

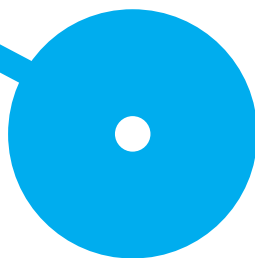
LSIRC

LICENCIATURE EM SEGURANÇA INFORMÁTICA EM
REDES DE COMPUTADORES

Análise e Configuração de uma Firewall com pfSense e Sistema IDS/IPS Snort

Pedro Antunes

MAIO, 2025



Análise e Configuração de uma Firewall com pfSense e Sistema IDS/IPS Snort

Segurança De Redes

Pedro Antunes

8230068

Professores

Silvestre Malta

João Oliveira

Resumo

Este relatório descreve a análise, configuração e testes de uma *firewall* baseada no sistema *pfSense*, no âmbito da unidade curricular de Segurança de Redes. O objetivo principal foi implementar políticas de controlo de tráfego, reforçando a segurança de uma rede simulada composta por máquinas virtuais.

Para isso, foram definidas regras personalizadas nas interfaces *LAN* e *WAN* da *firewall*, testando diferentes protocolos como *HTTP*, *FTP*, *Telnet* e *ICMP*. Adicionalmente, foi integrado o sistema *IDS/IPS Snort* para deteção e bloqueio de tráfego malicioso. Os testes práticos demonstraram a eficácia das políticas aplicadas e das funcionalidades de prevenção de intrusões, permitindo validar o funcionamento da infraestrutura em ambiente virtual.

Índice

Resumo	iii
Índice.....	iv
Índice de figuras.....	vii
Índice de tabelas	ix
Acrónimos e abreviaturas	x
1. Introdução	1
2. Planeamento das Políticas de Segurança	2
2.1. Objetivo da Firewall.....	2
2.2. Regras Definidas	2
2.3. Estratégia de Verificação das Regras.....	3
3. Preparação do Cenário com Máquinas Virtuais	4
3.1. Ferramenta de Virtualização	4
3.2. Configuração da Máquina Virtual - PFSense (Firewall)	4
3.3. Configuração da Máquina Virtual - Servidor Linux.....	4
3.4. Comunicação entre Máquinas.....	5
3.5. Testes de Conectividade Inicial.....	5
3.6. Desenho da Arquitetura da Implementação	6
3.7. Desenho pormenorizado da implementação	7
3.8. Funcionamento do Gateway	7
4. Configuração da Firewall	9
4.1. Tabela – Regras da Interface LAN (Interface 1)	10
4.1.1. Telnet (Porta 23)	11
4.1.2. FTP (Porta 21).....	12
4.1.3. Ping (ICMP).....	14

4.1.4.	Web (HTTP – Porta 80).....	17
4.1.5.	Email (SMTP – porta 25).....	18
4.2.	Tabela – Regras na Interface WAN (Interface 2)	20
4.2.1.	Bloquear ICMP (Ping) vindo do exterior	21
4.2.2.	Bloquear FTP (porta 21) e Telnet (porta 23) do exterior	21
4.2.3.	Bloquear Acesso à LAN desde o exterior	22
5.	Demonstração	24
5.1.	Listagem de todas as regras da firewall.....	24
5.1.1.	Regras LAN	24
5.1.2.	Regras WAN	25
5.2.	Demonstração do Funcionamento das Políticas	25
5.2.1.	Tabela de testes – Funcionamento das políticas	26
5.3.	Testes Realizados	27
5.3.1.	Teste 1 - Permitir ping da LAN para a firewall	27
5.3.2.	Teste 2 – Bloquear ping da LAN para a internet	27
5.3.3.	Teste 3 – Bloquear Telnet para o exterior	28
5.3.4.	Permitir Telnet interno (entre máquinas LAN)	28
5.3.5.	Teste 5 – Bloquear FTP de saída	28
5.3.6.	Teste 6 – Permitir HTTP (Web) para o exterior	29
5.3.7.	Bloquear ICMP à firewall (WAN).....	29
5.3.8.	Permitir DNS para fora	30
5.4.	Identificação de Protocolos Inseguros e Propostas de Melhoria	30
6.	IPS/IDS - Integração de um sistema de deteção/prevenção de intrusões.....	32
6.1.	Configuração do Snort	32
6.1.1.	Análise do funcionamento do IPS	34
6.2.	Análise das assinaturas existentes	35

6.2.1.	Regra ICMP – Detecção de ping externos	36
6.2.2.	Regra Scan – FTP Brute Force	37
6.2.3.	Regra Scan – NMAP TCP SYN Scan	38
6.3.	Alerta bloqueio para tráfego ICMP externo (criação da regra)	39
6.3.1.	Teste e evidência do bloqueio de tráfego ICMP externo (ping)	40
6.4.	Alerta para acesso a página com referência à palavra "Adult"	41
6.4.1.	Teste Realizado	42
7.	Conclusão	43
	Referências	44

Índice de figuras

Figura 1 - Configuração IP firewall	5
Figura 2 - Ping conectividad	5
Figura 3 - Acesso Browser Firewall	6
Figura 4 - Topologia da rede	7
Figura 5- Ping bem-sucedido para 8.8.8.8	8
Figura 6- Traceroute 8.8.8.8	8
Figura 7 - Configuração regra Telnet	11
Figura 8 - Bloquear telnet	12
Figura 9- Permiti FTP	13
Figura 10 - Bloquear FTP	14
Figura 11 - Permitir ICMP	15
Figura 12 - Bloquear ICMP	16
Figura 13 - Permitir HTTP	17
Figura 14 – Bloquear SMTP	18
Figura 15 - Permitir SMTP	19
Figura 16 - Bloquear ICMP (WAN)	21
Figura 17 - Bloquear FTP e Telnet	22
Figura 18 - Bloquear acesso à LAN	23
Figura 19 - Regras Aplicadas na LAN	24
Figura 20 - Regras Aplicadas na WAN	25
Figura 21 - Ping LAN para a firewall	27
Figura 22 - Ping para a internet	27
Figura 23 – Teste telnet Exterior	28
Figura 24 - Permitir telnet interno	28
Figura 25 - Ftp para fora da LAN	28
Figura 26 - Permitir HTTP exterior	29
Figura 27 - Firewall bloqueia ICMP	29
Figura 28 - Resolver DNS	30
Figura 29 - Instalação do Snort	32
Figura 30 - Configuração Snort	33

Figura 31 - Update das Rules	34
Figura 32 - Interface WAN ativada.....	34
Figura 33 - Analise funcionamento IPS	35
Figura 34 - Detecção pings externos	36
Figura 35- FTP Brute Force.....	37
Figura 36 - NMAP TCP SYN Scan	38
Figura 37 - Ping Máquina externa.....	40
Figura 38- Alerta ICMP	40
Figura 39 - Alerta Adult.....	41
Figura 40 - Teste "Adult"	42
Figura 41 - Alerta conteudo "Adult"	42

Índice de tabelas

Tabela 1 - Regras LAN10

Tabela 2 - Regras Interface WAN20

Tabela 3 - Protocolos Inseguros.....30

Tabela 4 - Proposta alteração31

Tabela 5 - WAN Rules analisadas.....35

Acrónimos e abreviaturas

LAN – Local Area Network: rede local que interliga dispositivos dentro de uma área limitada, como uma sala ou edifício.

WAN – Wide Area Network: rede de longa distância, como a Internet, que conecta dispositivos em diferentes localizações geográficas.

DHCP – Dynamic Host Configuration Protocol: protocolo que atribui automaticamente endereços IP a dispositivos numa rede.

IP – Internet Protocol: protocolo responsável pelo endereçamento e roteamento de pacotes na rede.

ICMP – Internet Control Message Protocol: protocolo usado para enviar mensagens de erro e diagnóstico (ex: ping).

HTTP – Hypertext Transfer Protocol: protocolo para comunicação web (ex: acesso a sites).

FTP – File Transfer Protocol: protocolo para transferência de ficheiros.

SMTP – Simple Mail Transfer Protocol: protocolo para envio de e-mails.

IDS – Intrusion Detection System: sistema que deteta possíveis intrusões na rede.

IPS – Intrusion Prevention System: sistema que além de detetar, bloqueia tráfego malicioso.

DNS – Domain Name System: sistema que traduz nomes de domínios (ex: google.com) para endereços IP.

SSH – Secure Shell: protocolo seguro para acesso remoto a dispositivos.

VM – Virtual Machine: máquina virtual usada para simular ambientes operacionais.

