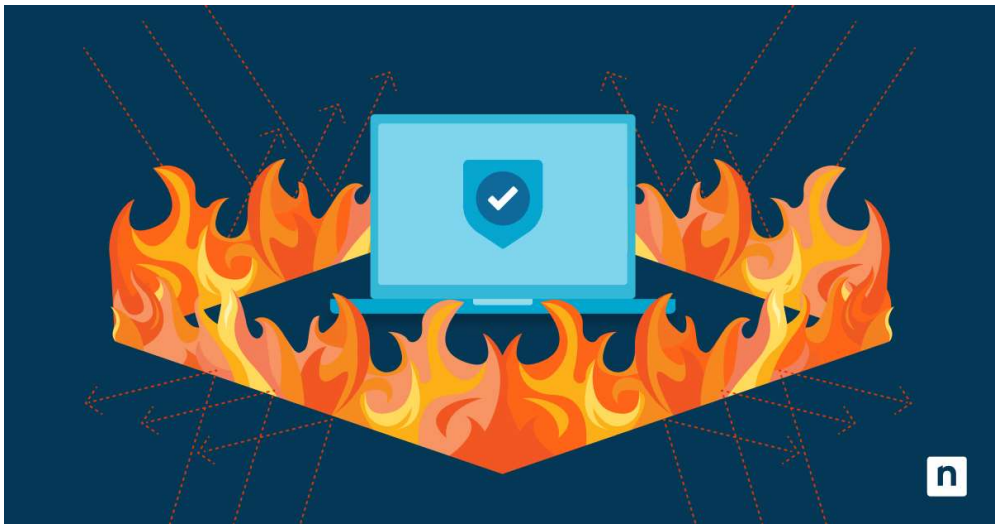
P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

Licenciatura em Segurança Informática em Redes de Computadores

Segurança de Redes

Trabalho Prático 2



David Santos – 8220651

Fábio da Cunha – 8210619

ESTG, julho de 2024

Resumo

Este trabalho prático, realizado no âmbito da Licenciatura em Segurança Informática em Redes de Computadores, teve como objetivo configurar e analisar a segurança de uma rede utilizando o pfSense, uma firewall de código aberto. Através de um cenário virtualizado, foram implementadas políticas de firewall e sistemas de detecção/prevenção de intrusões (IDS/IPS) para proteger a rede interna contra acessos não autorizados e ataques cibernéticos.

Os principais passos do trabalho incluíram:

Configuração das Interfaces de Rede: As interfaces do pfSense foram configuradas para fornecer endereços IP via DHCP à rede interna.

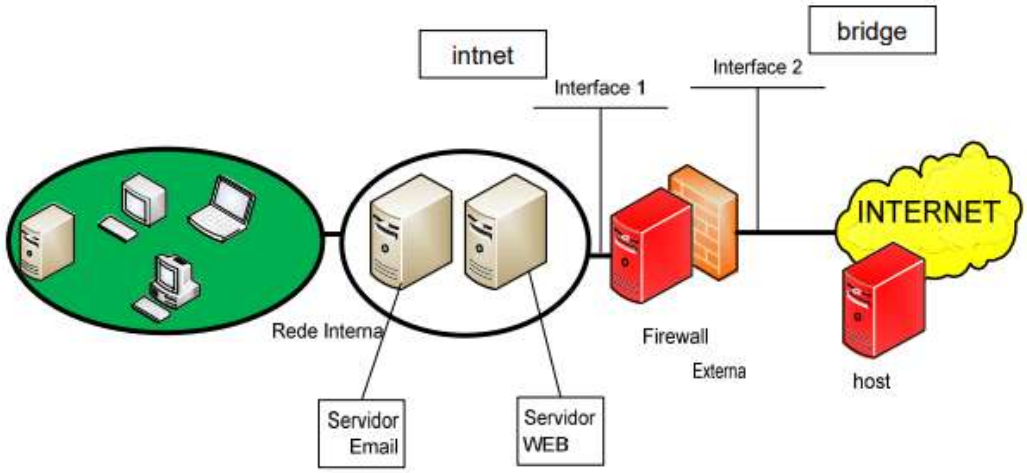
Configuração do Gateway: Incluiu a configuração do DNS Forwarder e do NAT para permitir que as máquinas da rede interna acessem a internet.

Implementação de Políticas de Firewall: Regras específicas foram criadas para controlar o tráfego entre a rede interna e externa, incluindo protocolos como Telnet, FTP, HTTP e SMTP.

Uso do Snort para IDS/IPS: O Snort foi instalado e configurado para monitorar e bloquear tráfego malicioso, com regras personalizadas para alertar e bloquear tráfego ICMP e detectar acessos a conteúdo adulto

Índice

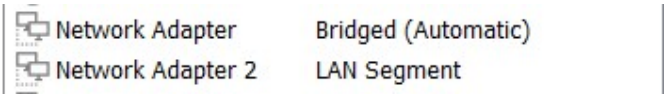
1. Montagem do cenário



1.1 Configuração das interfaces das máquinas

PFsense (Firewall)

As interfaces do PFsense foram configuradas da seguinte forma na aplicação de virtualização:



Com a máquina iniciada, procedemos para a configuração da interface LAN para usar o endereçamento fornecido:

IP a usar	Endereço	Subnet Mask
Rede Interna	10.120.59.0	255.255.255.0

Sendo assim, executámos os seguintes passos:

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.120.59.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.120.59.2
Enter the end address of the IPv4 client address range: 10.120.59.100
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 10.120.59.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.120.59.1/

Press <ENTER> to continue.
```

Após esta configuração, as interfaces do pfsense ficaram com os endereços presentes na figura abaixo:

```
WAN (wan)       -> em0        -> v4/DHCP4: 192.168.52.139/24
LAN (lan)       -> em1        -> v4: 10.120.59.1/24
```

Kali

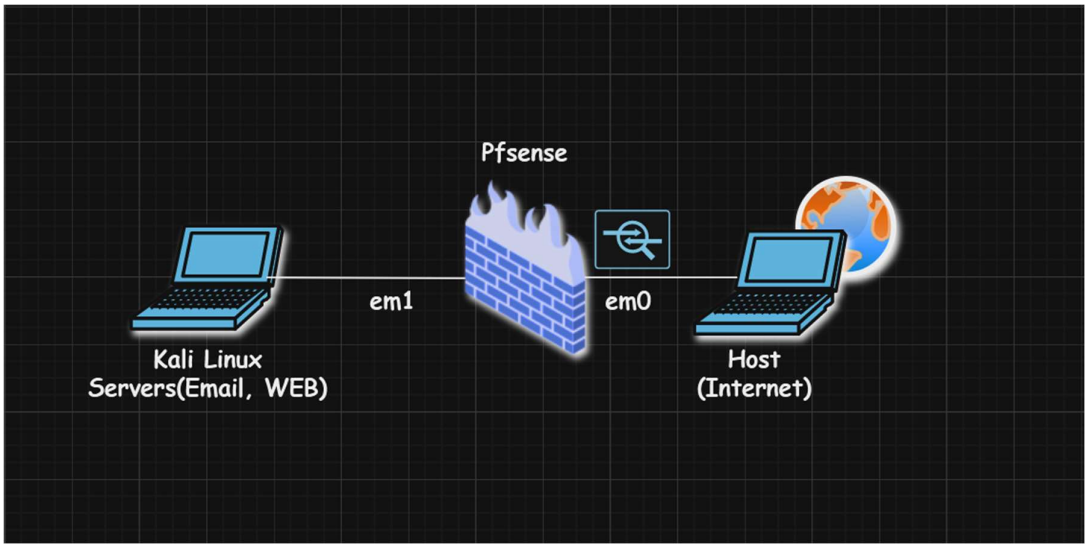
O kali apenas possui uma interface que foi configurada para ser da mesma rede interna que o nosso pfsene:

Com o kali a correr, configurámos essa interface para receber endereço IP de forma automática pelo servidor DHCP, que foi previamente configurado na interface LAN do pfsense, tal como podemos ver nas imagens abaixo:


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:40:df:e6:7e  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.120.59.2  netmask 255.255.255.0  broadcast 10.120.59.255
        inet6 fe80::cde2:9925:59de:abb  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e6:4d:4a  txqueuelen 1000  (Ethernet)
        RX packets 14  bytes 1888 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 115  bytes 11542 (11.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.2 Desenho pormenorizado da implementação



1.3 Configuração do Gateway

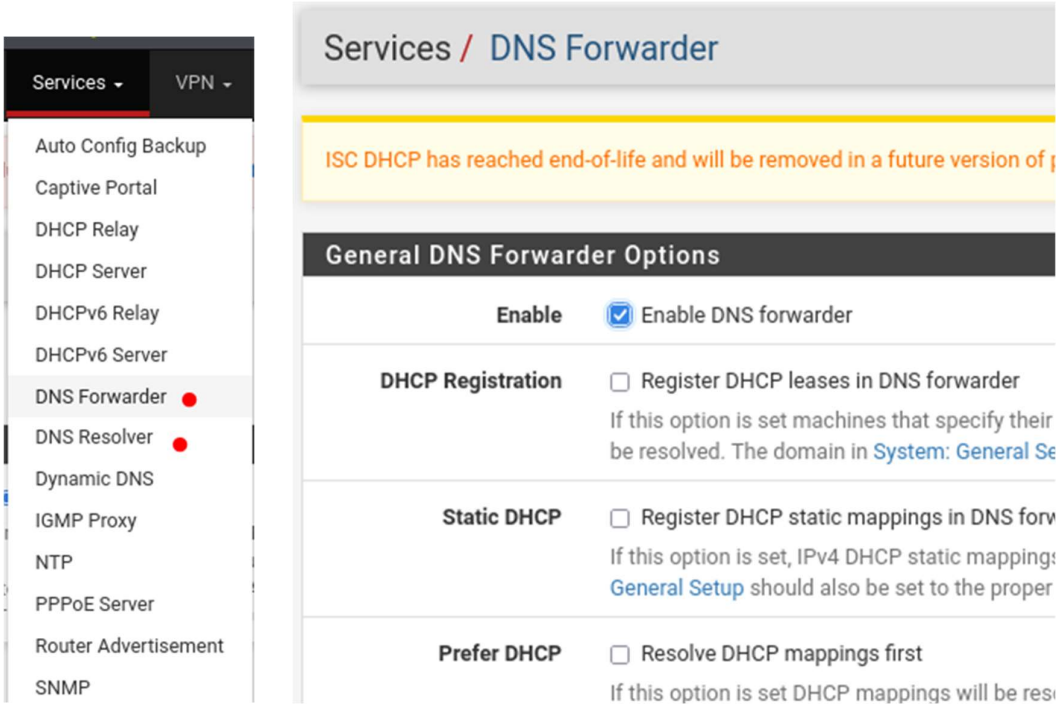
Neste cenário, para as máquinas de rede interna terem acesso ao mundo exterior (internet), tivemos que configurar o pfsense para servir como um gateway. A configuração de gateway está dividida em duas parte:

- Configuração de DNS Forwarder
- Configuração de NAT

DNS Forwarder

O DNS forwarder é um serviço que encaminha DNS **requests de maquina** na rede **interna** para servidores DNS externos, **que no nosso caso é** fornecidos pelo **nosso** provedor de Internet ou outros serviços DNS públicos como o Google DNS**.**

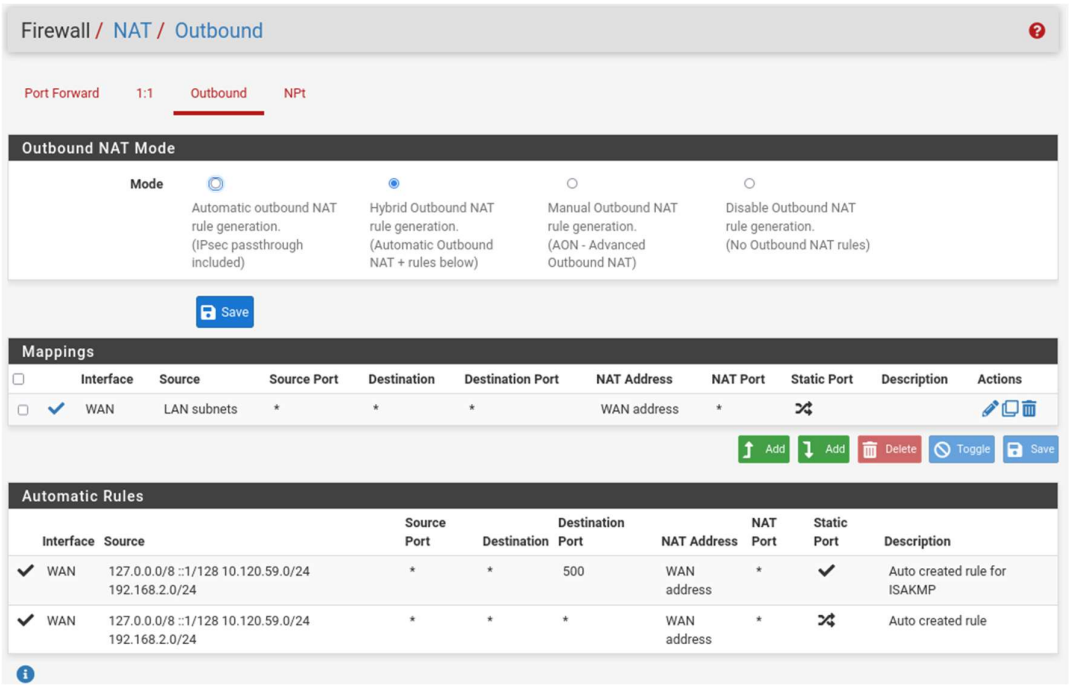
Para ativação deste serviço, tivemos, primeiramente que garantir que o DNS Resolver estava desativado, e posteriormente, na secção de DNS Forwarder ativámos a opção "Enable" , tal como apresentado:

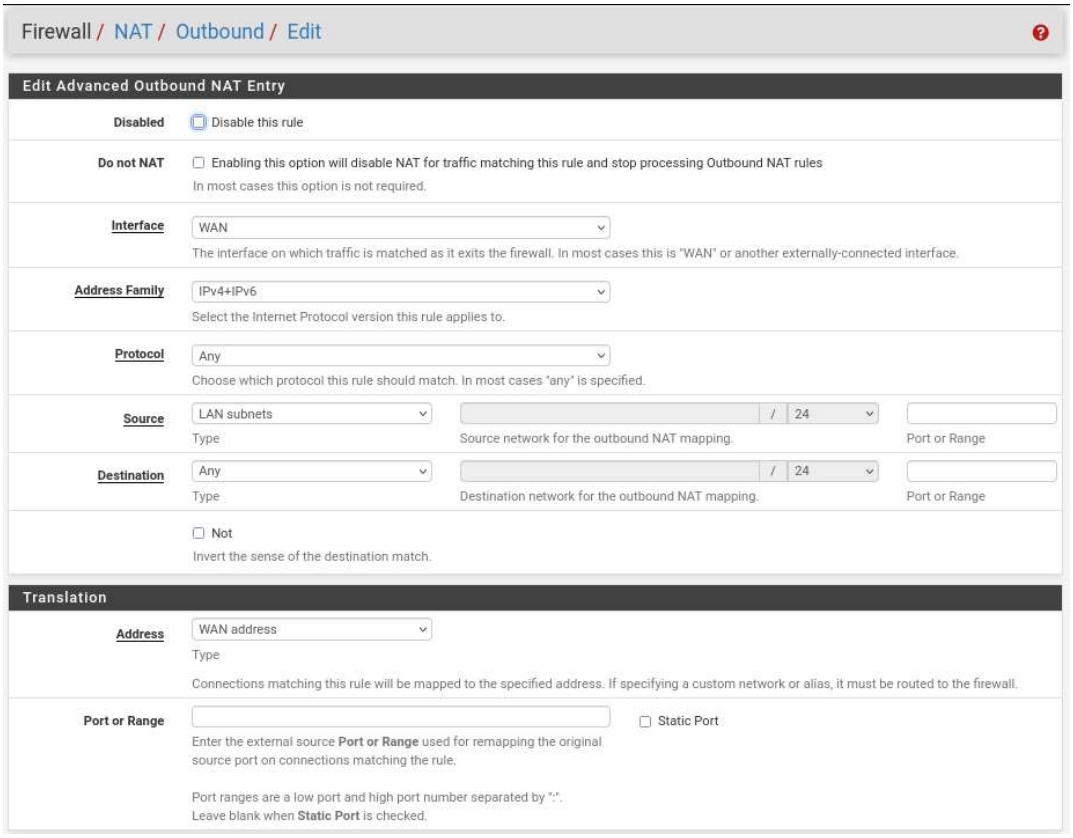


NAT

O NAT é um serviço essencial neste cenário que permite que as máquinas na rede interna acessem a Internet através de um único endereço IP público do pfSense, garantindo a tradução dos endereços IP privados para o endereço IP público ao sair para a rede externa.

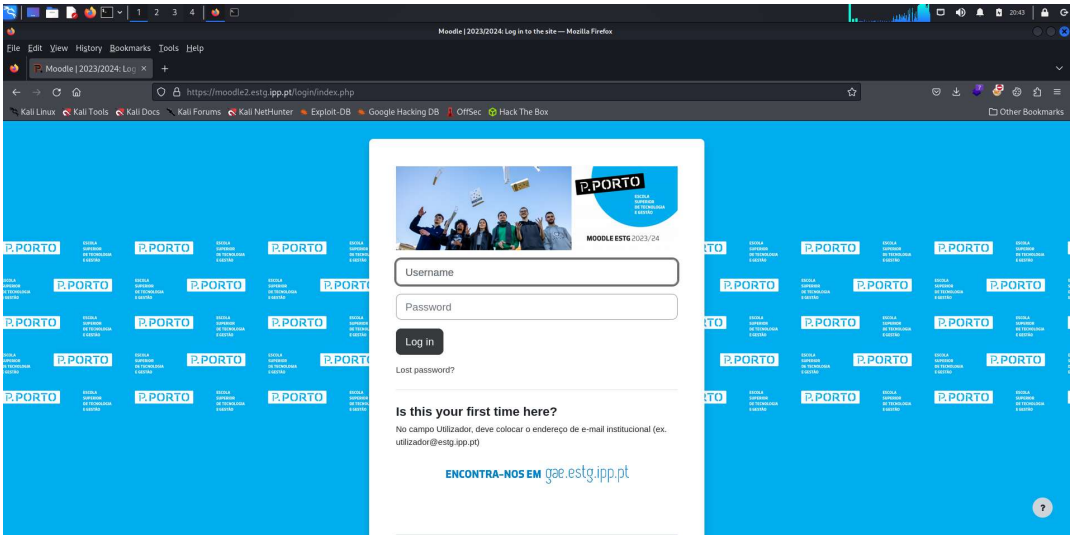
A configuração do NAT no pfsense foi a seguinte:


Firewall / NAT / Outbound
Port Forward
1:1
Outbound
NPt
Outbound NAT Mode
Mode
Automatic outbound NAT rule generation. (IPsec passthrough included)
Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
Disable Outbound NAT rule generation. (No Outbound NAT rules)
Save
Mappings
Interface Source Source Port Destination Destination Port NAT Address NAT Port Static Port Description Actions
WAN LAN subnets * * * WAN address *
Add Add Delete Toggle Save
Automatic Rules
Interface Source Source Port Destination Destination Port NAT Address NAT Port Static Port Description
WAN 127.0.0.0/8 ::1/128 10.120.59.0/24 192.168.2.0/24 * * 500 WAN address * Auto created rule for ISAKMP
WAN 127.0.0.0/8 ::1/128 10.120.59.0/24 192.168.2.0/24 * * * WAN address * Auto created rule

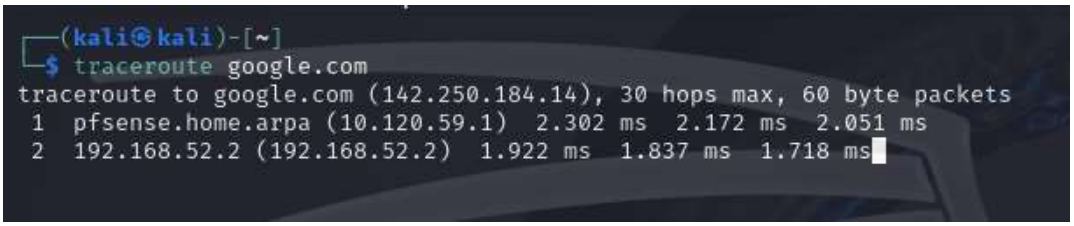

Firewall / NAT / Outbound / Edit
Edit Advanced Outbound NAT Entry
Disabled
Disable this rule
Do not NAT
Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.
Interface
WAN
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.
Address Family
IPv4+IPv6
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which protocol this rule should match. In most cases "any" is specified.
Source
LAN subnets
