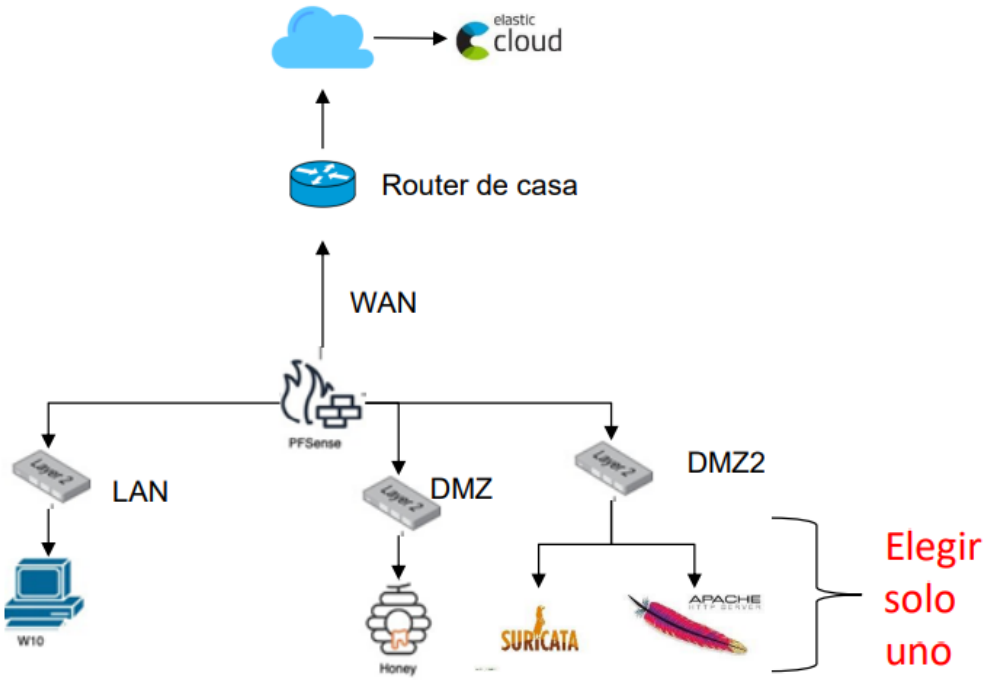
Blue Team Report

By Monica Licea Castro

We have been asked to create the following infrastructure:

Enunciado

Queremos montar la siguiente infraestructura:



Los requisitos que debe cumplir son los siguientes:

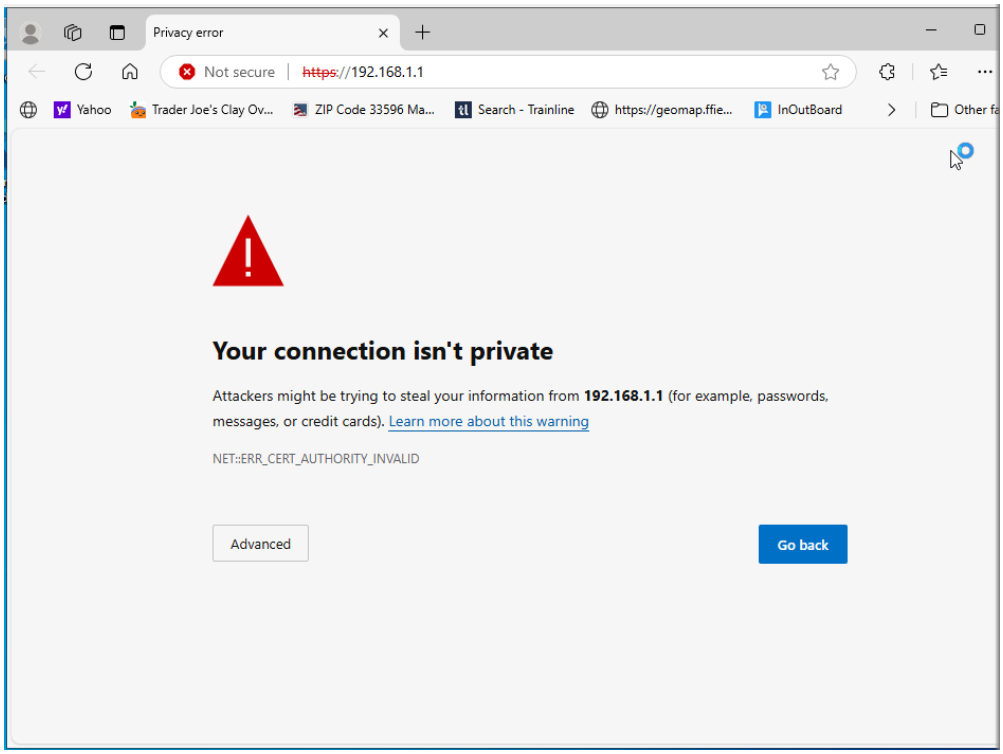
1. Debe tener un Pfsense en que se interconecten las redes LAN, DMZ y DMZ2
2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.
3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.
    1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2…) y debe ser accesible desde el exterior (red WAN) en ambos sentidos.
4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente. Se propone Suricata o Apache Server como posibles fuentes, pero se deja a elección del alumno.
5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el Windows 11 y la fuente elegida ubicada en la DMZ2.

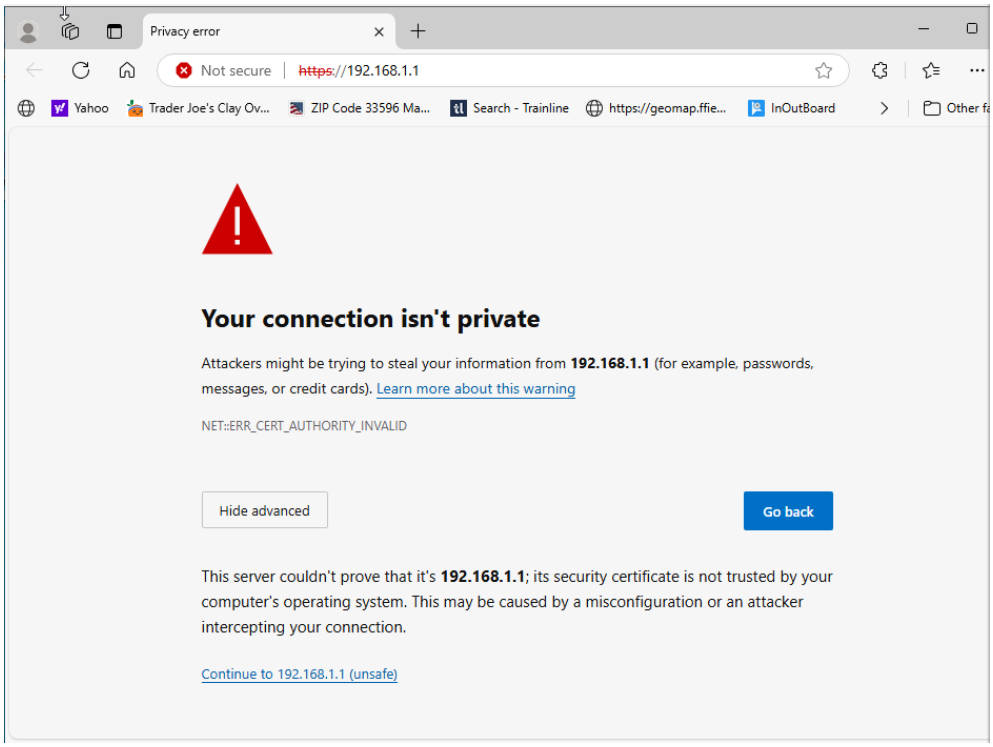
Criterios de evaluación de la memoria:

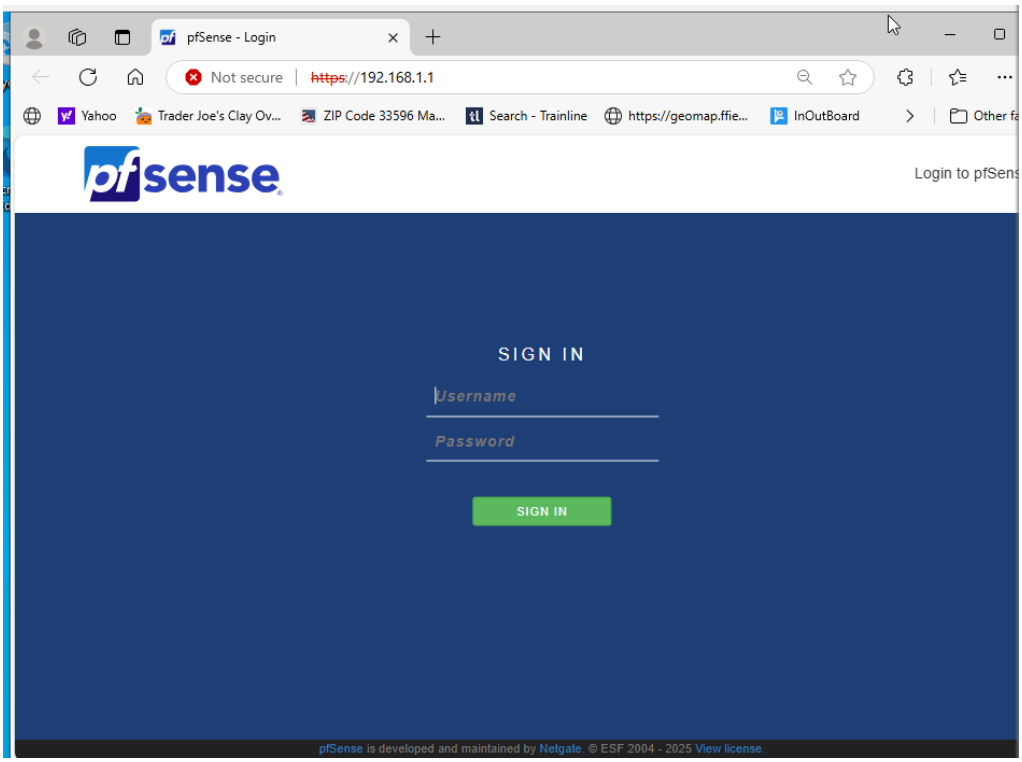
1. Debe contener evidencias y explicaciones que demuestren la correcta creación de la infraestructura de red en el PfSense.
2. Debe contener explicación y captura de las reglas de firewall elegidas para cada red (WAN, NAT, LAN, DMZ y DMZ2)
3. Debe contener evidencias de las políticas e integraciones asignadas a cada agente del SIEM (Elastic)
4. Debe contener evidencias que demuestren la correcta recepción de los logs, de todas las fuentes especificadas en el enunciado, en el SIEM (Elastic).

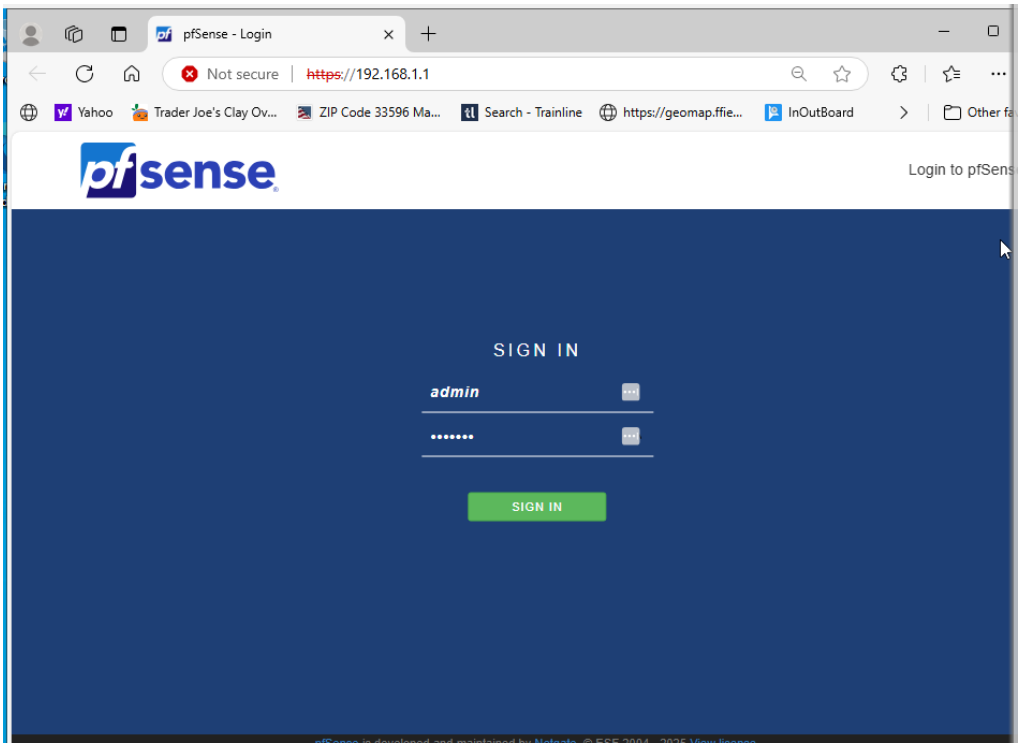
PFSense Configuration

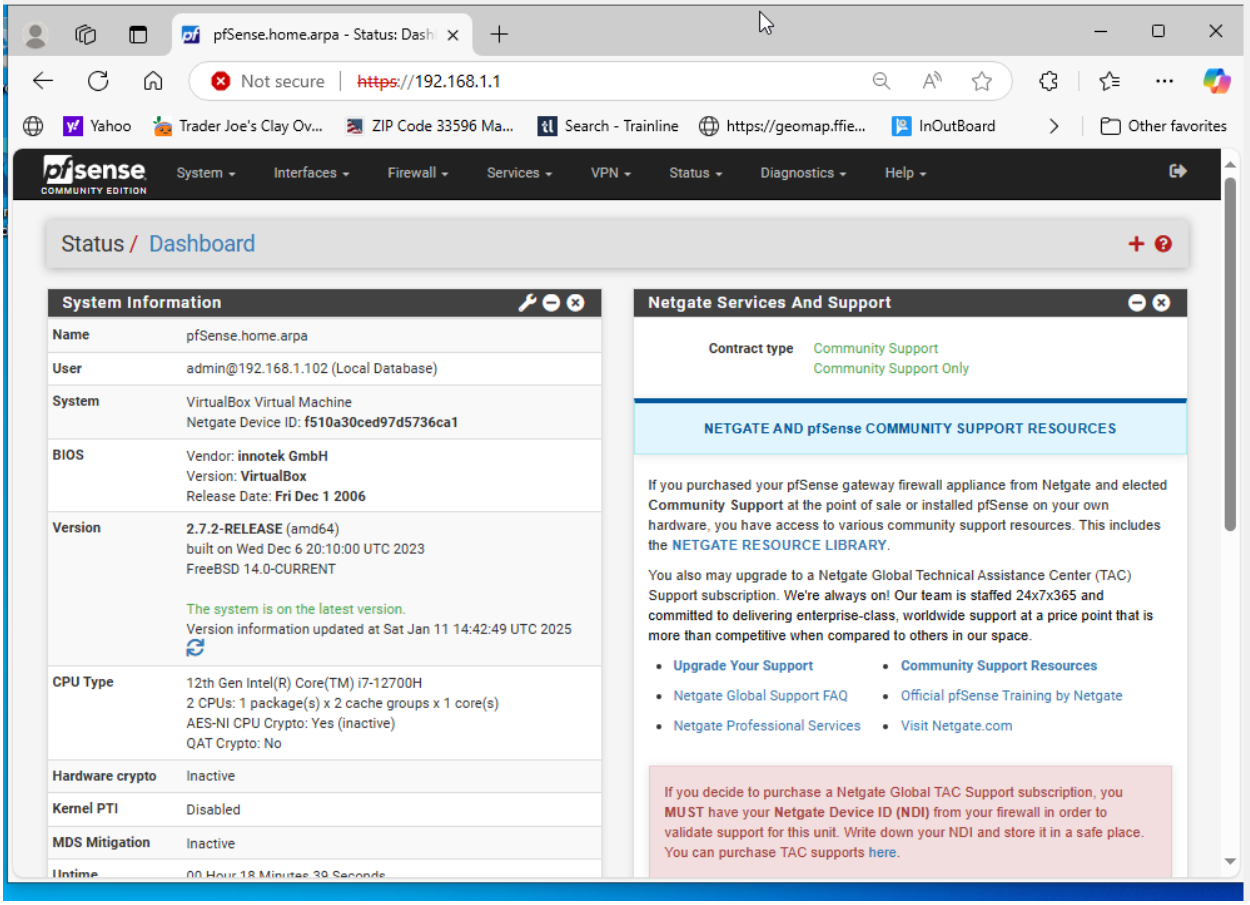
LAN v4: 192.168.1.1

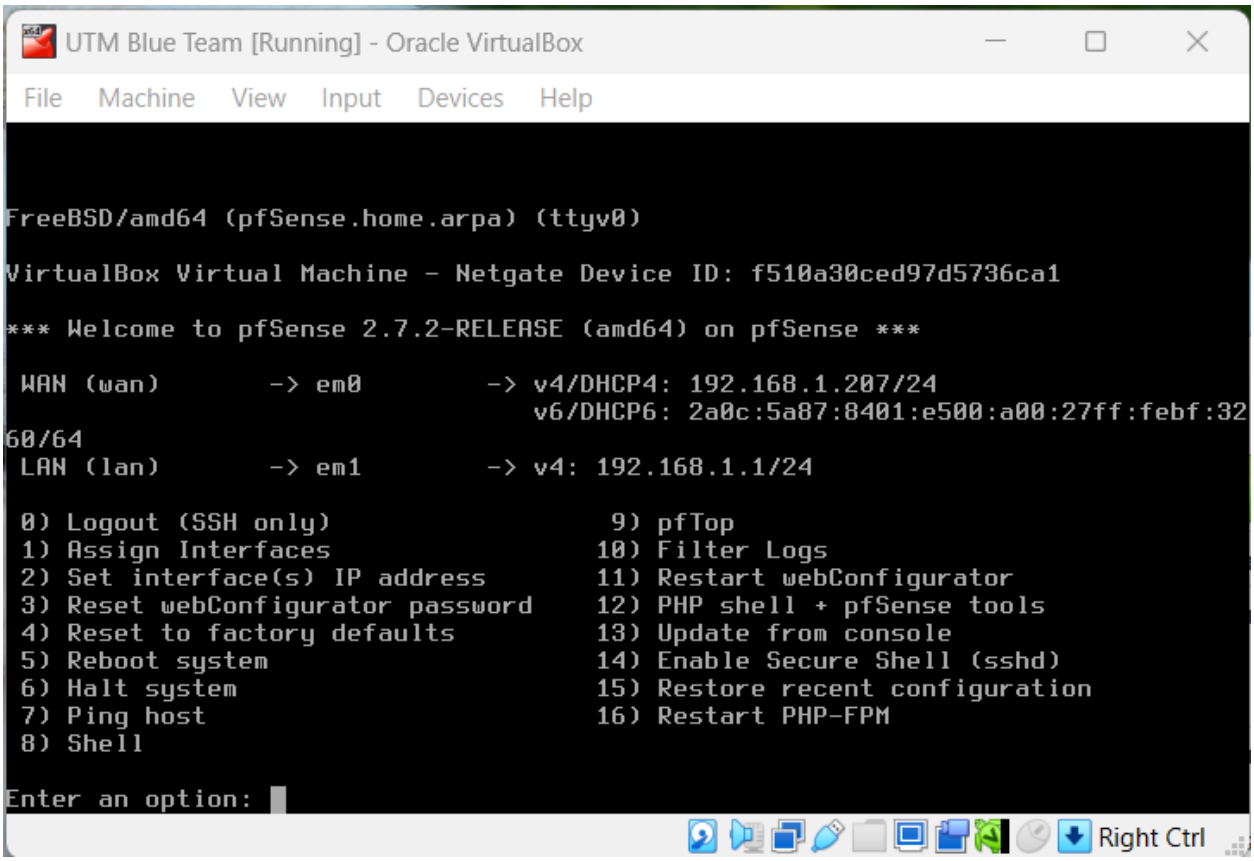




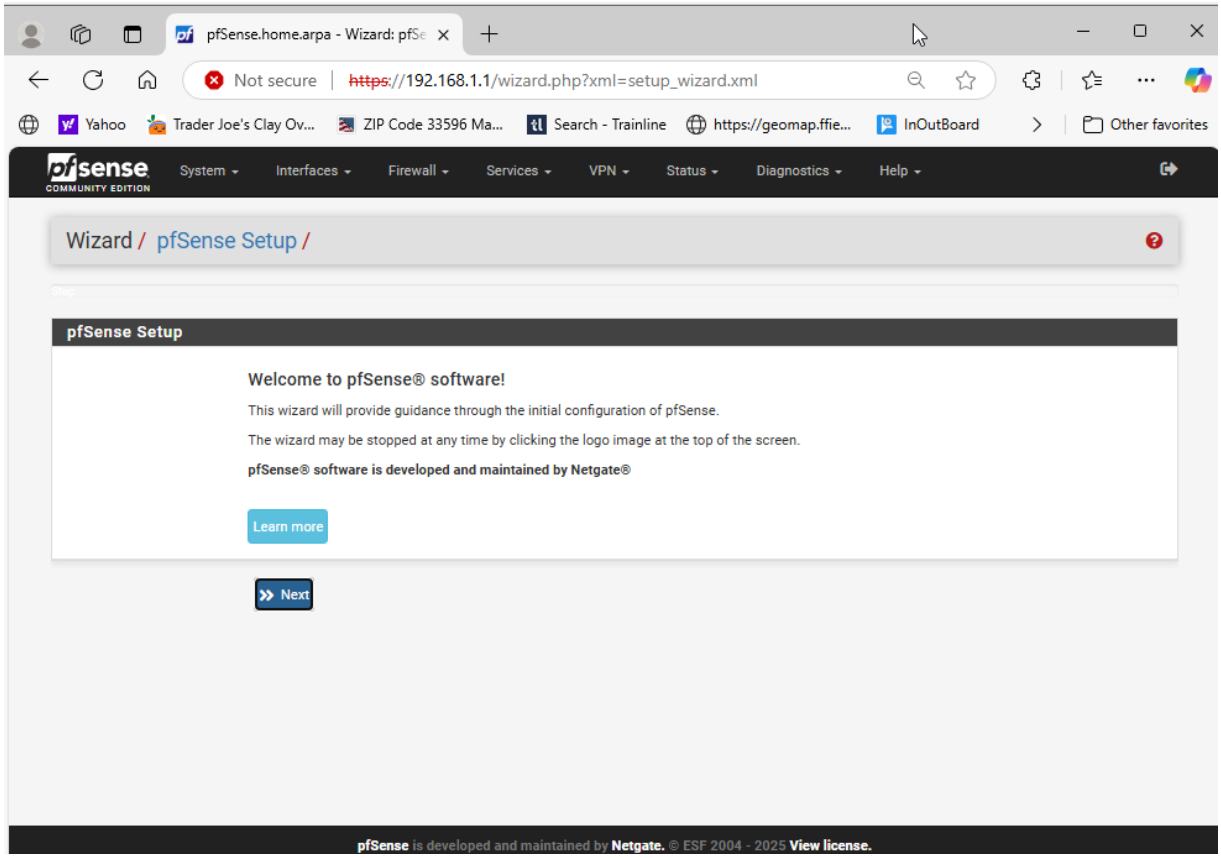

pfSense - Login
Not secure
https://192.168.1.1
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other fa
pfsense
Login to pfSens
SIGN IN
Username
Password
SIGN IN
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

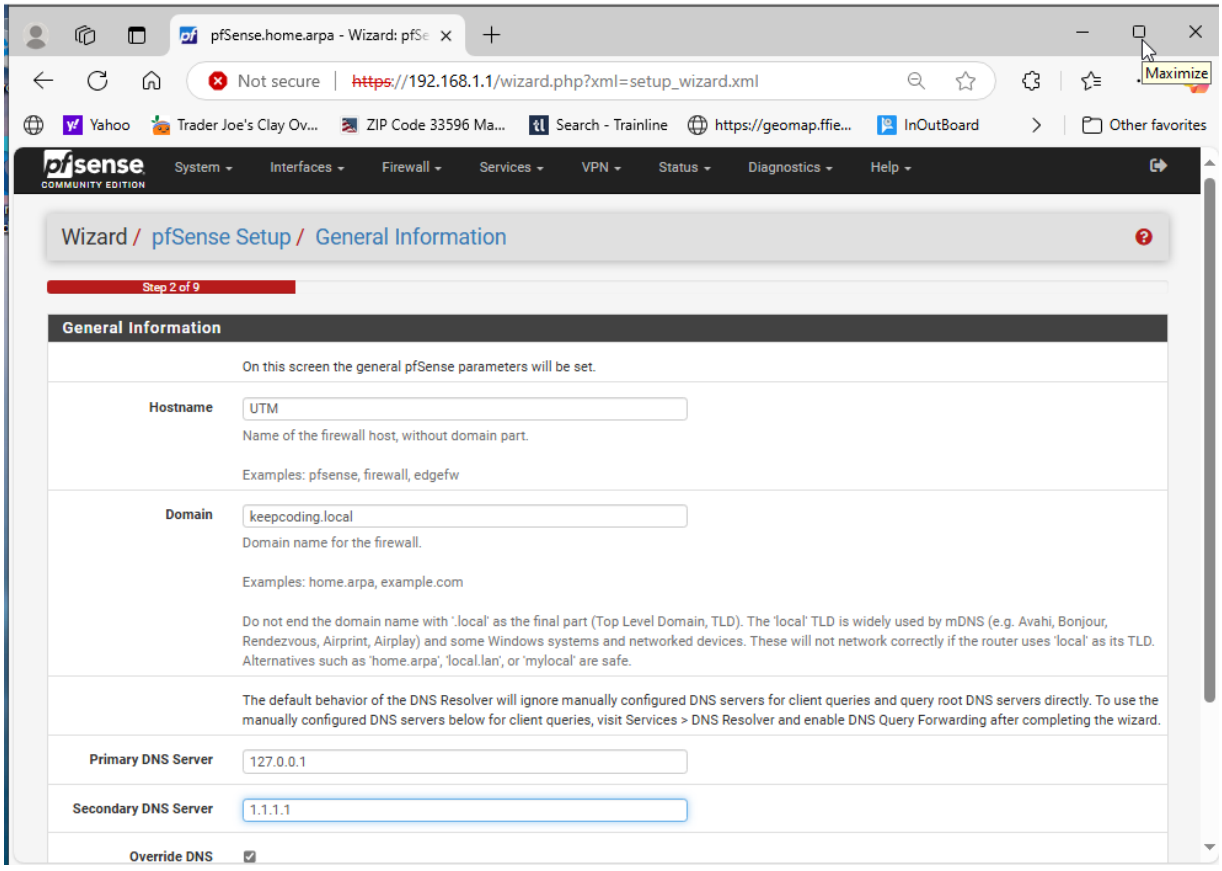

pfSense - Login
Not secure
https://192.168.1.1
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other fa
pfsense
Login to pfSens
SIGN IN
admin
SIGN IN

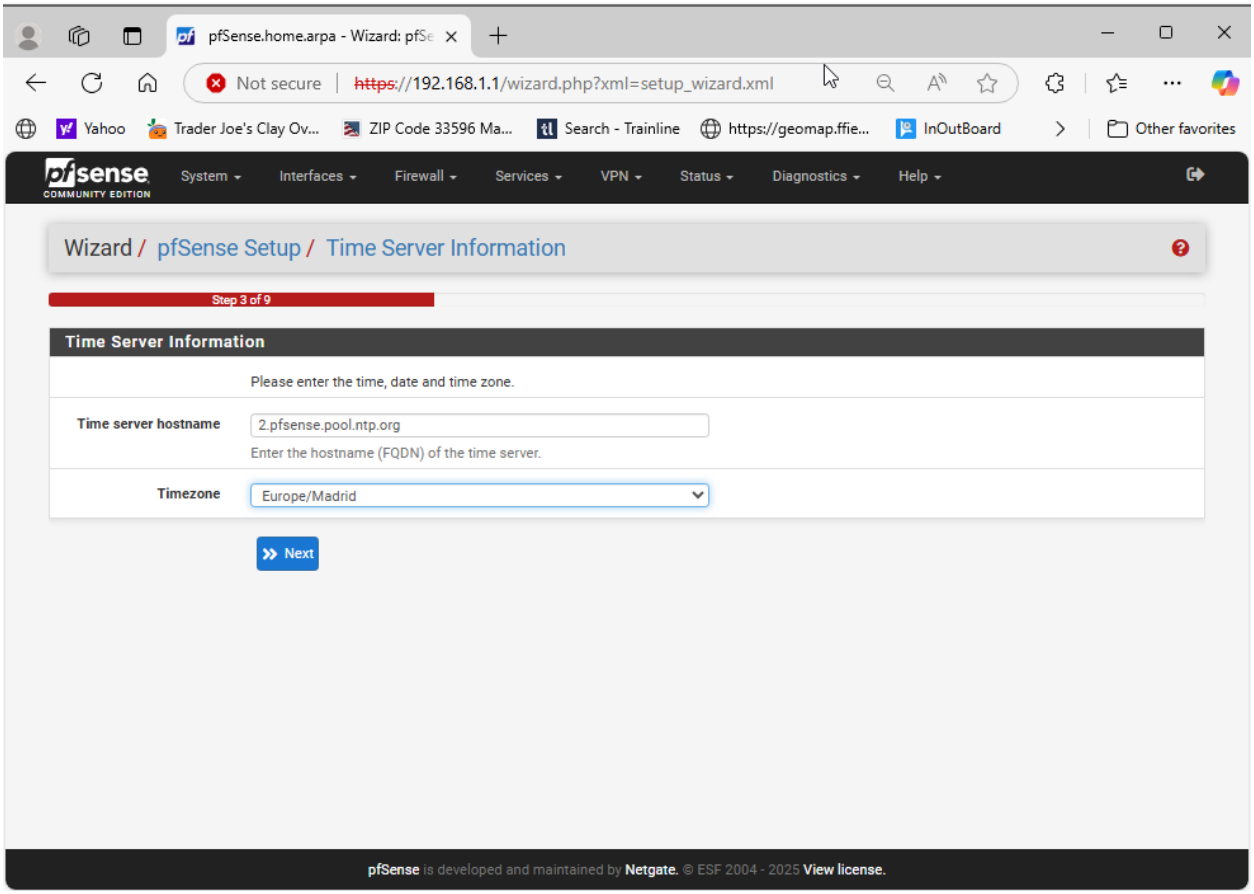

pfSense.home.arpa - Status: Dash
Not secure
https://192.168.1.1
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other favorites
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name
pfSense.home.arpa
User
admin@192.168.1.102 (Local Database)
System
VirtualBox Virtual Machine
Netgate Device ID: f510a30ced97d5736ca1
BIOS
Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006
Version
2.7.2-RELEASE (amd64)
built on Wed Dec 6 20:10:00 UTC 2023
FreeBSD 14.0-CURRENT
The system is on the latest version.
Version information updated at Sat Jan 11 14:42:49 UTC 2025
CPU Type
12th Gen Intel(R) Core(TM) i7-12700H
2 CPUs: 1 package(s) x 2 cache groups x 1 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto
Inactive
Kernel PTI
Disabled
MDS Mitigation
Inactive
Netgate Services And Support
Contract type
Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Upgrade Your Support
Community Support Resources
Netgate Global Support FAQ
Official pfSense Training by Netgate
Netgate Professional Services
Visit Netgate.com
If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.


