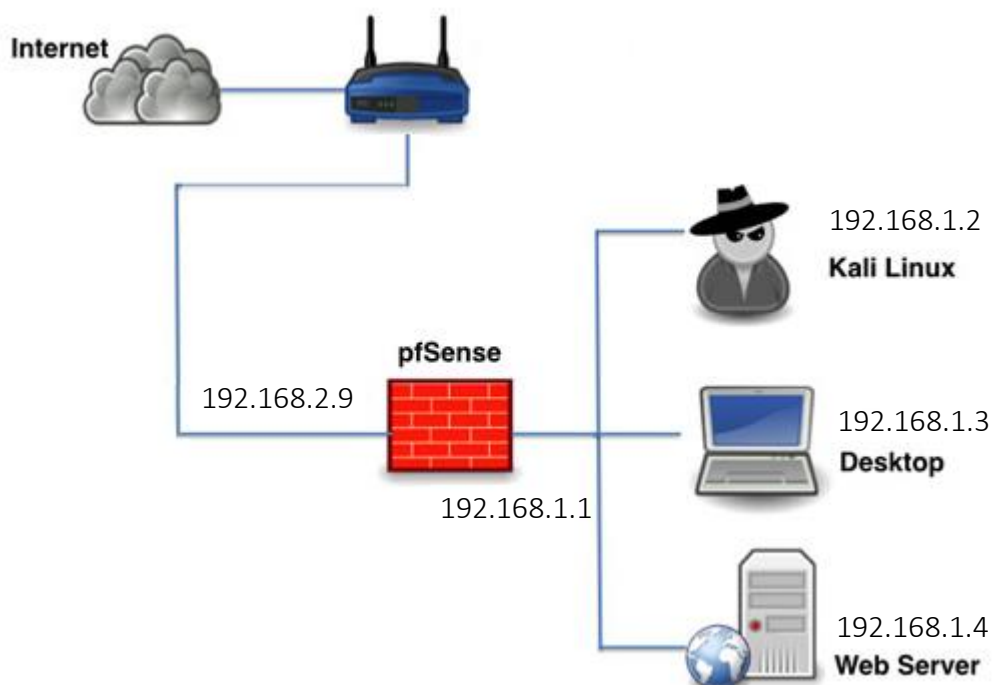


MODALIDADE:	Jovem + Digital	Não aplicável	
CURSO:	J+D 2/2026 Cibersegurança		
UC:	Cibersegurança Ativa	CÓDIGO UC:	9196
FORMADOR/A:	Bruno Silva	DATA:	

## OBJETIVOS

- Instalar, configurar e explorar a firewall PfSense

### Exemplo de digrama de construção e comunicação da firewall



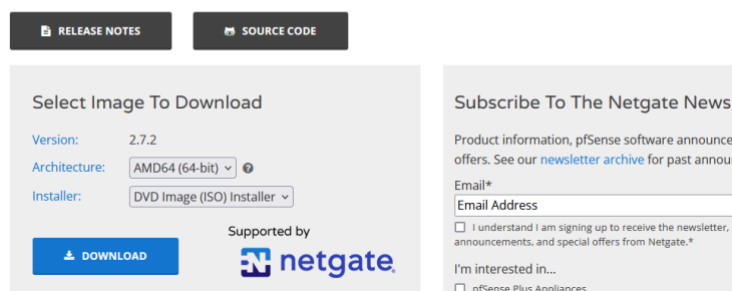
## Parte 1 – Configuração da máquina virtual

**Passo 1** – Retirar a imagem do pfsense da página oficial: <https://www.pfsense.org/download/> e selecionar as opções:

- **Architecture:** AMD64 (64-bit)
- **Installer:** DVD Image (ISO) Installer
- Se aparecer a opção Mirror deve indicar a localização mais próxima;

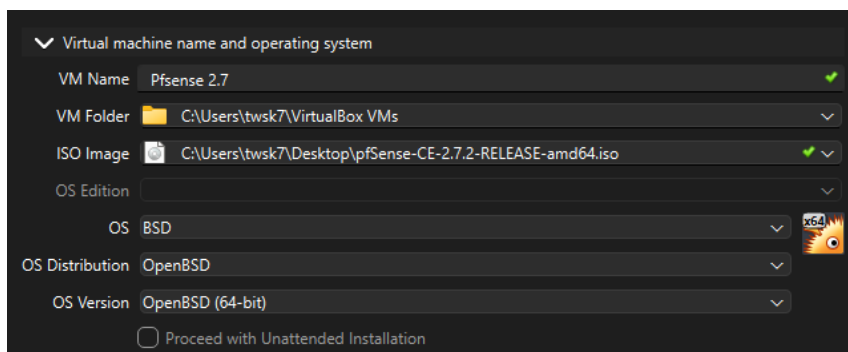
Latest Stable Version (Community Edition)

This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).



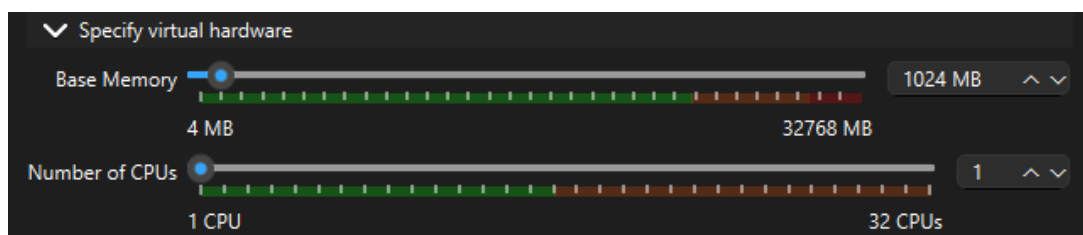
**Passo 2** – Vamos criar uma nova máquina virtual, do qual:

- **Nome:** Pfsense 2.8
- **ISO Image:** Colocar a localização da imagem que descarregou
- **OS:** BSD
- **Tipo:** OpenBSD
- **Versão:** OpenBSD (64-bit)

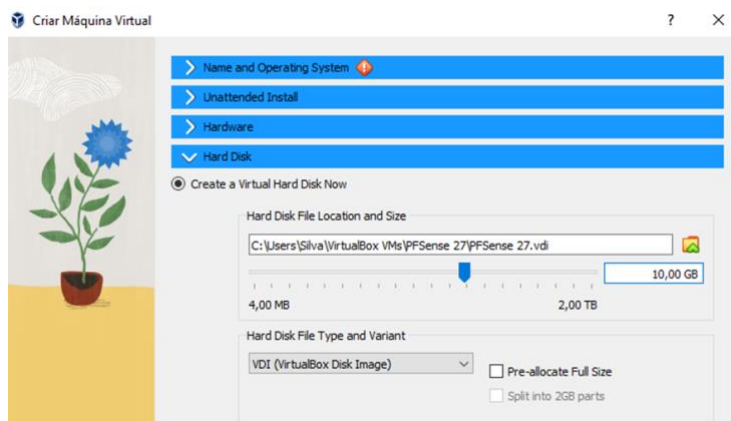


**Passo 3** – Em termos de hardware, defina os seguintes valores:

- **Memória Base:** 1024 MB (equivalente a 1GB de memória RAM) ou se quiser algo mais pode colocar até 2048 MB (equivalente a 2GB de memória RAM);
- **Núcleos de processador:** 1 (**OBIGATORIAMENTE**), pois o Pfsense só funciona em single-core (1 núcleo de processador);

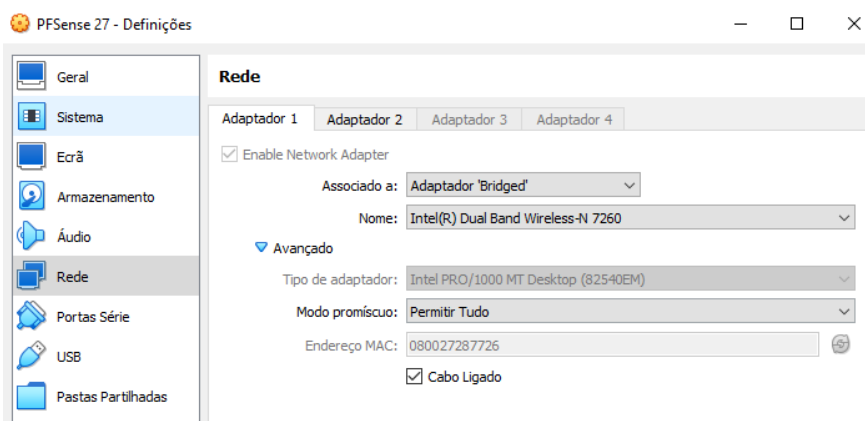


**Passo 4** – Criar disco rígido virtual com a extensão VDI e com 10 GB de espaço:

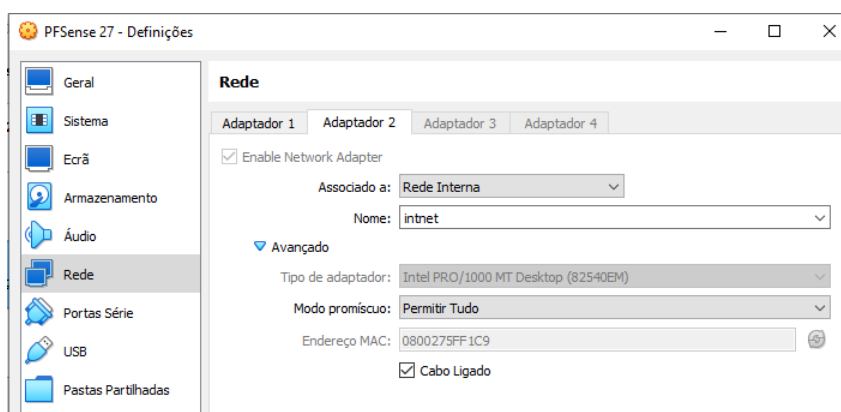


**Passo 5** – No separador rede, vamos ativar **2 adaptadores de rede** (placas de rede), do qual:

- **Adptador 1:** Bridge Mode (Adptador Bridge, que servirá para interface WAN, ou seja, por onde passa a ligação a internet do exterior) e **Modo promiscuo** Permitir Tudo;



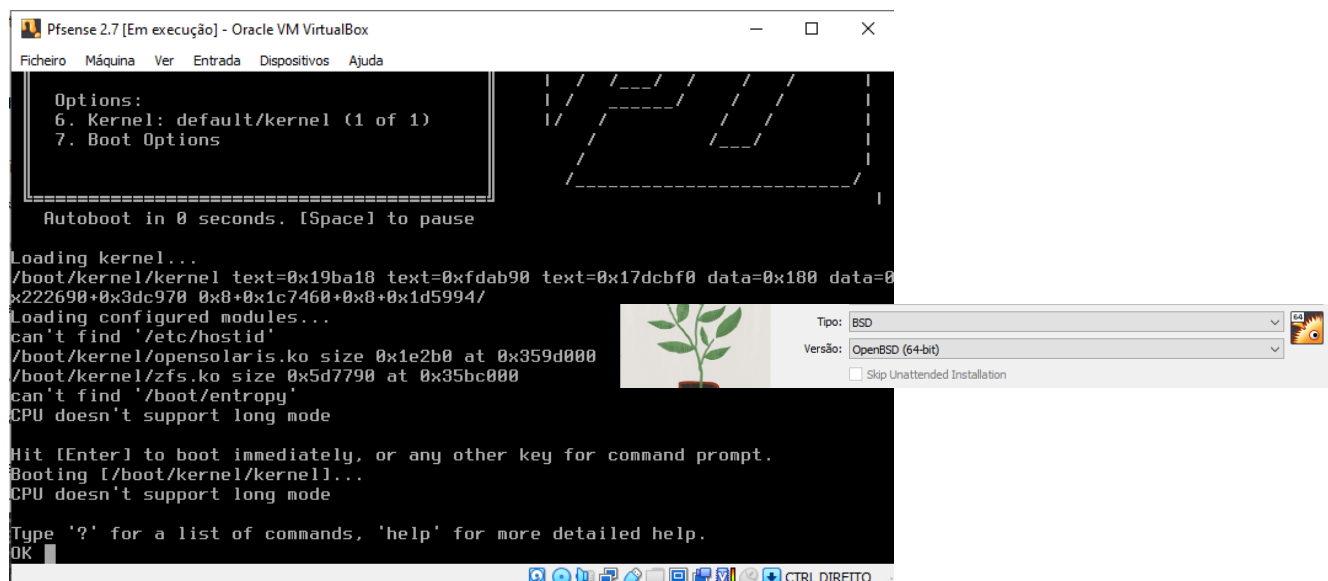
- **Aptador 2:** Rede interna (que serve para comunicar com os computadores que estão na rede LAN e interligados com esta firewall) e **Modo promiscuo** Permitir Tudo:



## Potenciais erros de inicialização

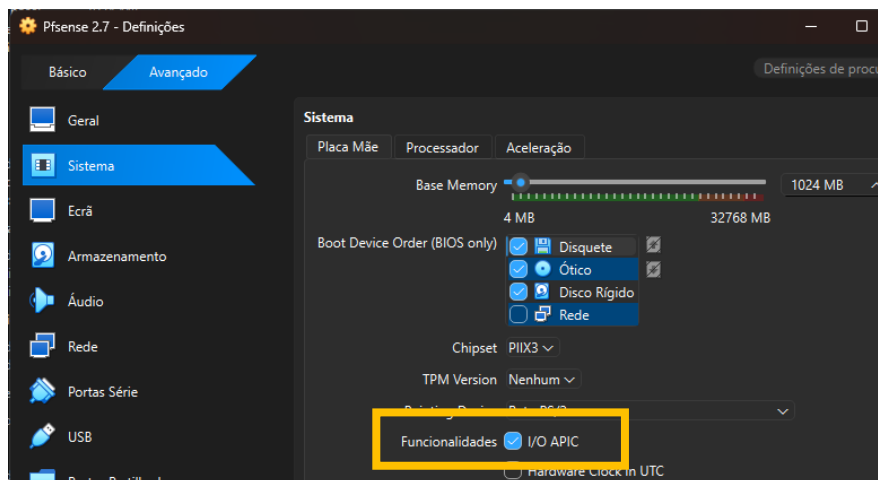
### ERRO “CPU doesn’t support long mode”

Ao arrancar a máquina virtual, pode aparecer o erro “*CPU doesn’t support long mode*”. Isto acontece ao fato de estar a fazer o processo de virtualização e não ter indicado que vai usar um sistema operativo de 64-bits. *Confirme se colocou as informações corretas no passo 2*, mais especificamente *a arquitetura da versão ser OpenBSD 64 Bit*:



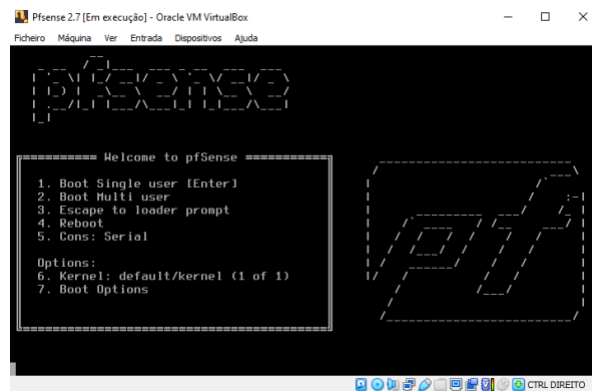
### ERRO “Panic: running without device atpic requires a local APIC”

Isto acontece ao fato de alguma configuração mal feita (como por exemplo configurações erradas do na identificação do sistema operativo aquando da criação da máquina virtual). Isto faz desativar uma funcionalidade de virtualização. Para resolver este problema, deve ir definições da máquina virtual, mais especificamente, escolher o separador “Sistema” e seleccionar a opção “I/O APIC”:

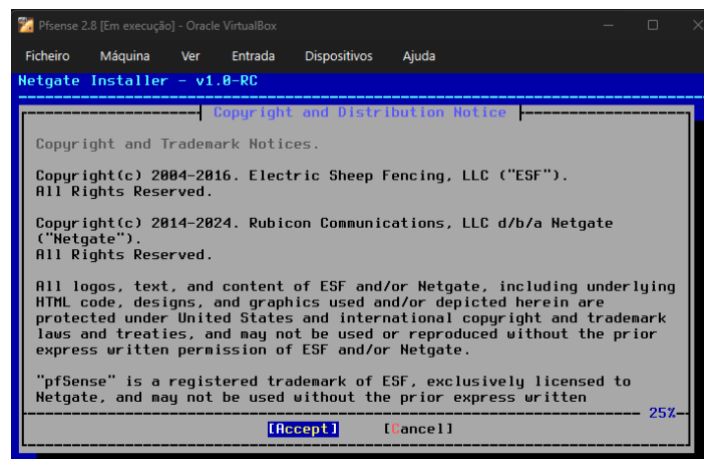


## Parte 2 – Configuração e Instalação da Firewall Pfsense

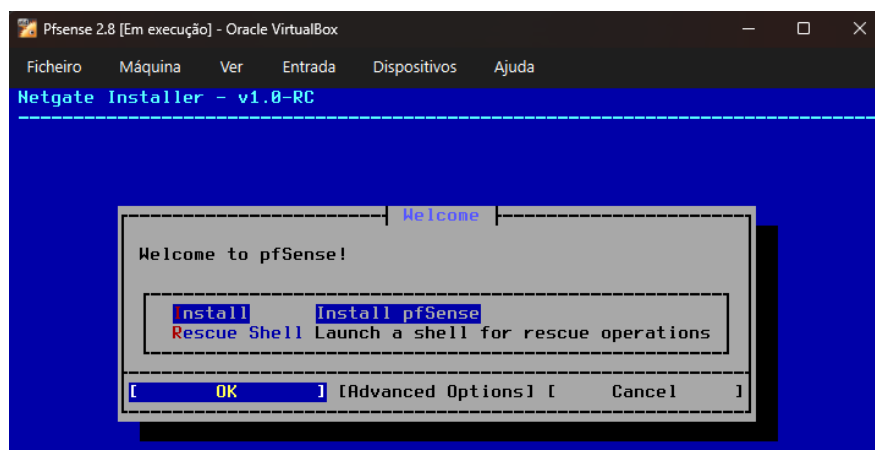
**Passo 1** – Se tudo correr bem a máquina virtual vai mostrar a tela principal e ao fim de 3 segundos, este arranca automaticamente para a configuração:



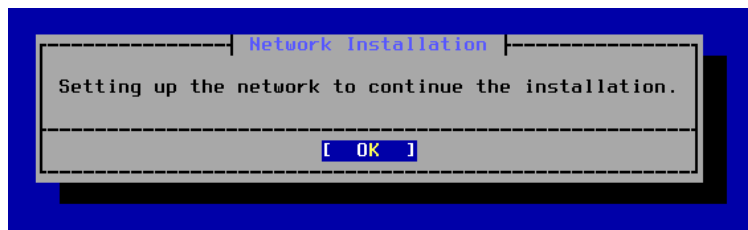
**Passo 2** – Aceitar os termos e condições:



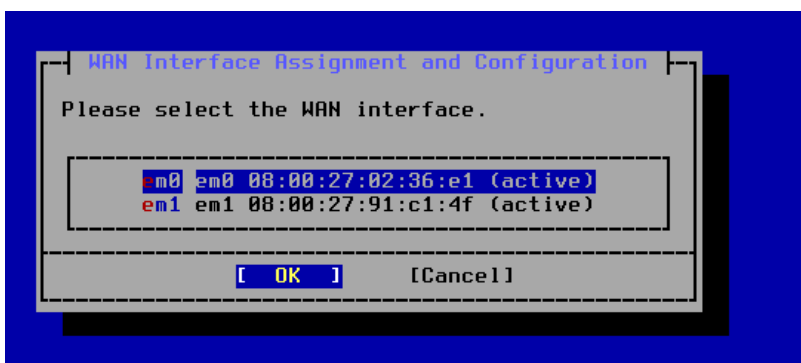
**Passo 3** – Selecionar a opção Install:



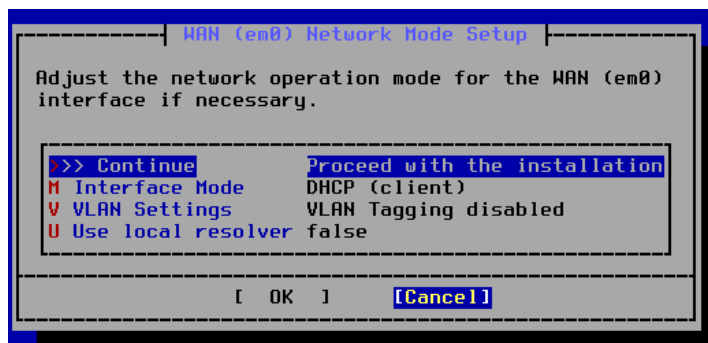
**Passo 4** – Confirme para configurar as interfaces de rede:



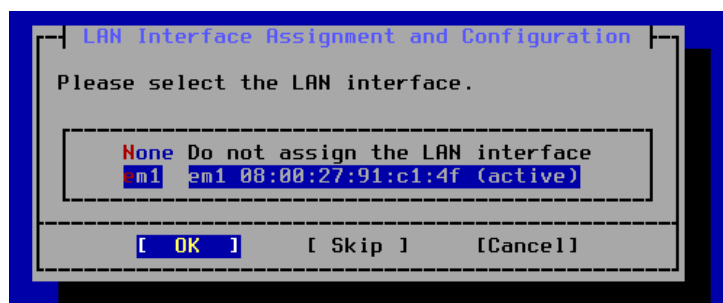
**Passo 5** – Selecione a interface em0 (neste caso será o adaptador bridge):



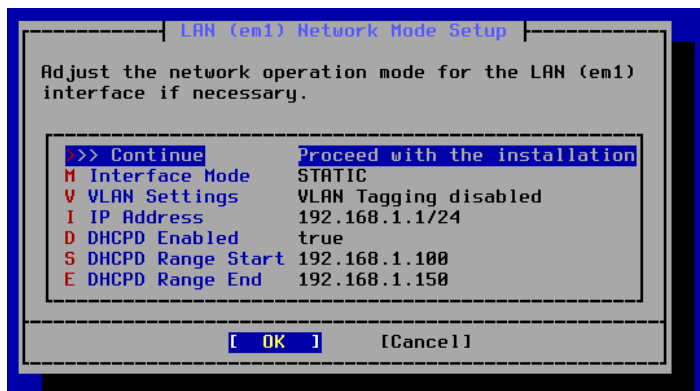
**Passo 6** – Peça para continuar a configuração (Continue):



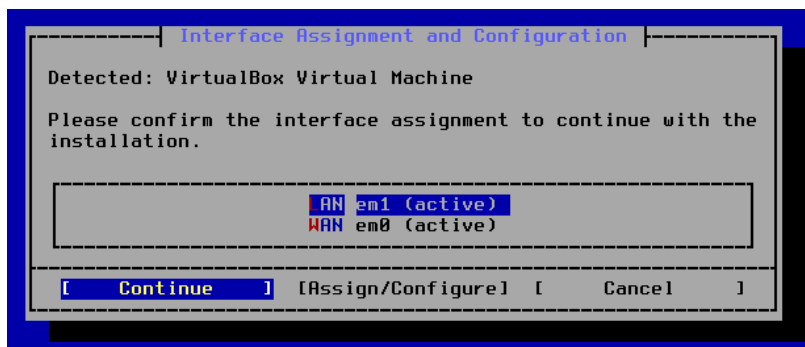
**Passo 7** – Configure a outra interface de rede, mais especificamente, a interface em1 (neste caso será a rede interna):



