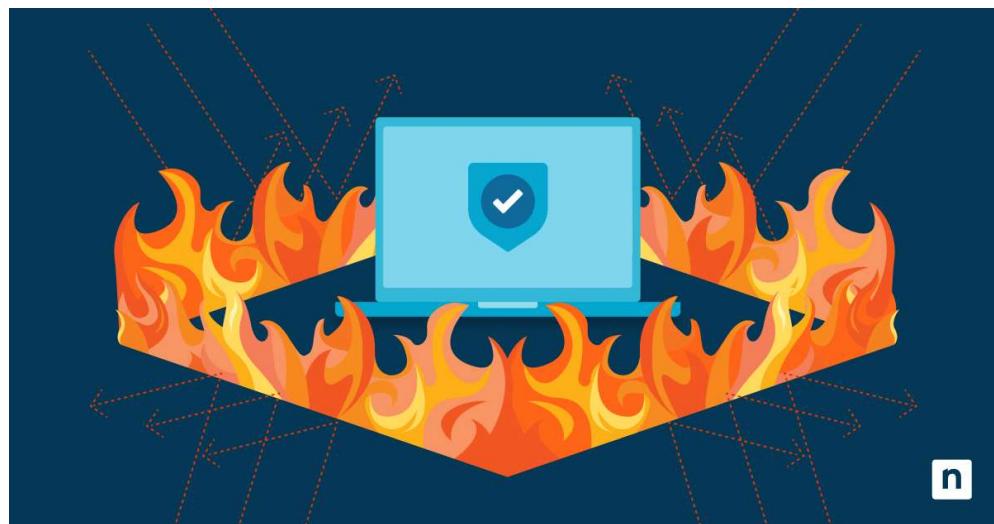


Licenciatura em Segurança Informática em Redes de Computadores

Segurança de Redes

Trabalho Prático 2



David Santos – 8220651

Fábio da Cunha – 8210619

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.

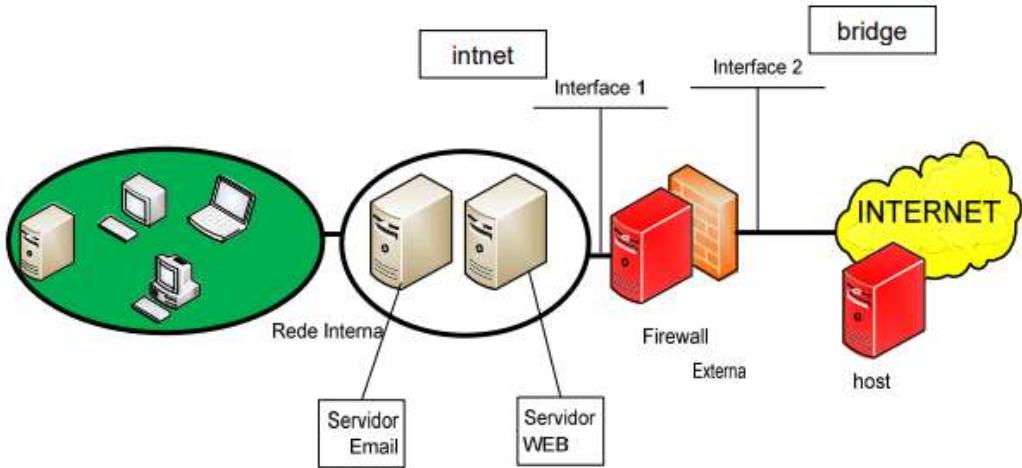
Uso do Snort para IDS/IPS: O Snort foi instalado e configurado para monitorar e bloquear tráfego malicioso, com regras personalizadas para alertar e bloquear tráfego ICMP e detectar acessos a conteúdo adulto

Índice

1.	Montagem do cenário	3
1.1	Configuração das interfaces das máquinas	3
	PFsense (Firewall).....	3
	Kali.....	4
1.2	Desenho pormenorizado da implementação	5
1.3	Configuração do Gateway.....	6
	DNS Forwarder	6
	NAT	6
	Verificação	8
2.	Políticas de firewall	9
2.1	Implementação das políticas LAN	10
	Telnet	10
	FTP.....	12
	Ping.....	14
	<i>SMTP Inbound</i>	15
2.2	Implementação das políticas WAN.....	18
	Telnet	18
	FTP.....	20
	Ping.....	22
	SMTP.....	24
	Web	26
3.	Demonstraçāo	26
3.1	Lista de todas as regras	27
	<i>LAN</i>	27
	<i>WAN</i>	27
3.2	Protocolos inseguros e proposta de alteração	29
	Propostas de Alteração para Melhorar a Segurança da Rede.....	29
	SMTSP (Porta 465) em vez de SMTP (Porta 25)	30
4.	IPS/IDS	31
4.1	Instalação e Configuração do Snort.....	31
	Configuração.....	32
4.2	Análise de Assinaturas existentes	37
	Assinaturas Snort	37
	Análises de exemplo	37