UTM Blue Team [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: f510a30ced97d5736ca1
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.207/24
v6/DHCP6: 2a0c:5a87:8401:e500:a00:27ff:febf:3260/64
LAN (lan) -> em1 -> 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:
Right Ctrl

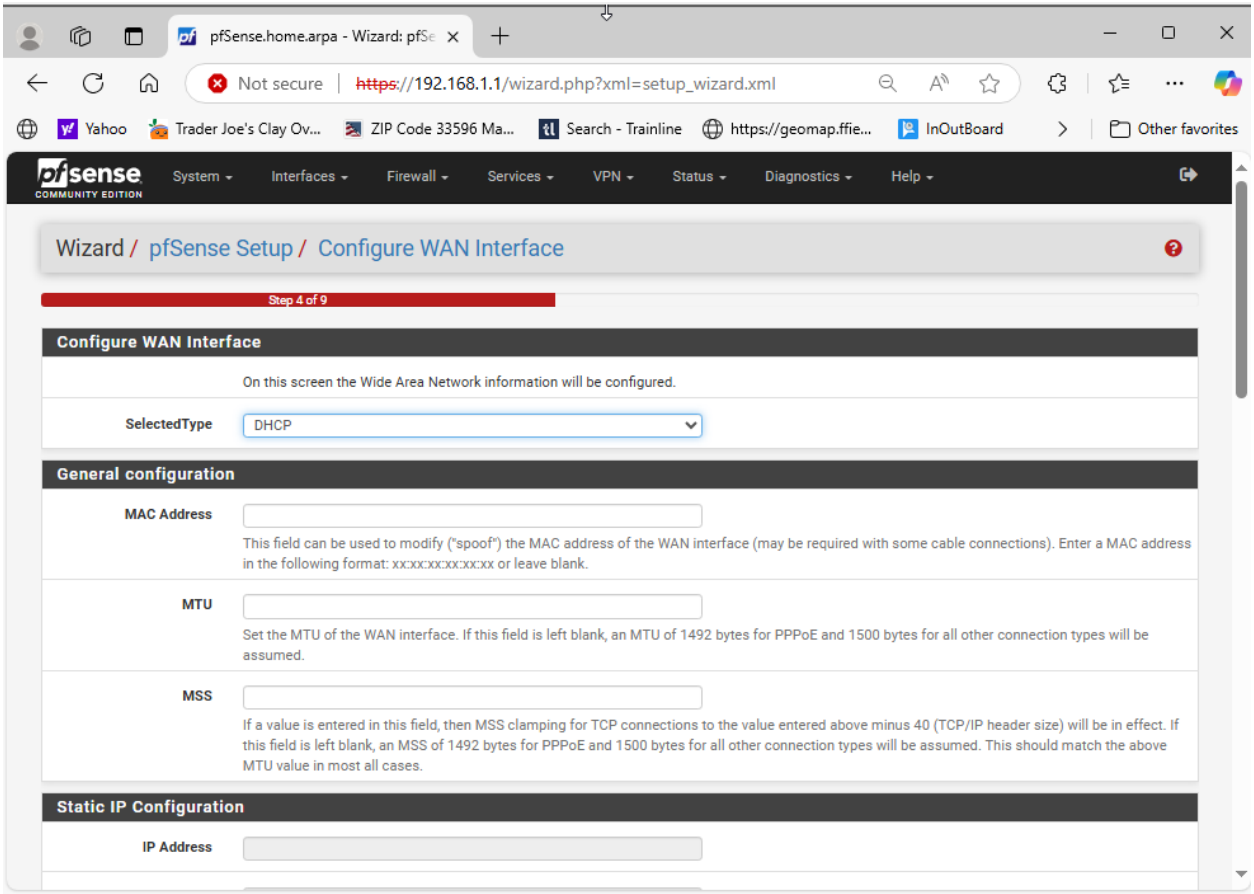
We now proceed with the PFSense Setup (establishing the domain and the DNS Servers)

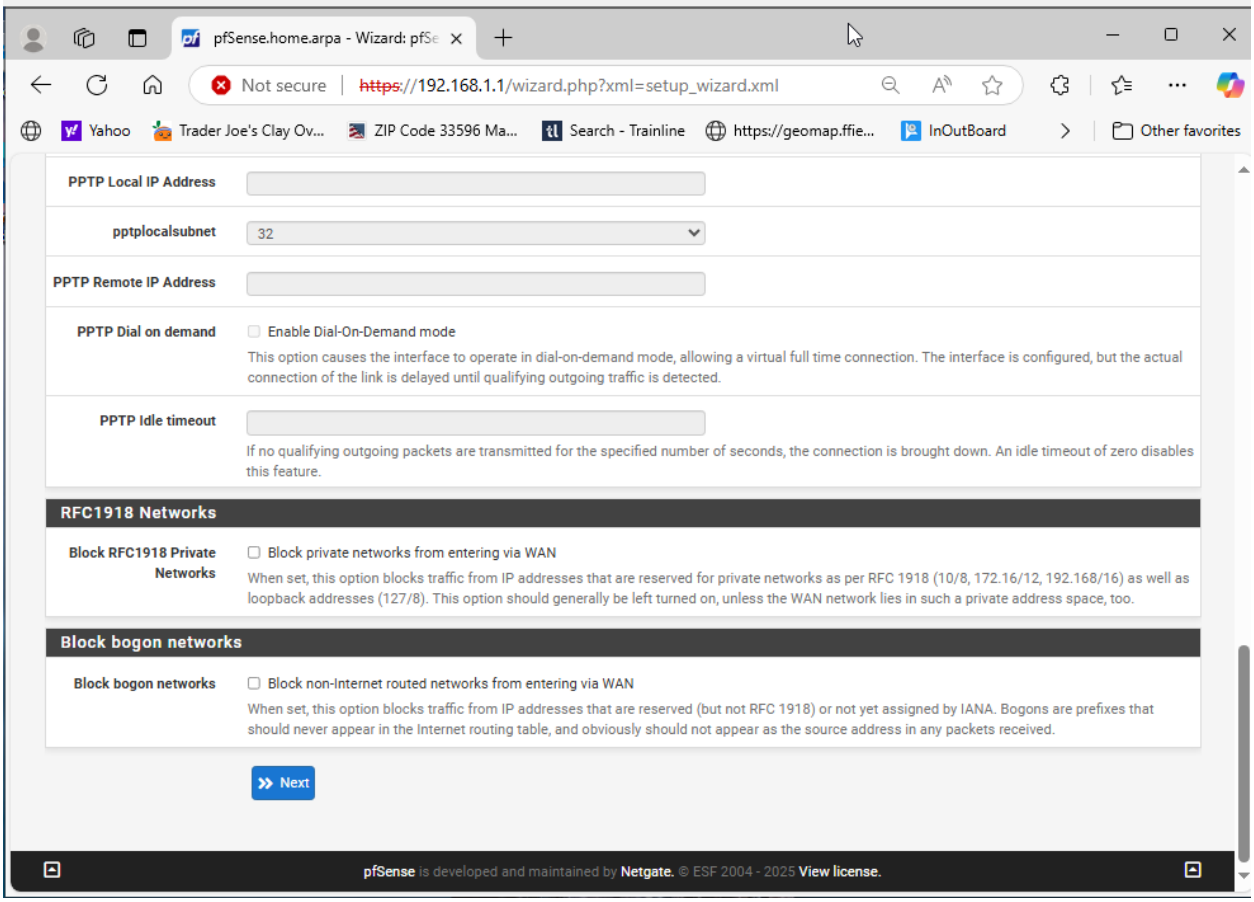




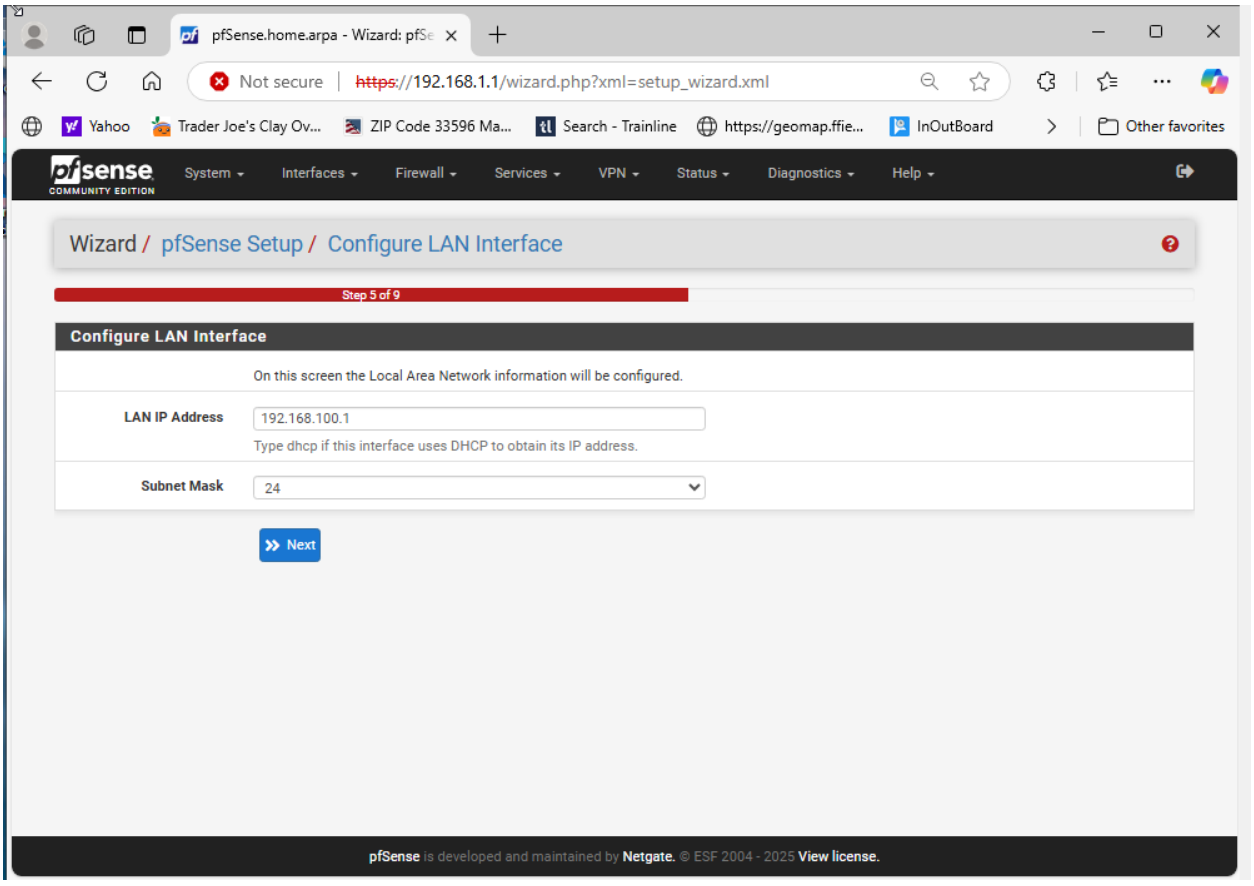


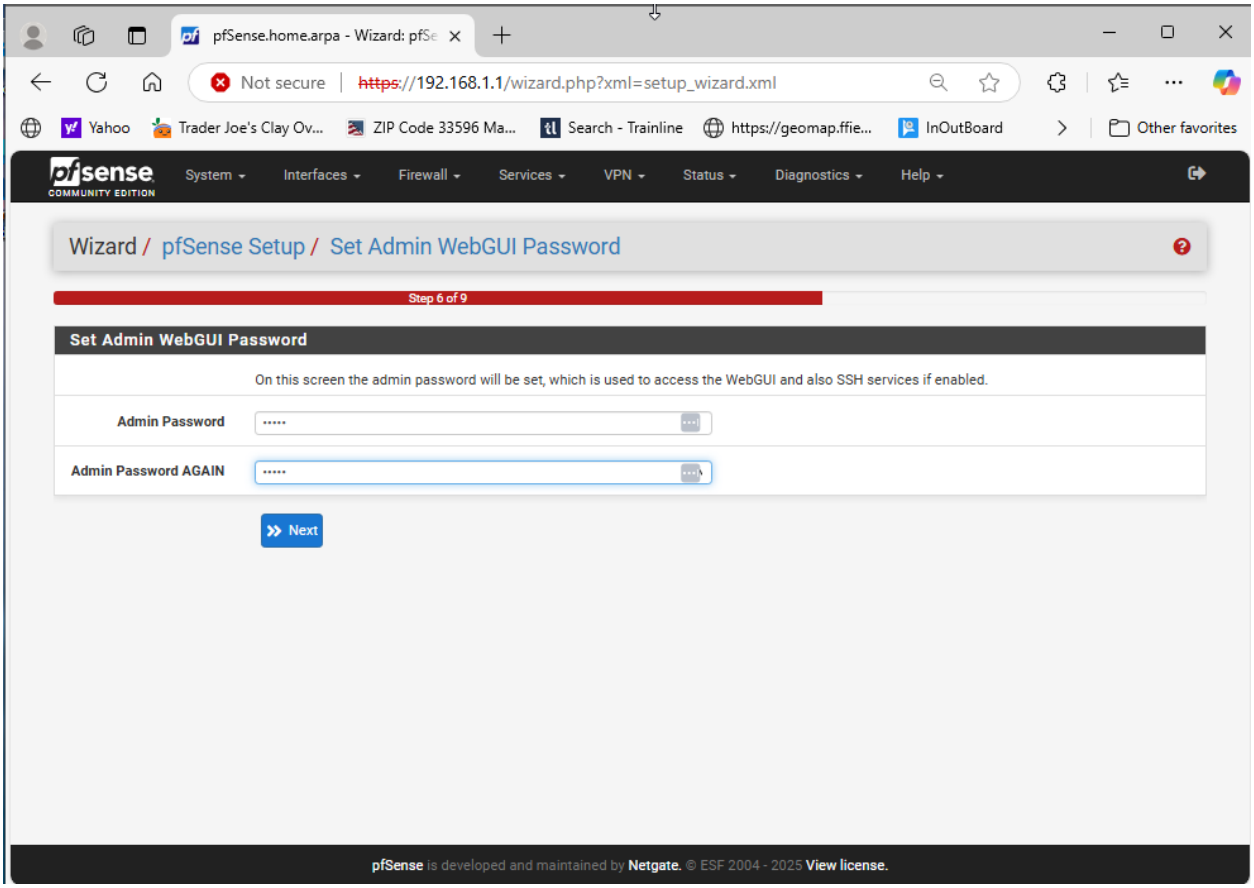
WAN Interface Configuration

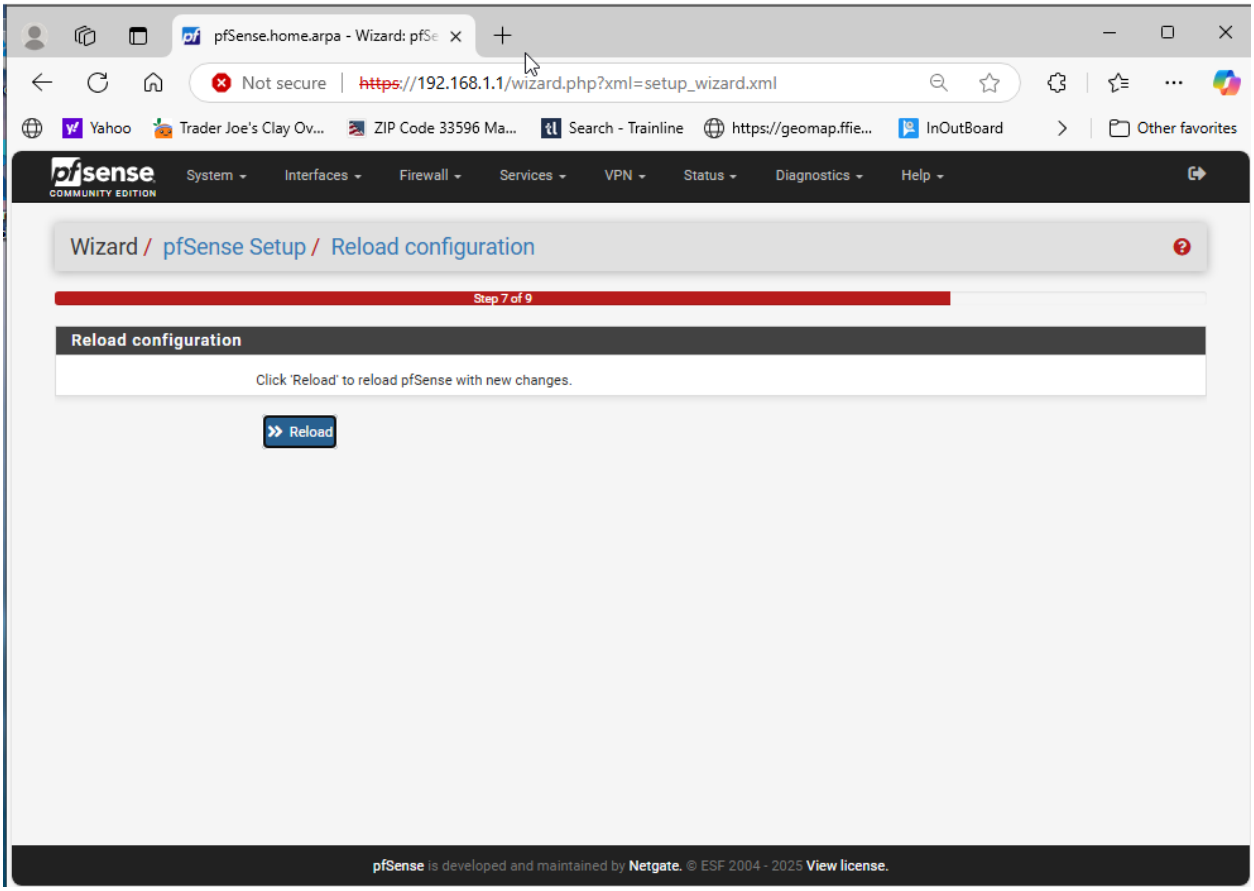


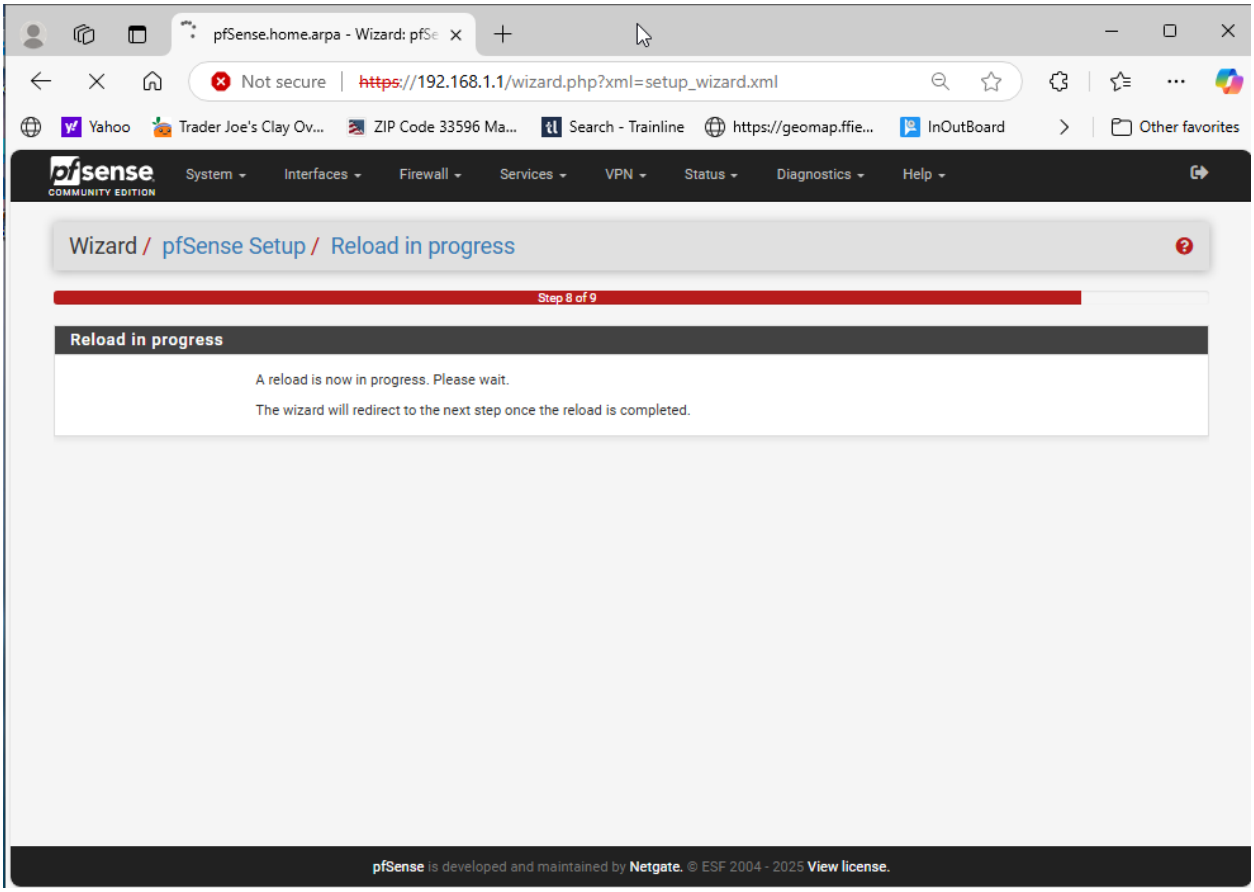


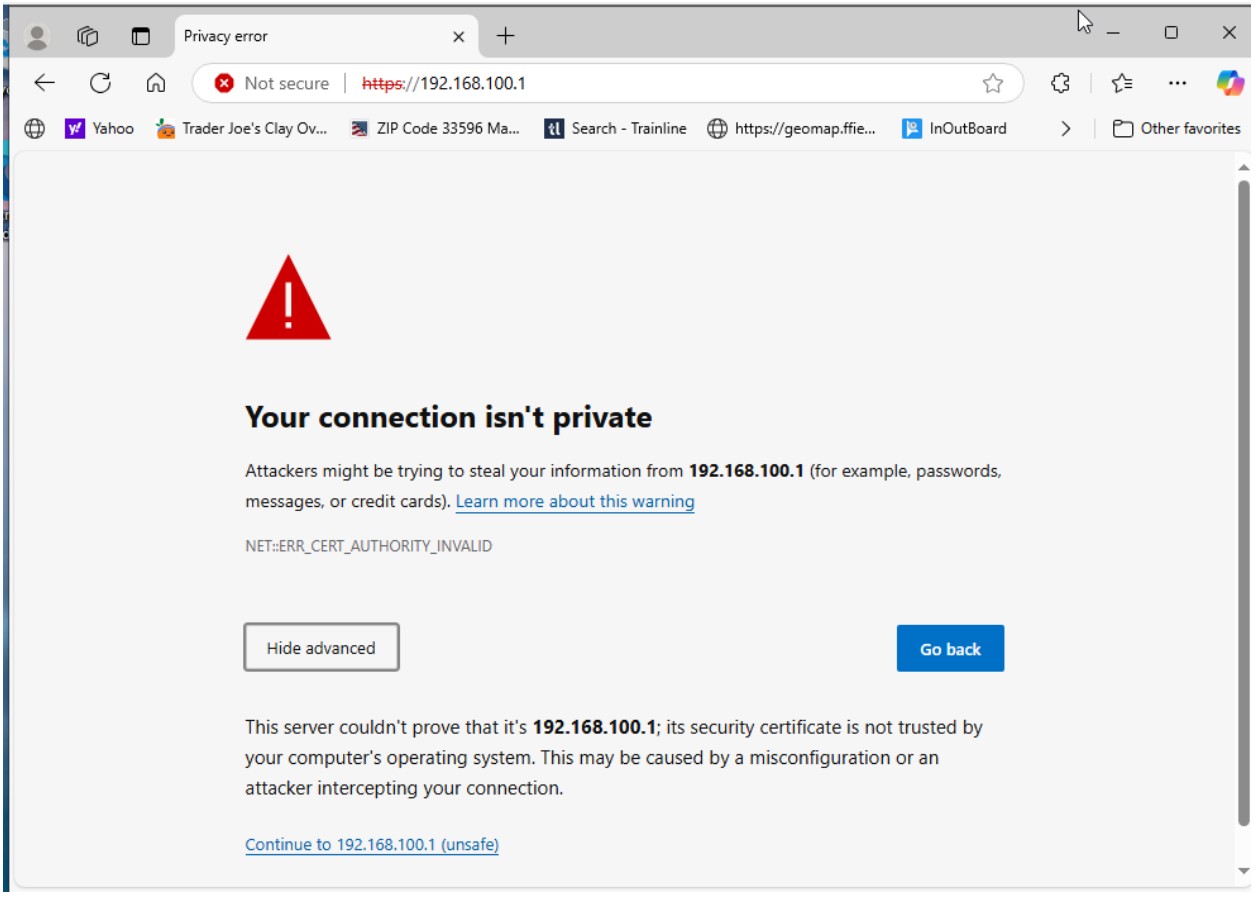
LAN Interface Configuration (we now select a different IP to give 192.168.1.1 back to the router)



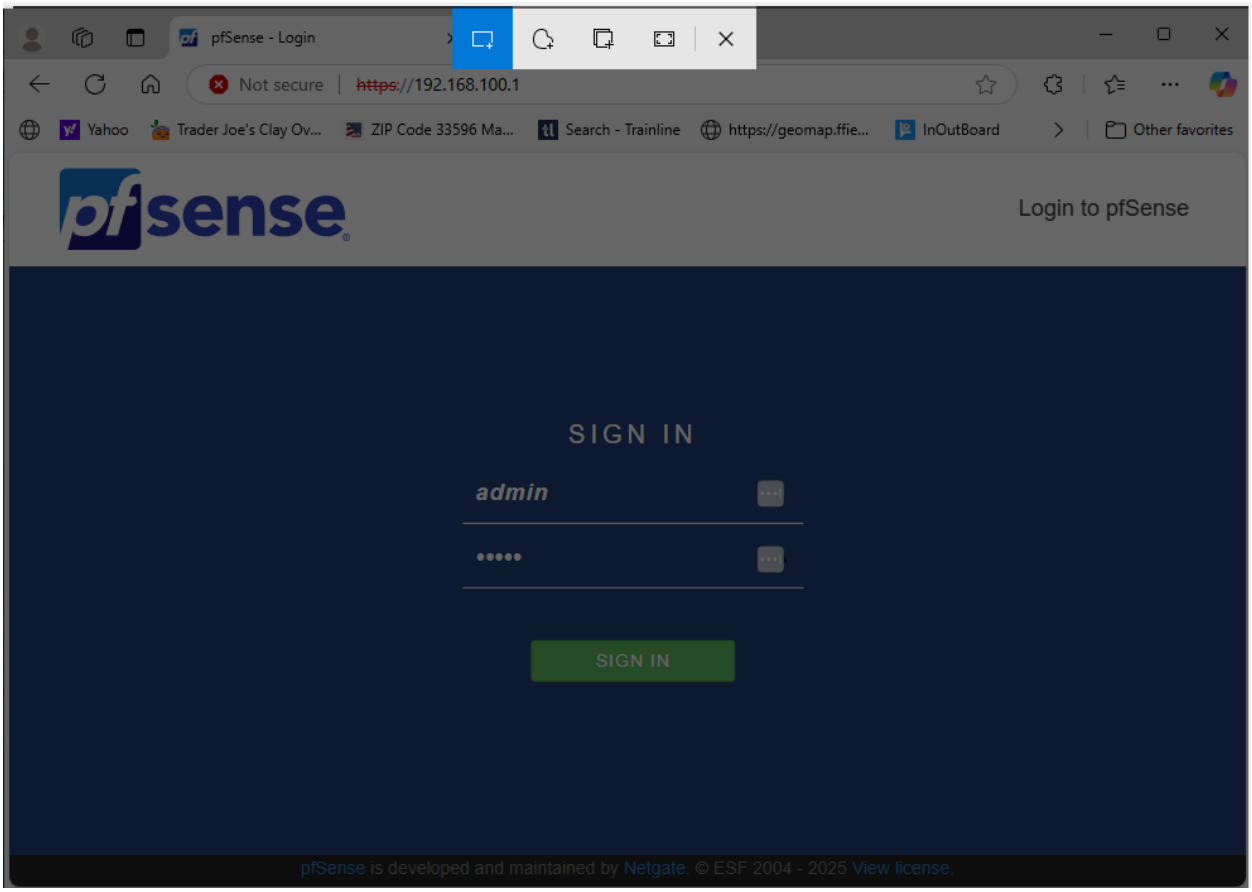

pfSense.home.arpa - Wizard: pfSe
Not secure
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other favorites
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Set Admin WebGUI Password
Step 6 of 9
Set Admin WebGUI Password
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.
Admin Password
Admin Password AGAIN
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

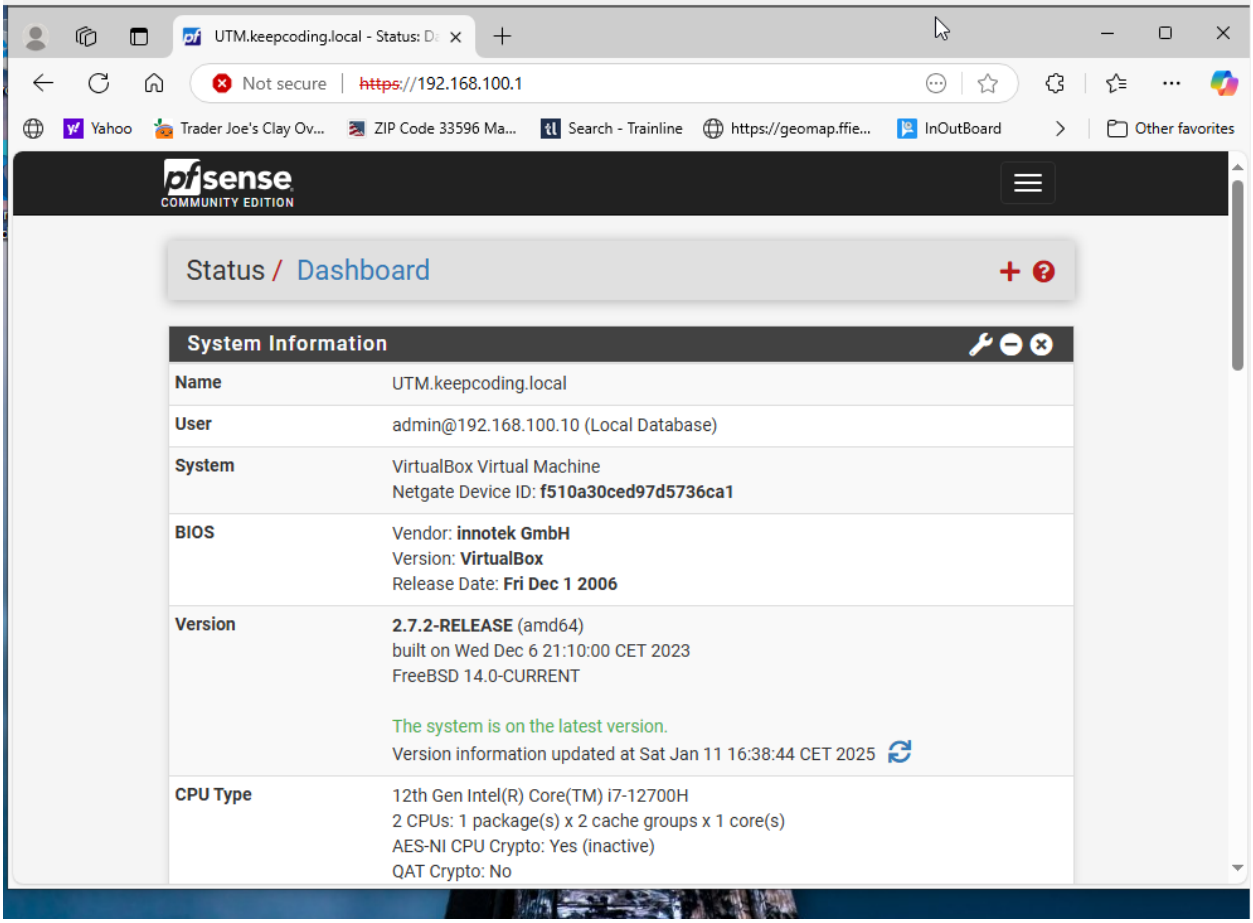

pfSense.home.arpa - Wizard: pfSe
Not secure
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other favorites
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Reload configuration
Step 7 of 9
Reload configuration
Click 'Reload' to reload pfSense with new changes.
Reload
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.


pfSense.home.arpa - Wizard: pfSe
Not secure
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other favorites
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Reload in progress
Step 8 of 9
Reload in progress
A reload is now in progress. Please wait.
The wizard will redirect to the next step once the reload is completed.
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