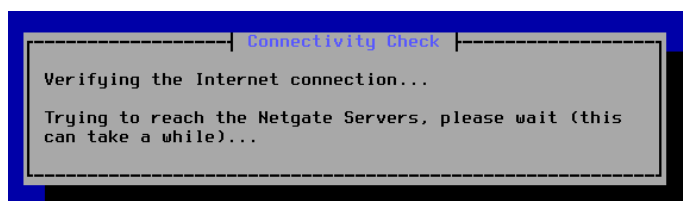
**Passo 8** – Peça para continuar a configuração (Continue):



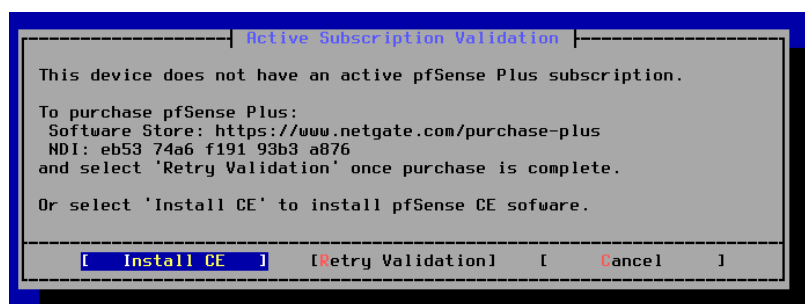
**Passo 9** – Peça para continuar a configuração (Continue):



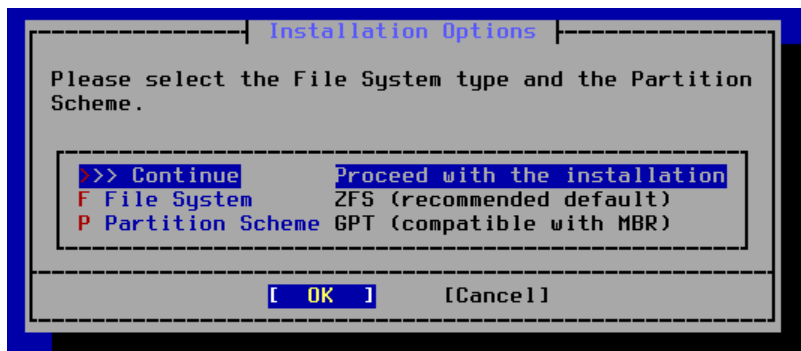
**Passo 10** – De seguida, vai ser verificada a configuração da internet (pelo adaptador bridge) e verificar se consegue ligar ao servidor remoto da NetGate:



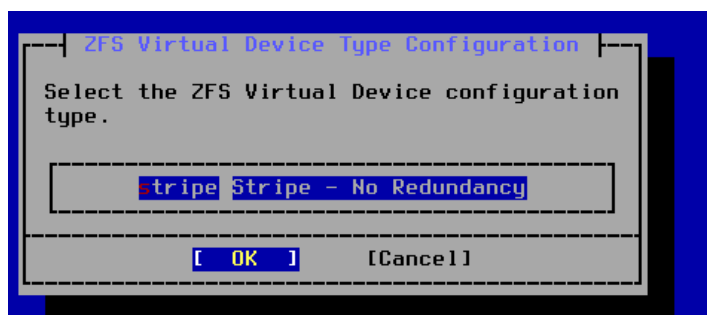
**Passo 11** – Pedir para instalar a versão CE (Community Edition):



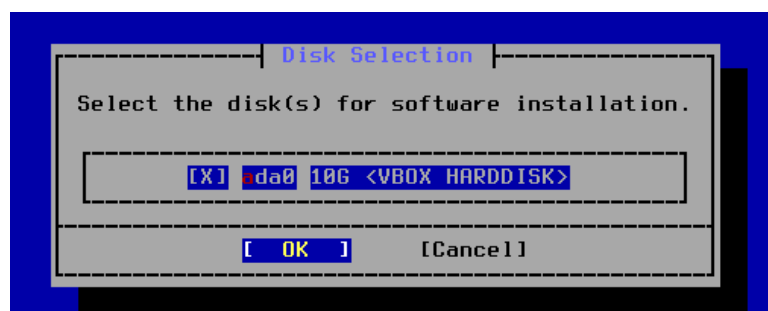
**Passo 12** – Peça para continuar a configuração (Continue):



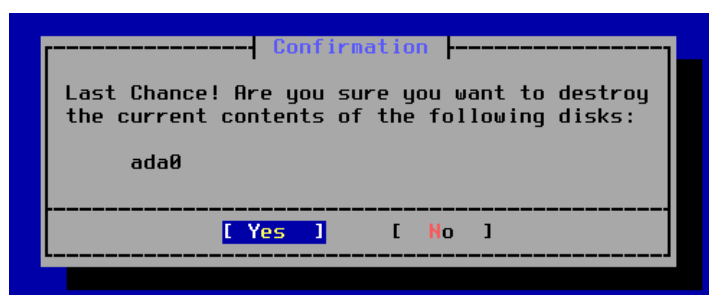
**Passo 13** – Peça para continuar a configuração (OK):



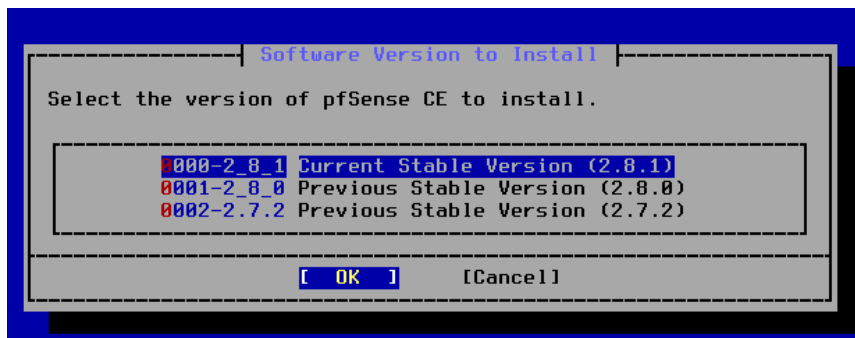
**Passo 14** – Peça para continuar a configuração (OK):



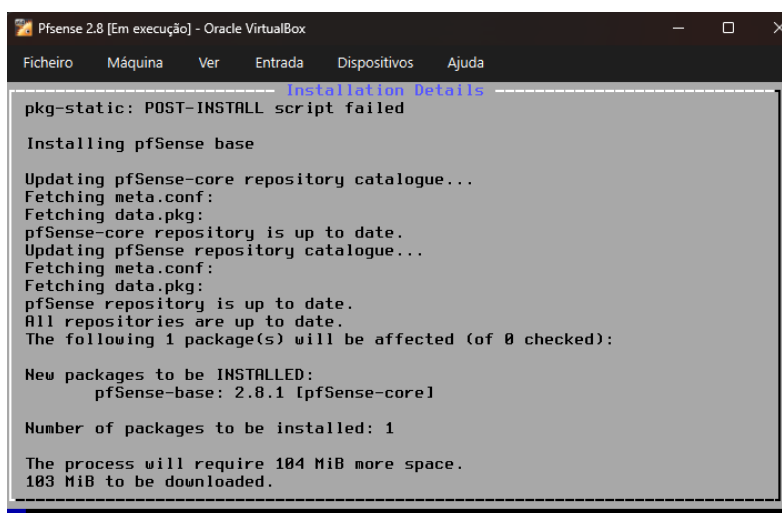
**Passo 15** – Confirme a instalação:



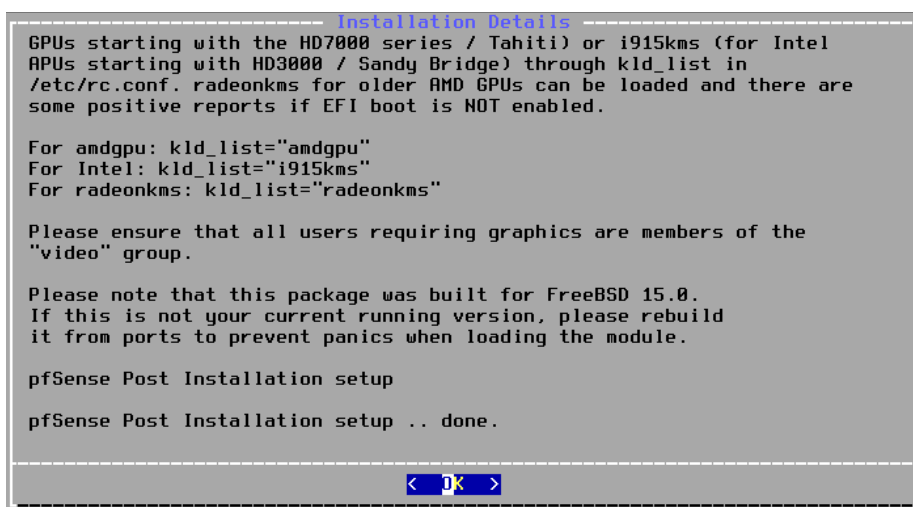
**Passo 16** – Selecione a versão mais recente (2.8.1):



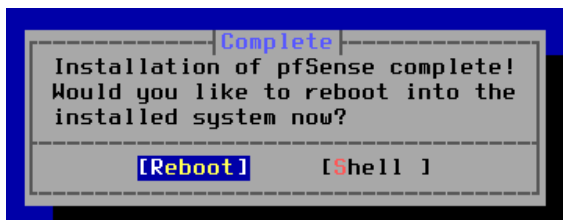
**Passo 17** – Deixar efetuar a instalação:



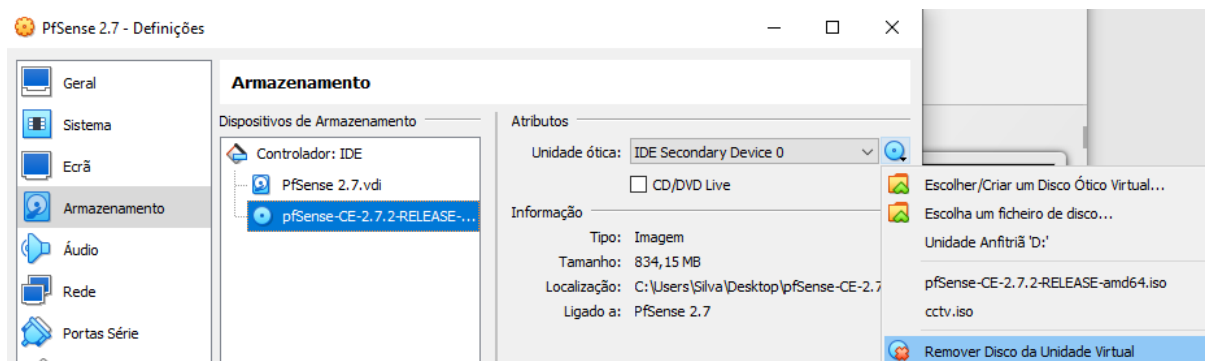
**Passo 18** – Após instalar carregue em OK:



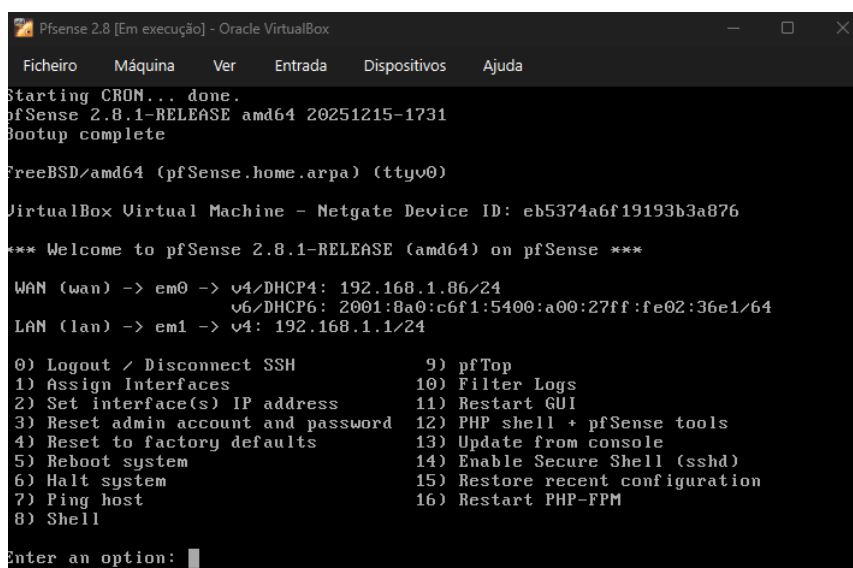
**Passo 19** – No final, este irá pedir para reiniciar a máquina virtual com a instalação do Pfsense. Selecione a opção Reboot:



**MUITO IMPORTANTE:** De seguida, quando a máquina virtual reiniciar, deve deitar a máquina virtual abaixo e remover a imagem da instalação, senão vai voltar a correr os passos anteriores:



**Passo 20** – Este vai acabar de fazer a configuração e costuma demorar um pouco. Quando finalizar, vai mostrar as informações da nossa firewall (do qual vai dar as informações dos endereços IP e afins, bem como um menu de escolhas):



A consola Pfsense permite executar tarefas de configuração, tais como:

- **Logout (somente ssh)**
- **Atribuir interfaces:** permite reconfigurar as vossas(s) interface(s) de rede;
- **Definir endereço IP da(s) interface(s):** podem definir endereços IP para as vossas interfaces de rede. Também é útil habilitar, desabilitar e configurar o serviço DHCP, aceder a interface gráfica (GUI) através de HTTP (em vez de HTTPS) e desabilitar a regra de bloqueio se o utilizador estiver bloqueado;
- **Redefinir senha do webConfigurator:** pode redefinir o utilizador e a senha do sistema para os valores padrão (admin/pfsense). O script também pode ativar ou gerar a conta padrão novamente, caso ela tenha sido desativada ou removida;
- **Redefinir para os padrões de fábrica:** para restaurar a configuração padrão do sistema, incluindo a remoção de software adicionado;
- **Reiniciar sistema:** oferece diferentes opções para reiniciar o sistema;
- **Halt system:** para desligar o sistema;
- **Ping host:** permite que você execute ping para fins de teste;
- **pfTop:** exibe o estado do sistema e os dados transferidos (útil para monitorar o sistema e diagnosticar problemas);
- **Filtrar Logs:** pode verificar os logs (registos) da firewall;
- **Reiniciar webConfigurator:** permite reiniciar processos vinculados à interface gráfica GUI, como nginx;
- **Ferramentas PHP Shell + pfSense:** permite executar código PHP (útil para programadores e utilizadores familiarizados com PHP);
- **Atualização do console:** atualizar o vosso sistema para sua última versão;
- **Habilitar Secure Shell (sshd):** para habilitar ou desabilitar o serviço SSH (certificados de segurança);
- **Restaurar configuração recente:** permite selecionar as últimas configurações do sistema para restauração;
- **Reinicie o PHP-FPM:** para reiniciar o serviço PHP (útil para resolver alguns problemas do webConfigurator);

**Passo 21 – Inicie a máquina virtual do UBUNTU** e de seguida, abra um navegador e coloque o endereço IP para aceder a firewall (normalmente será a segunda interface, ou seja, a interface LAN). Também temos de adicionar nova exceção e para tal basta prosseguir e aceitar os riscos):

```
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***  
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.86/24  
v6/DHCP6: 2001:8a0:c6f1:5400:a00:27ff:fe02:36e1/64  
LAN (lan) -> em1 -> v4: 192.168.1.1/24
```



Aviso: Potencial risco de segurança à frente

O Firefox detetou um potencial risco de segurança e não continuou para **192.168.1.75**. Se visitar este site, atacantes podem tentar furtar informação como palavras-passe, emails, ou detalhes de cartão de crédito.

[Saber mais...](#)

Retroceder (recomendado)

Avançado...

192.168.1.75 utiliza um certificado de segurança inválido.

O certificado não é de confiança porque é auto-assinado.

Código de erro: [MOZILLA\\_PKIX\\_ERROR\\_SELF\\_SIGNED\\_CERT](#)

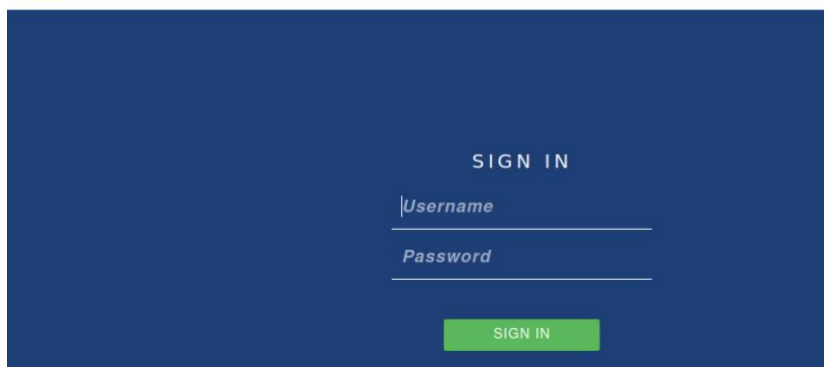
[Ver certificado](#)

Retroceder (recomendado)

ACEITAR O RISCO E CONTINUAR

**Passo 22 –** Para aceder a nossa página pela primeira vez, basta colocar os valores mais abaixo:

- **Utilizador:** admin
- **Password:** pfsense

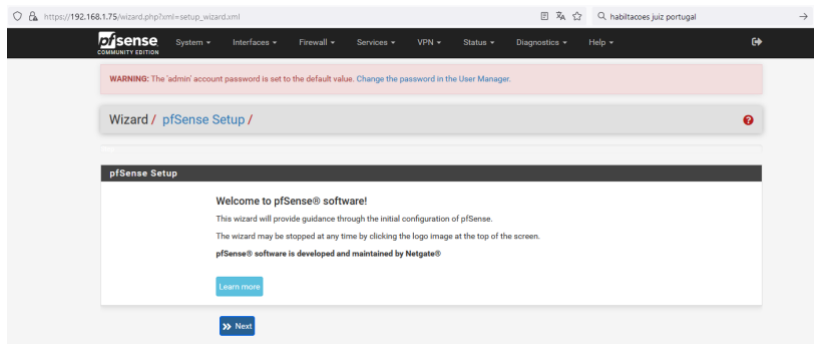


SIGN IN

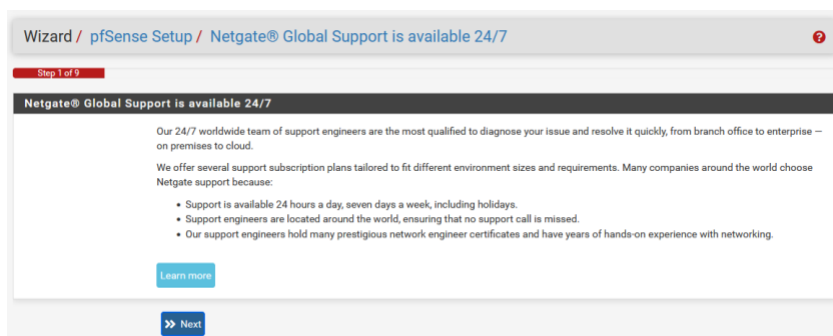
SIGN IN

**Passo 23** – Normalmente, será feito o tutorial de configuração inicial. Para tal, vamos realizar os seguintes passos:

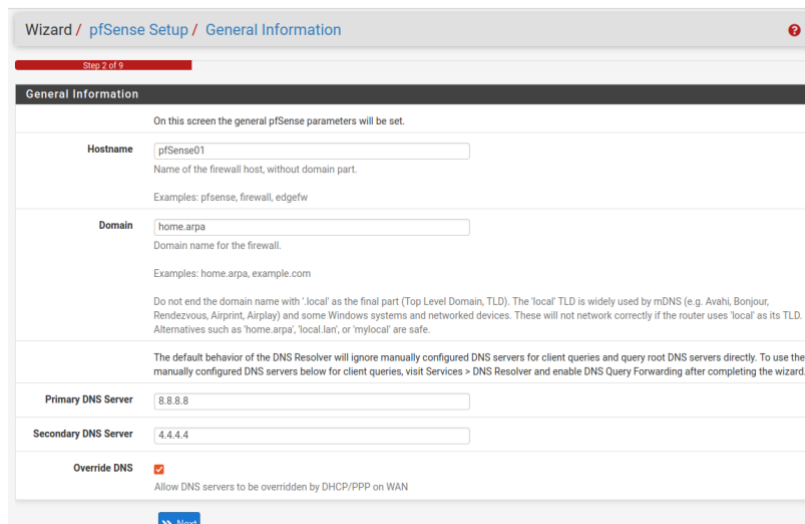
- Prosseguir com a instalação, clicando no botão azul-escuro Next:



- Prosseguir com a informação inicial, clicando no botão azul-escuro Next:



- Dar um nome a vossa máquina, como por exemplo “pfSense01”
- Deixar o domínio (domain) como home.arpa;
- Primary DNS: 8.8.8.8
- Secondary DNS: 4.4.4.4
- Override DNS: Selecionado



- Definir o fuso horário TimeZone como Europe/Lisbon:

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

**Time Server Information**

Please enter the time, date and time zone.

**Time server hostname**   
Enter the hostname (FQDN) of the time server.

**Timezone**

[Next](#)

- Na configuração da Interface WAN (ligação exterior), vamos deixar que este tenha um IP dinâmico (mas somente neste caso). Num ambiente de configuração mais avançado, devem ter um IP estático para que este não mude as configurações de deteção dos equipamentos nas redes informáticas:

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

**Configure WAN Interface**

On this screen the Wide Area Network information will be configured.

**SelectedType**

**General configuration**

**MAC Address**

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address

- Como estamos a utilizar endereços privados (como por exemplo, gamas de IP 192.168.1.x), não podemos ter seleccionadas as opções Block RFC1918 Private Networks e Block bogon networks. Verifique se está dessa forma!