4.3	Tráfego ICMP do exterior	41
	Alerta	41
	Barramento	41
	Verificação	42
4.4	Alerta para páginas com referência a “Adult”	43
5.	Conclusão.....	45

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:

	Network Adapter	Bridged (Automatic)
	Network Adapter 2	LAN Segment

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 pfsense:



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:

Editing Wired connection 1

Connection name: **Wired connection 1**

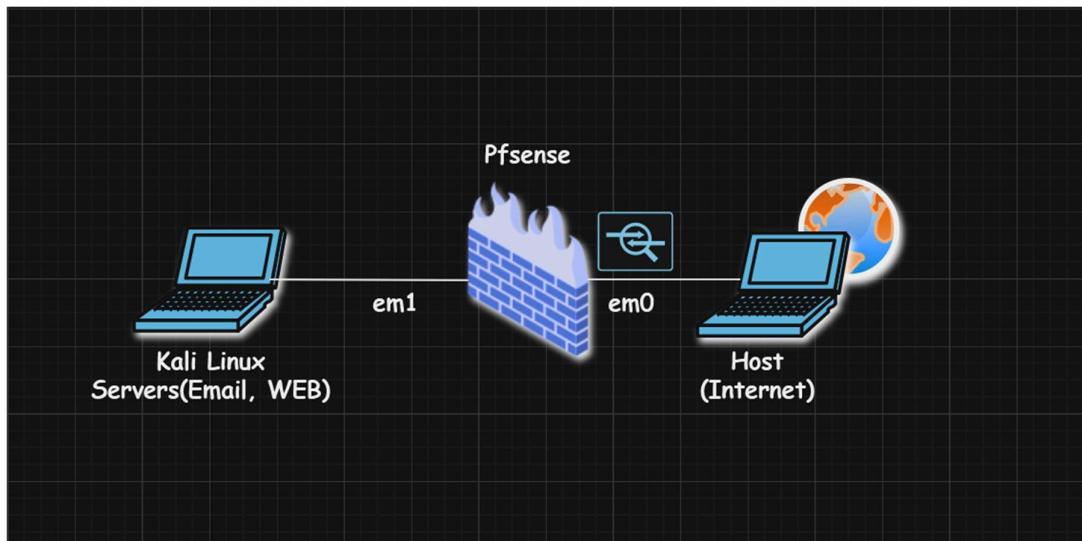
General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Automatic (DHCP)

```
(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

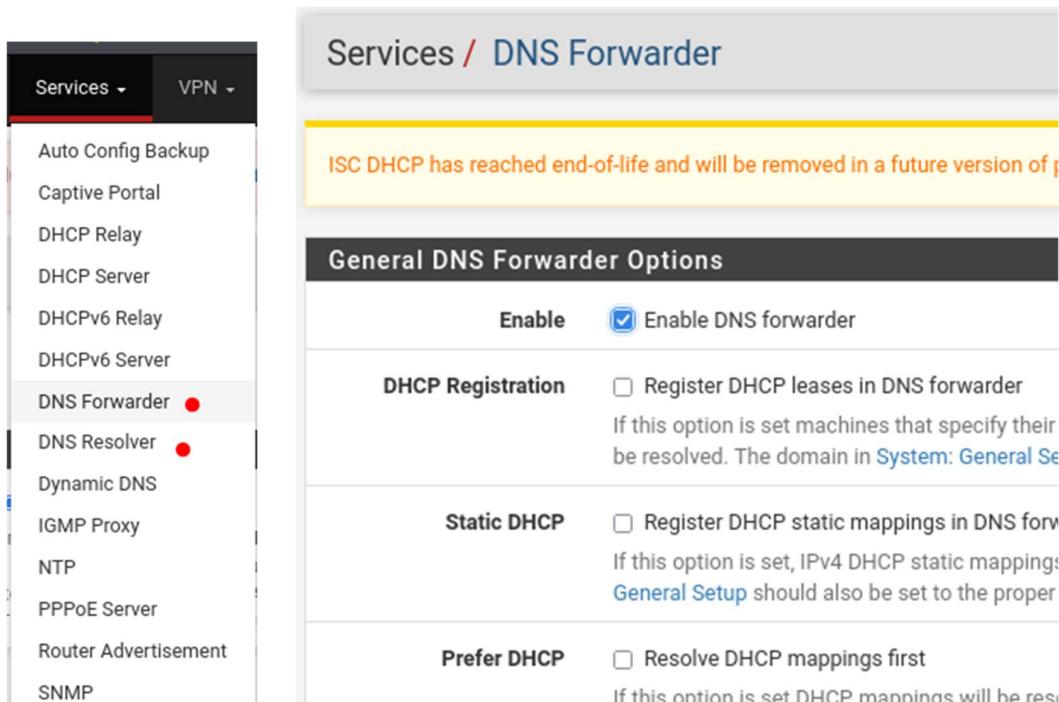
Neste cenário, para as máquinas de rede interna terem acesso ao mundo exterior (internet), tivemos que configurar o pfSense para servir como um gateway. A configuração de gateway está dividida em duas partes:

- 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 **nossa** 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

<input checked="" type="radio"/> Mode	Automatic outbound NAT rule generation. (IPsec passthrough included)	<input checked="" type="radio"/> Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	<input type="radio"/> Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	<input type="radio"/> 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	*	X		Edit Delete Toggle Save

Add **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	*	X	Auto created rule

[Info](#)

[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](#) / [24](#) [Port or Range](#)
Type Source network for the outbound NAT mapping.

Destination [Any](#) / [24](#) [Port or Range](#)
Type Destination network for the outbound NAT mapping.

Not
Invert the sense of the destination match.

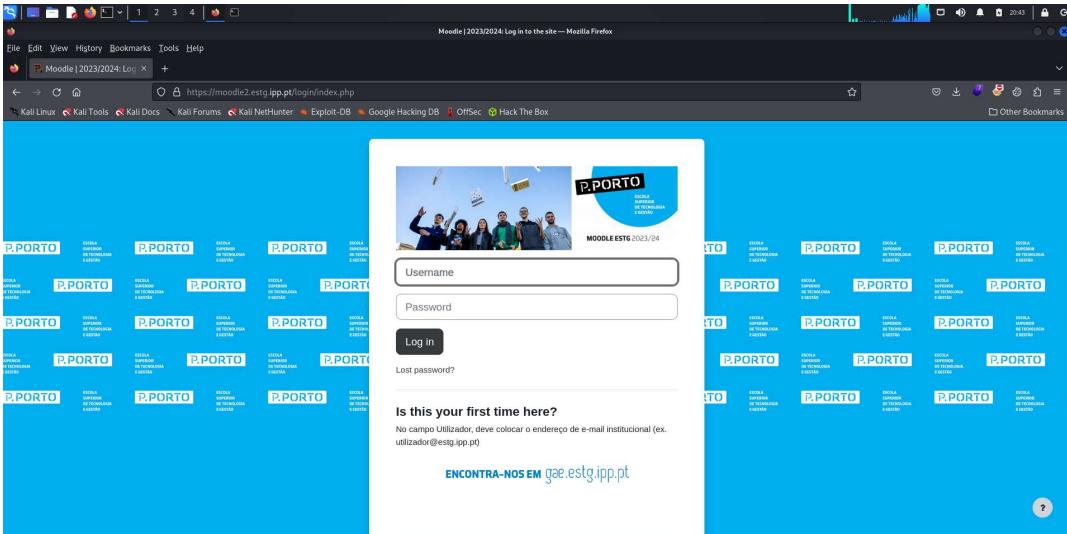
Translation

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 [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:

```
(kali㉿kali)-[~]
$ traceroute google.com
traceroute to google.com (142.250.184.14), 30 hops max, 60 byte packets
 1 pfsense.home.arp (10.120.59.1)  2.302 ms  2.172 ms  2.051 ms
 2 192.168.52.2 (192.168.52.2)  1.922 ms  1.837 ms  1.718 ms
```

2. Políticas de firewall

Protocolo	Interface 1		Interface 2	
	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:

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/494 KiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	2/9.29 MiB	IPv4	*	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6	*	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

2.1 Implementação das políticas LAN

Telnet

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	<input type="checkbox"/> 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	<input type="checkbox"/> 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.					

Outbound

Edit Firewall Rule

Action

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

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

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

Source

Invert match

10.120.59.1

/

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

/

Destination Port Range

Telnet (23)

Telnet (23)

From

Custom

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

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

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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	This Firewall (self)	Destination Address	/	
Destination Port Range	FTP (21)	From Custom	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	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Address or Alias	10.120.59.1	/	<input type="button" value="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	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button" value="Display Advanced"/>
Destination Port Range	From	Custom	To	Custom	
FTP (21)					
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	<input checked="" type="checkbox"/> 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	<input type="button" value="Display Advanced"/>

Ping

Inbound

Edit Firewall Rule

Action	<input type="button" value="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	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="LAN"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input type="button" value="ICMP"/>	Choose which IP protocol this rule should match.
ICMP Subtypes	<input type="button" value="Datagram conversion error"/> <input type="button" value="Echo reply"/> <input checked="" type="button" value="Echo request"/> <input type="button" value="Information reply"/>	
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.		
Source		
Source	<input type="checkbox"/> Invert match	<input type="button" value="Network"/> 10.120.59.0 / 24
Destination		
Destination	<input type="checkbox"/> Invert match	<input type="button" value="This Firewall (self)"/> Destination Address
Extra Options		
Log	<input checked="" type="checkbox"/> 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	<input type="text" value="Allow Ping 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.	

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	<input type="checkbox"/> 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	Echo request Information reply Information request IPv6, Iamhere	For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.
Source		
Source	<input type="checkbox"/> Invert match	Address or Alias /
Destination		
Destination	<input type="checkbox"/> Invert match	Any / Destination Address
Extra Options		
Log	<input checked="" type="checkbox"/> 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 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

Firewall / Rules / Edit

Edit Firewall Rule

Action	<input type="button" value="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	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="LAN"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match	<input type="text" value="Address or Alias"/> / <input type="text" value="10.120.59.1"/>
<input type="button" value="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	<input type="checkbox"/> Invert match	<input type="text" value="Any"/> / <input type="text" value="Destination Address"/>
Destination Port Range	<input type="button" value="SMTP (25)"/> From: <input type="text" value="Custom"/>	<input type="button" value="SMTP (25)"/> To: <input type="text" value="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	<input checked="" type="checkbox"/> 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	<input type="text" value="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

Edit Firewall Rule

<u>Action</u>	<input type="button" value="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.																		
<u>Disabled</u>	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.																		
<u>Interface</u>	<input type="button" value="LAN"/>	Choose the interface from which packets must come to match this rule.																		
<u>Address Family</u>	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.																		
<u>Protocol</u>	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match.																		
Source <table border="1"> <tr> <td><u>Source</u></td> <td><input type="checkbox"/> Invert match</td> <td><input type="button" value="Any"/></td> <td>Source Address</td> <td>/</td> <td><input type="checkbox"/></td> </tr> <tr> <td colspan="6" style="text-align: center;">Display Advanced</td> </tr> <tr> <td colspan="6">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.</td> </tr> </table>			<u>Source</u>	<input type="checkbox"/> Invert match	<input type="button" value="Any"/>	Source Address	/	<input type="checkbox"/>	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.					
<u>Source</u>	<input type="checkbox"/> Invert match	<input type="button" value="Any"/>	Source Address	/	<input type="checkbox"/>															
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 <table border="1"> <tr> <td><u>Destination</u></td> <td><input type="checkbox"/> Invert match</td> <td><input type="button" value="This Firewall (self)"/></td> <td>Destination Address</td> <td>/</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Destination Port Range</td> <td><input type="button" value="SMTP (25)"/></td> <td><input type="button" value="Custom"/></td> <td><input type="button" value="SMTP (25)"/></td> <td><input type="button" value="Custom"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>From</td> <td>Custom</td> <td>To</td> <td>Custom</td> <td colspan="2">Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port.</td> </tr> </table>			<u>Destination</u>	<input type="checkbox"/> Invert match	<input type="button" value="This Firewall (self)"/>	Destination Address	/	<input type="checkbox"/>	Destination Port Range	<input type="button" value="SMTP (25)"/>	<input type="button" value="Custom"/>	<input type="button" value="SMTP (25)"/>	<input type="button" value="Custom"/>	<input type="checkbox"/>	From	Custom	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.	
<u>Destination</u>	<input type="checkbox"/> Invert match	<input type="button" value="This Firewall (self)"/>	Destination Address	/	<input type="checkbox"/>															
Destination Port Range	<input type="button" value="SMTP (25)"/>	<input type="button" value="Custom"/>	<input type="button" value="SMTP (25)"/>	<input type="button" value="Custom"/>	<input type="checkbox"/>															
From	Custom	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 <table border="1"> <tr> <td><u>Log</u></td> <td><input checked="" type="checkbox"/> Log packets that are handled by this rule</td> <td>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).</td> </tr> <tr> <td><u>Description</u></td> <td colspan="2"><input type="button" value="Block all SMTP Inbound"/></td> <td>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.</td> </tr> </table>			<u>Log</u>	<input checked="" type="checkbox"/> 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).	<u>Description</u>	<input type="button" value="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.											
<u>Log</u>	<input checked="" type="checkbox"/> 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).																		
<u>Description</u>	<input type="button" value="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

The screenshot shows a 'Edit Firewall Rule' dialog with the following configuration:

- Action:** Block
- Disabled:** Disable this rule
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Invert match, Any, Source Address
- Destination:** Destination: This Firewall (self), Destination Port Range: Telnet (23) From: Custom To: Custom
- Extra Options:**
 - Log:** Log packets that are handled by this rule
 - Description:** Block all 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Any	Destination Address				
Destination Port Range	Telnet (23)	From	Custom	To	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	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Any	
<input type="button" value="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	<input type="checkbox"/> Invert match	This Firewall (self)	Destination Address
Destination Port Range	FTP (21)	From: Custom	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	<input checked="" type="checkbox"/> 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	<input type="button" value="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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	WAN address	Source Address
<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Invert match	Network	10.120.59.0
Destination Port Range	FTP (21)	From: Custom	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	<input checked="" type="checkbox"/> 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

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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match Any
Source Address /	
Destination	
Destination	<input type="checkbox"/> Invert match This Firewall (self)
Destination Address /	
Extra Options	
Log	<input checked="" type="checkbox"/> 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 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match
WAN address	Source Address
/	
Destination	
Destination	<input type="checkbox"/> Invert match
Any	Destination Address
/	
Extra Options	
Log	<input checked="" type="checkbox"/> 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

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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	This Firewall (self)	Destination Address
Destination Port Range	From	Custom	To
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	<input checked="" type="checkbox"/> 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 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.			

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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Any	Destination Address