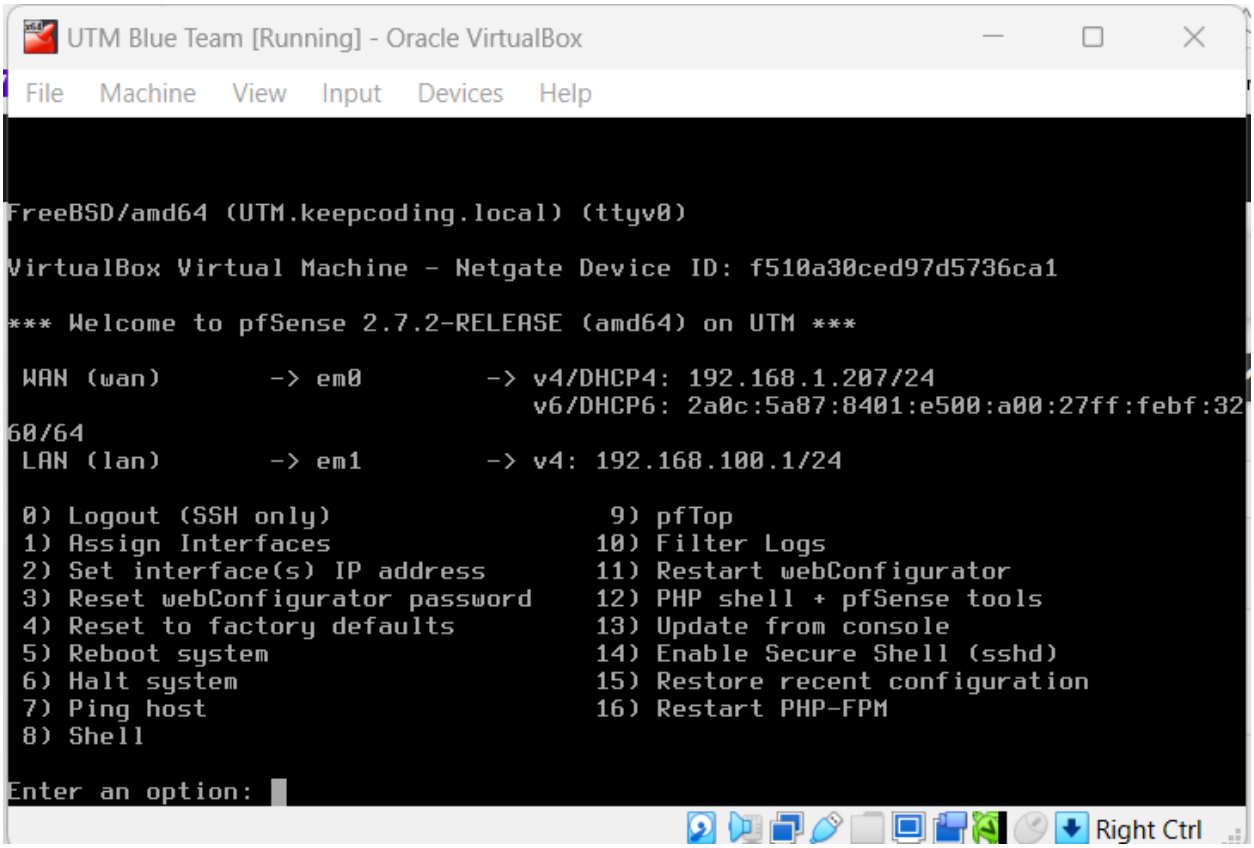

Privacy error
Not secure
https://192.168.100.1
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other favorites
Your connection isn't private
Attackers might be trying to steal your information from 192.168.100.1 (for example, passwords, messages, or credit cards). Learn more about this warning
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Go back
This server couldn't prove that it's 192.168.100.1; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Continue to 192.168.100.1 (unsafe)

Log back in to PFSense with the newly-assigned IP address

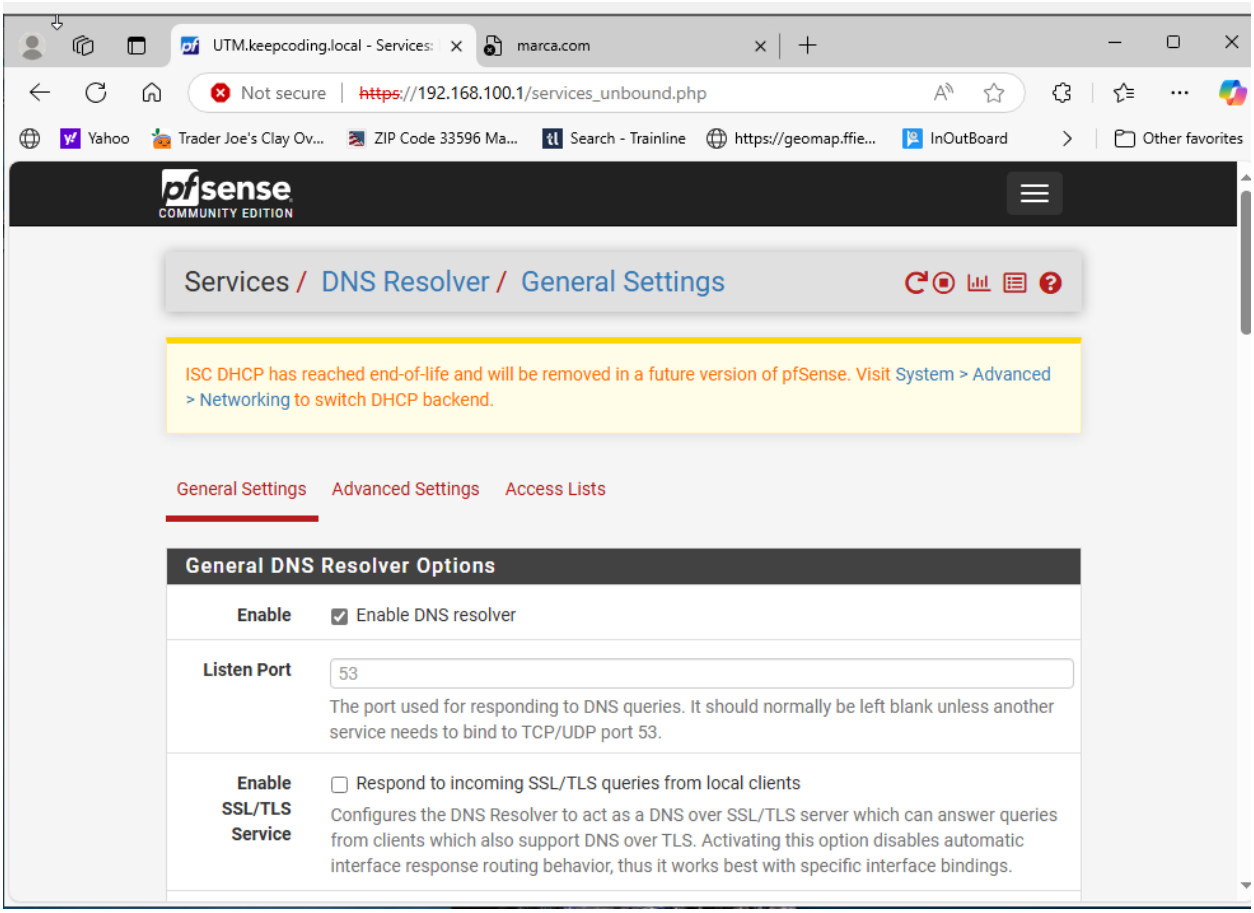


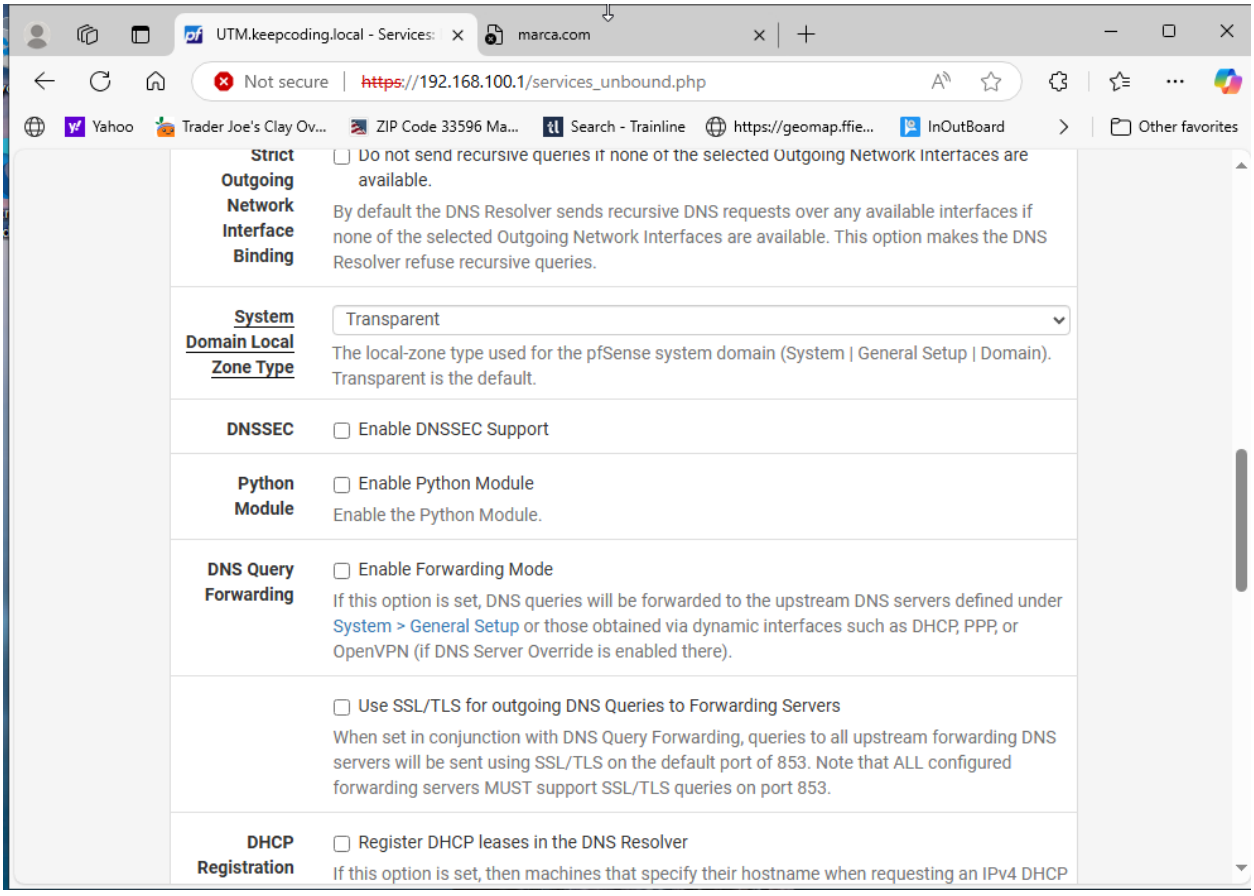



pfsense
COMMUNITY EDITION
Command Prompt
C:\Users\rabri>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : keepcoding.local
Link-local IPv6 Address . . . . . : fe80::3e3d:34c0:9add:6e49%15
IPv4 Address. . . . . : 192.168.100.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a00:27ff:fe97:ae20%15
192.168.100.1
C:\Users\rabri>

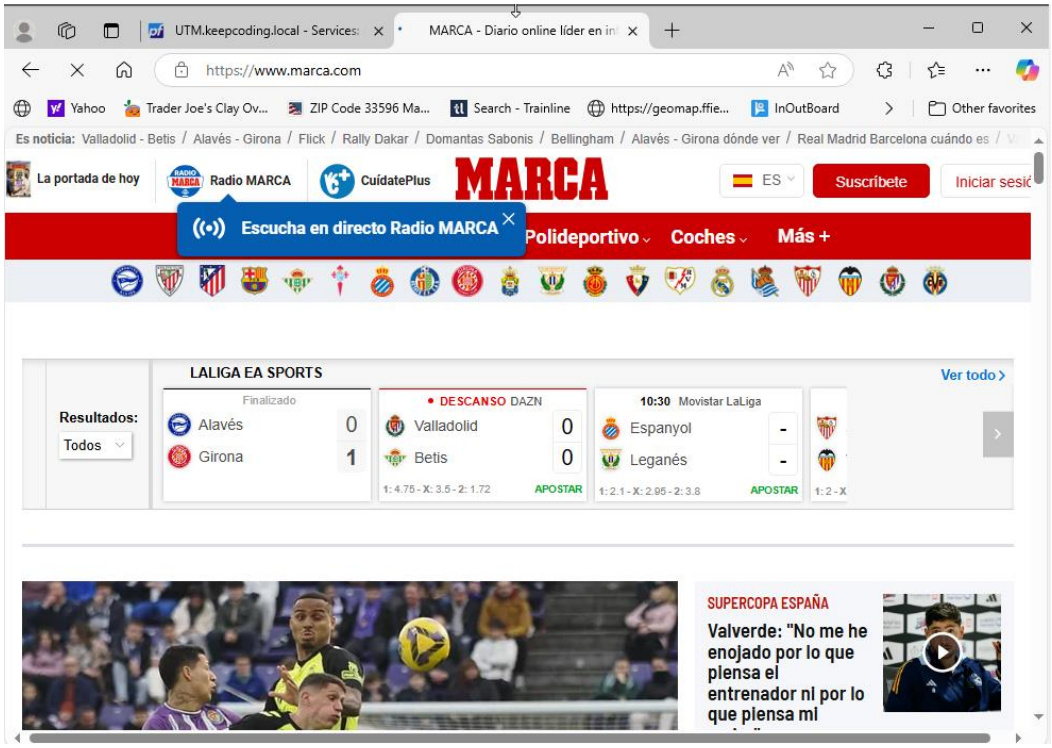

UTM Blue Team [Running] - Oracle VirtualBox
File Machine View Input Devices Help
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: f510a30ced97d5736ca1
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.207/24
v6/DHCP6: 2a0c:5a87:8401:e500:a00:27ff:febf:32
60/64
LAN (lan) -> em1 -> v4: 192.168.100.1/24
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:
Right Ctrl

DNS Resolver settings

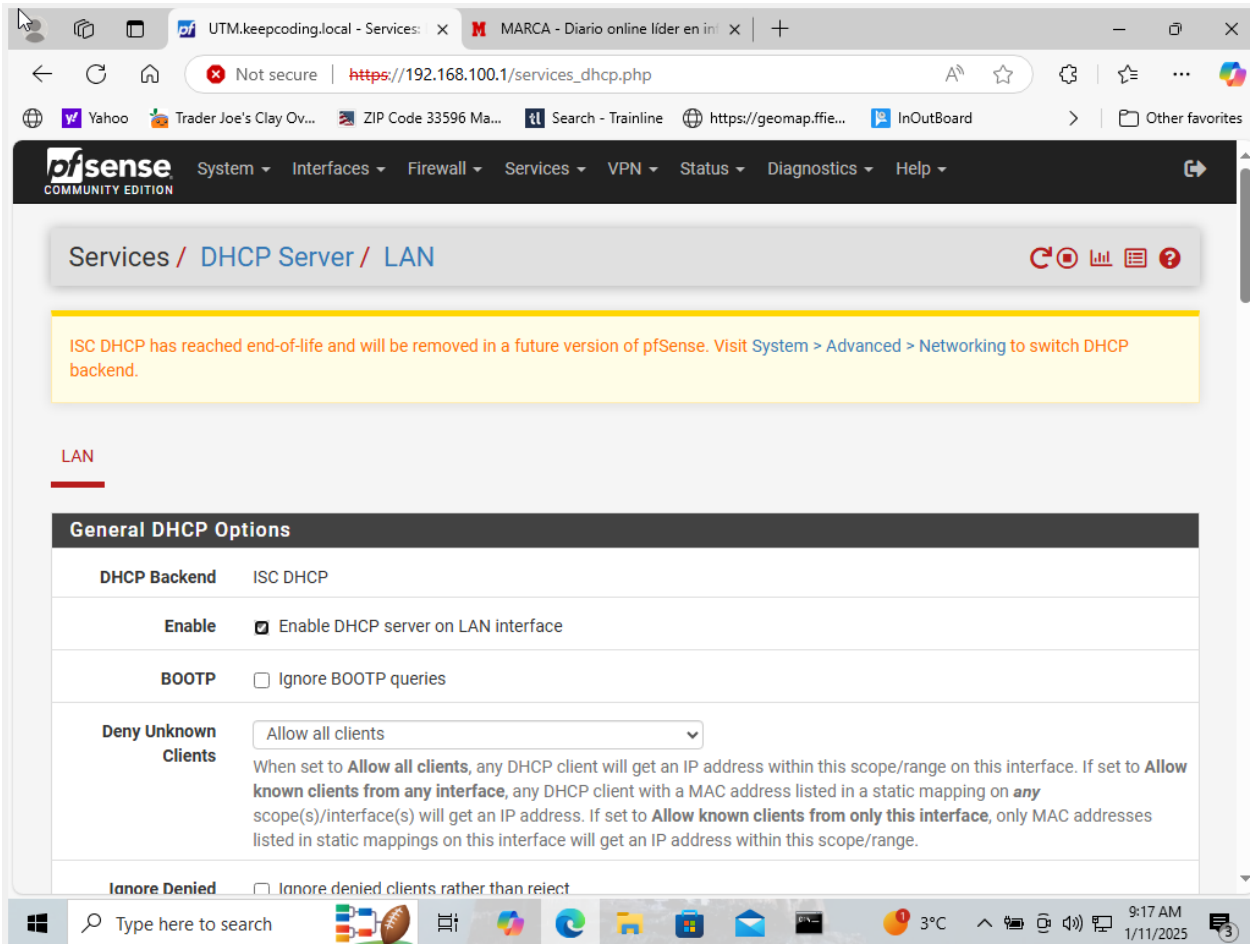




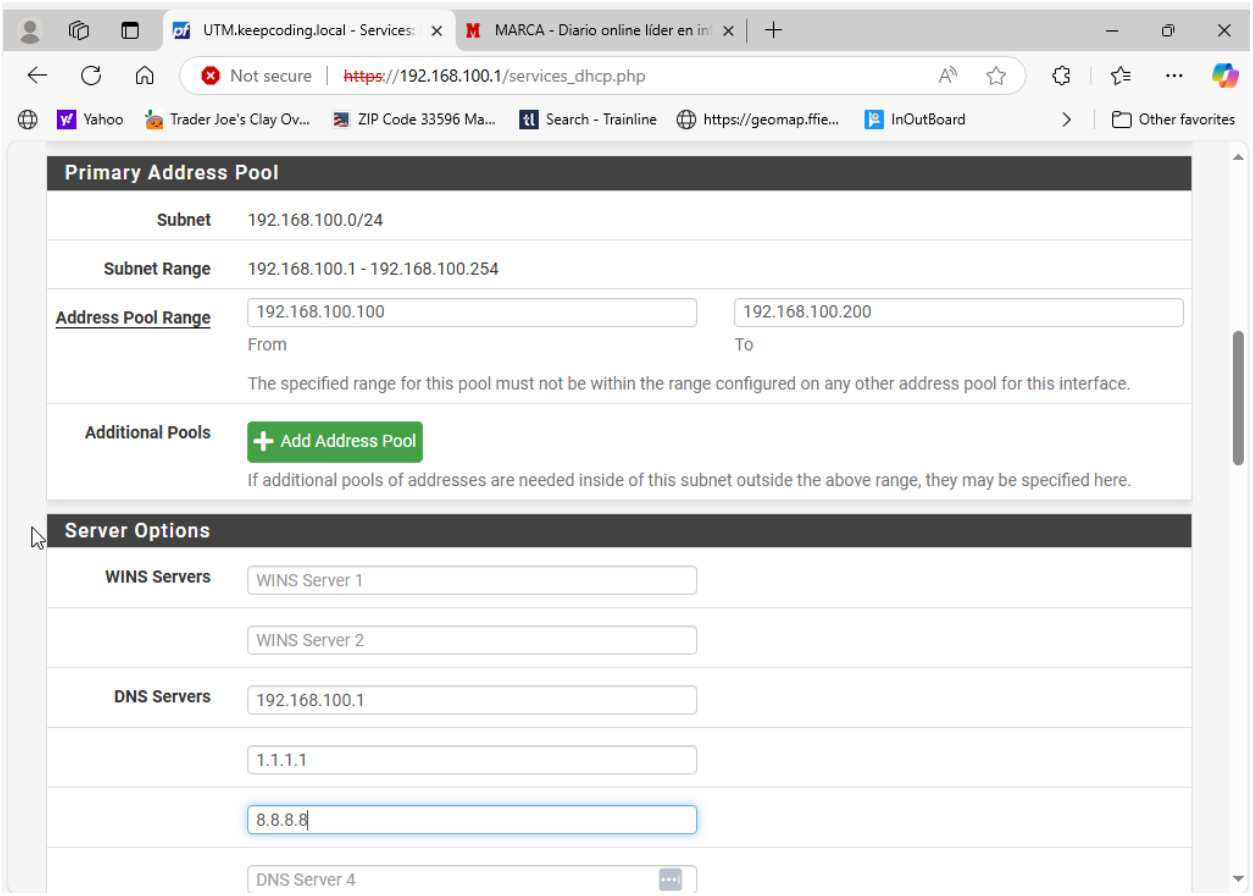
Internet Accessibility



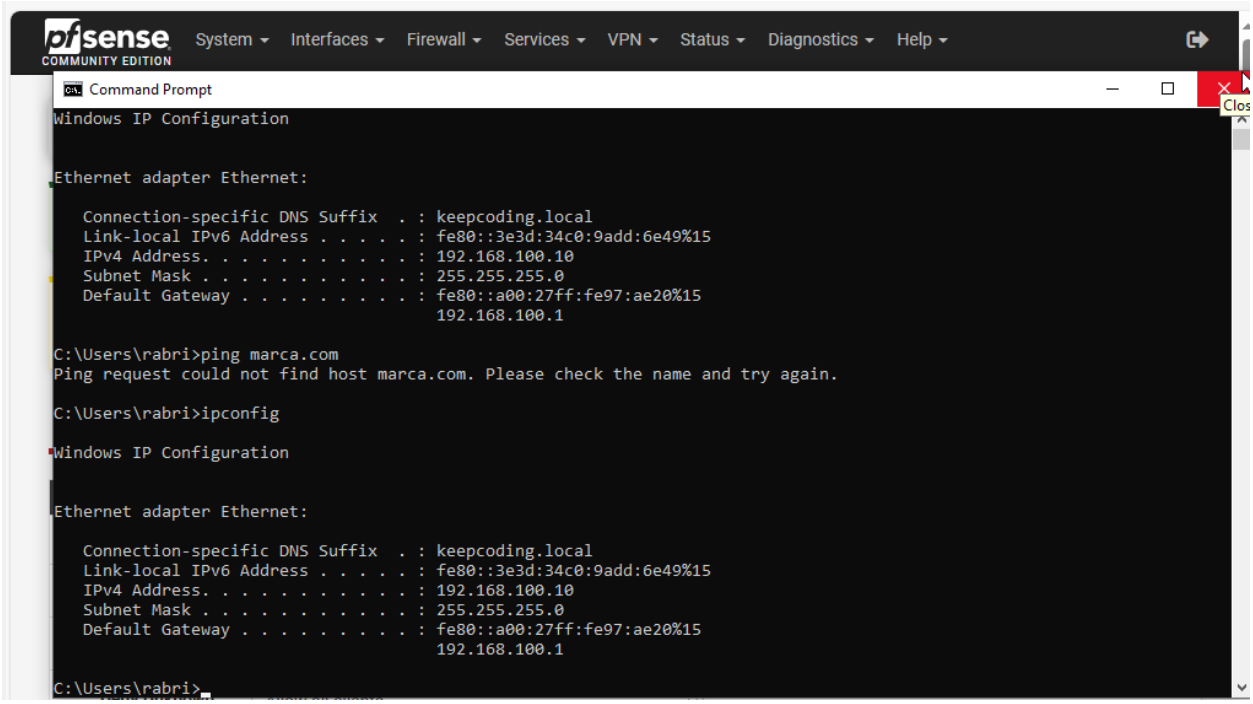
DHCP Server / LAN Configuration



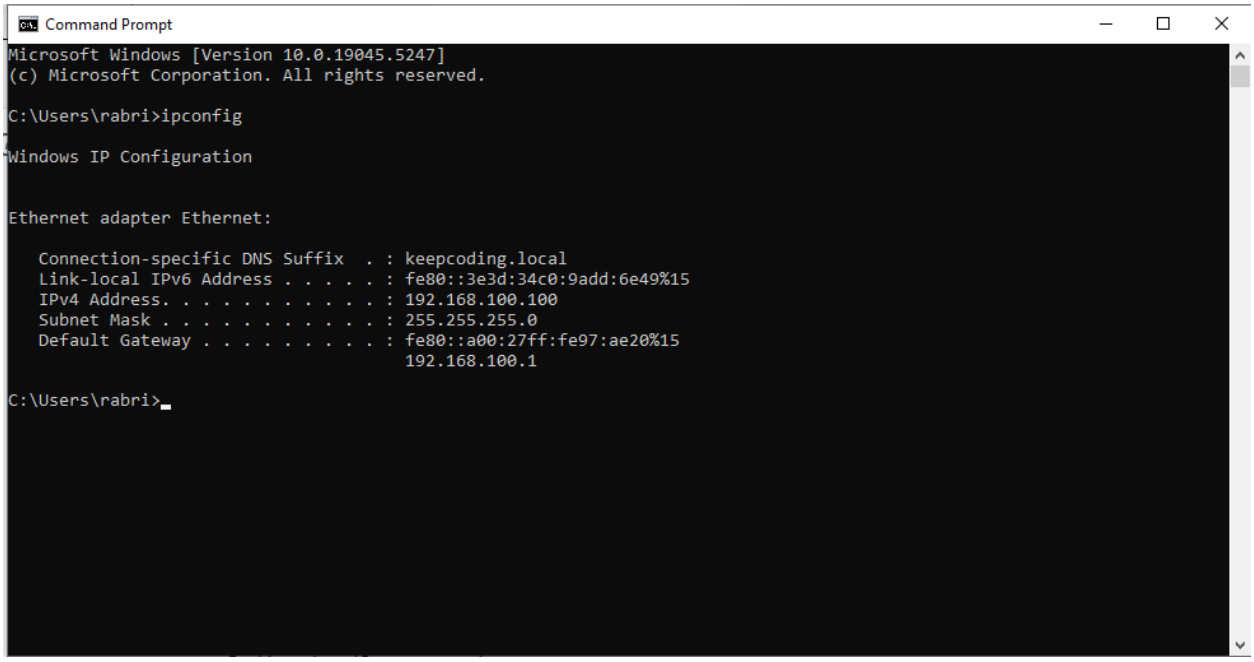
We assign a range of IP addresses to LAN and establish the DNS Servers



