P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

Licenciatura em Segurança Informática e Redes de Computadores

Segurança de Redes

Trabalho prático 2

Gonçalo Ferraz – 8220202

Tânia Morais – 8220190

Índice

Introdução

O segundo trabalho prático da unidade curricular, Segurança de Redes, tem como objetivo familiarizar o uso e a configuração de uma firewall.

Para este trabalho prático, utilizou-se duas máquinas virtuais, previamente instaladas no software de virtualização *Virtual Box*, sendo elas o *Kali* e o *Pfsense*.

Este trabalho é devido essencialmente por seis etapas, tais como:

1. Arquitetura da implementação
2. Implementação das políticas de firewall
3. Demonstração do funcionamento das políticas de firewall
4. Identificação de protocolos inseguros
5. Instalação do *snort*
6. IPS/IDS

1. Arquitetura de implementação

Nesta etapa, começou-se por fazer um desenho elucidativo de como iria decorrer a implementação.

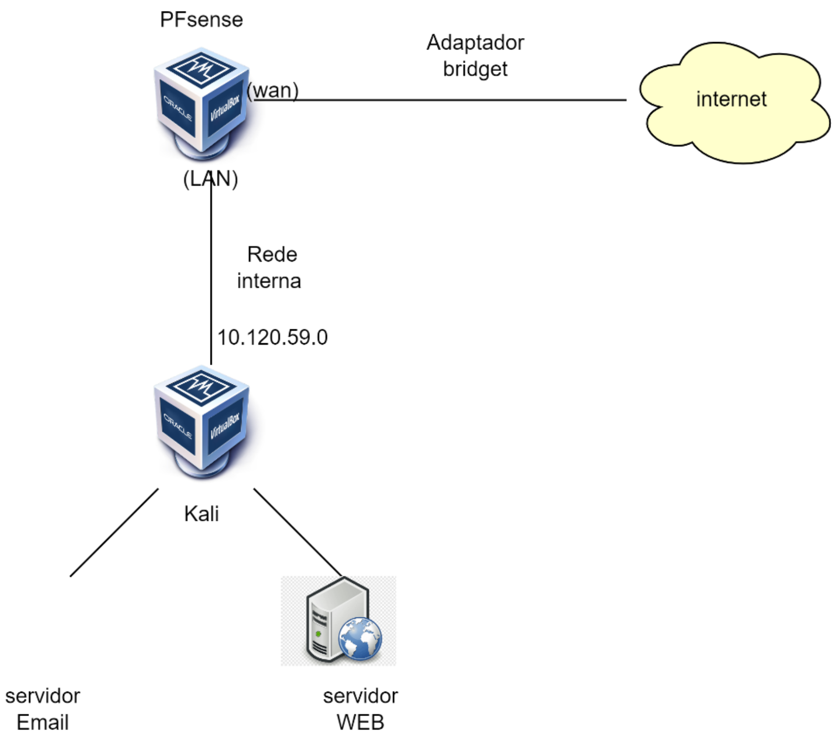
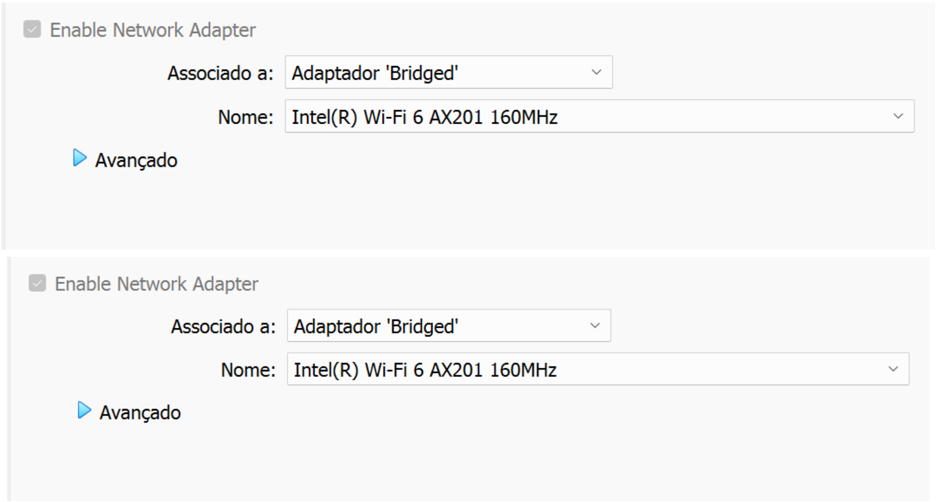


Figura 1- Arquitetura de implementação

Na figura 1, é possível perceber o recurso a duas máquinas virtuais, *Kali* e *Pfsense*, ambas interligas pela rede interna. Num dos casos, o *gateway* é o *Kali* no outro caso é o *Pfsense*. Nas imagens abaixo, são ilustradas as conexões de rede tanto no *Kali* como no *Pfsense*.



☑ Enable Network Adapter

Associado a: Adaptador 'Bridged'

Nome: Intel(R) Wi-Fi 6 AX201 160MHz

▷ Avançado

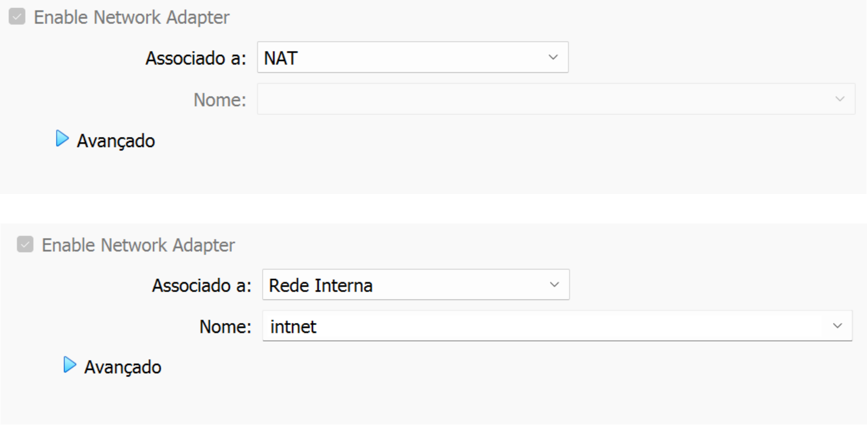
☑ Enable Network Adapter

Associado a: Adaptador 'Bridged'

Nome: Intel(R) Wi-Fi 6 AX201 160MHz

▷ Avançado

Figura 2- Conexões de rede referentes ao Kali



☑ Enable Network Adapter

Associado a: NAT

Nome:

▷ Avançado

☑ Enable Network Adapter

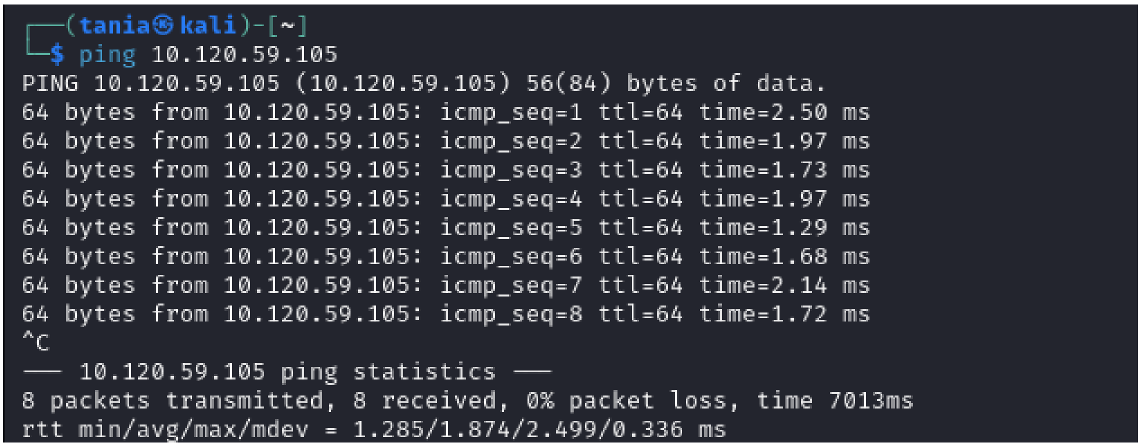
Associado a: Rede Interna

Nome: intnet

▷ Avançado

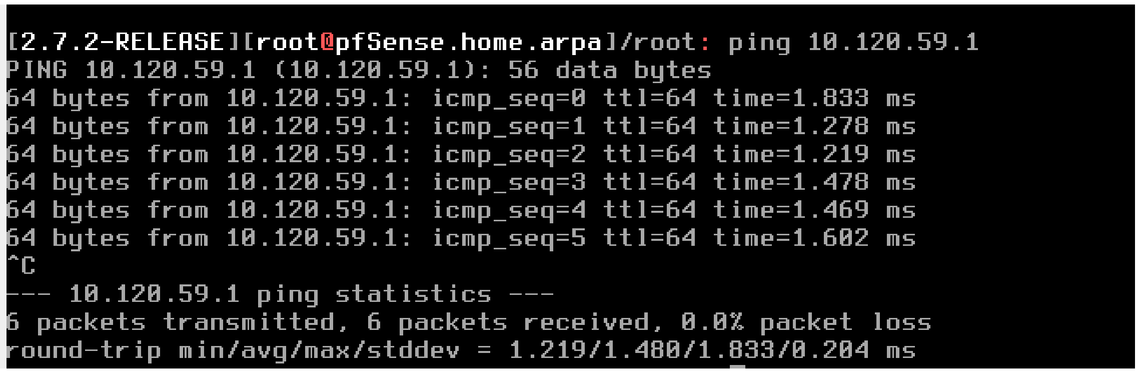
Figura 3- Conexões de rede referentes ao Pfsense

Por fim, testou -se a conectividade entre as máquinas:



```
┌──(tania㉿kali)-[~]
└─$ ping 10.120.59.105
PING 10.120.59.105 (10.120.59.105) 56(84) bytes of data.
64 bytes from 10.120.59.105: icmp_seq=1 ttl=64 time=2.50 ms
64 bytes from 10.120.59.105: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 10.120.59.105: icmp_seq=3 ttl=64 time=1.73 ms
64 bytes from 10.120.59.105: icmp_seq=4 ttl=64 time=1.97 ms
64 bytes from 10.120.59.105: icmp_seq=5 ttl=64 time=1.29 ms
64 bytes from 10.120.59.105: icmp_seq=6 ttl=64 time=1.68 ms
64 bytes from 10.120.59.105: icmp_seq=7 ttl=64 time=2.14 ms
64 bytes from 10.120.59.105: icmp_seq=8 ttl=64 time=1.72 ms
^C
--- 10.120.59.105 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7013ms
rtt min/avg/max/mdev = 1.285/1.874/2.499/0.336 ms
```

Figura 4- Ping kali – Pfsense

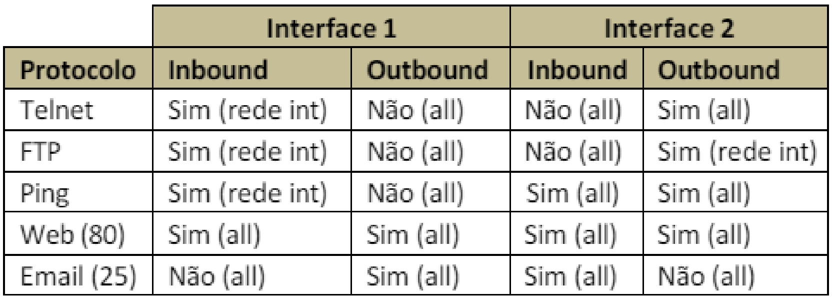


```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping 10.120.59.1
PING 10.120.59.1 (10.120.59.1): 56 data bytes
64 bytes from 10.120.59.1: icmp_seq=0 ttl=64 time=1.833 ms
64 bytes from 10.120.59.1: icmp_seq=1 ttl=64 time=1.278 ms
64 bytes from 10.120.59.1: icmp_seq=2 ttl=64 time=1.219 ms
64 bytes from 10.120.59.1: icmp_seq=3 ttl=64 time=1.478 ms
64 bytes from 10.120.59.1: icmp_seq=4 ttl=64 time=1.469 ms
64 bytes from 10.120.59.1: icmp_seq=5 ttl=64 time=1.602 ms
^C
--- 10.120.59.1 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.219/1.480/1.833/0.204 ms
```

Figura 5 - Ping Pfsense – Kali

1. Implementação das políticas da firewall

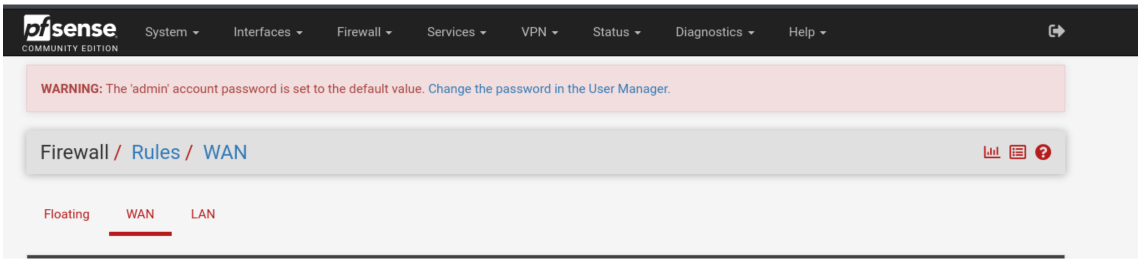
Nesta etapa, definiu-se as políticas de firewall como ilustradas na tabela inicial do *Case Study,* como está abaixo representada:



	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)

Figura 6 - Tabela fornecida para implementação de regras na firewall

Para tal começou-se por aceder página web do *Pfsense* através do ip da *LAN*, e após isso acedeu-se à *Firewall – Rules.*



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Figura 7 - Interface do Pfsense

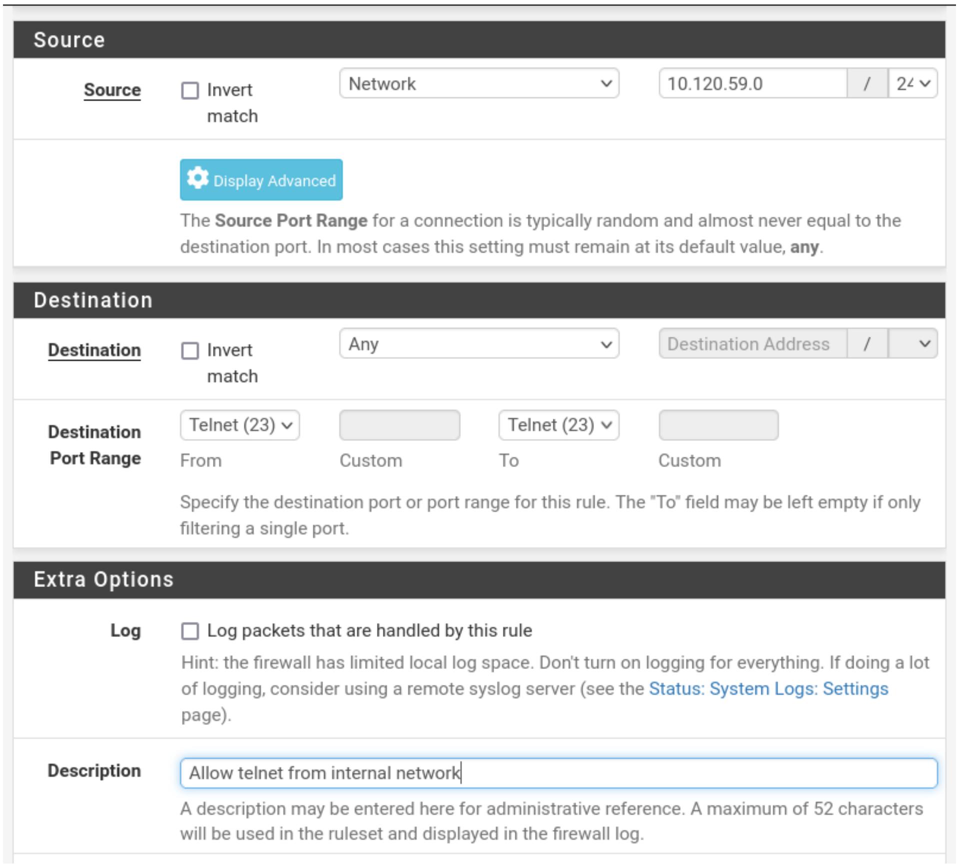
Interface LAN

- ***Telnet***

O **Telnet** é um protocolo de rede normalmente usado para agilizar o conserto de falhas em computadores.

Para o protocolo *telnet,* é permitido o tráfego especificado, utilizando um outro protocolo, TCP, pode partir de qualquer ip que se encontre dentro da rede especificada, 10.12.59.0/24, para qualquer destino, como especificado nas figuras abaixo, se for inbound, no caso de outbound o tráfego é bloqueado desde a o início até ao destino.

Inbound:



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 | 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

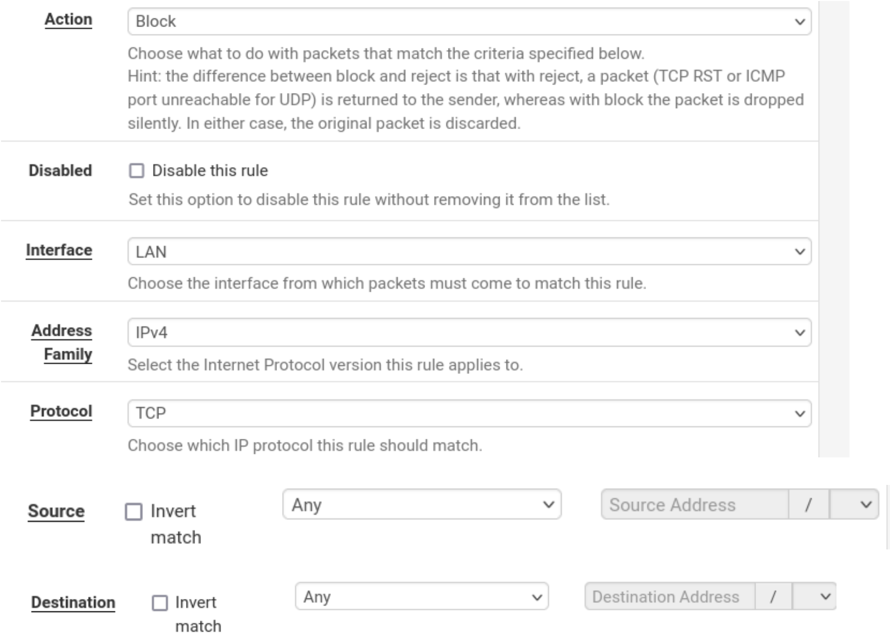
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description | Allow telnet 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.

Figura 8 - Definição de regra para o protocolo telnet

Outbound:



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 □ Invert match | Any | Source Address /

Destination □ Invert match | Any | Destination Address /

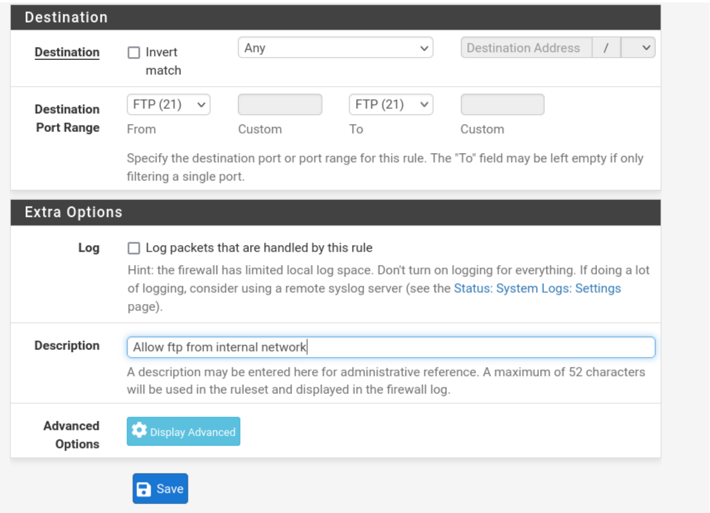
Figura 9 - Definição de regra para o protocolo telnet

- ***Serviço ftp***

O **FTP** é um serviço eficiente, protocolo de transferência de arquivos entre computadores em redes locais ou na internet.