Destination Port Range	SMTP (25)	From Custom	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	<input checked="" type="checkbox"/> 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.	
Display Advanced	

Web

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

The screenshot shows the 'Edit Firewall Rule' interface. The 'Action' dropdown is set to 'Pass'. The 'Interface' dropdown shows 'Any' selected, with options for WAN, LAN, and OpenVPN. The 'Direction' dropdown is set to 'any'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'TCP'. In the 'Source' section, the 'Source' dropdown is set to 'Any'. In the 'Destination' section, the 'Destination' dropdown is set to 'Any'. The 'Log' checkbox is checked, and the 'Description' field contains 'Allow all Web Traffic'. The 'Advanced Options' section has a 'Display Advanced' button.

Firewall / Rules / Floating / Edit

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.

Quick: Apply the action immediately on match.
Set this option to apply this action to traffic that matches this rule immediately.

Interface: Any
WAN
LAN
OpenVPN
Choose the Interface(s) for this rule.

Direction: any

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: HTTP (80) From: Custom 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 Web 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

3. Demonstação

3.1 Lista de todas as regras

LAN

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
<input checked="" type="checkbox"/>	0/6.95 MiB	*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	10.120.59.0/24	*	This Firewall (self)	*	*	*	none		
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.120.59.0/24	*	This Firewall (self)	21 (FTP)	*	none		Allow FTP from internal network	
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.120.59.1	*	*	21 (FTP)	*	none		Block all FTP outbound	
<input type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	10.120.59.1	*	*	*	*	*	none	Block all Ping outbound	
<input type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	10.120.59.0/24	*	This Firewall (self)	*	*	*	none	Block all Ping from firewall to LAN	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	This Firewall (self)	25 (SMTP)	*	none		Block all SMTP outbound	
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.120.59.1	*	*	25 (SMTP)	*	none		Allow SMTP outbound to all	
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.120.59.1	*	*	23 (Telnet)	*	none		Block all Telnet outbound	
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.120.59.0/24	*	*	23 (Telnet)	*	none		Allow Telnet from internal network	
<input type="checkbox"/>	0/103.18 MiB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

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
<input checked="" type="checkbox"/>	0/509 KIB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks.	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	This Firewall (self)	23 (Telnet)	*	none		Block all Telnet inbound	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	This Firewall (self)	21 (FTP)	*	none		Block all FTP inbound	
<input type="checkbox"/>	0/0 B	IPv4 TCP	WAN address	*	*	25 (SMTP)	*	none		Block all SMTP outbound	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	WAN address	*	10.120.59.0/24	21 (FTP)	*	none		Allow FTP outbound to Internal Network	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	WAN address	*	*	23 (Telnet)	*	none		Allow all Telnet outbound	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	This Firewall (self)	25 (SMTP)	*	none		Allow all SMTP inbound	
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	WAN address	*	*	*	*	none		Allow all Ping outbound	
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	*	*	This Firewall (self)	*	*	none		Allow all Ping inbound	
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	0/435 KIB	Any	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Allow all Web Traffic	

Add Add Delete Toggle Copy 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 interceptações, 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 intercepções. SMTP, quando usado na porta 25, não oferece criptografia por padrão, deixando as comunicações de email vulneráveis a ataques de intercepção 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.

Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: ● openvpn-client-export-2.6.7 ● openvpn-2.6.8_1 ● zip-3.0_1 ● 7-zip-23.01	
✓ snort	security	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	

- 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.

Oinkcode

9bc25c72ede5cfbc84c2a823578b990503d21068

Regenerate

Configuração

- Na barra superior, clique em Services > Snort > Global Settings

The screenshot shows the pfSense Package Manager interface. The left sidebar has 'System / Package Manager / Installed Packages'. The main area shows a table of installed packages:

Name	Category	Version	Description
openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN profiles.
snort	security	4.1.6_17	Snort is an open source network protocol analyzer, and anomaly detection system (IDS/IPS). Combining the benefits of signature,

Actions column includes icons for Remove, Information, and Reinstall. A note at the bottom says 'Newer version available'.

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

The screenshot shows the Snort Global Settings page. The 'Global Settings' tab is selected. Under 'Snort Subscriber Rules', there is a checkbox 'Enable Snort VRT' which is checked. Below it, there is a text input field labeled 'Snort Oinkmaster Code' containing the value '9bc25c72ede5cfbc84c2a823578b990503d21068'. Under 'Snort GPLv2 Community Rules', there is a checkbox 'Enable Snort GPLv2' which is unchecked. Under 'Emerging Threats (ET) Rules', there is a checkbox 'Enable ET Open' which is checked.

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

Snort Subscriber Rules	
Enable Snort VRT	<input checked="" type="checkbox"/> 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	9bc25c72ede5cfbc84c2a823578b990503d21068 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	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.	
Enable ET Pro	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account ETPro for Snort offers daily updates and extensive coverage of current malware threats.	
Sourcefire OpenAppID Detectors	
Enable OpenAppID	<input checked="" type="checkbox"/> 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	Installed Detection Package Version=366
Enable AppID Open Text Rules	<input checked="" type="checkbox"/> 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 .	
FEODO Tracker Botnet C2 IP Rules	
Enable FEODO Tracker Botnet C2 IP Rules	<input checked="" type="checkbox"/> Click to enable download of FEODO Tracker Botnet C2 IP rules
Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cride, Dridex, Geodo, Heodo and Fmotel.	

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

Rules Update Settings	
Update Interval	12 HOURS
Please select the interval for rule updates. Choosing NEVER disables auto-updates.	
Update Start Time	00:05
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	<input type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> 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	NEVER
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	<input type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.
<input type="button" value="Save"/>	

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

General Settings

Remove Blocked Hosts Interval	NEVER	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	<input type="checkbox"/>	Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/>	Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input type="checkbox"/>	Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

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

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	48387e5c523c486fdf3384ff5fec57ab9	Friday, 14-Jun-24 00:06:44 UTC
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	93617a718ee7b27cc2597c6558be159f	Friday, 14-Jun-24 00:06:44 UTC
Snort OpenApplD Detectors	c726cf937d84c651a20f2ac7c528384e	Monday, 20-May-24 16:21:13 UTC
Snort ApplID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Monday, 20-May-24 16:21:13 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update	Jun-14 2024 15:12	Result: Success
Update Rules	<input checked="" type="checkbox"/> Update Rules	<input type="button" value="Force Update"/>

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

- 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

Services / Snort / WAN - Interface Settings

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.)

Alert Settings

- Send Alerts to System Log: Snort will send Alerts to the firewall's system log. Default is Not Checked.
- Enable Packet Captures: Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
- Enable Unified2 Logging: Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

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

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.

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

Services / Snort / Interfaces

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
WAN (em0)	X ↻	AC-BNFA	DISABLED	WAN	Edit Delete

Actions: + Add Delete

- 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.

All rule categories have been de-selected. There currently are no inspection rules enabled for this Snort instance.

Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
WAN Settings	WAN Categories	WAN Rules	WAN Variables	WAN Preprocs	WAN IP Rep	WAN Logs				

Automatic Flowbit Resolution

Resolve Flowbits If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets (Categories) Snort will load at startup

Green icon - Category is auto-enabled by SID Mgmt conf files
Red icon - Category is auto-disabled by SID Mgmt conf files

Select All **Unselect All** **Save**

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Enable	Ruleset: Snort OPENAPPID Rules
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	<input type="checkbox"/>	openappid-ads.rules
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	<input type="checkbox"/>	openappid-browser_plugin.rules
<input type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-other.so.rules	<input type="checkbox"/>	openappid-business_applications.rules
<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	<input type="checkbox"/>	openappid-collaboration.rules
<input type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	<input type="checkbox"/>	openappid-database.rules
<input type="checkbox"/>	emerging-clarmy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-executable.so.rules	<input type="checkbox"/>	openappid-file_storage.rules

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

Stream5 Target-Based Stream Reassembly

Enable Use Stream5 session reassembly for TCP, UDP and/or ICMP traffic. Default is Checked.