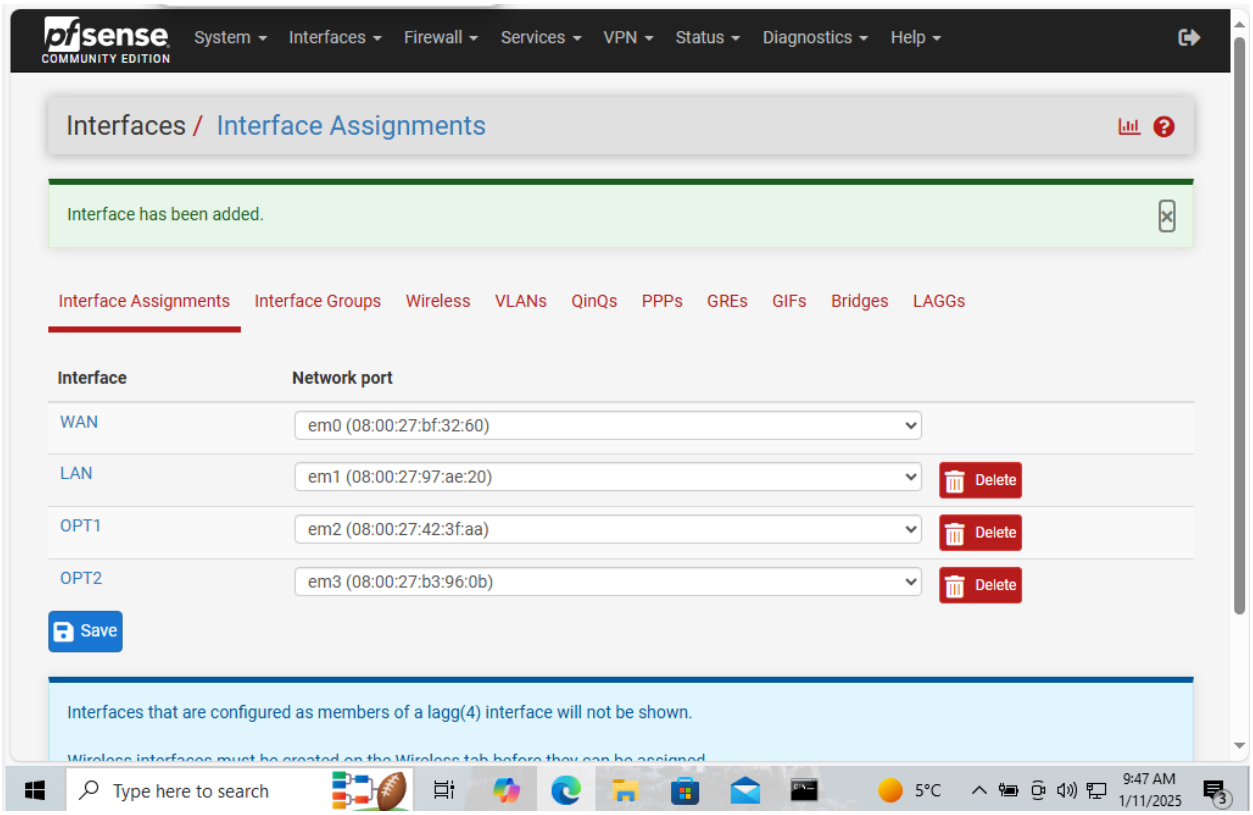
Previous IP Address: 192.168.100.10



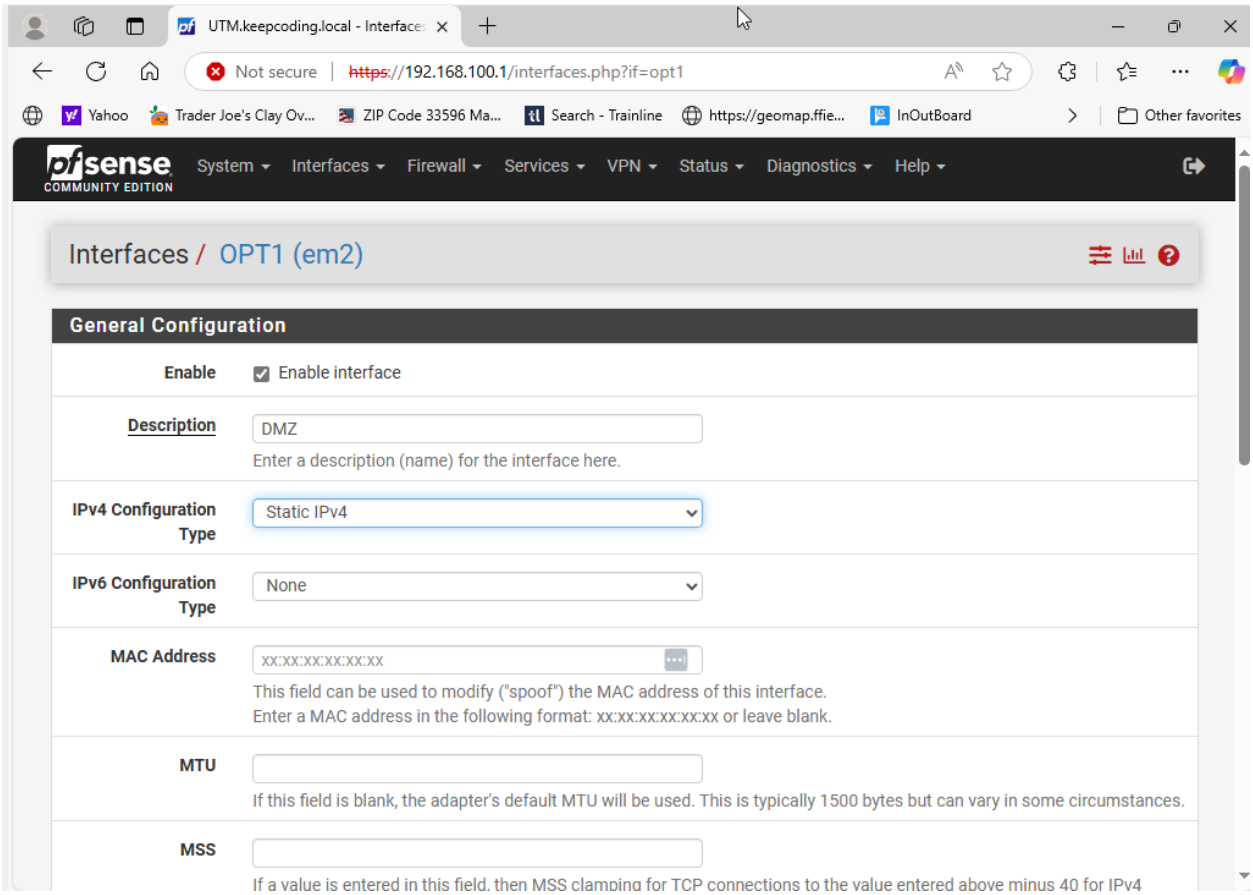
New IP Address: 192.168.100.100

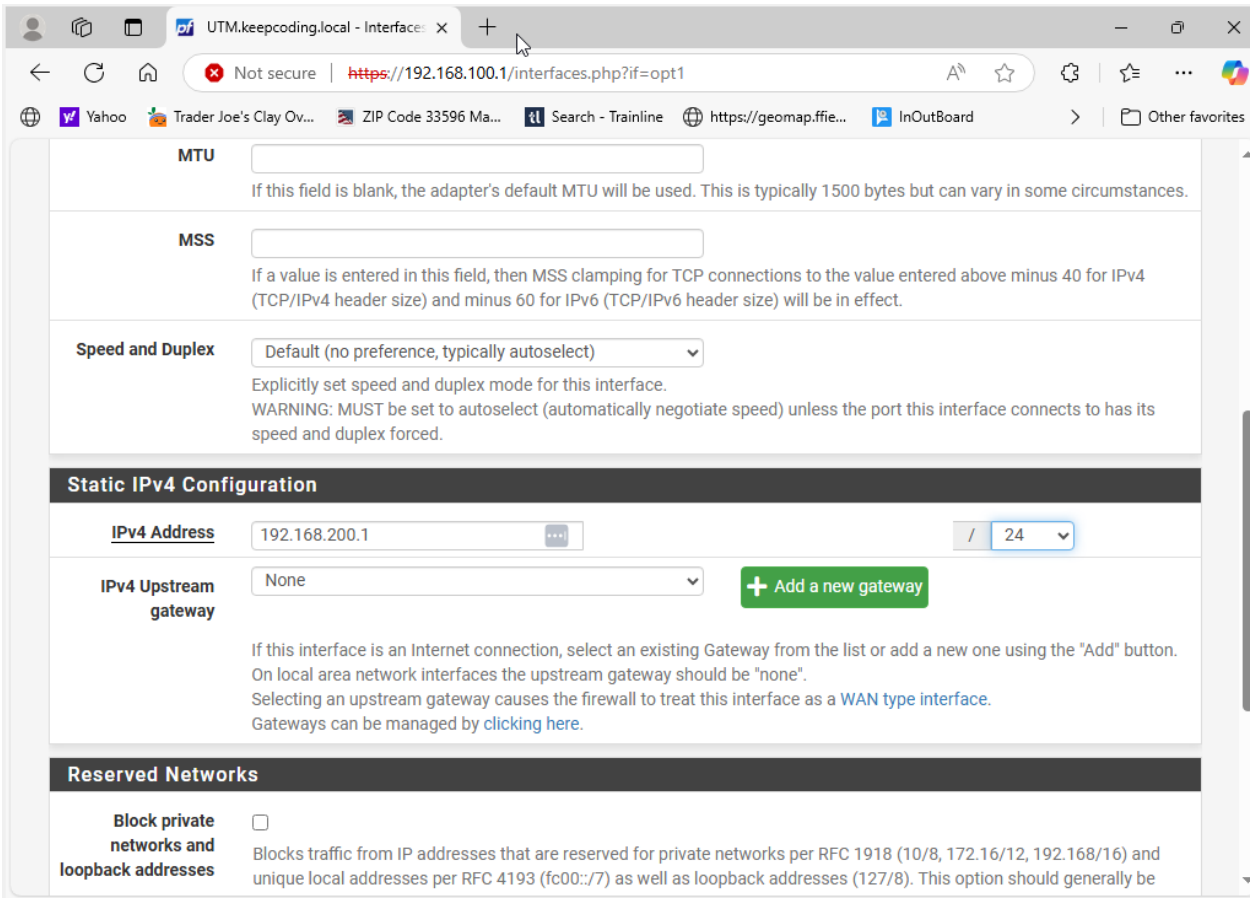


Interface Assignments to configure WAN, LAN, DMZ and DMZ2

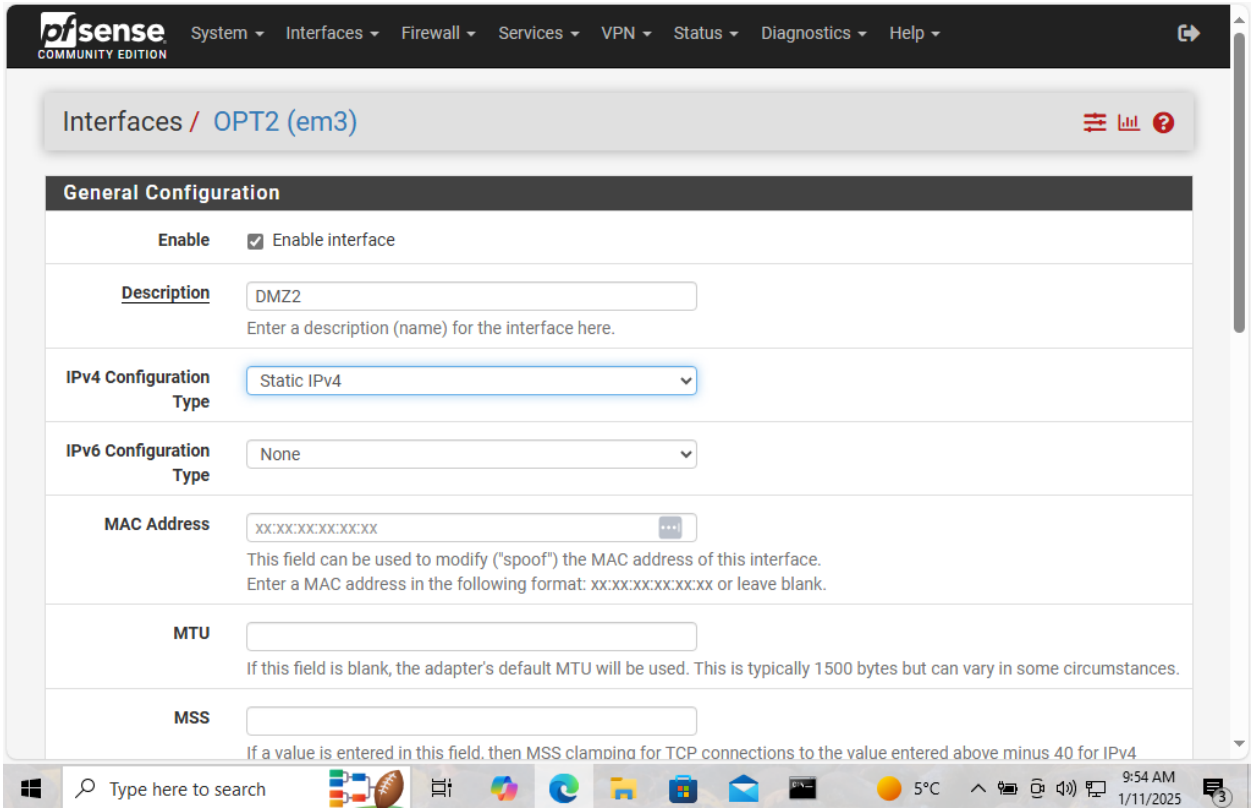


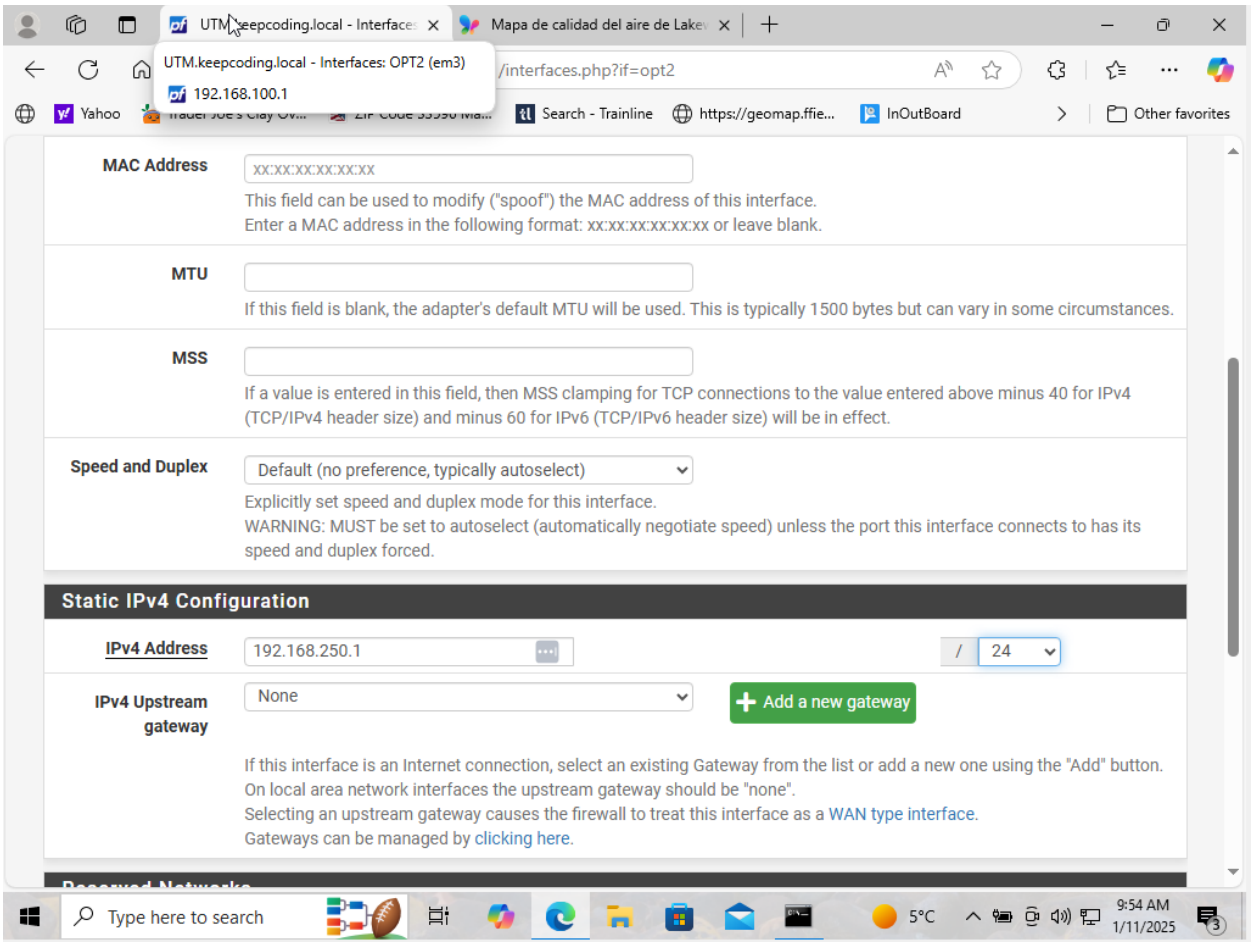
Establishing OPT1 Interface as DMZ and assignment of a static IPv4



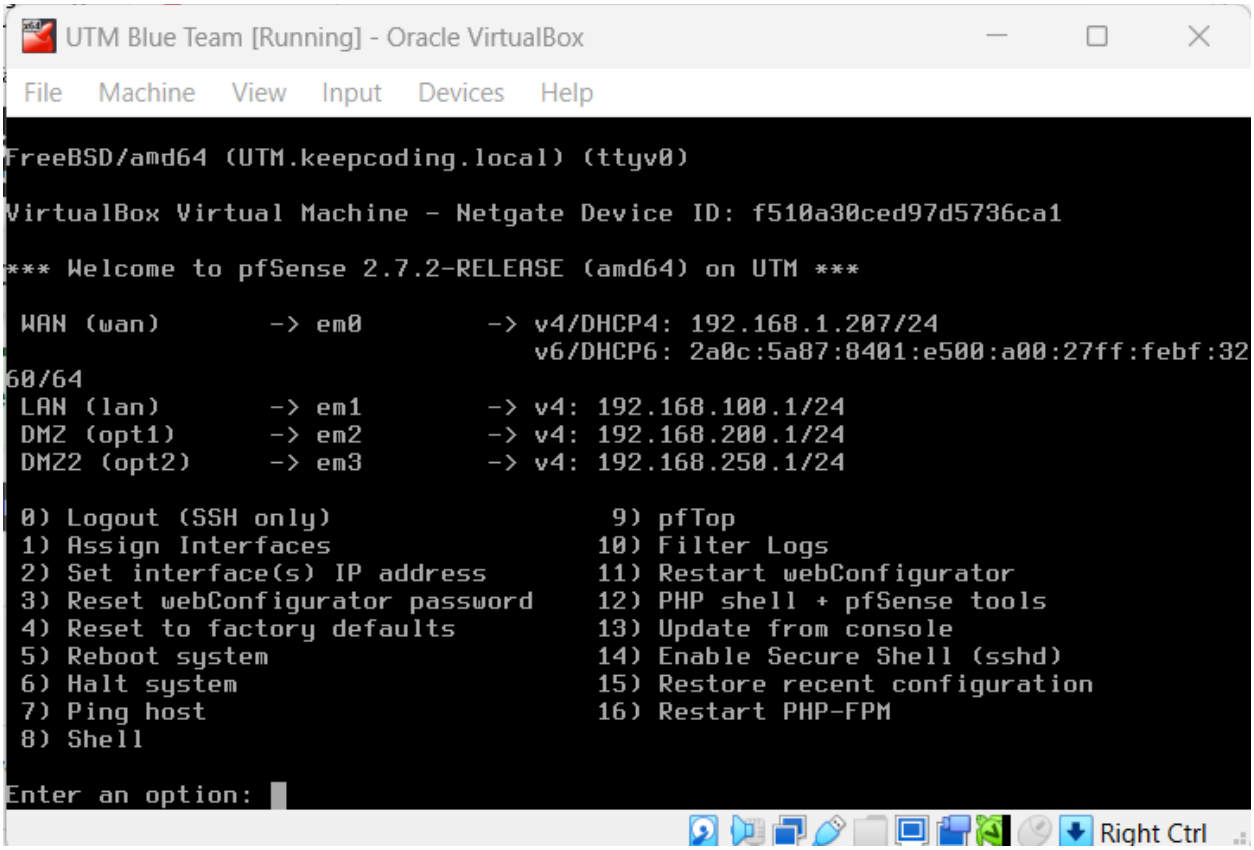


Establishing OPT2 Interface as DMZ2 and assignment of a static IPv4

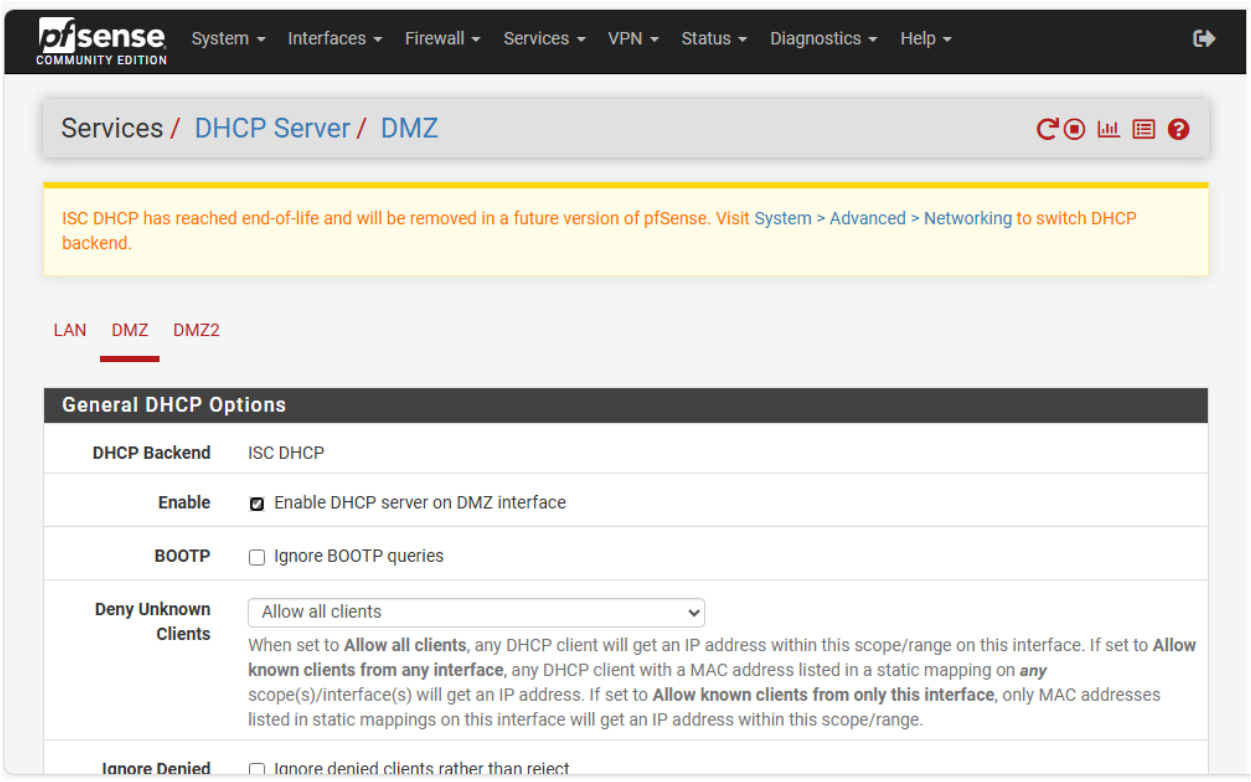




Checking the Configuration and IPs of WAN, LAN, DMZ and DMZ2



Configuration of the DHCP Server on DMZ, Assignment of a Specific IP Range and the DNS Servers



Primary Address Pool

Subnet	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	192.168.200.100 (From) — 192.168.200.150 (To) The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

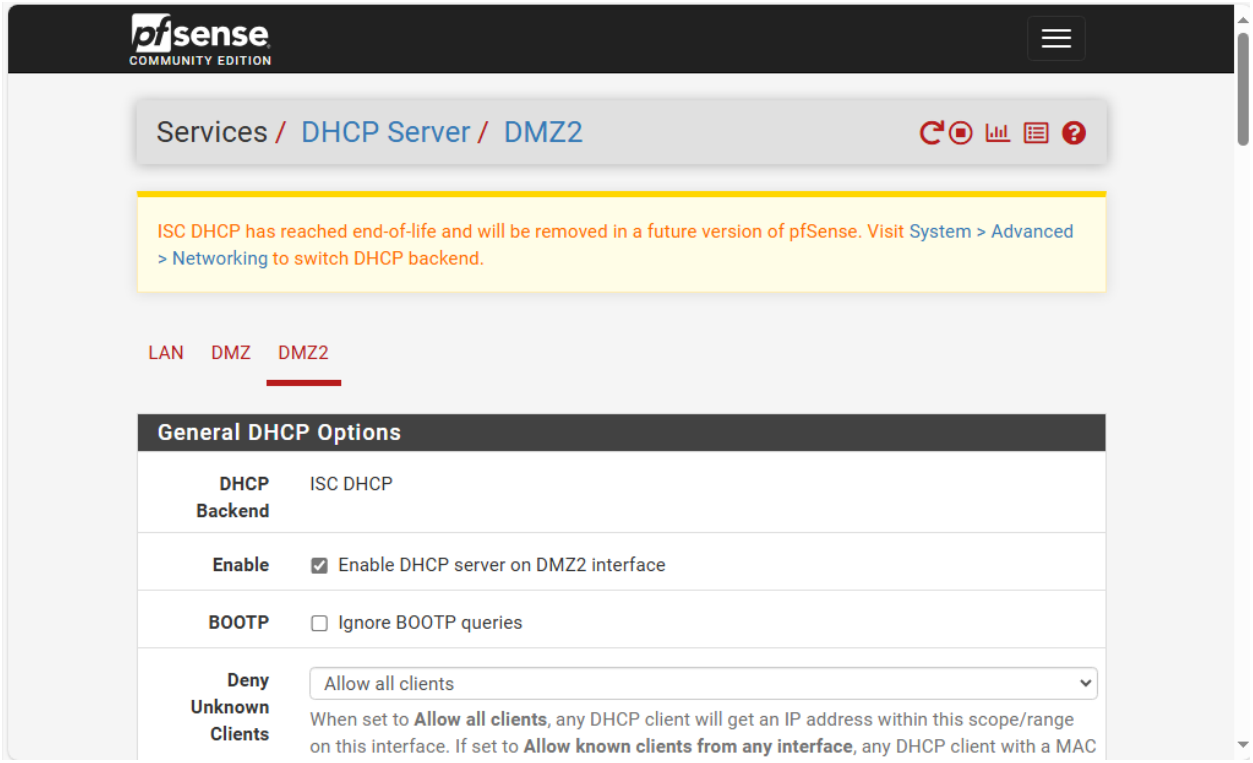
Server Options

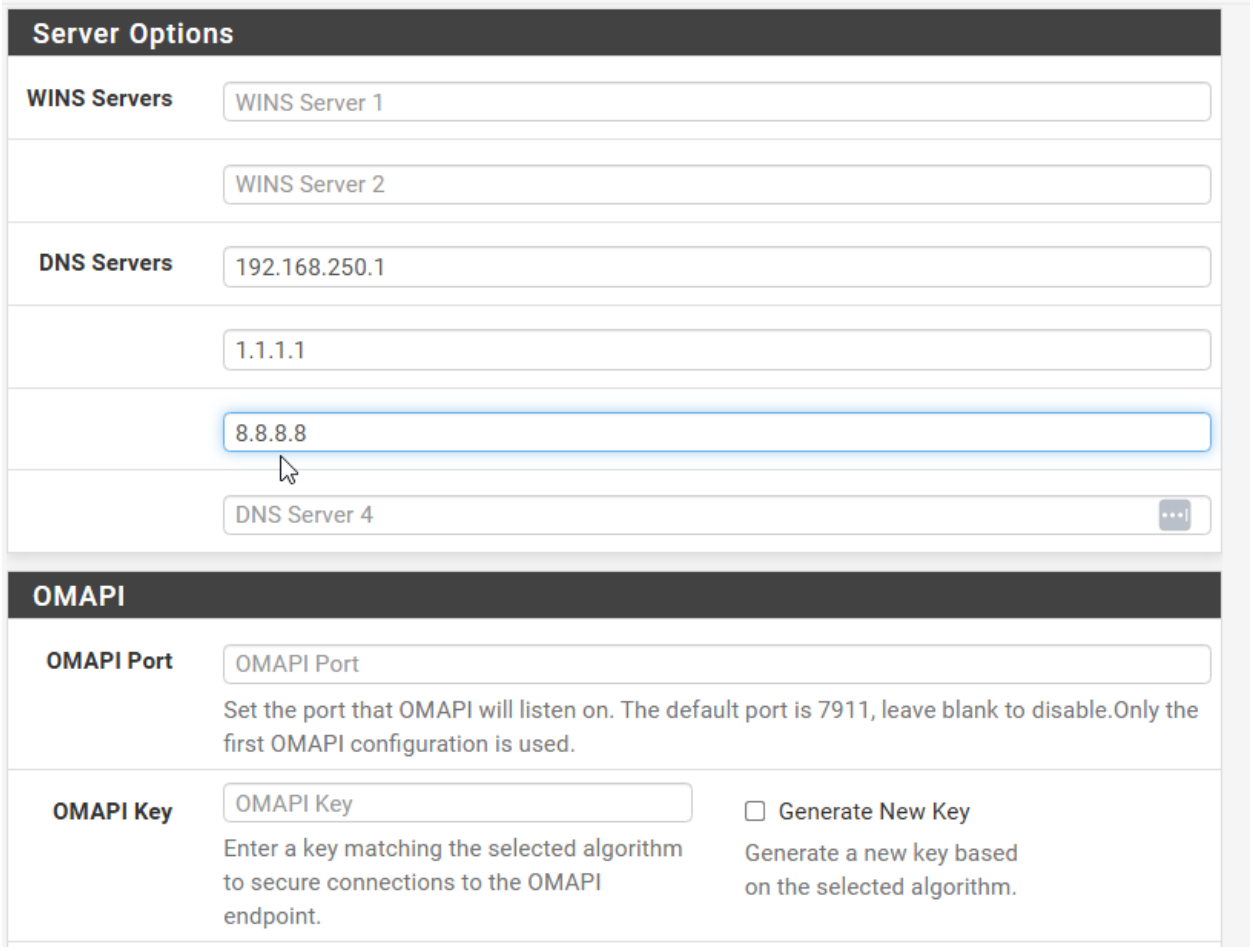
WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.200.1
	1.1.1.1
	8.8.8.8

Other DHCP Options

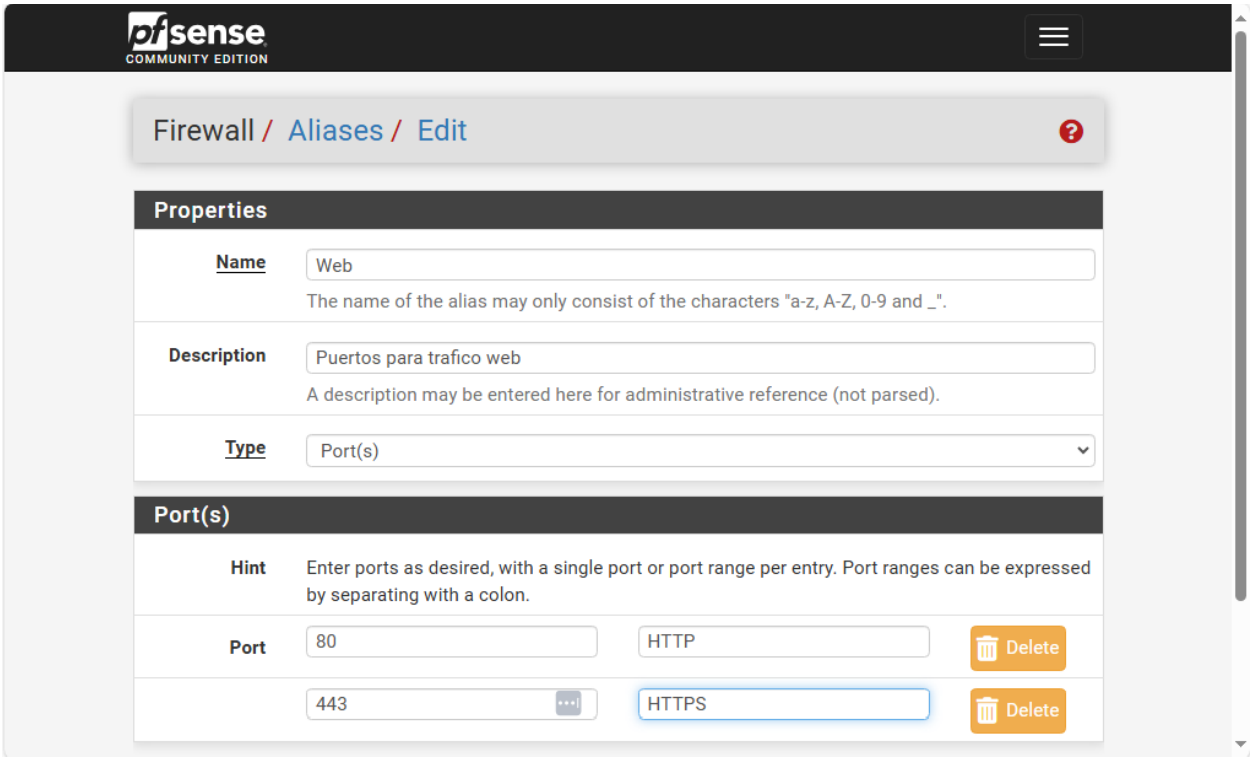
Gateway	192.168.200.1 The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name	keepcoding.local The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List	example.com;sub.example.com The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time	7200 This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time	86400 This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer	

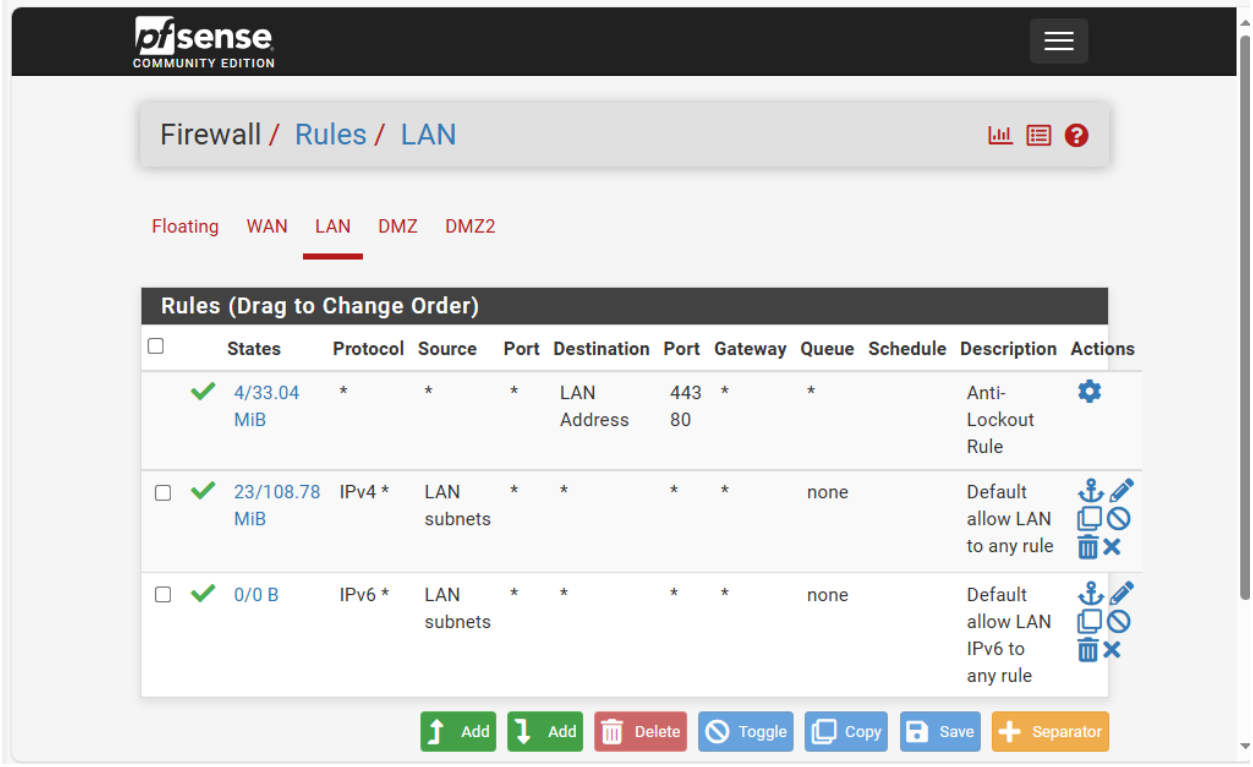
Configuration of the DHCP Server on DMZ2, Assignment of a Specific IP Range and the DNS Servers



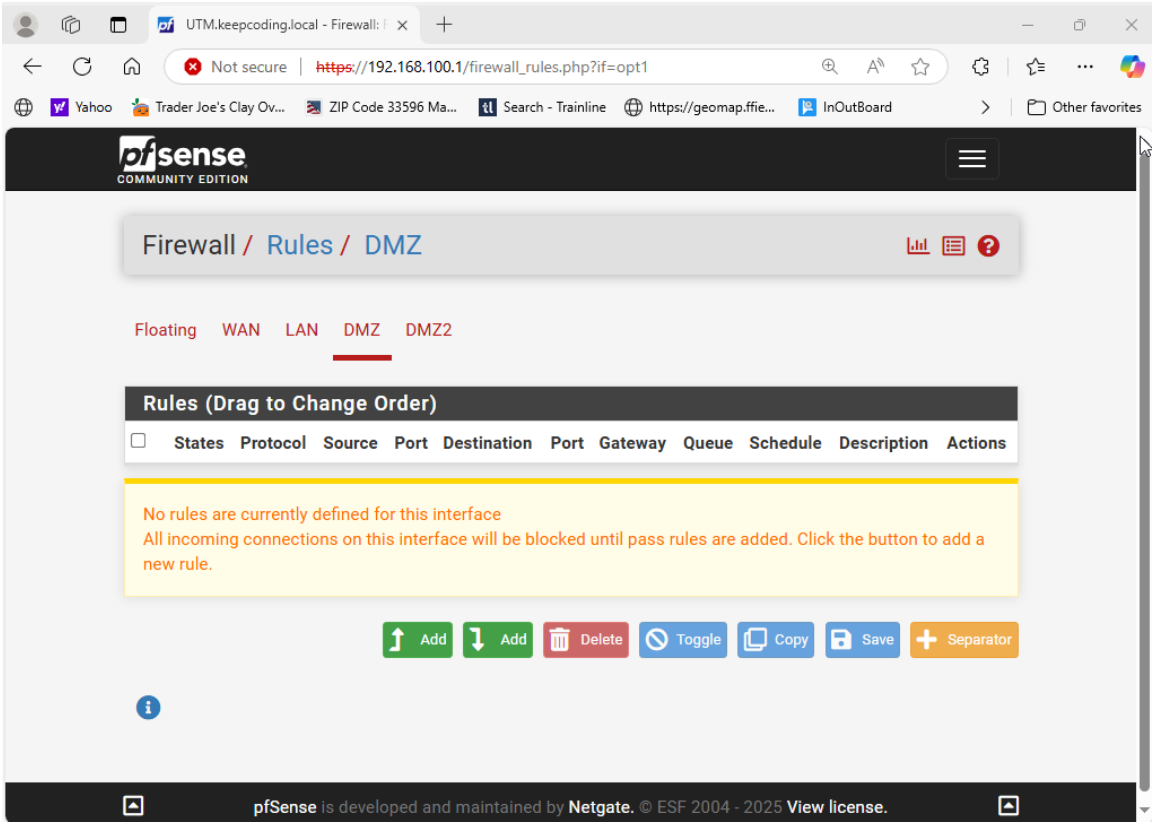


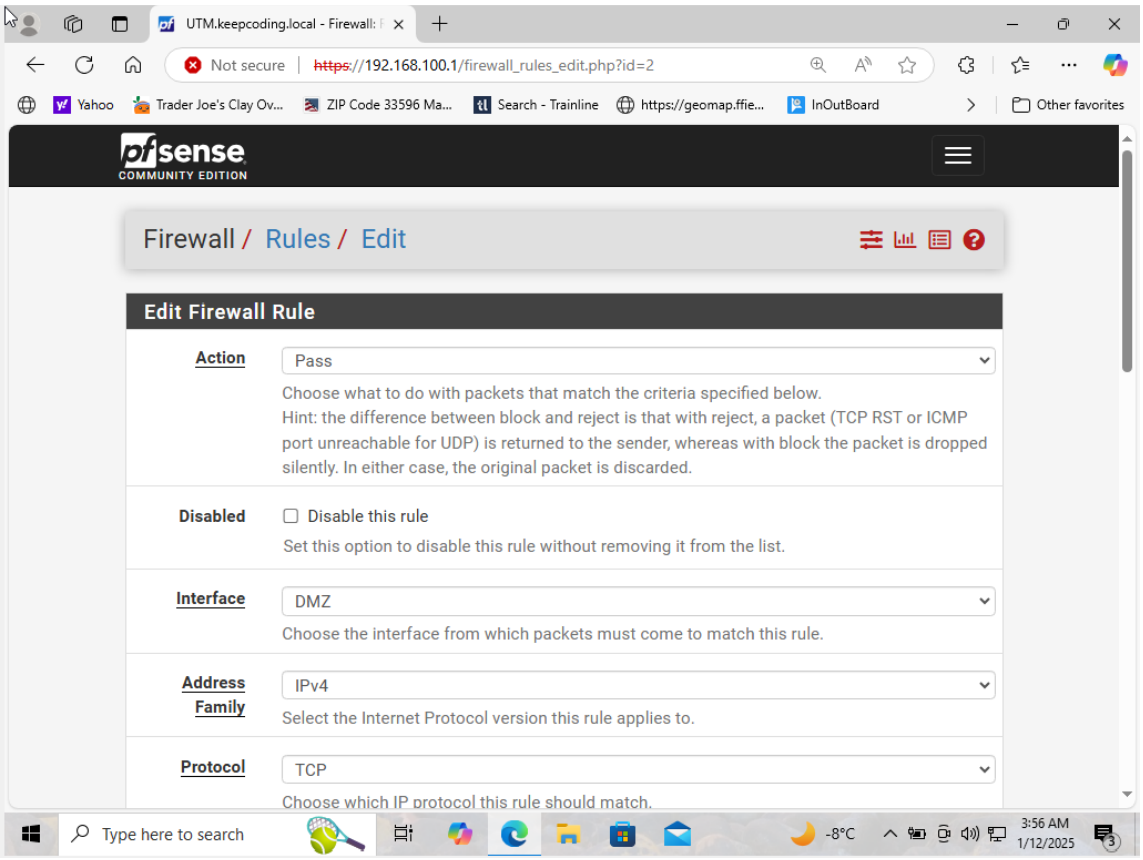
Establishing LAN rules regarding Web Ports on the Firewall (80 and 443)