NAT – Network Address Translation: técnica usada para permitir que vários dispositivos partilhem um único IP público.

pfSense – software open-source baseado em FreeBSD, usado como firewall e router.

Snort – ferramenta IDS/IPS open-source utilizada para deteção e bloqueio de tráfego suspeito.

Nmap – ferramenta de varrimento de rede usada para descobrir dispositivos e serviços ativos.

1. Introdução

Este trabalho prático tem como objetivo a configuração de uma firewall utilizando o PFSense, bem como a implementação de um sistema de deteção e prevenção de intrusões (Snort), num cenário de rede virtualizado. A atividade foi desenvolvida no âmbito da unidade curricular de Segurança de Redes, recorrendo a máquinas virtuais para simular um ambiente com rede interna, firewall e ligação ao exterior.

Através deste projeto pretende-se aplicar conhecimentos teóricos sobre políticas de segurança, controlo de tráfego e análise de pacotes, com o intuito de proteger os serviços internos contra acessos não autorizados e identificar potenciais ameaças. Durante o desenvolvimento foram seguidas as diretrizes fornecidas no enunciado, definindo-se regras de firewall específicas, testando o seu funcionamento, e configurando o Snort para gerar alertas com base em tráfego suspeito.

2. Planeamento das Políticas de Segurança

Antes de avançar para a parte prática da configuração da firewall, foi necessário decidir se ia manter as regras que o *PFSense* já traz por defeito ou se ia criar as minhas próprias regras. Optei por criar regras personalizadas, pois considero que isso me dá mais controlo sobre a rede, além de permitir cumprir melhor os objetivos do trabalho e as situações descritas no enunciado. Assim, consegui adaptar as regras ao cenário específico que construí.

2.1. Objetivo da Firewall

A firewall tem como principal função proteger os serviços e dispositivos da rede interna contra acessos não autorizados, especialmente tráfego vindo do exterior. Ao mesmo tempo, deve permitir que os utilizadores internos acessem serviços essenciais da Internet, como navegar em páginas web ou resolver nomes DNS. A política usada baseia-se no princípio do **“tudo é bloqueado, a não ser que seja explicitamente permitido”**, garantindo assim uma abordagem mais segura.

2.2. Regras Definidas

Com base nos objetivos, defini as seguintes regras principais que iriam ser implementadas na firewall:

- **Permitir tráfego HTTP e HTTPS da LAN para a Internet** – para permitir que os utilizadores internos possam navegar normalmente.
- **Permitir tráfego DNS da LAN para a Internet** – para garantir que é possível fazer resolução de nomes (ex: google.com → IP).
- **Permitir tráfego SSH entre máquinas da rede interna** – para permitir administração remota de forma segura.
- **Bloquear tráfego não solicitado vindo da Internet para a LAN** – para impedir tentativas de ligação externas não autorizadas.
- **Bloquear tráfego ICMP vindo do exterior (host externo)** – para evitar que a firewall responda a *pings* externos.
- **Permitir acesso à interface de gestão da firewall a partir da LAN** – necessário para configuração e manutenção via browser (HTTPS).

Estas regras serão configuradas manualmente na interface do *PFSense*.

2.3. Estratégia de Verificação das Regras

Para garantir que as regras estão realmente a funcionar como esperado, planeei realizar vários testes práticos depois da configuração. Alguns dos testes planeados foram:

- **Navegação web:** aceder a sites via browser para testar *HTTP/HTTPS*;
- **Testes de DNS:** usar o comando *nslookup* para ver se os nomes estão a ser resolvidos corretamente;
- **Pings externos:** tentar fazer *ping* à firewall a partir de uma máquina fora da rede para confirmar que o ICMP está bloqueado;
- **Testes internos:** usar *ping* e *ssh* entre máquinas internas para confirmar que a comunicação local está a funcionar;
- **Testes de serviços bloqueados:** tentar usar *telnet* em portas não autorizadas e verificar se são efetivamente bloqueadas

Os resultados destes testes serão apresentados mais à frente neste relatório.

3. Preparação do Cenário com Máquinas Virtuais

3.1. Ferramenta de Virtualização

Para a realização deste trabalho foi utilizada a ferramenta de virtualização **VirtualBox**, por ser gratuita, leve e bastante intuitiva. Permitiu criar e configurar facilmente o ambiente necessário para simular uma rede com firewall, servidor interno e tráfego externo.

3.2. Configuração da Máquina Virtual - PFSense (Firewall)

Foi criada uma máquina virtual com o sistema *PFSense*, que irá funcionar como firewall e gateway da rede. A instalação foi feita a partir da imagem ISO oficial (.iso).

Configuração da VM:

- **Sistema:** BSD → FreeBSD (64-bit)
- **RAM:** 1024 MB
- **Disco:** 8 GB (VDI, dinamicamente alocado)
- **Placas de rede:**
 - **Adaptador 1 (WAN):** ligado à rede NAT (simula a Internet)
 - **Adaptador 2 (LAN):** ligado a uma Rede Interna com o nome *intnet*

3.3. Configuração da Máquina Virtual - Servidor Linux

Foi também criada uma segunda máquina virtual com *Kali Linux*, que simula o servidor interno da empresa (*WEB / Email*).

Não foi necessária a instalação de serviços, sendo suficiente para testar regras da firewall e realizar acessos de rede.

Configuração da VM:

- **Sistema:** Linux → Debian (64-bit)
- **RAM:** 1024 MB
- **Disco:** 10 GB
- **Placa de rede:**
 - **Adaptador 1:** ligado à mesma Rede Interna (*intnet*) da firewall

3.4. Comunicação entre Máquinas

Após a instalação, a máquina Kali obteve automaticamente um IP atribuído pela firewall via DHCP.

Foi então possível testar a conectividade básica entre as duas VMs (ping da Kali para a firewall), e aceder à interface de gestão do *PFsense* através do browser (<https://192.168.1.1>), validando que o cenário estava funcional e corretamente montado.

3.5. Testes de Conectividade Inicial

Para garantir que as máquinas estavam a comunicar entre si realizem testes de conectividade entre a máquina *kali Linux* e o *PFsense*:

- Configuração na firewall:

Figura 1 - Configuração IP firewall

- Ping da máquina Kali para a firewall (IP da LAN):

```
ping 10.120.59.1
```

```
(kali㉿kali)-[~]
$ ping 10.120.59.1
PING 10.120.59.1 (10.120.59.1) 56(84) bytes of data.
64 bytes from 10.120.59.1: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 10.120.59.1: icmp_seq=2 ttl=64 time=0.847 ms
64 bytes from 10.120.59.1: icmp_seq=3 ttl=64 time=0.782 ms
64 bytes from 10.120.59.1: icmp_seq=4 ttl=64 time=0.763 ms
64 bytes from 10.120.59.1: icmp_seq=5 ttl=64 time=0.637 ms
^C
— 10.120.59.1 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4090ms
rtt min/avg/max/mdev = 0.637/0.844/1.194/0.187 ms
```

Figura 2 - Ping conectividad

- Acesso via web browser:

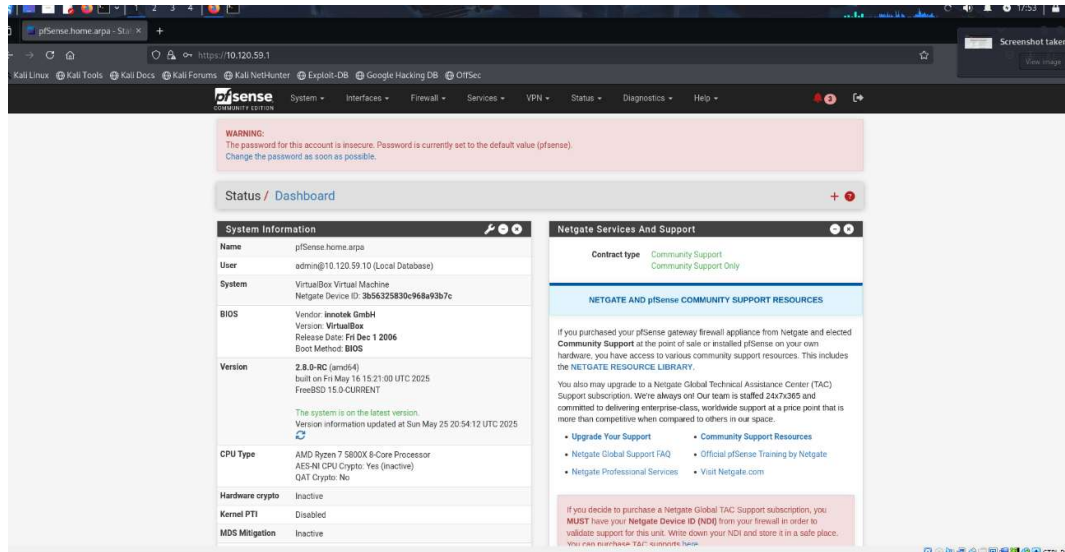


Figura 3 - Acesso Browser Firewall

Através destes testes foi possível confirmar que a máquina *Kali* está corretamente ligada à rede interna, com comunicação ativa com a *firewall*, validando a funcionalidade básica do cenário.

3.6. Desenho da Arquitetura da Implementação

O cenário foi implementado com recurso a máquinas virtuais criadas no *VirtualBox*, representando uma rede interna protegida por uma firewall. Foram utilizadas três VMs principais: uma com o *PFsense* (a *firewall*), uma com uma distribuição Linux (*Kali*), que simula um servidor WEB/Email interno, e uma terceira máquina com Kali Linux para simular um *host externo*.

A firewall (*PFsense*) foi configurada com duas interfaces de rede:

- **WAN (em0):** ligada à rede *NAT* do *VirtualBox*, simula a ligação ao exterior (Internet). Recebeu automaticamente o IP 10.0.2.15/24 via DHCP.
- **LAN (em1):** ligada à Rede Interna (nome: *LAN* no *VirtualBox*). Foi atribuída manualmente com o IP 10.120.59.1/24, de acordo com o endereçamento fornecido no enunciado.

A segunda máquina virtual, com Kali Linux, está ligada à mesma Rede Interna (LAN) e representa o servidor da empresa. Esta máquina recebeu o IP 10.120.59.10 manualmente

(numa fase inicial, devido a falhas no *DHCP*) e é utilizada para validar o funcionamento da *firewall*, aceder à *interface* web do *PFsense* e realizar testes de comunicação.

A terceira máquina virtual, também com Kali Linux, foi criada para representar um *host externo*. Está ligada à rede *NAT* (a mesma da interface *WAN* da *firewall*), permitindo simular tráfego vindo do exterior. Esta máquina foi utilizada para testar bloqueios de tráfego *ICMP*, tentativas de acesso a serviços internos e gerar eventos de alerta no sistema de deteção de intrusões (*Snort*).

A comunicação entre as *VMs* é feita através das redes configuradas: a *Rede Interna* isola a rede da empresa, enquanto a *NAT* permite simular a ligação à Internet. Este cenário garante separação clara entre interior e exterior, permitindo aplicar e testar regras de segurança em ambiente controlado.

3.7. Desenho pormenorizado da implementação

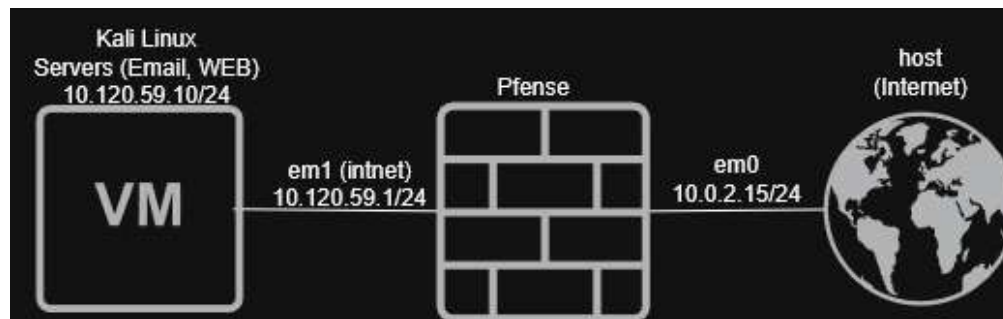


Figura 4 - Topologia da rede

3.8. Funcionamento do Gateway

Para validar o funcionamento do *pfSense* como *gateway*, foi atribuída à máquina da *LAN* o *IP* 10.120.59.10 com *gateway* 10.120.59.1.

Foi realizado um teste de *ping 8.8.8.8*, que respondeu corretamente, provando que o tráfego da *LAN* é corretamente encaminhado para a Internet via o *pfSense*.

Adicionalmente, a tabela de rotas (*ip route*) mostra o *gateway* como *default* via 10.120.59.1, confirmando o papel do *pfSense* como ponto de saída da rede interna.

Captura do ping bem-sucedido para 8.8.8.8

```
(kali@kali)-[~]
$ sudo ip route add default via 10.120.59.1
[sudo] password for kali:

(kali@kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=18.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=18.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=18.2 ms
^C
  8.8.8.8 ping statistics:
  4 packets transmitted, 4 received, 0% packet loss, time 3015ms
 rtt min/avg/max/mdev = 18.157/18.290/18.520/0.143 ms

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.120.59.10/24 scope global eth0
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:de:b3:cd:44 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

Figura 5- Ping bem-sucedido para 8.8.8.8

- Serve como prova que o tráfego sai da LAN, passa pelo *pfSense(gateway)*, e chega à internet.

Captura traceroute 8.8.8.8