Para o serviço ftp, as regras iniciais são muito semelhantes às regras descritas para o protocolo telnet, a única alteração é a porta de destino.

Inbound:



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: Allow ftp from internal network

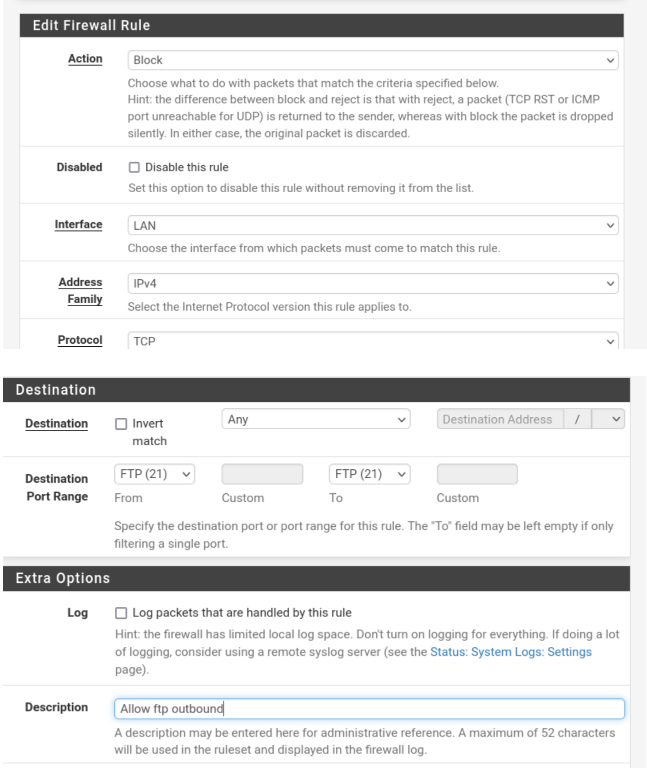
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

Save

Figura 10 - Regras de firewall para o serviço ftp

Outbound:



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

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: Allow 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.

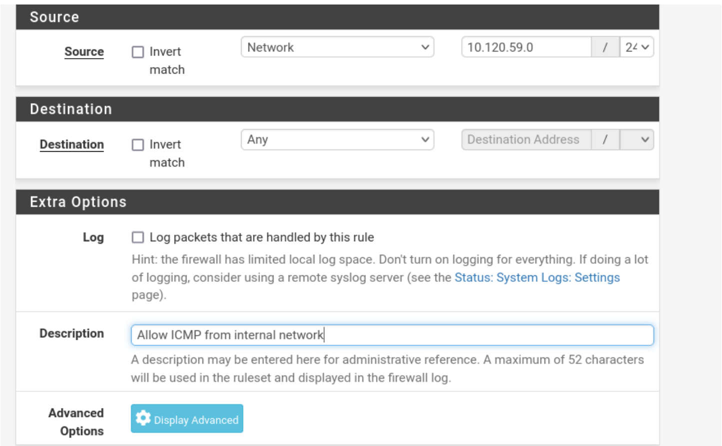
Figura 11 - Regra de firewall para o serviço ftp

- ICMP

O ICMP é um protocolo de camada de rede que permite a comunicação entre dispositivos em uma rede IP.

Este protocolo também permite o tráfego especificado, no entanto, o protocolo usado é o ICMP, uma vez que, o *Ping* usa esse mesmo protocolo. Pode ser executado através de uma rede com um determinado endereço com destino a qualquer endereço ip.

Inbound:



Source

Source □ Invert match | Network | 10.120.59.0 / 24

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).

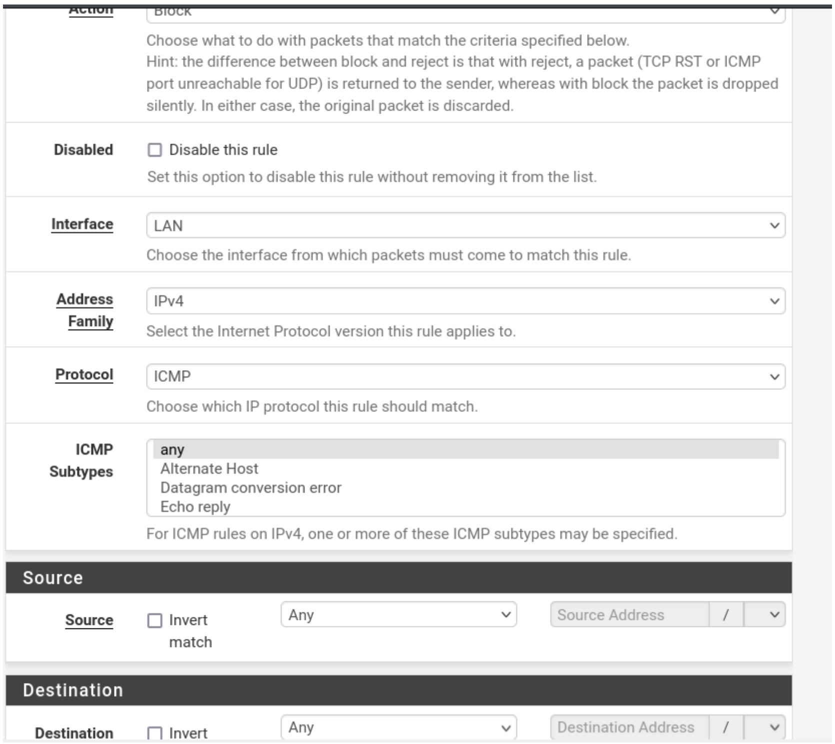
Description: Allow ICMP from internal network

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

Figura 12 - Regra de firewall para o protocolo ICMP

Outbound:



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: ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes: any, Alternate Host, Datagram conversion error, Echo reply

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

Source

Source □ Invert match | Any | Source Address /

Destination

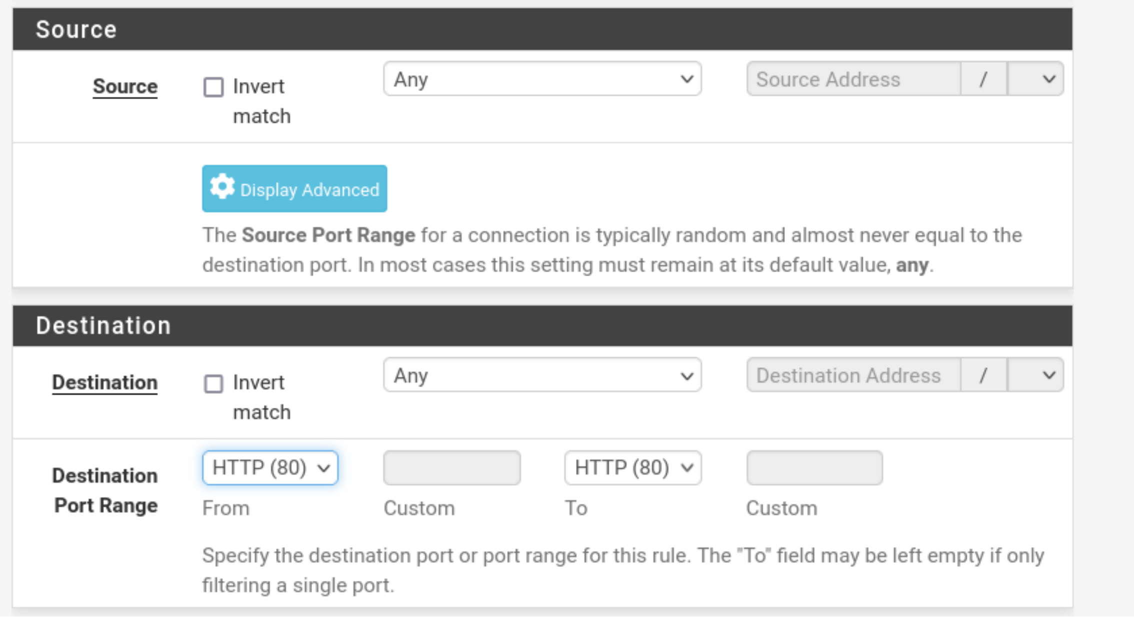
Destination □ Invert | Any | Destination Address /

Figura 13 - Regra de firewall para o protocolo ICMP

- WEB

O protocolo *HTTP* é um **protocolo** de transferência que possibilita que as pessoas que inserem a URL do seu site na Web possam ver os conteúdos e dados

Inbound:



Source

Source ☐ Invert match — Any — Source Address /

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

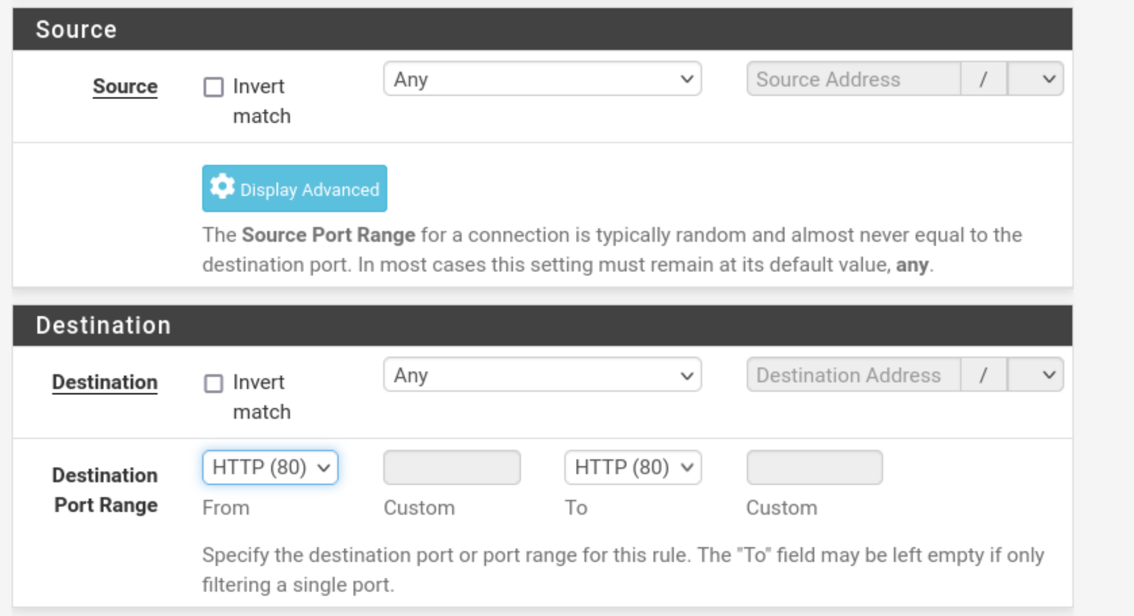
Destination ☐ Invert match — Any — Destination Address /

Destination Port Range — From: HTTP (80) — Custom: — To: HTTP (80) — Custom:

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

Figura 14 - Regras da firewall para protocolo HTTP

Outbound:



Source

Source ☐ Invert match — Any — Source Address /

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 — From: HTTP (80) — Custom: — To: HTTP (80) — Custom:

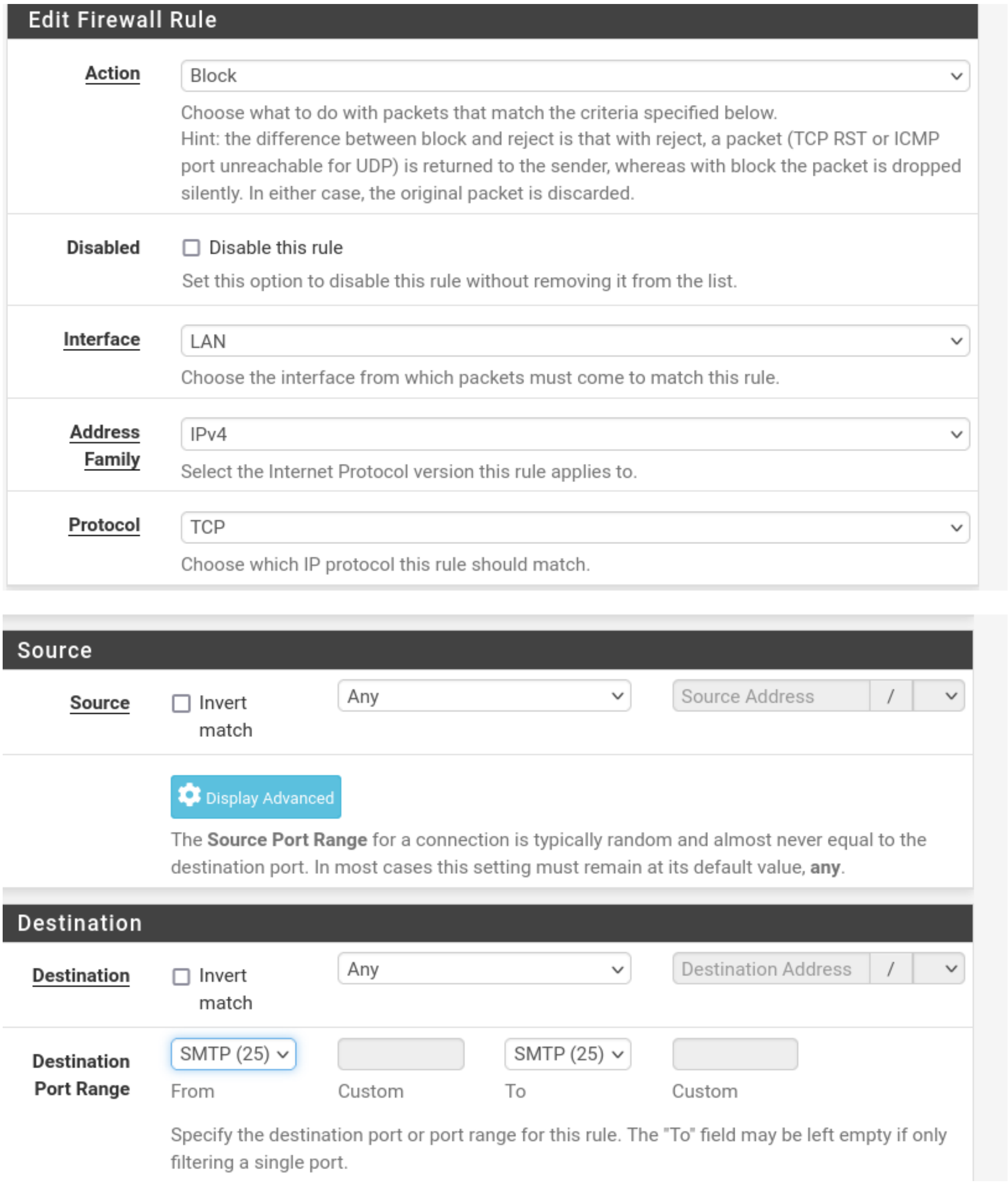
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Figura 15 - Regras da firewall para protocolo HTTP

- Email

O protocolo *SMTP* é o protocolo de transferência de email simples, que define a padronização das informações que identificam cada email e o caminho que ele deve percorrer para ser entregue de forma íntegra, sigilosa e segura

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: 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 /

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

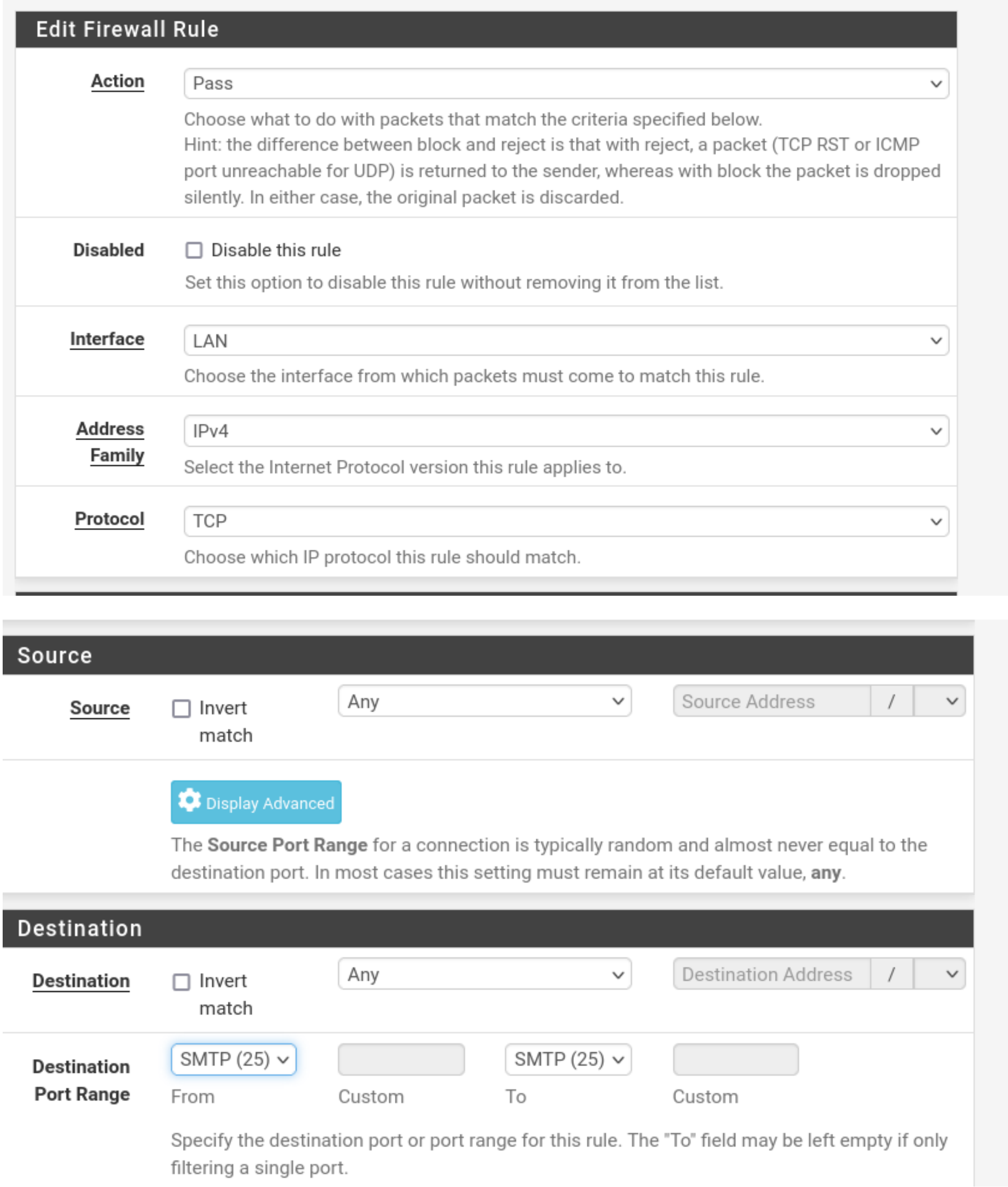
Destination: □ Invert match | Any | Destination Address /

Destination Port Range: From: SMTP (25) | Custom: | To: SMTP (25) | Custom:

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

Figura 16 - Regras para firewall para o protocolo Email

Outbound:



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 | Any | Source Address /

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

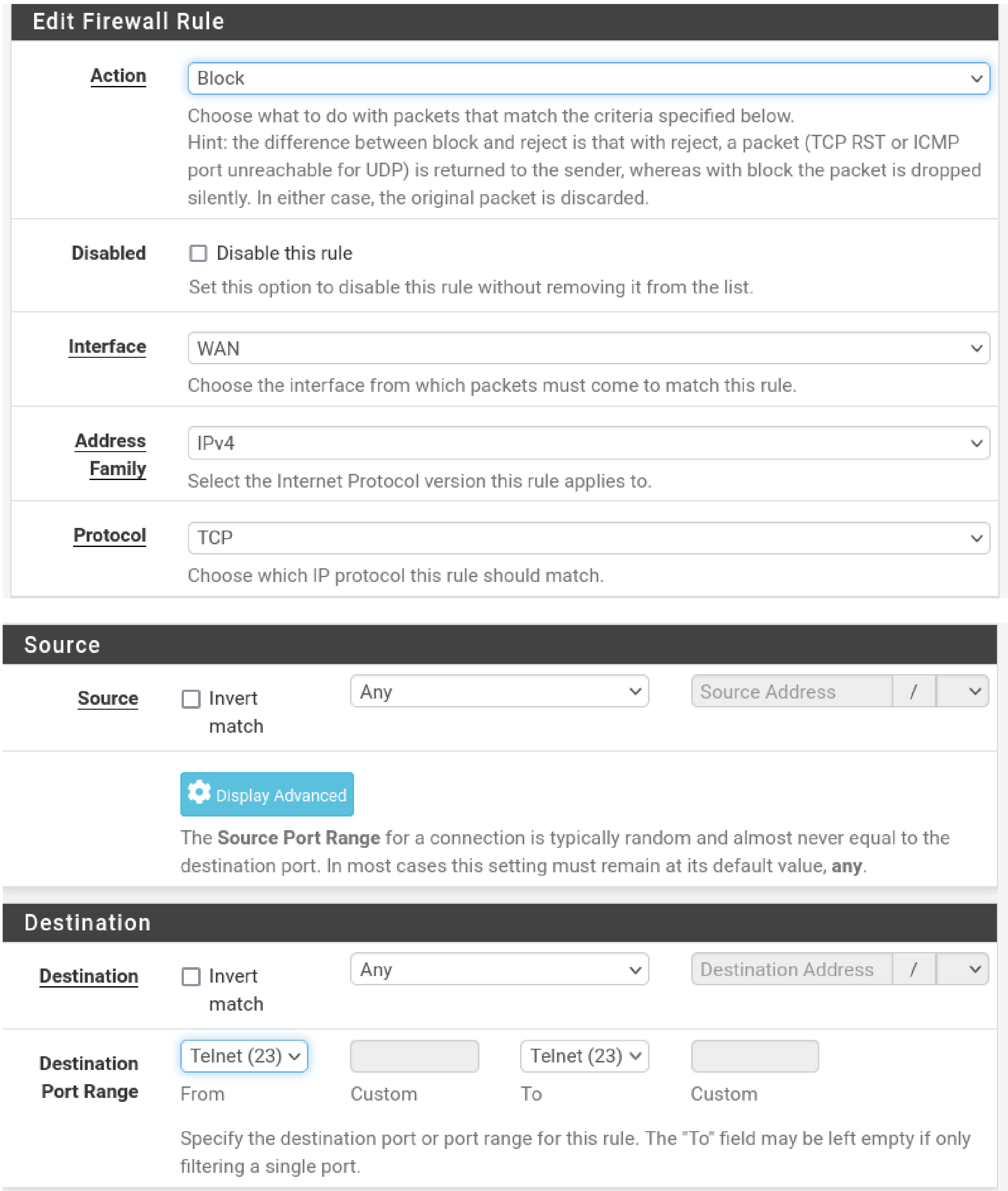
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Figura 17 - Regras para firewall para o protocolo Email

Interface WAN

- Protocolo telnet

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

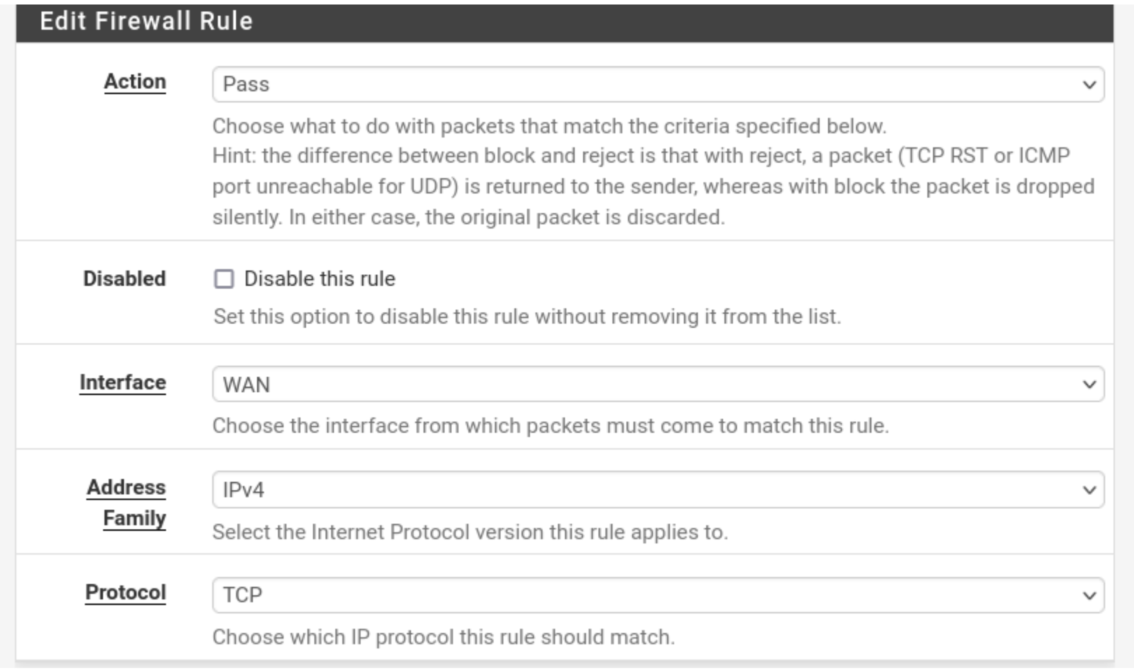
Destination: □ Invert match | Any | Destination Address /

Destination Port Range: From: Telnet (23) | Custom: | To: Telnet (23) | Custom:

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

Figura 18 - Regra de firewall protocolo telnet

Outbound:



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

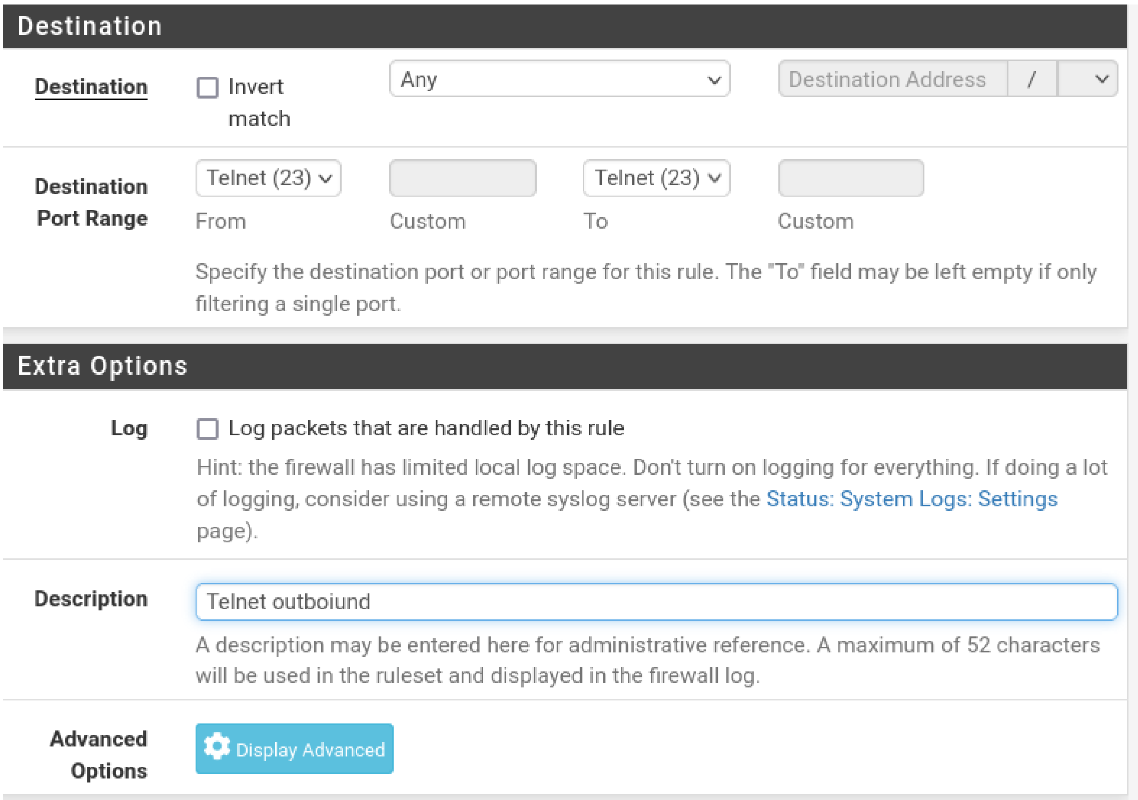
Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.



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).

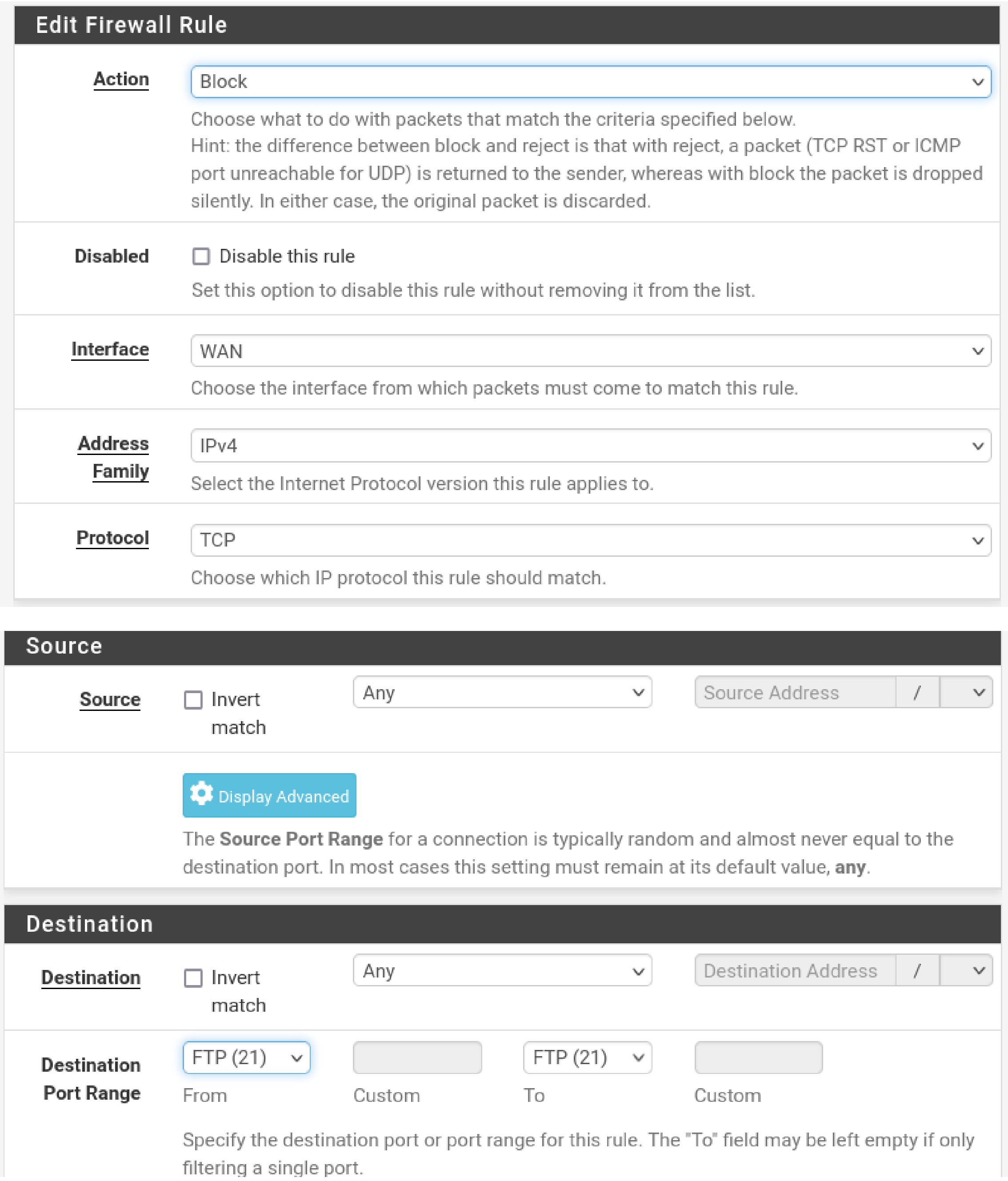
Description: Telnet outboiund

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

- Protocolo 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

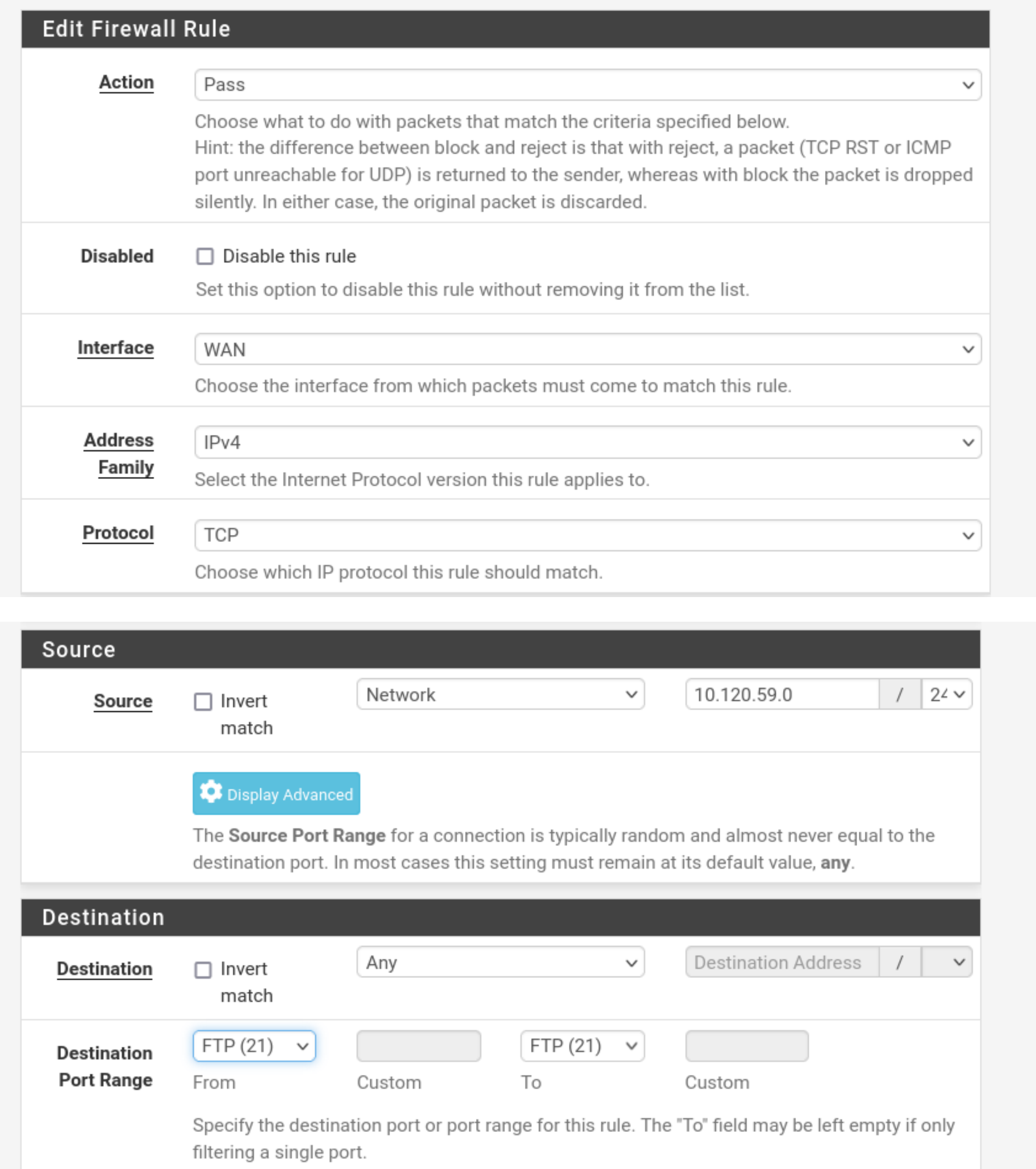
Destination: □ Invert match | Any | Destination Address /

Destination Port Range: From: FTP (21) | Custom: | To: FTP (21) | Custom:

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

Figura 13 - Regras de firewall do protocolo FTP

Outbound:



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 | Network | 10.120.59.0 / 24

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 /

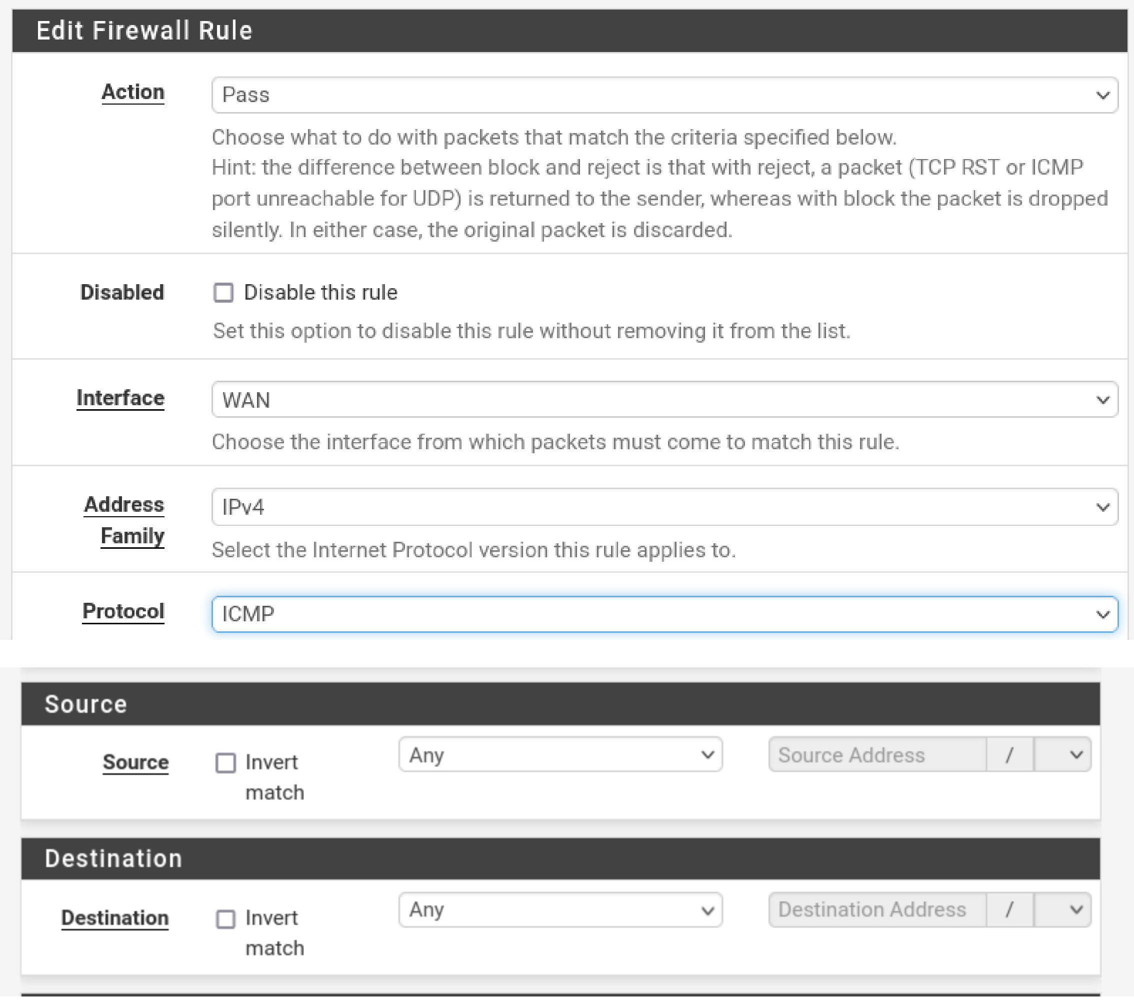
Destination Port Range: FTP (21) From | Custom | FTP (21) To | Custom

