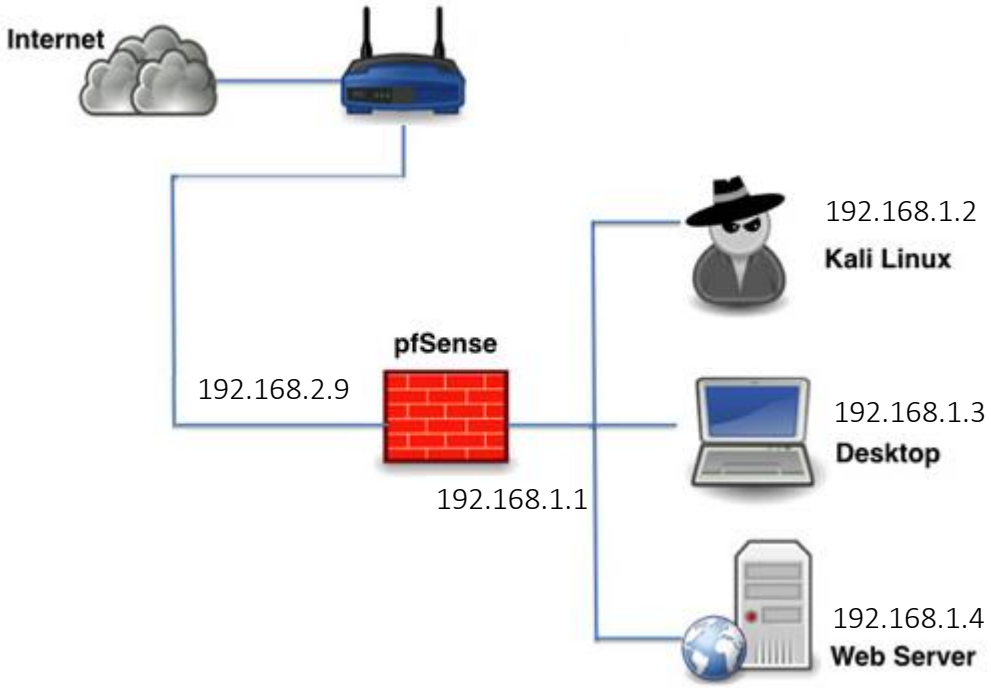
FICHA TRABALHO 5

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

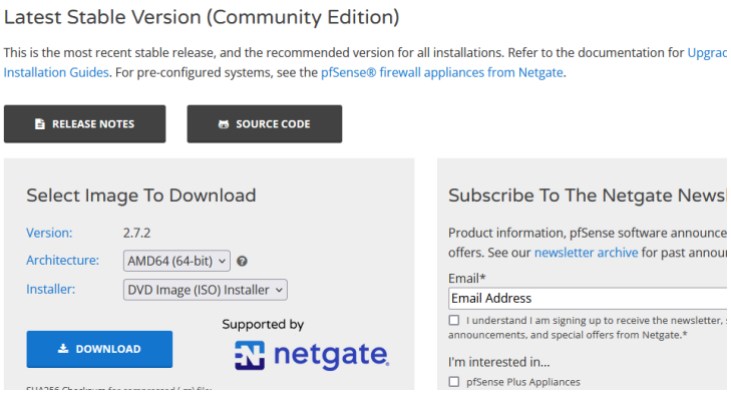
Exemplo de digrama de construção e comunicação da firewall



Parte 1 – Configuração da máquina virtual

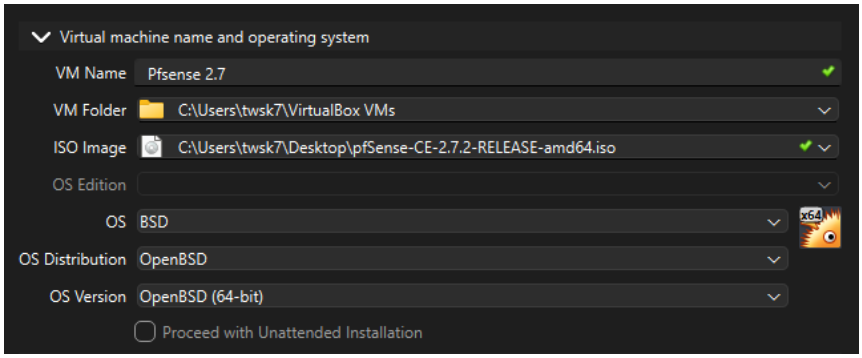
Passo 1 – Retirar a imagem do pfsense da página oficial: https://www.pfsense.org/download/ e selecionar as opções:

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



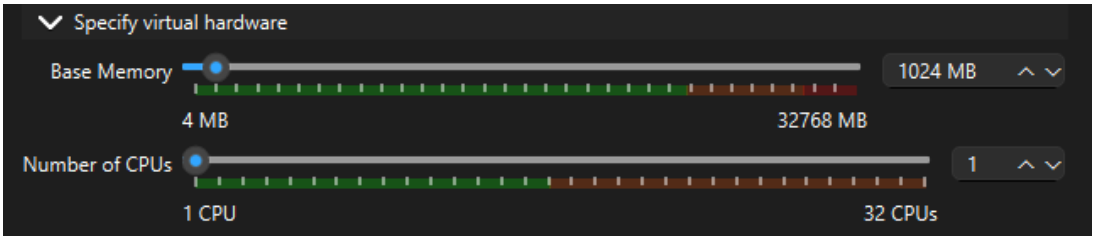
Passo 2 – Vamos criar uma nova máquina virtual, do qual:

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

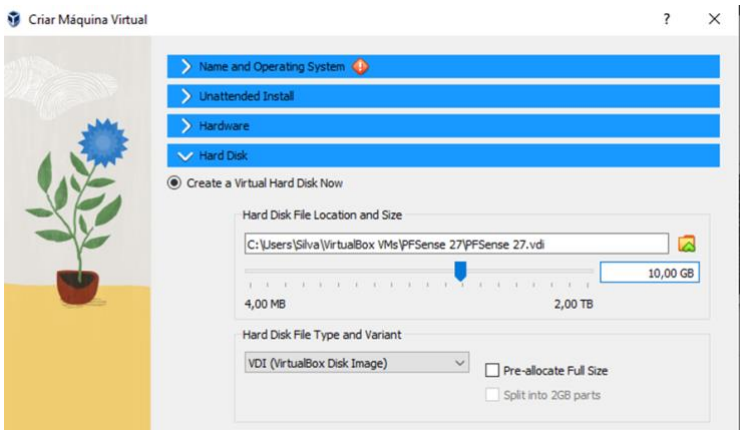


Passo 3 – Em termos de hardware, defina os seguintes valores:

- 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 (OBRIGATORIAMENTE), pois o Pfsense só funciona em single-core (1 núcleo de processador);



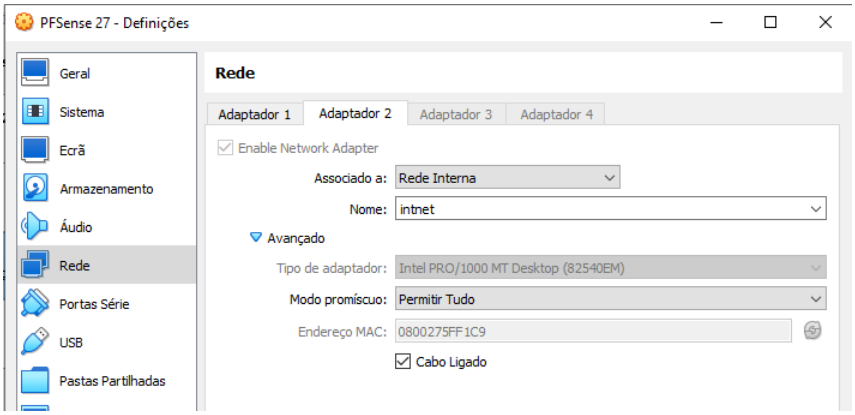
Passo 4 – Criar disco rígido virtual com a extensão VDI e com 10 GB de espaço:



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 promíscuo*** Permitir Tudo;

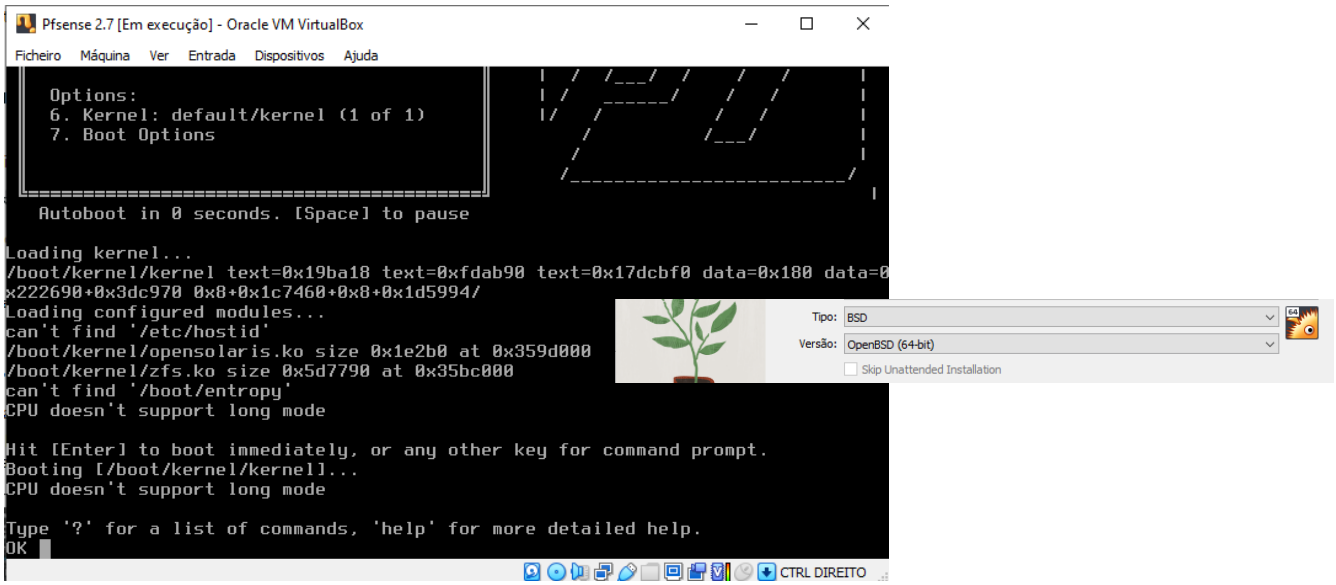
- ***Aptador 2:*** Rede interna (que serve para comunicar com os computadores que estão na rede LAN e interligados com esta firewall) e ***Modo promíscuo*** Permitir Tudo:



Potenciais erros de inicialização

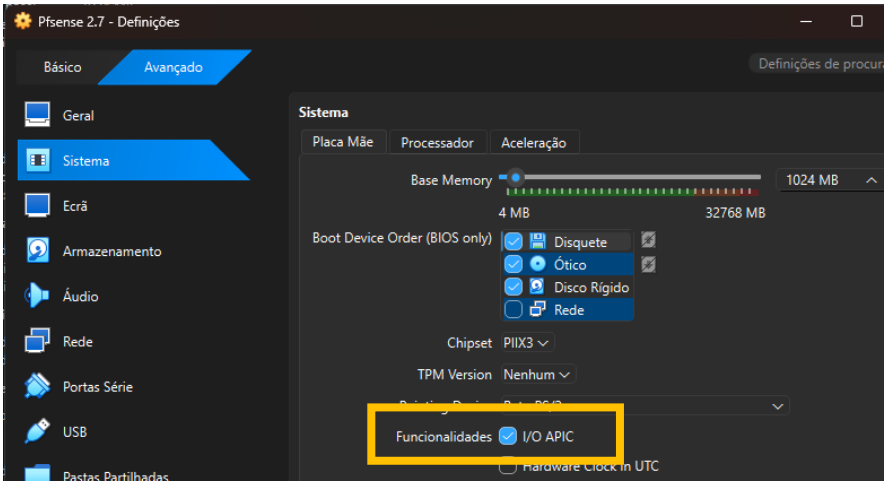
ERRO "CPU doesn´t support long mode"

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:***



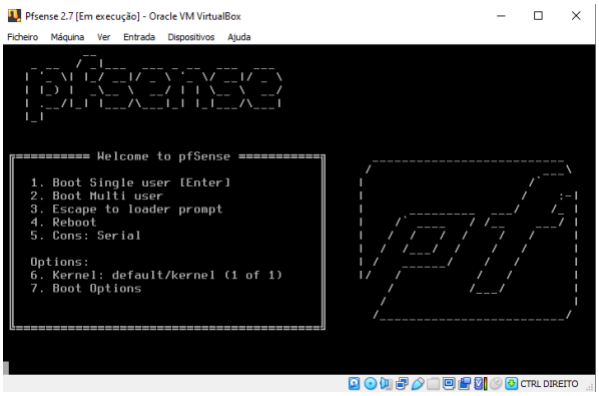
ERRO "Panic: running without device atpic requires a local APIC "

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 selecionar a opção "I/O APIC":

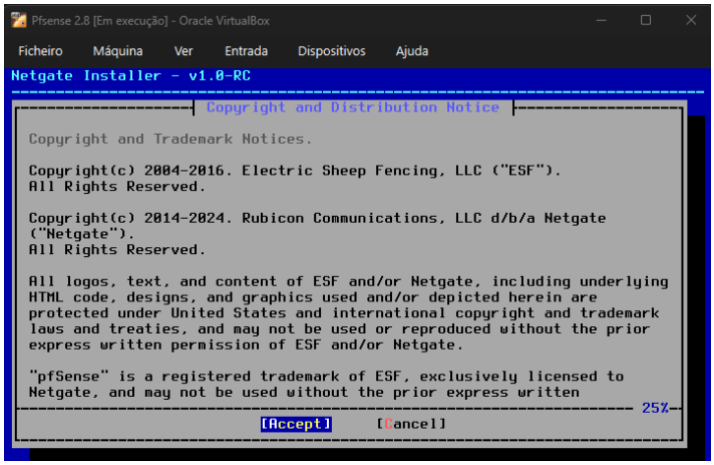


Parte 2 – Configuração e Instalação da Firewall Pfsense

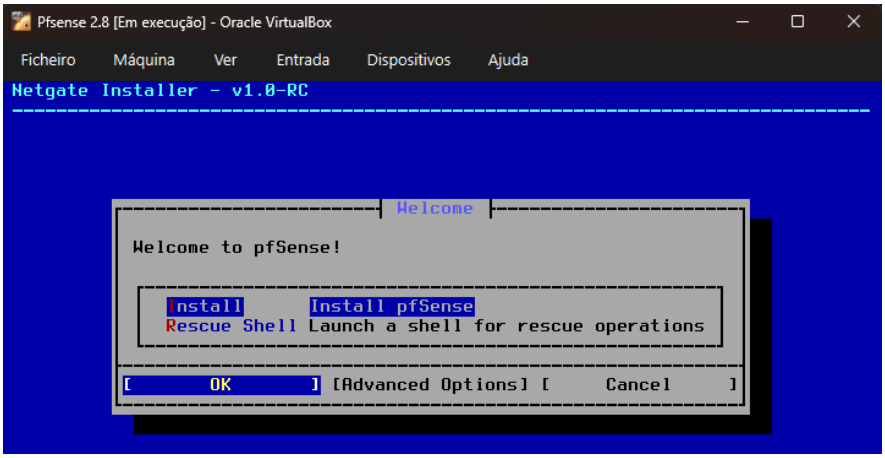
Passo 1 – Se tudo correr bem a máquina virtual vai mostrar a tela principal e ao fim de 3 segundos, este arranca automaticamente para a configuração:



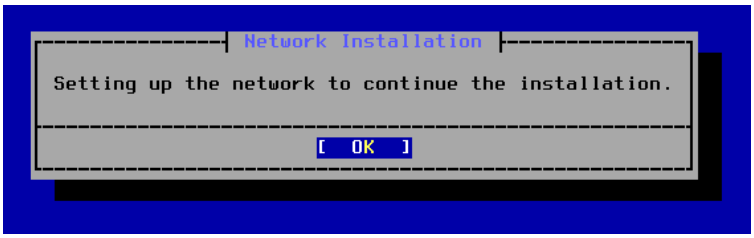
Passo 2 – Aceitar os termos e condições:



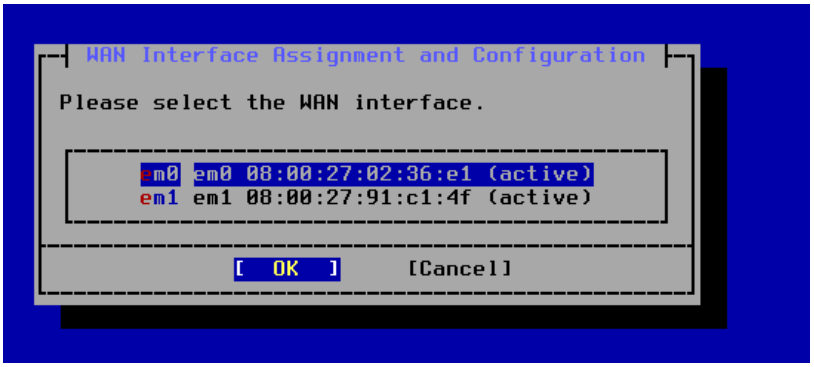
Passo 3 – Selecionar a opção Install:



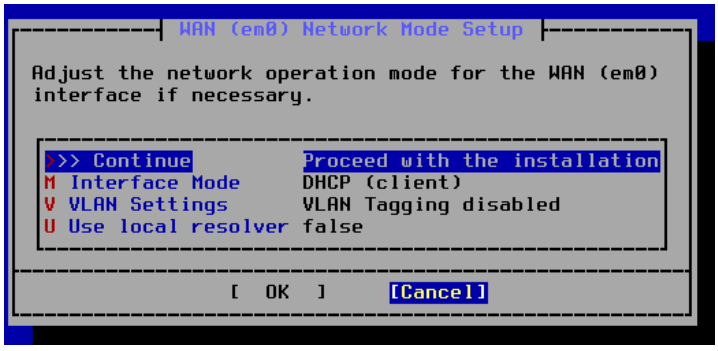
Passo 4 – Confirme para configurar as interfaces de rede:



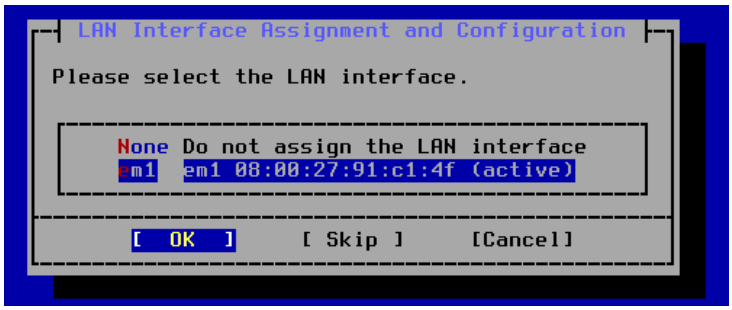
Passo 5 – Selecione a interface em0 (neste caso será o adaptador bridge):



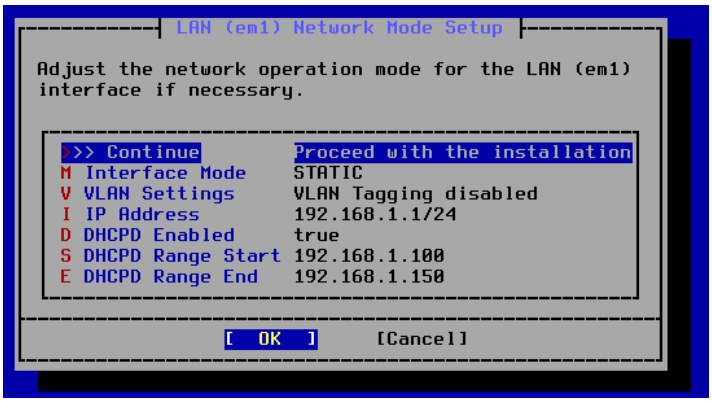
Passo 6 – Peça para continuar a configuração (Continue):



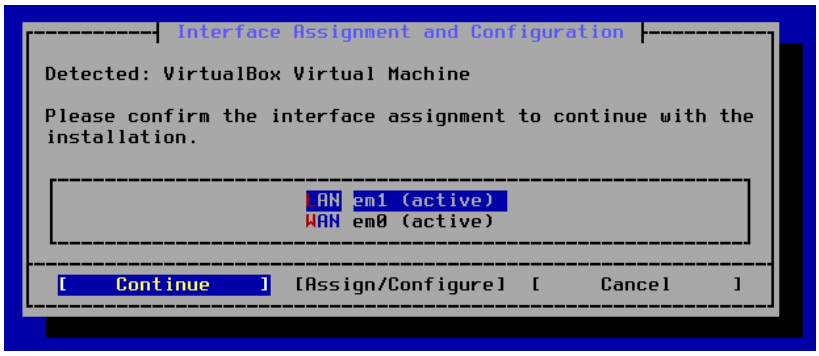
Passo 7 – Configure a outra interface de rede, mais especificamente, a interface em1 (neste caso será a rede interna):