```
(kali@kali)-[~]
$ ip route
default via 10.120.59.1 dev eth0
10.120.59.0/24 dev eth0 proto kernel scope link src 10.120.59.10
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
```

Figura 6- Traceroute 8.8.8.8

- Para mostrar que a rota padrão (default via) passa pelo *pfSense*.

4. Configuração da Firewall

Para controlar o tráfego entre a rede interna e o exterior, foram definidas várias regras na firewall (*PFSense*), com base nos princípios de segurança mínimos e nos requisitos do cenário. A configuração foi feita através do menu *Firewall > Rules*, aplicando regras distintas para as interfaces *LAN* e *WAN*.

4.1. Tabela – Regras da Interface LAN (Interface 1)

Tabela 1 - Regras LAN

Protocolo	Direção	Permitido?	Origem	Destino	Porta	Observações
Telnet	Inbound	Sim	LAN net	LAN net	23	Permitir dentro da rede interna
	Outbound	Não	LAN net	any (exceto LAN)	23	Bloquear saída para fora
FTP	Inbound	Sim	LAN net	LAN net	21	Permitir dentro da rede interna
	Outbound	Não	LAN net	any (exceto LAN)	21	Bloquear saída para fora
Ping (ICMP)	Inbound	Sim	LAN net	LAN net	ICMP	Permitir pings internos
	Outbound	Não	LAN net	any (exceto LAN)	ICMP	Bloquear pings externos
Web (HTTP)	Inbound	Sim	LAN net	any	80	Permitir navegação de saída para a Internet
	Outbound	Sim	LAN net	any	80	
Email (SMTP)	Inbound	Não	any	LAN net	25	Bloquear recepção de emails
	Outbound	Sim	LAN net	any	25	Permitir envio de emails para o exterior

4.1.1. Telnet (Porta 23)

Duas regras foram configuradas para controlar o uso de Telnet:

- Uma para permitir comunicações internas dentro da *LAN* (entre máquinas com IP 10.120.59.X)
- Outra para bloquear qualquer tentativa de acesso externo via *Telnet*, evitando comunicações inseguras com a Internet

Esta abordagem garante conformidade com o enunciado e protege a rede de ligações não cifradas para fora.

REGRA 1 -Permitir Telnet dentro da rede interna

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 /
 [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 /

Destination Port Range
 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 label and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Figura 7 - Configuração regra Telnet

REGRA 2 -Bloquear Telnet de saída (para fora da LAN)

The screenshot shows the 'Edit Firewall Rule' configuration window. The 'Action' is set to 'Block'. The 'Interface' is 'LAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'TCP'. The 'Source' section shows 'Source Address' as 'LAN subnets'. The 'Destination' section shows 'Destination Address' as 'Any' and 'Destination Port Range' as 'Telnet (23)'. The 'Extra Options' section has 'Log' checked. The 'Description' is 'Bloquear Telnet para fora da LAN'. The 'Advanced Options' section is visible at the bottom.

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 LAN subnets Source Address /

[Display Advanced](#)
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match Any Destination Address /

Destination Port Range Telnet (23) From Custom 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 Bloquear Telnet para fora da LAN
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Figura 8 - Bloquear telnet

4.1.2. FTP (Porta 21)

Foram criadas duas regras na interface LAN para gerir o tráfego FTP (porta 21). A primeira permite a utilização do protocolo dentro da rede interna, possibilitando testes entre máquinas virtuais da LAN.

A segunda regra bloqueia todas as tentativas de ligação FTP para o exterior, cumprindo a política definida no enunciado e reduzindo o risco de utilização de serviços inseguros fora da rede da organização.

REGRA 1 – Permitir FTP dentro da rede interna (LAN)

Edit Firewall Rule	
Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>TCP</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>LAN subnets</div> <div>Source Address</div> <div>/</div> <div></div> <div></div>
<div>⚙ Display Advanced</div> <div>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.</div>	
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>LAN subnets</div> <div>Destination Address</div> <div>/</div> <div></div> <div></div>
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>LAN subnets</div> <div>Destination Address</div> <div>/</div> <div></div> <div></div>
Destination Port Range	<div>FTP (21)</div> <div>From</div> <div>Custom</div> <div>FTP (21)</div> <div>To</div> <div>Custom</div>
<div>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</div>	
Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div>Permitir FTP dentro da LAN</div> <div>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.</div>
Advanced Options	<div>⚙ Display Advanced</div>

Figura 9- Permitti FTP

REGRA 2 – Bloquear FTP de saída (para fora da LAN)

The screenshot shows the 'Edit Firewall Rule' window in Mikrotik WinBox. The configuration is as follows:

- Action:** Block. A hint explains the difference between block and reject.
- Disabled:** ☐ Disable this rule. A hint explains the purpose of this option.
- Interface:** LAN. A hint explains the purpose of this field.
- Address Family:** IPv4. A hint explains the purpose of this field.
- Protocol:** TCP. A hint explains the purpose of this field.
- Source:**
 - ☐ Invert match
 - Source: LAN subnets
 - Source Address: [empty] / [empty]
 - [Display Advanced](#) button.
 - Hint: 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:**
 - ☐ Invert match
 - Destination: Any
 - Destination Address: [empty] / [empty]
 - Destination Port Range:** From: FTP (21) Custom To: FTP (21) Custom
 - Hint: 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. A hint explains the purpose of this option.
 - Description:** Bloquear FTP para fora da LAN. A hint explains the purpose of this field.
 - [Advanced Options](#) button.

Figura 10 - Bloquear FTP

4.1.3. Ping (ICMP)

Foram configuradas duas regras na interface *LAN* para controlar o protocolo *ICMP*:

- A primeira permite o envio de mensagens *ICMP* dentro da rede interna, úteis para testes de conectividade entre máquinas.
- A segunda bloqueia qualquer tentativa de envio de *ICMP* para redes externas, como forma de proteger a infraestrutura de varrimentos de rede e evitar que máquinas internas comuniquem com o exterior via *ping*.

REGRA 1 – Permitir ICMP dentro da LAN

Edit Firewall Rule	
Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>ICMP</div> <div>Choose which IP protocol this rule should match.</div>
ICMP Subtypes	<div><div>any</div><div>Alternate Host</div><div>Datagram conversion error</div><div>Echo reply</div></div> <div>For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>LAN subnets</div> <div>Source Address /</div>
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>LAN subnets</div> <div>Destination Address /</div>
Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div>Permitir ICMP interno (Ping LAN)</div> <div>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.</div>
Advanced Options	<div>Display Advanced</div>

Figura 11 - Permitir ICMP

REGRA 2 – Bloquear ICMP para fora da LAN

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

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

LAN subnets

Source Address

/

Destination

Destination

☒ Invert match

LAN subnets

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

Bloquear ICMP para fora

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

Advanced Options

Display Advanced

Figura 12 - Bloquear ICMP

4.1.4. Web (HTTP – Porta 80)

Esta regra permite que os dispositivos da rede interna (*LAN*) acessem a páginas web via protocolo *HTTP* (porta 80).

De acordo com a política do enunciado, o protocolo Web deve ser permitido tanto para entrada como saída, mas como não estamos a simular um servidor Web a receber pedidos, criamos apenas a regra de saída.

REGRA 1 – Permitir HTTP dentro da LAN

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

LAN subnets

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

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

Permitir HTTP da LAN para fora

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

Advanced Options

Display Advanced

Figura 13 - Permitir HTTP

4.1.5. Email (SMTP – porta 25)

Foram criadas duas regras para controlar o tráfego *SMTP* na interface *LAN*:

- A primeira impede a recepção de emails diretamente do exterior, bloqueando ligações destinadas ao IP da firewall na porta 25 (*SMTP*).
- A segunda permite que as máquinas internas possam enviar emails para servidores externos, como parte da política definida no enunciado.

Esta configuração impede abusos de email *inbound* e permite comunicação controlada *outbound*.

Regra 1 – Bloquear entrada de SMTP

Edit Firewall Rule			
Action	Block <small>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.</small>		
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>		
Interface	LAN <small>Choose the interface from which packets must come to match this rule.</small>		
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>		
Protocol	TCP <small>Choose which IP protocol this rule should match.</small>		
Source			
Source	<input type="checkbox"/> Invert match	Any	Source Address /
Display Advanced <small>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.</small>			
Destination			
Destination	<input type="checkbox"/> Invert match	LAN address	Destination Address /
Destination Port Range	SMTP (25)	From Custom	To SMTP (25) Custom
<small>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</small>			
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule <small>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).</small>		
Description	Bloquear recepção de SMTP na LAN <small>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.</small>		
Advanced Options	Display Advanced		

Figura 14 – Bloquear SMTP

Regra 2 – Permitir saída de SMTP

Edit Firewall Rule	
Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>TCP</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>LAN subnets</div> <div>Source Address</div> <div>/</div> <div></div>
<div>Display Advanced</div> <div>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.</div>	
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>Any</div> <div>Destination Address</div> <div>/</div> <div></div>
Destination Port Range	<div>SMTP (25)</div> <div>From</div> <div>Custom</div> <div>SMTP (25)</div> <div>To</div> <div>Custom</div> <div>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</div>
Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div>Permitir SMTP da LAN para a Internet</div> <div>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.</div>
Advanced Options	<div>Display Advanced</div>

Figura 15 - Permitir SMTP

4.2. Tabela – Regras na Interface WAN (Interface 2)

A interface WAN representa a ligação da firewall à Internet (rede externa). De acordo com a política do enunciado, foram criadas regras para impedir a entrada de tráfego inseguro ou não autorizado, garantindo a proteção da rede interna contra acessos externos indesejados.

Tabela 2 - Regras Interface WAN

Nº	Ação	Protocolo	Origem	Destino	Porta(s)	Descrição
1	Block	ICMP	any	WAN address	any	Bloquear pings do exterior
2	Block	TCP	any	WAN address	21, 23	Bloquear FTP e Telnet do exterior
3	Block	TCP	any	LAN subnet	any	Bloquear tentativas de acesso à rede LAN

4.2.1. Bloquear ICMP (Ping) vindo do exterior

Foi criada uma regra na interface *WAN* para bloquear pacotes *ICMP* direcionados ao endereço da firewall.

Esta medida impede que um *host* externo utilize *ping* ou outras formas de reconhecimento para identificar se a firewall está ativa.

The screenshot shows the 'Edit Firewall Rule' configuration window. The 'Action' is set to 'Block'. The 'Interface' is 'WAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'ICMP'. Under 'ICMP Subtypes', 'any' is selected. The 'Source' section shows 'Source Address' as 'Any'. The 'Destination' section shows 'Destination Address' as 'WAN address'. The 'Log' checkbox is unchecked. The 'Description' is 'Bloquear ICMP vindo do exterior'. The 'Advanced Options' button is visible at the bottom.

Edit Firewall Rule	
Action	Block <small>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.</small>
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
Interface	WAN <small>Choose the interface from which packets must come to match this rule.</small>
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>
Protocol	ICMP <small>Choose which IP protocol this rule should match.</small>
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply <small>For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.</small>
Source	
Source	<input type="checkbox"/> Invert match Any Source Address /
Destination	
Destination	<input type="checkbox"/> Invert match WAN address Destination Address /
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule <small>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).</small>
Description	Bloquear ICMP vindo do exterior <small>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.</small>
Advanced Options	Display Advanced

Figura 16 - Bloquear ICMP (WAN)

4.2.2. Bloquear FTP (porta 21) e Telnet (porta 23) do exterior

Esta regra foi criada para bloquear o tráfego direcionado às portas 21 (*FTP*) e 23 (*Telnet*), prevenindo acessos não autorizados a serviços potencialmente inseguros.

Foi configurada na interface *WAN*, aplicando-se a todo o tráfego vindo do exterior com destino ao endereço da firewall.

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

WAN address

Destination Address

/

Destination Port Range

FTP (21)

Custom

Telnet (23)

Custom

FromTo

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

Bloquear FTP e Telnet vindos de fora

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

Advanced Options

Display Advanced

Figura 17 - Bloquear FTP e Telnet

4.2.3. Bloquear Acesso à LAN desde o exterior

Esta regra foi configurada com o objetivo de proteger a rede interna contra acessos não autorizados.

Ao bloquear todas as tentativas de comunicação com a LAN vindas da interface WAN, garante-se que apenas tráfego iniciado a partir da rede interna pode estabelecer ligação, conforme os princípios de segurança definidos.

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

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

LAN subnets

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

Bloquear acesso à LAN a partir da WAN

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

Figura 18 - Bloquear acesso à LAN

5. Demonstração

Nesta secção é feita a verificação prática da configuração realizada na firewall, através da análise das regras aplicadas, testes de conectividade e validação do comportamento esperado.

O objetivo é confirmar que as políticas definidas estão corretamente implementadas, que os acessos autorizados funcionam como previsto e que o tráfego não autorizado está a ser efetivamente bloqueado.

5.1. Listagem de todas as regras da firewall

Foram criadas regras nas interfaces LAN e WAN do *pfSense*, com o objetivo de controlar o tráfego de acordo com a política definida no enunciado. Reorganizamos as regras para que fossem aplicadas corretamente, garantindo que as permissões específicas (como *Telnet*, *FTP* e *ICMP* dentro da *LAN*) fossem processadas antes das regras de bloqueio geral. Dessa forma, assegura-se que apenas o tráfego necessário é permitido, respeitando o princípio de menor privilégio e promovendo uma postura de segurança adequada, conforme exigido pelo caso de estudo

Abaixo apresentam-se prints das regras aplicadas a cada interface.

5.1.1. Regras LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/499 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	LAN subnets	23 (Telnet)	*	none		Permitir Telnet dentro da rede LAN	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	LAN subnets	21 (FTP)	*	none		Permitir FTP dentro da LAN	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	LAN subnets	*	LAN subnets	*	*	none		Permitir ICMP interno (Ping LAN)	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	LAN subnets	*	! LAN subnets	*	*	none		Bloquear ICMP para fora	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	*	80 (HTTP)	*	none		Permitir HTTP da LAN para fora	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	*	25 (SMTP)	*	none		Permitir SMTP da LAN para a Internet	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	LAN address	25 (SMTP)	*	none		Bloquear receção de SMTP na LAN	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	! LAN subnets	21 (FTP)	*	none		Bloquear FTP para fora da LAN	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	! LAN subnets	23 (Telnet)	*	none		Bloquear Telnet para fora da LAN	

Figura 19 - Regras Aplicadas na LAN

5.1.2. Regras WAN

Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	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 *	*	*	LAN subnets	*	*	none		Bloquear acesso à LAN a partir da WAN	🔗🔧🔍🗑️
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	WAN address	21 - 23	*	none		Bloquear FTP e Telnet vindos de fora	🔗🔧🔍🗑️
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	WAN address	*	*	none		Bloquear ICMP vindo do exterior	🔗🔧🔍🗑️

Figura 20 - Regras Aplicadas na WAN

5.2. Demonstração do Funcionamento das Políticas

Para validar a eficácia das regras configuradas na *firewall*, foram realizados testes práticos entre as várias máquinas virtuais do cenário — tanto na rede *interna* como a partir do *exterior*. Estes testes permitiram verificar que os serviços autorizados funcionam corretamente e que os protocolos não permitidos estão efetivamente bloqueados, conforme definido nas políticas do enunciado.

Os resultados confirmaram que:

- Os serviços permitidos, como *HTTP* e *SMTP* de saída, funcionam como esperado
- Protocolos considerados inseguros, como *Telnet*, *FTP* e *ICMP*, foram corretamente bloqueados para o exterior
- O acesso à rede interna a partir do exterior (via *WAN*) foi impedido
- Apenas comunicações internas explícitas foram autorizadas

Abaixo seguem exemplos de comandos utilizados e respectivos resultados, ilustrando o comportamento das políticas em funcionamento.

5.2.1. Tabela de testes – Funcionamento das políticas

Tabela 3 - Tabela de Testes

Nº	Teste	Origem	Destino	Protocolo/Porta	Esperado	Resultado
1	ping 10.120.59.1	Kali interna	Firewall (LAN)	ICMP	Permitir	Sucesso
2	ping 8.8.8.8	Kali interna	Google DNS	ICMP	Bloquear	Bloqueado
3	telnet google.com 23	Kali interna	Internet	TCP/23 (Telnet)	Bloquear	Bloqueado
4	ftp ftp.debian.org	Kali interna	Internet	TCP/21 (FTP)	Bloquear	Bloqueado
5	curl http://neverssl.com	Kali interna	Internet	TCP/80 (HTTP)	Permitir	Sucesso
6	ping 10.0.2.15	Kali externa	PFSense (WAN)	ICMP	Bloquear	Bloqueado
7	telnet 10.0.2.15 21 / 23	Kali externa	PFSense (WAN)	TCP/21–23	Bloquear	Bloqueado
8	telnet 10.120.59.10 23	Kali externa	Kali interna	TCP/23	Bloquear	Bloqueado
9	telnet 10.120.59.10 23	Kali interna	Kali interna	TCP/23	Permitir	Sucesso
10	nslookup google.com ou dig	Kali interna	DNS externo (UDP)	UDP/53	Permitir	Sucesso

5.3. Testes Realizados

Para que validasse as regras impostas, fiz vários testes como mostra a tabela em cima para confirmando assim que as regras que defini estão a funcionar.

5.3.1. Teste 1 - Permitir ping da LAN para a firewall

- **Objetivo:** Verificar se a máquina interna (*Kali*) consegue comunicar com a *firewall*.
- **Resultado esperado:** A firewall responde aos *pings*.