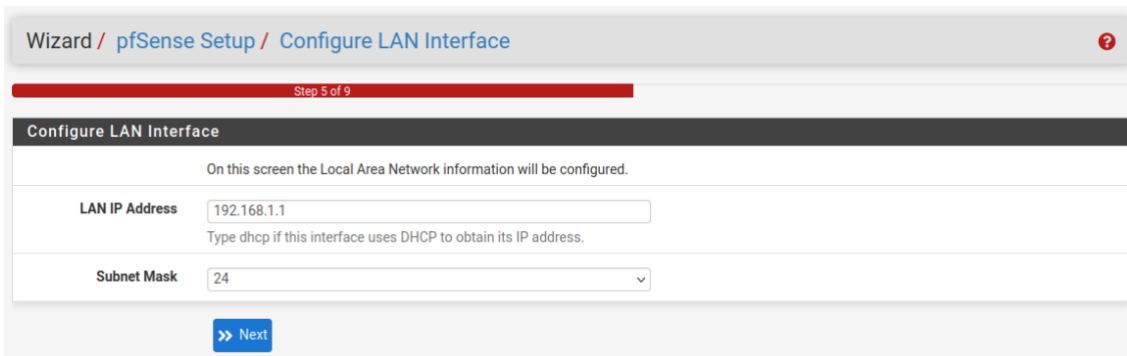
**Reserved Networks**

**Block private networks and loopback addresses**   
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

**Block bogon networks**   
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

- Na configuração da Interface LAN (rede interna que está depois da firewall), vamos indicar que o servidor vai ser acessível no endereço 192.168.1.1 que tem uma máscara 24:



Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

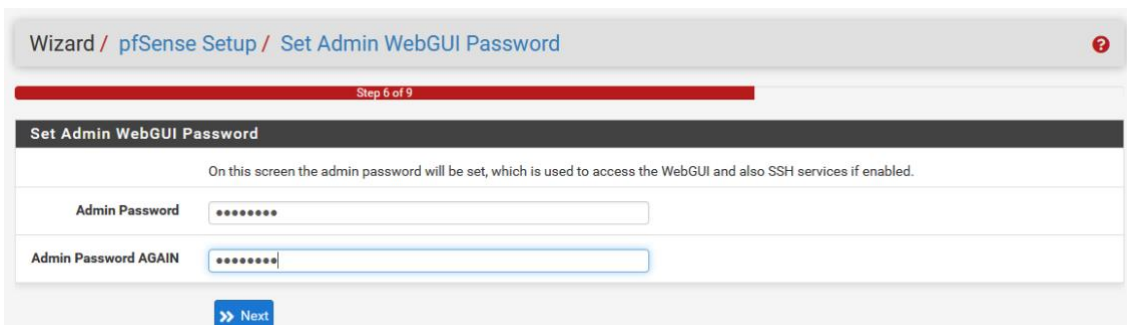
On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.1.1  
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

Next

- Definir a senha do admin, que é utilizada para aceder a interface web e também os serviços SSH (quando habilitados):



Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

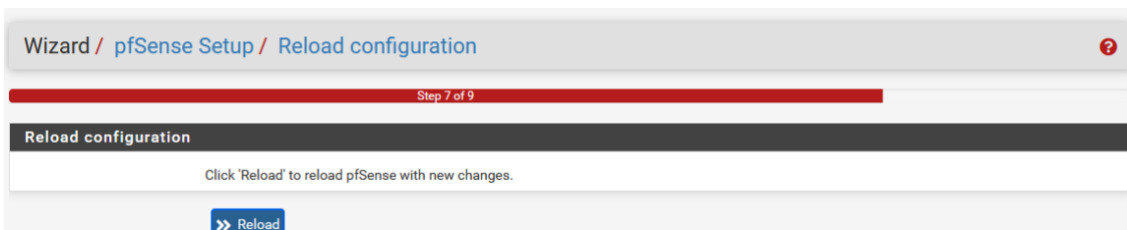
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: [obscured]

Admin Password AGAIN: [obscured]

Next

- Pedir para reiniciar o serviço e aplicar as novas modificações:



Wizard / pfSense Setup / Reload configuration

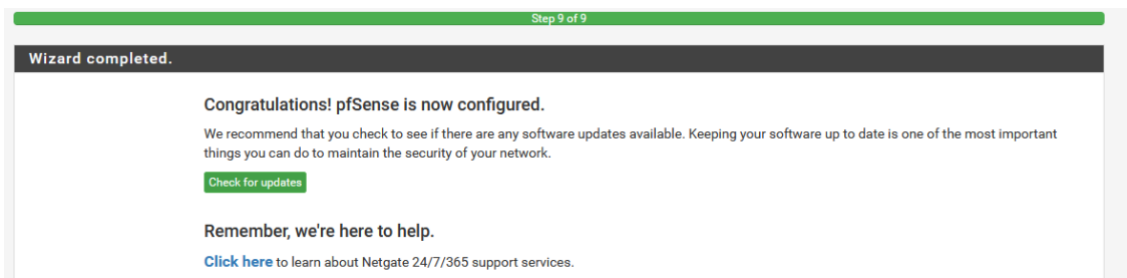
Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

Reload

Se tudo correr bem, será exibida a seguinte janela:



Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

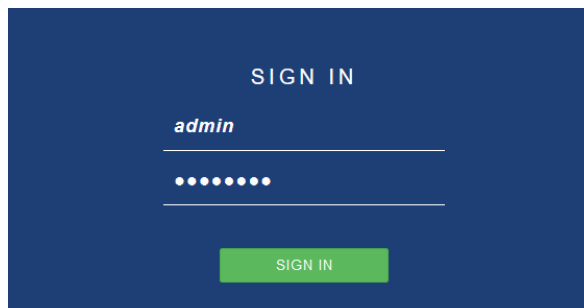
We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

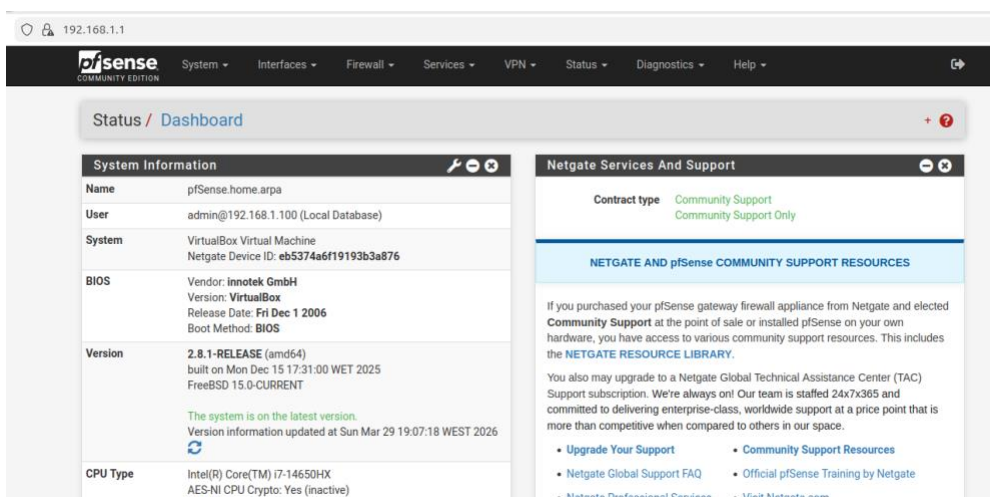
Remember, we're here to help.

Click here to learn about Netgate 24/7/365 support services.

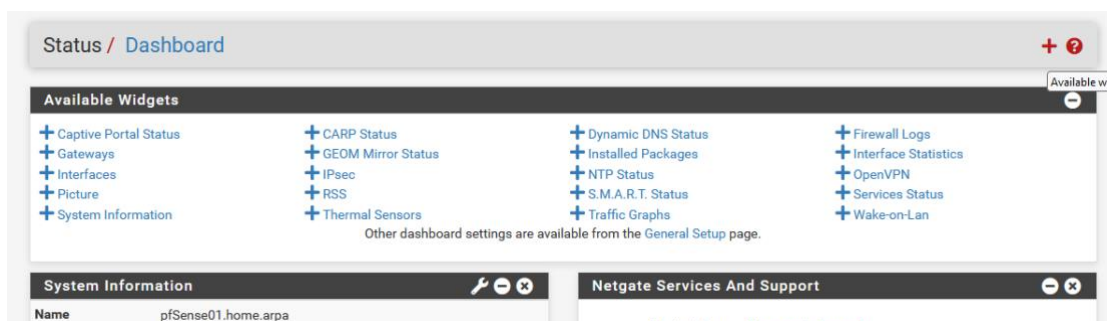
**Passo 25** - Faça o logout na aplicação e insira a nova password que acabou de definir.



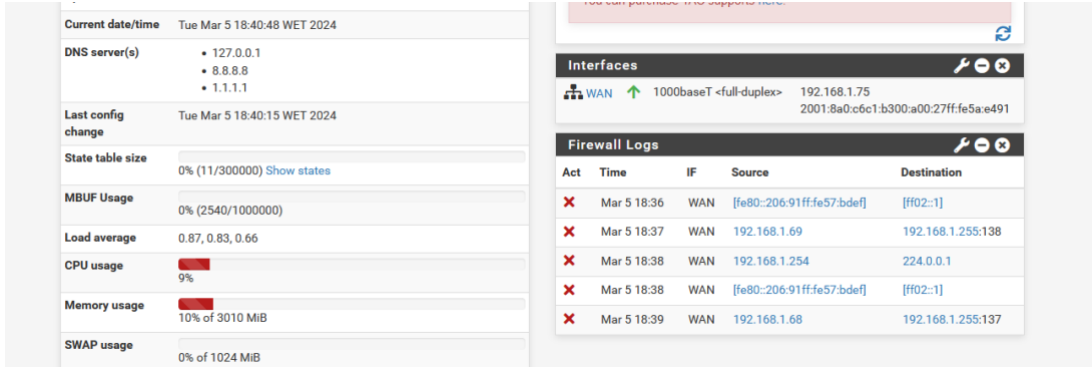
**Visualização da tela inicial:**



Se clicar no botão + (no separador Dashboard da página inicial, vão aparecer opções de personalização da página inicial):



Exemplo de implementação dos logs da firewall:



The screenshot displays the Mikrotik WinBox interface. On the left, the 'System' tab shows various status metrics:

- Current date/time: Tue Mar 5 18:40:48 WET 2024
- DNS server(s): 127.0.0.1, 8.8.8.8, 1.1.1.1
- Last config change: Tue Mar 5 18:40:15 WET 2024
- State table size: 0% (11/300000) Show states
- MBUF Usage: 0% (2540/1000000)
- Load average: 0.87, 0.83, 0.66
- CPU usage: 9%
- Memory usage: 10% of 3010 MiB
- SWAP usage: 0% of 1024 MiB

On the right, the 'Interfaces' tab shows the WAN interface configuration:

- WAN: 100baseT <full-duplex> 192.168.1.75
- MAC: 2001:8a0:c6c1:b300:a00:27ff:fe5a:e491

Below the interfaces, the 'Firewall Logs' tab displays a table of blocked traffic:

Act	Time	IF	Source	Destination
X	Mar 5 18:36	WAN	[fe80::206:91ff:fe57:bdef]	[ff02::1]
X	Mar 5 18:37	WAN	192.168.1.69	192.168.1.255:138
X	Mar 5 18:38	WAN	192.168.1.254	224.0.0.1
X	Mar 5 18:38	WAN	[fe80::206:91ff:fe57:bdef]	[ff02::1]
X	Mar 5 18:39	WAN	192.168.1.68	192.168.1.255:137

## Parte 3 – DHCP Leases (deteção de equipamentos na rede)

Neste momento será exibido uma ligação de rede (que será máquina que estiver ligada na rede interna).

Status / DHCP Leases

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

Search

Search Term:  All

Enter a search string or \*nix regular expression to filter entries.

IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.1.100	08:00:27:14:4c:1e	silva-VirtualBox		2024/04/12 19:03:16	2024/04/12 21:03:16	<input type="button" value="+"/> <input type="button" value="+"/>

Lease Utilization

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.1.10	192.168.1.245	1	236	0% of 236

Para ver todas as ligações detetadas (leases), vamos clicar no botão azul-claro “Show All Configured Leases”:

Status / DHCP Leases

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

Search

Search Term:  Start

Enter a search string or \*nix regular expression to filter entries.

IP Address	MAC Address	Hostname	Description	Start	End	Actions
No leases to display						

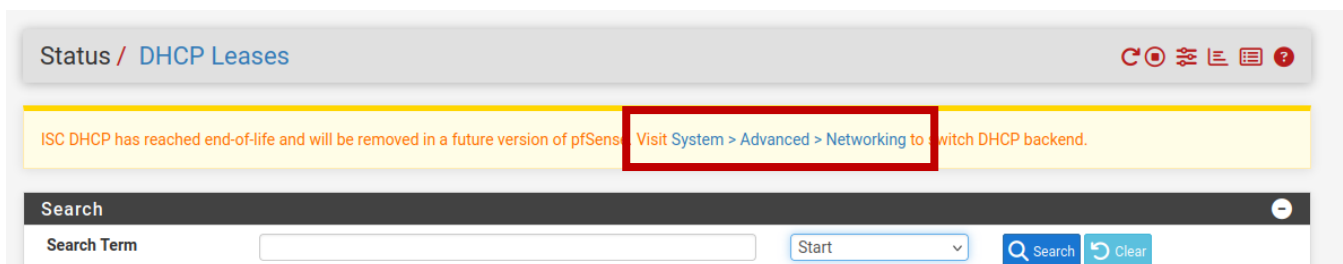
Lease Utilization

Interface	Pool Start	Pool End	Used	Capacity	Utilization
No leases are in use					

Para verificar a deteção de equipamentos na rede com DHCP, inicie a máquina virtual do Windows com o adaptador da rede na opção rede interna e dentro do sistema operativo, a placa de rede tem de estar a obter o IP automaticamente:

Leases							
	IP Address	MAC Address	Hostname	Description	Start	End	Actions
<input checked="" type="checkbox"/> <input type="button" value="↑"/>	192.168.1.96	08:00:27:0b:c6:c0	silva-PC		2024/05/01 13:53:04	2024/05/01 15:53:04	<input type="button" value="+"/> <input type="button" value="+"/>
<input checked="" type="checkbox"/> <input type="button" value="↑"/>	192.168.1.99	08:00:27:8e:cf:17	silva-VirtualBox		2024/05/01 13:36:09	2024/05/01 15:36:09	<input type="button" value="+"/> <input type="button" value="+"/>

No entanto, como pode ver no início da página, aparece um aviso a dizer que a tecnologia ISC DHCP está a chegar ao fim e que será removido nas próximas atualizações. Para precaver esta situação, vamos começar por clicar na hiperligação azul que irá remeter para as configurações de deteção da rede (Networking):



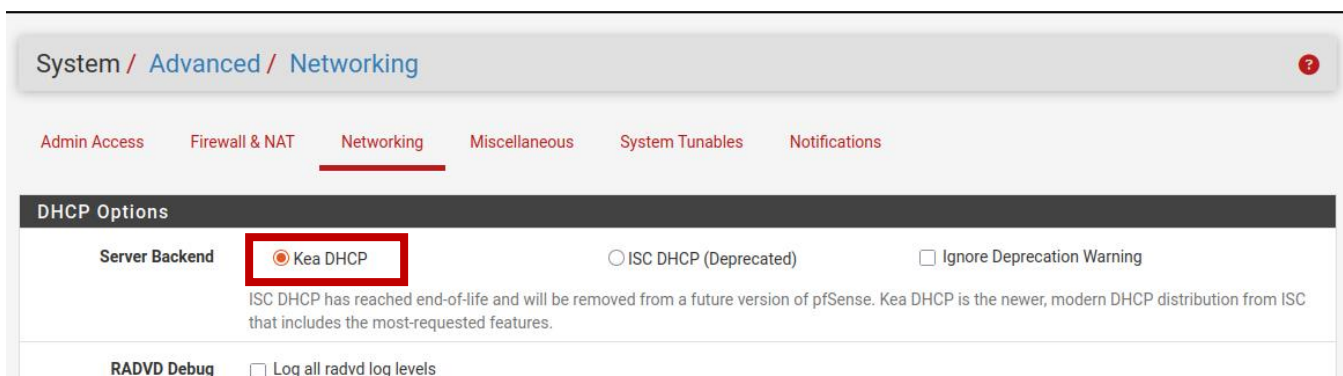
Status / DHCP Leases

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

Search

Search Term  Start

Nas configurações da nova página “Networking”, vamos seleccionar a tecnologia “Kea DHCP” que é o sistema de deteção mais moderno:



System / Advanced / Networking

Admin Access Firewall & NAT **Networking** Miscellaneous System Tunables Notifications

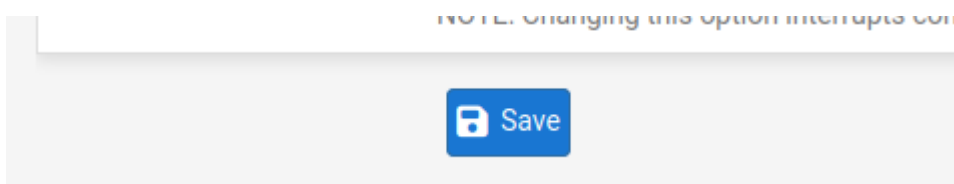
DHCP Options

Server Backend  Kea DHCP  ISC DHCP (Deprecated)  Ignore Deprecation Warning

ISC DHCP has reached end-of-life and will be removed from a future version of pfSense. Kea DHCP is the newer, modern DHCP distribution from ISC that includes the most-requested features.

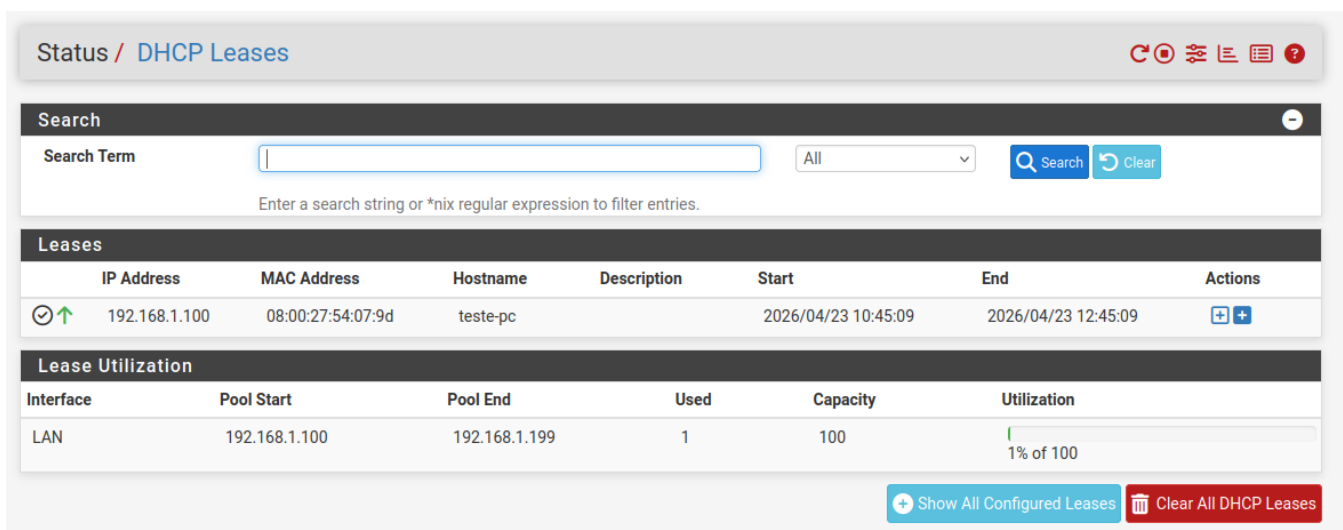
RADVD Debug  Log all radvd log levels

No final, deve ir até ao final da página e clicar no botão azul “Save” para guardar as novas alterações.



NOTE: Changing this option interrupts con...

Ative uma máquina Windows 7 e veja a deteção a acontecer em tempo real:



Status / DHCP Leases

Search

Search Term  All

Enter a search string or \*nix regular expression to filter entries.

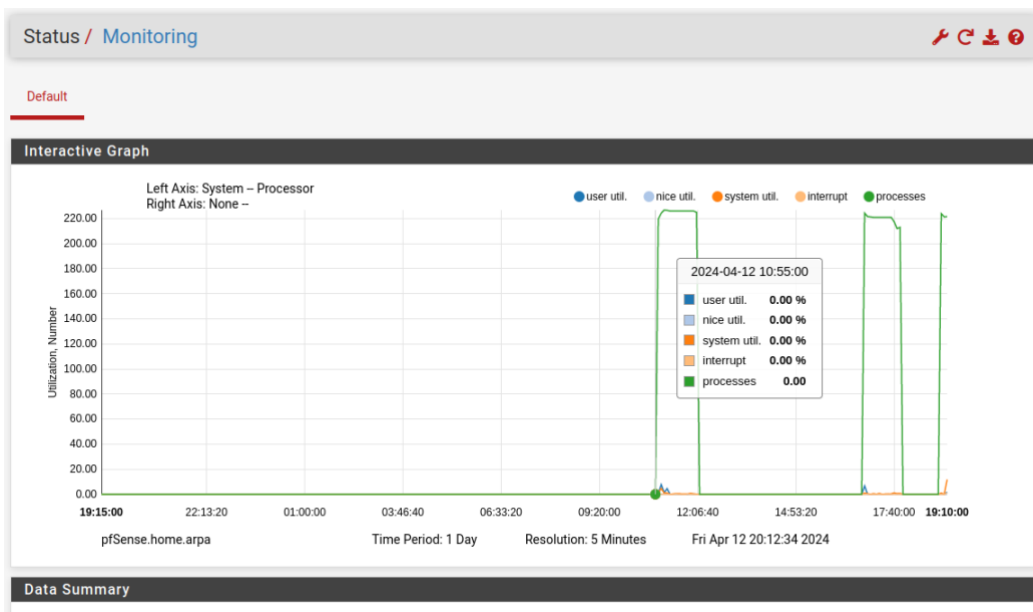
Leases

IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.1.100	08:00:27:54:07:9d	teste-pc		2026/04/23 10:45:09	2026/04/23 12:45:09	

Lease Utilization

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.1.100	192.168.1.199	1	100	<div style="width: 1%; background-color: green;">1% of 100</div>

## Parte 4 – Monitoring (Monitorização de atividades na rede)



## Parte 5 – System Logs (monitorização de eventos e alertas)

Status / System Logs / System / General 🔍 🛠️ 🚫

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

General Gateways Routing DNS Resolver Wireless GUI Service OS Boot

**Last 500 General Log Entries. (Maximum 500)**

Time	Process	PID	Message
Apr 12 17:44:02	kernel		Root mount waiting for: CAM usb1
Apr 12 17:44:02	kernel		Root mount waiting for: CAM usb1
Apr 12 17:44:02	kernel		Root mount waiting for: CAM usb1
Apr 12 17:44:02	kernel		uhub1: 12 ports with 12 removable, self powered
Apr 12 17:44:02	kernel		Root mount waiting for: CAM
Apr 12 17:44:02	kernel		Root mount waiting for: CAM
Apr 12 17:44:02	kernel		Root mount waiting for: CAM
Apr 12 17:44:02	kernel		Root mount waiting for: CAM
Apr 12 17:44:02	kernel		cd0 at ata1 bus 0 scbus1 target 0 lun 0
Apr 12 17:44:02	kernel		cd0: <VBOX CD-ROM 1.0> Removable CD-ROM SCSI device
Apr 12 17:44:02	kernel		cd0: Serial Number VB2-01700376

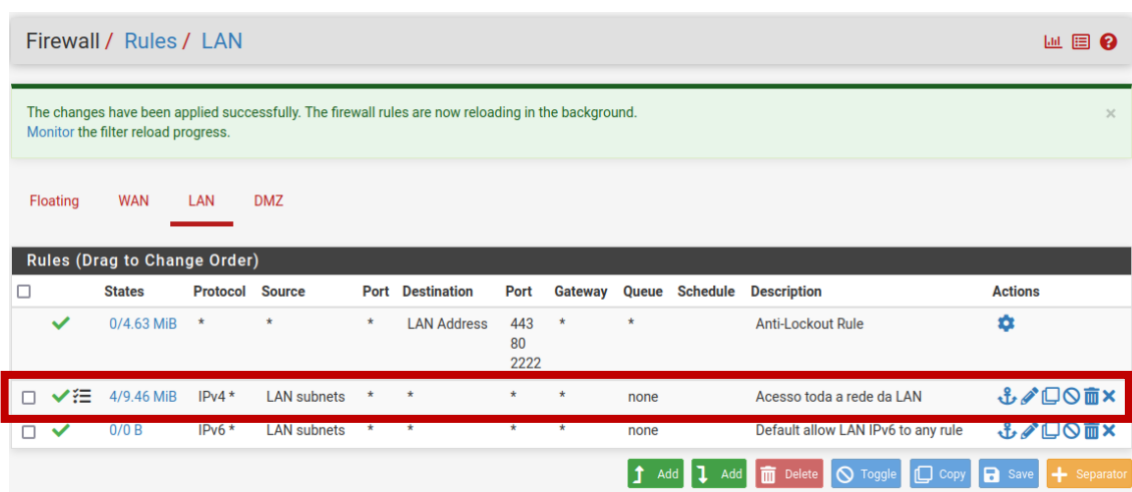
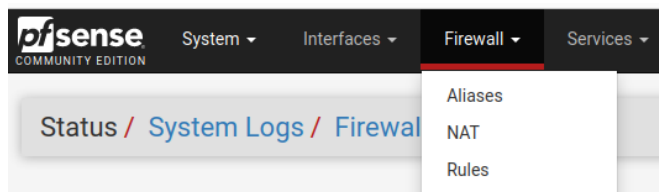
## Parte 6 – Regras da Firewall Pfsense

As regras, permitem estabelecer um conjunto de definições para que a firewall possa identificar e resolver os planos delineados para a nossa rede.