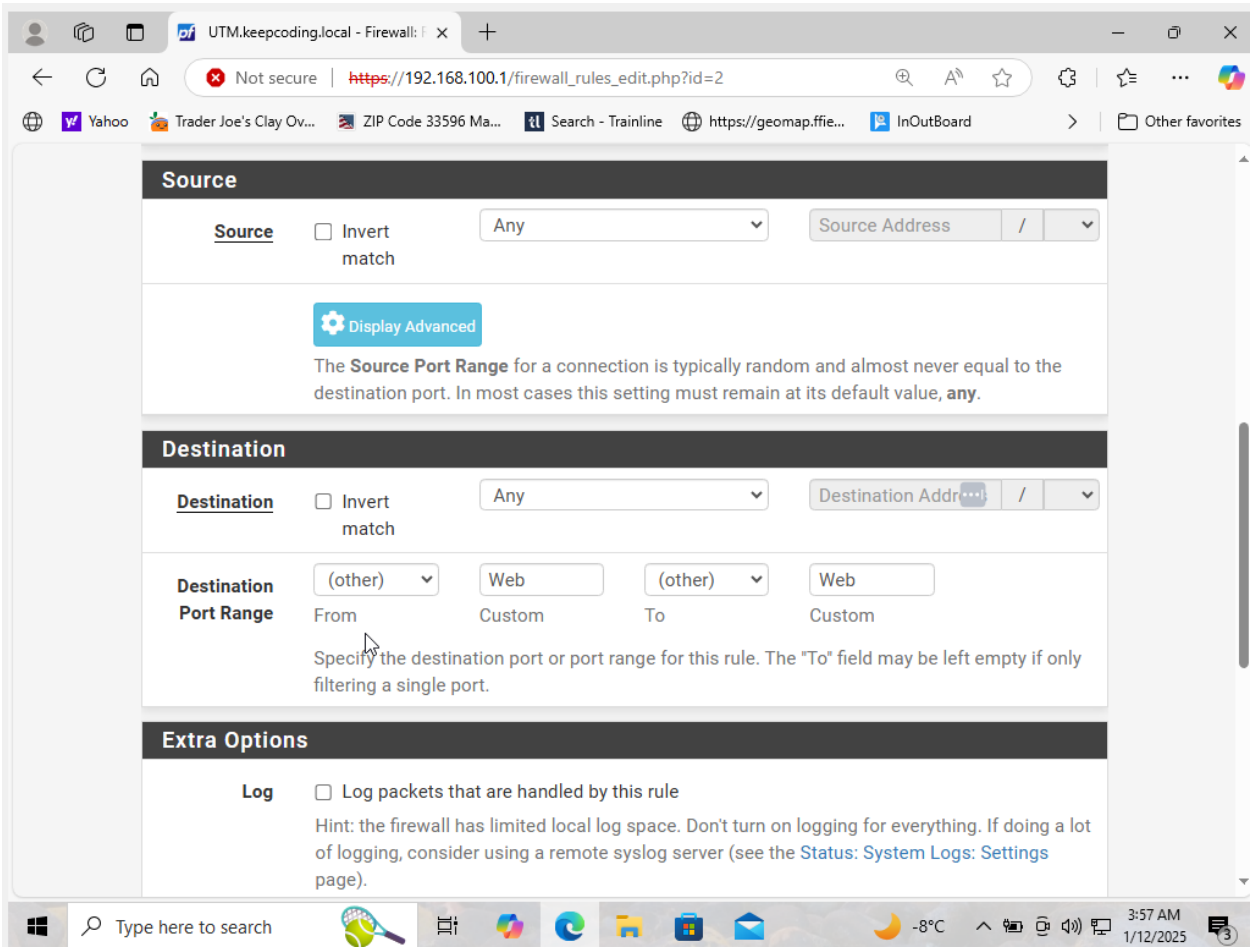


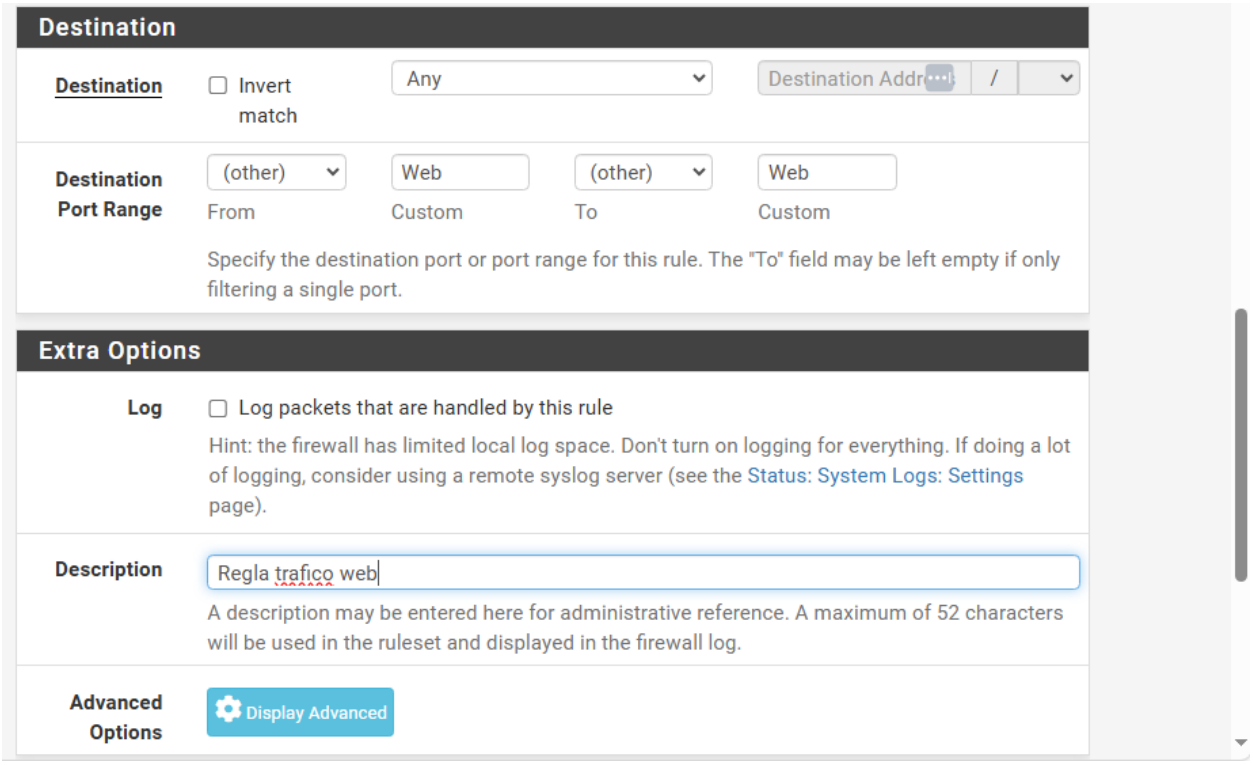


Establishing DMZ Rules Regarding Web Traffic on the Firewall with the Newly Created Rule

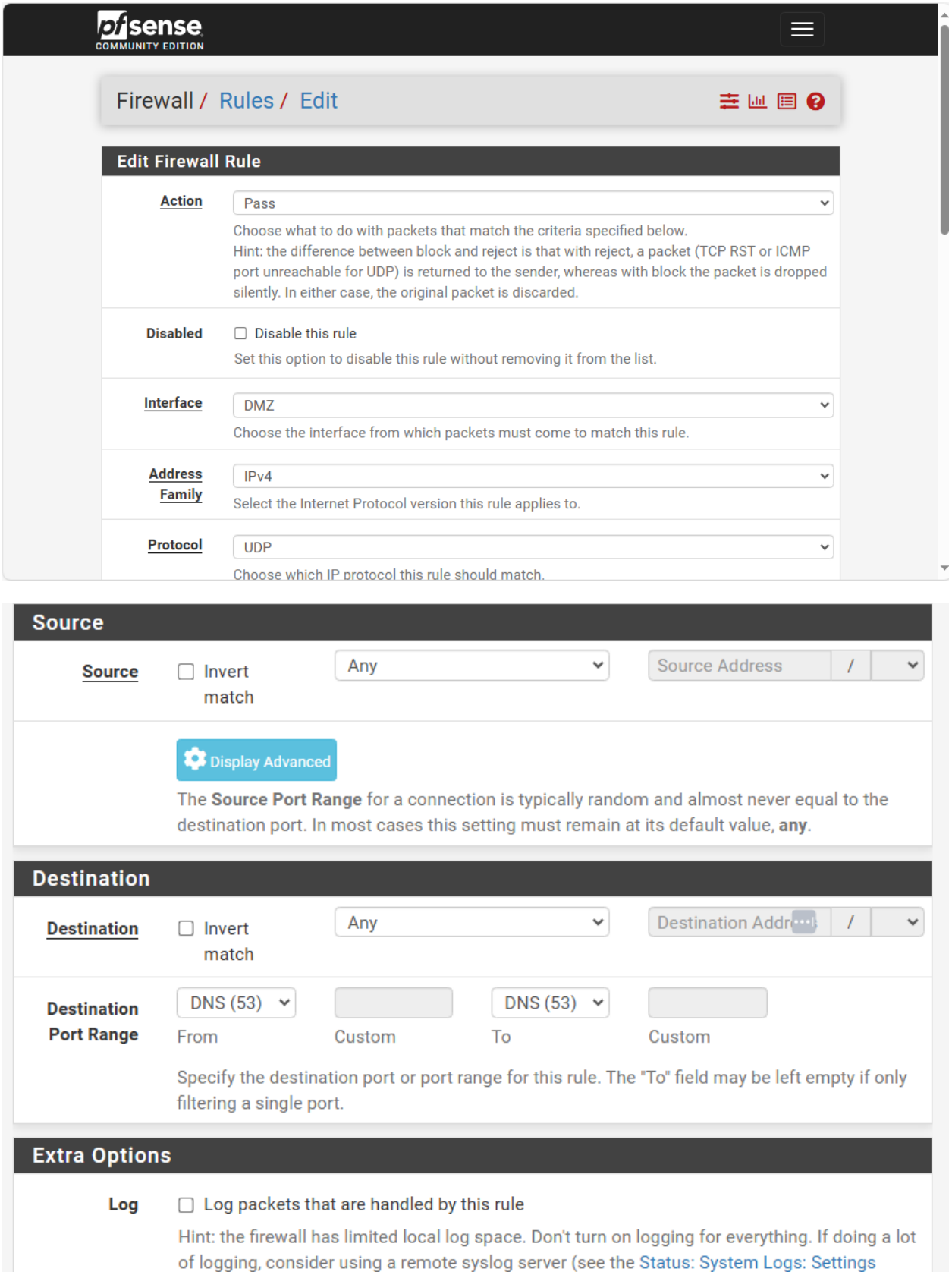





UTM.keepcoding.local - Firewall:
Not secure
https://192.168.100.1/firewall_rules_edit.php?id=2
Yahoo
Trader Joe's Clay Ov...
ZIP Code 33596 Ma...
Search - Trainline
https://geomap.ffie...
InOutBoard
Other favorites
Source
Source
Invert match
Any
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Addr
Destination Port Range
(other)
Web
From
Custom
(other)
Web
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Type here to search
-8°C
3:57 AM
1/12/2025


Destination
Destination
Invert match
Any
Destination Addr
Destination Port Range
(other)
Web
From
Custom
(other)
Web
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
Regla trafico web
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced

Establishing DMZ Rules Regarding DNSs on the Firewall



Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☑ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description Regla trafico DNS

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Rule Information

Tracking ID	1736679768
Created	1/12/25 12:02:48 by admin@192.168.100.100 (Local Database)
Updated	1/12/25 12:02:48 by admin@192.168.100.100 (Local Database)

Establishing DMZ Rules Regarding ICMP Protocol on the Firewall

pfSense COMMUNITY EDITION

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass

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 DMZ

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 ICMP

Choose which IP protocol this rule should match

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 DMZ

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 ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

Alternate Host
Datagram conversion error
Echo reply
Echo request

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source ☐ Invert match | Any | Source Address | /

Destination

Destination ☐ Invert match | Any | Destination Addr... | /

Extra Options

Log ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description Regla ICMP request

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

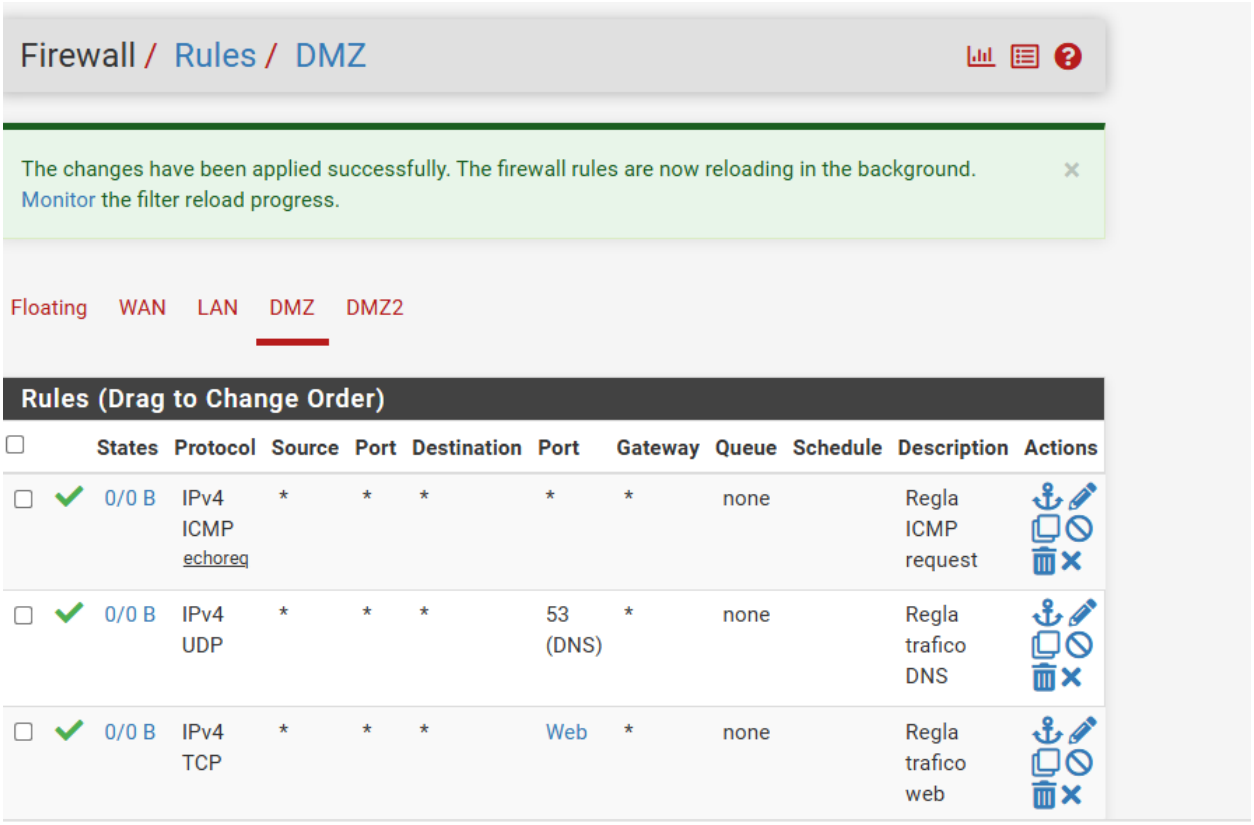
Rule Information

Tracking ID 1736679996

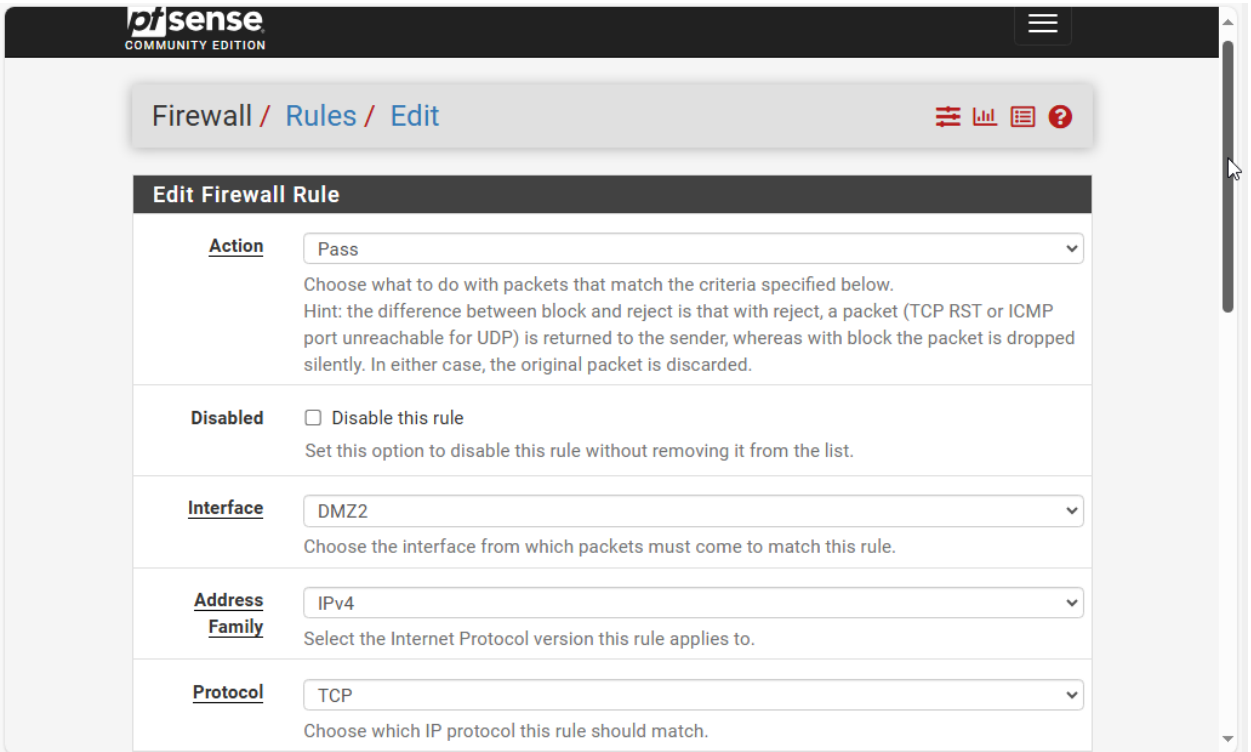
Created 1/12/25 12:06:36 by admin@192.168.100.100 (Local Database)

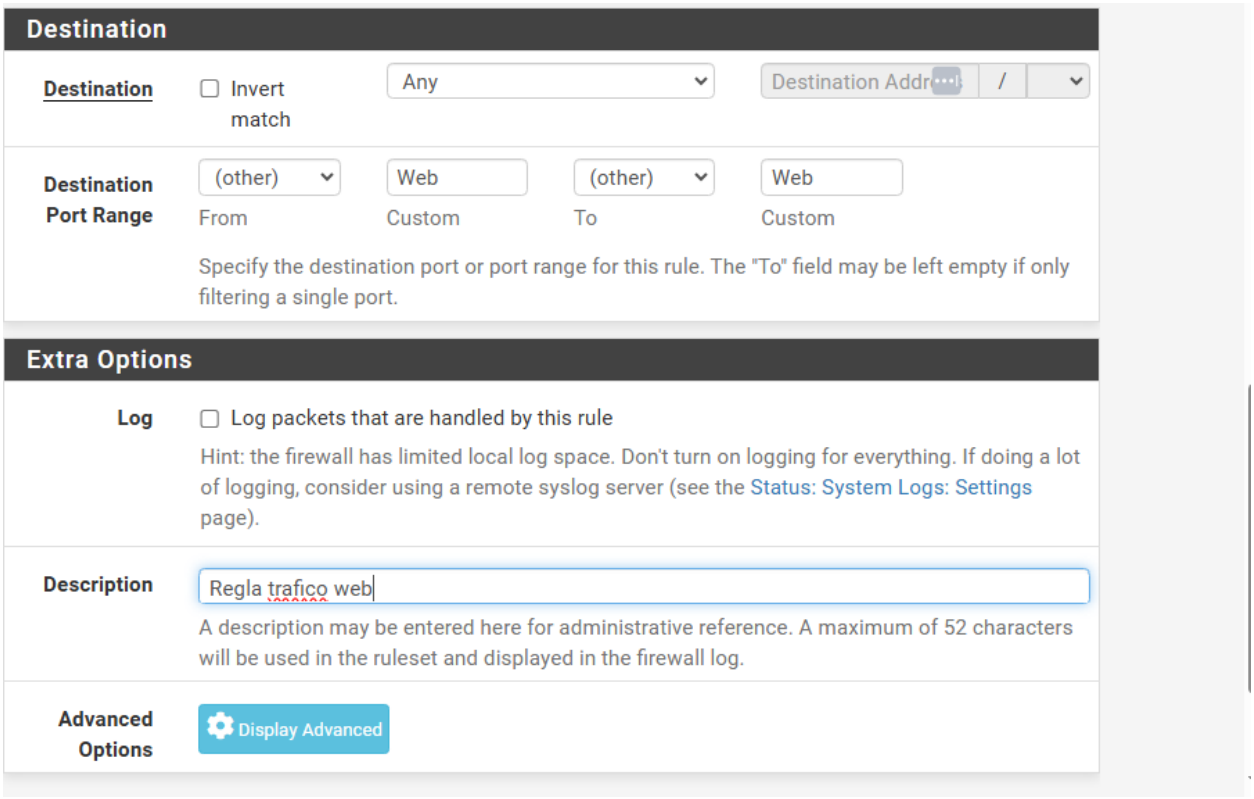
Updated 1/12/25 12:09:35 by admin@192.168.100.100 (Local Database)

DMZ Firewall Rules

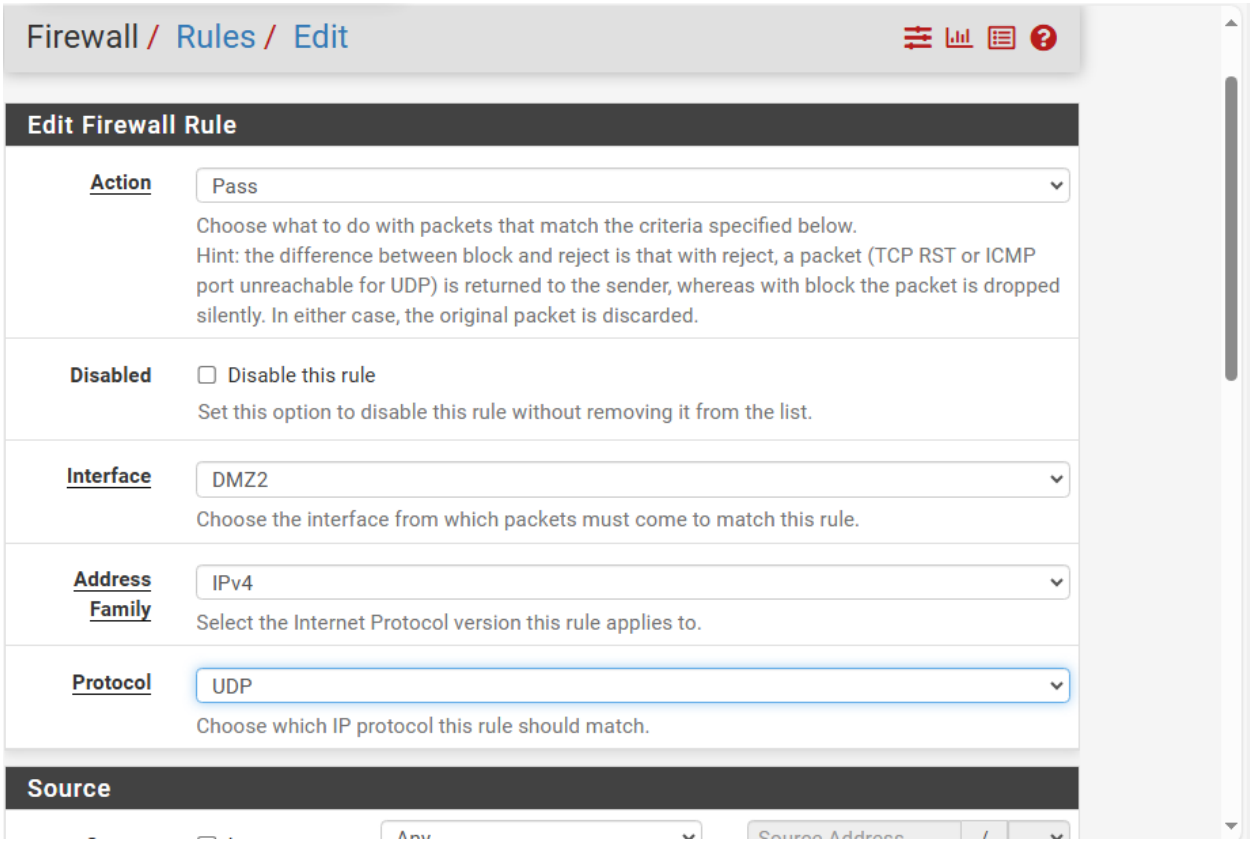


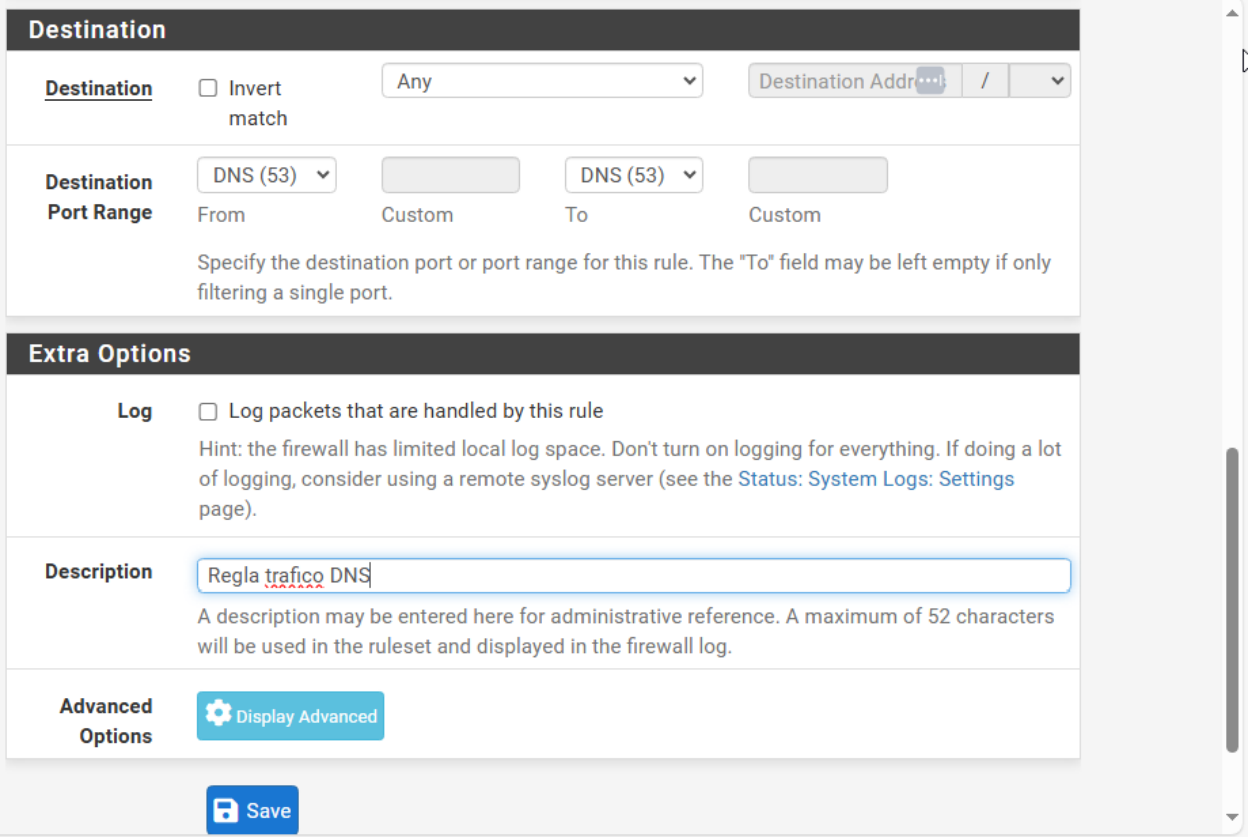
Establishing DMZ2 Rules Regarding Web Traffic on the Firewall with the Newly Created Port Rule