```
(kali㉿kali)-[~]  
$ ping 10.120.59.1  
PING 10.120.59.1 (10.120.59.1) 56(84) bytes of data:  
64 bytes from 10.120.59.1: icmp_seq=1 ttl=64 time=0.676 ms  
64 bytes from 10.120.59.1: icmp_seq=2 ttl=64 time=1.08 ms  
64 bytes from 10.120.59.1: icmp_seq=3 ttl=64 time=0.524 ms  
64 bytes from 10.120.59.1: icmp_seq=4 ttl=64 time=0.502 ms  
64 bytes from 10.120.59.1: icmp_seq=5 ttl=64 time=0.786 ms  
^C  
— 10.120.59.1 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4072ms  
rtt min/avg/max/mdev = 0.502/0.713/1.078/0.209 ms
```

Figura 21 - Ping LAN para a firewall

5.3.2. Teste 2 – Bloquear ping da LAN para a internet

- **Objetivo:** Confirmar que ICMP está bloqueado para destinos fora da LAN.
- **Resultado esperado:** Sem resposta (*timeout*).

```
(kali㉿kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
^C  
— 8.8.8.8 ping statistics —  
7 packets transmitted, 0 received, 100% packet loss, time 6135ms
```

Figura 22 - Ping para a internet

5.3.3. Teste 3 – Bloquear Telnet para o exterior

- **Objetivo:** Confirmar que *Telnet* está bloqueado para o exterior.
- **Resultado esperado:** Conexão recusada ou sem resposta.

```
(kali㉿kali)-[~]  
$ telnet towel.blinkenlights.nl 23  
Trying 213.136.8.188 ...  
^C  
  
(kali㉿kali)-[~]  
$
```

Figura 23 – Teste telnet Exterior

5.3.4. Permitir Telnet interno (entre máquinas LAN)

- **Objetivo:** Confirmar que Telnet está permitido dentro da LAN, para isso abri outra máquina e fiz o teste.
- **Resultado esperado:** Conexão aceite.

```
(kali㉿kali)-[~]  
$ telnet 10.120.59.11  
Trying 10.120.59.11 ...  
Connected to 10.120.59.11.  
Escape character is '^]'.  
  
Linux 6.12.20-amd64 (localhost) (pts/1)  
vbox login: login: timed out after 60 secondsConnection closed by foreign host.
```

Figura 24 - Permitir telnet interno

5.3.5. Teste 5 – Bloquear FTP de saída

- **Objetivo:** Confirmar que FTP esta bloqueado para fora da LAN.
- **Resultado esperado:** Conexão recusada.

```
(kali㉿kali)-[~]  
$ ftp ftp.debian.org  
Trying 146.75.90.132:21 ...  
^C  
  
(kali㉿kali)-[~]  
$
```

Figura 25 - Ftp para fora da LAN

5.3.6. Teste 6 – Permitir HTTP (Web) para o exterior

- **Objetivo:** Confirmar que HTTP esta bloqueado para fora da LAN.
- **Resultado esperado:** Página carrega.

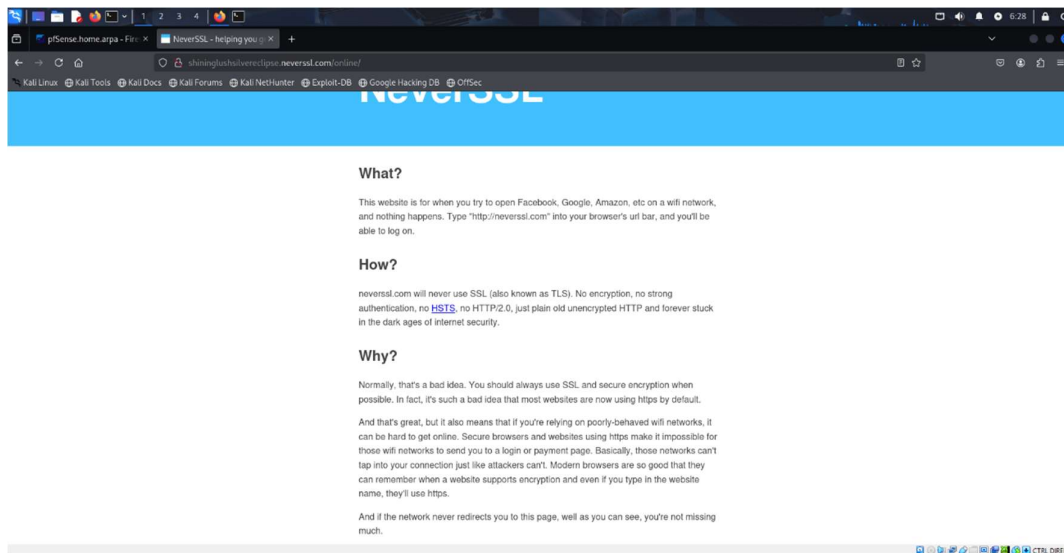


Figura 26 - Permitir HTTP exterior

5.3.7. Bloquear ICMP à firewall (WAN)

- **Objetivo:** Bloquear *ICMP* para a *firewall* vindo do exterior.
- **Resultado esperado:** Conexão não aceite.

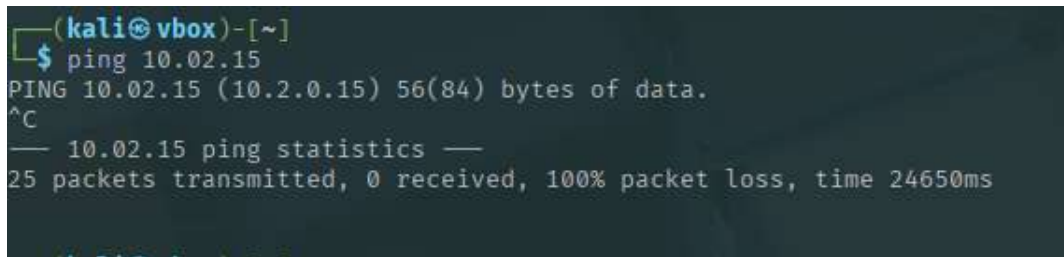


Figura 27 - Firewall bloqueia ICMP

5.3.8. Permitir DNS para fora

- **Objetivo:** Máquinas internas conseguem resolver nomes DNS.
- **Resultado esperado:** Conseguir resolver DNS.

```
(kali㉿kali)-[~]  
$ nslookup google.com  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
Name:   google.com  
Address: 142.250.184.174  
Name:   google.com  
Address: 2a00:1450:4003:801::200e
```

Figura 28 - Resolver DNS

5.4. Identificação de Protocolos Inseguros e Propostas de Melhoria

Durante a implementação das políticas de segurança definidas no enunciado, foram identificados vários protocolos considerados inseguros por não utilizarem mecanismos de encriptação ou por serem suscetíveis a ataques.

Protocolos inseguros identificados:

Tabela 3 - Protocolos Inseguros

Protocolo	Porta	Motivo de insegurança
Telnet	23	Transmite dados e credenciais em texto claro
FTP	21	Sem encriptação, vulnerável a <i>sniffing</i> de dados
SMTP	25	Pode ser usado para envio de spam ou <i>spoofing</i>
ICMP	—	Pode ser explorado para mapeamento e ataques <i>DDoS</i>

Propostas de alteração às regras:

Tabela 4 - Proposta alteração

Protocolo	Substituir por	Nova Recomendação de Regra
Telnet	SSH (porta 22)	Bloquear totalmente Telnet; permitir SSH autenticado
FTP	SFTP / SCP (via SSH)	Bloquear FTP; permitir apenas SFTP autenticado
SMTP	SMTPS (465) ou Submission (587)	Bloquear 25 para saída; permitir 465/587 com autenticação
ICMP	—	Permitir apenas dentro da LAN, bloquear ICMP externo

Apesar de algumas destas regras permitirem o funcionamento básico exigido no exercício, não seriam recomendadas em ambientes reais de produção. Protocolos como *Telnet* e *FTP* devem ser completamente substituídos por alternativas seguras, e o tráfego *SMTP* deve ser controlado com filtros *anti-spam* e autenticação.

A *firewall* deve adotar uma política de “deny by default”, permitindo apenas o tráfego estritamente necessário, com foco na segurança e minimização da superfície de ataque.

6. IPS/IDS - Integração de um sistema de detecção/prevenção de intrusões

Para reforçar a segurança da arquitetura implementada, foi integrado um sistema de detecção/prevenção de intrusões (*IDS/IPS*).

Foi utilizado o *Snort*, um dos *IDS/IPS* mais conhecidos e eficazes, instalado diretamente na *firewall pfSense*.

Instalação do *Snort*:

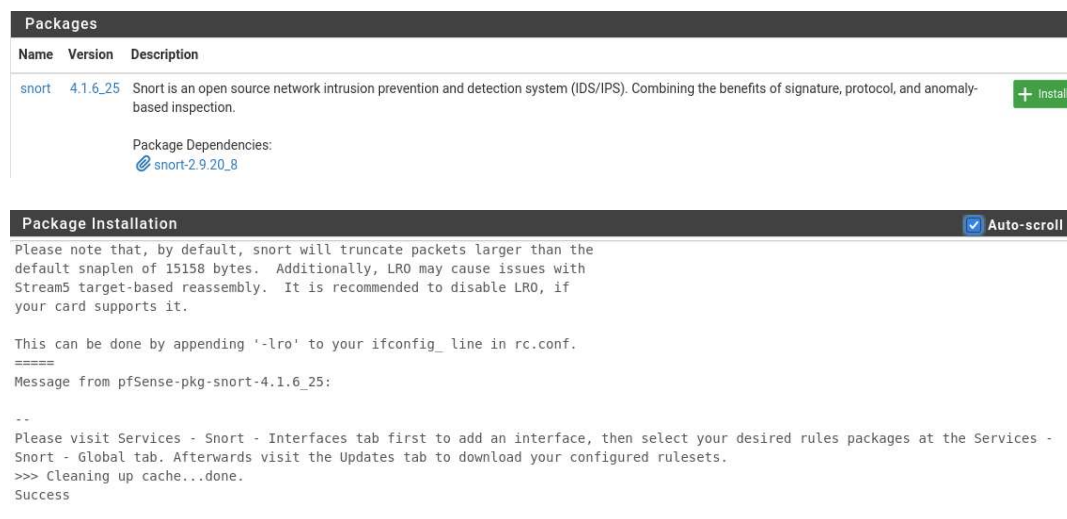


Figura 29 - Instalação do *Snort*

6.1. Configuração do *Snort*

O *Snort* foi configurado na *interface WAN*, de forma a monitorizar todo o tráfego proveniente da *Internet*. Foram ativadas regras da comunidade, e a funcionalidade de "*Block Offenders*" foi ativada para simular um modo *IPS*.

Configuração efetuada:

- **Pacote** instalado: *snort*
- **Interface** monitorizada: *WAN*
- **Tipo de regras**: *Snort GPLv2 Community Rules*
- **Ação**: Detetar e bloquear tráfego suspeito

General Settings	
Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<div>WAN (em0) ▼</div> <div>Choose the interface where this Snort instance will inspect traffic.</div>
Description	<div>WAN</div> <div>Enter a meaningful description here for your reference.</div>
Snap Length	<div>1518 ▼</div> <div>Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.</div>

Snort GPLv2 Community Rules	
Enable Snort GPLv2	<input checked="" type="checkbox"/> Click to enable download of Snort GPLv2 Community rules
<div>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.</div>	

Emerging Threats (ET) Rules	
Enable ET Open	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules
<div>ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.</div>	
Enable ET Pro	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
<div>Sign Up for an ETPro Account</div> <div>ETPro for Snort offers daily updates and extensive coverage of current malware threats.</div>	

Sourcefire OpenAppID Detectors	
Enable OpenAppID	<input checked="" type="checkbox"/> Click to enable download of Sourcefire OpenAppID Detectors
<div>The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.</div>	
OpenAppID Version	N/A (Not Downloaded)
Enable AppID Open Text Rules	<input checked="" type="checkbox"/> Click to enable download of the AppID Open Text Rules

Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	<div>Legacy Mode ▼</div> <div>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.</div> <div>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, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</div>
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	<div>BOTH ▼</div> <div>Select which IP extracted from the packet you wish to block. Default is BOTH.</div>

Figura 30 - Configuração Snort

Update das Rules aplicadas:

Installed Rule Set MD5 Signature		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
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 Downloaded	Not Downloaded

Update Your Rule Set		
Last Update	Unknown	Result: Unknown
Update Rules	Update Rules	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.		

Figura 31 - Update das Rules

Depois de ter dado update às regras, voltei à aba *Interfaces* e ativei a *interface* da *WAN*.

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

Figura 32 - Interface WAN ativada

6.1.1. Análise do funcionamento do IPS

Apesar de não terem sido gerados alertas durante os testes práticos com ferramentas como o *nmap*, a configuração do sistema IPS (*Snort*) foi corretamente realizada na interface *WAN* da *firewall pfSense*.

Foram ativadas categorias de regras relevantes, como *scan.rules* e *attack-responses.rules*, e o sistema foi configurado com a opção *Block Offenders* para atuar em modo de prevenção.

Foram realizados testes a partir de uma máquina externa (com acesso via rede bridge), simulando tráfego malicioso com varrimentos de portas.

Estes testes permitiram validar que o tráfego estava a ser encaminhado corretamente pela interface monitorizada pelo *Snort*, cumprindo o posicionamento pretendido para um *IPS* em linha com o tráfego externo.

Embora os alertas não tenham surgido na interface gráfica do *pfSense*, os passos realizados confirmam a presença de um sistema de inspeção e a preparação da infraestrutura para deteção e mitigação de ameaças em tempo real.

```
(kali@kali)-[~]
$ nmap -Pn -A 192.168.1.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 08:48 EDT
Nmap scan report for 192.168.1.23
Host is up.
All 1000 scanned ports on 192.168.1.23 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 242.36 seconds
```

Figura 33 - Analise funcionamento IPS

6.2. Analise das assinaturas existentes

As assinaturas no *Snort* são regras que definem padrões específicos de tráfego considerados suspeitos ou maliciosos.

Durante a configuração, foram analisadas e ativadas várias assinaturas relevantes, adaptadas ao cenário proposto.

Abaixo apresentam-se alguns exemplos analisados diretamente na interface *WAN Rules*:

SID	Categoria	Descrição
2100365	ICMP	Gera alerta para tentativas de "ping" (ICMP Echo Request) com tipo de código indefinido.
2010642	Scan	FTP Brute Force
2000537	Scan	Detecta o Nmap SYN scan (-sS) com janela TCP específica

Tabela 5 - WAN Rules analisadas

Estas regras foram escolhidas por permitirem testar funcionalidades específicas no contexto do *IPS*, como inspeção de *ICMP*, deteção de *scans* e controlo de conteúdo.

6.2.1. Regra ICMP – Detecção de ping externos

- Para monitorizar tráfego *ICMP* (*pings*) vindo do exterior da rede para a firewall, foi ativada a seguinte regra:



Figura 34 - Detecção pings externos

- **Objetivo:** Alertar sobre tentativas de "*ping*" com códigos ICMP não padronizados, vindas de fora da rede local.
- **Importância:** Esse tipo de tráfego pode indicar um scan ou reconhecimento externo.
- **SID:** 2100365
- **Classe:** misc-activity
- **Confiança:** Média
- **Severidade:** Informacional

6.2.2. Regra Scan – FTP Brute Force

View Rules Text

Category

emerging-scan.rules

GID:SID

1:2010642

Rule Text

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt"; flow:established,to_server; content:"USER "; nocase; depth:5; content:"root"; within:15; nocase; threshold: type threshold, track by_src, count 5, seconds 60; classtype:attempted-recon; sid:2010642; rev:3; metadata:created_at 2010_07_30, confidence Medium, signature_severity Informational, updated_at 2010_07_30;)
```

Close

Figura 35- FTP Brute Force

- Avisa quando são feitas múltiplas tentativas de login FTP como *root* vindas de um único IP.
Exige:
 - Que o conteúdo da mensagem contenha "*USER*" e "*root*" (tentativa de login como root)
 - Que ocorra pelo menos 5 vezes em 60 segundos do mesmo IP (*threshold*)
- Define o tipo de ameaça como tentativa de reconhecimento (*classtype:attempted-recon*)
- Gera alertas com confiança média e severidade informacional

6.2.3. Regra Scan – NMAP TCP SYN Scan



Figura 36 - NMAP TCP SYN Scan

- Deteta varredura de portas com *Nmap -sS* (*SYN scan*), muito usada em fase de reconhecimento de um ataque.
- Especifica uma janela *TCP* (*window*) de 2048, que é comum na assinatura padrão do *Nmap*.
- Utiliza:
 - *flags:S,12* para identificar pacotes com sinalização *SYN*
 - *dsize:0* e *ack:0* para indicar que é um pacote vazio com requisição de conexão
- *Threshold* evita alertas duplicados (1 alerta por destino a cada 60s)
- Classificado como reconhecimento (*attempted-recon*), com baixa severidade

6.3. Alerta bloqueio para tráfego ICMP externo (criação da regra)

Foi criada uma regra personalizada para detetar tentativas de *ping* (*ICMP Echo Request*) vindas do exterior para a *firewall*:

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ALERTA - ICMP PING EXTERNO DETETADO"; itype:8; sid:1000001; rev:1;)
```

Explicação da regra:

- alert → ação
- icmp → protocolo
- \$EXTERNAL_NET -> \$HOME_NET → tráfego vindo de fora
- itype:8 → tipo de pacote = ping (echo request)
- sid → ID único da tua regra
- rev → revisão (se editares depois, aumentas)

De seguido foi criada uma regra para bloquear o tráfego ICMP:

```
drop icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"BLOQUEIO - ICMP externo (ping)"; itype:8; sid:1000002; rev:1;)
```

Explicação da regra:

- drop: esta ação faz com que o Snort bloqueie o pacote (em vez de apenas alertar)
- icmp: protocolo usado por pings
- \$EXTERNAL_NET any -> \$HOME_NET any: corresponde a tráfego vindo de fora da rede para dentro
- itype:8: identifica pacotes do tipo Echo Request (ping)
- msg:"...": mensagem exibida no alerta e nos logs
- sid:1000002: identificador único da regra (usar valor acima de 1 milhão para regras custom)
- rev:1: primeira versão da regra

6.3.1. Teste e evidência do bloqueio de tráfego ICMP externo (ping)

Foi efetuado um *ping* a partir da máquina *host* (externa) com destino ao *IP* da máquina que atua como *firewall* (VM com *Snort*):

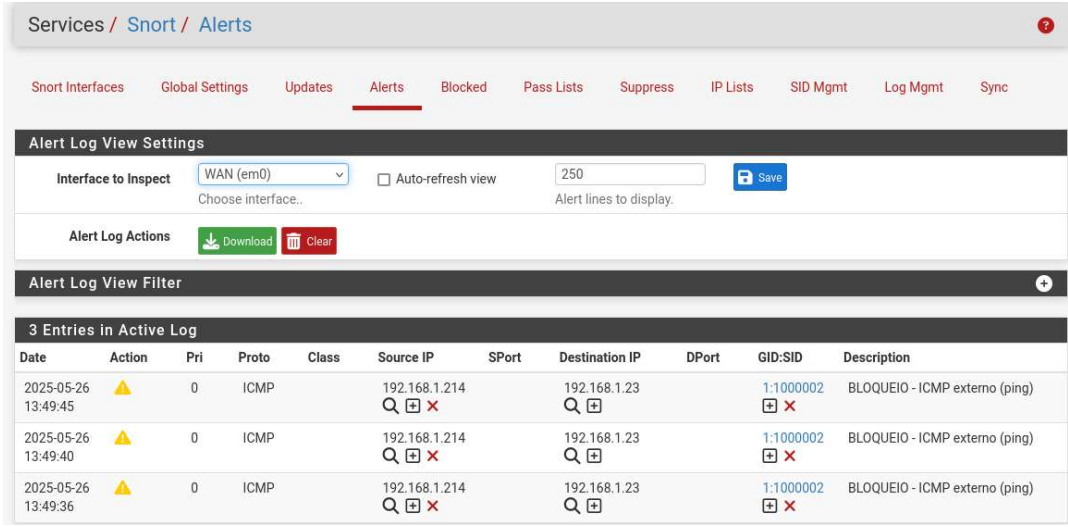
```
Pinging 192.168.1.23 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.23:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 37 - Ping Máquina externa