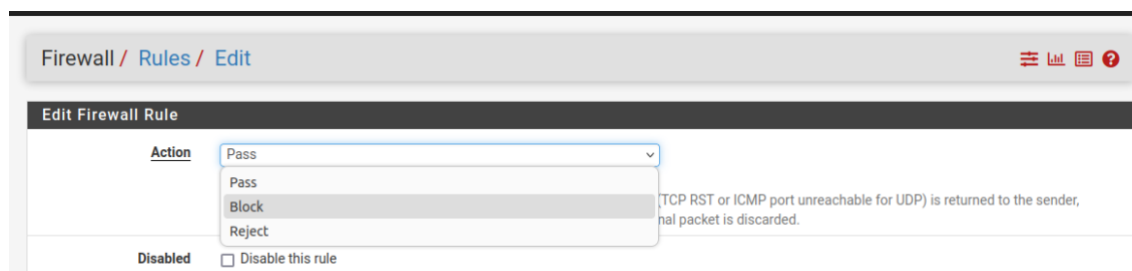
Como tal, devemos ter em consideração uma regra muito importante: *as regras funcionam por hierarquia/prioridade de colocação*, ou seja, *a regra que estiver mais acima é a primeira a ser respeitada e só depois é que começa a processar todas as outras*.

### 6.1 - Regras de bloqueio de internet geral na LAN

- Para bloquear a internet na interface LAN, vamos ao menu superior e selecionar as opções Firewall → Rules. De seguida, deve selecionar a regra IPV4 Lan Subnets (que já vem configurada automaticamente):



- Coloque a propriedade Action como Block:



- Mais abaixo, ative a opção Log (para aparecer a regra de bloqueio nos logs da firewall), e coloque a descrição “Bloquear toda a rede da LAN”:

The screenshot shows the 'Extra Options' section of a firewall rule configuration. The 'Log' checkbox is checked, with a sub-option 'Log packets that are handled by this rule'. A hint below states: '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)'. The 'Description' field contains the text 'Bloquear toda a rede da LAN'. Below this is a note: '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.' There is also an 'Advanced Options' section with a 'Display Advanced' button. The 'Rule Information' section shows a 'Tracking ID' of '0100000101' and an 'Updated' timestamp of '4/14/24 19:49:13 by admin@192.168.1.100 (Local Database)'. A 'Save' button is at the bottom.

- Tente abrir um navegador e ver se consegue aceder a algum website. Se tudo correr como o que foi especificado, será bloqueado e nos eventos da firewall (Status → System Logs), irá visualizar a seguinte informação:

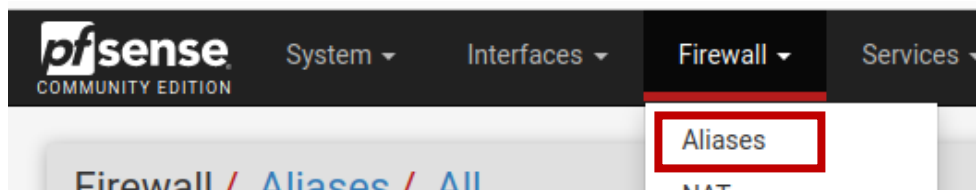
The screenshot shows the 'Status / System Logs / Firewall / Normal View' page. The 'Firewall' tab is selected. Below the navigation tabs, there are three view options: 'Normal View', 'Dynamic View', and 'Summary View'. The main content area displays 'Last 286 Firewall Log Entries. (Maximum 500)'. A table shows the log entries with columns: Action, Time, Interface, Rule, Source, Destination, and Protocol. The 'Time' column header is highlighted with a red box. The table shows three entries, all with a red 'X' in the Action column, indicating blocked traffic. The entries are ordered chronologically from newest to oldest.

Action	Time	Interface	Rule	Source	Destination	Protocol
X	Apr 30 19:24:13	LAN	Bloquear toda a rede da LAN (100000101)	192.168.1.99:58491	192.168.1.1:53	UDP
X	Apr 30 19:24:13	LAN	Bloquear toda a rede da LAN (100000101)	192.168.1.99:60964	192.168.1.1:53	UDP
X	Apr 30 19:24:13	LAN	Bloquear toda a rede da LAN (100000101)	192.168.1.99:50023	192.168.1.1:53	UDP

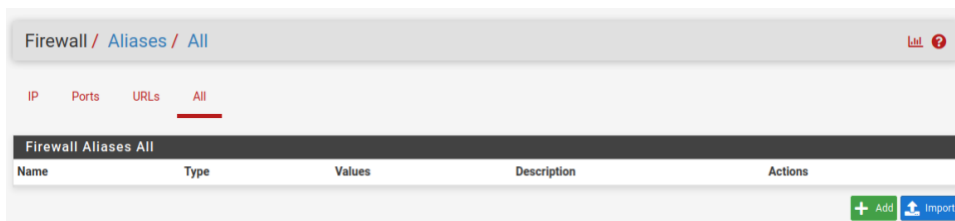
**NOTA IMPORTANTE:** Verifique o separador Time, pois a ordenação da firewall mostra os dados por ordem crescente. *Clique em cima no nome duas vezes separadas e veja a ordenação de forma decrescente.*

## 6.2 - Regras de bloqueio por um domínio específico (exemplo do Facebook) + Aliases

- Também podemos bloquear domínios específicos na rede. Como tal, vamos em primeiro criar um alias (agrupamento de informação para depois ativar a regra mais facilmente). No menu superior, deve seleccionar as opções Firewall → Aliases:

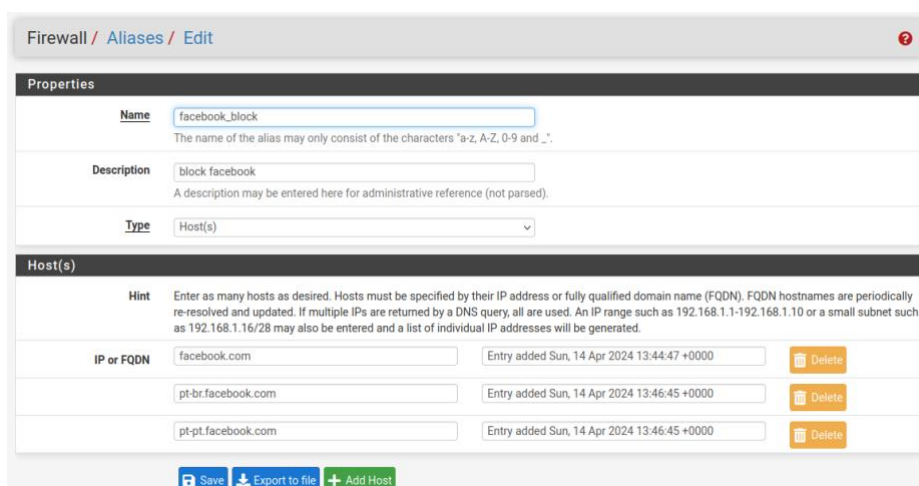


- Clique no botão verde ADD:

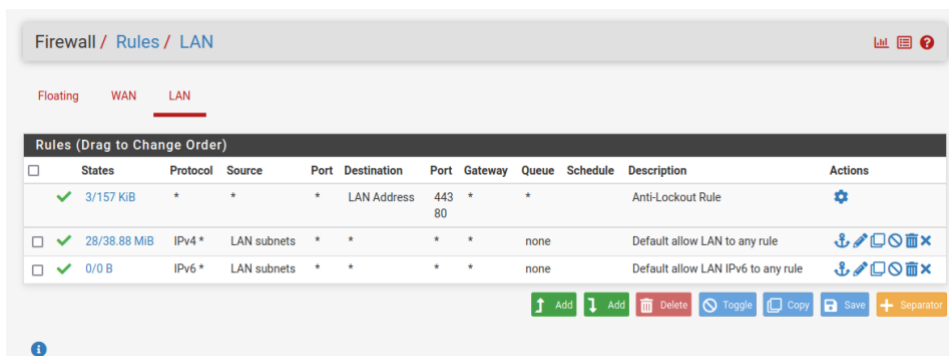


Indique as seguintes informações:

- **Nome:** Facebook\_block;
- **Descrição:** Block\_facebook (depois vamos importar este nome nas regras);
- **Tipo:** Host (domínio);
- Para tal, não podemos esquecer, que os websites e aplicações podem ter várias maneiras de acesso, como por exemplo, o Facebook, tem o acesso normal (Facebook.com), mas também, versão portuguesa, pt-pt.facebook.com e a versão do brasil pt-br.facebook.com.
  - Indique estes parâmetros na zona dos Hosts:



- Volte ao separador das regras da firewall e vamos definir uma regra para que qualquer computador na LAN não possa aceder ao website Facebook. Como tal, clique no botão ADD com seta para cima (para indicar que esta regra é a primeira a ser implementada, antes de qualquer regra que já exista):



- Coloque os valores:
  - **Ação:** Reject;
  - **Interface:** LAN;
  - **Address Family:** apenas IPv4;
  - **Protocolo:** UDP/TCP;
  - **Origem:** Any;
  - **Destino:** selecione a opção Address or Alias e no campo mais a frente coloque o nome que deu na descrição dos passos anteriores (para este importar todos os domínios em vez de um único específico):

Firewall / Rules / Edit

### 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   /

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.

- Mais abaixo, ative a opção Log (para aparecer a regra de bloqueio nos logs da firewall), e coloque a descrição “Regra de bloqueio do facebook”:

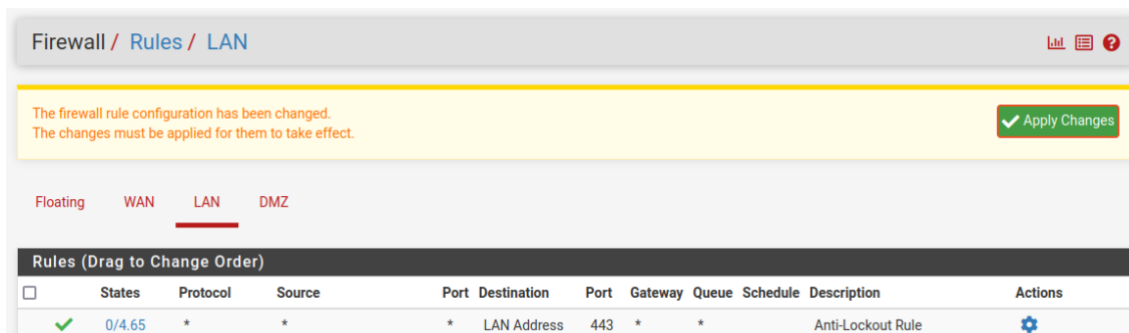
**Extra Options**

**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 the [Status: System Logs: Settings](#) page).

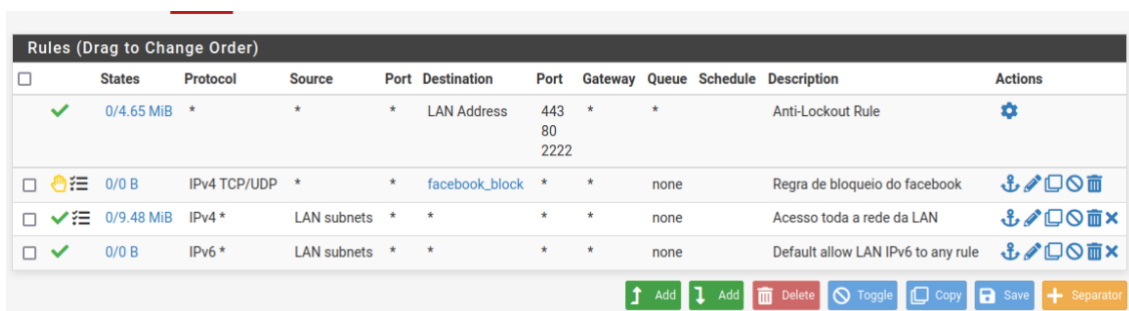
**Description**    
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the rule log.

**Advanced Options**

**Muito Importante:** Não esquecer de gravar as últimas alterações no final da página. De seguida, a firewall vai pedir para aplicar as novas regras de configuração, e como tal, deve clicar no botão verde “Apply Changes”:



**Resultado da regra aplicada:**



- Tente abrir um navegador e ver se consegue aceder a algum website. Se tudo correr como o que foi especificado, será bloqueado e nos eventos da firewall (Status → System Logs), irá visualizar a seguinte informação:

✗	May 1 14:37:51	LAN	Regra de bloqueio do facebook (1713102341)	192.168.1.99:33378	157.240.212.35:443	TCP:S
✗	May 1 14:37:51	LAN	Default deny rule IPv6 (1000000105)	[fe80::45a:b8a9:664d:7645]:59688	[2a03:2880:f152:82:face:b00c:0:25de]:443	TCP:S
✗	May 1 14:37:51	LAN	Default deny rule IPv6 (1000000105)	[fe80::45a:b8a9:664d:7645]:59676	[2a03:2880:f152:82:face:b00c:0:25de]:443	TCP:S
✗	May 1 14:37:51	LAN	Default deny rule IPv6 (1000000105)	[fe80::45a:b8a9:664d:7645]:59672	[2a03:2880:f152:82:face:b00c:0:25de]:443	TCP:S
✗	May 1 14:37:51	LAN	Regra de bloqueio do facebook (1713102341)	192.168.1.99:33362	157.240.212.35:443	TCP:S

### 6.3 – Schedule - Agendamento de horários para serviços de rede

Por vezes pode haver a necessidade de fazer agendamentos de permissões e negações de serviços em determinados horários.

Para realizar esta tarefa, temos de trabalhar 3 seções:

1. Criar agendamento de serviços (**Firewall** → **Schedules**);
2. Criar o Alias para indicar os computadores ou rede (para depois associar o Schedule) para importar as definições mais rapidamente;
3. Criar regra e implementar os dois passos anteriores;

*Neste exemplo, queremos permitir acesso na rede LAN apenas entre as 20h e a 00H em determinados dias (neste caso desde o dia 1 de maio até 5 de Maio).*

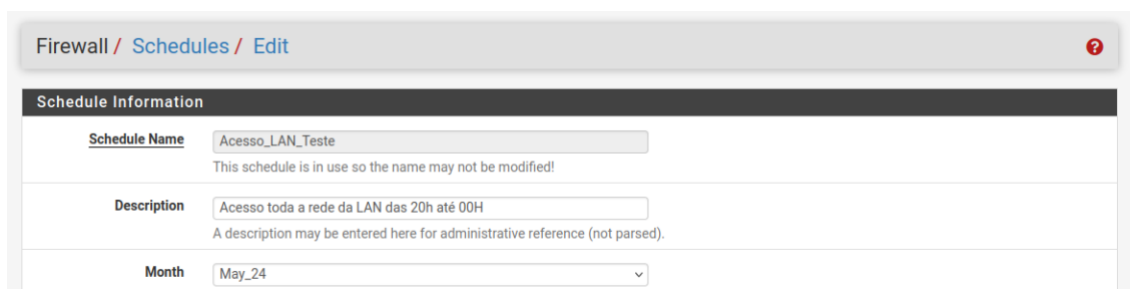
1. Criar agendamento de serviços (Firewall → Schedules);

Clicar no botão ADD:



Colocar as informações (como na imagem mais abaixo):

**Nota Importante:** Deve em primeiro selecionar os dias no calendário e só depois indicar as horas de início e de fim. Após a inserção dessa informação é que deverá carregar no botão verde “Add Time”:



**Date**

May_2024						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

**Time**

<input type="text" value="0"/>	<input type="text" value="00"/>	<input type="text" value="20"/>	<input type="text" value="00"/>
Start Hrs	Start Mins	Stop Hrs	Stop Mins

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

**Time range description**

A description may be entered here for administrative reference (not parsed).

+ Add Time
Clear selection

---

**Configured Ranges**

May 1 - 5	0:00	20:00		Delete
Day(s)	Start time	Stop time	Description	

Save

Gravar as novas informações.

2. Criar o Alias para indicar os computadores ou rede (para depois associar o Schedule) para importar as definições mais rapidamente;

**Nota Importante:** No separador Host(s), se desejar colocar um domínio inteiro (em vez de alguns equipamentos, deve colocar o IP do domínio e a máscara de rede.

Exemplo: se a rede está em 192.168.1.xx então o domínio será 192.168.1.0/24

Firewall / Aliases / Edit

---

**Properties**

**Name**   
The name of the alias may only consist of the characters \*a-z, A-Z, 0-9 and \_\*.

**Description**   
A description may be entered here for administrative reference (not parsed).

**Type**

---

**Host(s)**

**Hint** Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostname re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

**IP or FQDN**

Save
+ Add Host

Depois de gravar as novas alterações, e voltar a editar o alias, repare que este colocou todos os hosts do domínio:

Host(s)		
<b>Hint</b>	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.	
<b>IP or FQDN</b>	192.168.1.0	toda a rede lan
	192.168.1.1	toda a rede lan
	192.168.1.2	toda a rede lan
	192.168.1.3	toda a rede lan
	192.168.1.4	toda a rede lan
	192.168.1.5	toda a rede lan
	192.168.1.253	toda a rede lan
	192.168.1.254	toda a rede lan
	192.168.1.255	toda a rede lan

Save Export to file Add Host

### 3. Criar regra e implementar os dois passos anteriores;

Criar uma nova regra com ação de bloqueio para não deixar aceder a rede LAN fora do horário estabelecido (neste exemplo a rede só deve funcionar entre as 20h e as 00H):

- **Action:** Block;
- **Interface:** LAN;
- **Address Family:** IPv4
- **Protocol:** Any

Firewall / Rules / Edit

#### Edit Firewall Rule

**Action** Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN

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

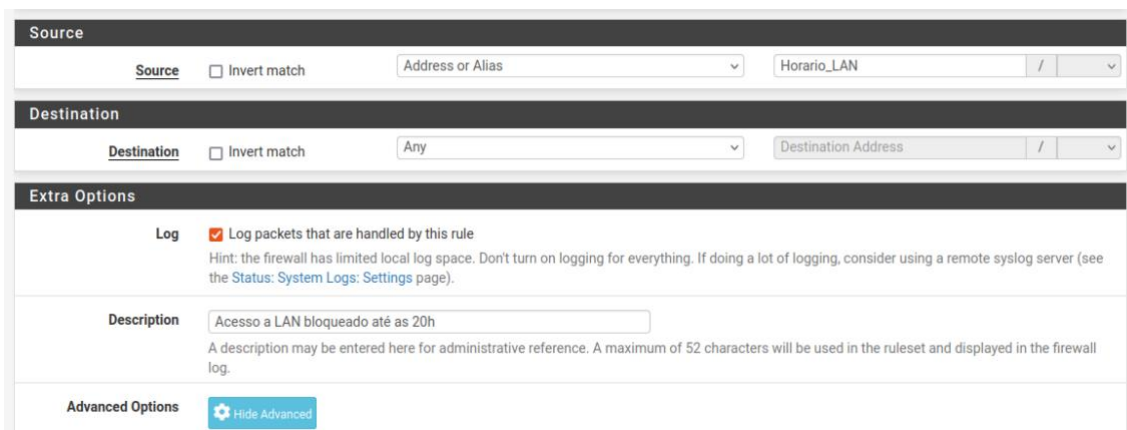
**Address Family** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** Any

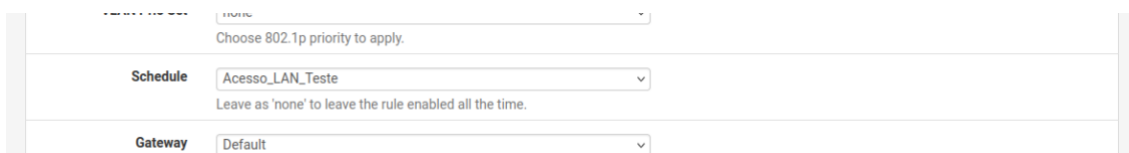
Choose which IP protocol this rule should match.

- **Source:** Address or Alias e escrever o nome Horário\_LAN (tem de ser o mesmo nome dado no Aliases, do qual, basta escrever as primeiras iniciais e este filtra e obtém o nome em causa);
- **Destination:** Any
- **Ativar Log;**
- **Description:** Acesso a Lan bloqueado até as 20H;



The screenshot shows the configuration for a firewall rule. The **Source** section has 'Address or Alias' selected and 'Horario\_LAN' entered. The **Destination** section has 'Any' selected. In the **Extra Options** section, the **Log** checkbox is checked with the text 'Log packets that are handled by this rule'. The **Description** field contains 'Acesso a LAN bloqueado até as 20h'. At the bottom, there is a blue button labeled 'Show Advanced'.

- **Clicar no botão azul com o nome "Show Advanced"** e perto do final, vamos ter uma opção para indicar a regra do agendamento (que foi feito no passo 1):



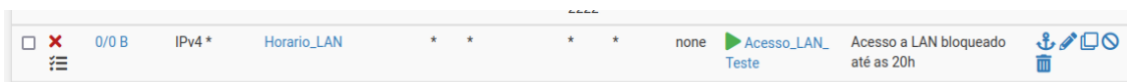
The screenshot shows the **Schedule** section of the firewall rule configuration. The dropdown menu is set to 'Acesso\_LAN\_Teste'. Below the dropdown, it says 'Leave as 'none' to leave the rule enabled all the time.' The **Gateway** section below is set to 'Default'.