Type
Source network for the outbound NAT mapping.
24
Port or Range
Destination
Any
Type
Destination network for the outbound NAT mapping.
24
Port or Range
Not
Invert the sense of the destination match.
Translation
Address
WAN address
Type
Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.
Port or Range
Static Port
Enter the external source Port or Range used for remapping the original source port on connections matching the rule.
Port ranges are a low port and high port number separated by ":".
Leave blank when Static Port is checked.

Verificação

A partir do Kali (rede interna), já se tem acesso a internet:



Traceroute para google.com:

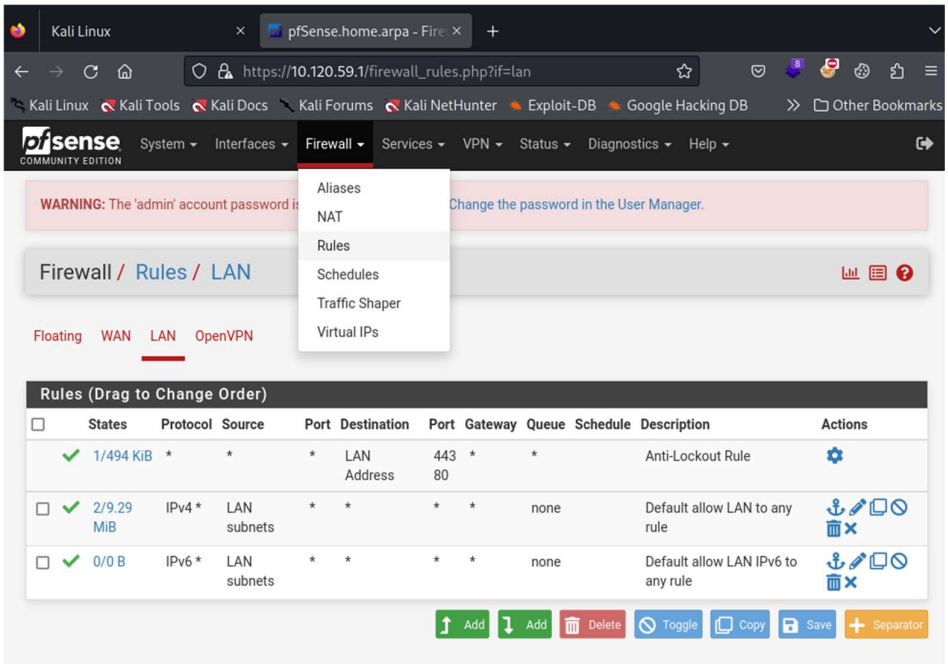


2. Políticas de firewall

	Interface 1		Interface 2	
Protocolo	**Inbound**	**Outbound**	**Inbound**	**Outbound**
Telnet	Sim (rede int)	Não (all)	Não (all)	Sim (all)
FTP	Sim (rede int)	Não (all)	Não (all)	Sim (rede int)
Ping	Sim (rede int)	Não (all)	Sim (all)	Sim (all)
Web (80)	Sim (all)	Sim (all)	Sim (all)	Sim (all)
Email (25)	Não (all)	Sim (all)	Sim (all)	Não (all)

Tendo em conta as políticas podemos afirmar que o objetivo da firewall é proteger a rede interna (10.120.59.0/24) de acessos não autorizados, controlando e monitorando o tráfego entre a rede interna e externa, além de detetar e prevenir possíveis intrusões.

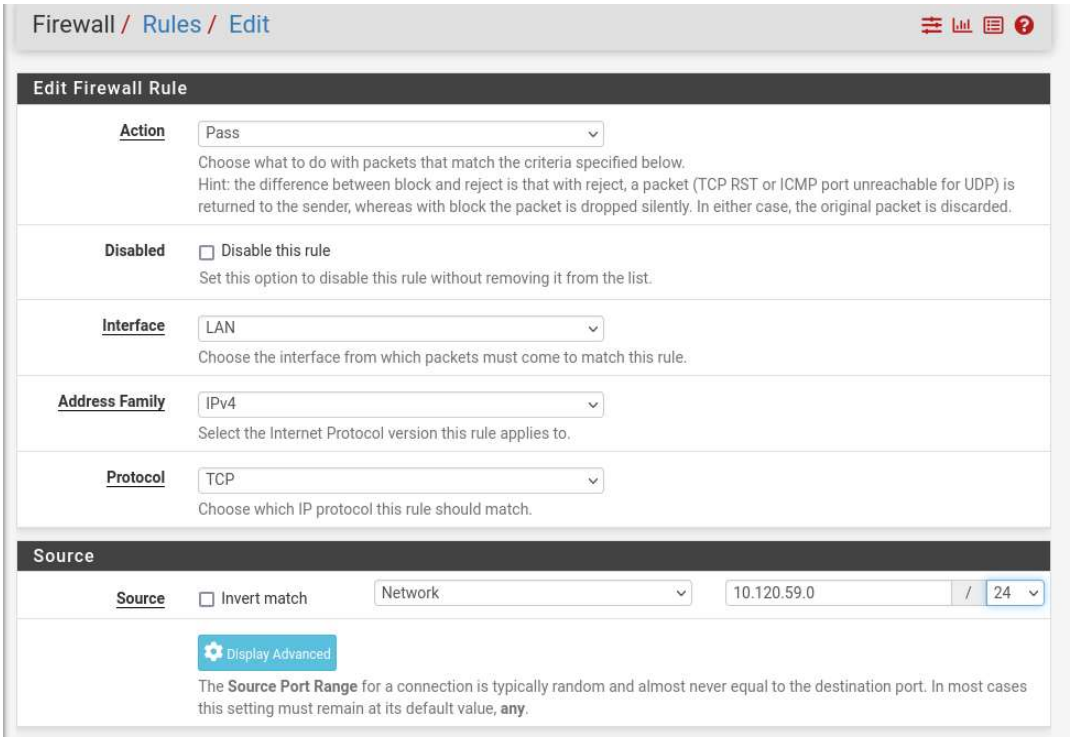
Para adicionar regras na firewall acessamos ao separador Firewall > Rules:



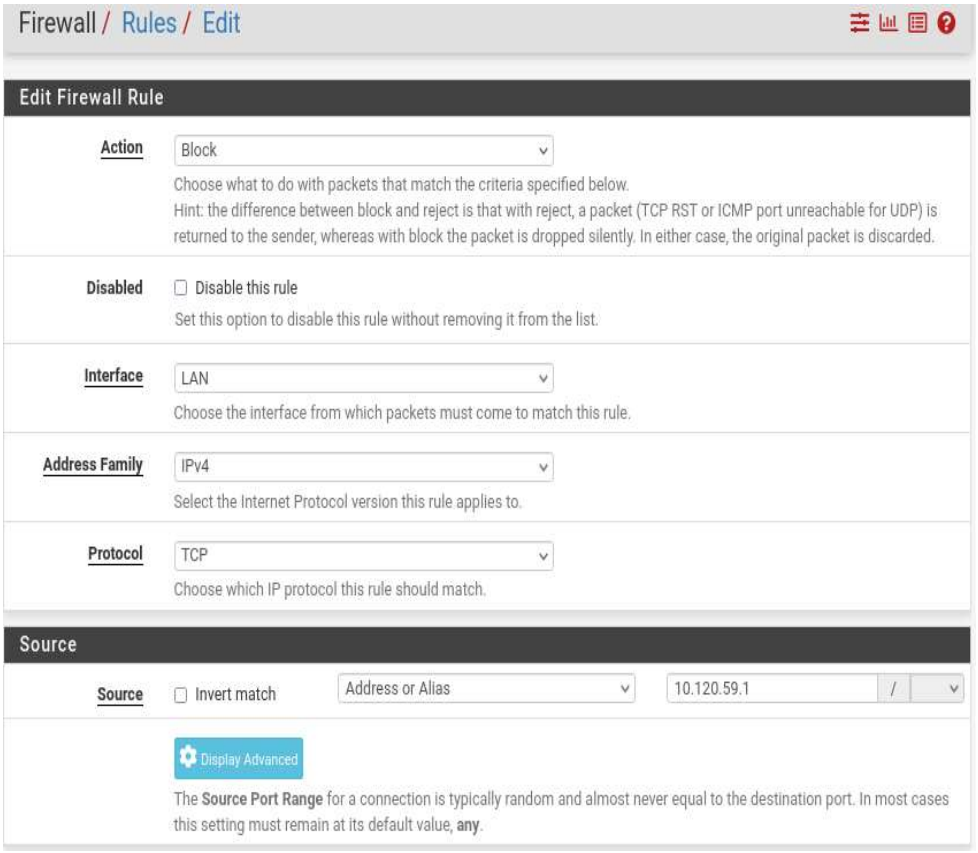
2.1 Implementação das políticas LAN

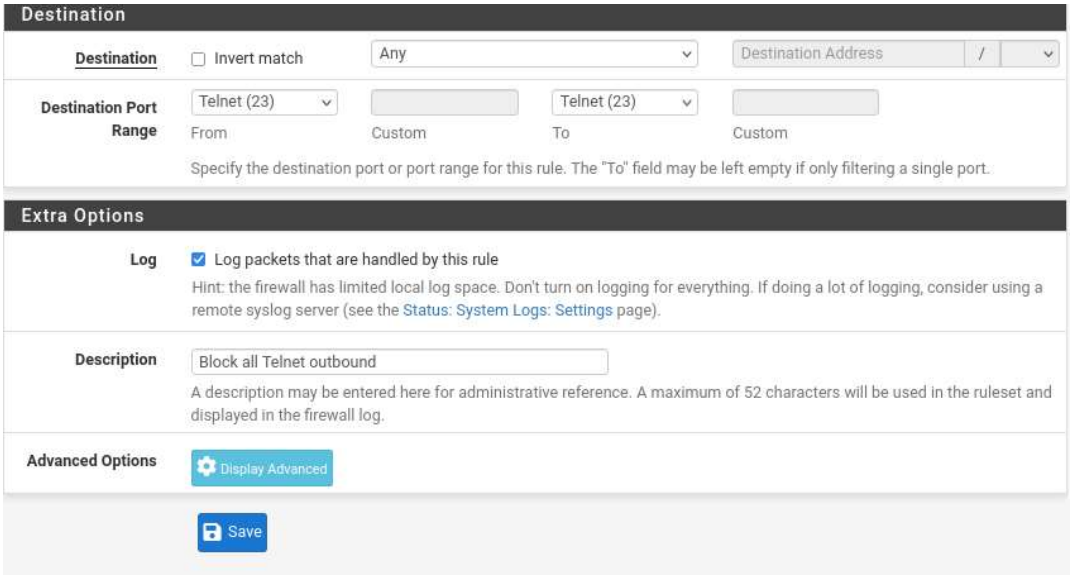
Telnet

Inbound



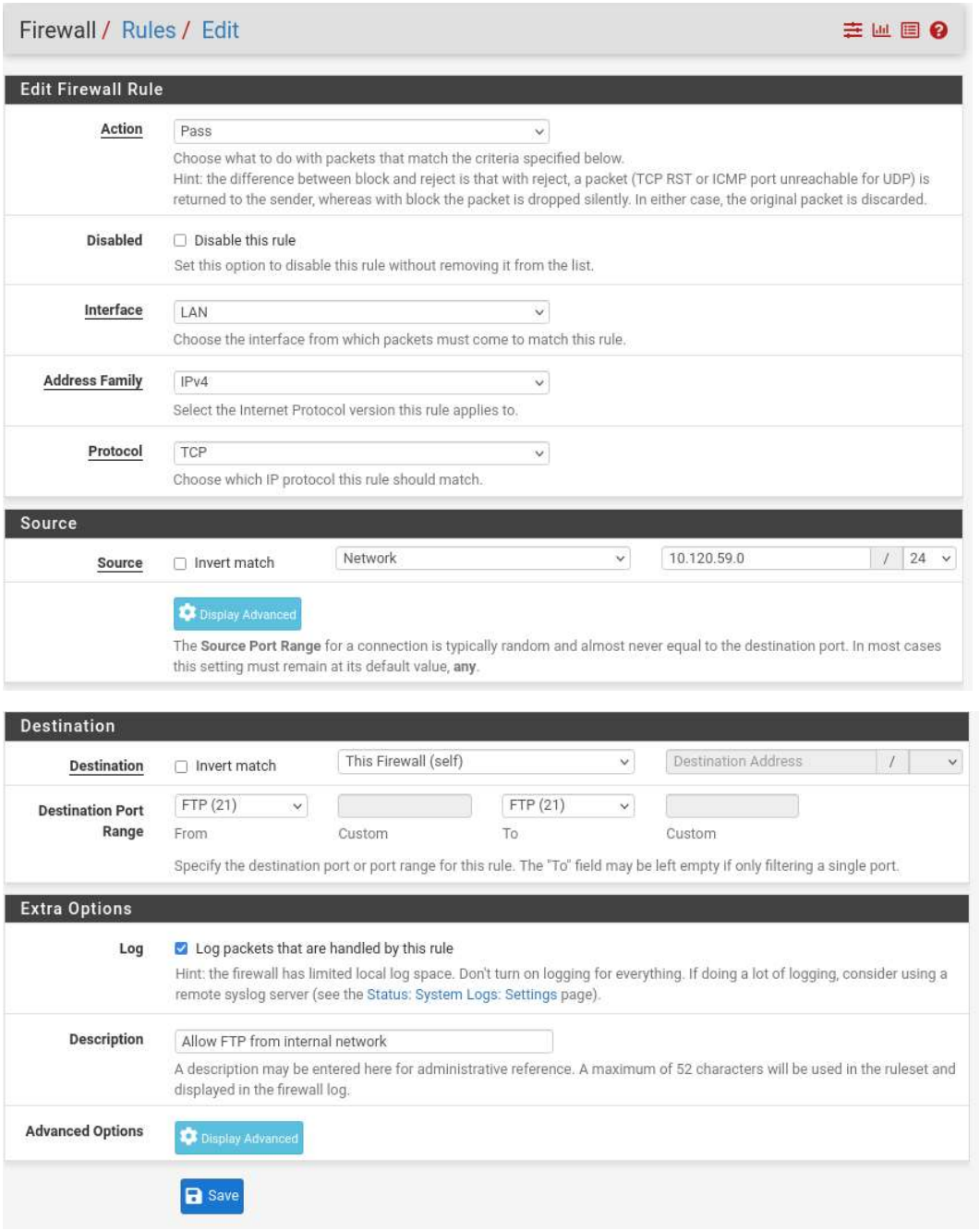
Outbound


Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
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
LAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
Address or Alias
10.120.59.1
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.

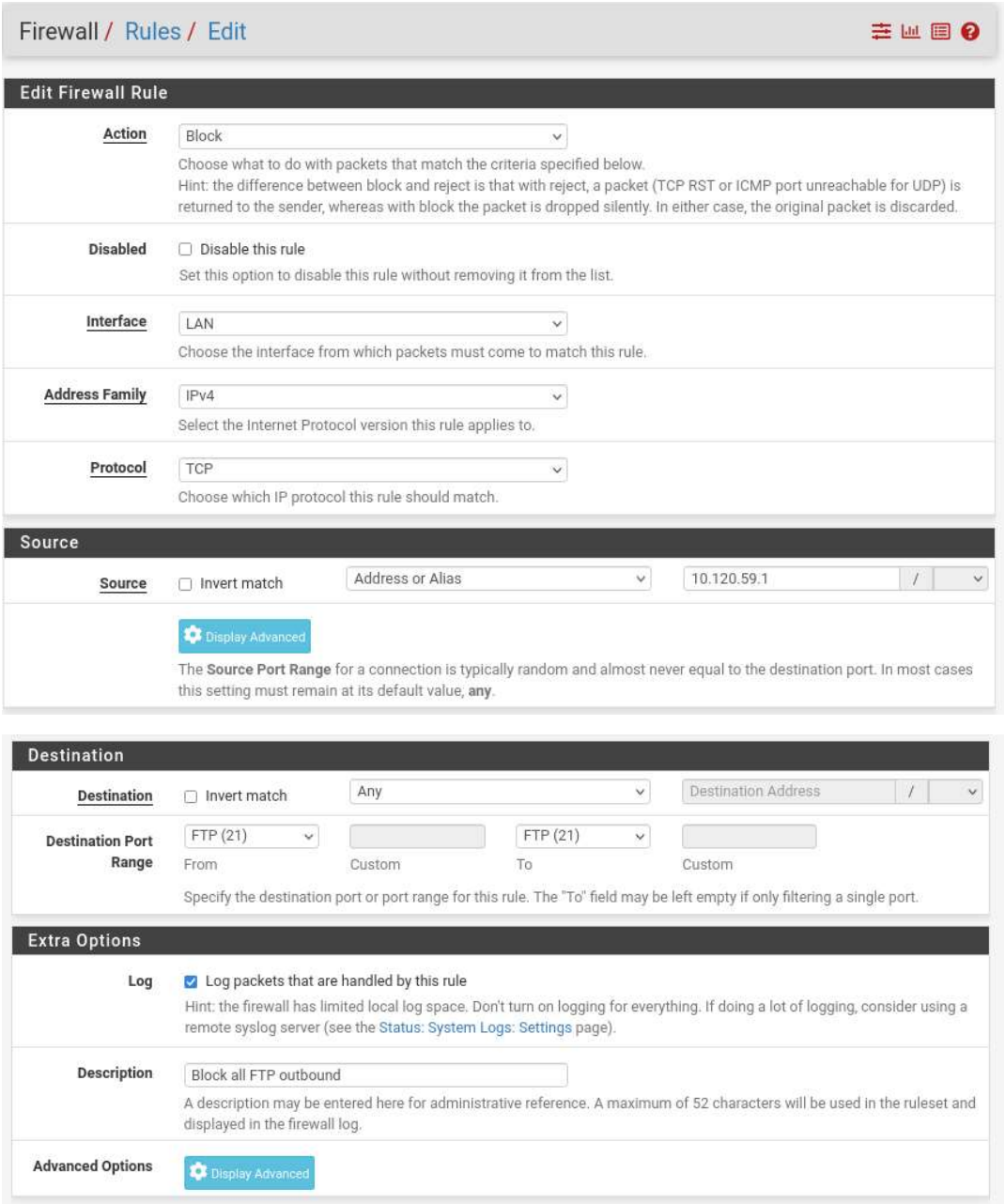

Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
Telnet (23)
From
Custom
Telnet (23)
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled 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
Block all Telnet outbound
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
Save

FTP

Inbound

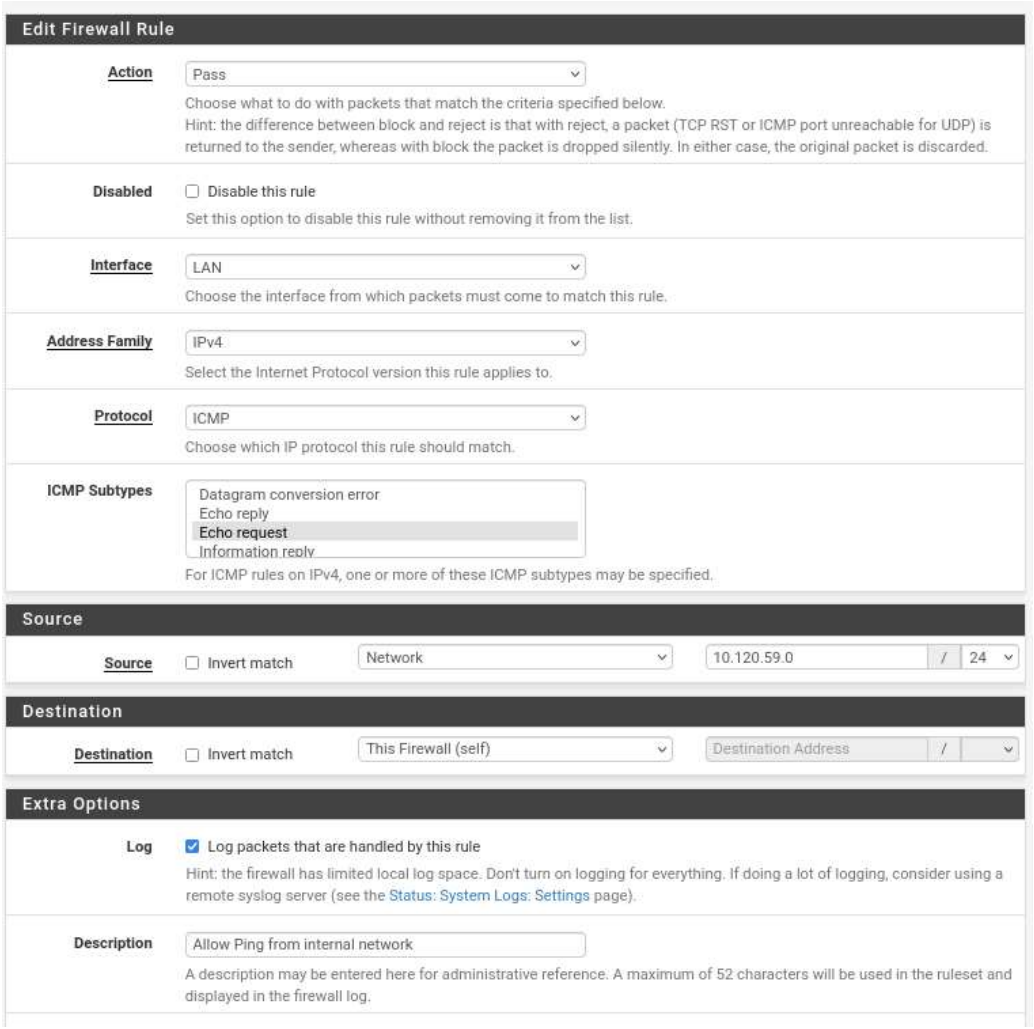

Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet 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
LAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
Network
10.120.59.0
/
24
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
This Firewall (self)
Destination Address
Destination Port Range
FTP (21)
From
Custom
FTP (21)
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
Allow FTP from internal network
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
Save

Outbound

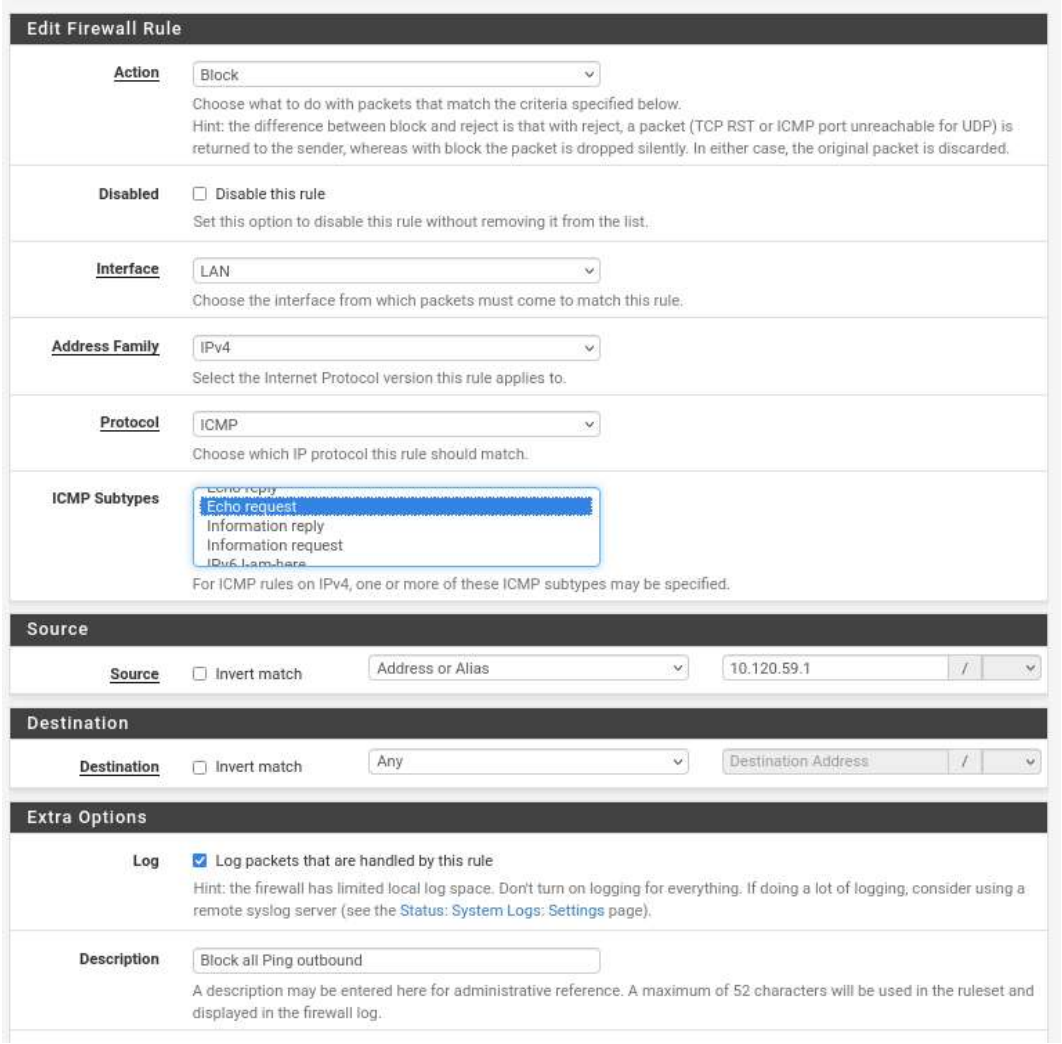

Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet 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
LAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
Address or Alias
10.120.59.1
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 Address
Destination Port Range
FTP (21)
From
Custom
FTP (21)
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
Block all FTP outbound
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

Ping

Inbound

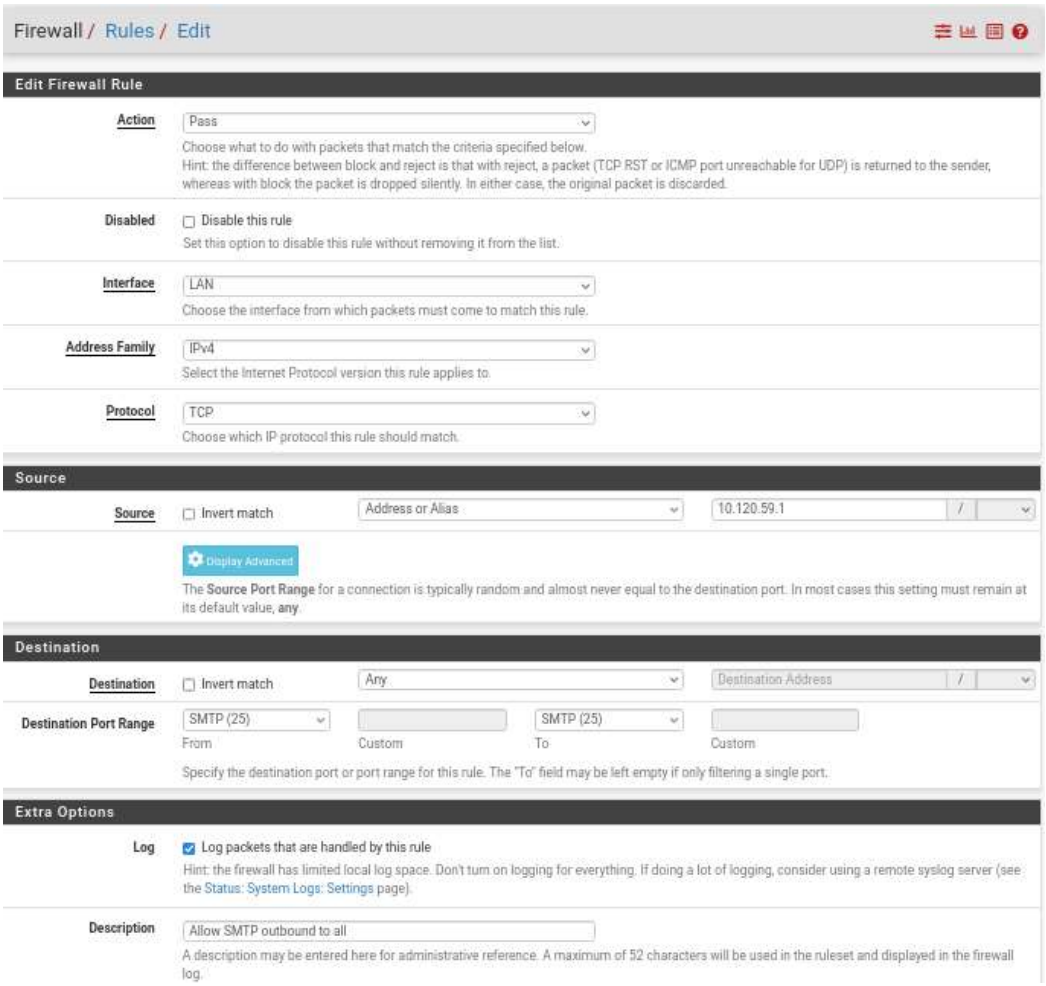


Outbound

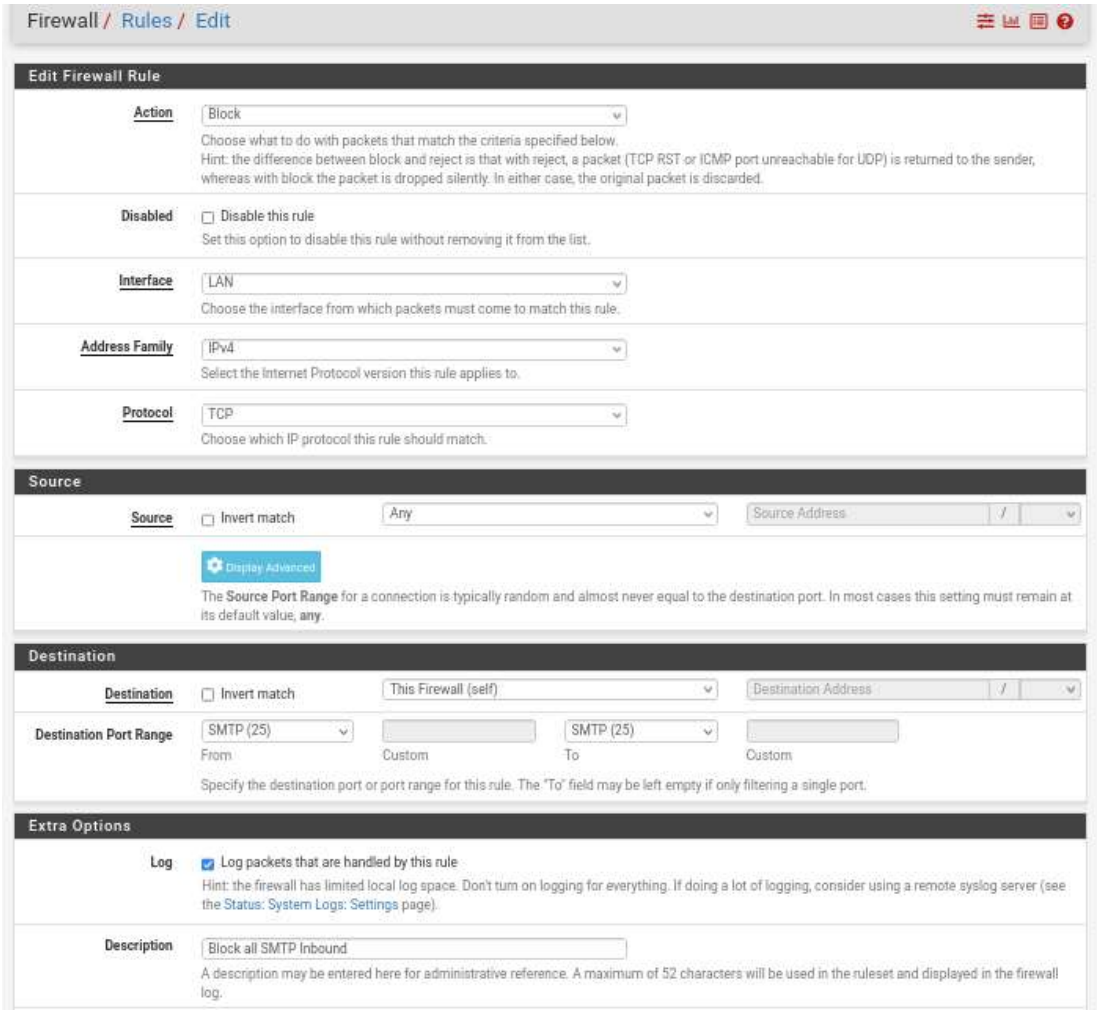


SMTP

Inbound


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
LAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