- O *ping* não obteve resposta.
- A mensagem apresentada foi: "Request timed out"

Em simultâneo, o *Snort* detetou o tráfego *ICMP* de entrada e gerou um alerta, tal como mostrado na figura abaixo:



The screenshot shows the 'Services / Snort / Alerts' page. The 'Alerts' tab is selected. Under 'Alert Log View Settings', 'Interface to Inspect' is set to 'WAN (em0)'. Under 'Alert Log View Filter', there are 3 entries in the active log. The table below represents the data shown in the screenshot.

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-05-26 13:49:45	⚠	0	ICMP		192.168.1.214		192.168.1.23		1:1000002	BLOQUEIO - ICMP externo (ping)
2025-05-26 13:49:40	⚠	0	ICMP		192.168.1.214		192.168.1.23		1:1000002	BLOQUEIO - ICMP externo (ping)
2025-05-26 13:49:36	⚠	0	ICMP		192.168.1.214		192.168.1.23		1:1000002	BLOQUEIO - ICMP externo (ping)

Figura 38- Alerta ICMP

Este resultado demonstra que a regra personalizada de bloqueio de *pings* externos está funcional, tanto ao nível da deteção (*IDS*), como do bloqueio efetivo (*IPS*), cumprindo os requisitos definidos para proteção da *firewall*.

6.4. Alerta para acesso a página com referência à palavra "Adult"

Para detetar tentativas de acesso a conteúdos potencialmente impróprios, foi criada uma regra *Snort* personalizada que verifica se a palavra "*Adult*" aparece no tráfego *HTTP* de saída.

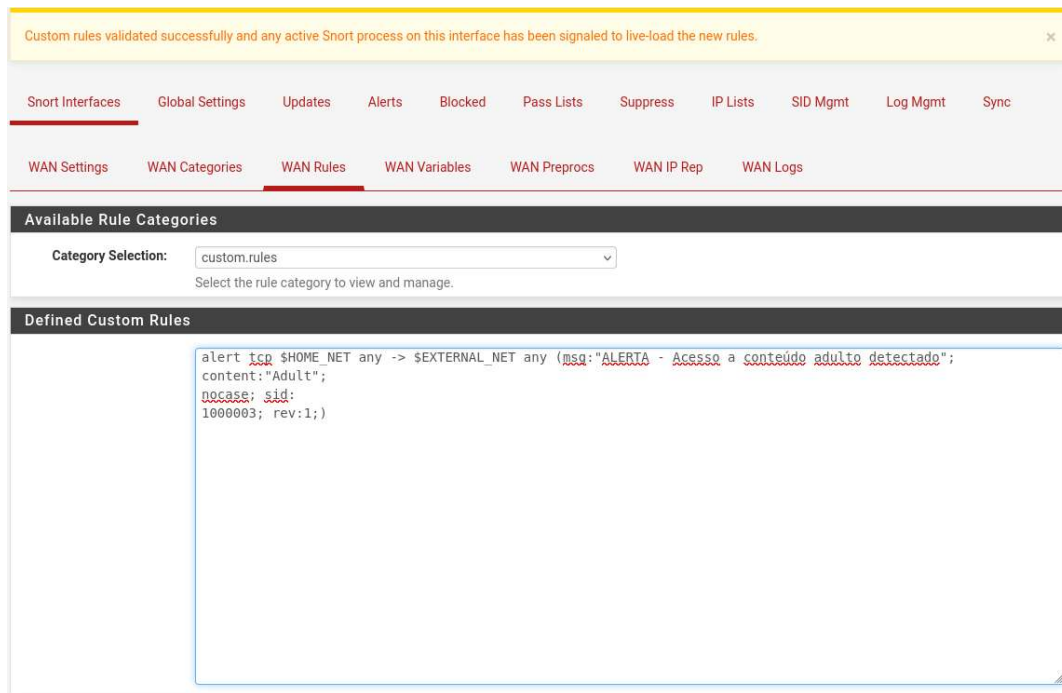


Figura 39 - Alerta Adult

- A regra verifica se máquinas internas (*\$HOME_NET*) acedem a páginas externas contendo o termo "*Adult*", ignorando caixa (maiúsculas/minúsculas).
- Pode ser usada em redes escolares, empresariais ou ambientes com políticas restritas de navegação.

6.4.1. Teste Realizado

Para realizar o teste da regra de detecção de conteúdos com referência à palavra "Adult", foi executado o seguinte comando a partir de uma máquina interna (na LAN):

```
(kali@kali)-[~]$ curl http://testphp.vulnweb.com/?=Adult
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) { if ((appName=="Netscape")&06(parseInt(appVersion)=4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
// -->
</script>
</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
<h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
<h2 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner">Acunetix Web Vulnerability Scanner</a></h2>
<div id="globalNav">
<table border="0" cellpadding="0" cellspacing="0" width="100%">
<tr>
<td align="left">
<a href="index.php?home">home</a> | <a href="categories.php?categories">categories</a> | <a href="artists.php?artists">artists</a> | <a href="disclaimer.php?disclaimer">disclaimer</a> | <a href="cart.php?your cart">your cart</a> |
<a href="guestbook.php?guestbook">guestbook</a> |
<a href="AJAX/index.php?AJAX Demo">AJAX Demo</a>
</td>
<td align="right">
</td>
</tr>
</table>
</div>
</div>
<!-- end masthead -->
<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
<h2 id="pageName">welcome to our page</h2>
<div classe="story">
```

Figura 40 - Teste "Adult"

Como resultado, o Snort gerou um alerta, visível na interface gráfica na secção de Alertas, conforme mostrado abaixo:

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Alert Log View Settings

Interface to InspectWAN (em0)Auto-refresh view250Save

Choose interface..Alert lines to display.

Alert Log ActionsDownloadClear

Alert Log View Filter+

5 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-05-26 13:58:07	🚩	0	TCP		192.168.1.23	10646	44.228.249.3	80	1:1000003	ALERTA - Acesso a conteúdo adulto detectado

Figura 41 - Alerta conteúdo "Adult"

Este teste comprova que a regra personalizada está funcional, detetando com sucesso tráfego HTTP que contenha a palavra "Adult", conforme solicitado nos objetivos do trabalho.

42

7. Conclusão

Este trabalho permitiu perceber, na prática, como a utilização combinada do *pfSense* com o *Snort* contribui para a criação de um ambiente de rede mais seguro e controlado. Ao longo das configurações e testes realizados, foi possível implementar regras personalizadas, gerar alertas e bloquear tráfego indesejado, comprovando a eficácia destas ferramentas na detecção e prevenção de ameaças.

Verificou-se a capacidade de resposta perante diferentes tipos de tráfego suspeito, como *pings* externos, tentativas de acesso a conteúdos inapropriados e scans de rede. A experiência demonstrou também a importância de manter uma monitorização contínua e uma configuração adequada para garantir a proteção da rede interna.

Para além da componente técnica, este trabalho reforçou a noção de que a segurança não depende apenas do software utilizado, mas também de uma gestão cuidada, atualização constante das assinaturas, e conhecimento sobre os protocolos e serviços em uso.

No geral, foi uma oportunidade importante para consolidar conhecimentos teóricos e aplicá-los em cenários reais, aproximando a experiência prática do que se encontra num contexto profissional.

Referências

- [1] pfSense. The pfSense Project. Disponível em: <https://www.pfsense.org/>
- [2] Cisco. Snort - Network Intrusion Detection System. Disponível em: <https://www.snort.org/>
- [3] Netgate. Documentation. Disponível em: <https://docs.netgate.com/pfsense/en/latest/>
- [4] Cisco Talos. Snort User Manual. Disponível em: <https://docs.snort.org/>
- [5] Proofpoint. Threats Open Rules. Disponível em: <https://rules.emergingthreats.net/>