### Testes de implementação:

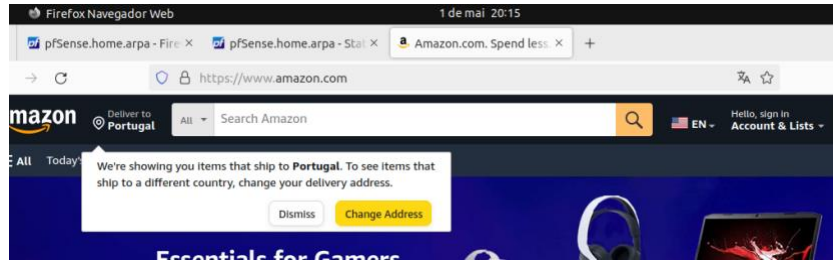
- **Resultado antes das 20H no dia 1 de Maio:**



- **Resultado da regra antes das 20H:**



- *Resultado depois das 20H no dia 1 de Maio:*



- *Resultado da regra depois das 20H:*

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/6.12 MIB	*	*	*	LAN Address	443 80 2222	*	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	Horario_LAN	*	*	*	*	none	Acesso_LAN_ Tests	Acesso a LAN bloqueado até as 20h	
<input type="checkbox"/>	0/0 B	IPv4 *	EasyRuleBlockHostsLAN	*	*	*	*	none		This rule is not currently active because its period has expired	

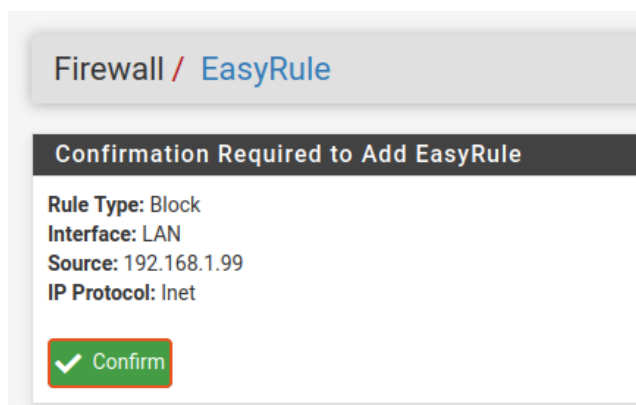
#### 6.4 - EasyRule - Regras de bloqueio por deteção e identificação

Ao analisar as informações dos eventos na firewall, podemos visualizar os dados de origem e destino da comunicação entre equipamentos.

Caso queira bloquear um computador nas regras da firewall, basta clicar na opção – (menos) atrás do endereço IP (normalmente até aparece uma caixa a indicar a mensagem “EasyRule: Add to Block List”):



Este vai abrir uma nova janela para confirmar esta opção.



Ao confirmar, o EasyRule vai fazer duas operações:

- Cria/edita o Alias com os vários endereços que foram pedidos para bloquear;



Firewall / Aliases / Edit

**Properties**

**Name** EasyRuleBlockHostsLAN  
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description** Blocked via EasyRule  
A description may be entered here for administrative reference (not parsed).

**Type** Network(s)

**Network(s)**

**Hint** Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN				
192.168.1.100	/	32	Entry added Wed, 17 Apr 2024 09:37:59 +0000	Delete
192.168.1.99	/	32	Description	Delete

Save Export to file Add Network

- Cria regra (apenas uma vez) para bloquear o conteúdo definido no Alias anterior;

Firewall / Rules / LAN

Floating WAN LAN DMZ

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/3.66 MiB	*	*	*	LAN Address	443 80 2222	*	*	*	Anti-Lockout Rule	⚙️
<input type="checkbox"/>	0/4 KIB	IPv4 *	EasyRuleBlockHostsLAN	*	*	*	*	none		Blocked via EasyRule	📌 ⚙️ 🗑️
<input type="checkbox"/>	0/4 KIB	IPv4 *	facebook_	*	facebook_	*	*	none		Regra de bloqueio do facebook	📌 ⚙️ 🗑️
<input type="checkbox"/>	0/8.06 MiB	UDP		*	block	*	*	none			📌 ⚙️ 🗑️
<input checked="" type="checkbox"/>	0/8.06 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	📌 ⚙️ 🗑️
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 ⚙️ 🗑️

Add Add Delete Toggle Copy Save Separator

## Parte 7 – Ativar DMZ no Pfsense

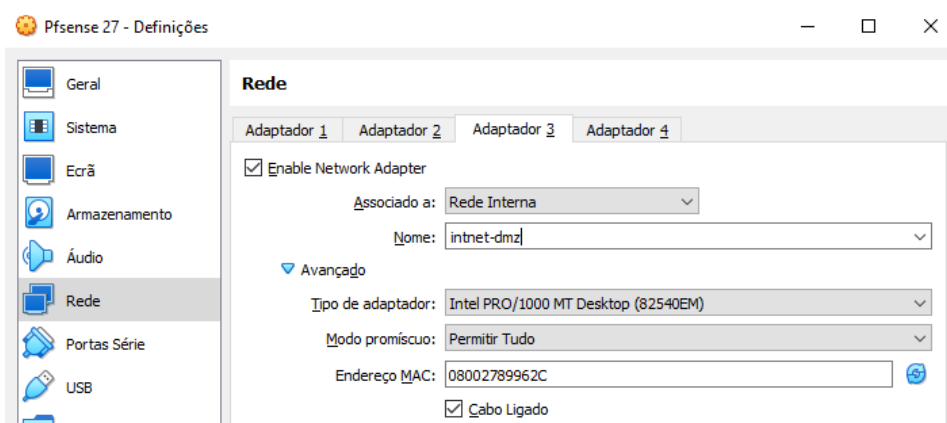
Para adicionar uma nova interface, mais especificamente, incluir a interface DMZ (Zona desmilitarizada), vamos ter de adicionar uma placa de rede adicional nas propriedades da máquina virtual.

Com esta opção, vamos ter 3 interfaces na firewall Pfsense:

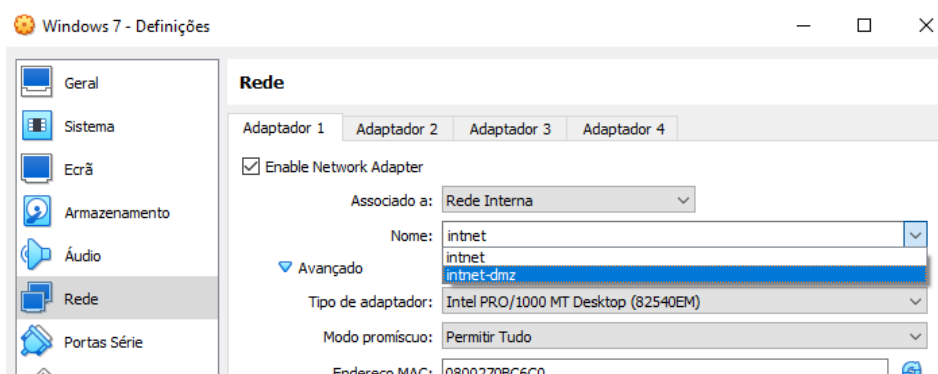
- Interface WAN
- Interface LAN
- Interface DMZ

**Passo 1** – Desligue a máquina virtual do pfsense e de seguida vamos as definições da mesma;

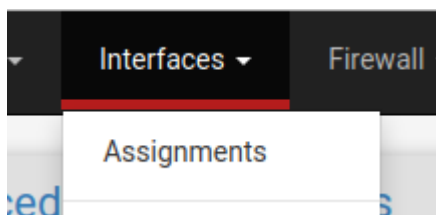
**Passo 2** – Dentro das definições da máquina virtual, vamos clicar na opção rede e adicionar um novo adaptador (em rede interna) e na opção do nome, vamos dar um nome diferente, para que este crie duas redes diferentes com o nome “intnet-dmz”:



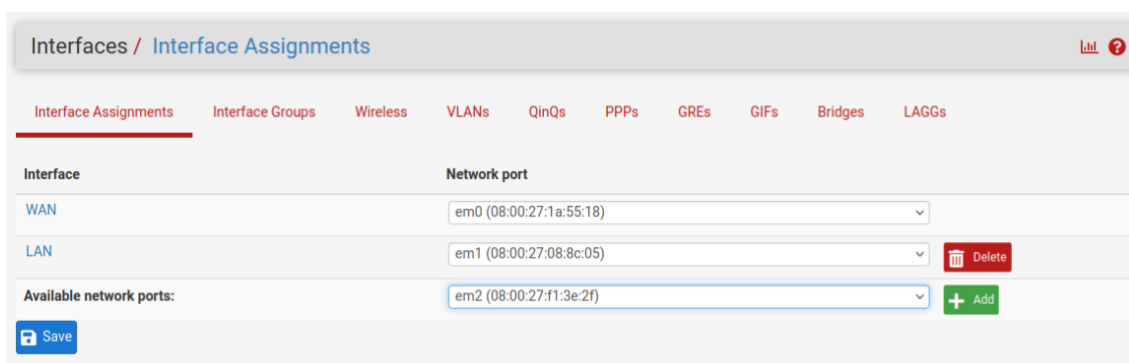
**Passo 3** - Vamos colocar a máquina virtual do Windows 7 dentro da interface DMZ. Para tal, deve ir as propriedades de rede da máquina virtual e mudar o adaptador de rede para a rede interna e no nome deve colocar a nova interface que foi criada no passo anterior:



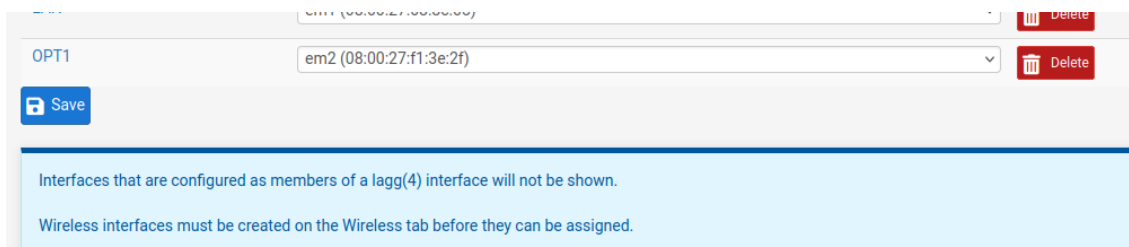
**Passo 4** – Entrar na plataforma online do pfsense e no menu superior deve seleccionar as opções *Interfaces* → *Assignments*



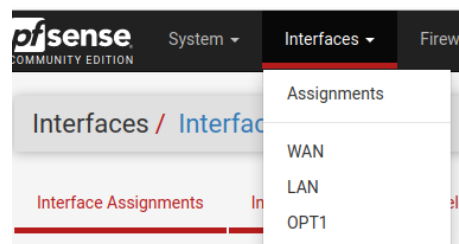
**Passo 5** – Se tudo correr bem, será disponibilizada a nova interface da DMZ:



De seguida, clique no botão ADD no lado direito para proceder a configuração e no final das opções, clique em Save para salvar as novas configurações;



**Passo 6** – Para aceder à interface da DMZ, deve ir ao menu superior e clicar nas opções Interfaces → OPT1 (normalmente este é o nome):



**Passo 7** – Dentro da interface da DMZ, deve realizar os seguintes passos:

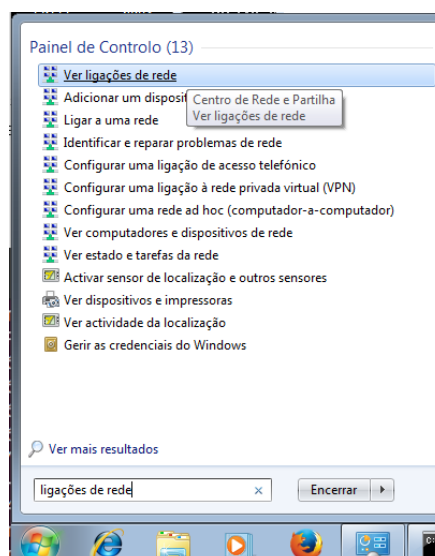
- Habilitar a interface;
- Mudar o nome para DMZ;

- Configuração IPv4 deve ser: Static IPv4;
- Mais abaixo no separador “Static IPv4 Configuration”, vamos indicar que queremos a rede da DMZ na interface com o IP 192.168.2.254/24:

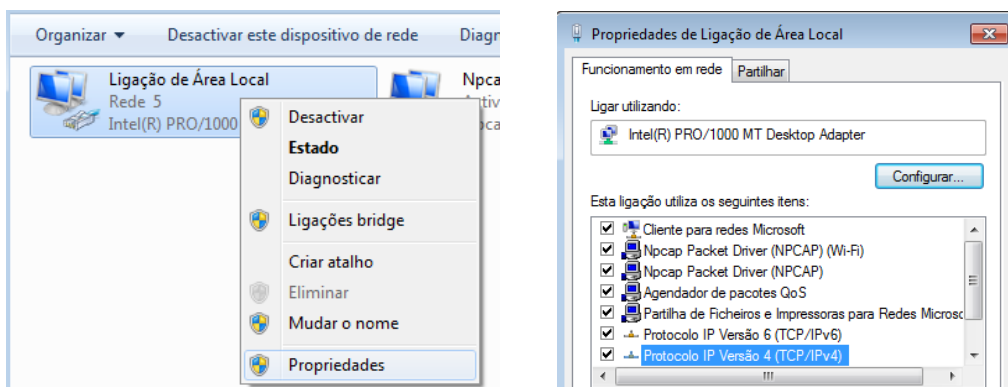
No final, deve ir ao fundo da página e clicar em Save para salvar as novas configurações. Após assumir as novas configurações, não esqueça que é necessário aplicar as novas alterações:

**Passo 8** – Inicie a máquina virtual do Windows 7 e quando esta estiver operacional, devemos alterar os dados da placa de rede para atribuir um IP estático (tal como definido anteriormente). Para tal, faça os seguintes passos:

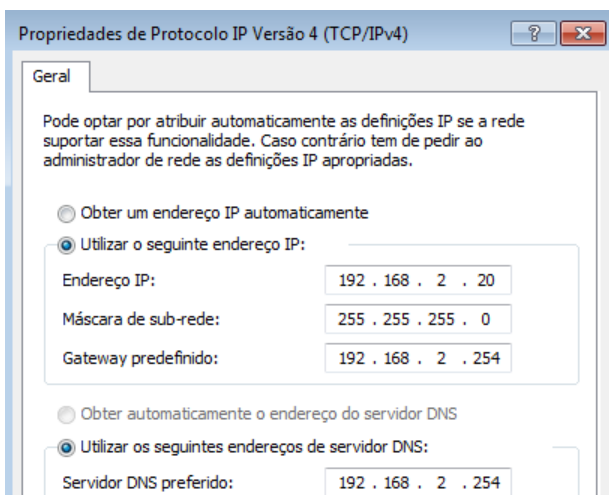
- Clicar no iniciar do Windows e escrever a expressão “ligações de rede” e clicar na opção com o nome “ver ligações de rede”:



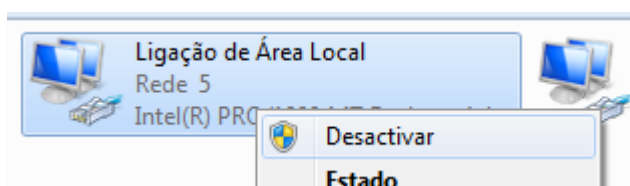
- Na opção ligação de rede local, deve clicar com o lado direito do rato em cima da opção e seleccionar “Propriedades” e seleccionar a opção Protocolo IP Versão 4 (TCP/IPv4):



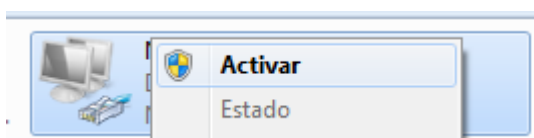
- Alterar a gama de endereço IP para um IP estático e colocar as seguintes propriedades:



Guarde as novas alterações de seguida, deve reiniciar a interface de rede no Windows:



E voltar a ativar:



Quando a interface for reiniciada e se tentar fazer ping na interface DMZ da firewall Pfense, este ainda não vai funcionar:

```

C:\Windows\system32\cmd.exe
C:\Users\silva>ping 192.168.2.254
A fazer ping para 192.168.2.254 com 32 bytes de dados:
Control-C
^C
C:\Users\silva>_
  
```

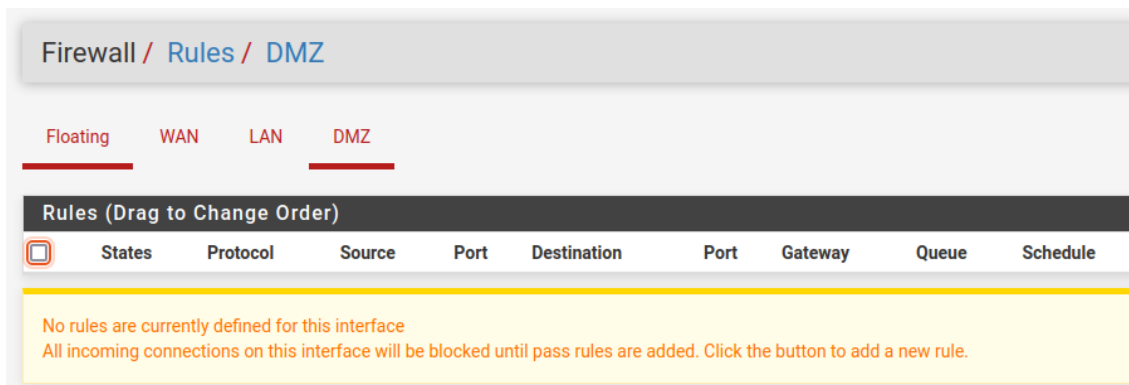
Isto acontece, pois ainda não existe nenhuma regra padrão para trabalhar nessa interface.

Mas quando estiver numa máquina ligada na rede LAN, este vai permitir pingar a interface DMZ:

```

root@silva-VirtualBox: /home/silva × silva@silva-VirtualBox: ~
root@silva-VirtualBox:/home/silva# ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 56(84) bytes of data.
64 bytes from 192.168.2.254: icmp_seq=1 ttl=64 time=0.399 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=0.545 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=0.431 ms
64 bytes from 192.168.2.254: icmp_seq=4 ttl=64 time=0.475 ms
^C
--- 192.168.2.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3065ms
rtt min/avg/max/mdev = 0.399/0.462/0.545/0.054 ms
root@silva-VirtualBox:/home/silva#
  
```

**Passo 9** – Para tal, vamos ter de criar algumas regras essenciais na interface DMZ, do qual, ainda não deve ter nada. Para tal, vamos ao menu superior da firewall Pfsense e clique nas opções **Firewall** → **Rules** e mais abaixo escolha a opção DMZ:



Adicione as seguintes regras:

**Regra DNS:**

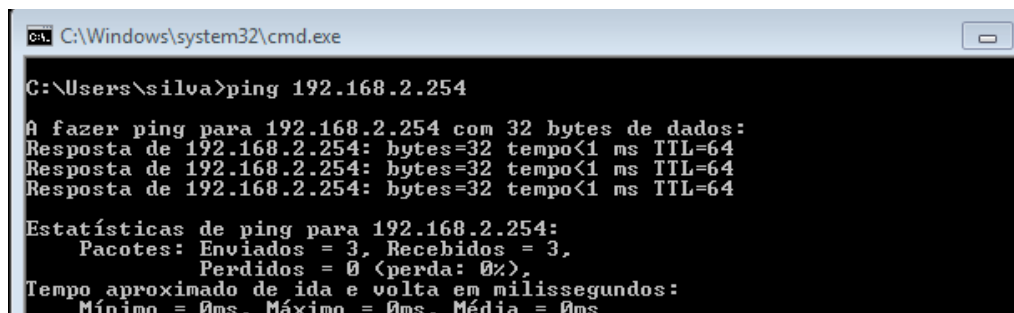
- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: UDP
- Source: DMZ subnets
- Destination: DMZ address

- Porta FROM: 53 (DNS)
- Porta TO: 53 (DNS)
- Extra Options:
  - Ativar a opção Log;
  - Description: Ativar o protocolo DNS na interface DMZ

### Regra ICMP:

- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: ICMP
- Extra Options:
  - Ativar a opção Log;
  - Description: Ativar o protocolo ICMP na interface DMZ

Depois de ativar estas duas regras, não esqueça de aplicar as novas alterações e de seguida, vamos a máquina virtual do Windows 7 e faça ping para a interface DMZ, só que desta vez, como já foram dadas as novas regras, conseguimos fazer ter sucesso:



```
C:\Windows\system32\cmd.exe

C:\Users\silva>ping 192.168.2.254

À fazer ping para 192.168.2.254 com 32 bytes de dados:
Resposta de 192.168.2.254: bytes=32 tempo<1 ms TTL=64
Resposta de 192.168.2.254: bytes=32 tempo<1 ms TTL=64
Resposta de 192.168.2.254: bytes=32 tempo<1 ms TTL=64

Estatísticas de ping para 192.168.2.254:
    Pacotes: Enviados = 3, Recebidos = 3,
              Perdidos = 0 (perda: 0%),
    Tempo aproximado de ida e volta em milissegundos:
      Mínimo = 0ms, Máximo = 0ms, Média = 0ms
```

Como podemos ter outros serviços dentro da DMZ, vamos também colocar as seguintes regras adicionais:

### Regra NTP (Network Time Protocol - sincronizar relógios de computadores):

- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: UDP
- Source: DMZ subnets
- Destination: DMZ address
  - Porta FROM: 123 (NTP)
  - Porta TO: 123 (NTP)
- Extra Options:

- Ativar a opção Log;
- Description: Ativar a regra NTP na interface DMZ

### **Regra FTP** (File Transfer Protocol):

- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: TCP
- Source: DMZ subnets
- Destination: any
  - Porta FROM: 21 (FTP)
  - Porta TO: 21 (FTP)
- Extra Options:
  - Ativar a opção Log;
  - Description: Ativar a regra FTP na interface DMZ

### **Regra HTTP:**

- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: TCP
- Source: DMZ subnets
- Destination: any
  - Porta FROM: 80 (HTTP)
  - Porta TO: 80 (HTTP)
- Extra Options:
  - Ativar a opção Log;
  - Description: Ativar a regra HTTP na interface DMZ

### **Regra HTTPS (c/ SSL):**

- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: TCP
- Source: DMZ subnets
- Destination: any
  - Porta FROM: 443 (HTTPS)

- Porta TO: 443 (HTTPS)
- Extra Options:
  - Ativar a opção Log;
  - Description: Ativar a regra HTTPS na interface DMZ

**Resumo Regras:**

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	2/18 KIB	IPv4 UDP	DMZ subnets	*	DMZ address	53 (DNS)	*	none		Ativar o protocolo DNS na interface DMZ	
<input type="checkbox"/>	0/600 B	IPv4 ICMP any	*	*	*	*	*	none		Ativar o protocolo ICMP na interface DMZ	
<input type="checkbox"/>	0/0 B	IPv4 UDP	DMZ subnets	*	DMZ address	123 (NTP)	*	none		Ativar a regra NTP na interface DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ subnets	*	*	21 (FTP)	*	none		Ativar a regra FTP na interface DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	none		Ativar a regra HTTP na interface DMZ	
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ subnets	*	*	443 (HTTPS)	*	none		Ativar a regra HTTPS na interface DMZ	

**Passo 10** – No entanto, também podemos pingar qualquer endereço na interface LAN. Faça o ping num endereço que esteja na interface LAN e verifique o resultado do ping. Caso seja afirmativo, temos de bloquear os pedidos ICMP. Como tal, adicione regra para bloquear pings para dentro da lan e proteger as interfaces:

**Regra ICMP:**

- Action: Block
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: ICMP
- Source: Any
- Destination: LAN Subnets
- Extra Options:
  - Ativar a opção Log;
  - Description: Bloquear o protocolo ICMP na interface DMZ para LAN

**Esta regra tem de ser a primeira regra a ser executada:**

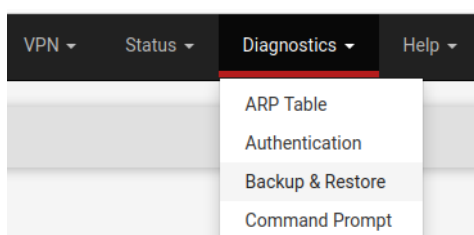
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	LAN subnets	*	*	none		Bloquear ping para lan	

## Parte 8 – Backup e Restore

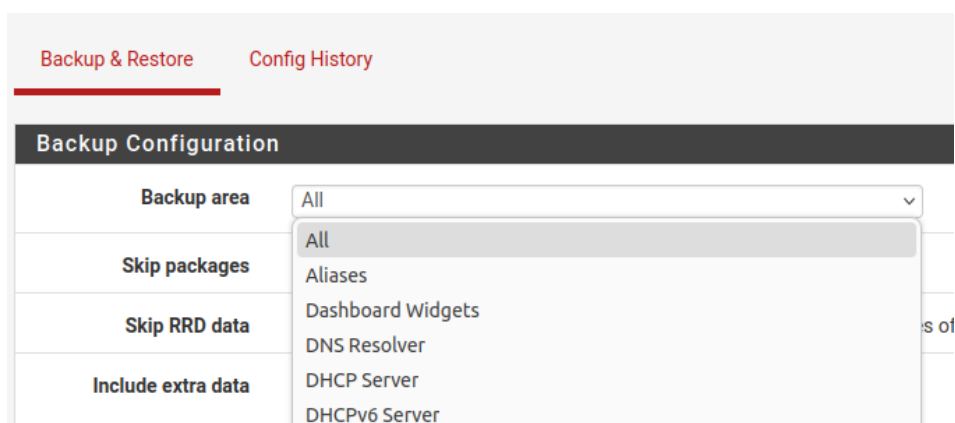
O sistema de backup do pfSense é muito importante para usar em eventuais problemas de hardware ou atualizações que não tenham sido efetuadas com sucesso. Como tal, vamos ver como fazer o backup e eventualmente o restore (restaurar).