Address or Alias
10.120.59.1
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 Address
Destination Port Range
SMTP (25)
From
Custom
SMTP (25)
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
Allow SMTP outbound to all
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.

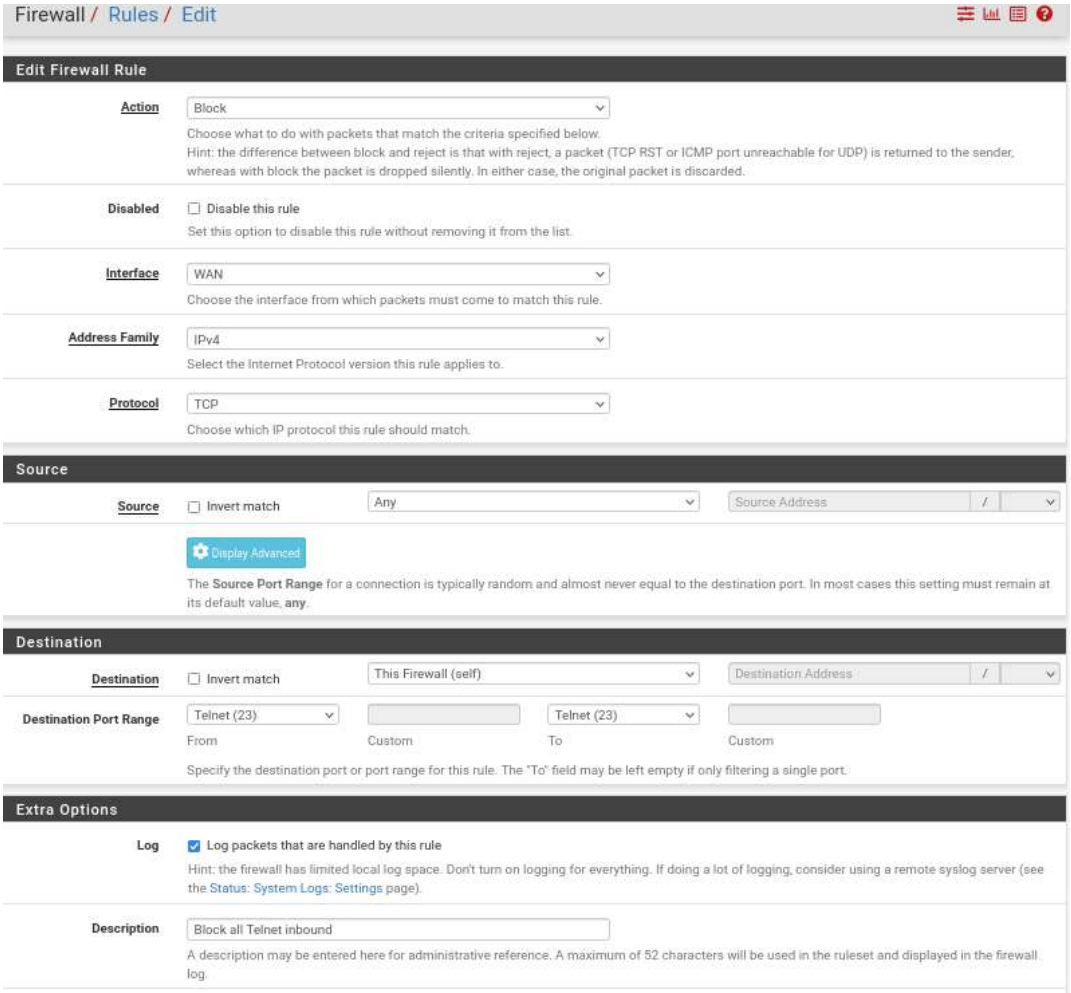
Outbound


Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
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
LAN
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
TCP
Choose which IP protocol this rule should match.
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
This Firewall (self)
Destination Address
Destination Port Range
SMTP (25)
From
Custom
SMTP (25)
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
Block all SMTP Inbound
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.

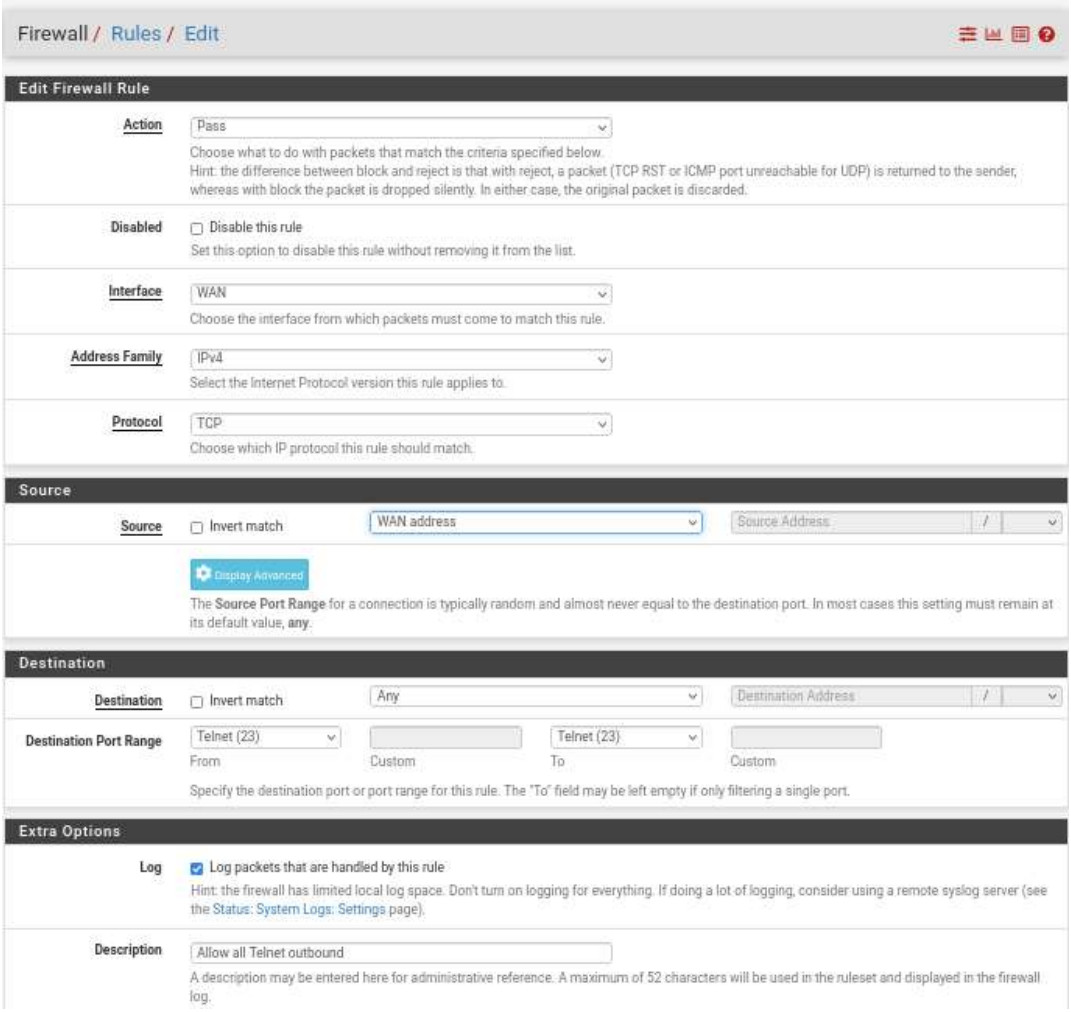
2.2 Implementação das políticas WAN

Telnet

Inbound

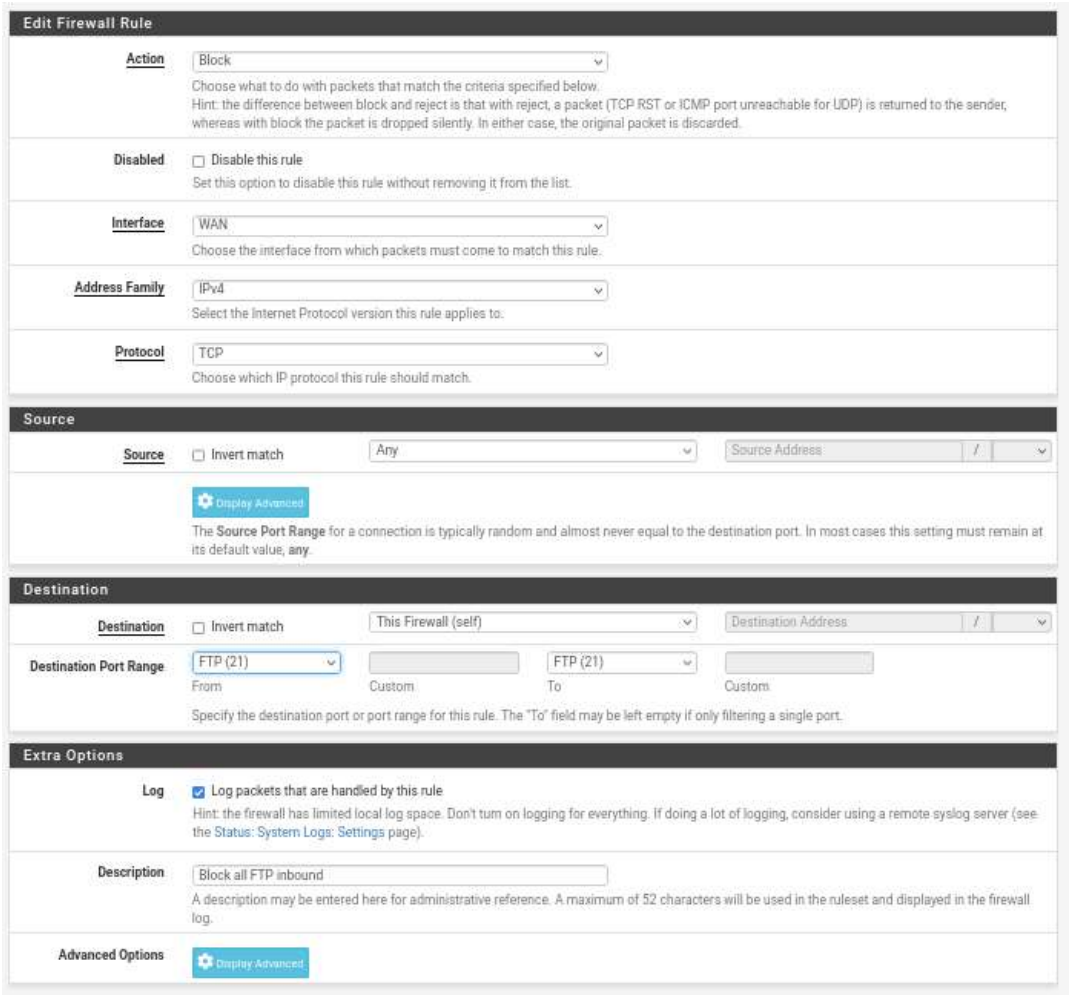


Outbound

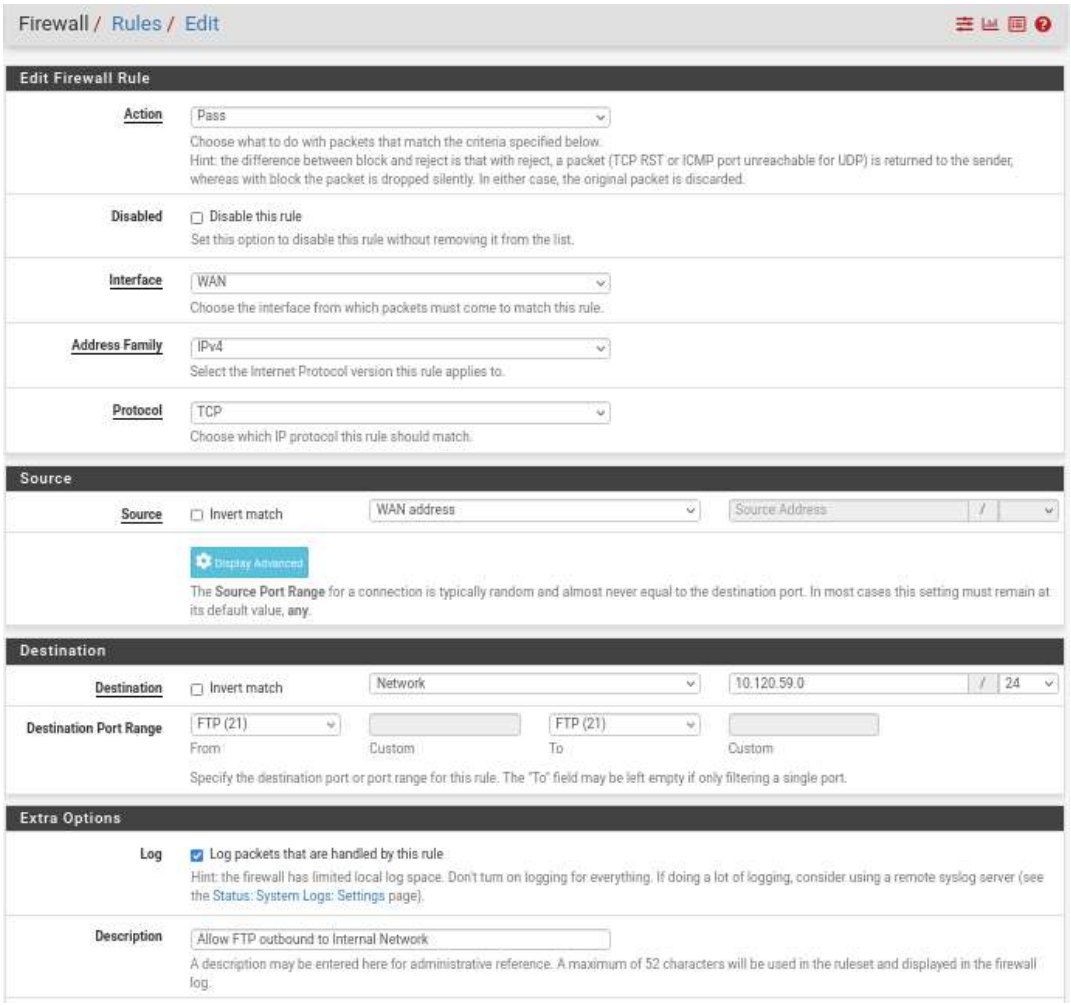

Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet 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
WAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
WAN address
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 Address
Destination Port Range
Telnet (23)
From
Custom
Telnet (23)
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
Allow all Telnet outbound
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.

FTP

Inbound

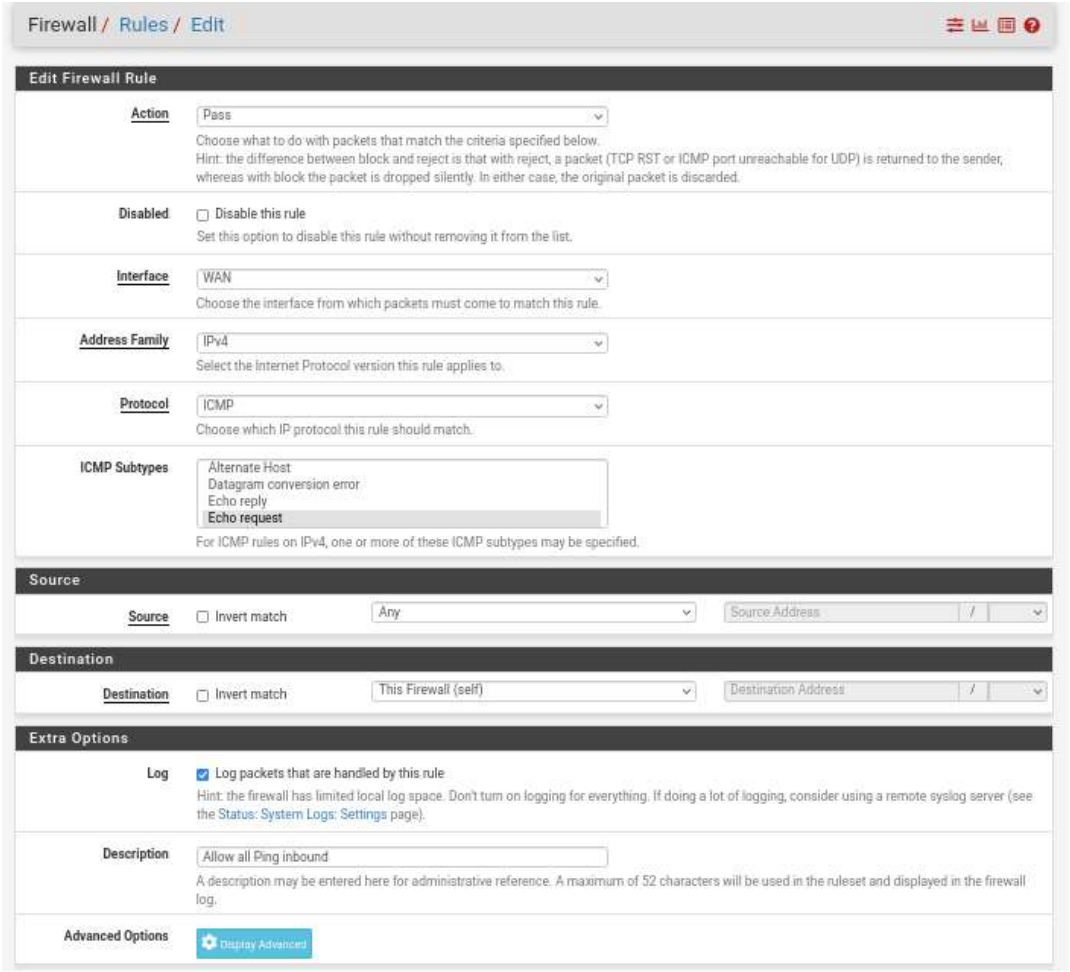

Edit Firewall Rule
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. 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
WAN
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
TCP
Choose which IP protocol this rule should match.
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
This Firewall (self)
Destination Address
Destination Port Range
FTP (21)
From
Custom
FTP (21)
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
Block all FTP inbound
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

Outbound

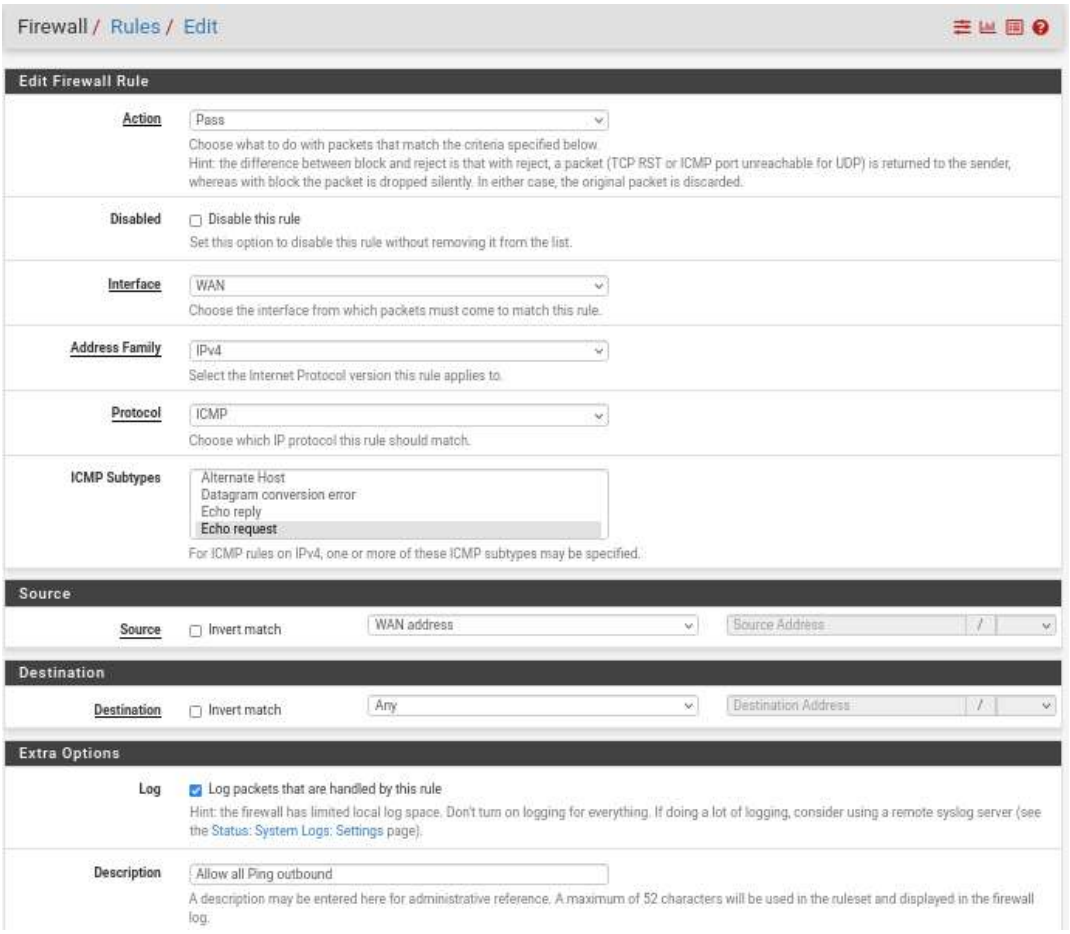

Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet 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
WAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
WAN address
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
Network
10.120.59.0
24
Destination Port Range
FTP (21)
From
Custom
FTP (21)
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
Allow FTP outbound to Internal Network
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.

Ping

Inbound

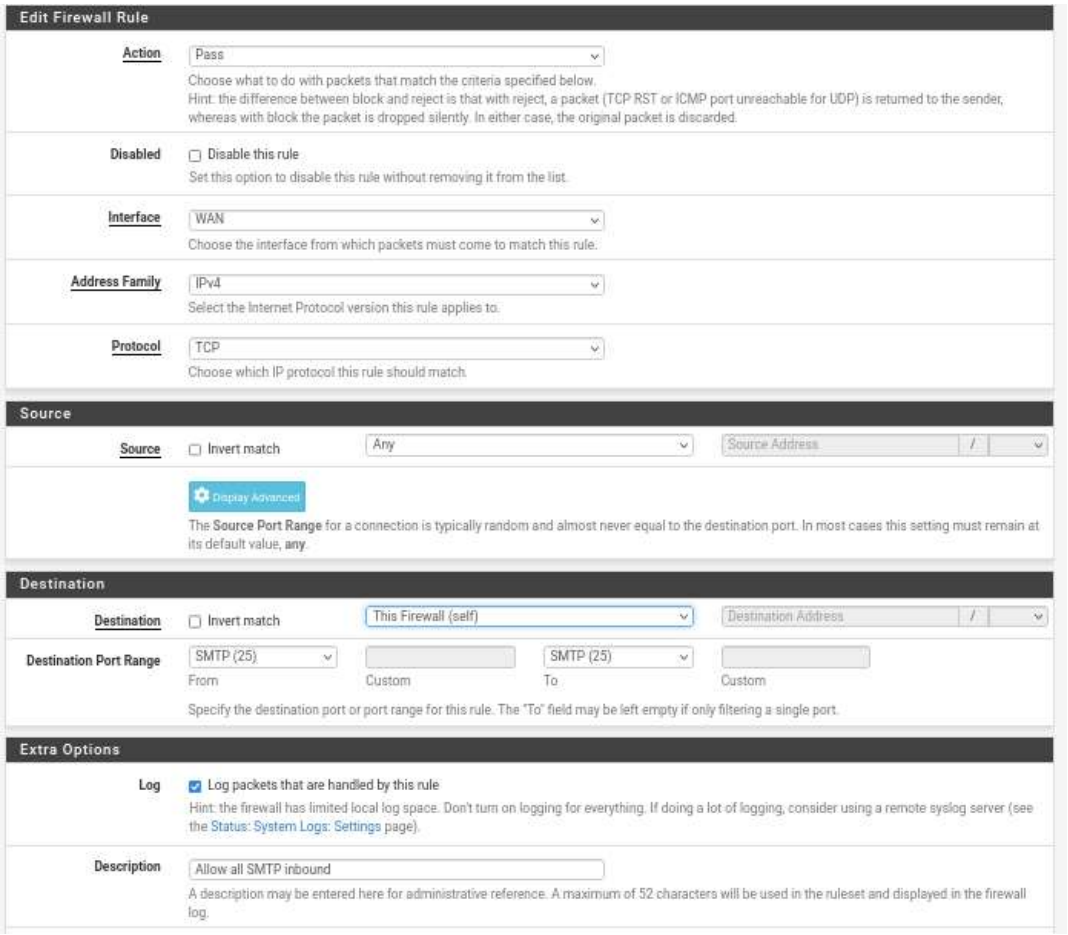


Outbound

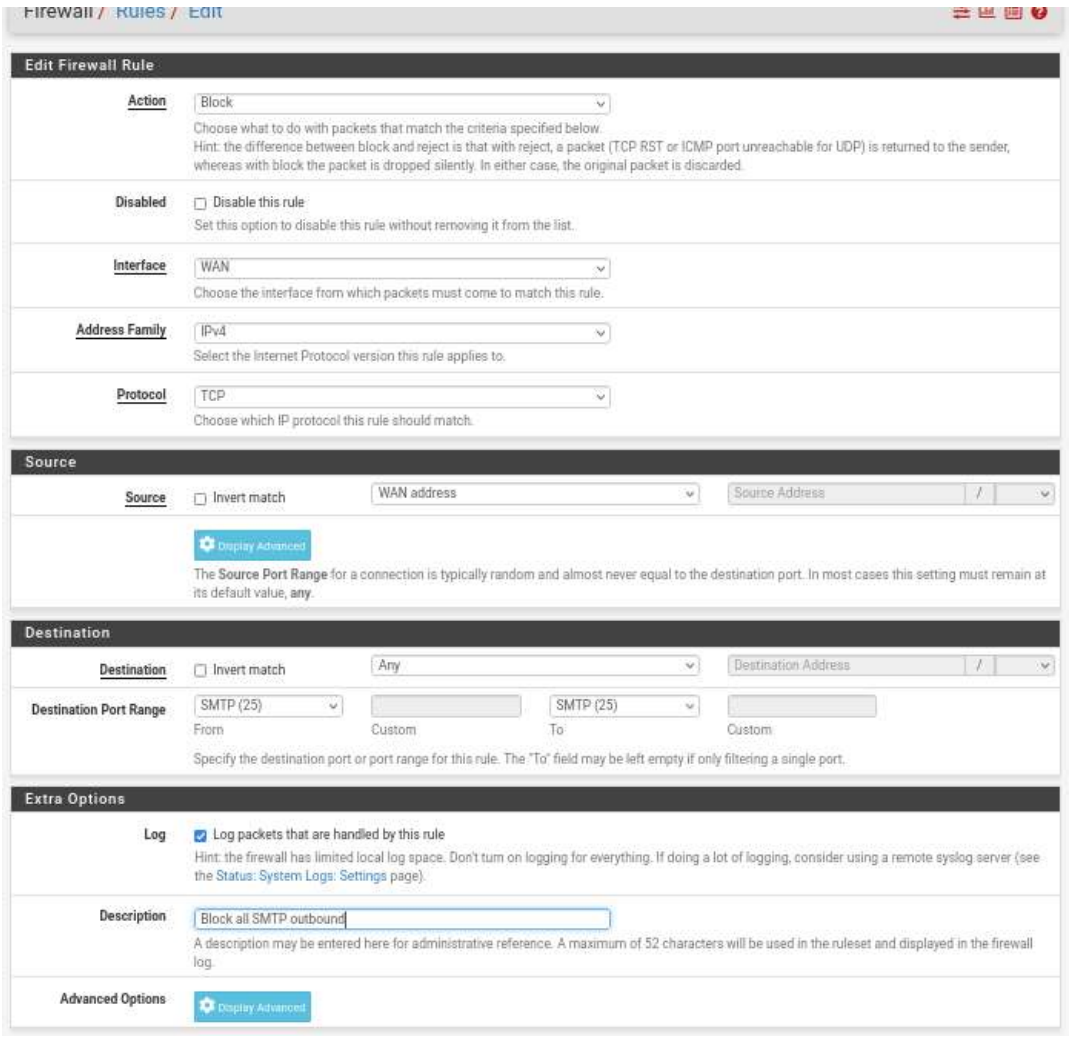

Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet 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
WAN
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
WAN address
Source Address
Destination
Destination
Invert match
Any
Destination Address
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
Allow all Ping outbound
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.

SMTP

Inbound

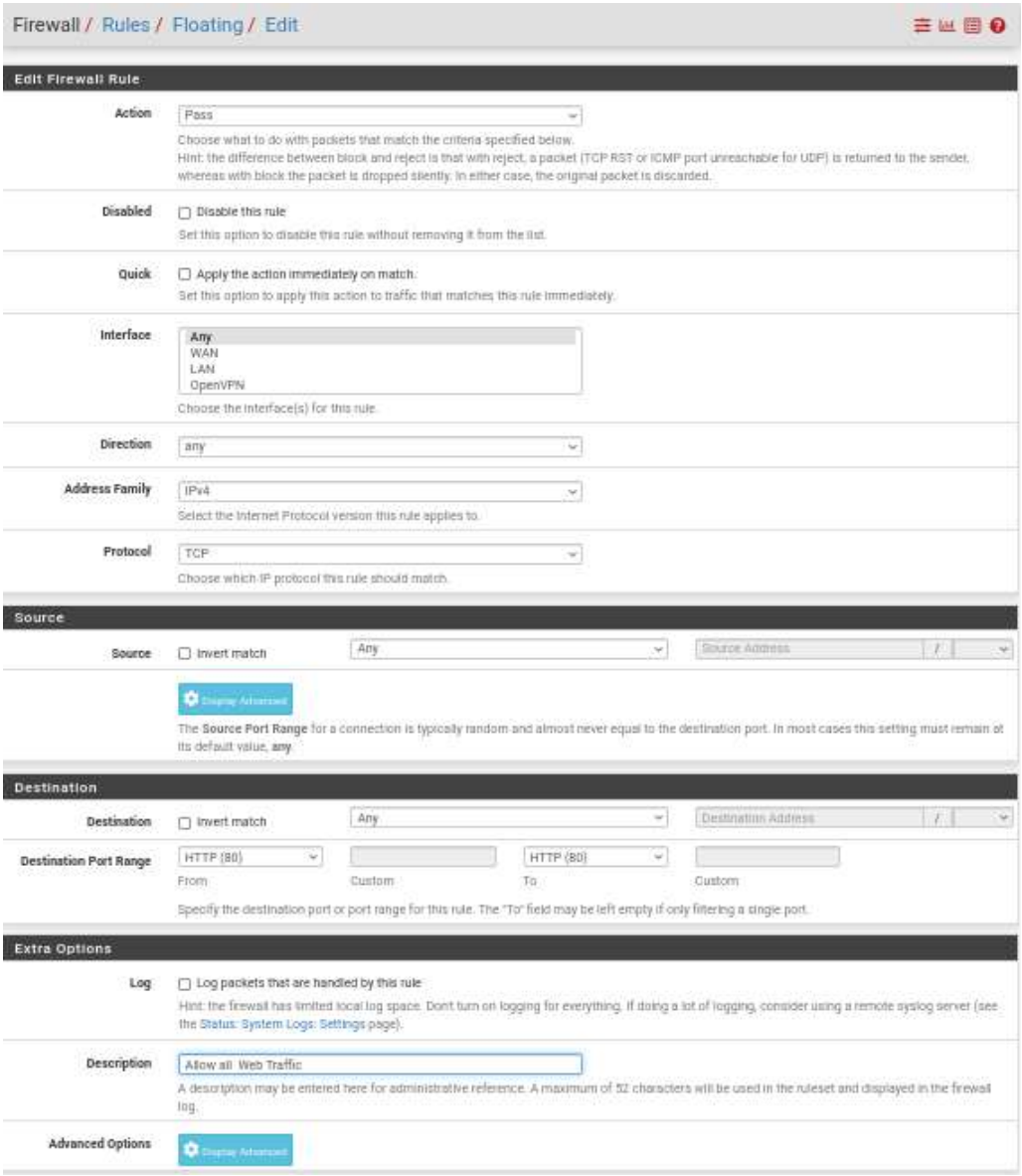


Outbound


Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
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
WAN
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
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
WAN address
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 Address
Destination Port Range
SMTP (25)
From
Custom
SMTP (25)
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
Block all SMTP outbound
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

Web

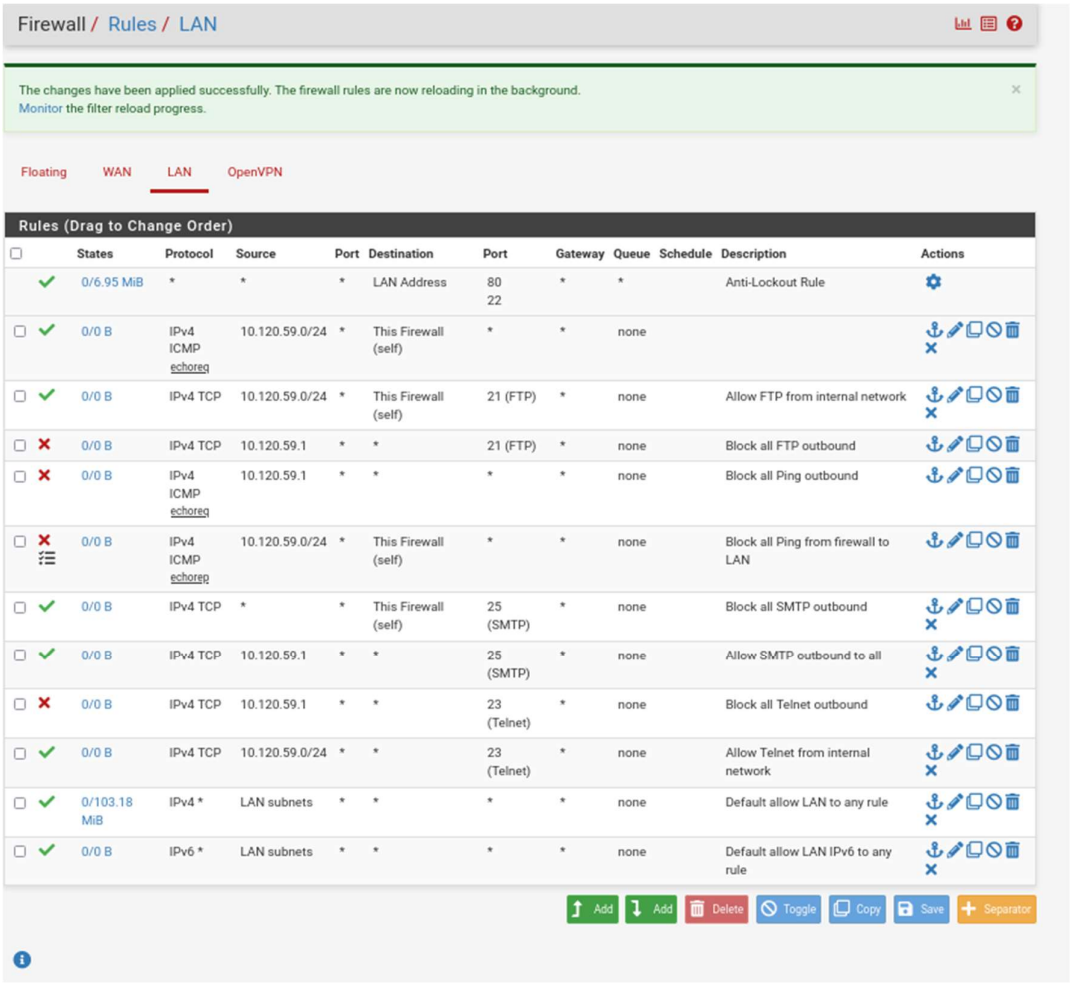
Decidimos colocar na interface floating porque ele abrange tanto a interface WAN como a interface LAN, onde o tráfico WEB em ambos estão como “pass”.



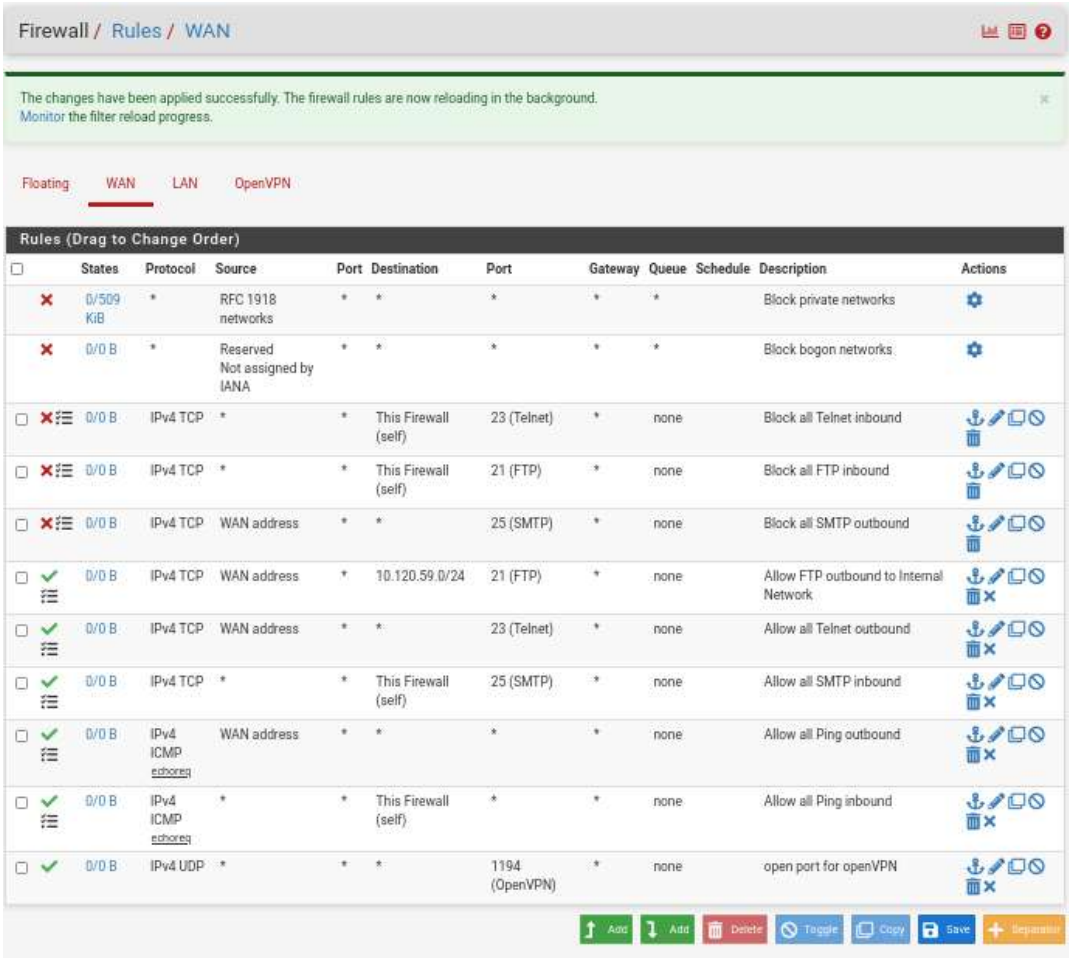
3. Demonstação

3.1 Lista de todas as regras

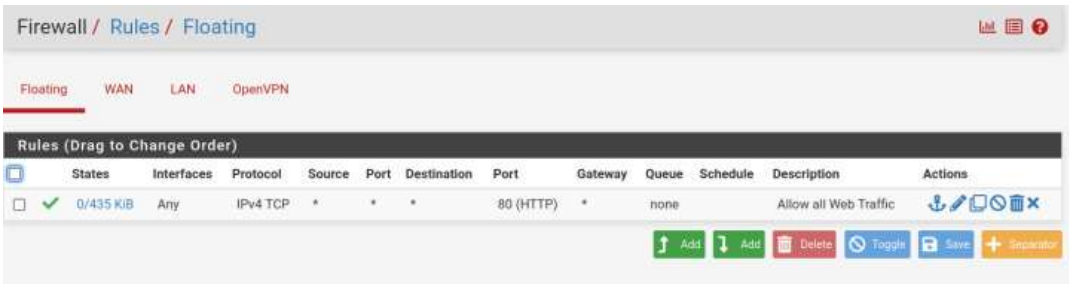
LAN



WAN


Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
OpenVPN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/509 KiB
*
RFC 1918 networks
*
*
*
*
*
Block private networks
0/0 B
*
Reserved Not assigned by IANA
*
*
*
*
*
Block bogon networks
0/0 B
IPv4 TCP
*
*
This Firewall (self)
23 (Telnet)
*
none
Block all Telnet inbound
0/0 B
IPv4 TCP
*
*
This Firewall (self)
21 (FTP)
*
none
Block all FTP inbound
0/0 B
IPv4 TCP
WAN address
*
*
25 (SMTP)
*
none
Block all SMTP outbound
0/0 B
IPv4 TCP
WAN address
*
10.120.59.0/24
21 (FTP)
*
none
Allow FTP outbound to Internal Network
0/0 B
IPv4 TCP
WAN address
*
*
23 (Telnet)
*
none
Allow all Telnet outbound
0/0 B
IPv4 TCP
*
*
This Firewall (self)
25 (SMTP)
*
none
Allow all SMTP inbound
0/0 B
IPv4 ICMP echoreq
WAN address
*
*
*
*
none
Allow all Ping outbound
0/0 B
IPv4 ICMP echoreq
*
*
This Firewall (self)
*
*
none
Allow all Ping inbound
0/0 B
IPv4 UDP
*
*
*
1194 (OpenVPN)
*
none
open port for openVPN
Add
Add
Delete
Toggle
Copy
Save
Separator

Floating


Firewall / Rules / Floating
Floating
WAN
LAN
OpenVPN
Rules (Drag to Change Order)
States
Interfaces
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/435 KiB
Any
IPv4 TCP
*
*
*
80 (HTTP)
*
none
Allow all Web Traffic
Add
Add
Delete
Toggle
Save
Separator

3.2 Protocolos inseguros e proposta de alteração

Neste trabalho, identificamos que os protocolos Telnet, FTP, HTTP e SMTP são considerados inseguros. A principal vulnerabilidade desses protocolos é que eles não utilizam criptografia, resultando em transmissão de dados em texto claro, o que pode expor informações sensíveis a interceptações e ataques.

Propostas de Alteração para Melhorar a Segurança da Rede

Para aumentar a segurança da rede montada, é altamente recomendável substituir esses protocolos inseguros por suas versões seguras:

- Telnet (port 23) passa a SSH (port 22);
- FTP (port 21) passa a SFTP (port 22);
- HTTP (port 80) passa a HTTPS (port 443);
- SMTP (port 25) passa a SMTPS (port 465).

Propomos estas alterações pelos seguintes motivos:

SSH (Porta 22) em vez de Telnet (Porta 23)

O SSH (Secure Shell) oferece uma camada de criptografia robusta que protege a confidencialidade e a integridade dos dados transmitidos. Além disso, SSH proporciona uma autenticação segura, prevenindo o acesso não autorizado. Ao contrário do Telnet, que transmite dados em texto claro e é vulnerável a intercetações, o SSH criptografa todas as informações, impedindo que dados sensíveis sejam capturados por invasores.

SFTP (Porta 22) em vez de FTP (Porta 21)

O SFTP (SSH File Transfer Protocol) utiliza o protocolo SSH para garantir uma conexão segura e criptografada durante a transferência de arquivos. Isso elimina as vulnerabilidades associadas ao FTP, que envia dados em texto claro e é suscetível a ataques de interceptação e manipulação de dados. SFTP não apenas criptografa a transmissão de dados, mas também assegura que a comunicação seja autenticada, proporcionando uma troca de arquivos segura.

HTTPS (Porta 443) em vez de HTTP (Porta 80)

Segurança: HTTPS (Hypertext Transfer Protocol Secure) emprega SSL/TLS para criptografar a comunicação entre o cliente e o servidor. Isso protege os dados contra interceptações e ataques man-in-the-middle. Diferentemente do HTTP, que transmite dados em texto claro e expõe informações sensíveis como credenciais de login e dados pessoais, o HTTPS

garante que todas as informações trocadas entre o cliente e o servidor sejam criptografadas, oferecendo assim uma camada adicional de segurança.

SMTPS (Porta 465) em vez de SMTP (Porta 25)

Segurança: SMTPS (SMTP Secure) adiciona criptografia às comunicações de email, protegendo tanto as credenciais de login quanto o conteúdo das mensagens contra intercetações. SMTP, quando usado na porta 25, não oferece criptografia por padrão, deixando as comunicações de email vulneráveis a ataques de intercetação e manipulação. Ao utilizar SMTPS, as mensagens são criptografadas durante o trânsito, garantindo que apenas os destinatários pretendidos possam acessar o conteúdo das mensagens.

Considerações em relação ao Ping

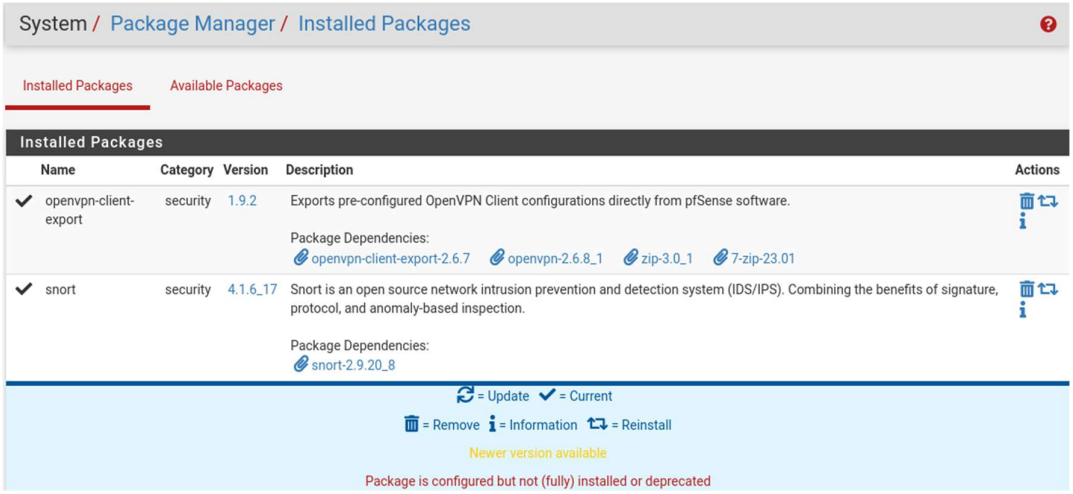
O uso do Ping, apesar de útil para diagnósticos de rede, pode ser explorado em cenários de ataque, como ataques de negação de serviço e mapeamento de rede por atacantes para identificar dispositivos e suas vulnerabilidades. Portanto, é recomendável considerar o bloqueio do tráfego ICMP em ambientes onde a segurança é crítica, para mitigar o risco de tais ataques e reduzir a exposição da rede a ameaças externas.

Após implementar essas alterações, é essencial bloquear todo o tráfego não necessário, criando regras específicas para permitir apenas os novos protocolos seguros (SSH, SFTP, HTTPS e SMTPS).

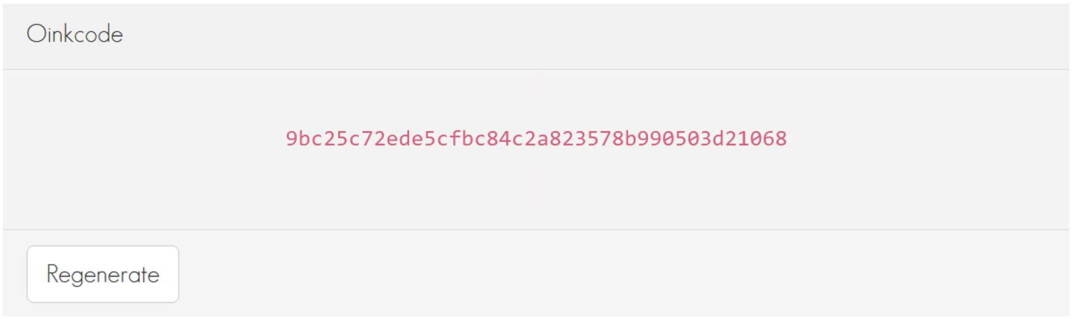
4. IPS/IDS

4.1 Instalação e Configuração do Snort

- Instalamos o pacote Snort acessando a System > Package Manager > Available Packages, pesquisamos por Snort e instalamos.

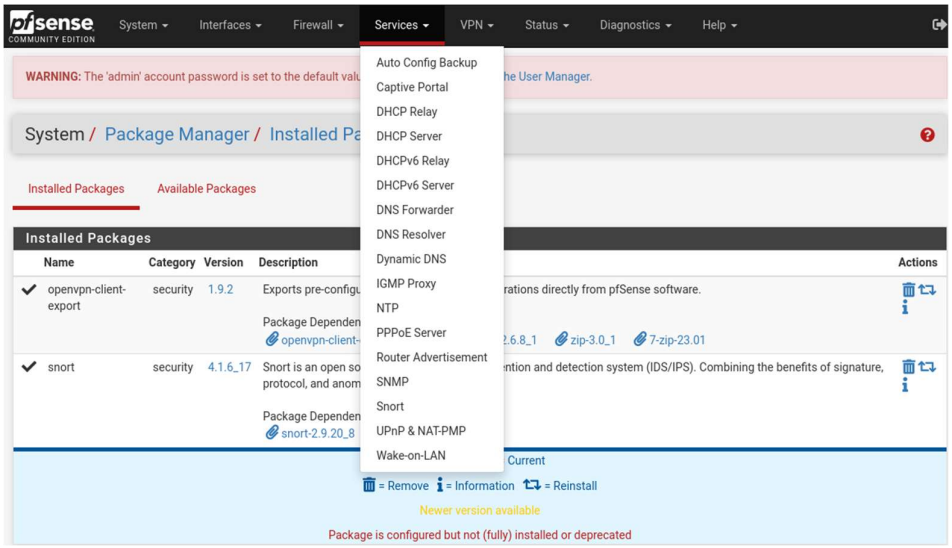


- Criámos uma conta no website do Snort: https://www.snort.org/
  De seguida, em My Account > Oinkcode, guardámos o Oinkcode para posterior uso na pfSense.

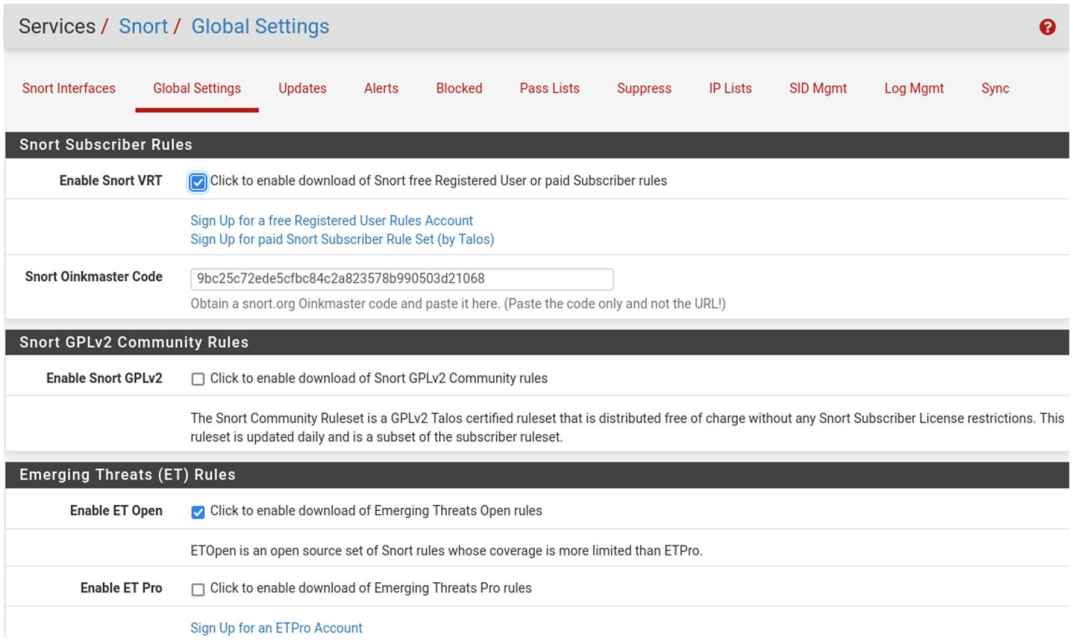


Configuração

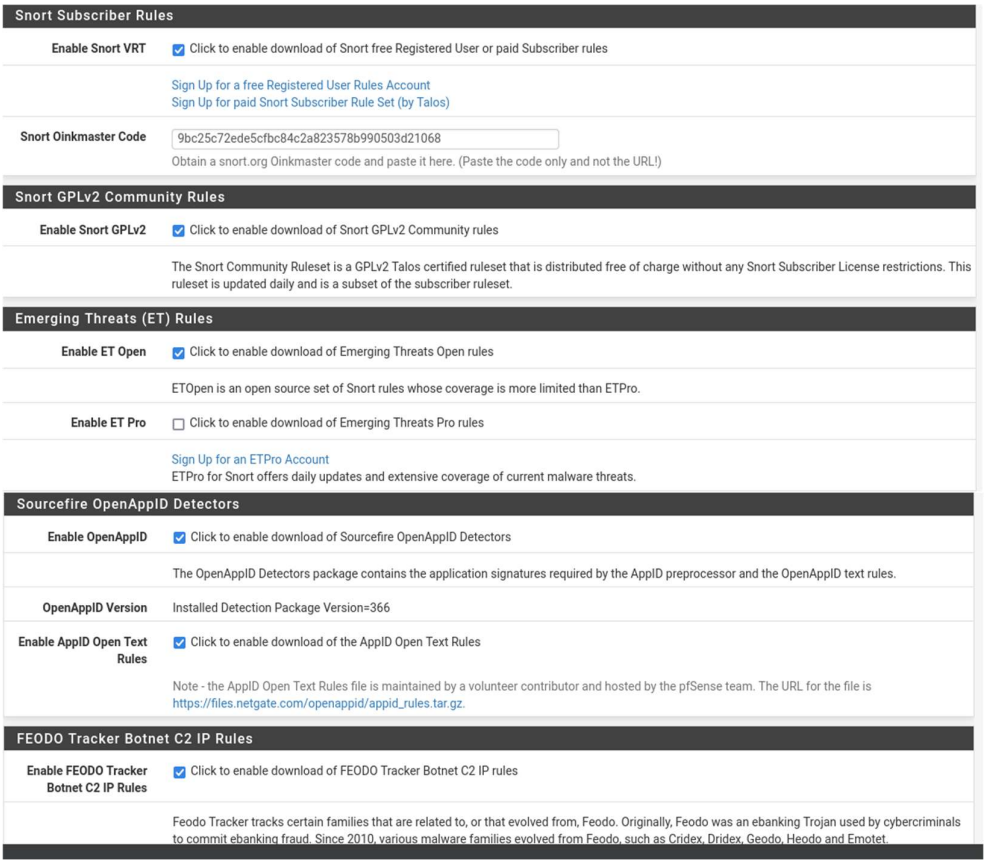
- Na pfSense em Services > Snort > Global Settings



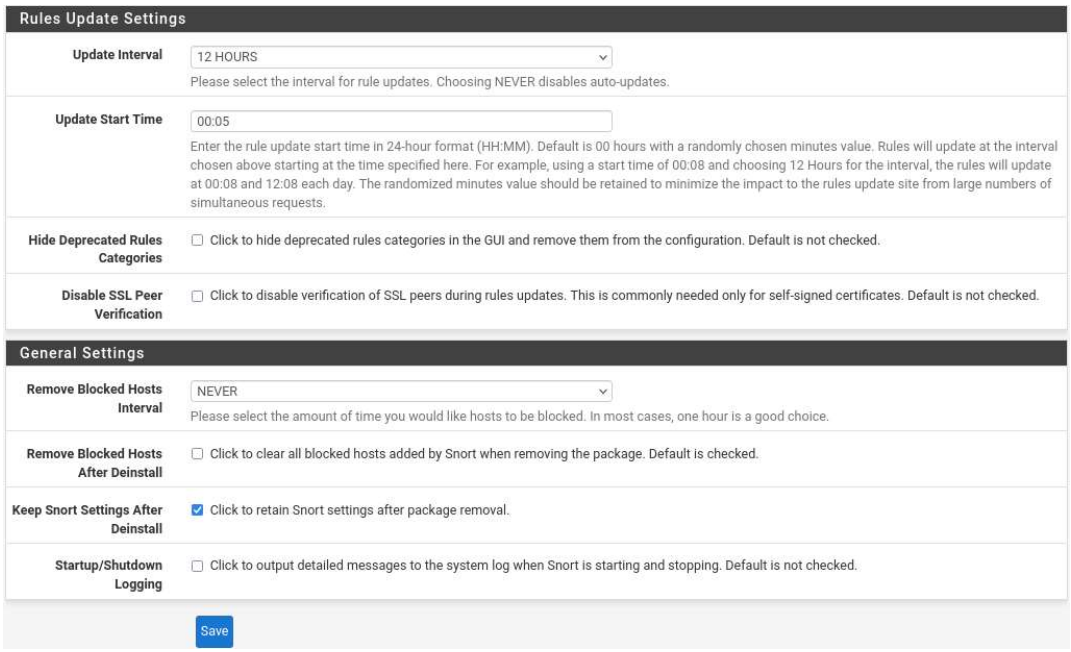
- Ativamos a opção “Enable Snort VRT” e na caixa de texto “Snort Oinkmaster Code” inserimos o código obtido no website do Snort



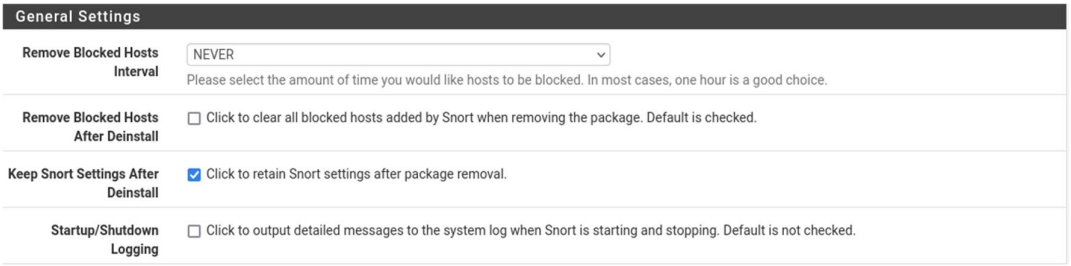
- Ativamos as opções “Enable Snort GPLv2”, “Enable ET Open”, “Enable OpenAppID”, “Enable FEODO Tracker Botnet C2 IP Rules”



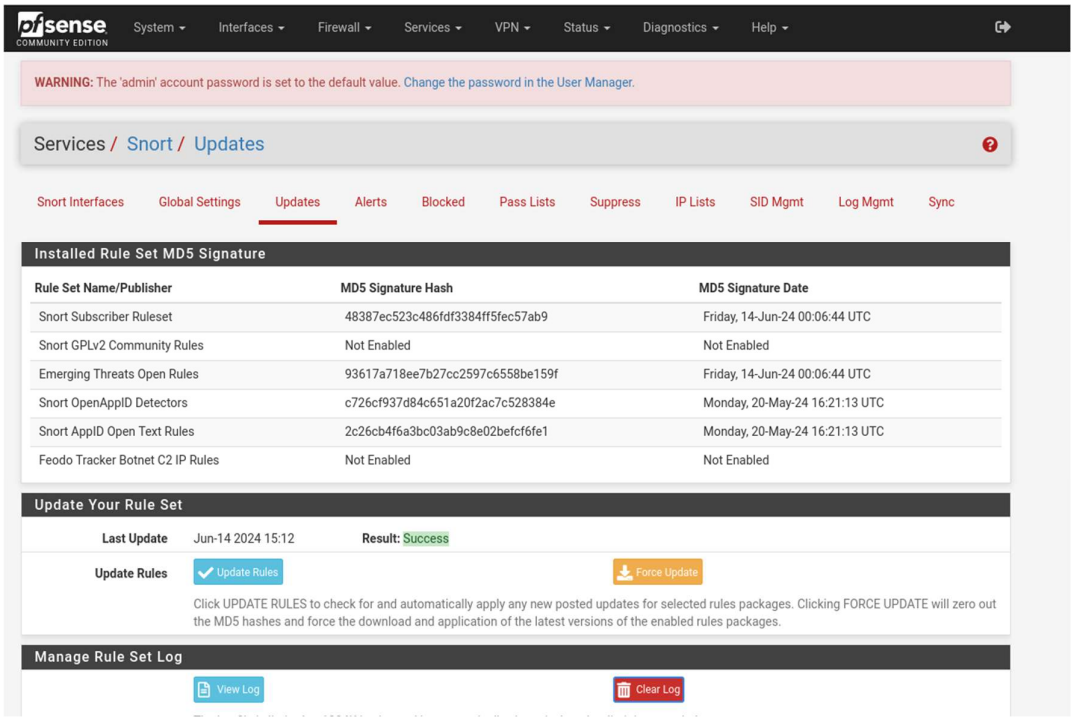
- Alteramos o “Update Interval” para 12 HOURS e deixamos o “Update Start Time” em 00:05



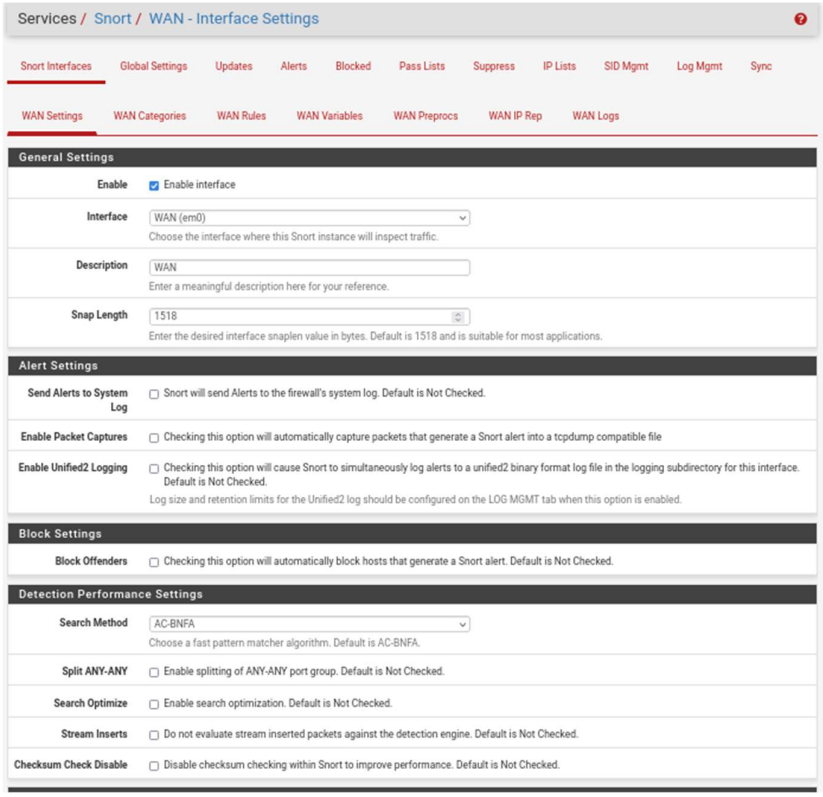
- Também deixamos o “Remove Blocked Hosts Interval” como ”Never”

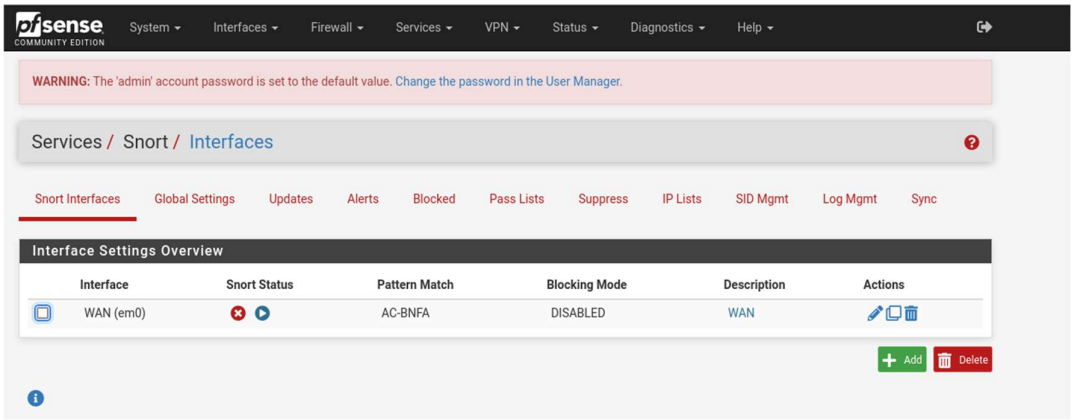


- Acedemos ao separador Updates (Services > Snort > Updates) e atualizamos as regras clicando em Update Rules

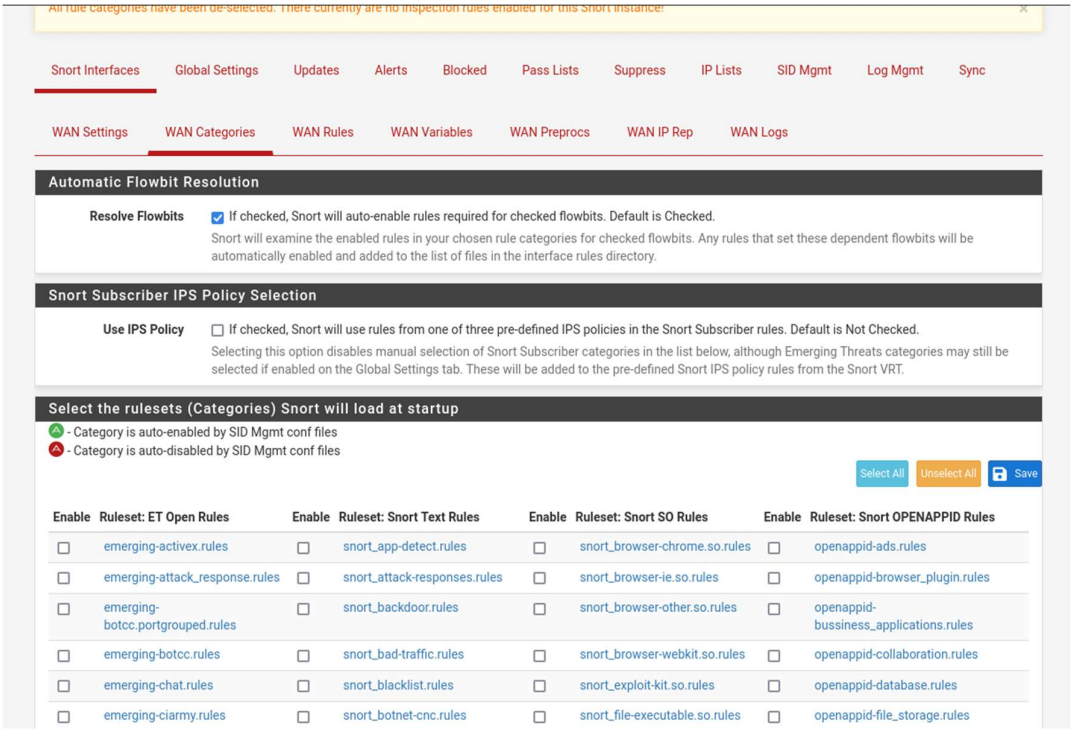


- De seguida no separador Snort Interfaces, adicionamos uma interface e ativámos a opção Enable Interface. Na mesma tela escolhemos a interface WAN e demos uma descrição

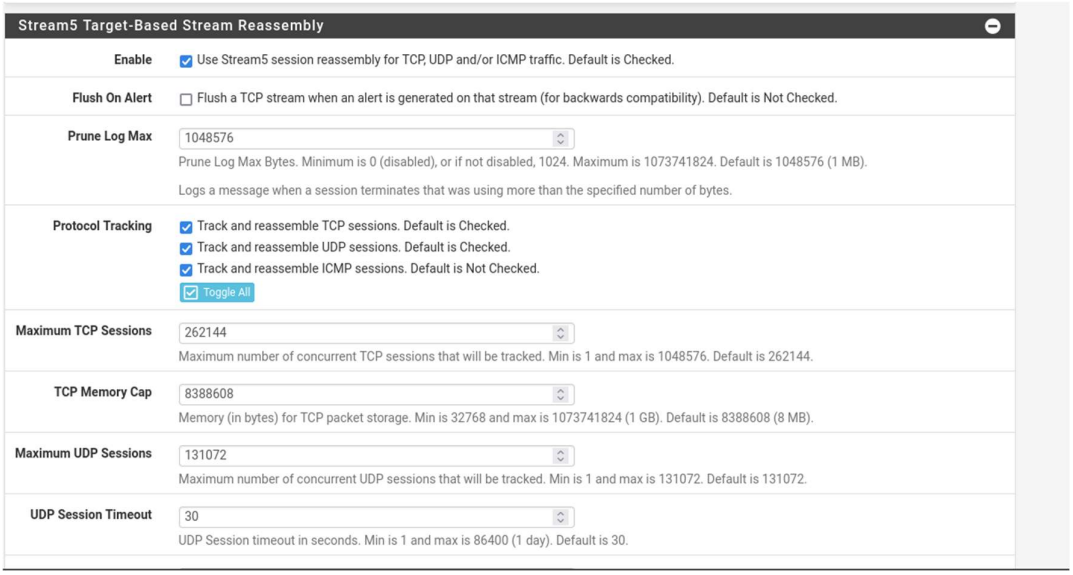




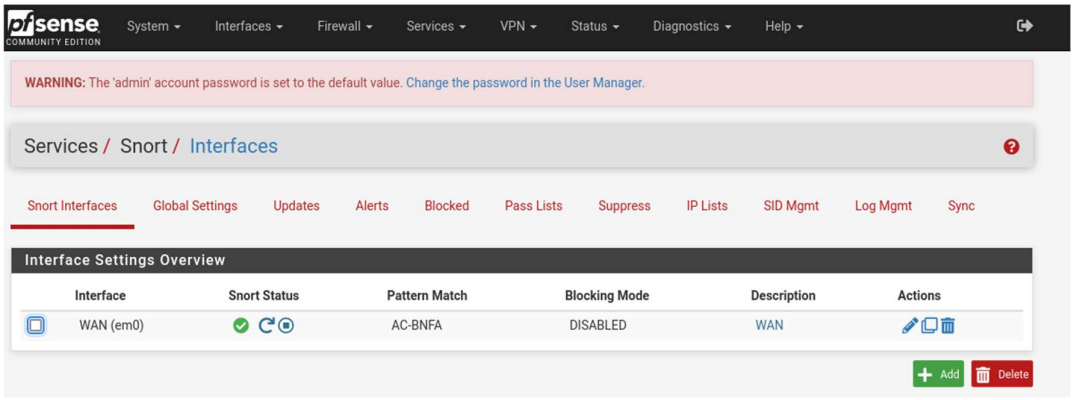
- Com a interface criada, começamos verificando o separador "WAN Categories". Dependendo do que desejamos bloquear, já existem várias categorias com regras predefinidas para vulnerabilidades conhecidas, que podem ser ativadas conforme necessário.



- De seguida no separador “WAN Preprocs” e dentro da secção “Stream5 Target-Based Stream Reassembly”, ativamos a opção “Track and reassemble ICMP sessions”.



- Por fim, demos start na interface WAN do Snort



4.2 Análise de Assinaturas existentes

Assinaturas Snort

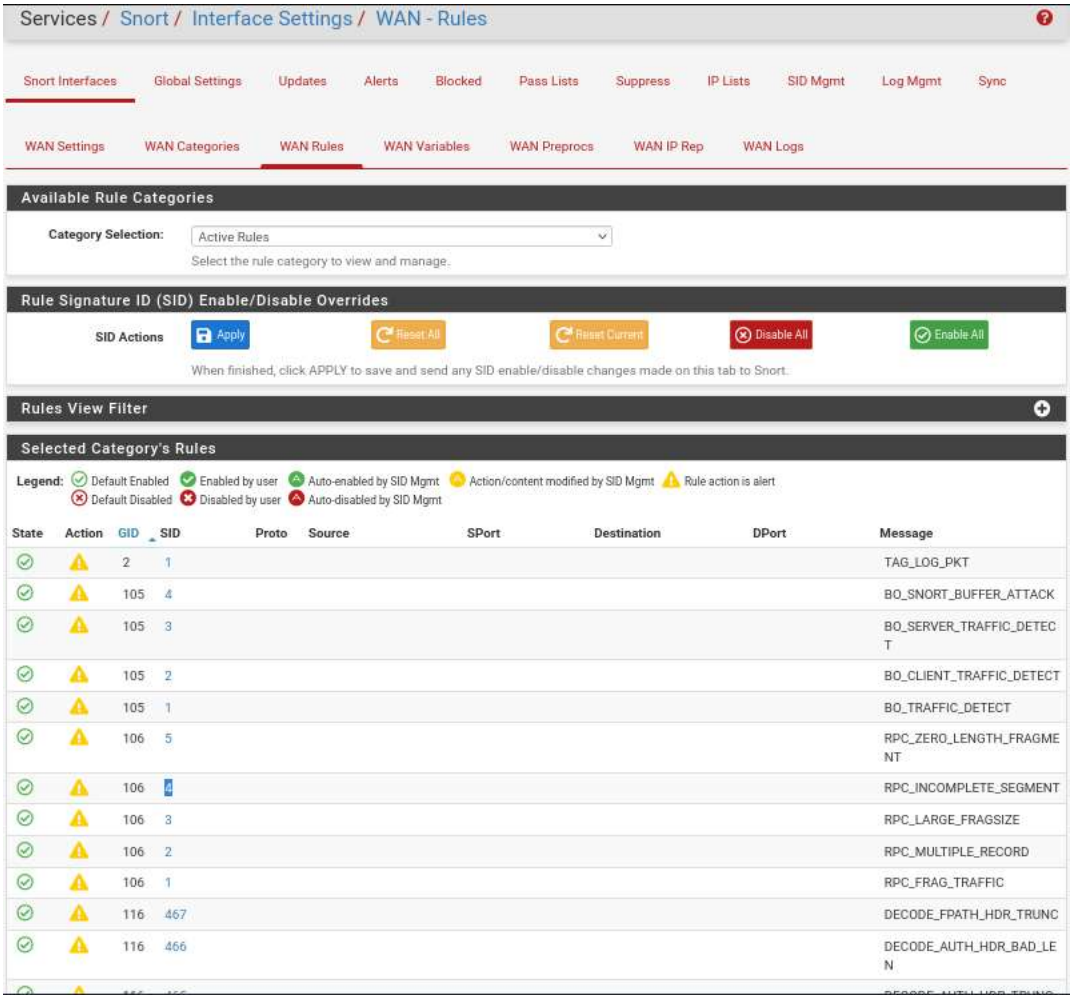
Assinaturas no *Snort* são regras predefinidas, escritas em uma linguagem específica do *Snort*, que identificam padrões de tráfego de rede associados a comportamentos suspeitos ou maliciosos conhecidos permitindo, assim, a deteção de uma vasta gama de atividades indesejadas. Exemplos de atividades passam por ataques de negação de serviço (*DoS*), tentativas de exploração de vulnerabilidades, tráfego gerado por *malware*, e outras anomalias na rede.

Cada assinatura é composta por diversos elementos, incluindo identificadores únicos conhecidos por *SIDs*, descrições, ações a serem tomadas quando a assinatura é acionada, e parâmetros específicos que definem o padrão de tráfego a ser detetado.

Elas são essenciais, permitindo uma resposta rápida a incidentes, monitoração contínua da rede e análise forense de ataques. Elas podem ser personalizadas e atualizadas regularmente, garantindo proteção contra novas ameaças e ajudando a manter a segurança da rede robusta e eficiente.

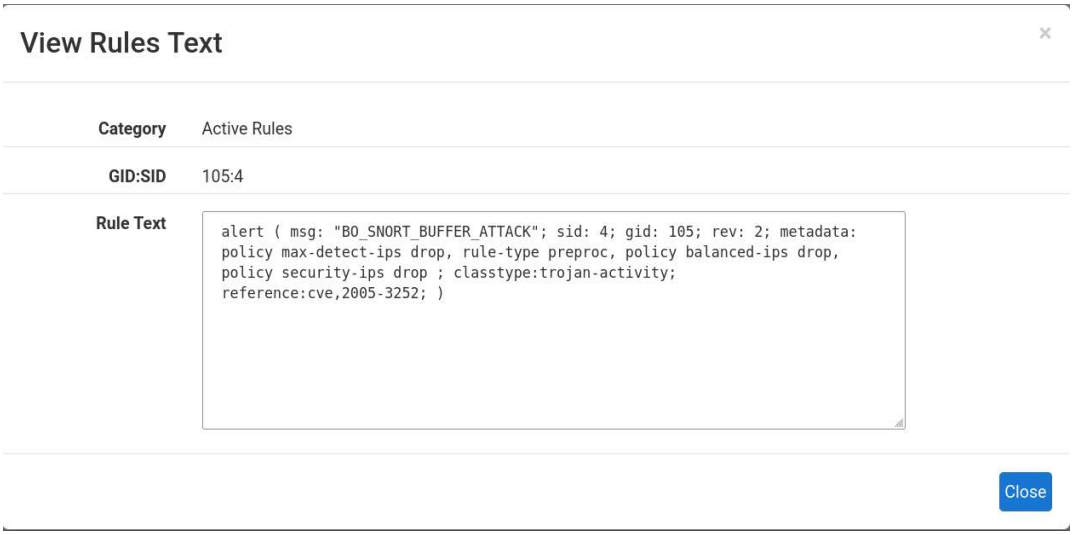
Análises de exemplo

Para “**Active Rules**”:



A regra 116:1 (DECODE_NOT_IPV4_DGRAM) indica a detecção de pacote que não é um datagrama IPv4 válido, importante para identificar tráfego anômalo que pode representar uma tentativa de exploração de vulnerabilidade no protocolo de rede.

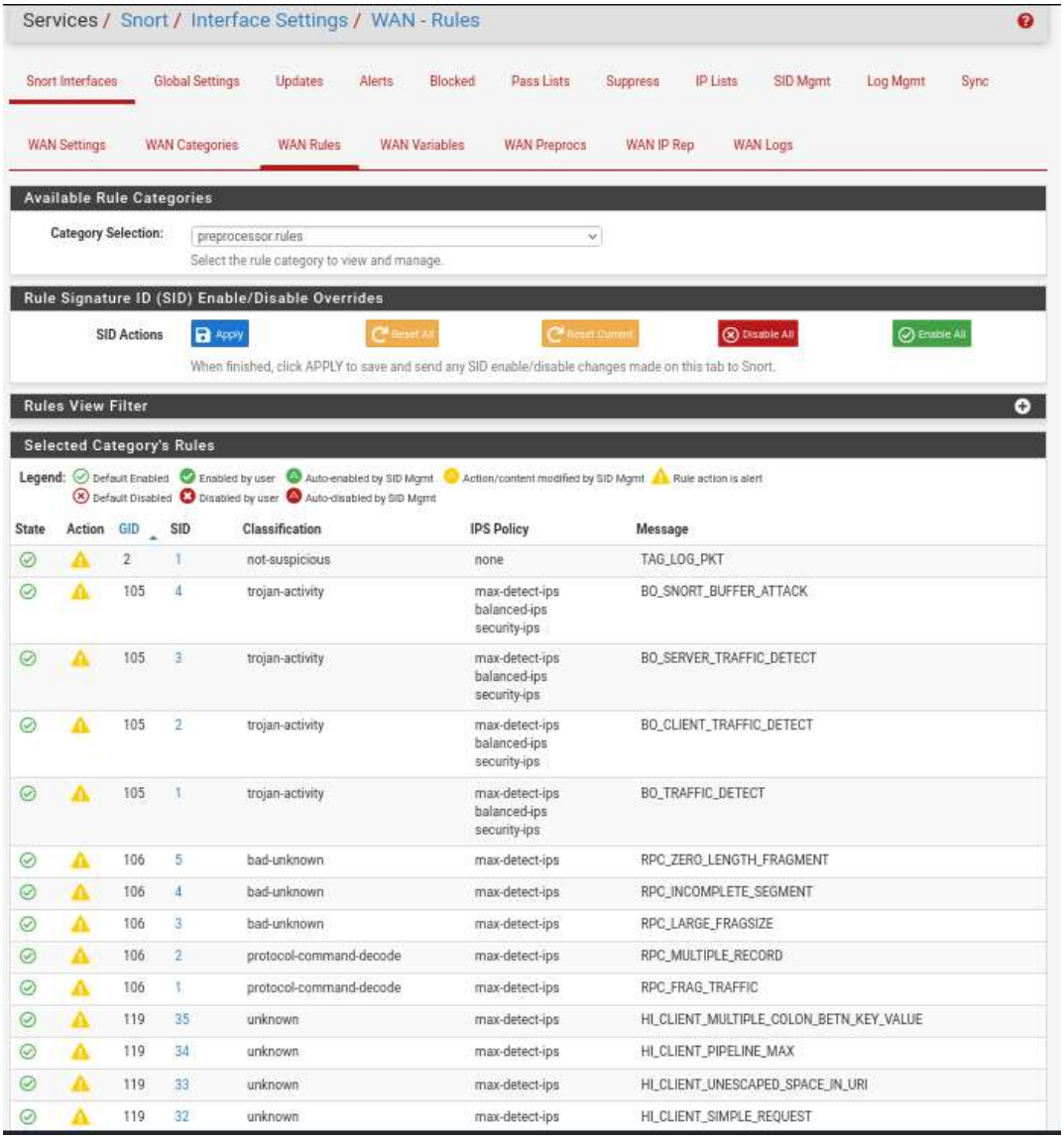
A regra 105:4 (BO_SNORT_BUFFER_ATTACK) deteta tentativas de ataque de *buffer overflow* direcionadas ao *Snort*, uma técnica utilizada para comprometer o sistema através da sobrecarga do *buffer*.



A regra 106:4 (RPC_INCOMPLETE_SEGMENT) monitora segmentos incompletos no protocolo RPC, ajudando a identificar tráfego malformado ou tentativas de ataques fragmentados.

Passando para categorias diferentes, destacaram-se algumas regras da categoria *preprocessor.rules*.

Estas tratam-se de regras específicas que atuam em conjunto com os preprocessadores do Snort que são módulos que processam o tráfego antes que ele seja analisado pelas regras de detecção normais.



Uma regra de exemplo que se destaca é a 105:2 (BO_CLIENT_TRAFFIC_DETECT), que alerta sobre a detecção de tráfego de cliente associado a atividade de trojan, utilizando políticas de detecção IPS que incluem descarte de pacotes para maximizar a segurança. Essa assinatura é crucial para identificar potenciais tentativas de exploração de vulnerabilidades conhecidas oferecendo uma camada adicional de defesa contra ameaças de segurança na rede.

A análise das assinaturas acima nos fornece uma base sólida para os próximos tópicos, nos quais criaremos as nossas próprias regras, tais como alertas e bloqueios de tráfego ICMP do exterior, entre outras medidas de segurança.

4.3 Tráfego ICMP do exterior

Alerta

Na interface WAN no Snort, em WAN Rules, adicionamos a seguinte regra para alertar o tráfego ICMP (Ping) vindo do exterior:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping detected"; sid:1000001;
rev:1; classtype:icmp-event;)
```