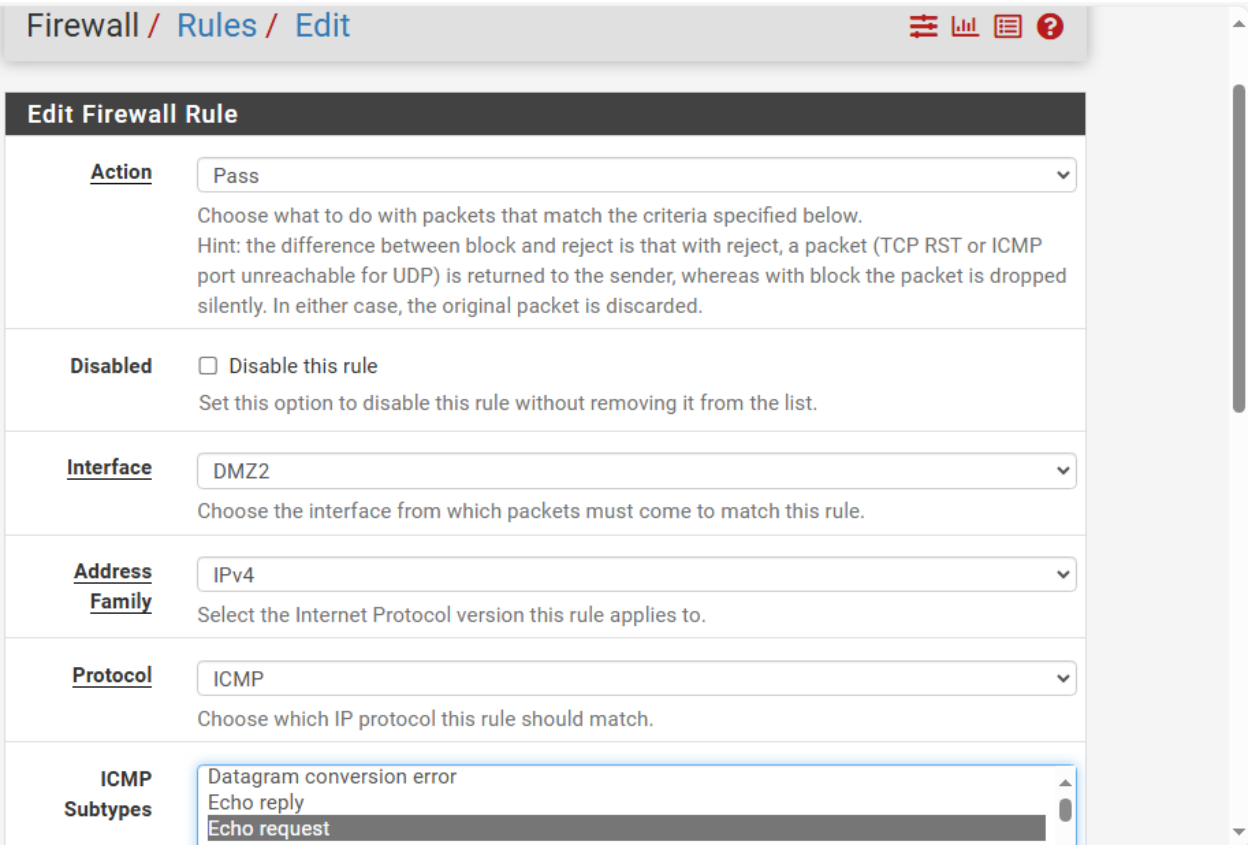


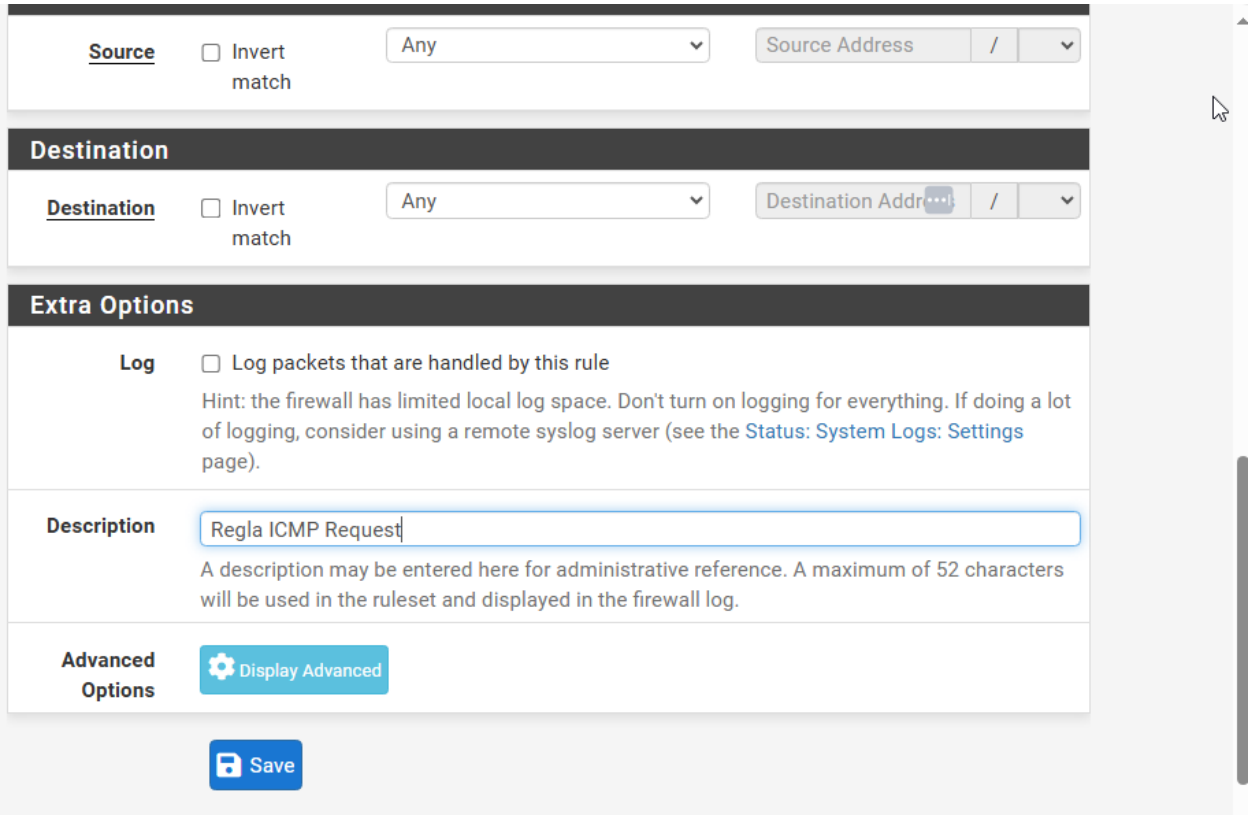
Establishing DMZ2 Rules Regarding DNSs on the Firewall



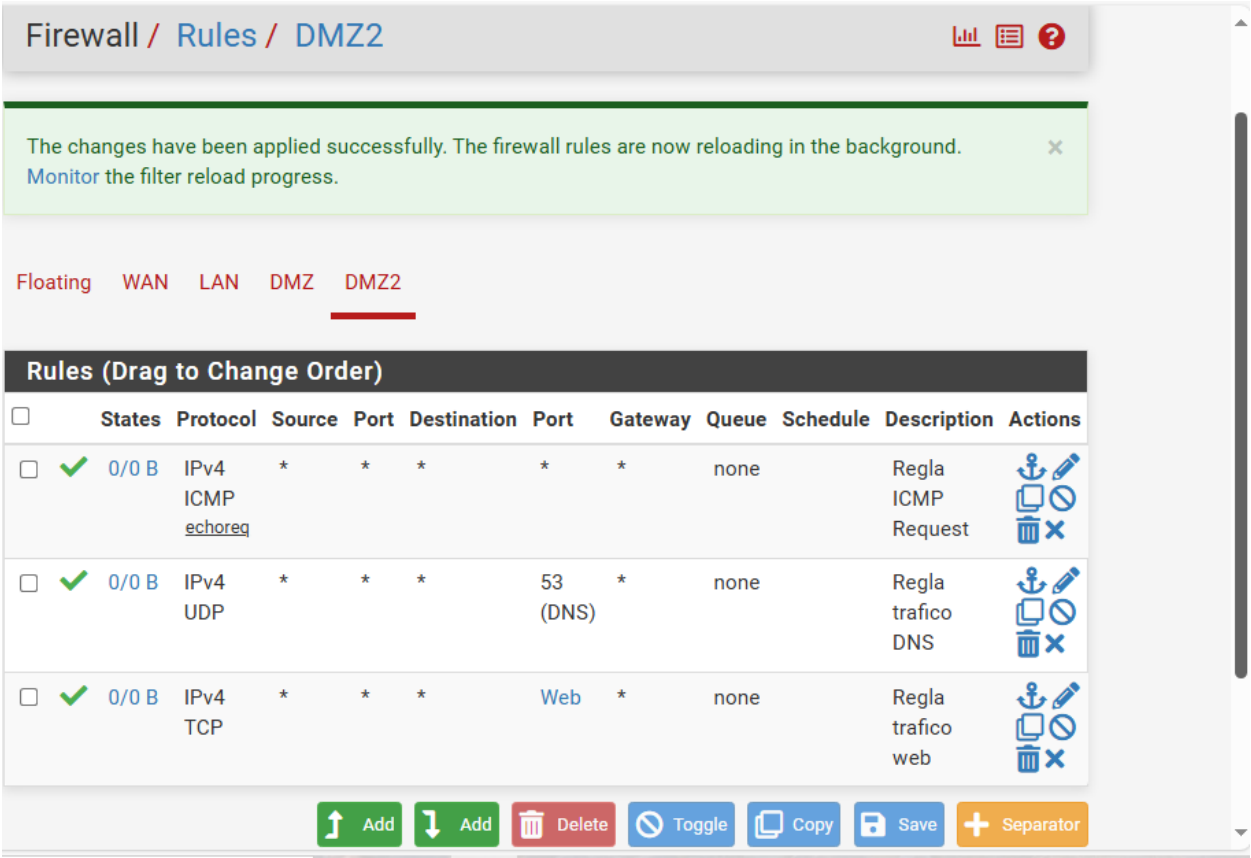


Establishing DMZ Rules Regarding ICMP Protocol on the Firewall

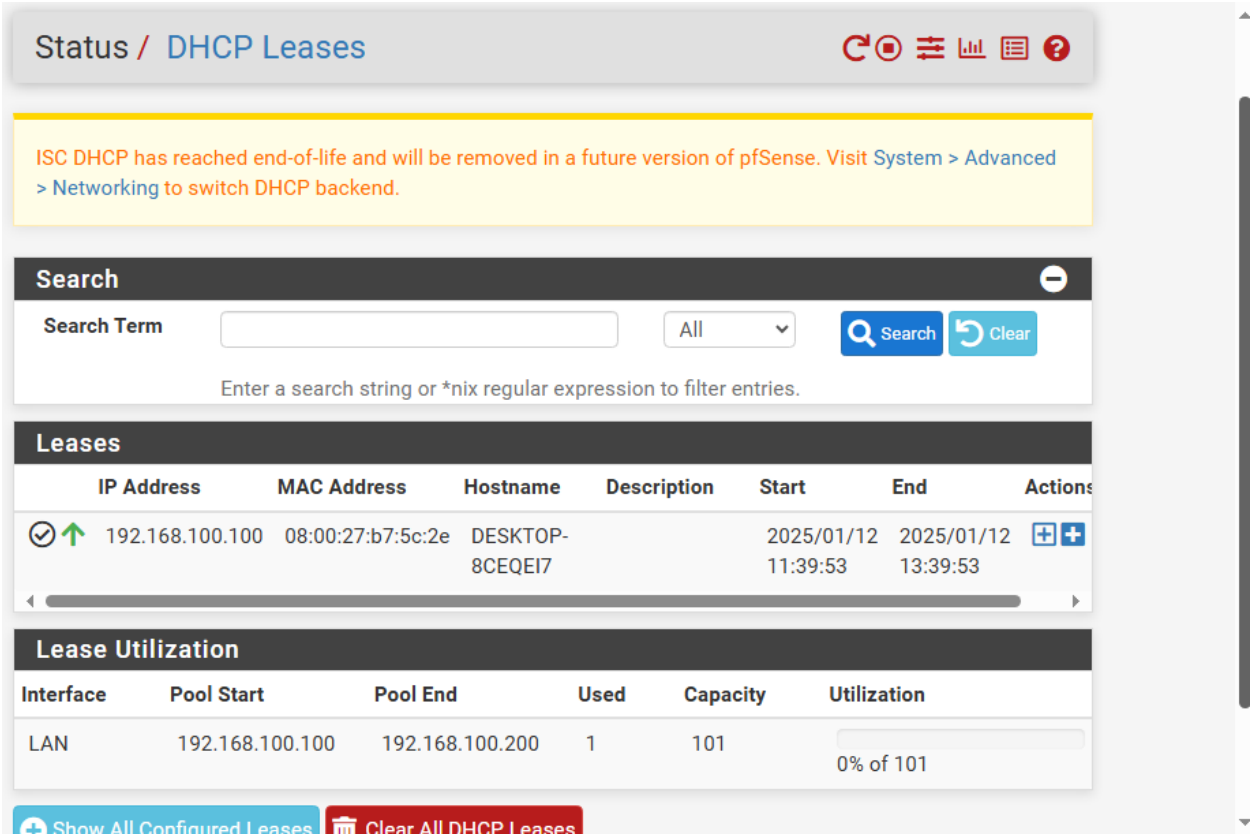




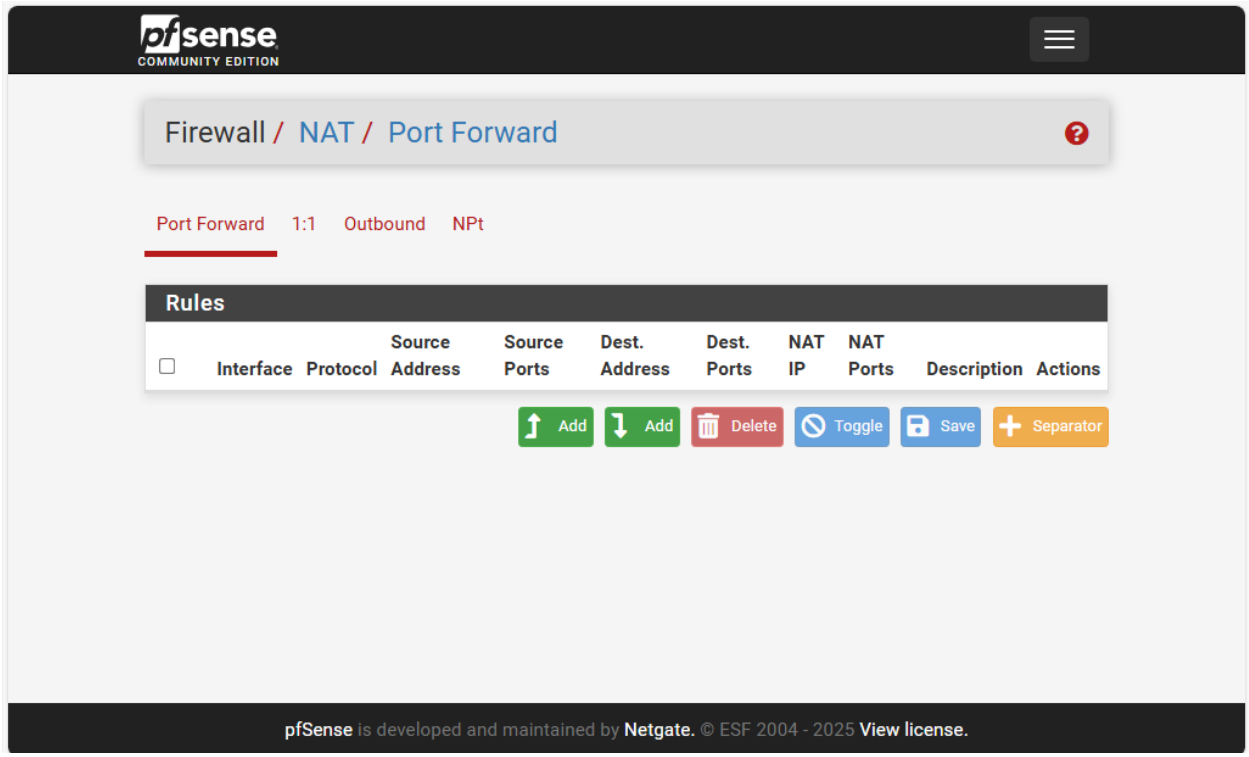
DMZ Firewall Rules

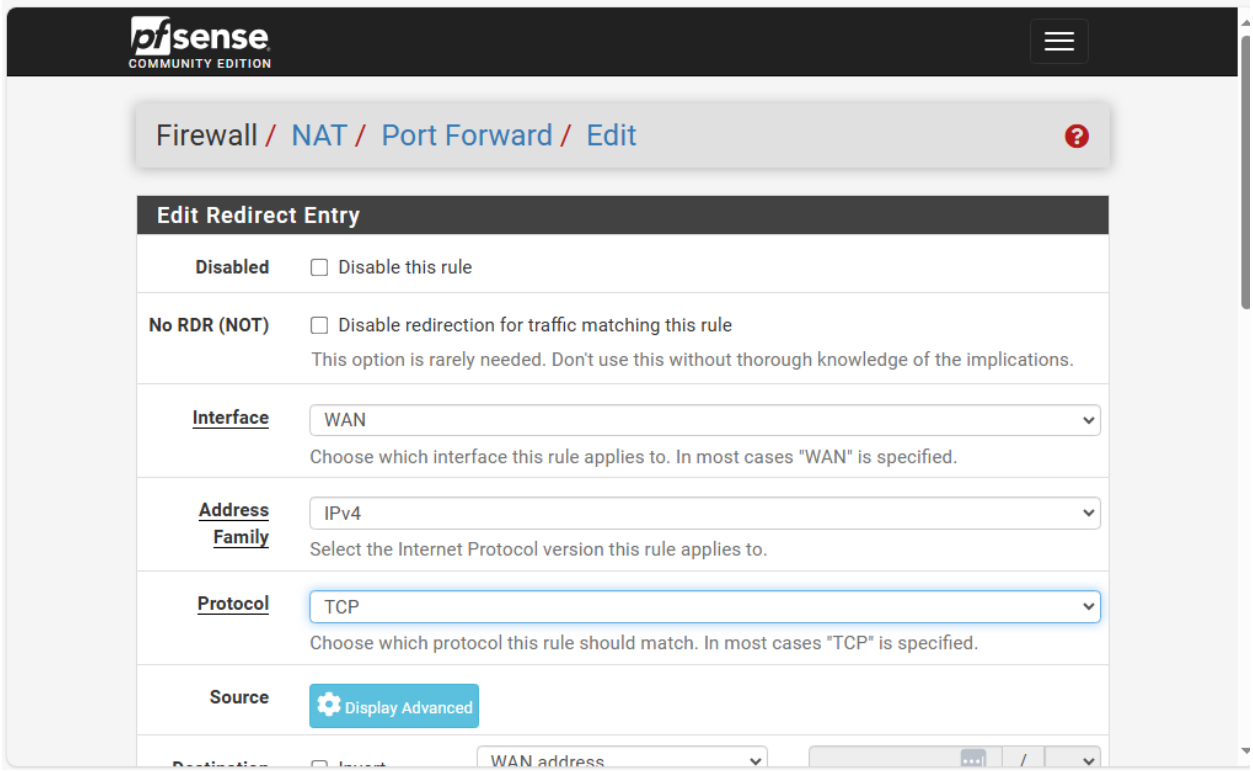


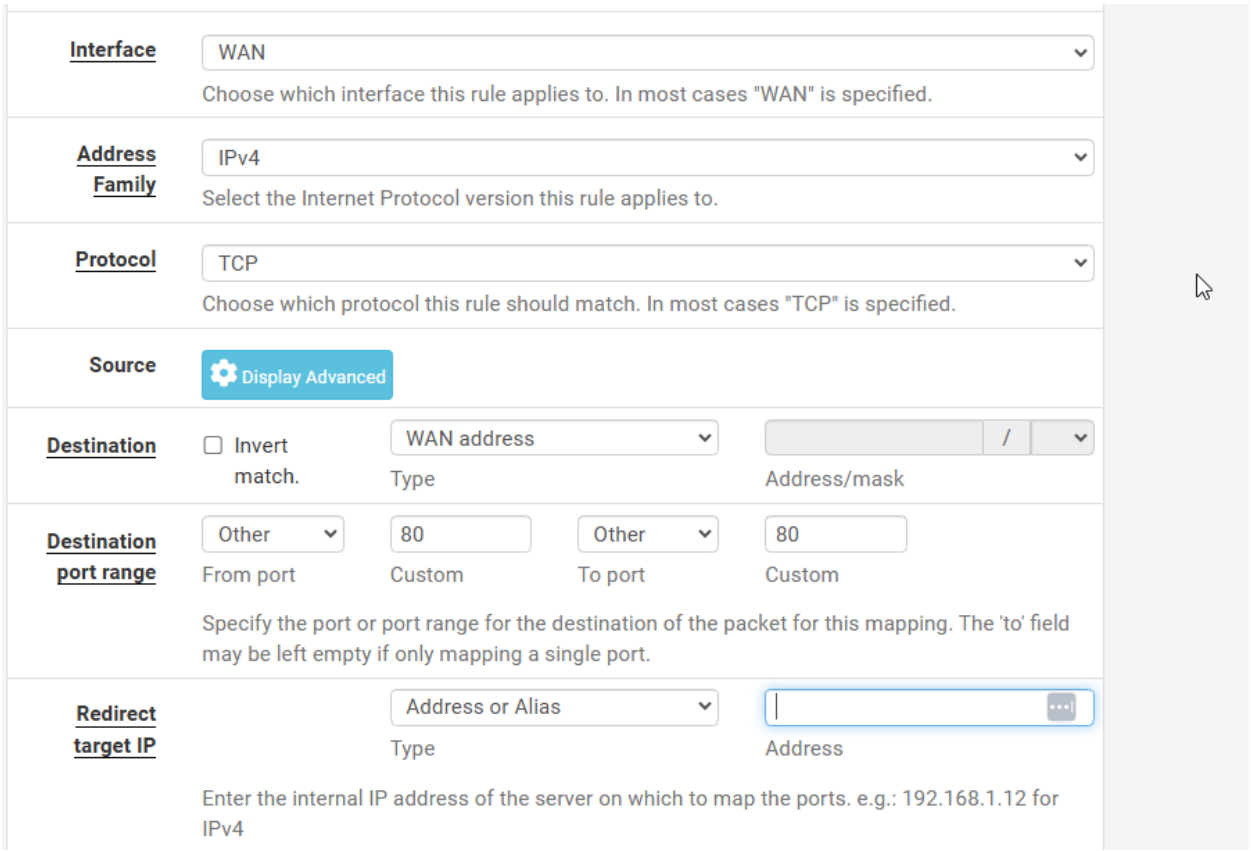
DHCP Status

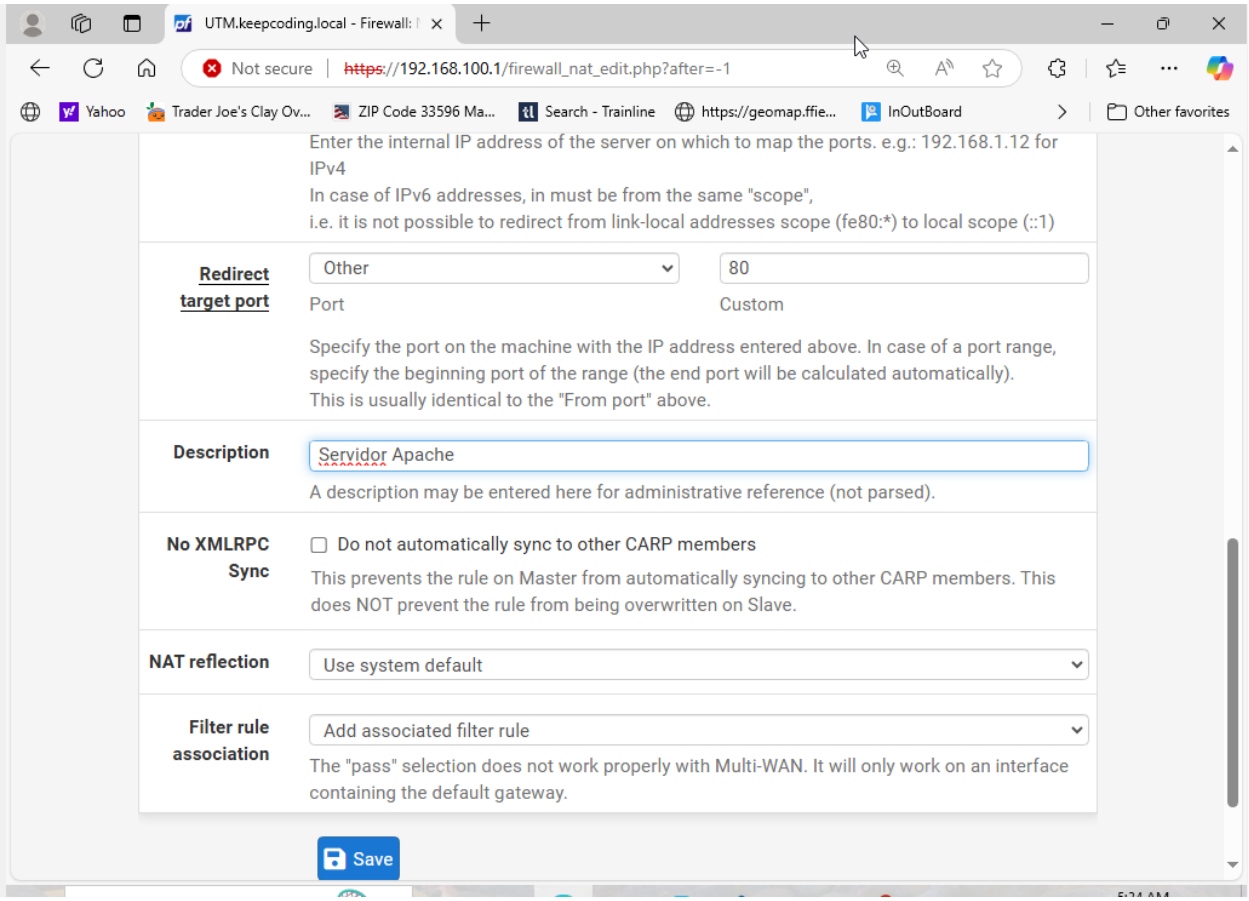


Port Forward Configuration on WAN for NAT on the Firewall

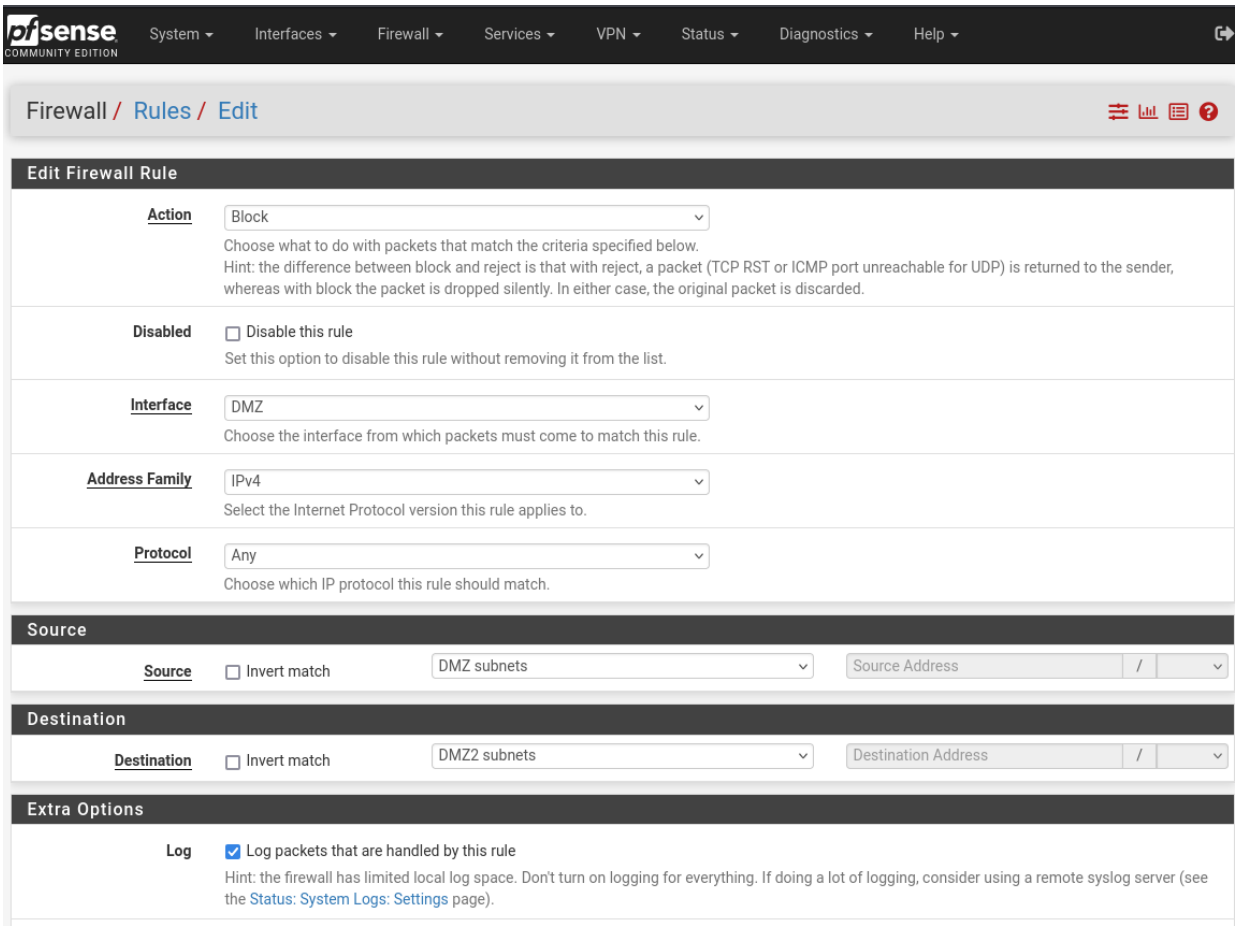



pfsense
COMMUNITY EDITION
Firewall / NAT / Port Forward / Edit
Edit Redirect Entry
Disabled
Disable this rule
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface
WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.
Source
Display Advanced
WAN address

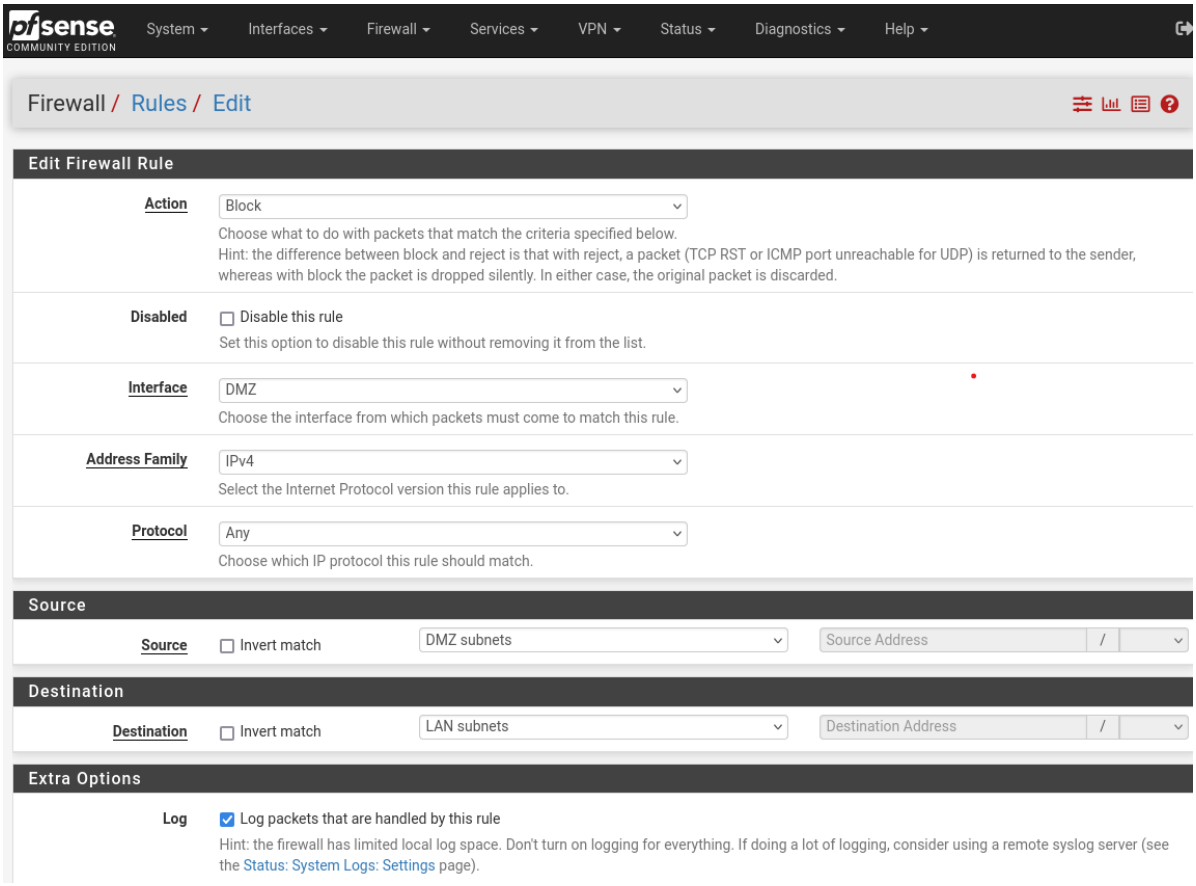

Interface
WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.
Source
Display Advanced
Destination
Invert match.
WAN address
Type
Address/mask
Destination port range
Other
From port
80
Custom
Other
To port
80
Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP
Address or Alias
Type
Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4