### 8.1 - Backup

**Passo 1** – Para realizar o backup manual, devemos ir ao menu superior da aplicação e clicar nas opções **Diagnostics** → **Backup & Restore**



**Passo 2** – Na opção **Backup Area** tem a possibilidade de realizar backup de todas as configurações, ou, pode especificar o que deseja especificamente:

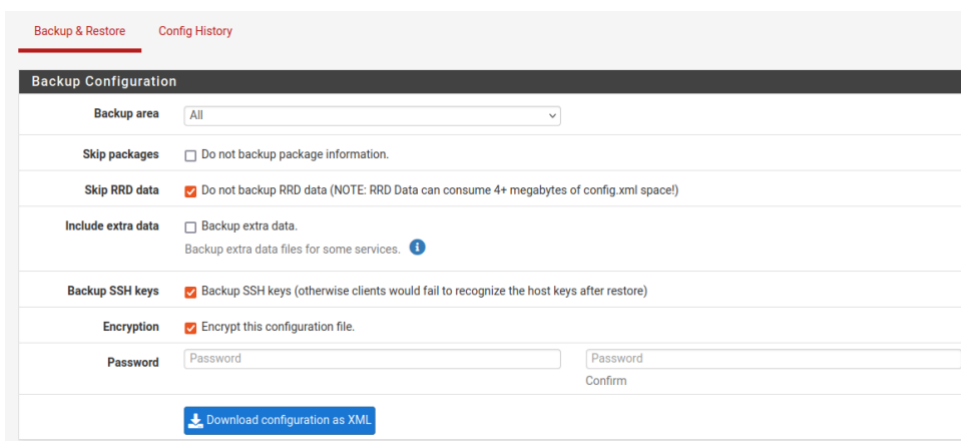


**Passo 3** – Para além da opção Backup Area, temos os seguintes campos:

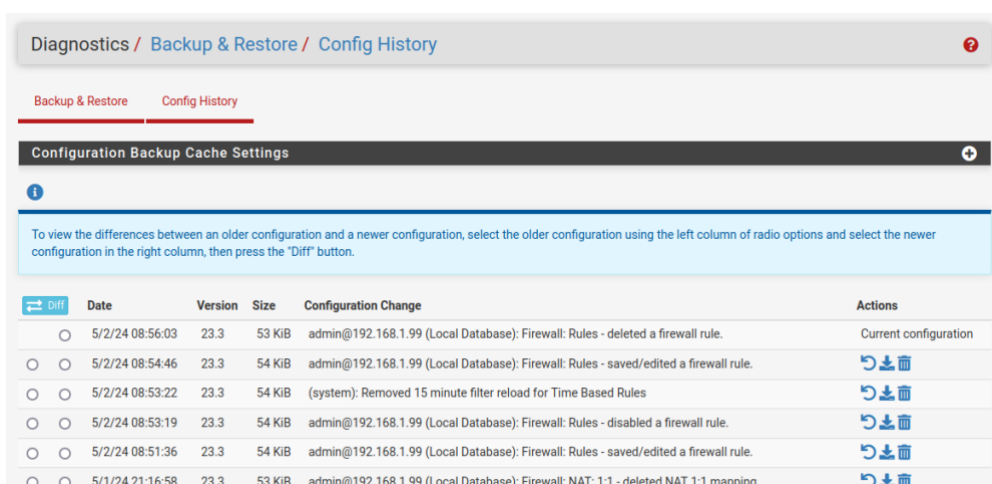
- **Skip packages:** não guardar informações de aplicações/pacotes que foram adicionados no pfSense. **Não seleccione esta opção**, pois pode ser importante preservar a informação das aplicações que foram instaladas na firewall;
- **Skip RRD Data:** O firewall coleta e mantém dados sobre o desempenho do sistema e, em seguida, armazena esses dados em arquivos Round-Robin Database (RRD). Por esse motivo e para não
















incluir toda essas informações nos backups (pois leva imensa informação), *vamos deixar esta opção selecionada*;

- **Include extra data:** Permite armazenar os dados extra de estados de serviços de computadores ligados por DHCP entre outros estados. *Não seleccione esta opção*, pois para este exemplo, não existe necessidade de guardar esse tipo de informação;
- **Backup SSH Keys:** esta opção aparece, se tiver configurado acessos SSH na firewall. Como tal, deve seleccionar essa opção;
- **Encryption:** por uma boa norma de segurança, ative esta opção e defina uma password para proteger os dados do backup;



*Opcional* – Também pode ver tudo o que aconteceu na firewall na opção “Config History”:



Diff	Date	Version	Size	Configuration Change	Actions
<input checked="" type="radio"/>	5/2/24 08:56:03	23.3	53 KiB	admin@192.168.1.99 (Local Database): Firewall: Rules - deleted a firewall rule.	Current configuration
<input type="radio"/>	5/2/24 08:54:46	23.3	54 KiB	admin@192.168.1.99 (Local Database): Firewall: Rules - saved/edited a firewall rule.	  
<input type="radio"/>	5/2/24 08:53:22	23.3	54 KiB	(system): Removed 15 minute filter reload for Time Based Rules	  
<input type="radio"/>	5/2/24 08:53:19	23.3	54 KiB	admin@192.168.1.99 (Local Database): Firewall: Rules - disabled a firewall rule.	  
<input type="radio"/>	5/2/24 08:51:36	23.3	54 KiB	admin@192.168.1.99 (Local Database): Firewall: Rules - saved/edited a firewall rule.	  
<input type="radio"/>	5/1/24 21:16:58	23.3	53 KiB	admin@192.168.1.99 (Local Database): Firewall: NAT: 1:1 - deleted NAT 1:1 mapping.	  

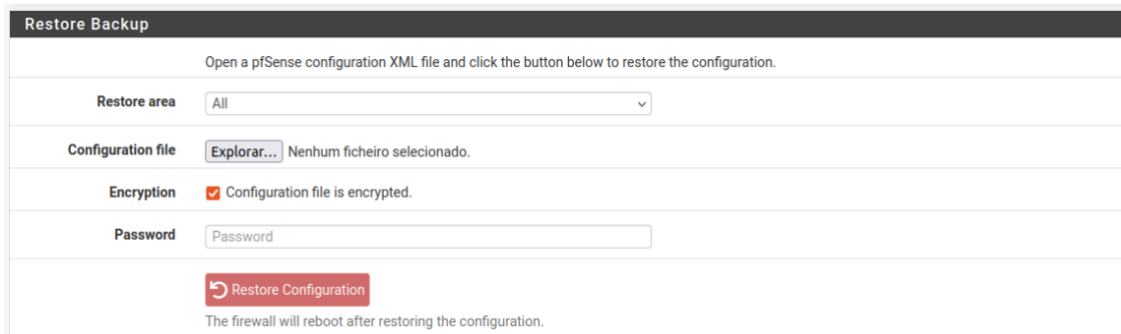
### 8.2 - Restore

Muitas vezes precisamos restaurar o backup em outro sistema, até mesmo em hardware pfSense diferente. Uma vez feito o backup, o pfSense realiza a restauração com todas as regras e configurações do último backup válido. Para fazer a restauração do pfSense devemos ir ao menu superior da aplicação e clicar nas opções **Diagnostics** → **Backup & Restore**

Se quiser restaurar tudo, não precisa mudar nada, agora caso deseje restaurar alguma opção parcialmente, basta escolher em **Restore area** o que precisa de fazer.

Caso tenha colocado uma password para encriptar os dados, deve clicar na opção **Encryption** e digite a senha do backup e clique no botão vermelho escrito Restore Configuration.

O pfSense vai pedir para reiniciar e após o processo para deixar tudo operacional.



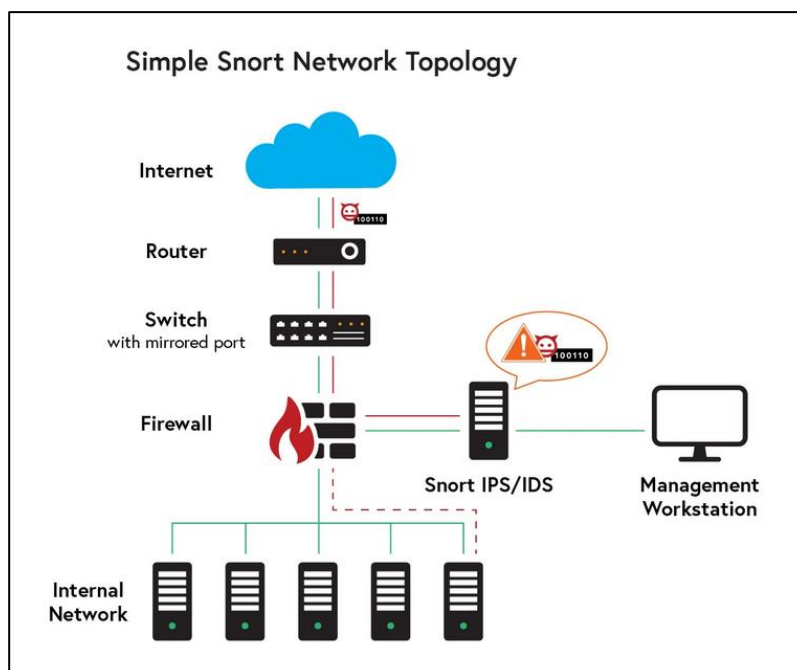
The screenshot shows the 'Restore Backup' web interface. At the top, it says 'Restore Backup' and 'Open a pfSense configuration XML file and click the button below to restore the configuration.' Below this, there are several fields: 'Restore area' with a dropdown menu set to 'All'; 'Configuration file' with an 'Explorar...' button and the text 'Nenhum ficheiro selecionado.'; 'Encryption' with a checked checkbox and the text 'Configuration file is encrypted.'; and 'Password' with an empty text input field. At the bottom, there is a red button labeled 'Restore Configuration' and a note: 'The firewall will reboot after restoring the configuration.'

## Parte 9 - SNORT e PFSENSE

O Snort (<https://www.snort.org/>) é um sistema de deteção de intrusões (IDS) e de prevenção de intrusões (IPS) amplamente utilizado para monitorizar o tráfego de rede em tempo real e identificar atividades suspeitas ou maliciosas. Esta aplicação analisa pacotes de dados com base em regras e assinaturas, permitindo detetar ataques como tentativas de invasão, malware, scans de portas e outras ameaças.

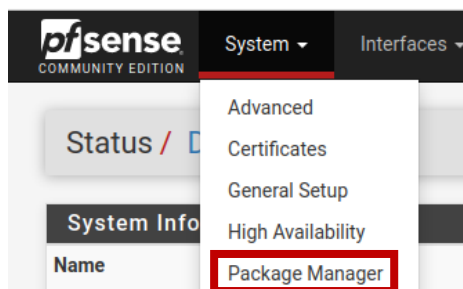


A integração do Snort no pfSense permite adicionar capacidades de IDS diretamente na firewall. Com esta combinação, o administrador pode monitorizar o tráfego que entra e sai da rede, gerar alertas em tempo real e até bloquear automaticamente endereços IP suspeitos. Esta solução é muito utilizada em ambientes empresariais e académicos para reforçar a segurança da infraestrutura de rede, proporcionando maior visibilidade e resposta rápida a incidentes.

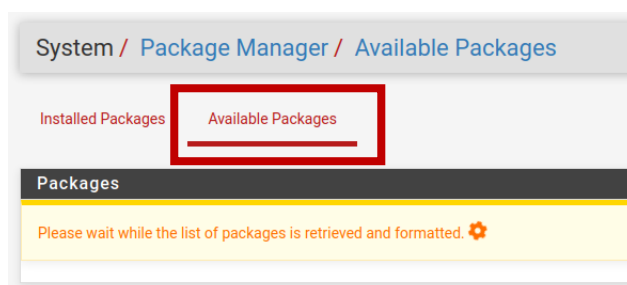


## 9.1 – Configuração e Instalação Snort

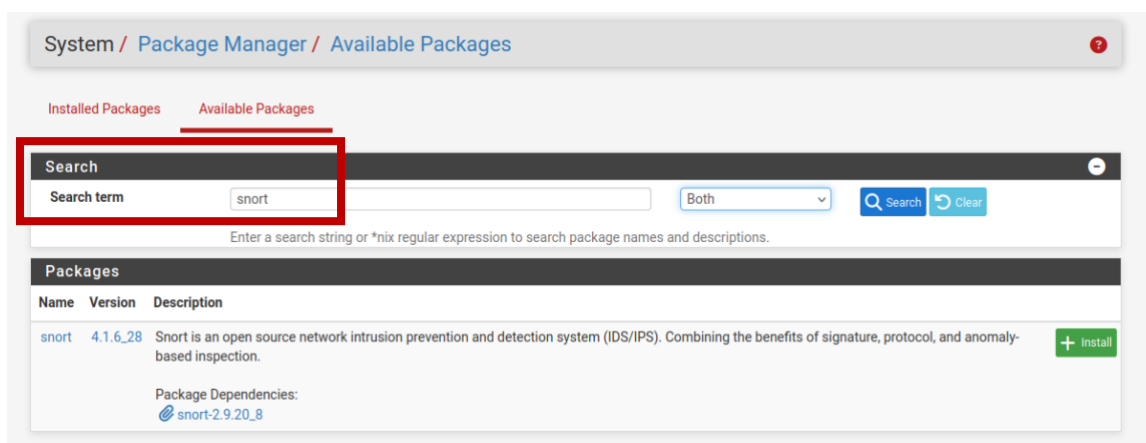
**Passo 1** – Para realizar a instalação do Snort no PFSense, devemos ir ao menu superior da aplicação e clicar nas opções *System* → *Package Manager*:



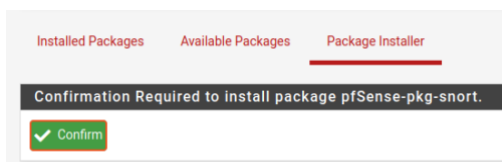
**Passo 2** – Na nova página, vamos clicar no separador “Available Package”:



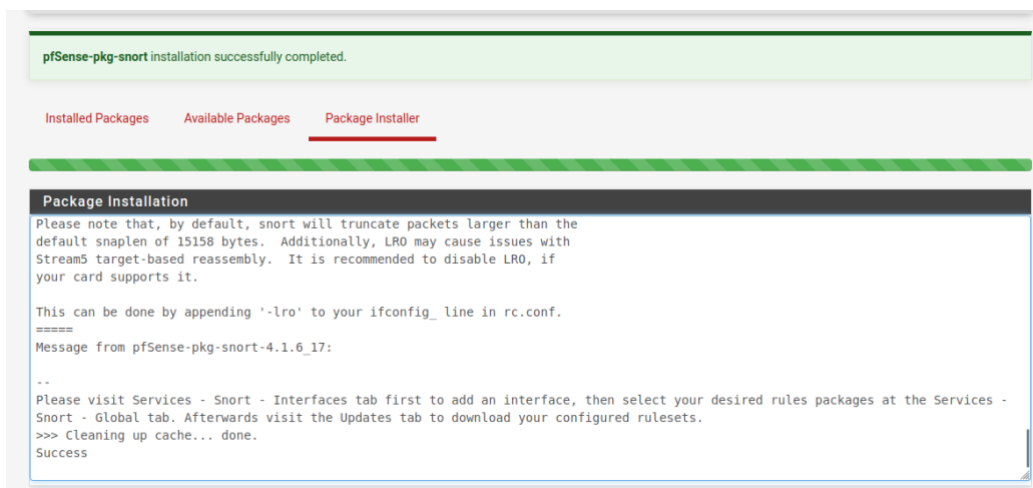
**Passo 3** – Na caixa de pesquisa, procure pelo termo “snort”:



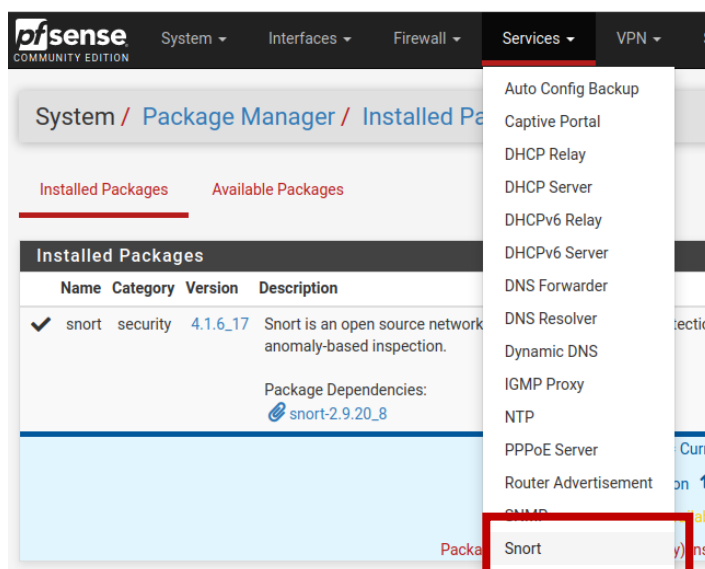
**Passo 4** – Confirme o botão para continuar a instalação:



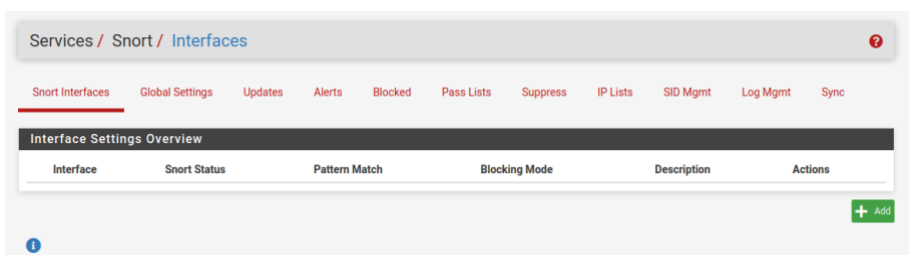
**Passo 5** – Deve esperar que a instalação conclua todo o processo de instalação, e no final deverá aparecer a mensagem de sucesso:



**Passo 6** – Concluído o passo anterior, vamos selecionar a menu principal da firewall e clicar nas opções **Services** → **Snort**:

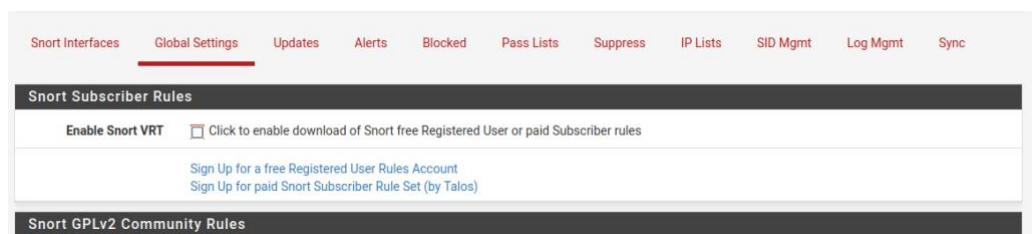


Quando abrir a nova janela, será exibida a informação das interfaces do Snort para realizar a configuração:



**Passo 7 – Vamos selecionar o separador “Global Settings” e ativar as seguintes opções:**

- **Enable Snort VRT:** permite fazer download das regras dos servidores Snort para utilizadores registados (que é gratuito) ou para subscritores da plataforma (que tem as regras pagas).



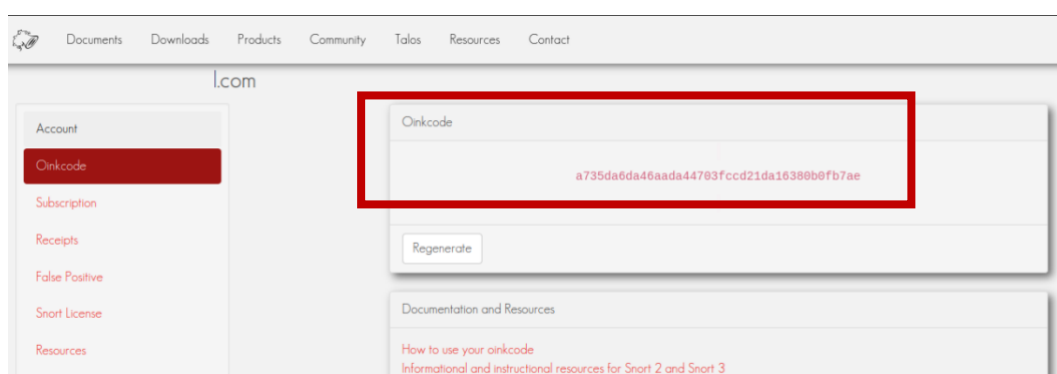
Ao ativar esta opção, temos de colocar o código de acesso ao serviço, conhecido como “**Snort Oinkmaster Code**” para autenticação dos utilizadores.