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

Figura 14 - Regras de firewall protocolo Ftp

- Protocolo ICMP

Inbound:



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

Source

Source: □ Invert match | Any | Source Address /

Destination

Destination: □ Invert match | Any | Destination Address /

Figura 15 - Regras de firewall procotolo ICMP

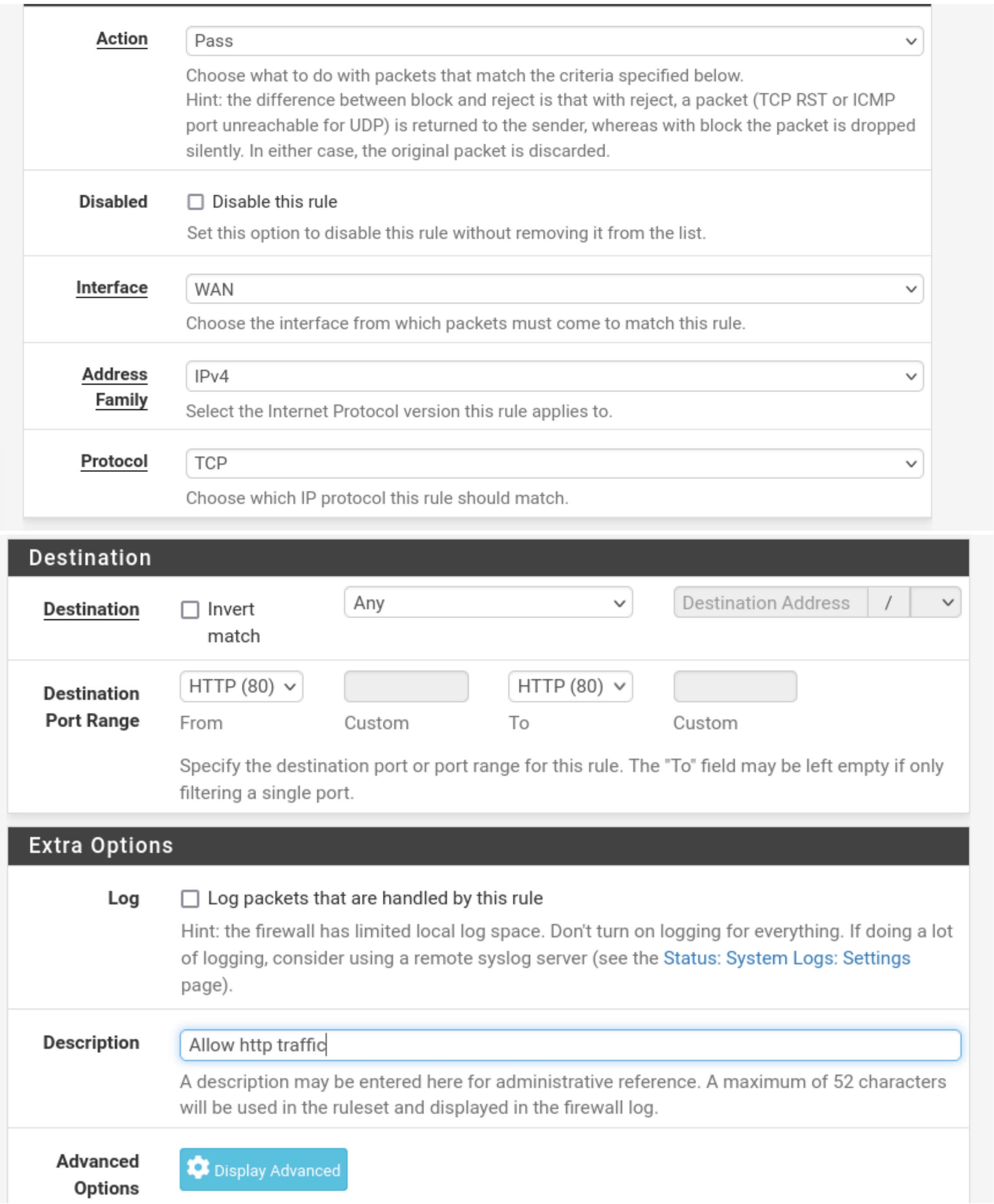
Outbound:

As regras de firewall aplicadas para o protocolo *ICMP* no tráfego *outbound* são iguais às regras aplicadas para o tráfego *inbound*.

- **Protocolo WEB, *HTTP***

Este protocolo permite o tráfego especificado, é aplicado na interface interna e utiliza o protocolo TCP. *Source:* Network para uma gama de endereços ip específica, 10.120.59.0/24. Definindo a porta HTTP (80) como porta de destino.

Inbound:



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.

Destination

Destination: □ Invert match | Any | Destination Address /

Destination Port Range: HTTP (80) From | Custom | HTTP (80) 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 http traffic
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:

Figura 16 - Regras firewall protocolo WEB

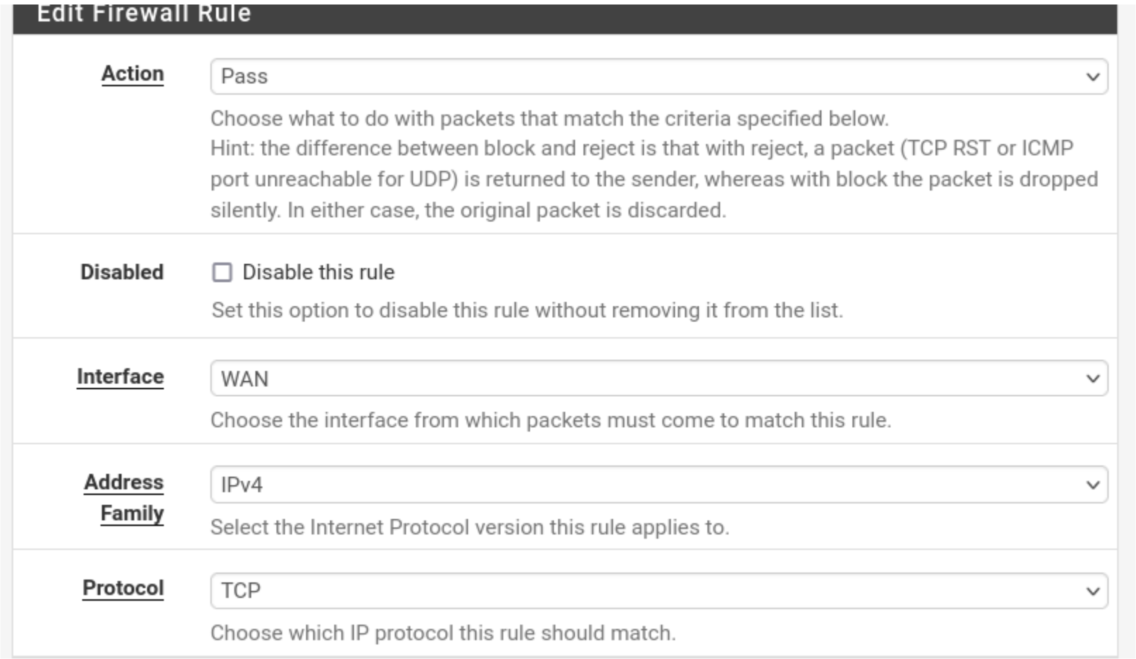
Outbound:

As regras aplicadas para o tráfego *outbound* são idênticas às regras aplicadas para o tràfego *inbound*.

- ***Protocolo Email, SMTP***

Este protocolo bloqueia todo o tráfego especificado, usando também, o protocolo TCP, destinando-se a qualquer ip. Define a porta 25, SMTP, como porta de destino.

Inbound:



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

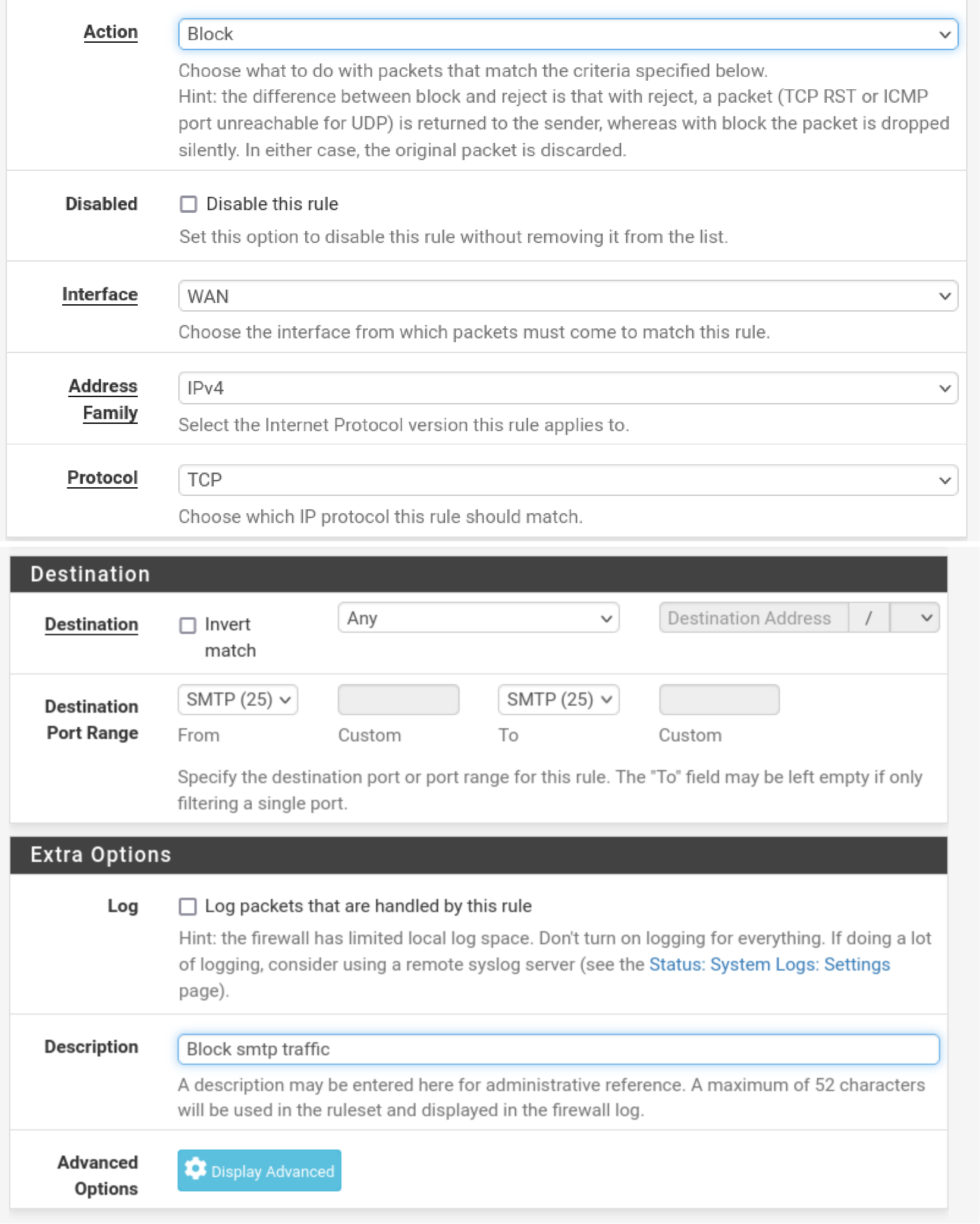
Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.

Figura 17 - Regras de firewall protocolo Email

Outbound:



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.

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 smtp traffic

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

Figura 18 - Regra de firewall para protocolo de email

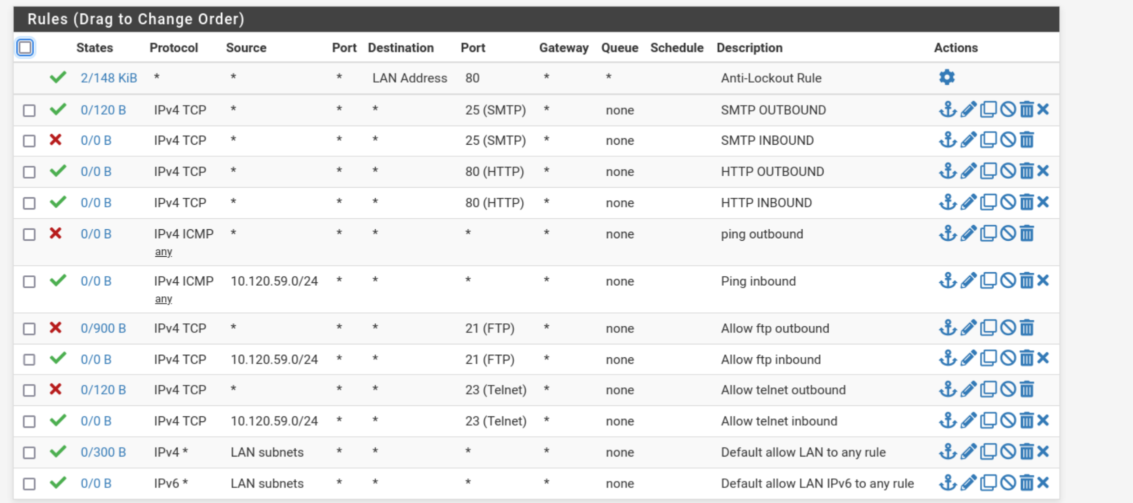
2. Demonstração das políticas de firewall

Para a testagem/ demonstração das políticas de firewall, utilizou-se dois métodos, um deles foi através do comando abaixo representado (não foi possível utilizar o método abaixo para o protocolo ICMP):

nmap -p(port) ip_do_servidor

O outro método utilizado foi a testagem dos serviços através da linha de comandos, para tal usou-se o *host,* o *Kali* e o *Pfsense.*

1. Interface LAN

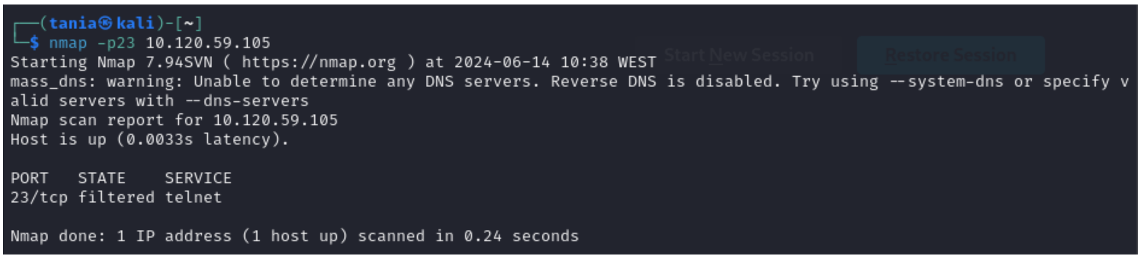


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	2/148 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✓	0/120 B	IPv4 TCP	*	*	*	25 (SMTP)	*	none		SMTP OUTBOUND	⚓✎❐⦸🗑✕
□	✗	0/0 B	IPv4 TCP	*	*	*	25 (SMTP)	*	none		SMTP INBOUND	⚓✎❐⦸🗑
□	✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		HTTP OUTBOUND	⚓✎❐⦸🗑✕
□	✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		HTTP INBOUND	⚓✎❐⦸🗑✕
□	✗	0/0 B	IPv4 ICMP any	*	*	*	*	*	none		ping outbound	⚓✎❐⦸🗑
□	✓	0/0 B	IPv4 ICMP any	10.120.59.0/24	*	*	*	*	none		Ping inbound	⚓✎❐⦸🗑✕
□	✗	0/900 B	IPv4 TCP	*	*	*	21 (FTP)	*	none		Allow ftp outbound	⚓✎❐⦸🗑
□	✓	0/0 B	IPv4 TCP	10.120.59.0/24	*	*	21 (FTP)	*	none		Allow ftp inbound	⚓✎❐⦸🗑✕
□	✗	0/120 B	IPv4 TCP	*	*	*	23 (Telnet)	*	none		Allow telnet outbound	⚓✎❐⦸🗑
□	✓	0/0 B	IPv4 TCP	10.120.59.0/24	*	*	23 (Telnet)	*	none		Allow telnet inbound	⚓✎❐⦸🗑✕
□	✓	0/300 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	⚓✎❐⦸🗑✕
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓✎❐⦸🗑✕

Figura 19 - Regras implementadas na firewall

- Protocolo telnet

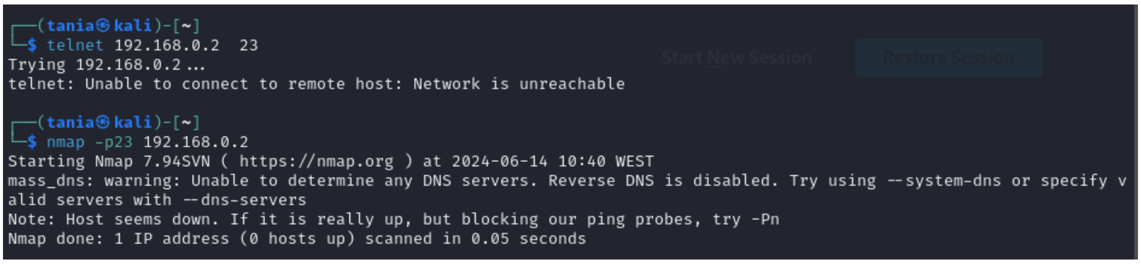


```
┌──(tania㉿kali)-[~]
└─$ nmap -p23 10.120.59.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:38 WEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 10.120.59.105
Host is up (0.0033s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Figura 20 - Interface 1 inbound

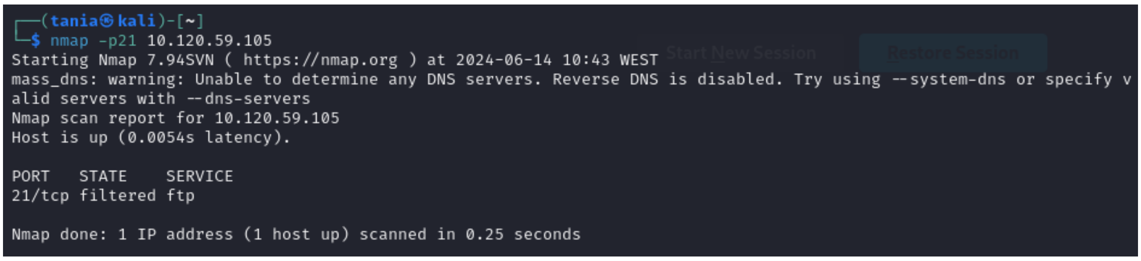


```
┌──(tania㉿kali)-[~]
└─$ telnet 192.168.0.2  23
Trying 192.168.0.2 ...
telnet: Unable to connect to remote host: Network is unreachable