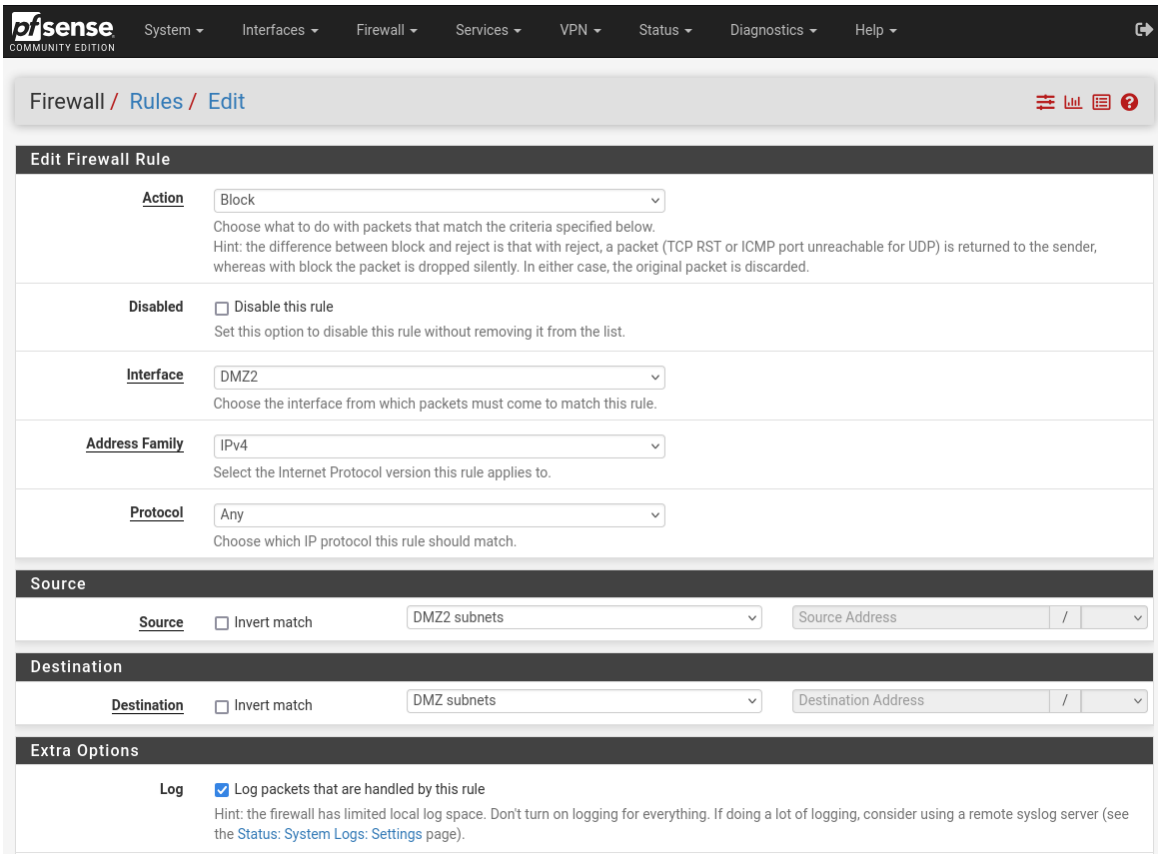
Blocking DMZ2 from Accessing DMZ



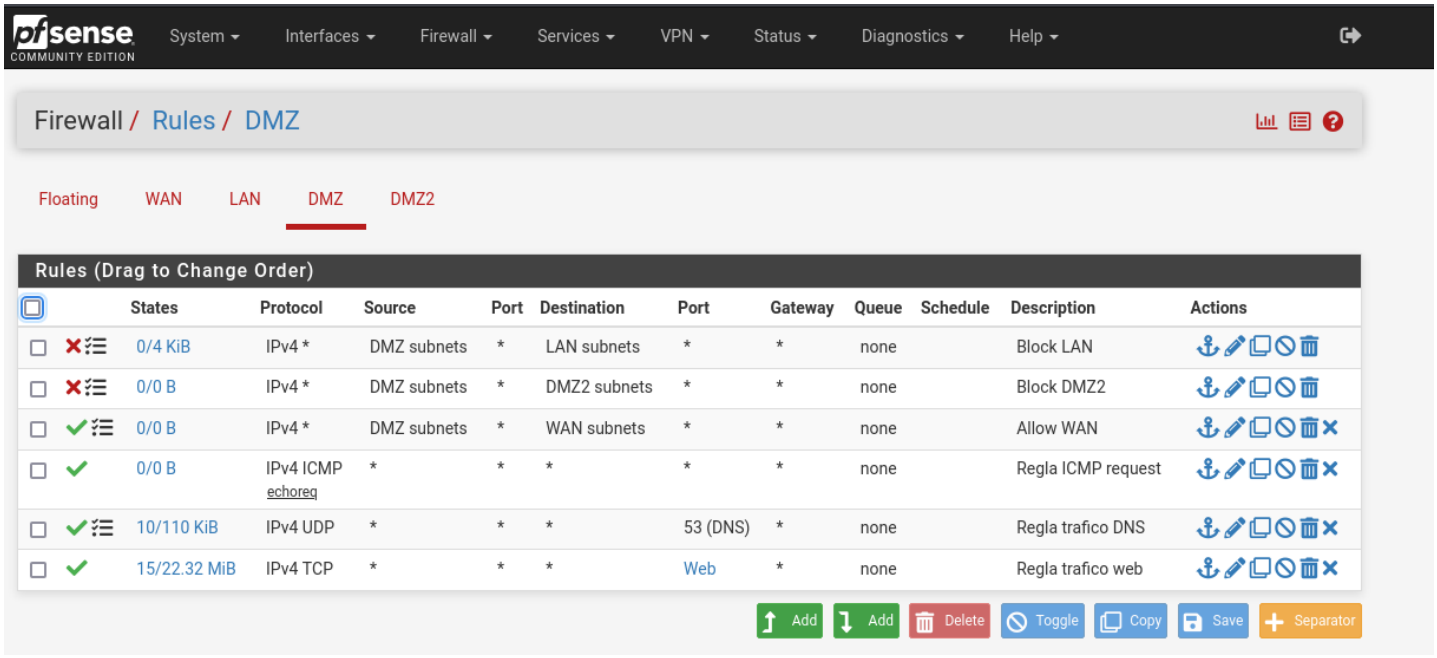
Blocking LAN from Accessing DMZ



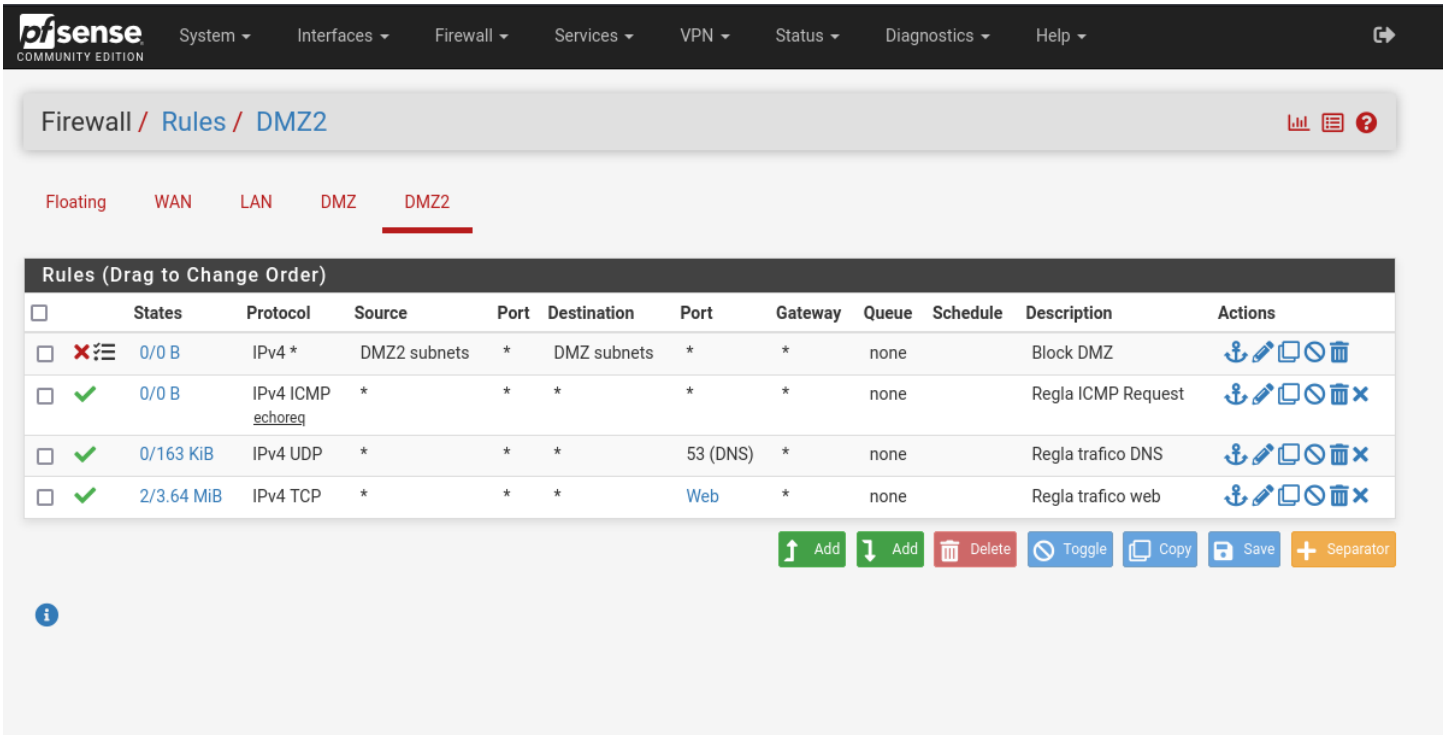
Blocking DMZ from Accessing DMZ2



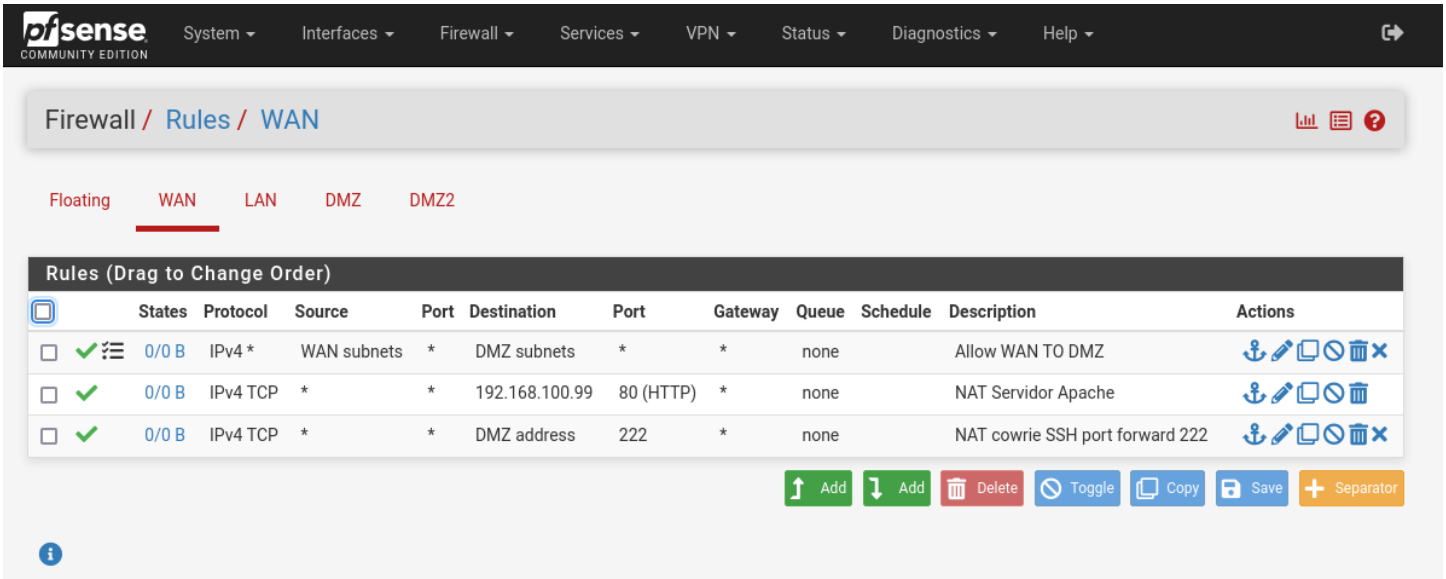
DMZ Rules



DMZ2 Rules



WAN Rules



LAN, DMZ and DMZ2 Configuration

A Windows 10 VM on LAN

A Kali Linux VM on DMZ

A Kali Linux VM on DMZ2

Then

A Honeypot on DMZ

And

Suricata on DMZ2

Elastic Configuration to receive and show logs from the three virtual machines.

elastic

192.168.1.1

192.168.1.207

pfsense

LAN
NETWORK

192.168.100.1

DMZ
Network

192.168.200.1

192.168.250.1

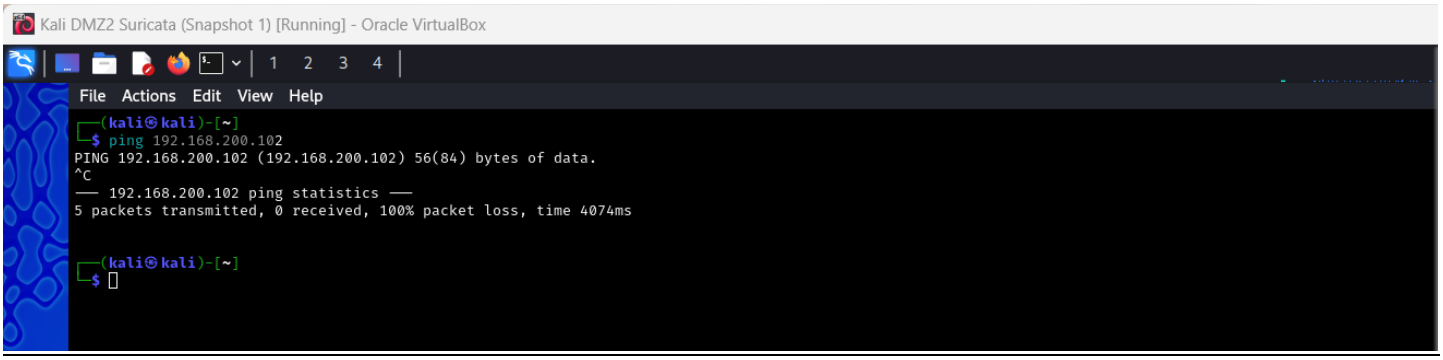
192.168.100.103

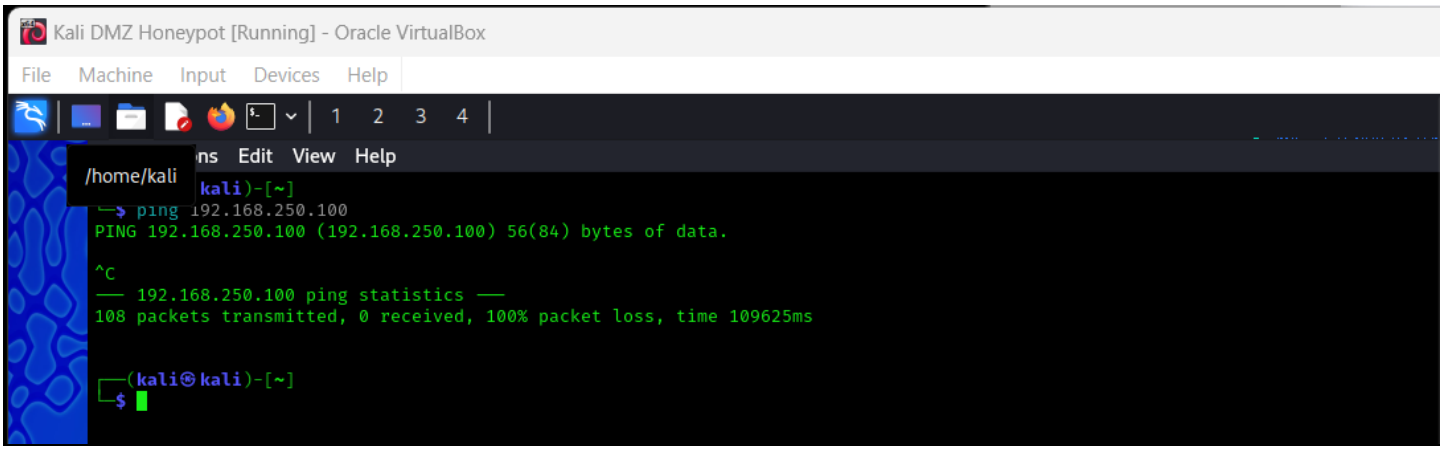
192.168.200.103

192.168.250.100

SURICATA

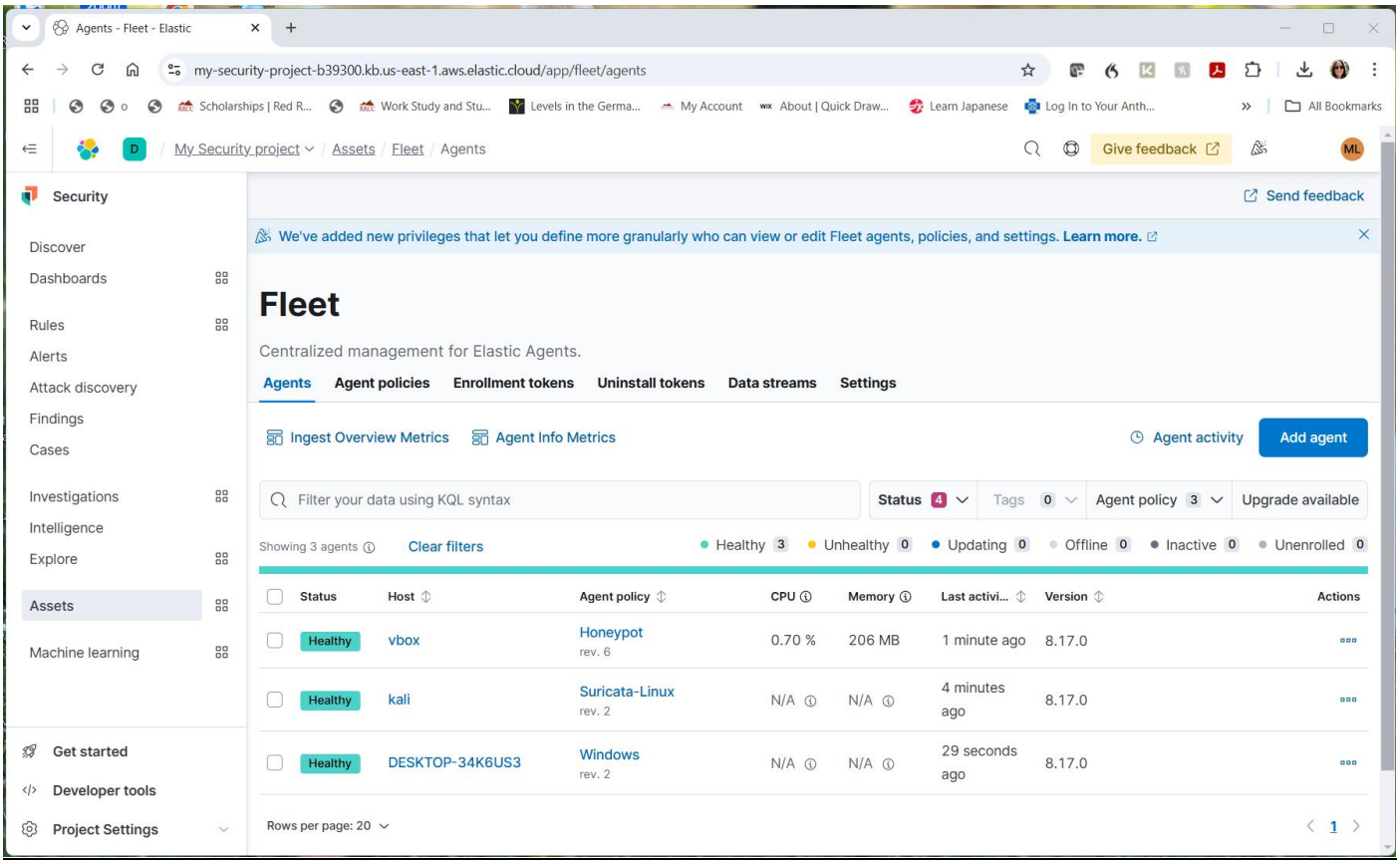
No communication between DMZ and DMZ2

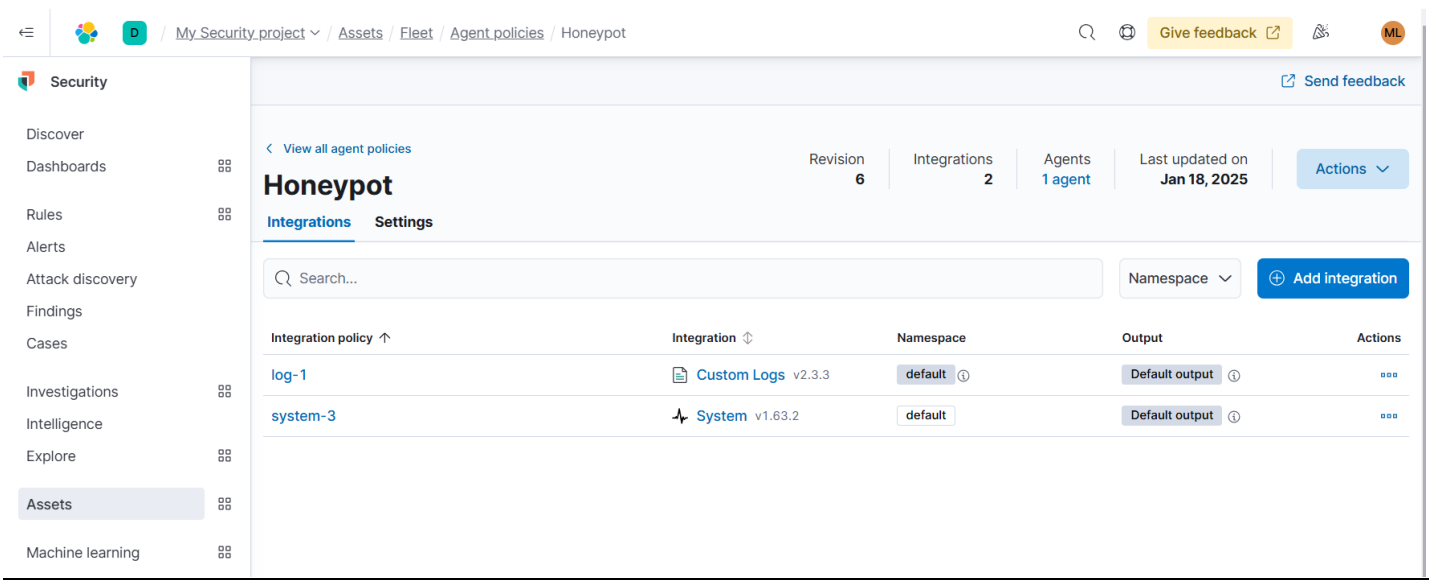


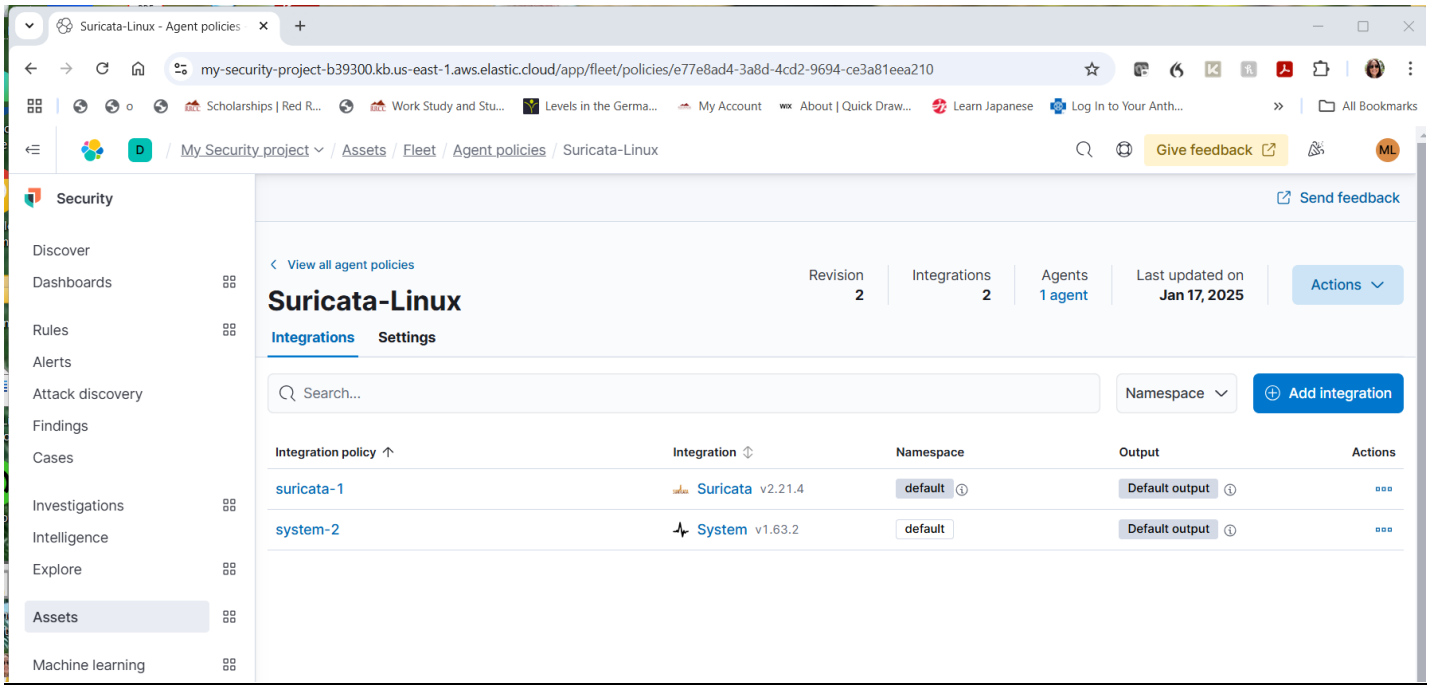


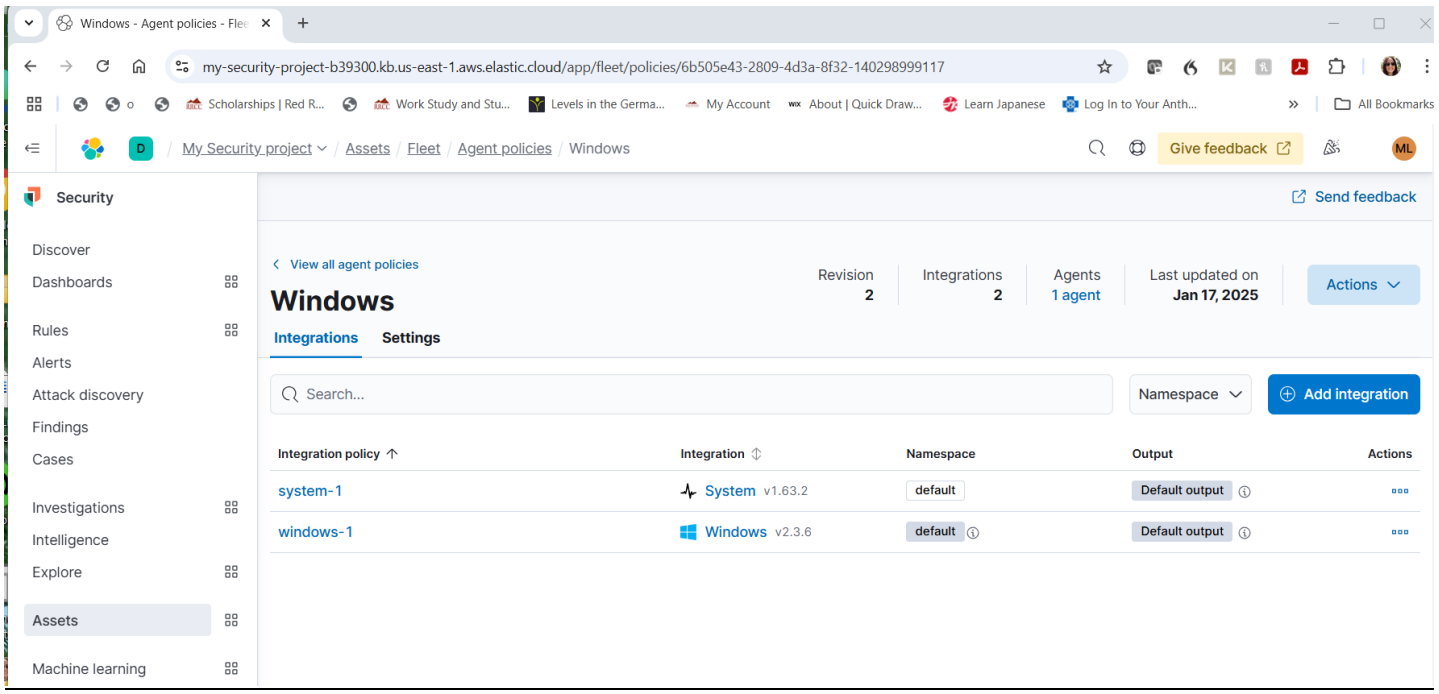
Elastic Cloud Configuration

Three Agent Policies: Windows with Windows Integration, Honeypot with Custom Logs Integration, and Suricata with Suricata Integration.