O **Oinkmaster Code** (ou **Oinkcode**) é um código único associado à nossa conta no site oficial do Snort. Este serve para descarregar automaticamente os conjuntos de regras (rulesets) do Snort.

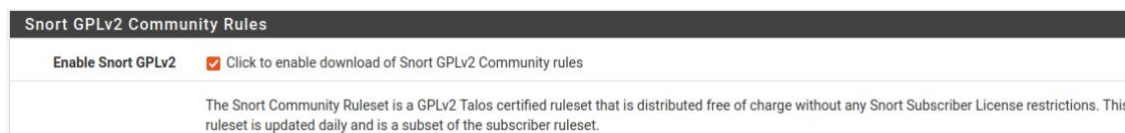
No pfSense, quando configuramos o pacote Snort, podemos inserir esse Oinkcode em **Global Settings** para ativar:

- **Community Rules** – gratuitas, sem Oinkcode;
- **Registered Rules** – gratuitas, mas, as regras para utilizadores registados só estão atualizadas por um período de 30 dias;
- **Subscriber Rules** – pagas e atualizadas em tempo real.

**Faça o registo no portal do Snort e obtenha o OinkCode!**



- **Enable Snort GPLv2:** permite fazer download das regras comunitárias dos servidores Snort (como falado mais acima).



- **Enable ET Open:** permite ativar as prevenções contra ameaças externas;

Emerging Threats (ET) Rules	
Enable ET Open	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules

- **Enable OpenAppID**

- **Enable AppID Open Text Rules:** permite ativar e verificar quais as aplicações que estão a utilizar;

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	
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 <a href="https://files.netgate.com/openappid/appid_rules.tar.gz">https://files.netgate.com/openappid/appid_rules.tar.gz</a> .	

- **Enable FEODO Tracker Botnet C2 IP Rules:** oferece uma lista de bloqueio de endereços IP associados aos botnets C2. Ele pode ser usado para bloquear o tráfego de botnet C2 de máquinas infetadas para servidores que estão sob o controle de cibercriminosos.

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 Cridex, Dridex, Geodo, Heodo and Emotet.	

- **Rules Update Interval**

- **Update Interval:** vai permitir fazer a atualização das regras em intervalos de tempo. Vamos configurar para atualizar as regras de 1 em 1 dia;
- **Update Time:** indicar a que horas é que vai fazer a atualização das regras. Defina 23:00;
- **Hide Deprecated Rules Categories:** para ocultar categorias de regras obsoletas na interface web (GUI) e removê-las da configuração.

Rules Update Settings	
Update Interval	1 DAY Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	23:00 Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Hide Deprecated Rules Categories	<input checked="" 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.

**Passo 8 – Vamos seleccionar o separador “Updates” e ativar as seguintes opções:**

Clicar na opção “UPDATE RULES” para descarregar as regras do Snort (tal como configurado anteriormente):

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID

**Installed Rule Set MD5 Signature**

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

**Update Your Rule Set**

Last Update: Unknown Result: **Unknown**

Update Rules:  Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules pack:

**Rules Update Task**

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.

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

**Installed Rule Set MD5 Signature**

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	82b7855bc92d55c7d240923f7f82d34c	Thursday, 23-Apr-26 11:58:43 WEST
Emerging Threats Open Rules	99121f2598fde91b125502f17fdf792e	Thursday, 23-Apr-26 11:58:47 WEST
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Thursday, 23-Apr-26 11:58:43 WEST
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Thursday, 23-Apr-26 11:58:43 WEST
Feodo Tracker Botnet C2 IP Rules		Thursday, 23-Apr-26 11:58:47 WEST

**Update Your Rule Set**

Last Update: Apr-23 2026 11:58 Result: **Success**

Update Rules:  Update Rules

Vamos analisar os outros separadores:

SNORT ALERTS

SNORT BLOCKED

SNORT PASS LISTS

SNORT SUPPRESS

## SNORT IP LISTS

### 9.2 – Interfaces de captura Snort

De seguida, vamos *adicionar a interface para monitorizar (neste caso será a LAN)*. Como tal, vamos seleccionar ao *separador “Snort Interfaces”* e clicar no botão verde “+ Add”:

#### Definir interfaces (LAN Settings)

- Na interface, seleccione a opção LAN (o campo da descrição muda automaticamente para o mesmo nome):

- Seção Alert Settings
  - Ativar as opções:
    - “Send Alerts to System Log”
    - Enable Packet Captures

**Alert Settings**

**Send Alerts to System Log**  Snort will send Alerts to the firewall's system log. Default is Not Checked.

**System Log Facility**   
Select system log Facility to use for reporting. Default is LOG\_AUTH.

**System Log Priority**   
Select system log Priority (Level) to use for reporting. Default is LOG\_ALERT.

**Enable Packet Captures**  Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

**Packet Capture File Size**

- Ativar a opção “Block Offenders”

**Block Settings**

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

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

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

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

**Muito importante:** Na opção “Which IP to Block”, vamos deixar a opção **BOTH**, bloqueando apenas a origem do tráfego de onde vem o ataque.

Se for selecionado BOTH, isto significa que, a origem do ataque e o destino vão ser bloqueados, se um hacker tentar entrar no vosso sistema e os destinos desejados pelo mesmo.

### Categorias das interfaces (LAN Categories) e definição de regras

Após a configuração do passo anterior, podemos configurar **as novas opções que surgiram logo ao lado do separador LAN Settings**.

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mg

LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN 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 the:

Neste ponto, vamos selecionar todas as regras que importou previamente, pois será uma mais-valia para a nossa análise (mas não selecione a opção Use IPS Policy):

**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**

- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files

Buttons: **Select All** (highlighted), **Inselect All**, **Save**

Enable	Ruleset: ET Open Rules	Snort Subscriber rules are not enabled.	Enable	Ruleset: Snort OPENAPPID Rules
<input checked="" type="checkbox"/>	emerging-activex.rules		<input checked="" type="checkbox"/>	openappid-ads.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules		<input checked="" type="checkbox"/>	openappid-browser_plugin.rules
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules		<input checked="" type="checkbox"/>	openappid-bussiness_applications.rules
<input checked="" type="checkbox"/>	emerging-botcc.rules		<input checked="" type="checkbox"/>	openappid-collaboration.rules
<input checked="" type="checkbox"/>	emerging-chat.rules		<input checked="" type="checkbox"/>	openappid-database.rules
<input checked="" type="checkbox"/>	emerging-ciarmy.rules		<input checked="" type="checkbox"/>	openappid-file_storage.rules
<input checked="" type="checkbox"/>	emerging-compromised.rules		<input checked="" type="checkbox"/>	openappid-file_transfer.rules
<input checked="" type="checkbox"/>	emerging-current_events.rules		<input checked="" type="checkbox"/>	openappid-games.rules
<input checked="" type="checkbox"/>	emerging-deleted.rules		<input checked="" type="checkbox"/>	openappid-hacktools.rules
<input checked="" type="checkbox"/>	emerging-dns.rules		<input checked="" type="checkbox"/>	openappid-mail.rules
<input checked="" type="checkbox"/>	emerging-dos.rules		<input checked="" type="checkbox"/>	openappid-messaging.rules
<input checked="" type="checkbox"/>	emerging-drop.rules		<input checked="" type="checkbox"/>	openappid-mobile.rules

No final, deve ativar o serviço (pois ele está desativado), do qual deve clicar no botão azul (por debaixo do título “Snort Status” para arrancar a interface:

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress

**Interface Settings Overview**

Interface	Snort Status	Pattern Match	Blocking Mode
LAN (em1)	<input checked="" type="checkbox"/>	AC-BNFA	DISABLED

Quando o serviço ficar operacional, teremos a seguinte imagem com a confirmação:

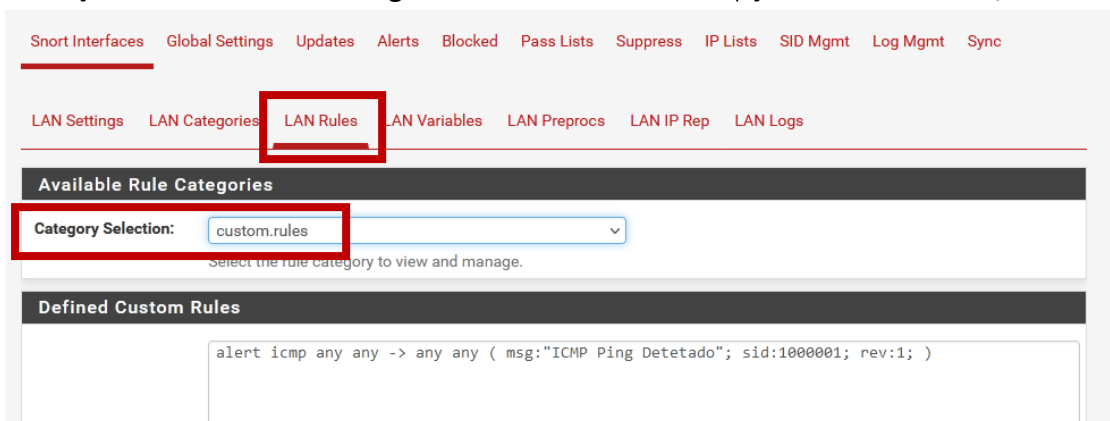
**Interface Settings Overview**

Interface	Snort Status	Pattern Match
LAN (em1)	<input checked="" type="checkbox"/>	AC-BNFA

### 9.3 – Separador LAN Rules: Testes com regras das interfaces

Nesta seção podem definir regras específicas de monitorização ou até indicar as próprias regras, como por exemplo:

- Para fazer a colocação das regras específicas, vamos ter de seleccionar o separador “LAN Rules”;
- Na seção “Available Rule Categories” deve seleccionar a opção “custom.rules”;



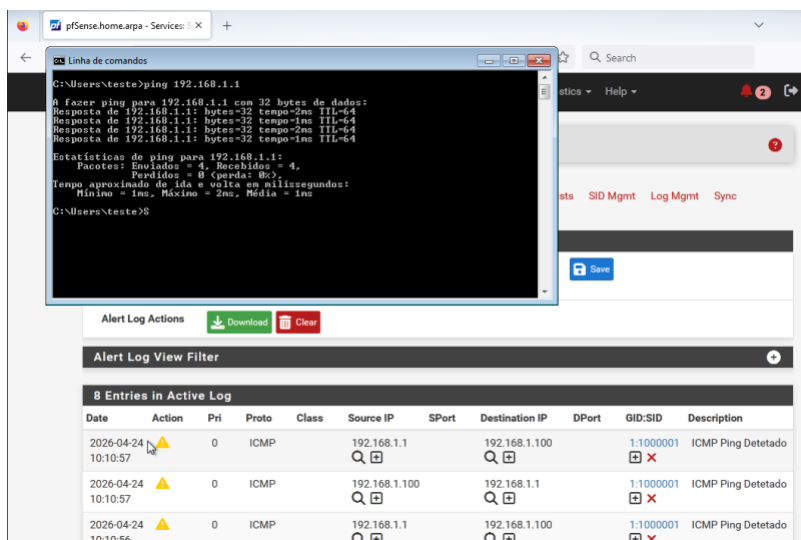
- No final, deve gravar as novas alterações;

1- Definir regras específicas para pings icmp, acesso FTP e SSH

Definir alertas para pings efetuados na rede:

*alert icmp any any -> \$HOME\_NET any ( msg:"ICMP PING detetado"; sid:100001; rev:1; )*

Grave as novas alterações e teste o alerta. Como tal, vamos a máquina virtual que esteja na rede LAN da firewall (netse caso o Windows 7) e fazemos ping para a firewall (ou pode ser para outro equipamento na rede):



Definir alertas para tentativa de acesso ao servidor FTP:

*alert tcp any any -> any 21 ( msg:"Acesso FTP detetado"; sid:100002; rev:1; )*

Grave as novas alterações e teste o alerta. Como tal, vamos utilizar o programa FileZilla para tentar ligar remotamente a uma máquina e ver a tentativa da ligação (mesmo sem efetuar a ligação com sucesso):

The screenshot shows the Snort Alerts interface. At the top, there are navigation tabs: Snort Interfaces, Global Settings, Updates, Alerts (selected), Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. Below the tabs is the 'Alert Log View Settings' section, which includes a dropdown for 'Interface to Inspect' (set to LAN (em1)), an 'Auto-refresh' checkbox, and a text input for 'Alert lines to display' (set to 250). There are 'Download' and 'Clear' buttons. Below this is the 'Alert Log View Filter' section. The main part of the screenshot is a table titled '3 Entries in Active Log'.

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2026-04-24 10:32:30	⚠	0	TCP		192.168.1.100	49481	94.23.79.17	21	1:1000002	Acesso FTP detetado
2026-04-24 10:32:30	⚠	0	TCP		192.168.1.100	49481	94.23.79.17	21	1:1000002	Acesso FTP detetado
2026-04-24 10:21:16	⚠	0			fe80::a00:27ff:fe91:c14f		ff02::1		1:1000001	ICMP Ping Detetado

Definir alertas para tentativa de acesso ao servidor SSH:

*alert tcp any any -> \$HOME\_NET 22 ( msg:"Acesso SSH detetado"; sid:100003; rev:1; )*

Volte a ir ao menu Snort Interface, edite as configurações dentro da interface que já está configurada e seleccione a opção LAN Preprocs:

The screenshot shows the 'Services / Snort / Interface Settings / LAN - Preprocessors and Flow' page. At the top, there are navigation tabs: Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. Below the tabs are sub-tabs: LAN Settings, LAN Categories, LAN Rules, LAN Variables, LAN Preprocs (selected), LAN IP Rep, and LAN Logs. The main content area is titled 'Important Preprocessor Information' and contains a warning message: 'Rules may be dependent on enabled preprocessors! Disabling preprocessors may result in Snort startup failure unless all of the corresponding preprocessor-dependent rules are also disabled. Do not disable any default-enabled preprocessors on this page unless you are very skilled with using Snort. If you experience Snort start-up errors or failures after making changes to preprocessors, try resetting all preprocessor configurations to their defaults, and then attempt to start Snort.'

Deslize a janela para baixo até encontrar o separador (que está agrupado), com o nome “Portscan Detection” e clique no botão + que está no lado direito:

*Procure pelo separador “SSH Detection” e:*

*Verificar se a opção “Enable SSH Detection” está ativada;*

*Verificar se as 3 últimas opções estão seleccionadas (para ataques via exploits);*

SSH Detection	
Enable SSH Detection	<input checked="" type="checkbox"/> The SSH preprocessor detects various Secure Shell exploit attempts. Default is Checked.
Server Ports	22 Specifies which ports the SSH preprocessor should inspect traffic to. For multiple ports, separate values with commas. A configured Port Alias may also be specified. Default port is 22.
Max Encrypted Packets	20 Specifies the number of stream reassembled encrypted packets that Snort will inspect before ignoring a given SSH session. Once max_encrypted_packets packets have been seen, Snort ignores the session to increase performance. Default is 20.
Max Client Bytes	19600 Specifies the number of unanswered bytes allowed to be transferred before alerting on Challenge-Response Overflow or CRC 32. This number must be hit before max_encrypted_packets packets are sent, or else Snort will ignore the traffic. Default is 19600.
Max Server Version Length	100 Specifies the maximum number of bytes allowed in the SSH server version string before alerting on the Secure CRT server version string overflow. Default is 100.
Enable Challenge-Response Overflow	<input checked="" type="checkbox"/> Enable checking for the Challenge-Response Overflow exploit. Default is Checked.
Enable Secure CRT Exploit	<input checked="" type="checkbox"/> Enable checking for the Secure CRT exploit. Default is Checked.
Enable CRC 32 Exploit	<input checked="" type="checkbox"/> Enable checking for the CRC 32 exploit. Default is Checked.
Enable Protocol Mismatch Exploit	<input checked="" type="checkbox"/> Enable checking for the Protocol Mismatch exploit. Default is Checked.

Por último, vamos abrir o separador “FTP and Telnet global options” e verificar se este grupo está ativo no enable:

FTP and Telnet Global Options	
Enable	<input checked="" type="checkbox"/> Normalize/Decode FTP and Telnet traffic and protocol anomalies. Default is Checked.
Inspection Type	stateful Choose to operate in stateful or stateless mode. The default is stateful.
Check Encrypted Traffic	<input checked="" type="checkbox"/> Continue to check an encrypted session for subsequent command to cease encryption. Default is Checked.
Alert on Encrypted Commands	<input type="checkbox"/> Alert on encrypted FTP and Telnet command channels. Default is Not Checked.

Resultados:

Ping ICMP e conectar ftp

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.375 ms
^C
— 192.168.1.100 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.375/0.375/0.375/0.000 ms