┌──(tania㉿kali)-[~]
└─$ nmap -p23 192.168.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:40 WEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.05 seconds
```

Figura 21 - Interface 1 outbound

- Protocolo ftp

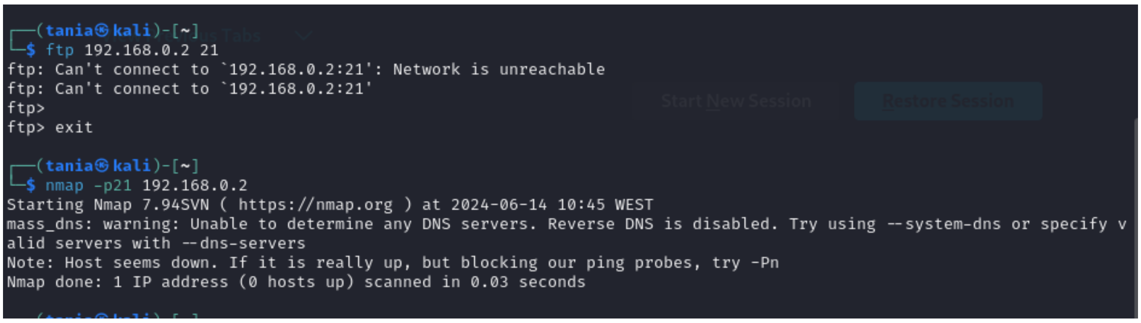


```
┌──(tania㉿kali)-[~]
└─$ nmap -p21 10.120.59.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:43 WEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 10.120.59.105
Host is up (0.0054s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Figura 22 - Interface 1 inbound

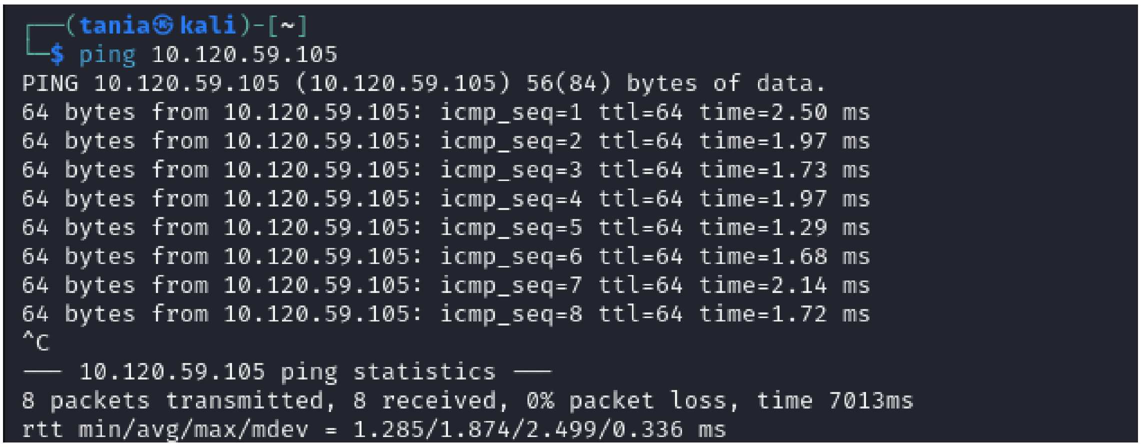


```
┌──(tania㉿kali)-[~]
└─$ ftp 192.168.0.2 21
ftp: Can't connect to `192.168.0.2:21': Network is unreachable
ftp: Can't connect to `192.168.0.2:21'
ftp>
ftp> exit

┌──(tania㉿kali)-[~]
└─$ nmap -p21 192.168.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:45 WEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.03 seconds
```

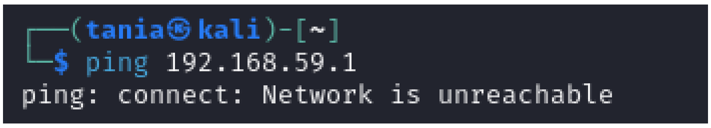
Figura 23 - Interface 1 outbound

- ICMP



```
┌──(tania㉿kali)-[~]
└─$ ping 10.120.59.105
PING 10.120.59.105 (10.120.59.105) 56(84) bytes of data.
64 bytes from 10.120.59.105: icmp_seq=1 ttl=64 time=2.50 ms
64 bytes from 10.120.59.105: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 10.120.59.105: icmp_seq=3 ttl=64 time=1.73 ms
64 bytes from 10.120.59.105: icmp_seq=4 ttl=64 time=1.97 ms
64 bytes from 10.120.59.105: icmp_seq=5 ttl=64 time=1.29 ms
64 bytes from 10.120.59.105: icmp_seq=6 ttl=64 time=1.68 ms
64 bytes from 10.120.59.105: icmp_seq=7 ttl=64 time=2.14 ms
64 bytes from 10.120.59.105: icmp_seq=8 ttl=64 time=1.72 ms
^C
--- 10.120.59.105 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7013ms
rtt min/avg/max/mdev = 1.285/1.874/2.499/0.336 ms
```

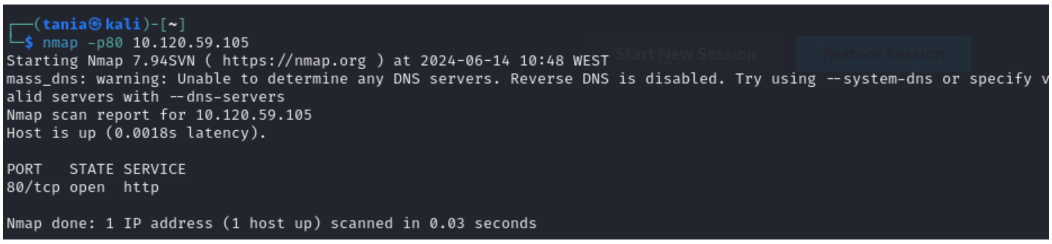
Figura 24 - Interface 1 inbound



```
┌──(tania㉿kali)-[~]
└─$ ping 192.168.59.1
ping: connect: Network is unreachable
```

Figura 25 - Interface 2 outbound

- WEB

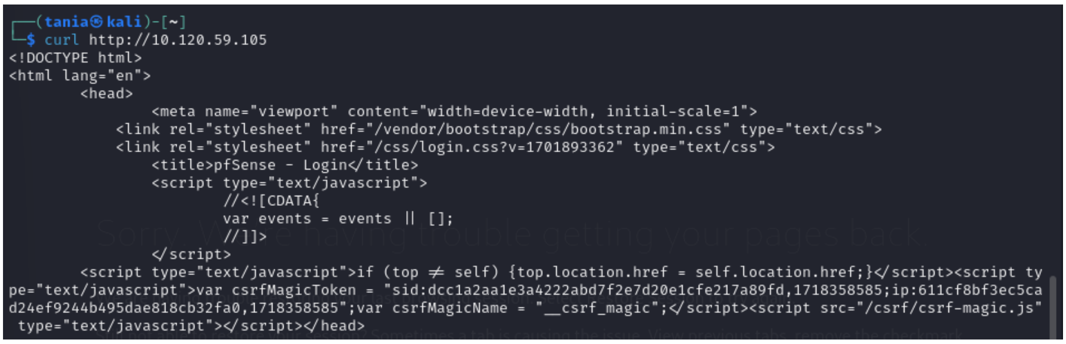


```
┌──(tania㉿kali)-[~]
└─$ nmap -p80 10.120.59.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:48 WEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 10.120.59.105
Host is up (0.0018s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

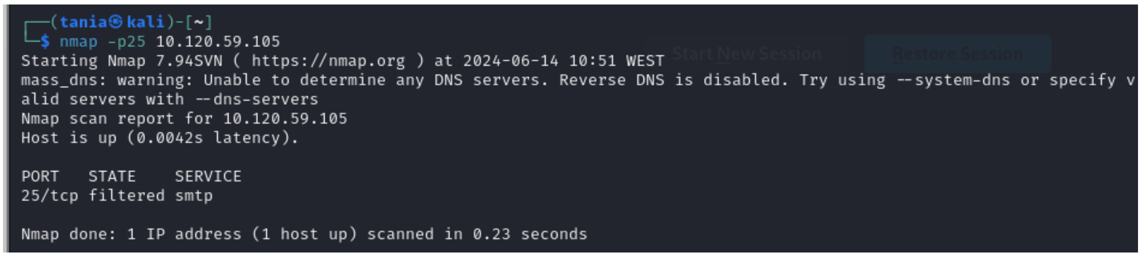
Figura 26 - Interface 1 inbound



```
┌──(tania㉿kali)-[~]
└─$ curl http://10.120.59.105
<!DOCTYPE html>
<html lang="en">
        <head>
                <meta name="viewport" content="width=device-width, initial-scale=1">
            <link rel="stylesheet" href="/vendor/bootstrap/css/bootstrap.min.css" type="text/css">
            <link rel="stylesheet" href="/css/login.css?v=1701893362" type="text/css">
                <title>pfSense - Login</title>
                <script type="text/javascript">
                        //<![CDATA{
                        var events = events || [];
                        //]]>
                </script>
        <script type="text/javascript">if (top != self) {top.location.href = self.location.href;}</script><script ty
pe="text/javascript">var csrfMagicToken = "sid:dcc1a2aa1e3a4222abd7f2e7d20e1cfe217a89fd,1718358585;ip:611cf8bf3ec5ca
d24ef9244b495dae818cb32fa0,1718358585";var csrfMagicName = "__csrf_magic";</script><script src="/csrf/csrf-magic.js"
 type="text/javascript"></script></head>
```

Figura 27 - Interface 1 outbound

- Email

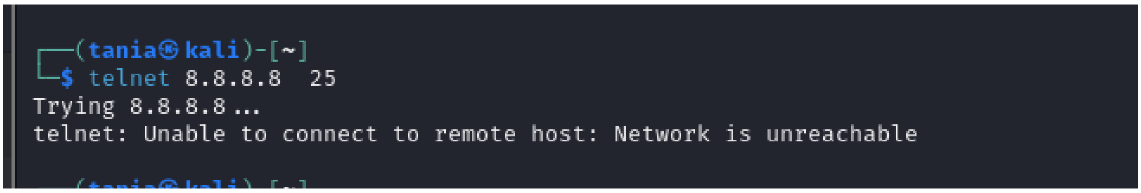


```
┌──(tania㉿kali)-[~]
└─$ nmap -p25 10.120.59.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:51 WEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 10.120.59.105
Host is up (0.0042s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Figura 28 - Interface 1 inbound

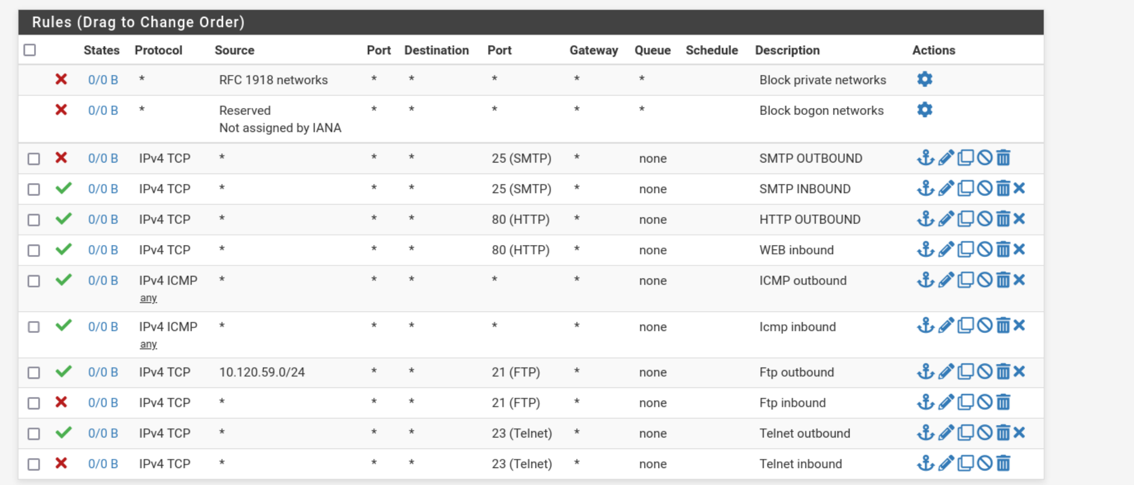


```
┌──(tania㉿kali)-[~]
└─$ telnet 8.8.8.8  25
Trying 8.8.8.8 ...
telnet: Unable to connect to remote host: Network is unreachable

┌──(tania㉿kali)-[~]
```

Figura 29 - Interface 1 outbound

2. Interface WAN

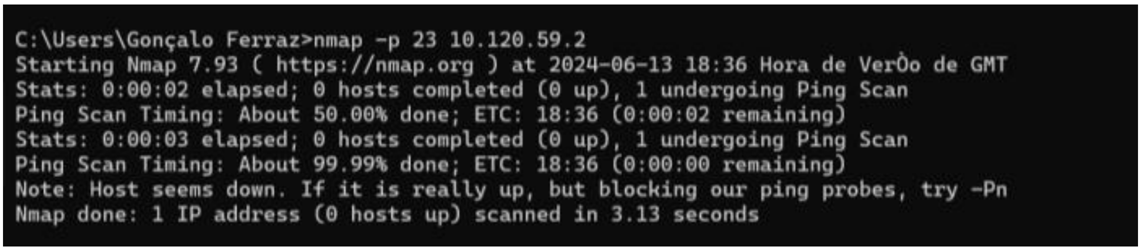


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✕	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✕	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✕	0/0 B	IPv4 TCP	*	*	*	25 (SMTP)	*	none		SMTP OUTBOUND	⚓✎❐⊘🗑
□	✓	0/0 B	IPv4 TCP	*	*	*	25 (SMTP)	*	none		SMTP INBOUND	⚓✎❐⊘🗑✕
□	✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		HTTP OUTBOUND	⚓✎❐⊘🗑✕
□	✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		WEB inbound	⚓✎❐⊘🗑✕
□	✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none		ICMP outbound	⚓✎❐⊘🗑✕
□	✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none		Icmp inbound	⚓✎❐⊘🗑✕
□	✓	0/0 B	IPv4 TCP	10.120.59.0/24	*	*	21 (FTP)	*	none		Ftp outbound	⚓✎❐⊘🗑✕
□	✕	0/0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none		Ftp inbound	⚓✎❐⊘🗑
□	✓	0/0 B	IPv4 TCP	*	*	*	23 (Telnet)	*	none		Telnet outbound	⚓✎❐⊘🗑✕
□	✕	0/0 B	IPv4 TCP	*	*	*	23 (Telnet)	*	none		Telnet inbound	⚓✎❐⊘🗑

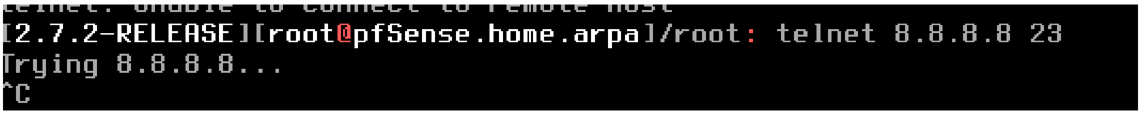
Figura 30 - Regras implementadas na firewall

- Telnet



```
C:\Users\Gonçalo Ferraz>nmap -p 23 10.120.59.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-13 18:36 Hora de VerÒo de GMT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 18:36 (0:00:02 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 99.99% done; ETC: 18:36 (0:00:00 remaining)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

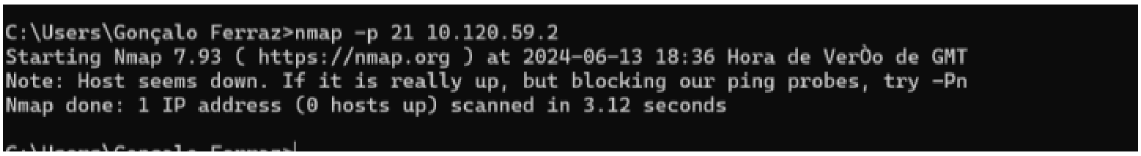
Figura 31 - Protocolo telnet Interface 2 inbound



```
telnet: Unable to connect to remote host
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: telnet 8.8.8.8 23
Trying 8.8.8.8...
^C
```

Figura 32 - Protocolo telnet interface 2 outbound

- Serviço ftp

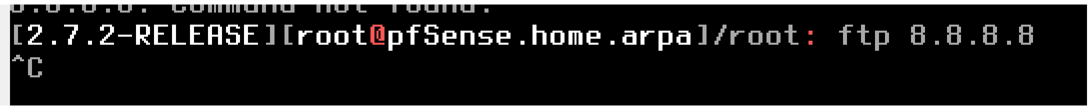


```
C:\Users\Gonçalo Ferraz>nmap -p 21 10.120.59.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-13 18:36 Hora de VerÒo de GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds

C:\Users\Gonçalo Ferraz>
```

Figura 33 - Interface 2 inbound

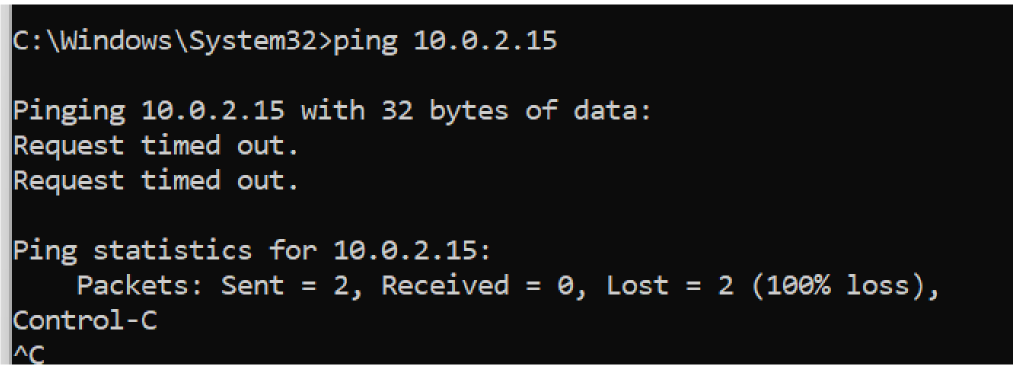
Não foi possível realizar a devida testagem do tráfego outbound.