Agents - Fleet - Elastic
my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/fleet/agents
My Security project / Assets / Fleet / Agents
Give feedback
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Ingest Overview Metrics
Agent Info Metrics
Agent activity
Add agent
Filter your data using KQL syntax
Status 4
Tags 0
Agent policy 3
Upgrade available
Showing 3 agents
Clear filters
Healthy 3
Unhealthy 0
Updating 0
Offline 0
Inactive 0
Unenrolled 0
Status
Host
Agent policy
CPU
Memory
Last activi...
Version
Actions
Healthy
vbox
Honeypot
rev. 6
0.70 %
206 MB
1 minute ago
8.17.0
Healthy
kali
Suricata-Linux
rev. 2
N/A
N/A
4 minutes ago
8.17.0
Healthy
DESKTOP-34K6US3
Windows
rev. 2
N/A
N/A
29 seconds ago
8.17.0
Rows per page: 20
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine learning
Get started
Developer tools
Project Settings


My Security project / Assets / Fleet / Agent policies / Honeypot
Give feedback
Send feedback
View all agent policies
Honeypot
Revision 6
Integrations 2
Agents 1 agent
Last updated on Jan 18, 2025
Actions
Integrations
Settings
Search...
Namespace
Add integration
Integration policy
Integration
Namespace
Output
Actions
log-1
Custom Logs v2.3.3
default
Default output
system-3
System v1.63.2
default
Default output
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine learning





[Honeypot Logs]

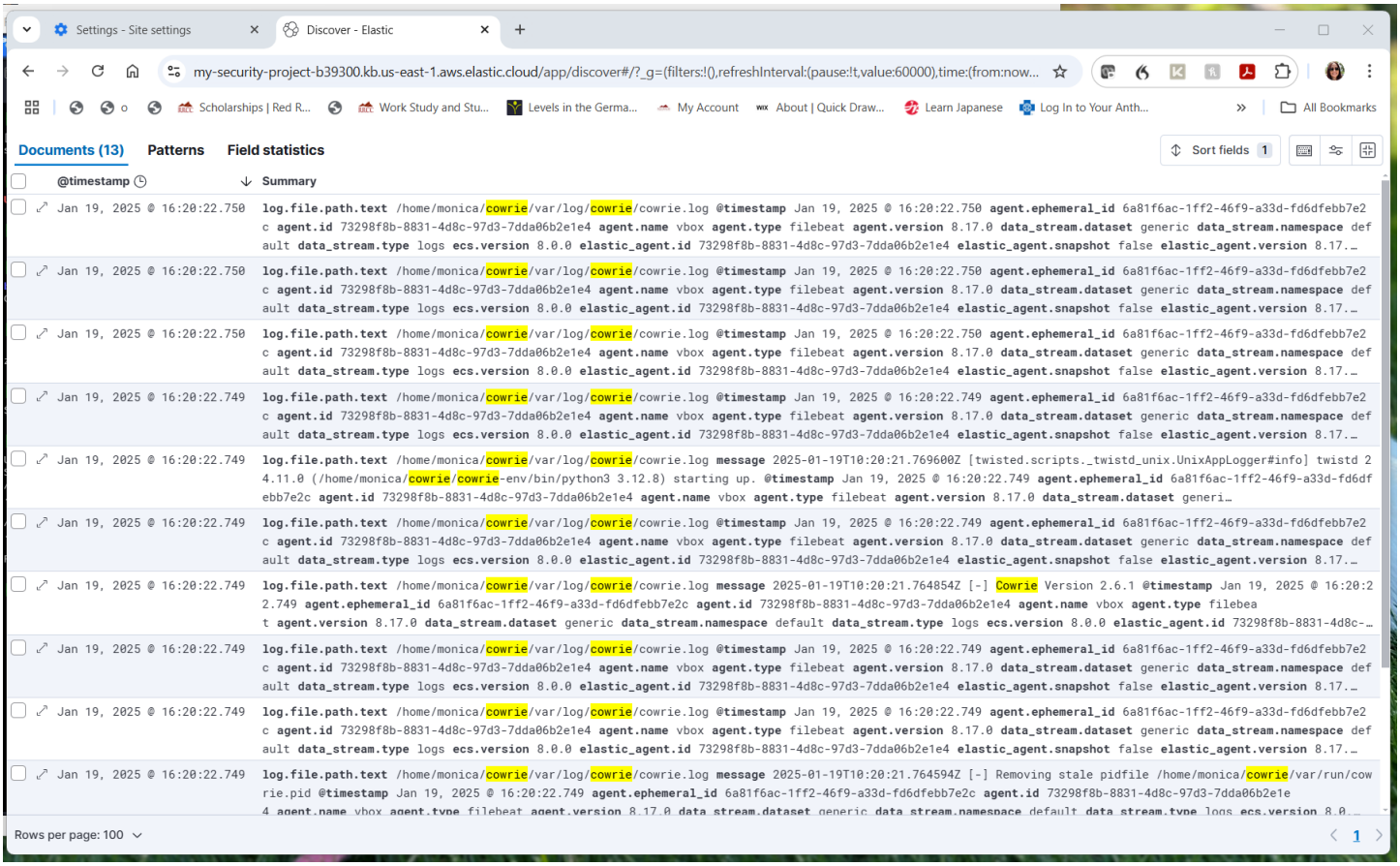
HONEYPOT LOG (SSH)


```
{
  "@timestamp": [
    "2025-01-18T15:16:23.027Z"
  ],
  "agent.ephemeral_id": [
    "4835f548-938e-479e-98c0-98f0a9206057"
  ],
  "agent.id": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
  ],
  "agent.name": [
    "vbox"
  ],
  "agent.type": [
    "filebeat"
  ],
  "agent.version": [
    "8.17.0"
  ],
  "data_stream.dataset": [
    "generic"
  ],
  "data_stream.namespace": [
    "default"
  ],
  "data_stream.type": [
    "logs"
  ],
```

```
  "ecs.version": [
    "8.0.0"
  ],
  "elastic_agent.id": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "elastic_agent.version": [
    "8.17.0"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "event.dataset": [
    "generic"
  ],
  "event.ingested": [
    "2025-01-18T15:17:32.000Z"
  ],
  "host.architecture": [
    "x86_64"
  ],
  "host.containerized": [
    false
  ],
  "host.hostname": [
    "vbox"
  ],
  "host.id": [
    "b8a20186aff447eabf70e5019ed33327"
  ],
  "host.ip": [
    "192.168.200.103",
    "fe80::a00:27ff:fe81:e1fb"
  ],
  "host.mac": [
    "08-00-27-81-E1-FB"
  ],
  "host.name": [
    "vbox"
  ],
  "host.os.codename": [
```

```
    "kali-rolling"
  ],
  "host.os.family": [
    "debian"
  ],
  "host.os.kernel": [
    "6.11.2-amd64"
  ],
  "host.os.name": [
    "Kali GNU/Linux"
  ],
  "host.os.name.text": [
    "Kali GNU/Linux"
  ],
  "host.os.platform": [
    "kali"
  ],
  "host.os.type": [
    "linux"
  ],
  "host.os.version": [
    "2024.4"
  ],
  "input.type": [
    "log"
  ],
  "log.file.path": [
    "/home/monica/cowrie/var/log/cowrie/cowrie.log"
  ],
  "log.file.path.text": [
    "/home/monica/cowrie/var/log/cowrie/cowrie.log"
  ],
  "log.offset": [
    8742
  ],
  "message": [
    "2025-01-18T10:13:37.646101Z [HoneyPotSSHTransport,2,127.0.0.1] SSH client hassh fingerprint:
0babd4b68a5f3757987be75fe35ad60a"
  ],
  "_id": "AZR5_RMpTxFMiMikkiqg",
  "_index": ".ds-logs-generic-default-2025.01.18-000001",
  "_score": null
}
```


COWRIE LOG



HONEYPOT LOG (COWRIE)


```
{
 "@timestamp": [
  "2025-01-19T15:20:22.750Z"
 ],
 "agent.ephemeral_id": [
  "6a81f6ac-1ff2-46f9-a33d-fd6dfebb7e2c"
 ],
 "agent.id": [
  "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
 ],
 "agent.name": [
  "vbox"
 ],
 "agent.type": [
  "filebeat"
 ],
 "agent.version": [
  "8.17.0"
 ],
 "data_stream.dataset": [
  "generic"
 ],
```

```
  "data_stream.namespace": [
    "default"
  ],
  "data_stream.type": [
    "logs"
  ],
  "ecs.version": [
    "8.0.0"
  ],
  "elastic_agent.id": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "elastic_agent.version": [
    "8.17.0"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "event.dataset": [
    "generic"
  ],
  "event.ingested": [
    "2025-01-19T15:20:41.000Z"
  ],
  "host.architecture": [
    "x86_64"
  ],
  "host.containerized": [
    false
  ],
  "host.hostname": [
    "vbox"
  ],
  "host.id": [
    "b8a20186aff447eabf70e5019ed33327"
  ],
  "host.ip": [
    "192.168.200.103",
    "fe80::a00:27ff:fe81:e1fb"
  ],
  "host.mac": [
```

```
    "08-00-27-81-E1-FB"
  ],
  "host.name": [
    "vbox"
  ],
  "host.os.codename": [
    "kali-rolling"
  ],
  "host.os.family": [
    "debian"
  ],
  "host.os.kernel": [
    "6.11.2-amd64"
  ],
  "host.os.name": [
    "Kali GNU/Linux"
  ],
  "host.os.name.text": [
    "Kali GNU/Linux"
  ],
  "host.os.platform": [
    "kali"
  ],
  "host.os.type": [
    "linux"
  ],
  "host.os.version": [
    "2024.4"
  ],
  "input.type": [
    "log"
  ],
  "log.file.path": [
    "/home/monica/cowrie/var/log/cowrie/cowrie.log"
  ],
  "log.file.path.text": [
    "/home/monica/cowrie/var/log/cowrie/cowrie.log"
  ],
  "log.offset": [
    972
  ],
  "message": [
    "2025-01-19T10:20:21.820728Z [-] Ready to accept SSH connections"
  ],
```

"_id": "AZR_JhMpTxFMiMjevX6A",
"_index": ".ds-logs-generic-default-2025.01.18-000001",
"_score": null
}

LOG

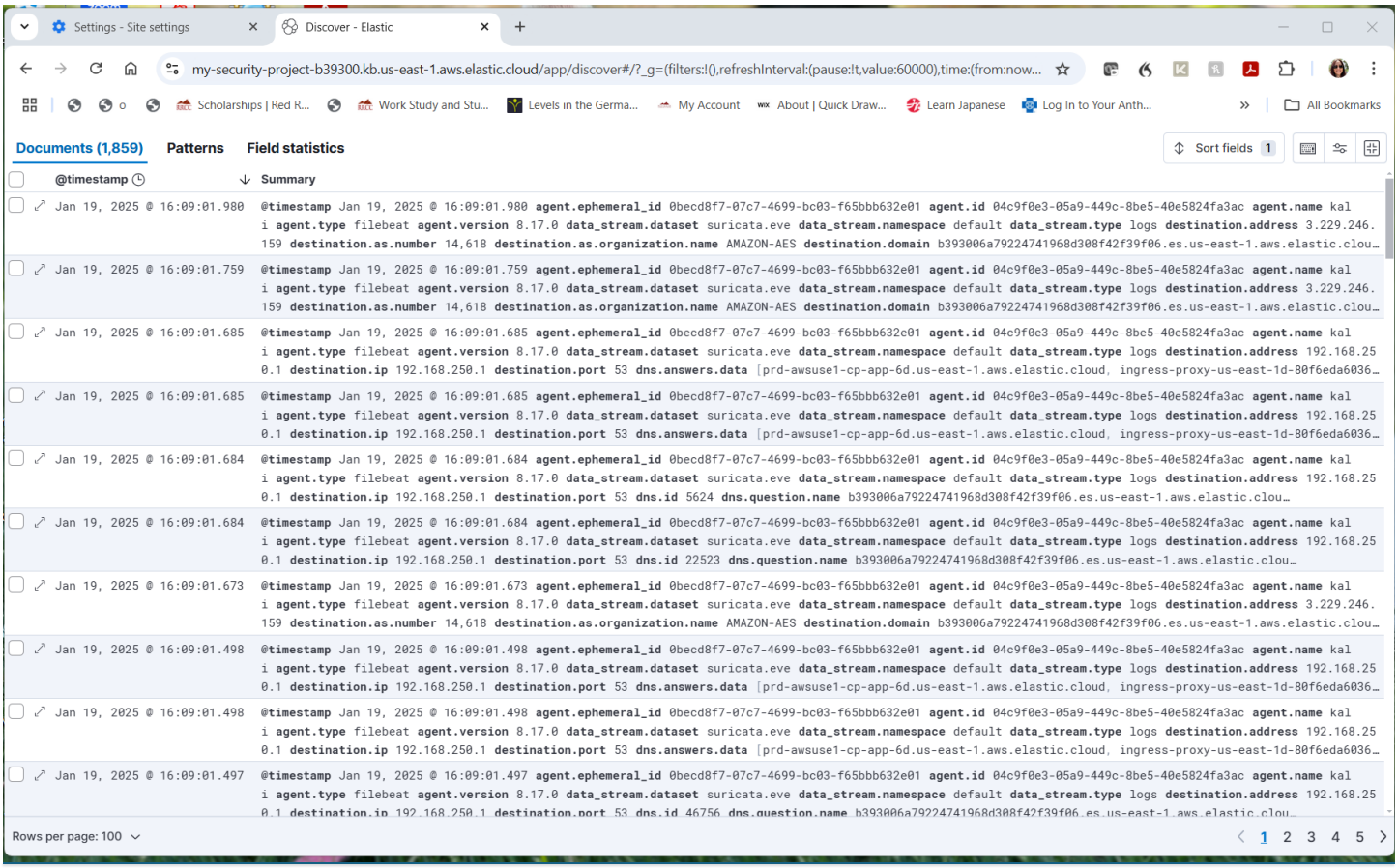
{
"@timestamp": [
"2025-01-19T12:12:37.017Z"
],
"agent.ephemeral_id": [
"c306da15-d257-4eff-9786-2770ed2f8f9c"
],
"agent.id": [
"73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
],
"agent.name": [
"vbox"
],
"agent.type": [
"filebeat"
],
"agent.version": [
"8.17.0"
],
"component.binary": [
"filebeat"
],
"component.dataset": [
"elastic_agent.filebeat"
],
"component.id": [
"log-default"
],
"component.type": [
"log"
],
"data_stream.dataset": [
"elastic_agent.filebeat"
],
"data_stream.namespace": [
"default"
],
"data_stream.type": [

```
    "logs"
  ],
  "ecs.version": [
    "8.0.0"
  ],
  "elastic_agent.id": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "elastic_agent.version": [
    "8.17.0"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "event.dataset": [
    "elastic_agent.filebeat"
  ],
  "event.ingested": [
    "2025-01-19T12:12:58.000Z"
  ],
  "host.architecture": [
    "x86_64"
  ],
  "host.containerized": [
    false
  ],
  "host.hostname": [
    "vbox"
  ],
  "host.id": [
    "b8a20186aff447eabf70e5019ed33327"
  ],
  "host.ip": [
    "192.168.200.103",
    "fe80::a00:27ff:fe81:e1fb"
  ],
  "host.mac": [
    "08-00-27-81-E1-FB"
  ],
  "host.name": [
    "vbox"
```

```
  ],
  "host.os.codename": [
    "kali-rolling"
  ],
  "host.os.family": [
    "debian"
  ],
  "host.os.kernel": [
    "6.11.2-amd64"
  ],
  "host.os.name": [
    "Kali GNU/Linux"
  ],
  "host.os.name.text": [
    "Kali GNU/Linux"
  ],
  "host.os.platform": [
    "kali"
  ],
  "host.os.type": [
    "linux"
  ],
  "host.os.version": [
    "2024.4"
  ],
  "input.type": [
    "filestream"
  ],
  "input_id": [
    "cfb5c92f-eb75-42ca-aa73-233b83186800"
  ],
  "log.file.device_id": [
    "2049"
  ],
  "log.file.inode": [
    "1204044"
  ],
  "log.file.path": [
    "/opt/Elastic/Agent/data/elastic-agent-8.17.0-96f2b9/logs/elastic-agent-20250119.ndjson"
  ],
  "log.level": [
    "info"
  ],
  "log.logger": [
```

```
    "input"
  ],
  "log.offset": [
    80155
  ],
  "log.origin.file.line": [
    179
  ],
  "log.origin.file.name": [
    "log/input.go"
  ],
  "log.origin.function": [
    "github.com/elastic/beats/v7/filebeat/input/log.NewInput"
  ],
  "log.source": [
    "log-default"
  ],
  "message": [
    "Configured paths: [/home/monica/cowrie/var/log/cowrie/*.log]"
  ],
  "service.name": [
    "filebeat"
  ],
  "_id": "AZR-exMpTxFMiMgBp7dL",
  "_index": ".ds-logs-elastic_agent.filebeat-default-2025.01.17-000001",
  "_score": null
}
```


SURICATA LOGS



SURICATA LOG


```
{
 "@timestamp": [
  "2025-01-19T15:09:01.980Z"
 ],
 "agent.ephemeral_id": [
  "0becd8f7-07c7-4699-bc03-f65bbb632e01"
 ],
 "agent.id": [
  "04c9f0e3-05a9-449c-8be5-40e5824fa3ac"
 ],
 "agent.name": [
  "kali"
 ],
 "agent.type": [
  "filebeat"
 ],
 "agent.version": [
  "8.17.0"
 ],
 "data_stream.dataset": [
  "suricata.eve"
 ],
```

```
  "data_stream.namespace": [
    "default"
  ],
  "data_stream.type": [
    "logs"
  ],
  "destination.address": [
    "3.229.246.159"
  ],
  "destination.as.number": [
    14618
  ],
  "destination.as.organization.name": [
    "AMAZON-AES"
  ],
  "destination.as.organization.name.text": [
    "AMAZON-AES"
  ],
  "destination.domain": [
    "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
  ],
  "destination.geo.city_name": [
    "Ashburn"
  ],
  "destination.geo.continent_name": [
    "North America"
  ],
  "destination.geo.country_iso_code": [
    "US"
  ],
  "destination.geo.country_name": [
    "United States"
  ],
  "destination.geo.location": [
    {
      "coordinates": [
        -77.49030003324151,
        39.046899997629225
      ],
      "type": "Point"
    }
  ],
  "destination.geo.region_iso_code": [
    "US-VA"
```

```
  ],
  "destination.geo.region_name": [
    "Virginia"
  ],
  "destination.ip": [
    "3.229.246.159"
  ],
  "destination.port": [
    443
  ],
  "ecs.version": [
    "8.11.0"
  ],
  "elastic_agent.id": [
    "04c9f0e3-05a9-449c-8be5-40e5824fa3ac"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "elastic_agent.version": [
    "8.17.0"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "event.category": [
    "network"
  ],
  "event.created": [
    "2025-01-19T15:09:02.557Z"
  ],
  "event.dataset": [
    "suricata.eve"
  ],
  "event.ingested": [
    "2025-01-19T15:09:13.000Z"
  ],
  "event.kind": [
    "event"
  ],
  "event.module": [
    "suricata"
  ],
  "event.type": [
```

```
    "protocol"
  ],
  "input.type": [
    "log"
  ],
  "log.file.path": [
    "/var/log/suricata/eve.json"
  ],
  "log.offset": [
    932835
  ],
  "network.community_id": [
    "1:mIYSy0WPZDkZk0A7C4wxAWV/9rE="
  ],
  "network.protocol": [
    "tls"
  ],
  "network.transport": [
    "tcp"
  ],
  "observer.hostname": [
    "kali"
  ],
  "observer.ip": [
    "192.168.250.100",
    "fe80::c6b6:99d7:2858:f4ac",
    "172.17.0.1"
  ],
  "observer.mac": [
    "02-42-28-1D-78-B4",
    "08-00-27-CB-7E-F5"
  ],
  "observer.product": [
    "Suricata"
  ],
  "observer.type": [
    "ids"
  ],
  "observer.vendor": [
    "OISF"
  ],
  "related.hosts": [
    "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
  ],
```

```
  "related.ip": [
    "192.168.250.100",
    "3.229.246.159"
  ],
  "source.address": [
    "192.168.250.100"
  ],
  "source.ip": [
    "192.168.250.100"
  ],
  "source.port": [
    58890
  ],
  "suricata.eve.event_type": [
    "tls"
  ],
  "suricata.eve.flow_id": [
    "1538408431940806"
  ],
  "suricata.eve.in_iface": [
    "eth0"
  ],
  "suricata.eve.pkt_src": [
    "wire/pcap"
  ],
  "suricata.eve.tls.sni": [
    "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
  ],
  "suricata.eve.tls.version": [
    "TLS 1.3"
  ],
  "tags": [
    "forwarded",
    "suricata-eve"
  ],
  "tls.client.server_name": [
    "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
  ],
  "tls.version": [
    "1.3"
  ],
  "tls.version_protocol": [
    "tls"
  ],
```

"_id": "AZR_HBMpTxFMiMhftn7-",
"_index": ".ds-logs-suricata.eve-default-2025.01.17-000001",
"_score": null
}

LOG

{
"@timestamp": [
"2025-01-16T13:26:35.520Z"
],
"agent.ephemeral_id": [
"e6f3b52c-fe37-4357-9223-35f6c361c328"
],
"agent.id": [
"f752d655-1242-4066-888a-8c1c9043f3e5"
],
"agent.name": [
"kali"
],
"agent.type": [
"filebeat"
],
"agent.version": [
"8.17.0"
],
"data_stream.dataset": [
"suricata.eve"
],
"data_stream.namespace": [
"default"
],
"data_stream.type": [
"logs"
],
"destination.address": [
"35.193.143.25"
],
"destination.as.number": [
396982
],
"destination.as.organization.name": [
"GOOGLE-CLOUD-PLATFORM"
],
"destination.as.organization.name.text": [

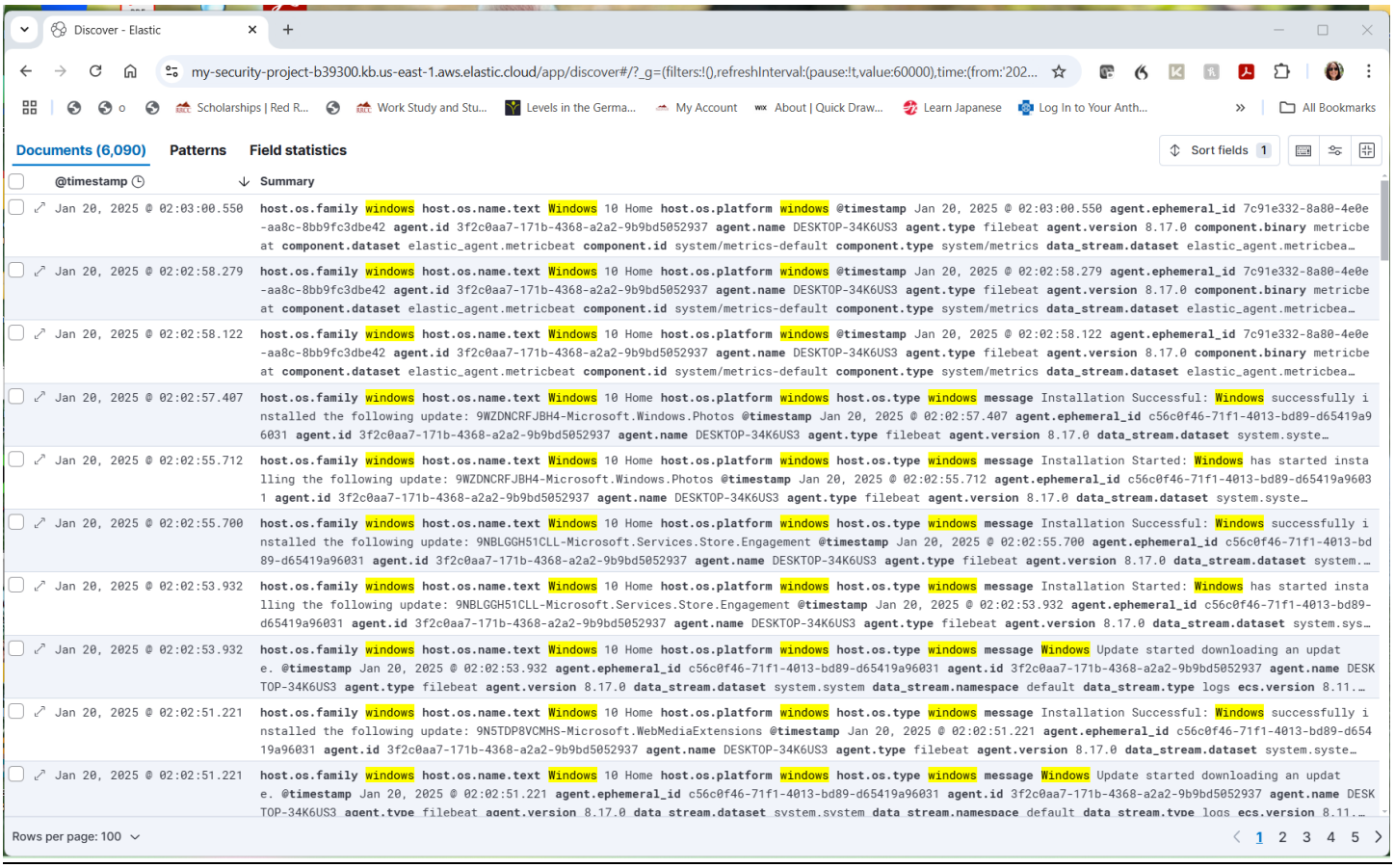
```
"GOOGLE-CLOUD-PLATFORM"
],
"destination.domain": [
"add9e71f48304c70804ecca975a324e3.us-central1.gcp.cloud.es.io"
],
"destination.geo.city_name": [
"Council Bluffs"
],
"destination.geo.continent_name": [
"North America"
],
"destination.geo.country_iso_code": [
"US"
],
"destination.geo.country_name": [
"United States"
],
"destination.geo.location": [
{
"coordinates": [
-95.8517,
41.2591
],
"type": "Point"
}
],
"destination.geo.region_iso_code": [
"US-IA"
],
"destination.geo.region_name": [
"Iowa"
],
"destination.ip": [
"35.193.143.25"
],
"destination.port": [
443
],
"ecs.version": [
"8.11.0"
],
"elastic_agent.id": [
"f752d655-1242-4066-888a-8c1c9043f3e5"
],
```

"elastic_agent.snapshot": [
false
],
"elastic_agent.version": [
"8.17.0"
],
"event.agent_id_status": [
"verified"
],
"event.category": [
"network"
],
"event.created": [
"2025-01-16T13:26:35.675Z"
],
"event.dataset": [
"suricata.eve"
],
"event.ingested": [
"2025-01-16T13:26:49.000Z"
],
"event.kind": [
"event"
],
"event.module": [
"suricata"
],
"event.type": [
"protocol"
],
"input.type": [
"log"
],
"log.file.path": [
"/var/log/suricata/eve.json"
],
"log.offset": [
1430128
],
"network.community_id": [
"1:+FxyBDlZf2ZBD4x5BsAYWnWTJyc="
],
"network.protocol": [
"tls"

```
],
"network.transport": [
"tcp"
],
"observer.hostname": [
"kali"
],
"observer.ip": [
"172.17.0.1"
],
"observer.mac": [
"02-42-23-12-56-E6",
"08-00-27-CB-7E-F5"
],
"observer.product": [
"Suricata"
],
"observer.type": [
"ids"
],
"observer.vendor": [
"OISF"
],
"related.hosts": [
"add9e71f48304c70804ecca975a324e3.us-central1.gcp.cloud.es.io"
],
"related.ip": [
"192.168.250.100",
"35.193.143.25"
],
"source.address": [
"192.168.250.100"
],
"source.ip": [
"192.168.250.100"
],
"source.port": [
51934
],
"suricata.eve.event_type": [
"tls"
],
"suricata.eve.flow_id": [
"1121390172740121"
```

```
],
"suricata.eve.in_iface": [
"eth0"
],
"suricata.eve.pkt_src": [
"wire/pcap"
],
"suricata.eve.tls.sni": [
"add9e71f48304c70804ecca975a324e3.us-central1.gcp.cloud.es.io"
],
"suricata.eve.tls.version": [
"TLS 1.3"
],
"tags": [
"forwarded",
"suricata-eve"
],
"tls.client.server_name": [
"add9e71f48304c70804ecca975a324e3.us-central1.gcp.cloud.es.io"
],
"tls.version": [
"1.3"
],
"tls.version_protocol": [
"tls"
],
"_id": "UwVLb5QBo0ylF2SyjXhq",
"_index": ".ds-logs-suricata.eve-default-2025.01.15-000001",
"_score": null
}
```

WINDOWS LOGS



WINDOWS LOG

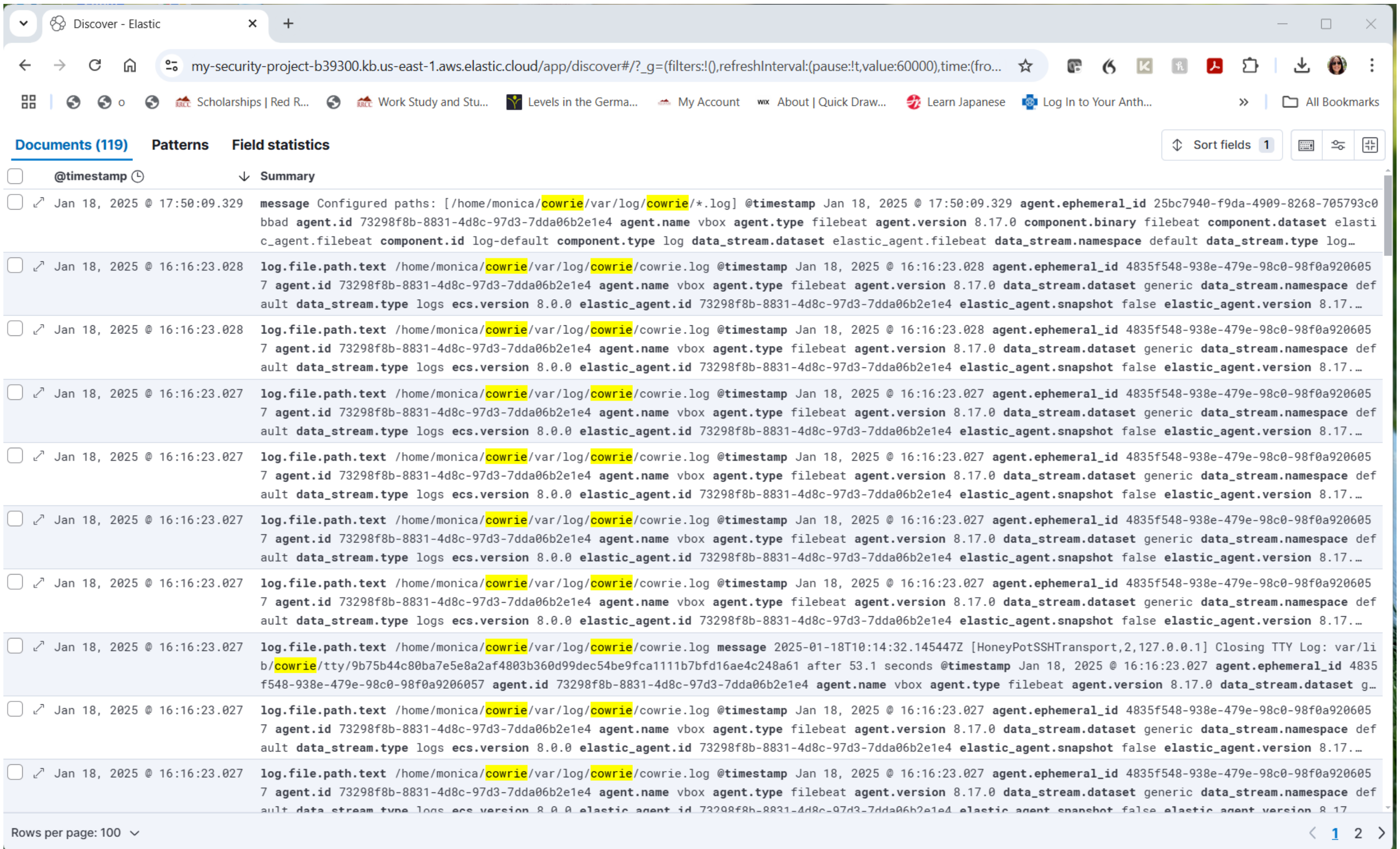
{
"@timestamp": [
"2025-01-20T01:02:53.932Z"
],
"agent.ephemeral_id": [
"c56c0f46-71f1-4013-bd89-d65419a96031"
],
"agent.id": [
"3f2c0aa7-171b-4368-a2a2-9b9bd5052937"
],
"agent.name": [
"DESKTOP-34K6US3"
],
"agent.name.text": [
"DESKTOP-34K6US3"
],
"agent.type": [
"filebeat"

```
  ],
  "agent.version": [
    "8.17.0"
  ],
  "data_stream.dataset": [
    "system.system"
  ],
  "data_stream.namespace": [
    "default"
  ],
  "data_stream.type": [
    "logs"
  ],
  "ecs.version": [
    "8.11.0"
  ],
  "elastic_agent.id": [
    "3f2c0aa7-171b-4368-a2a2-9b9bd5052937"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "elastic_agent.version": [
    "8.17.0"
  ],
  "event.action": [
    "Windows Update Agent"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "event.code": [
    "43"
  ],
  "event.created": [
    "2025-01-20T01:02:55.199Z"
  ],
  "event.dataset": [
    "system.system"
  ],
  "event.ingested": [
    "2025-01-19T16:03:12.000Z"
  ],
  "event.kind": [
```

```
    "event"
  ],
  "event.module": [
    "system"
  ],
  "event.provider": [
    "Microsoft-Windows-WindowsUpdateClient"
  ],
  "host.architecture": [
    "x86_64"
  ],
  "host.hostname": [
    "DESKTOP-34K6US3"
  ],
  "host.id": [
    "c5a4c4f9-536a-40b9-b44c-56f35adff986"
  ],
  "host.ip": [
    "fe80::28d9:f8f2:b83:5f13",
    "192.168.100.103"
  ],
  "host.mac": [
    "08-00-27-B8-8F-2B"
  ],
  "host.name": [
    "desktop-34k6us3"
  ],
  "host.os.build": [
    "19045.2965"
  ],
  "host.os.family": [
    "windows"
  ],
  "host.os.kernel": [
    "10.0.19041.2965 (WinBuild.160101.0800)"
  ],
  "host.os.name": [
    "Windows 10 Home"
  ],
  "host.os.name.text": [
    "Windows 10 Home"
  ],
  "host.os.platform": [
    "windows"
```

```
  ],
  "host.os.type": [
    "windows"
  ],
  "host.os.version": [
    "10.0"
  ],
  "input.type": [
    "winlog"
  ],
  "log.level": [
    "information"
  ],
  "message": [
    "Installation Started: Windows has started installing the following update: 9NBLGGH51CLL-Microsoft.Services.Store.Engagement"
  ],
  "winlog.api": [
    "wineventlog"
  ],
  "winlog.channel": [
    "System"
  ],
  "winlog.computer_name": [
    "DESKTOP-34K6US3"
  ],
  "winlog.event_data.updateGuid": [
    "{3f6608fd-a63e-4c0a-ac23-3d0a81a8fe70}"
  ],
  "winlog.event_data.updateRevisionNumber": [
    "1"
  ],
  "winlog.event_data.updateTitle": [
    "9NBLGGH51CLL-Microsoft.Services.Store.Engagement"
  ],
  "winlog.event_id": [
    "43"
  ],
  "winlog.keywords": [
    "Installation",
    "Started"
  ],
  "winlog.opcode": [
    "Installation"
```

```
  ],
  "winlog.process.pid": [
    4224
  ],
  "winlog.process.thread.id": [
    9428
  ],
  "winlog.provider_guid": [
    "{945a8954-c147-4acd-923f-40c45405a658}"
  ],
  "winlog.provider_name": [
    "Microsoft-Windows-WindowsUpdateClient"
  ],
  "winlog.record_id": [
    "648"
  ],
  "winlog.task": [
    "Windows Update Agent"
  ],
  "winlog.user.domain": [
    "NT AUTHORITY"
  ],
  "winlog.user.identifier": [
    "S-1-5-18"
  ],
  "winlog.user.name": [
    "SYSTEM"
  ],
  "winlog.user.type": [
    "User"
  ],
  "winlog.version": [
    1
  ],
  "_id": "AZR_TRMpTxFMiMjKzJPG",
  "_index": ".ds-logs-system.system-default-2025.01.17-000001",
  "_score": null
}
```



All logs were received successfully.

The rules of the project specified that DMZ2 was not allowed to access the DMZ, however...

...No rule was specified to prevent Monica from accessing the DMZ. 😊