Flush On Alert Flush a TCP stream when an alert is generated on that stream (for backwards compatibility). Default is Not Checked.

Prune Log Max 1048576
Prune Log Max Bytes. Minimum is 0 (disabled), or if not disabled, 1024. Maximum is 1073741824. Default is 1048576 (1 MB).
Logs a message when a session terminates that was using more than the specified number of bytes.

Protocol Tracking
 Track and reassemble TCP sessions. Default is Checked.
 Track and reassemble UDP sessions. Default is Checked.
 Track and reassemble ICMP sessions. Default is Not Checked.
 Toggle All

Maximum TCP Sessions 262144
Maximum number of concurrent TCP sessions that will be tracked. Min is 1 and max is 1048576. Default is 262144.

TCP Memory Cap 8388608
Memory (in bytes) for TCP packet storage. Min is 32768 and max is 1073741824 (1 GB). Default is 8388608 (8 MB).

Maximum UDP Sessions 131072
Maximum number of concurrent UDP sessions that will be tracked. Min is 1 and max is 131072. Default is 131072.

UDP Session Timeout 30
UDP Session timeout in seconds. Min is 1 and max is 86400 (1 day). Default is 30.

- Por fim, demos start na interface WAN do Snort

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
WAN (em0)	✓ C @	AC-BNFA	DISABLED	WAN	Edit Delete Sync

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”:

Services / Snort / Interface Settings / WAN - Rules

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Available Rule Categories

Category Selection: Active Rules Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Rules View Filter

Selected Category's Rules

Legend: ✓ Default Enabled ✓ Enabled by user ● Auto-enabled by SID Mgmt ● Action/content modified by SID Mgmt ⚠ Rule action is alert
✗ Default Disabled ✗ Disabled by user ● Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	⚠	2	1						TAG_LOG_PKT
✓	⚠	105	4						BO_SNORT_BUFFER_ATTACK
✓	⚠	105	3						BO_SERVER_TRAFFIC_DETECT
✓	⚠	105	2						BO_CLIENT_TRAFFIC_DETECT
✓	⚠	105	1						BO_TRAFFIC_DETECT
✓	⚠	106	5						RPC_ZERO_LENGTH_FRAGMETN
✓	⚠	106	4						RPC_INCOMPLETE_SEGMENT
✓	⚠	106	3						RPC_LARGE_FRAGSIZE
✓	⚠	106	2						RPC_MULTIPLE_RECORD
✓	⚠	106	1						RPC_FRAG_TRAFFIC
✓	⚠	116	467						DECODE_FPATH_HDR_TRUNC
✓	⚠	116	466						DECODE_AUTH_HDR_BAD_LENGTH

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.

View Rules Text

Category	Active Rules
GID:SID	116:1
Rule Text	<pre>alert (msg:"DECODE_NOT_IPV4_DGRAM"; sid:1; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)</pre>

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*.

View Rules Text

Category	Active Rules
GID:SID	105:4
Rule Text	<pre>alert (msg: "BO_SNORT_BUFFER_ATTACK"; sid: 4; gid: 105; rev: 2; metadata: policy max-detect-ips drop, rule-type preproc, policy balanced-ips drop, policy security-ips drop ; classtype:trojan-activity; reference:cve,2005-3252;)</pre>

[Close](#)

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

View Rules Text

Category	Active Rules
GID:SID	106:4
Rule Text	<pre>alert (msg: "RPC_INCOMPLETE_SEGMENT"; sid: 4; gid: 106; rev: 2; metadata: policy max-detect-ips drop, rule-type preproc, service sunrpc, policy security-ips alert ; classtype:bad-unknown;)</pre>

[Close](#)

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.

Services / Snort / Interface Settings / WAN - Rules

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Available Rule Categories

Category Selection: Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Rules View Filter

Selected Category's Rules

Legend:

- Default Enabled
- Enabled by user
- Auto-enabled by SID Mgmt
- Action/content modified by SID Mgmt
- Rule action is alert
- Default Disabled
- Disabled by user
- Auto-disabled by SID Mgmt

State	Action	GID	SID	Classification	IPS Policy	Message
<input checked="" type="checkbox"/>	!	2	1	not-suspicious	none	TAG_LOG_PKT
<input checked="" type="checkbox"/>	!	105	4	trojan-activity	max-detect-ips balanced-ips security-ips	BO_SNORT_BUFFER_ATTACK
<input checked="" type="checkbox"/>	!	105	3	trojan-activity	max-detect-ips balanced-ips security-ips	BO_SERVER_TRAFFIC_DETECT
<input checked="" type="checkbox"/>	!	105	2	trojan-activity	max-detect-ips balanced-ips security-ips	BO_CLIENT_TRAFFIC_DETECT
<input checked="" type="checkbox"/>	!	105	1	trojan-activity	max-detect-ips balanced-ips security-ips	BO_TRAFFIC_DETECT
<input checked="" type="checkbox"/>	!	106	5	bad-unknown	max-detect-ips	RPC_ZERO_LENGTH_FRAGMENT
<input checked="" type="checkbox"/>	!	106	4	bad-unknown	max-detect-ips	RPC_INCOMPLETE_SEGMENT
<input checked="" type="checkbox"/>	!	106	3	bad-unknown	max-detect-ips	RPC_LARGE_FRAGSIZE
<input checked="" type="checkbox"/>	!	106	2	protocol-command-decode	max-detect-ips	RPC_MULTIPLE_RECORD
<input checked="" type="checkbox"/>	!	106	1	protocol-command-decode	max-detect-ips	RPC_FRAG_TRAFFIC
<input checked="" type="checkbox"/>	!	119	35	unknown	max-detect-ips	HLCLIENT_MULTIPLE_COLON_BETN_KEY_VALUE
<input checked="" type="checkbox"/>	!	119	34	unknown	max-detect-ips	HLCLIENT_PIPELINE_MAX
<input checked="" type="checkbox"/>	!	119	33	unknown	max-detect-ips	HLCLIENT_UNESCAPED_SPACE_IN_URI
<input checked="" type="checkbox"/>	!	119	32	unknown	max-detect-ips	HLCLIENT_SIMPLE_REQUEST

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 variável 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 facilitar 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 tráfego, 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 variável 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 facilitar 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
```

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Available Rule Categories

Category Selection: custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
drop icmp any any -> $HOME_NET any (msg:"ICMP Ping Blocked"; sid:1000002; rev:1; classtype:icmp-event;)
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping detected"; sid:1000001; rev:1; classtype:icmp-event;)
```

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:

```
C:\Windows\System32>ping 192.168.1.224

Pinging 192.168.1.224 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.224:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\System32>
```

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

The screenshot shows the pfSense web interface with the following details:

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Alert Log View Settings:**
 - Interface to Inspect: WAN (em0)
 - Auto-refresh view: checked
 - Choose interface: Choose interface..
 - Alert lines to display: 250
 - Save button
- Alert Log Actions:** Download, Clear.
- Alert Log View Filter:** A search bar with a plus sign (+).
- Table:** Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-06-14 19:30:57	⚠️	3	ICMP	Generic ICMP event	192.168.1.1		192.168.1.224		1:1000001	ICMP Ping detected
2024-06-14 19:30:57	⚠️	3	ICMP	Generic ICMP event	192.168.1.1		192.168.1.224		1:1000002	ICMP Ping Blocked
2024-06-14 19:30:57	⚠️	3	ICMP	Generic ICMP event	192.168.1.224		192.168.1.1		1:1000001	ICMP Ping detected
2024-06-14 19:30:57	⚠️	3	ICMP	Generic ICMP event	192.168.1.224		192.168.1.1		1:1000002	ICMP Ping Blocked
2024-06-14 19:30:57	⚠️	3	ICMP	Generic ICMP event	192.168.1.1		192.168.1.224		1:1000001	ICMP Ping detected

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, seguimos 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:1000003: 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_header);
```

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>