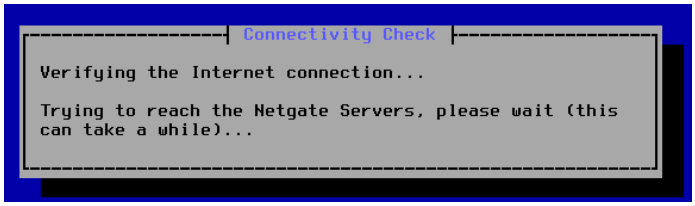
Passo 8 – Peça para continuar a configuração (Continue):



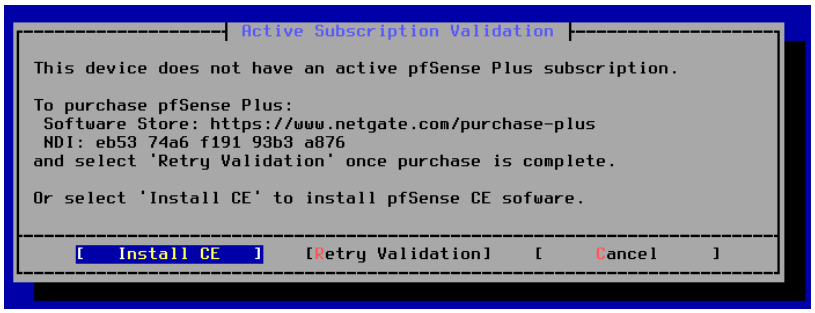
Passo 9 – Peça para continuar a configuração (Continue):



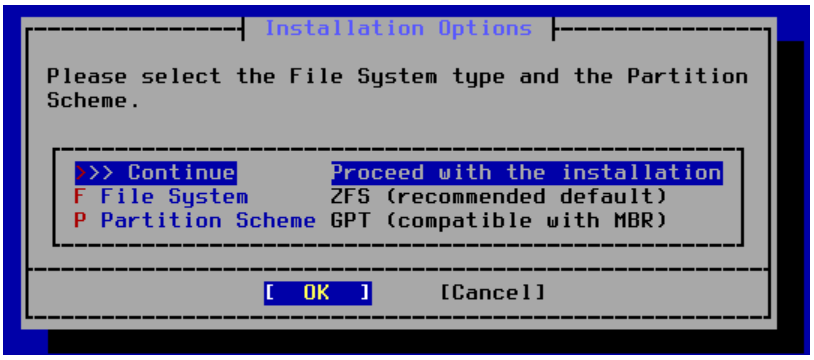
Passo 10 – De seguida, vai ser verificada a configuração da internet (pelo adaptador bridge) e verificar se consegue ligar ao servidor remoto da NetGate:



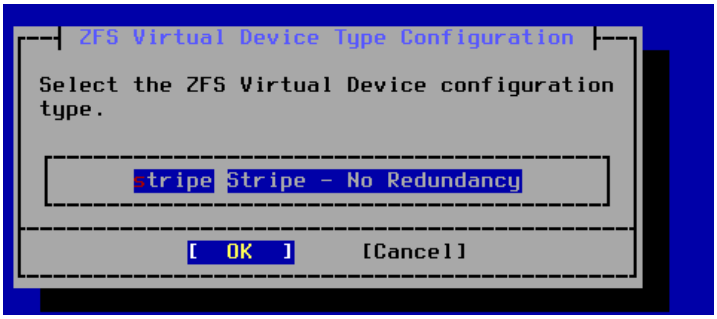
Passo 11 – Pedir para instalar a versão CE (Community Edition):



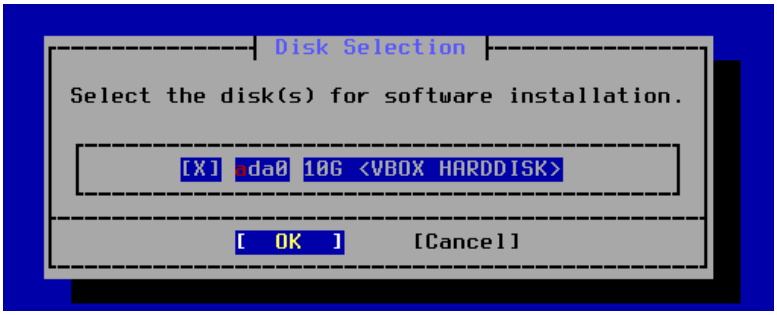
Passo 12 – Peça para continuar a configuração (Continue):



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

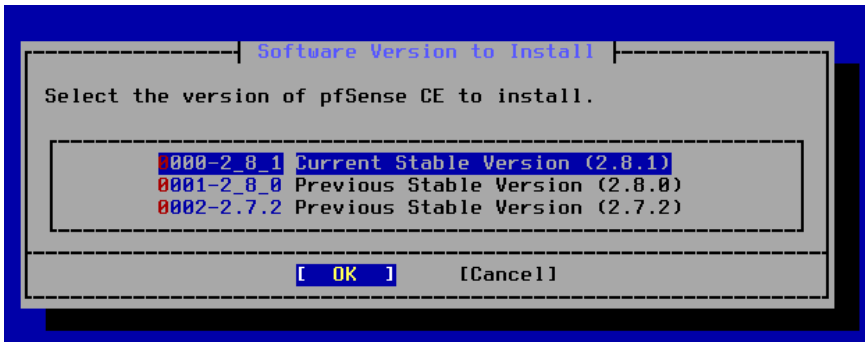


Passo 14 – Peça para continuar a configuração (OK):

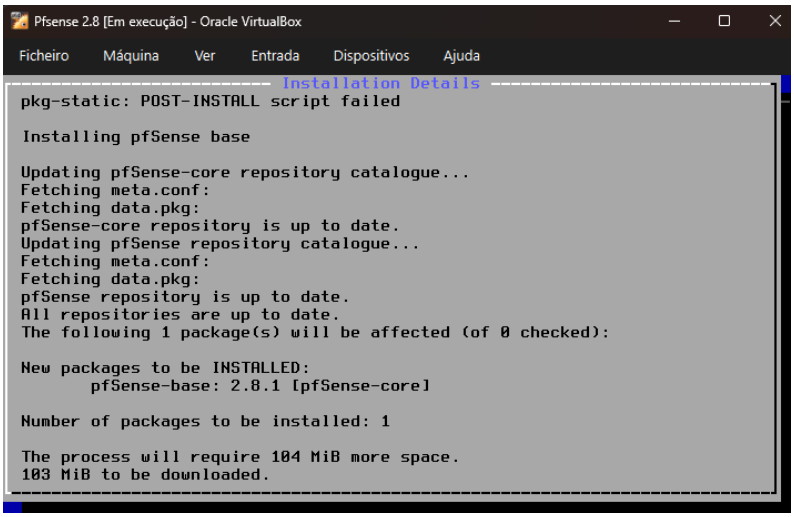


Passo 15 – Confirme a instalação:

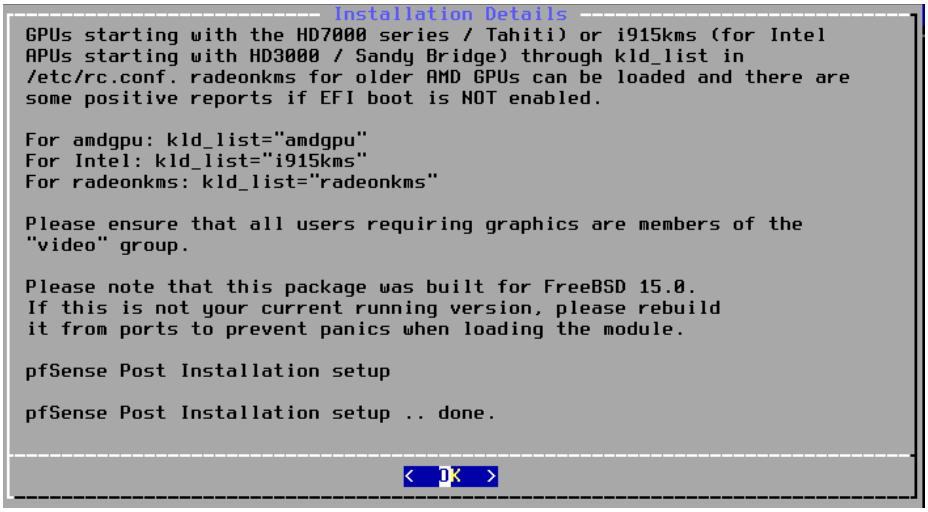
Passo 16 – Selecione a versão mais recente (2.8.1):



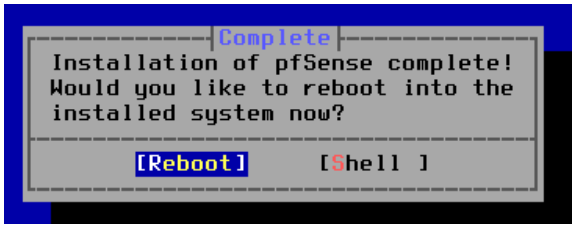
Passo 17 – Deixar efetuar a instalação:



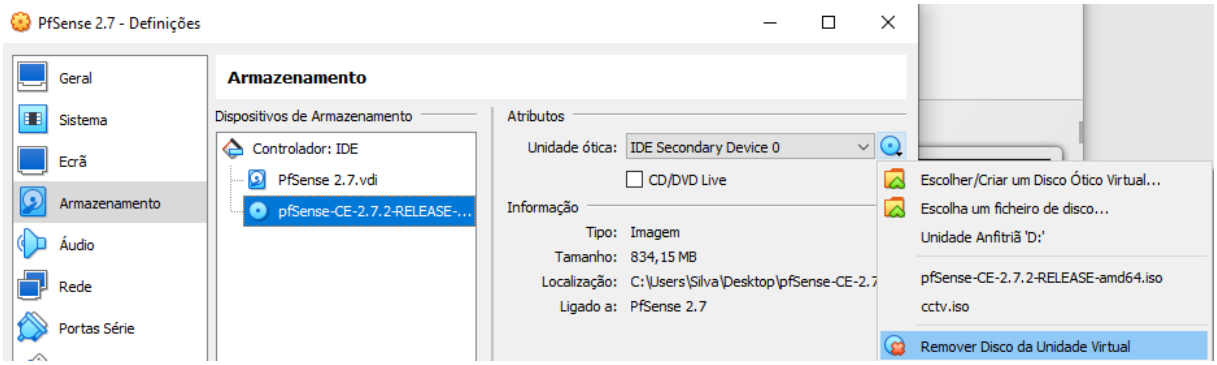
Passo 18 – Após instalar carregue em OK:



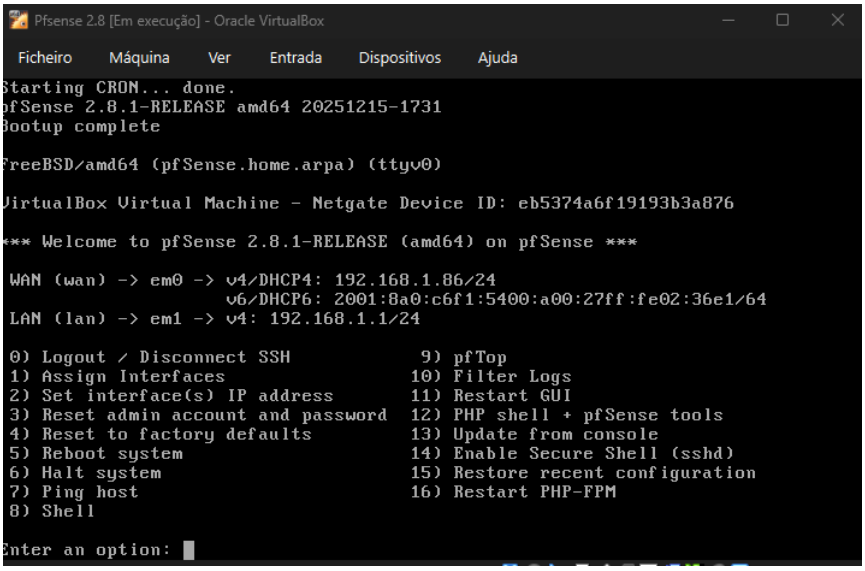
Passo 19 – No final, este irá pedir para reiniciar a máquina virtual com a instalação do Pfsense. Selecione a opção Reboot:



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:



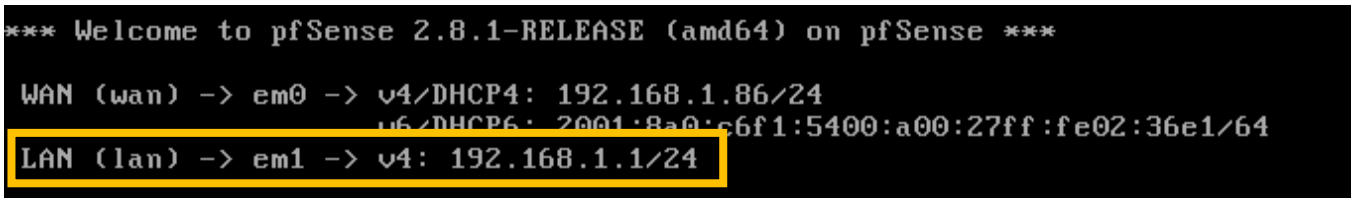
Passo 20 – Este vai acabar de fazer a configuração e costuma demorar um pouco. Quando finalizar, vai mostrar as informações da nossa firewall (do qual vai dar as informações dos endereços IP e afins, bem como um menu de escolhas):

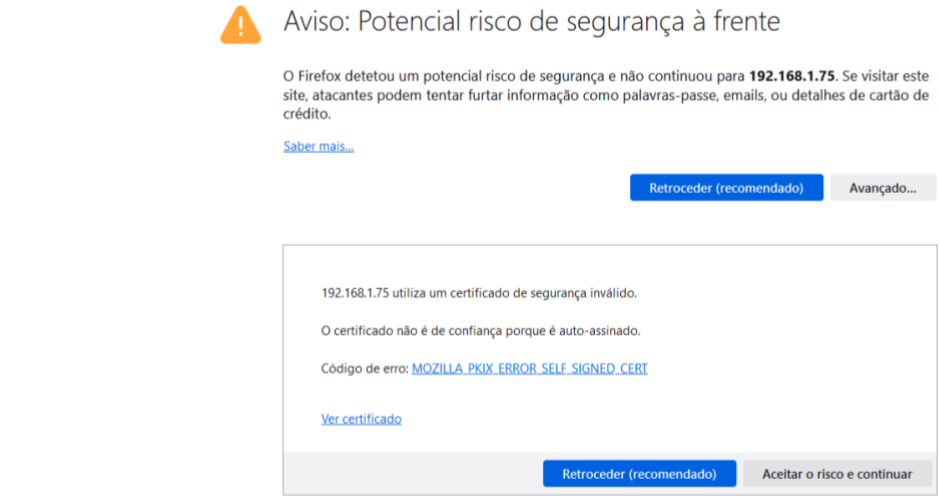


A consola Pfsense permite executar tarefas de configuração, tais como:

- 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 r**einiciar o serviço PHP (útil para resolver alguns problemas do webConfigurator);