```
0.0.0.0: Command not found.
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ftp 8.8.8.8
^C
```

Figura 34 - Interface 2 outbound

- ICMP

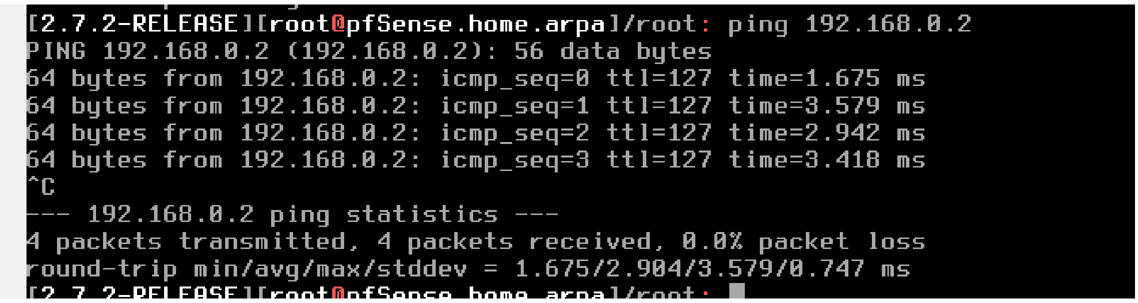


```
C:\Windows\System32>ping 10.0.2.15

Pinging 10.0.2.15 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.0.2.15:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
```

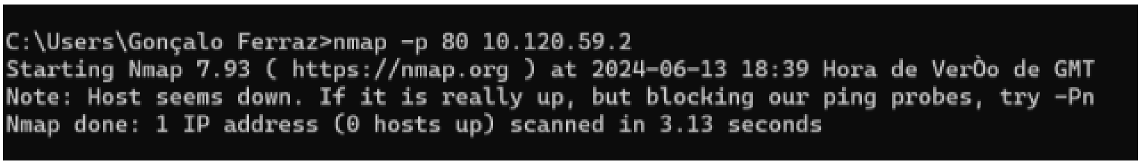
Figura 35 - Protocolo ICMP interface 2 inbound



```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2): 56 data bytes
64 bytes from 192.168.0.2: icmp_seq=0 ttl=127 time=1.675 ms
64 bytes from 192.168.0.2: icmp_seq=1 ttl=127 time=3.579 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=127 time=2.942 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=127 time=3.418 ms
^C
--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.675/2.904/3.579/0.747 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

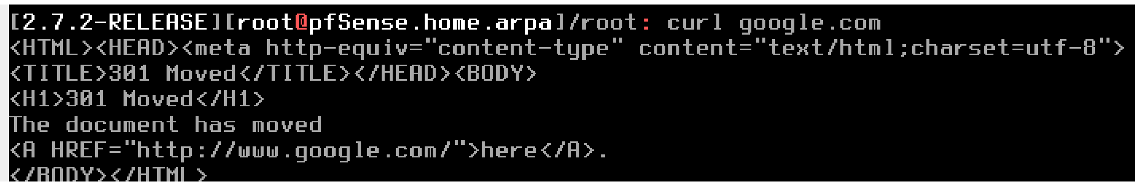
Figura 36 - Protocolo ICMP interface 2 outbound

- WEB



```
C:\Users\Gonçalo Ferraz>nmap -p 80 10.120.59.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-13 18:39 Hora de VerÒo de GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

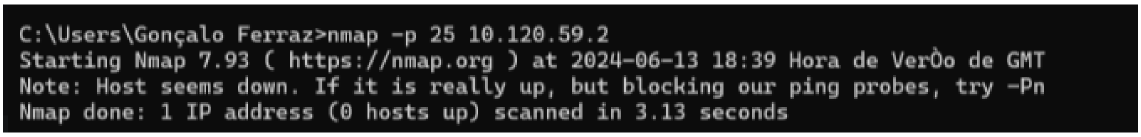
Figura 37 - Interface 2 inbound



```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

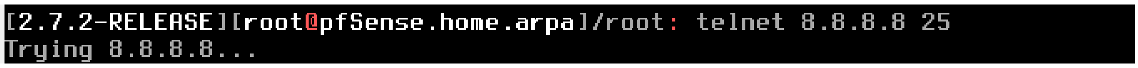
Figura 38 - Interface 2 outbound

- SMTP



```
C:\Users\Gonçalo Ferraz>nmap -p 25 10.120.59.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-13 18:39 Hora de VerÒo de GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

Figura 39 - Interface 2 inbound



```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: telnet 8.8.8.8 25
Trying 8.8.8.8...
```

Figura 40 - Interface 2 outbound

3. Identificação de protocolos inseguros

Os protocolos inseguros são o telnet, ftp, *HTTP* e SMTP. Dado que, o telnet porque não possui nenhum tipo de criptografia logo, permite a descoberta de senhas e captura de informações. Já o serviço ftp, também não possui qualquer tipo de criptografia, logo os dados trafegados na rede podem ser intercetados por qualquer outra pessoa. Contudo o SMTP também é inseuro pois tem autenticação básica, vulnerável a ataques Man-In-The-Middle, suscetível a spam e spoofing. *HTTP* é um protocolo que por padrão não é criptografado, ou seja, se alguém intercetar o pacote com dados enviados entre o navegador e o servidor onde o site está hospedado, ela será capaz de ler as informações contidas nele.

De tal modo, deve -se alterar o protocolo telnet pelo protocolo SSH, o protocolo ftp pelo protocolo SFTP, o protocolo *HTTP* pelo protocolo *HTTPS* e, por fim, o protocolo SMTP pelo protocolo SMTPS.

Abaixo são demonstradas as devidas alterações para cada um dos protocolos nas políticas de firewall.

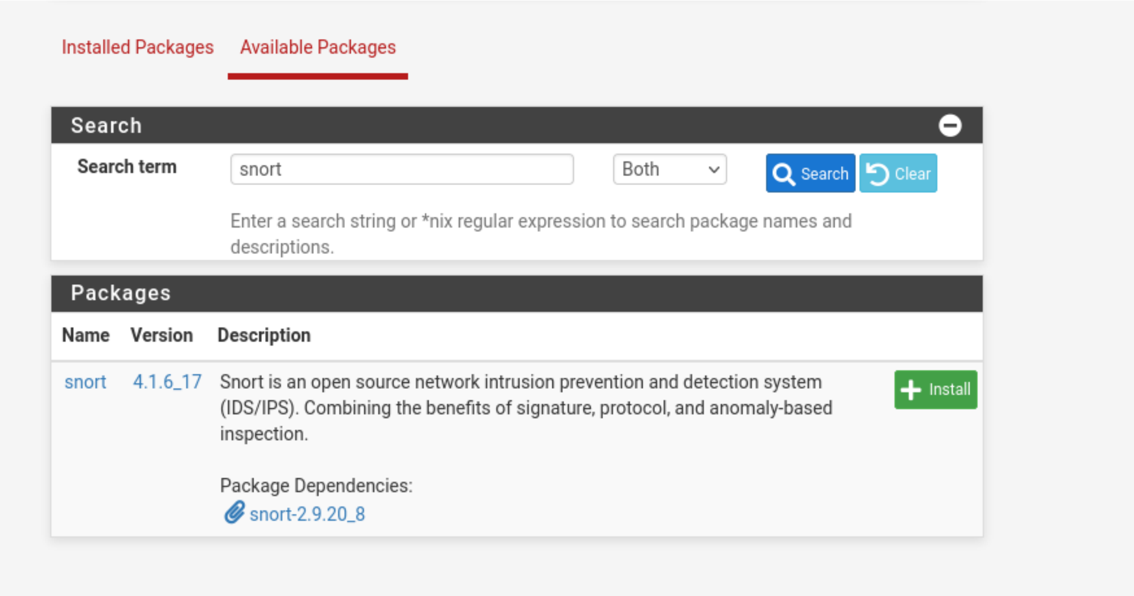
	Interface 1		**Interface 2**	
Protocolo	*inbound*	*Outbound*	*inbound*	*Outbound*
SSH	Sim (rede interna)	Não(all)	Não(all)	Sim (all)
HTTPS	Sim (all)	Sim(all)	Sim(all)	Sim(all)
SMTPS	Não(all)	Sim(all)	Sim(all)	Não(all)
SFTP	Sim (rede interna)	Não(all)	Não(all)	Sim (rede interna)

Tabela 1 - Regras para firewall

4. Instalação *snort*

Snort é um dos melhores Sistemas de Prevenção de Intrusão (IPS) de código aberto do mundo, mantido e desenvolvido pela Cisco.

Para proceder à instalação do snort acedeu-se à interface gráfica do *Pfsense*, de seguida, *System -> Package manager.* Acedendo à seguinte página:



snort

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20_8

Figura 41 - Available packages

Após encontrar o software snort procede-se à devida instalação. Depois de instalado, já é possível encontrá-lo em *Services*, como demonstrado abaixo:

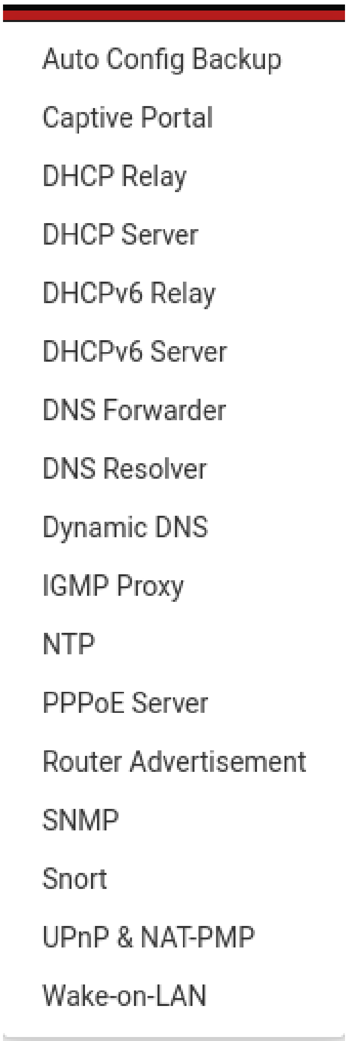
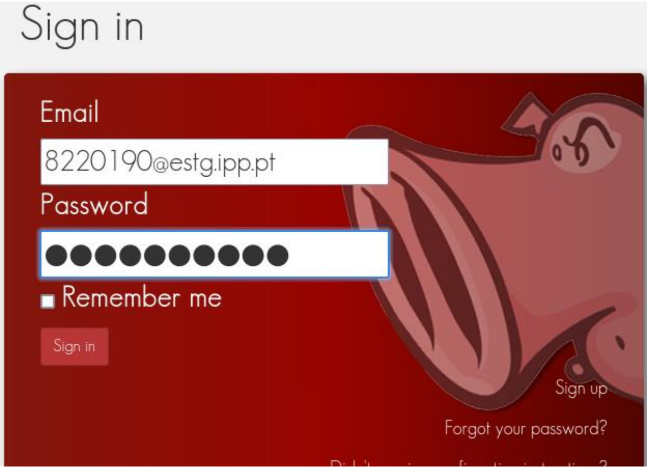


Figura 42 - Services Pfsense

Procede-se agora à configuração...

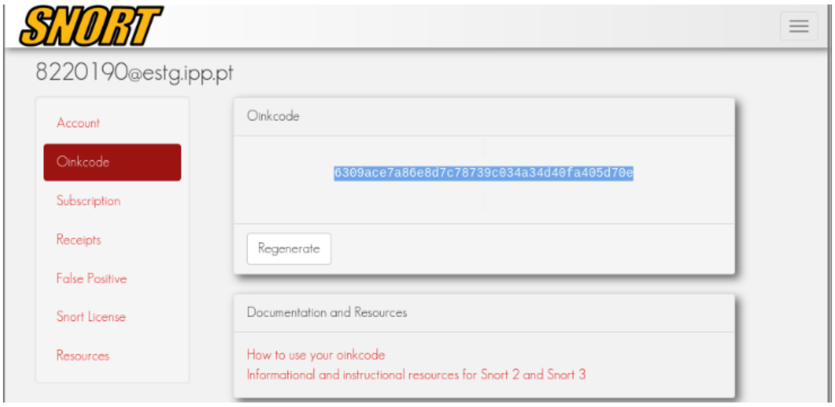
Começa-se por aceder à site oficial do snort para registo de conta.



Email: 8220190@estg.ipp.pt

Password: ●●●●●●●●●●●

Figura 43 - Registo de conta



SNORT

8220190@estg.ipp.pt

- Account
- Oinkcode
- Subscription
- Receipts
- False Positive
- Snort License
- Resources

Oinkcode

6309ace7a86e8d7c78739c034a34d40fa405d70e

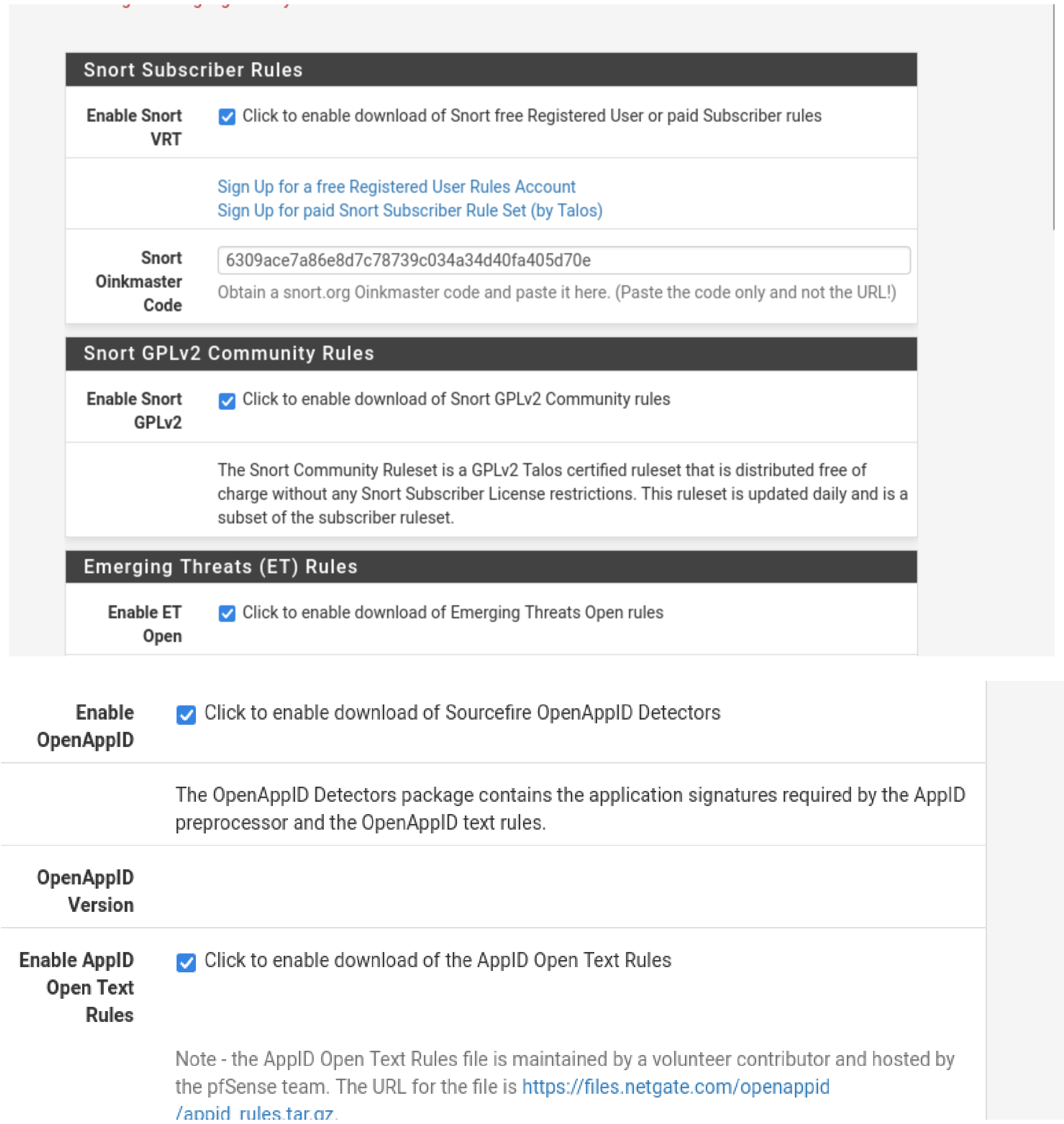
Regenerate

Documentation and Resources

How to use your oinkcode
Informational and instructional resources for Snort 2 and Snort 3

Figura 44 – Oinkcode

Sendo assim, copia-se o código acima descrito para ser possível configurar corretamente o software snort. Abaixo são demonstradas todas as configurações:



Snort Subscriber Rules

Enable Snort VRT	☑ Click to enable download of Snort free Registered User or paid Subscriber rules
	Sign Up for a free Registered User Rules Account Sign Up for paid Snort Subscriber Rule Set (by Talos)
Snort Oinkmaster Code	6309ace7a86e8d7c78739c034a34d40fa405d70e Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

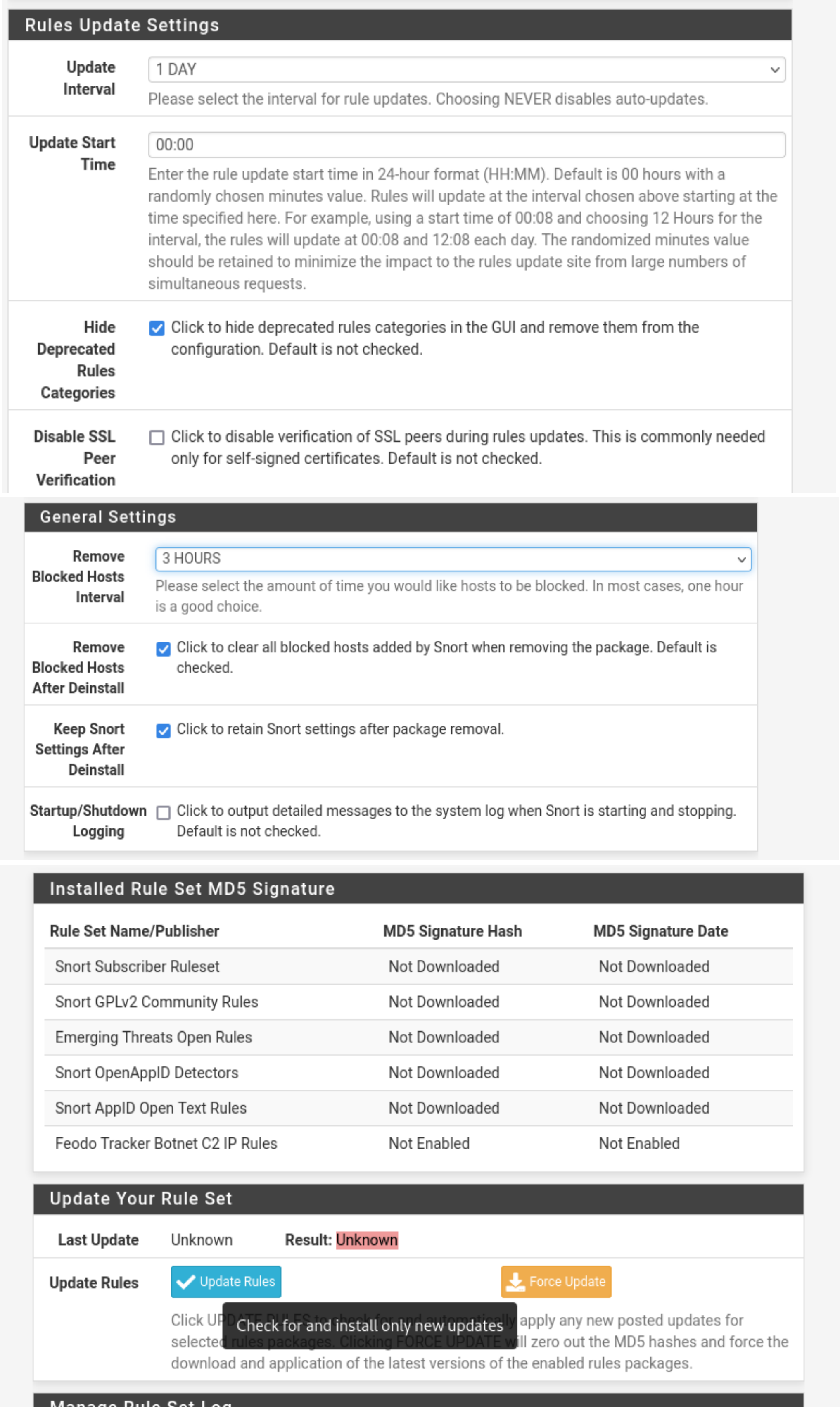
Enable Snort GPLv2	☑ Click to enable download of Snort GPLv2 Community rules
	The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open	☑ Click to enable download of Emerging Threats Open rules

Enable OpenAppID	☑ Click to enable download of Sourcefire OpenAppID Detectors
	The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.
OpenAppID Version	
Enable AppID Open Text Rules	☑ Click to enable download of the AppID Open Text Rules Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.

Figura 45 - Configuração 1



Rules Update Settings

Update Interval: 1 DAY
Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time: 00:00
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

Hide Deprecated Rules Categories: ☑ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification: □ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

General Settings

Remove Blocked Hosts Interval: 3 HOURS
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

Remove Blocked Hosts After Deinstall: ☑ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

Keep Snort Settings After Deinstall: ☑ Click to retain Snort settings after package removal.

Startup/Shutdown Logging: □ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Downloaded	Not Downloaded
Snort AppID Open Text Rules	Not Downloaded	Not Downloaded
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

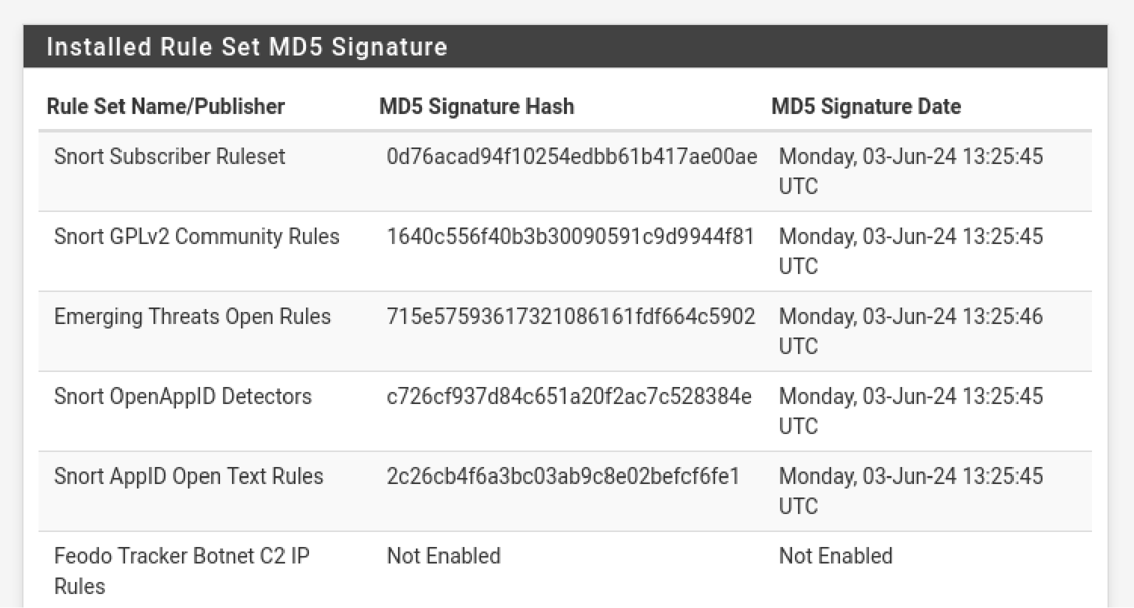
Last Update Unknown **Result:** Unknown

Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

Figura 46 - Configuração 2

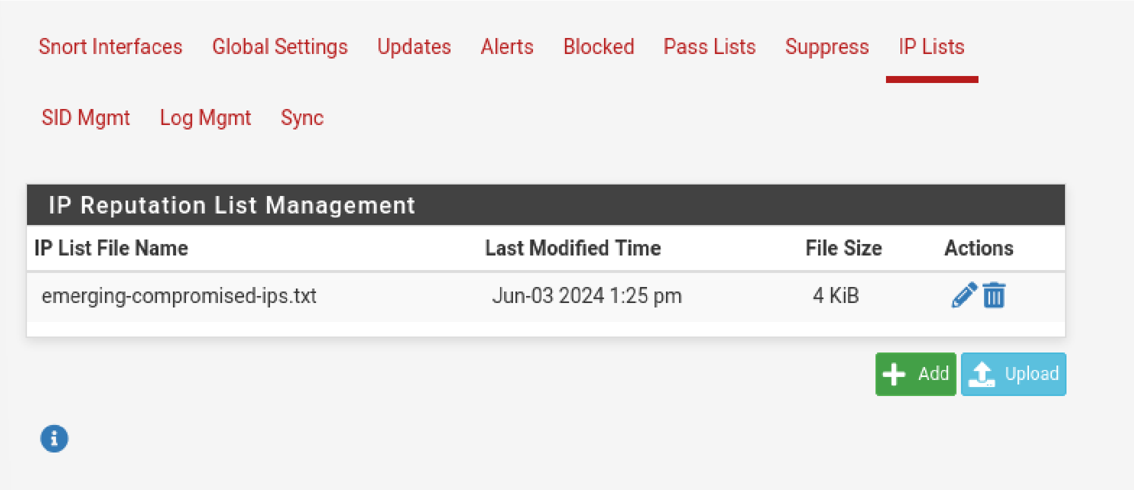


Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	0d76acad94f10254edbb61b417ae00ae	Monday, 03-Jun-24 13:25:45 UTC
Snort GPLv2 Community Rules	1640c556f40b3b30090591c9d9944f81	Monday, 03-Jun-24 13:25:45 UTC
Emerging Threats Open Rules	715e57593617321086161fdf664c5902	Monday, 03-Jun-24 13:25:46 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Monday, 03-Jun-24 13:25:45 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Monday, 03-Jun-24 13:25:45 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Figura 47 - Regras instaladas

Acedendo agora a *IP Lists:*

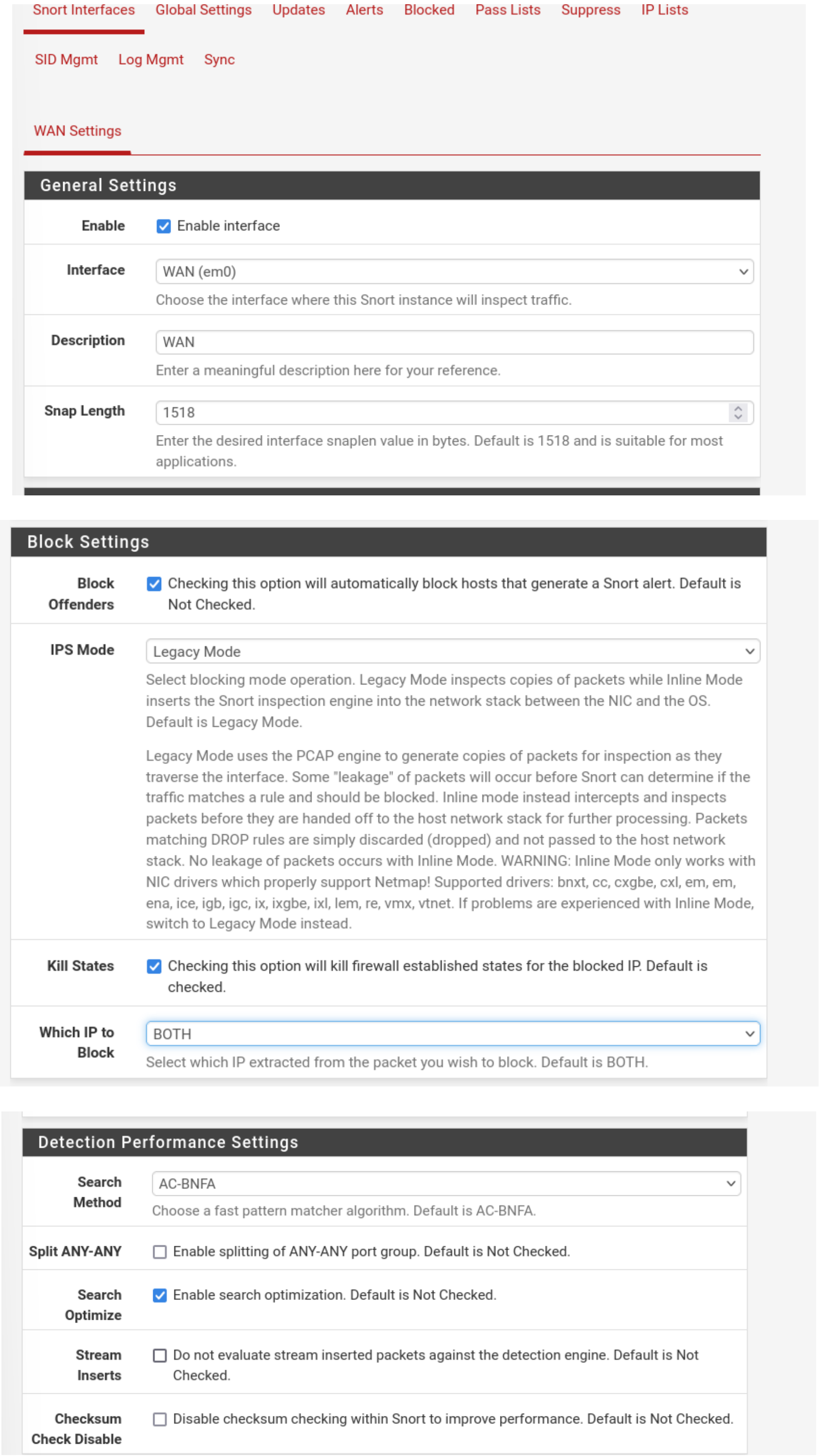


IP Reputation List Management

IP List File Name	Last Modified Time	File Size	Actions
emerging-compromised-ips.txt	Jun-03 2024 1:25 pm	4 KiB	

Figura 48 - IP LISTS

Adicionar uma interface:



General Settings

Enable	☑ Enable interface
Interface	WAN (em0) Choose the interface where this Snort instance will inspect traffic.
Description	WAN Enter a meaningful description here for your reference.
Snap Length	1518 Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

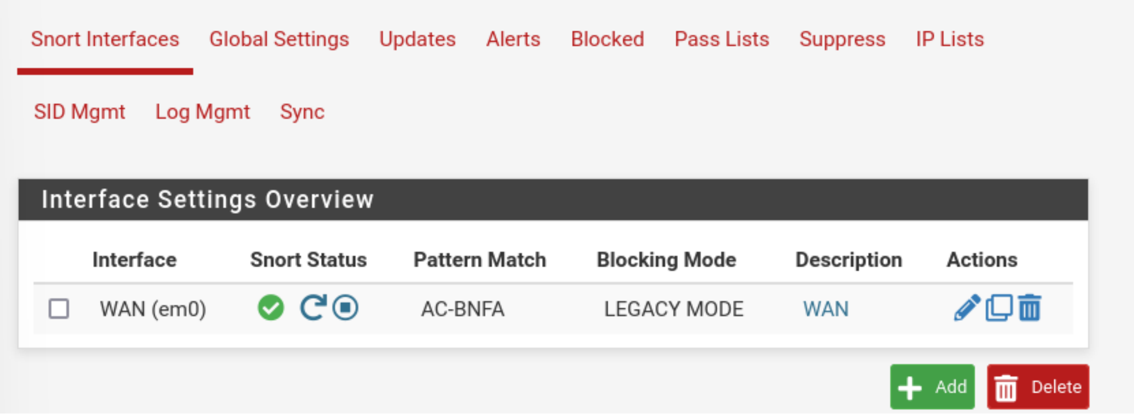
Block Settings

Block Offenders	☑ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode. Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Kill States	☑ Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	BOTH Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Search Method	AC-BNFA Choose a fast pattern matcher algorithm. Default is AC-BNFA.
Split ANY-ANY	□ Enable splitting of ANY-ANY port group. Default is Not Checked.
Search Optimize	☑ Enable search optimization. Default is Not Checked.
Stream Inserts	□ Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
Checksum Check Disable	□ Disable checksum checking within Snort to improve performance. Default is Not Checked.

Figura 49 - Adicionar uma interface

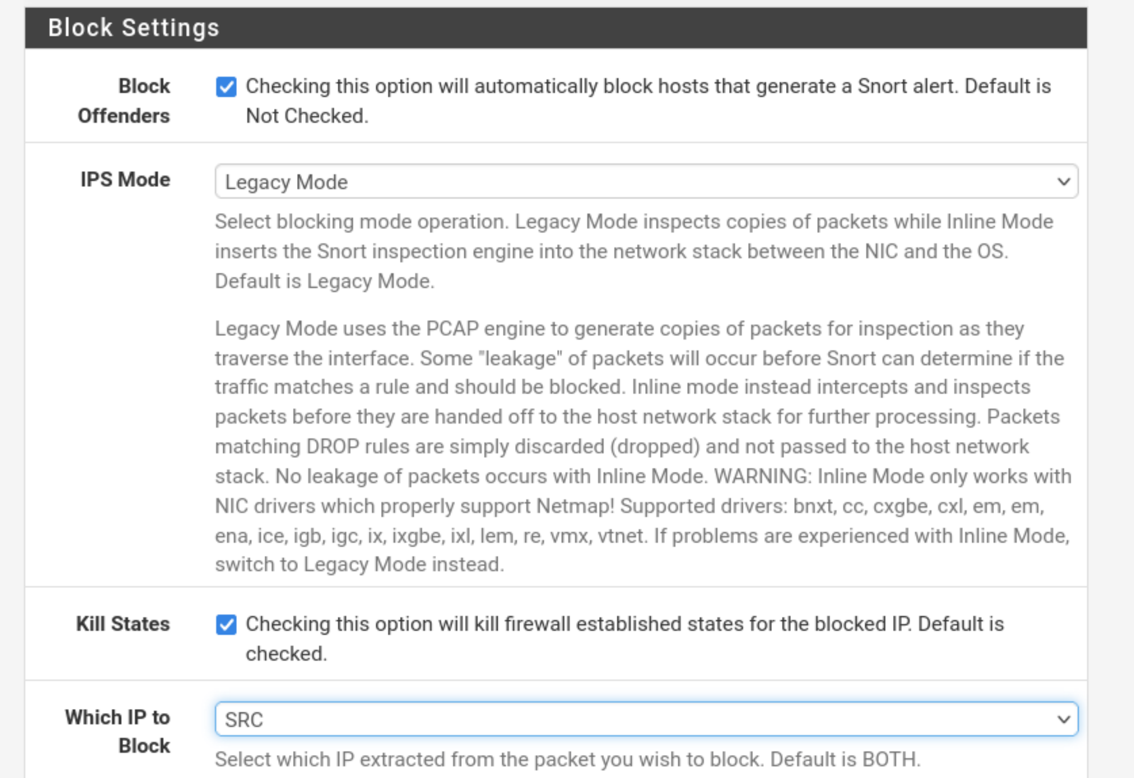


Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	✓	AC-BNFA	LEGACY MODE	WAN	

Figura 50 - Interfaces

Adicionar interface L



Block Settings

Block Offenders ☑ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

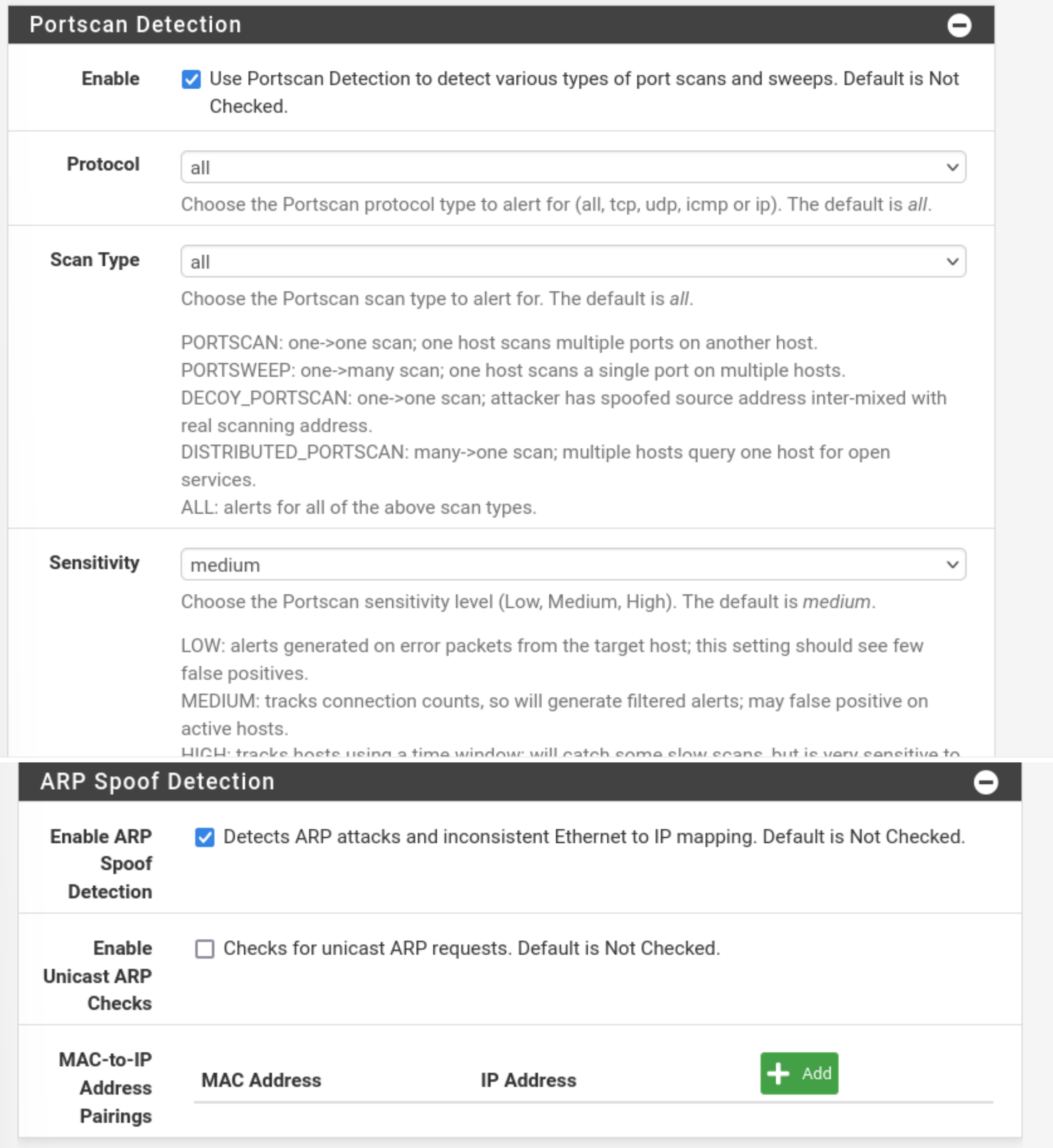
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☑ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block SRC

Select which IP extracted from the packet you wish to block. Default is BOTH.

AN:



Portscan Detection

Enable ☑ Use Portscan Detection to detect various types of port scans and sweeps. Default is Not Checked.

Protocol all

Choose the Portscan protocol type to alert for (all, tcp, udp, icmp or ip). The default is *all*.

Scan Type all

Choose the Portscan scan type to alert for. The default is *all*.

PORTSCAN: one->one scan; one host scans multiple ports on another host.
PORTSWEEP: one->many scan; one host scans a single port on multiple hosts.
DECOY_PORTSCAN: one->one scan; attacker has spoofed source address inter-mixed with real scanning address.
DISTRIBUTED_PORTSCAN: many->one scan; multiple hosts query one host for open services.
ALL: alerts for all of the above scan types.

Sensitivity medium

Choose the Portscan sensitivity level (Low, Medium, High). The default is *medium*.

LOW: alerts generated on error packets from the target host; this setting should see few false positives.
MEDIUM: tracks connection counts, so will generate filtered alerts; may false positive on active hosts.
HIGH: tracks hosts using a time window; will catch some slow scans, but is very sensitive to

ARP Spoof Detection

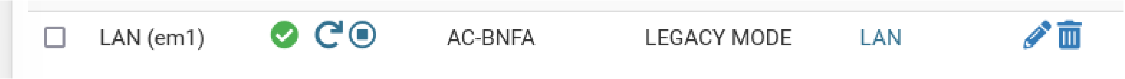
Enable ARP Spoof Detection ☑ Detects ARP attacks and inconsistent Ethernet to IP mapping. Default is Not Checked.

Enable Unicast ARP Checks ☐ Checks for unicast ARP requests. Default is Not Checked.

MAC-to-IP Address Pairings

MAC Address	IP Address	+ Add

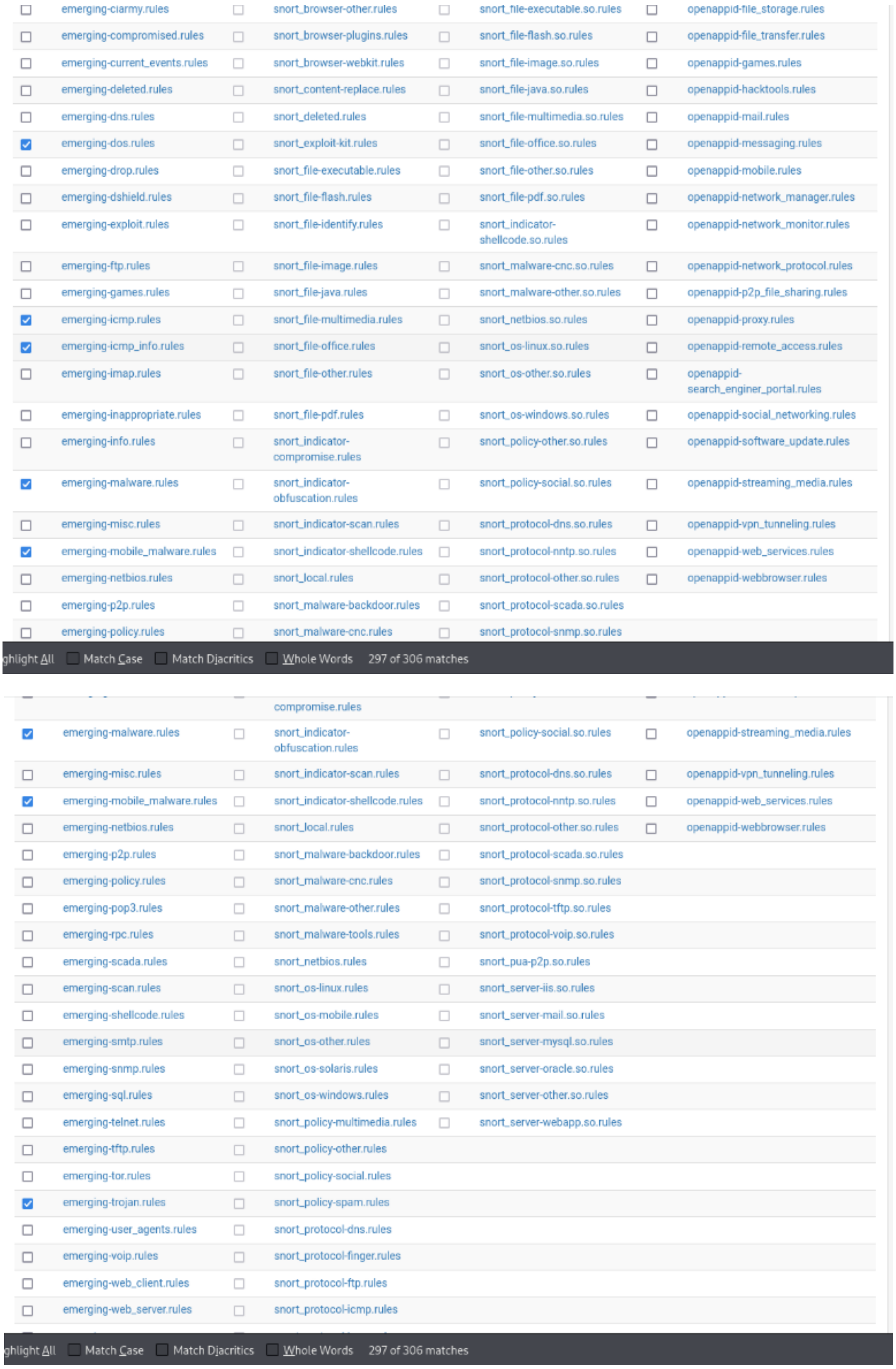
Figura 51 - Interface LAN



☐	LAN (em1)	✓	AC-BNFA	LEGACY MODE	LAN	

Wan categories

Ativou-se categorias relacionas com ataques externos, como *Malware, DOS, TROJAN e, também, o protocolo ICMP*



☐ emerging-ciarmy.rules
☐ emerging-compromised.rules
☐ emerging-current_events.rules
☐ emerging-deleted.rules
☐ emerging-dns.rules
☑ emerging-dos.rules
☐ emerging-drop.rules
☐ emerging-dshield.rules
☐ emerging-exploit.rules
☐ emerging-ftp.rules
☐ emerging-games.rules
☑ emerging-icmp.rules
☑ emerging-icmp_info.rules
☐ emerging-imap.rules
☐ emerging-inappropriate.rules
☐ emerging-info.rules
☑ emerging-malware.rules
☐ emerging-misc.rules
☑ emerging-mobile_malware.rules
☐ emerging-netbios.rules
☐ emerging-p2p.rules
☐ emerging-policy.rules

☐ snort_browser-other.rules
☐ snort_browser-plugins.rules
☐ snort_browser-webkit.rules
☐ snort_content-replace.rules
☐ snort_deleted.rules
☐ snort_exploit-kit.rules
☐ snort_file-executable.rules
☐ snort_file-flash.rules
☐ snort_file-identify.rules
☐ snort_file-image.rules
☐ snort_file-java.rules
☐ snort_file-multimedia.rules
☐ snort_file-office.rules
☐ snort_file-other.rules
☐ snort_file-pdf.rules
☐ snort_indicator-compromise.rules
☐ snort_indicator-obfuscation.rules
☐ snort_indicator-scan.rules
☐ snort_indicator-shellcode.rules
☐ snort_local.rules
☐ snort_malware-backdoor.rules
☐ snort_malware-cnc.rules

☐ snort_file-executable.so.rules
☐ snort_file-flash.so.rules
☐ snort_file-image.so.rules
☐ snort_file-java.so.rules
☐ snort_file-multimedia.so.rules
☐ snort_file-office.so.rules
☐ snort_file-other.so.rules
☐ snort_file-pdf.so.rules
☐ snort_indicator-shellcode.so.rules
☐ snort_malware-cnc.so.rules
☐ snort_malware-other.so.rules
☐ snort_netbios.so.rules
☐ snort_os-linux.so.rules
☐ snort_os-other.so.rules
☐ snort_os-windows.so.rules
☐ snort_policy-other.so.rules
☐ snort_policy-social.so.rules
☐ snort_protocol-dns.so.rules
☐ snort_protocol-nntp.so.rules
☐ snort_protocol-other.so.rules
☐ snort_protocol-scada.so.rules
☐ snort_protocol-snmp.so.rules

☐ openappid-file_storage.rules
☐ openappid-file_transfer.rules
☐ openappid-games.rules
☐ openappid-hacktools.rules
☐ openappid-mail.rules
☐ openappid-messaging.rules
☐ openappid-mobile.rules
☐ openappid-network_manager.rules
☐ openappid-network_monitor.rules
☐ openappid-network_protocol.rules
☐ openappid-p2p_file_sharing.rules
☐ openappid-proxy.rules
☐ openappid-remote_access.rules
☐ openappid-search_enginer_portal.rules
☐ openappid-social_networking.rules
☐ openappid-software_update.rules
☐ openappid-streaming_media.rules
☐ openappid-vpn_tunneling.rules
☐ openappid-web_services.rules
☐ openappid-webbrowser.rules

ghlight All ☐ Match Case ☐ Match Diacritics ☐ Whole Words 297 of 306 matches

☑ emerging-malware.rules
☐ emerging-misc.rules
☑ emerging-mobile_malware.rules
☐ emerging-netbios.rules
☐ emerging-p2p.rules
☐ emerging-policy.rules
☐ emerging-pop3.rules
☐ emerging-rpc.rules
☐ emerging-scada.rules
☐ emerging-scan.rules
☐ emerging-shellcode.rules
☐ emerging-smtp.rules
☐ emerging-snmp.rules
☐ emerging-sql.rules
☐ emerging-telnet.rules
☐ emerging-tftp.rules
☐ emerging-tor.rules
☑ emerging-trojan.rules
☐ emerging-user_agents.rules
☐ emerging-voip.rules
☐ emerging-web_client.rules
☐ emerging-web_server.rules

compromise.rules
☐ snort_indicator-obfuscation.rules
☐ snort_indicator-scan.rules
☐ snort_indicator-shellcode.rules
☐ snort_local.rules
☐ snort_malware-backdoor.rules
☐ snort_malware-cnc.rules
☐ snort_malware-other.rules
☐ snort_malware-tools.rules
☐ snort_netbios.rules
☐ snort_os-linux.rules
☐ snort_os-mobile.rules
☐ snort_os-other.rules
☐ snort_os-solaris.rules
☐ snort_os-windows.rules
☐ snort_policy-multimedia.rules
☐ snort_policy-other.rules
☐ snort_policy-social.rules
☐ snort_policy-spam.rules
☐ snort_protocol-dns.rules
☐ snort_protocol-finger.rules
☐ snort_protocol-ftp.rules
☐ snort_protocol-icmp.rules

☐ snort_policy-social.so.rules
☐ snort_protocol-dns.so.rules
☐ snort_protocol-nntp.so.rules
☐ snort_protocol-other.so.rules
☐ snort_protocol-scada.so.rules
☐ snort_protocol-snmp.so.rules
☐ snort_protocol-tftp.so.rules
☐ snort_protocol-voip.so.rules
☐ snort_pua-p2p.so.rules
☐ snort_server-iis.so.rules
☐ snort_server-mail.so.rules
☐ snort_server-mysql.so.rules
☐ snort_server-oracle.so.rules
☐ snort_server-other.so.rules
☐ snort_server-webapp.so.rules

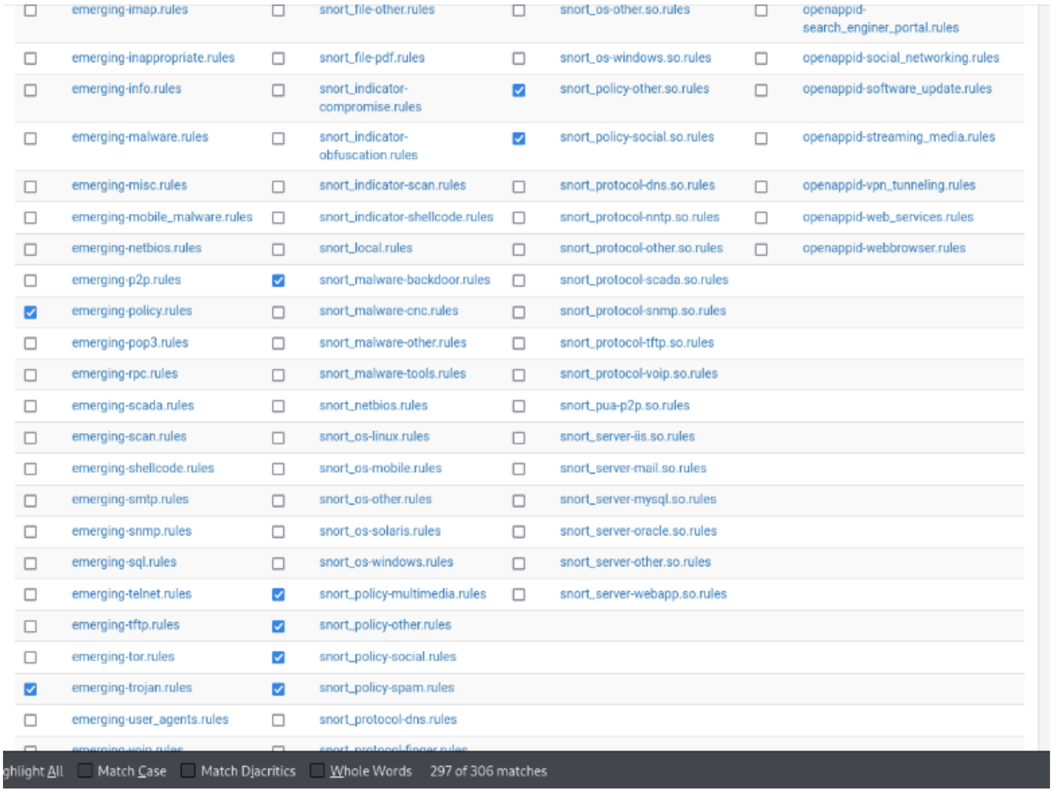
☐ openappid-streaming_media.rules
☐ openappid-vpn_tunneling.rules
☐ openappid-web_services.rules
☐ openappid-webbrowser.rules

ghlight All ☐ Match Case ☐ Match Diacritics ☐ Whole Words 297 of 306 matches

Figura 52 - Wan categories

LAN categories:

Define-se as categorias que detetam atividades suspeitas na rede interna, tais como, *Trojan* e *Blackdoor*.



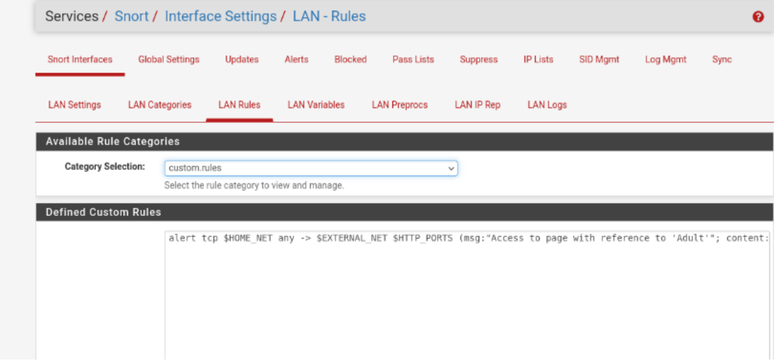
□	emerging-imap.rules	□	snort_file-other.rules	□	snort_os-other.so.rules	□	openappid-search_enginer_portal.rules
□	emerging-inappropriate.rules	□	snort_file-pdf.rules	□	snort_os-windows.so.rules	□	openappid-social_networking.rules
□	emerging-info.rules	□	snort_indicator-compromise.rules	☑	snort_policy-other.so.rules	□	openappid-software_update.rules
□	emerging-malware.rules	□	snort_indicator-obfuscation.rules	☑	snort_policy-social.so.rules	□	openappid-streaming_media.rules
□	emerging-misc.rules	□	snort_indicator-scan.rules	□	snort_protocol-dns.so.rules	□	openappid-vpn_tunneling.rules
□	emerging-mobile_malware.rules	□	snort_indicator-shellcode.rules	□	snort_protocol-nntp.so.rules	□	openappid-web_services.rules
□	emerging-netbios.rules	□	snort_local.rules	□	snort_protocol-other.so.rules	□	openappid-webbrowser.rules
□	emerging-p2p.rules	☑	snort_malware-backdoor.rules	□	snort_protocol-scada.so.rules		
☑	emerging-policy.rules	□	snort_malware-cnc.rules	□	snort_protocol-snmp.so.rules		
□	emerging-pop3.rules	□	snort_malware-other.rules	□	snort_protocol-tftp.so.rules		
□	emerging-rpc.rules	□	snort_malware-tools.rules	□	snort_protocol-voip.so.rules		
□	emerging-scada.rules	□	snort_netbios.rules	□	snort_pua-p2p.so.rules		
□	emerging-scan.rules	□	snort_os-linux.rules	□	snort_server-iis.so.rules		
□	emerging-shellcode.rules	□	snort_os-mobile.rules	□	snort_server-mail.so.rules		
□	emerging-smtp.rules	□	snort_os-other.rules	□	snort_server-mysql.so.rules		
□	emerging-snmp.rules	□	snort_os-solaris.rules	□	snort_server-oracle.so.rules		
□	emerging-sql.rules	□	snort_os-windows.rules	□	snort_server-other.so.rules		
□	emerging-telnet.rules	☑	snort_policy-multimedia.rules	□	snort_server-webapp.so.rules		
□	emerging-tftp.rules	☑	snort_policy-other.rules				
□	emerging-tor.rules	☑	snort_policy-social.rules				
☑	emerging-trojan.rules	☑	snort_policy-spam.rules				
□	emerging-user_agents.rules	□	snort_protocol-dns.rules				
□	emerging-voip.rules	□	snort_protocol-finger.rules				

Figura 53 - LAN categories

5. IPS/IDS

O IPS/IDS são recursos que examinam o tráfego na rede, para detetar e prevenir os acessos não autorizados na mesma, protegendo-a da exploração das vulnerabilidades.

Para este tópico configura-se um alerta para páginas que tenham como referência a palavra *Adult*.



Available Rule Categories

Category Selection: custom.rules

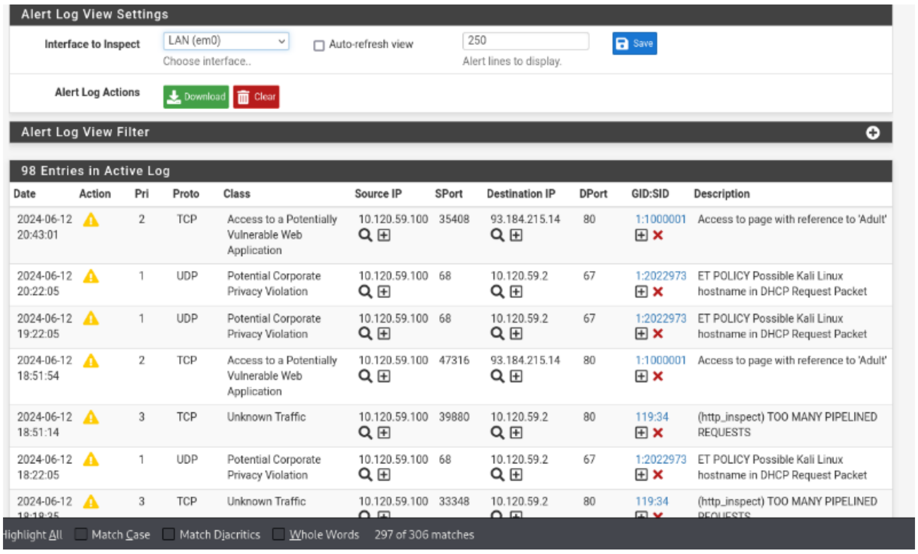
Select the rule category to view and manage.

Defined Custom Rules

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Access to page with reference to 'Adult'"; content:
```

Figura 54 - Alerta para a palavra "Adult"

Por fim, acedeu-se a um *URL* que continha a palavra *Adult* para testagem.



Alert Log View Settings

Interface to Inspect: LAN (em0) — Choose interface..

□ Auto-refresh view

250 — Alert lines to display.

98 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-06-12 20:43:01	⚠	2	TCP	Access to a Potentially Vulnerable Web Application	10.120.59.100	35408	93.184.215.14	80	1:1000001	Access to page with reference to 'Adult'
2024-06-12 20:22:05	⚠	1	UDP	Potential Corporate Privacy Violation	10.120.59.100	68	10.120.59.2	67	1:2022973	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
2024-06-12 19:22:05	⚠	1	UDP	Potential Corporate Privacy Violation	10.120.59.100	68	10.120.59.2	67	1:2022973	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
2024-06-12 18:51:54	⚠	2	TCP	Access to a Potentially Vulnerable Web Application	10.120.59.100	47316	93.184.215.14	80	1:1000001	Access to page with reference to 'Adult'
2024-06-12 18:51:14	⚠	3	TCP	Unknown Traffic	10.120.59.100	39880	10.120.59.2	80	119:34	(http_inspect) TOO MANY PIPELINED REQUESTS
2024-06-12 18:22:05	⚠	1	UDP	Potential Corporate Privacy Violation	10.120.59.100	68	10.120.59.2	67	1:2022973	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
2024-06-12	⚠	3	TCP	Unknown Traffic	10.120.59.100	33348	10.120.59.2	80	119:34	(http_inspect) TOO MANY PIPELINED

Figura 55 - Testagem

Conclusão

Com este trabalho prático, conclui-se que foi proveitoso dado que, foi possível aprender um pouco mais sobre o funcionamento de uma *firewall* e, também do IPS/IDS. Inicialmente, foram apresentadas algumas dificuldades na instalação do *Pfsense*, contudo conseguiu-se ultrapassá-las.

Bibliografia

Instalação snort

Ferramenta de desenho

IPS/IDS