Explicação:

```
alert : indica que deve ser gerado um alerta quando a regra corresponder
icmp : protocolo
any any -> $HOME_NET any : ip e portas de origem e destino. $HOME_NET é uma variavel que
existe no pfSense que permite facilitar a definição de endereços da rede local (pfSense)
msg:” ICMP Ping detected” : Mensagem que aparece no alerta
sid:1000001 : (Security ID) é um identificador único da regra para facilicar a identificação
e gestão
rev:1 : Número de versão da regra, ajuda a controlar alterações na regra

 classtype:icmp-event:Classifica o evento como relacionado a ICMP
```

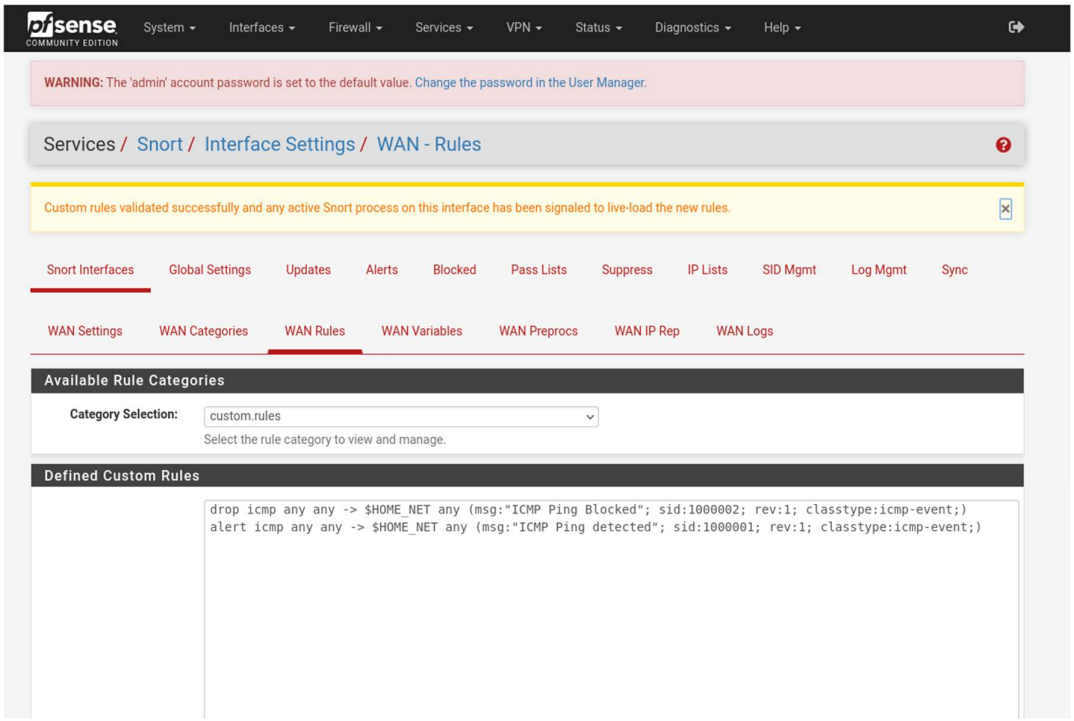
Barramento

Já para o barramento desse tipo de tráfico, adicionamos a seguinte regra:

```
drop icmp any any -> $HOME_NET any (msg:"ICMP Ping Blocked"; sid:1000002;
rev:1; classtype:icmp-event;)
```

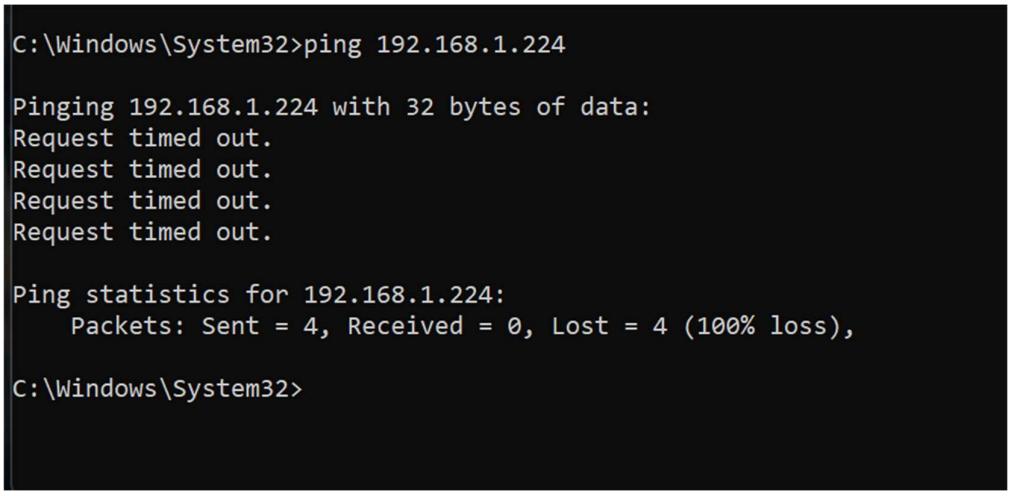
Explicação

```
drop: indica que deve ser feito um drop quando a regra corresponder
icmp : protocolo
any any -> $HOME_NET any : ip e portas de origem e destino. $HOME_NET é uma variavel que
existe no pfSense que permite facilitar a definição de endereços da rede local (pfSense)
msg:” ICMP Ping Blocked” : Mensagem que aparece no drop
sid:1000002 : (Security ID) é um identificador único da regra para facilicar a identificação
e gestão
rev:1 : Número de versão da regra, ajuda a controlar alterações na regra
classtype:icmp-event:Classifica o evento como relacionado a ICMP
```

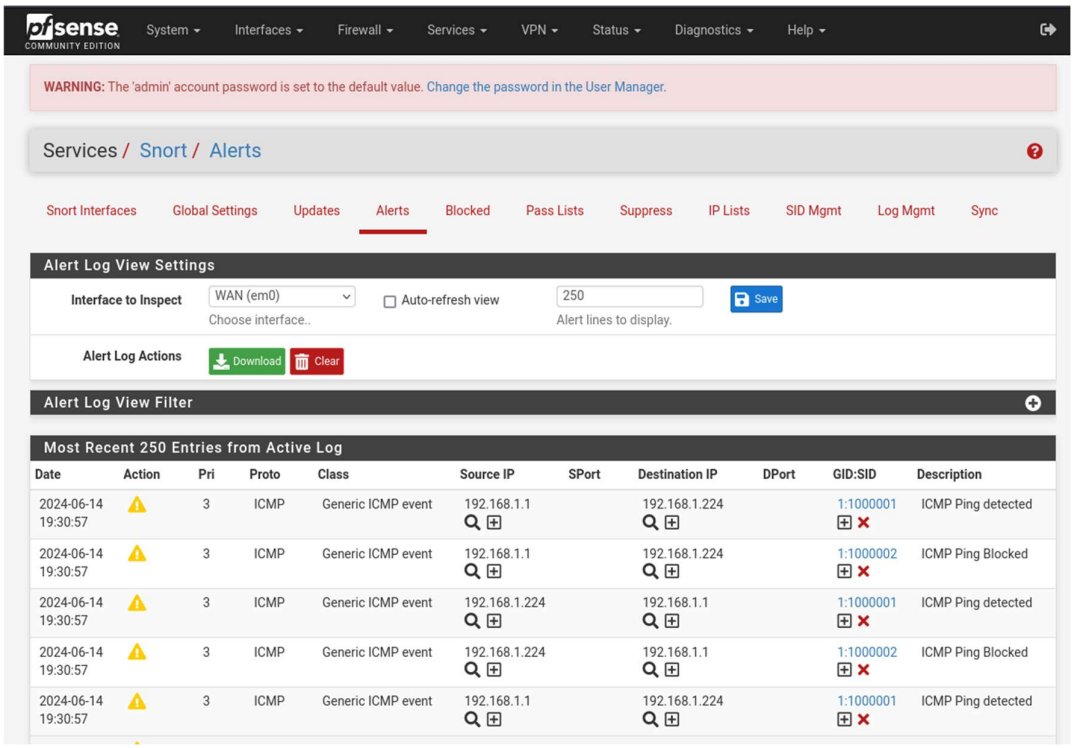


Verificação

Podemos simplesmente executar uma ferramenta de ping a partir de um dispositivo externo para demonstrar o funcionamento da regra. No nosso caso, utilizaremos o nosso próprio host para fazer ping para o endereço ip da interface WAN do Pfsense:



Podemos verificar o funcionamento das regras implementadas em Services > Snort > Alerts:



4.4 Alerta para páginas com referência a “Adult”

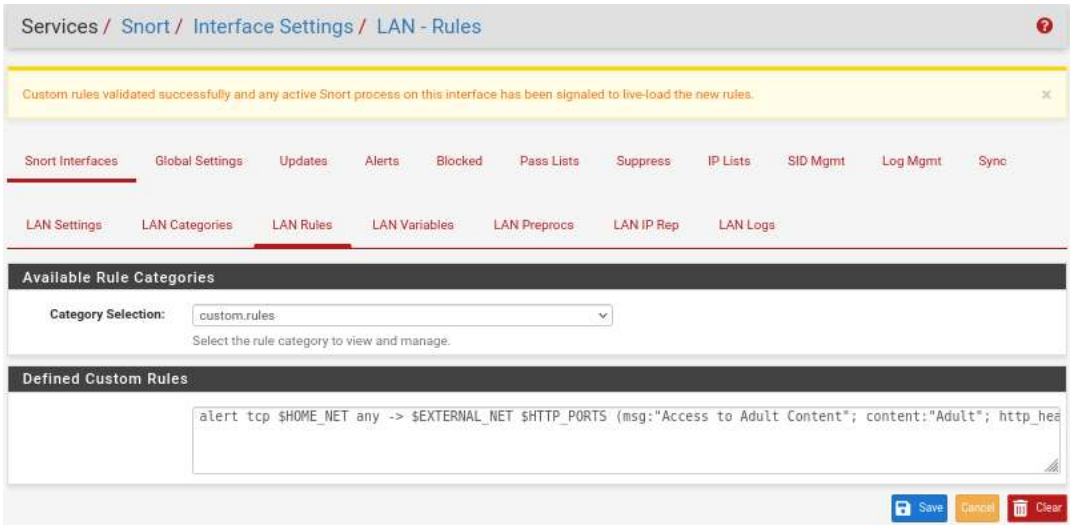
Para configurar alertas de acesso a páginas com referência a conteúdo adulto, originado de qualquer máquina da rede interna, seguímos os seguintes passos:

Na interface snort para a LAN, acessamos ao separador “LAN Rules”, e na categoria “custom.rules” adicionámos o seguinte código:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Access to Adult Content"; content:"Adult"; http_header; nocase; sid:1000003; rev:1;)
```

Explicação

```
alert tcp: Especifica que a regra é para tráfego TCP.
$HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS: Define que o tráfego de qualquer porta na rede interna ($HOME_NET) para qualquer porta HTTP no exterior ($EXTERNAL_NET) deve ser analisado.
msg:"Access to Adult Content": Mensagem que será registrada quando a regra for acionada.
content:"Adult": Padrão de conteúdo que a regra está procurando. Pode ser modificado para detectar outras palavras-chave conforme necessário.
http_header: Define que a busca deve ser feita no cabeçalho HTTP.
nocase: Ignora a distinção entre maiúsculas e minúsculas ao procurar o padrão.
sid:1000001: Identificador único da assinatura.
rev:1: Versão da regra.
```


Services / Snort / Interface Settings / LAN - Rules
Custom rules validated successfully and any active Snort process on this interface has been signaled to live-load the new rules.
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
LAN Settings
LAN Categories
LAN Rules
LAN Variables
LAN Preprocs
LAN IP Rep
LAN Logs
Available Rule Categories
Category Selection:
custom.rules
Select the rule category to view and manage.
Defined Custom Rules
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Access to Adult Content"; content:"Adult"; http_hea
Save
Cancel
Clear

5. Conclusão

A conclusão do trabalho mostrou que a configuração e uso do pfSense junto com o Snort resultaram em um ambiente seguro e monitorado, capaz de detectar e prevenir diversos tipos de ataques cibernéticos.

Os principais pontos são:

Efetividade do pfSense e Snort: As ferramentas foram eficazes na proteção da rede interna contra acessos não autorizados e tráfego malicioso.

Monitoramento e Detecção Contínuos: A configuração permitiu detectar rapidamente incidentes e responder eficazmente a ameaças.

Propostas de Melhoria: Foram feitas recomendações para melhorar a segurança dos protocolos utilizados, sugerindo a migração para versões mais seguras como SSH, SFTP, HTTPS e SMTPS.

Importância da Atualização: A segurança das redes exige atualização contínua das assinaturas e políticas de segurança para se proteger contra novas ameaças.

Este trabalho destacou a importância de uma abordagem proativa para a segurança de redes, usando ferramentas robustas e atualizadas para garantir proteção contra o crescente número de ameaças cibernéticas.

Referências

https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html

https://blog.infnet.com.br/engenharia_de_redes/snort-o-que-e/

https://www.fortinet.com/br/resources/cyberglossary/snort

https://dev.to/sankethj/detect-dos-ping-etc-using-snort-4gab