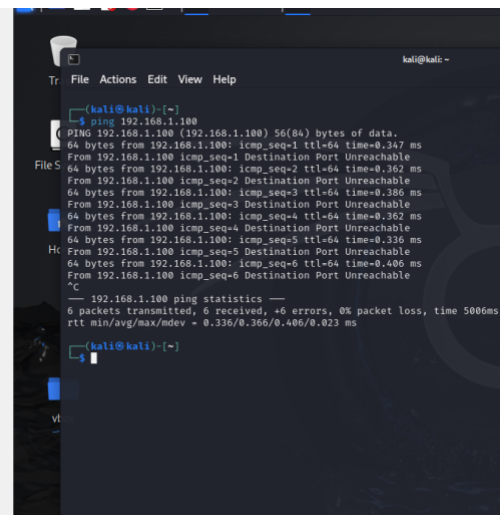
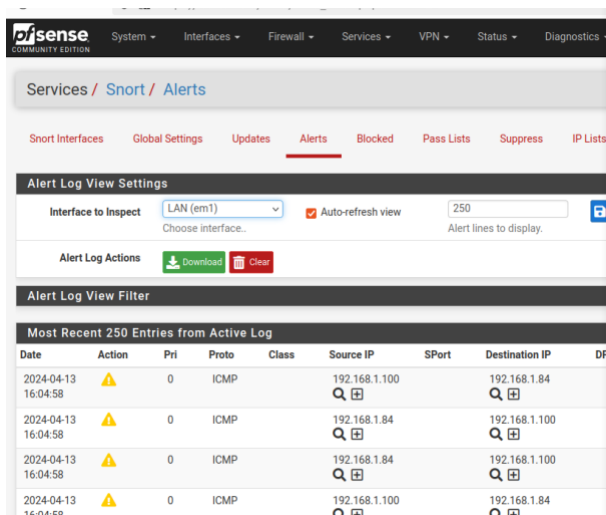
(kali@kali)-[~]
└─$ ftp silva1@192.168.1.100
Connected to 192.168.1.100.
220 (vsFTPd 3.0.5)
530 Non-anonymous sessions must use encryption.
ftp: Login failed

```

16 Entries in Active Log										
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-04-13 15:32:10	⚠	0	TCP		192.168.1.84	44392	192.168.1.100	21	1:100002	Acesso FTP detetado
2024-04-13 15:32:10	⚠	0	TCP		192.168.1.84	44392	192.168.1.100	21	1:100002	Acesso FTP detetado
2024-04-13 15:32:06	⚠	0	TCP		192.168.1.84	44392	192.168.1.100	21	1:100002	Acesso FTP detetado
2024-04-13 15:32:06	⚠	0	TCP		192.168.1.84	44392	192.168.1.100	21	1:100002	Acesso FTP detetado
2024-04-13 15:32:06	⚠	0	TCP		192.168.1.84	44392	192.168.1.100	21	1:100002	Acesso FTP detetado
2024-04-13 15:32:06	⚠	0	TCP		192.168.1.84	44392	192.168.1.100	21	1:100002	Acesso FTP detetado
2024-04-13 15:32:01	⚠	0	ICMP		192.168.1.100		192.168.1.84		1:100001	ICMP PING detetado
2024-04-13 15:32:01	⚠	0	ICMP		192.168.1.84		192.168.1.100		1:100001	ICMP PING detetado
2024-04-13 15:31:58	⚠	3	TCP	Not Suspicious Traffic	192.168.1.100	57388	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management

2 – Altere a regra do ICMP de alert para reject, guarde as alterações e faça novamente ping entre as máquinas virtuais e após isso, veja ou que aconteceu no separador “Blocked”:

*reject icmp any any -> \$HOME\_NET any ( msg:"ICMP PING detetado"; sid:100001; rev:1; )*

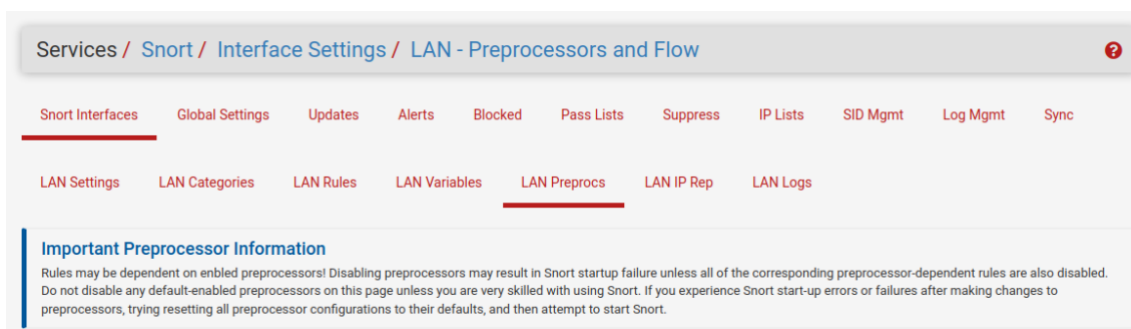


3 – Volte a colocar a primeira regra como alert:

*alert icmp any any -> \$HOME\_NET any ( msg:"ICMP PING detetado"; sid:100001; rev:1; )*

De seguida, vamos tentar atacar a rede com um Scan baseado no Nmap para ver as portas abertas nos nossos sistemas. Como tal, vamos ter de ativar algumas operações adicionais.

Volte a ir ao menu Snort Interface, edite as configurações dentro da interface que já está configurada e selecione a opção LAN Preprocs:

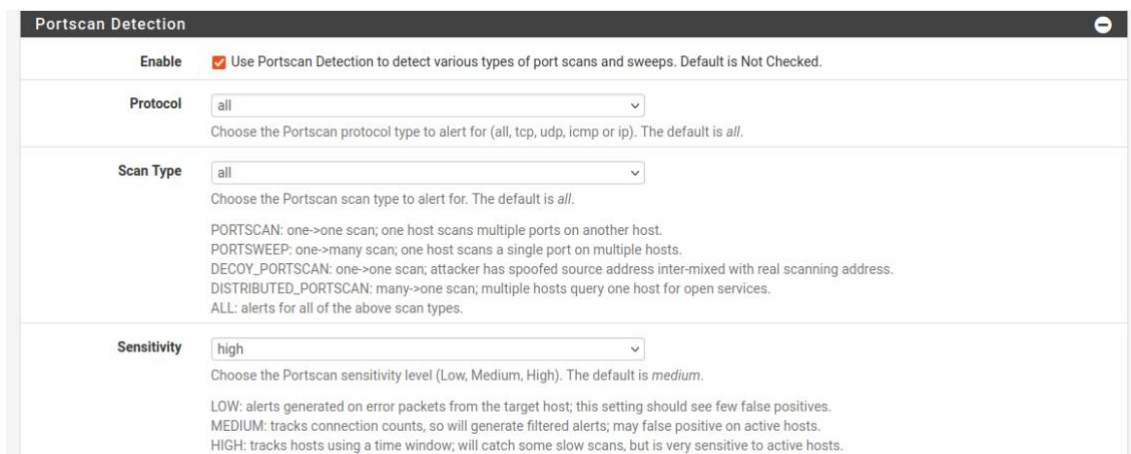


Deslize a janela para baixo até encontrar o separador (que está agrupado), com o nome “Portscan Detection” e clique no botão + que está no lado direito:



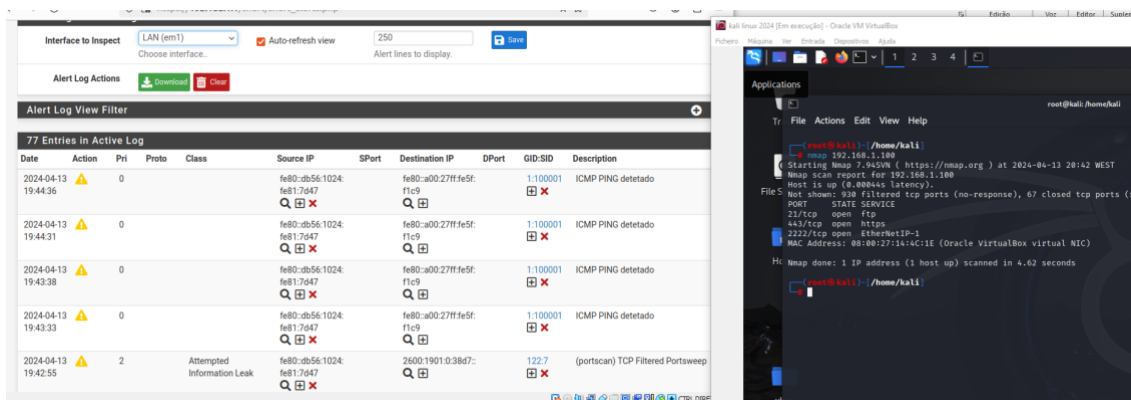
Dentro deste grupo:

- ative a opção Enable “Use Portscan Detection to detect various types of port scans and sweeps”;
- na opção “Sensitivity” coloque o valor High;

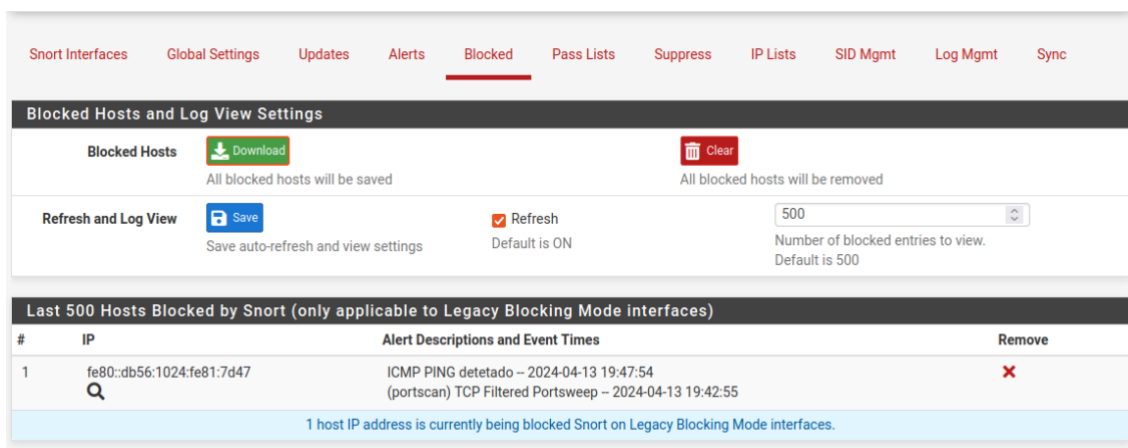


Volte a ir para a zona dos alerts do Snort e na máquina do atacante, faça o comando “nmap ip\_da\_vitima” (ex: nmap 192.168.1.100)

Recarregue a página dos alerts e verifique este apanhar os dados do ataque:



Como ativou as opções avançadas nas configurações para deteção máxima, o snort vai entender este tipo de ataque como malicioso e vai colocar o endereço como bloqueado, tal como demonstra a seguinte imagem do separador “Blocked”:



## Parte 10 – Limitar velocidade dentro da firewall



Imagine o seguinte cenário:

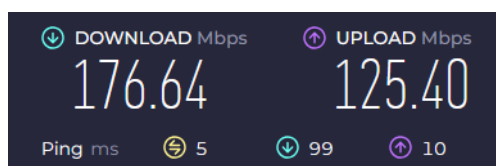
Temos a rede WAN que permite a entrada da internet na nossa firewall e assim comunicar com as redes internas (redes LAN, pois podemos ter mais do que uma, tal como demonstra a seguinte imagem:

Interfaces			
WAN1	↑	1000baseT <full-duplex>	111.111.111.121
LAN11	↑	1000baseT <full-duplex>	192.168.11.1
LAN12	↑	1000baseT <full-duplex>	192.168.12.1

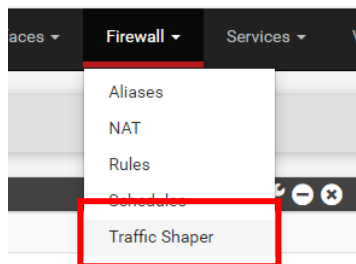
Como tal, podemos colocar limites no acesso a internet como uma norma de segurança adicional dentro da firewall.

Como tal, vamos fazer os seguintes passos, mas neste caso prático, apenas vamos aplicar as regras numa rede LAN (com a máquina virtual da SEDE que temos trabalhado ao longo das fichas de trabalho):

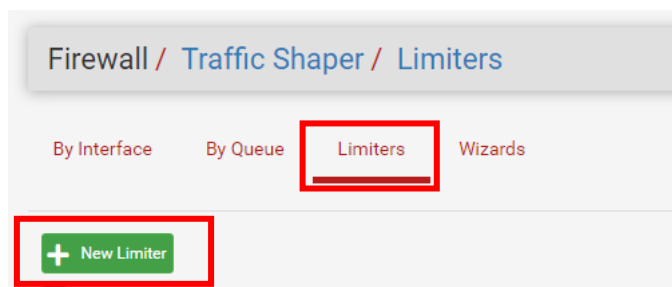
Suponha que estes são os valores da velocidade da sua Internet:



**Passo 1** – Vamos até ao menu Firewall → Traffic Shaper

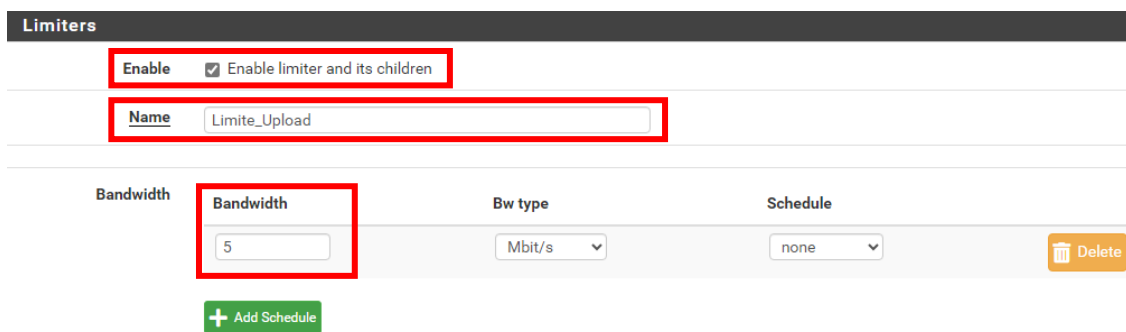


**Passo 2** – Selecione o separador “Limiters” e depois carregue no botão New Limiter para adicionar uma nova limitação (neste passo apenas vamos dizer os parâmetros da configuração):



**Passo 3** – Vamos criar as configurações para o Upload. Coloque as seguintes informações:

- **Enable:** ative esta opção
- **Name:** Limite\_Upload
- **Bandwidth:** 5 (por defeito já vem Mbit/s)



**Passo 4** – No campo Mask, podemos escolher as opções "origem (source)" para definir que estamos a trabalhar o upload ou "destino (destiny)" para definir que estamos a trabalhar o download. Para tal, vamos:

- **Mask:** seleccionar a opção Source Address para indicar que quero trabalhar o Upload de dados;
  - Deixar os valores 32 e 128 para aplicar a regra em todos os hosts da LAN;

- **Description:** colocar a informação “Limitar Upload na rede LAN”;

**Mask** Source addresses

If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.

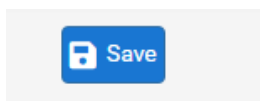
32 IPv4 mask bits  
255.255.255.255/?

128 IPv6 mask bits  
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?

**Description** Limitar Upload na rede LAN

A description may be entered here for administrative reference (not parsed).

**Passo 5** – Não esqueça de gravar as novas informações;



**Passo 6** – Aplique as novas alterações:

The traffic shaper configuration has been changed.  
The changes must be applied for them to take effect.

Apply Changes

By Interface By Queue **Limiters** Wizards

Limite\_Upload

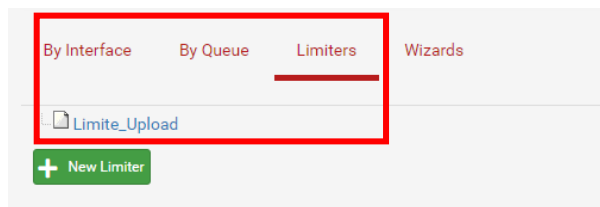
+ New Limiter

**Limiters**

Enable  Enable limiter and its children

Name Limite\_Upload

**Resultado da criação do limite:**



**Passo 7** – Vamos fazer a mesma tarefa para o Download de ficheiros, mas com algumas modificações, em especial no campo Mask que ao contrário do Upload que usa Source Addresses o Dowload vai usar a opção Destination Addresses:

Vamos criar as configurações para o Download. Coloque as seguintes informações:

- **Enable:** ative esta opção
- **Name:** Limite\_Download
- **Bandwidth:** 10 (por defeito já vem Mbit/s)
- **Mask:** seleccionar a opção Destination Address para indicar que quero trabalhar o Download de dados;
  - Deixar os valores 32 e 128 para aplicar a regra em todos os hosts da LAN;
- **Description:** colocar a informação “Limitar Download na rede LAN”;

**Limiters**

**Enable**  Enable limiter and its children

**Name** Limite\_Download

**Bandwidth**

Bandwidth	Bw type	Schedule
10	Mbit/s	none

[+ Add Schedule](#) [Delete](#)

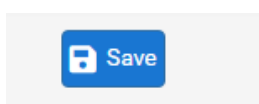
**Mask** Destination addresses

If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.

IPv4 mask bits: 32 (255.255.255.255/?)  
IPv6 mask bits: 128 (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?)

**Description** Limitar Download na rede LAN  
A description may be entered here for administrative reference (not parsed).

**Passo 8** – Não esqueça de gravar as novas informações;



**Passo 9** – Aplique as novas alterações:

Firewall / Traffic Shaper / Limiters

The traffic shaper configuration has been changed.  
The changes must be applied for them to take effect.

[✔ Apply Changes](#)

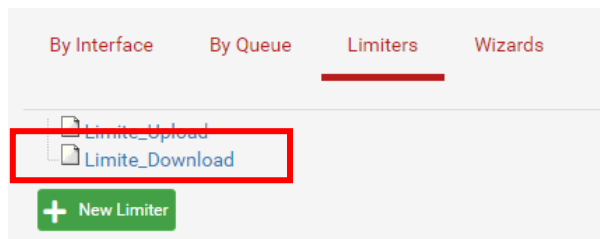
By Interface | By Queue | **Limiters** | Wizards

Limiters

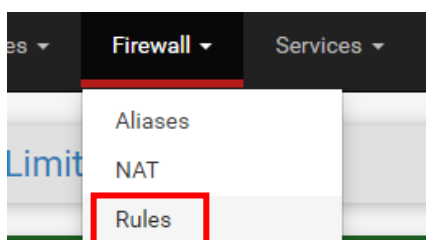
**Enable**  Enable limiter and its children

**Name** Limite\_Download

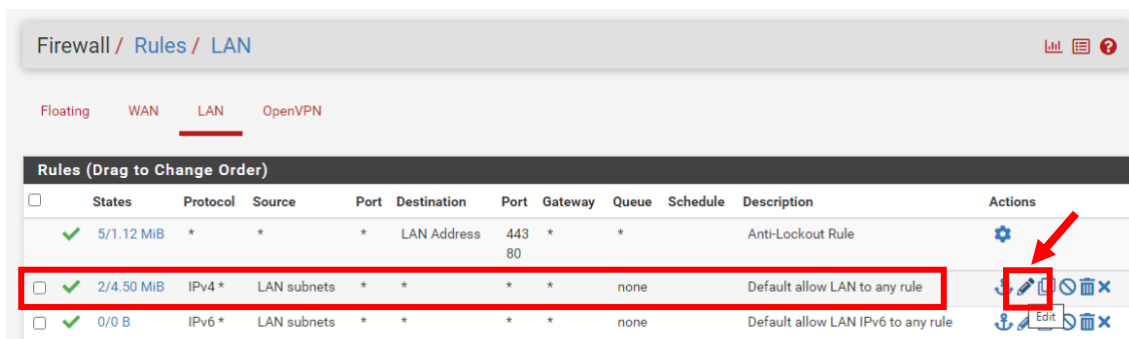
Resultado:



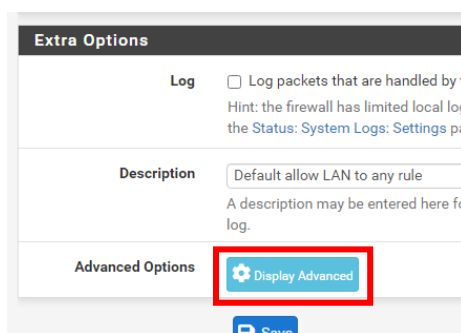
**Passo 10** – No próximo passo, vamos associar a regra dos limites na rede LAN (pois apenas criamos as indicações, mas ainda falta associar as mesmas nas regras da firewall). Vamos ao menu **Firewall** → **Rules**:



Clique no separador LAN e de seguida, vamos clique no botão do lápis para alterar as definições da rede IPv4\*:



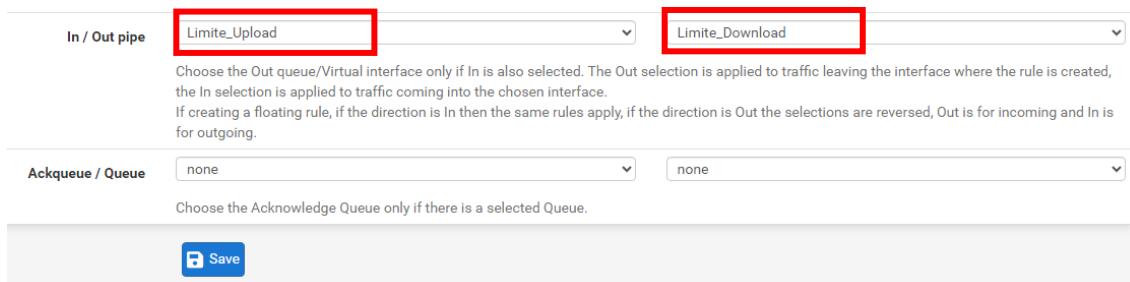
Dentro da regra, deve ir ao fundo da página e clicar no botão **Display Advanced** para aceder as propriedades avançadas das configurações da regra:



Este vai abrir várias opções, mas a que queremos está quase no fundo da página com o nome “In/Out Pipe”. Deve aplicar as configurações que fez no limitador, mais especificamente:

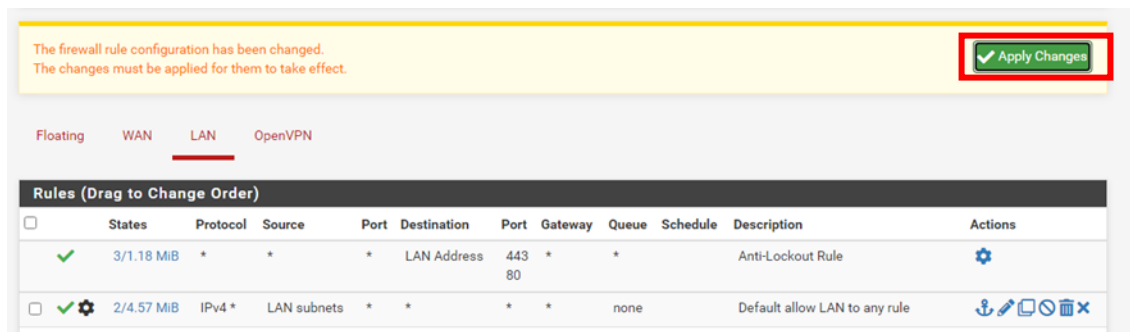
- **1º Campo** → Colocar o limitador “Limite Upload”
- **2º Campo** → Colocar o limitador “Limite Download”

Este por sua vez, vai definir a regra com base nos limitadores que serão impostos na rede da LAN.

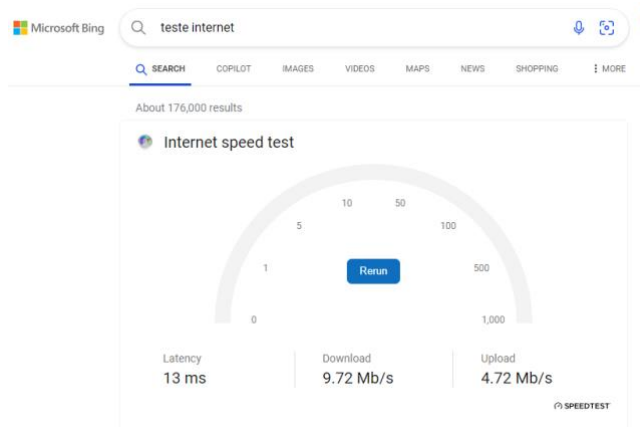


Não esquecer de gravar as novas alterações.

**Passo 11** – Faça a aplicação das novas alterações e depois repare que vai aparecer uma roda dentada no início da regra:



**Passo 12** – Teste a ligação da LAN na máquina virtual (que esteja ligada na rede LAN):



## Permitir ping na rede WAN

De notar que, por defeito a firewall do PfSense bloqueia todos os pacotes “ping”, incluídos protocolos ICMP, por razões de segurança. Contudo, pode haver situações que seja necessário verificar as conexões com a firewall, como por exemplo, nos programas de monitorização, como o Zabbix para verificar se a firewall está online ou offline.

**Passo 1** – Abra uma linha de comandos (cmd) e faça ping na firewall da sede (neste exemplo o IP é o 192.168.1.121):

```

C:\Users\Silva>ping 192.168.1.121

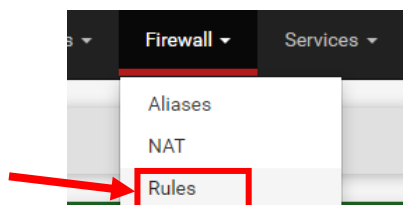
Pinging 192.168.1.121 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.121:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
  
```

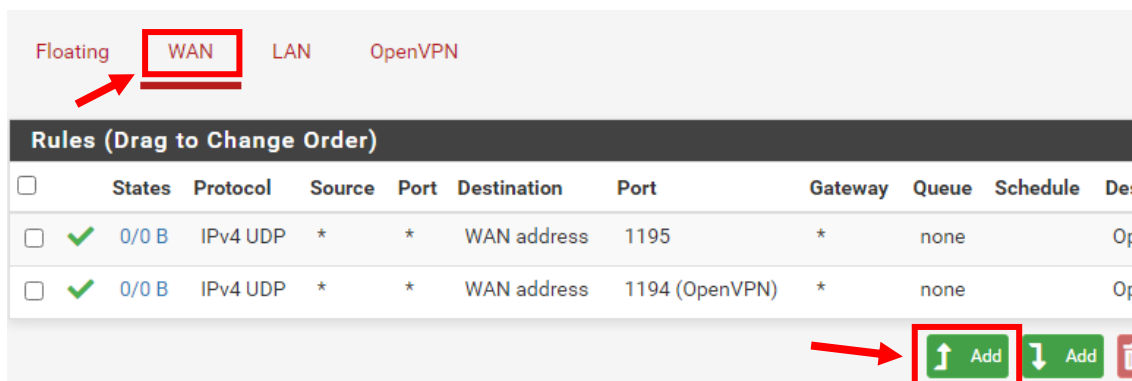
Repare que a resposta foi negativa e os pacotes não obtiveram qualquer resposta!

Vamos adicionar uma nova regra na interface WAN para permitir o protocolo ICMP:

**Passo 1** – Vamos ao menu da firewall e seleccione as opções Firewall → Rules:



**Passo 2** – Seleccione o separador WAN e clique no botão ADD para adicionar nova regra:



**Passo 3** – Coloque as seguintes opções:

- Action: Pass
- Interface: WAN
- Address Family: IPv4
- Protocol: ICMP
- ICMP Subtypes: Any

**Edit Firewall Rule**

**Action** Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** WAN

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

**Address Family** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** ICMP

Choose which Internet protocol this rule should match.

**ICMP Subtypes** any

Alternate host unreachable  
Datagram conversion error  
Echo reply

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

**Passo 4** – Nas próximas seções deve fazer as seguintes ações:

- Seção Origem (Source) deve selecionar a opção ANY;
- Seção Destino (Destination), deve selecionar a opção This Firewall (self);
- Seção Extra Options:
  - Selecionar a opção Log, para permitir os registos de atividade;
  - Colocar a descrição “Permitir Ping Wan”;

**Source**

**Source**  Invert match Any

Source Address /

**Destination**

**Destination**  Invert match This Firewall (self)

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).

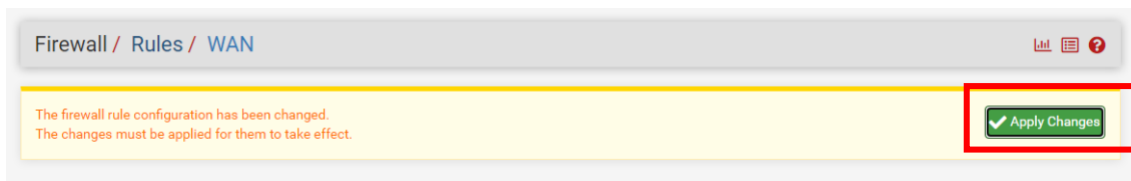
**Description** Permitir Ping WAN  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

[Save](#)

No final não esqueça de gravar as novas alterações.

Passo 5 – Aplique as novas alterações:



Passo 6 – Recebida a confirmação da aplicação da regra, vamos fazer novamente o PING ao servidor da firewall da SEDE e veja a reposta com sucesso:

