tab

Tailscale

Check current connection status

tailscale status

View all connected peers

tailscale peers

Ping a peer by Tailscale hostname

tailscale ping [hostname]

Re-authenticate or reconnect

tailscale up

Check subnet routes being advertised

tailscale status --json | jq .Self.AllowedIPs

Pi-hole

Check Pi-hole container status

docker logs pihole --tail 20

Update Pi-hole blocklists

GUI -> Tools -> Update Gravity

Check DNS query log

GUI -> Query Log

Flush DNS cache

docker exec pihole pihole restartdns

Documentation maintained as a living document — updated with each lab change.

Author: Ahmed Ashraf | github.com/CSCOD3X | May 2026

Active project — continuously updated as new components are implemented and validated.