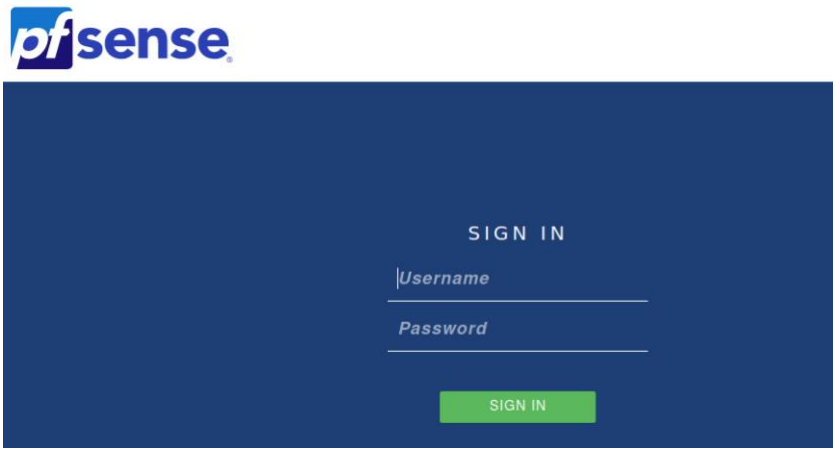
Passo 21 – Inicie a máquina virtual do UBUNTU e de seguida, abra um navegador e coloque o endereço IP para aceder a firewall (normalmente será a segunda interface, ou seja, a interface LAN). Também temos de adicionar nova exceção e para tal basta prosseguir e aceitar os riscos):





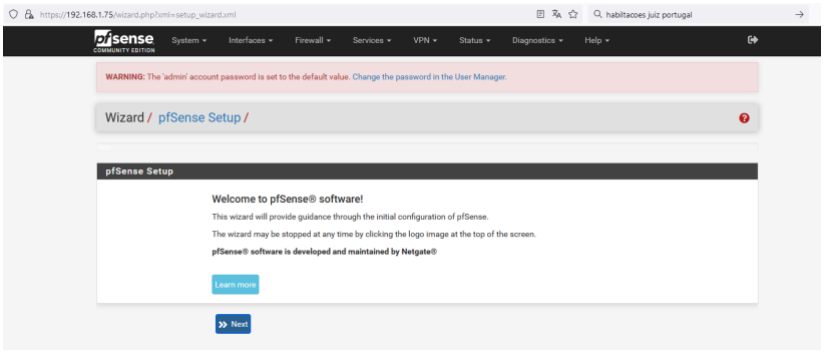
Passo 22 – Para aceder a nossa página pela primeira vez, basta colocar os valores mais abaixo:

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

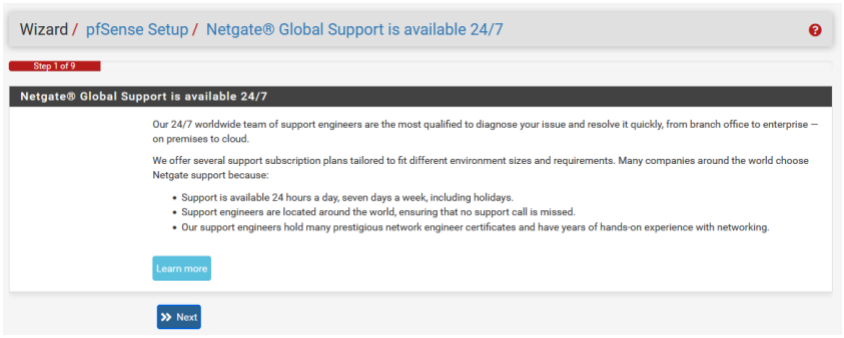


Passo 23 – Normalmente, será feito o tutorial de configuração inicial. Para tal, vamos realizar os seguintes passos:

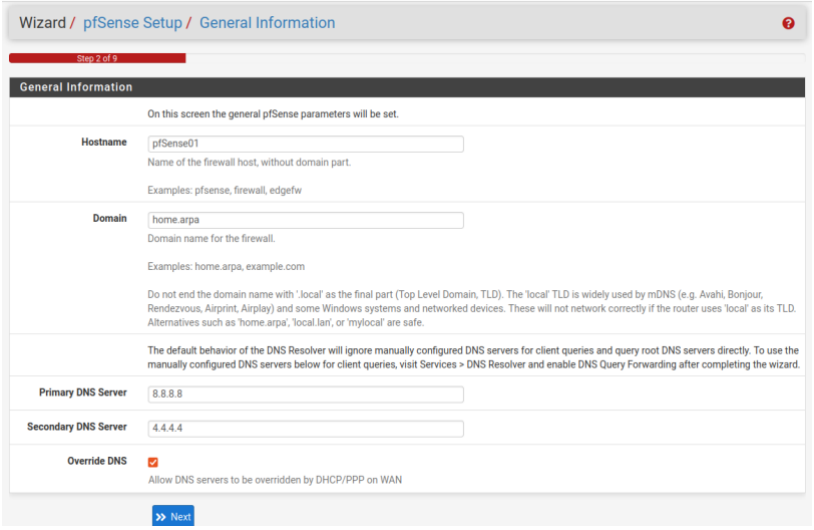
- Prosseguir com a instalação, clicando no botão azul-escuro Next:



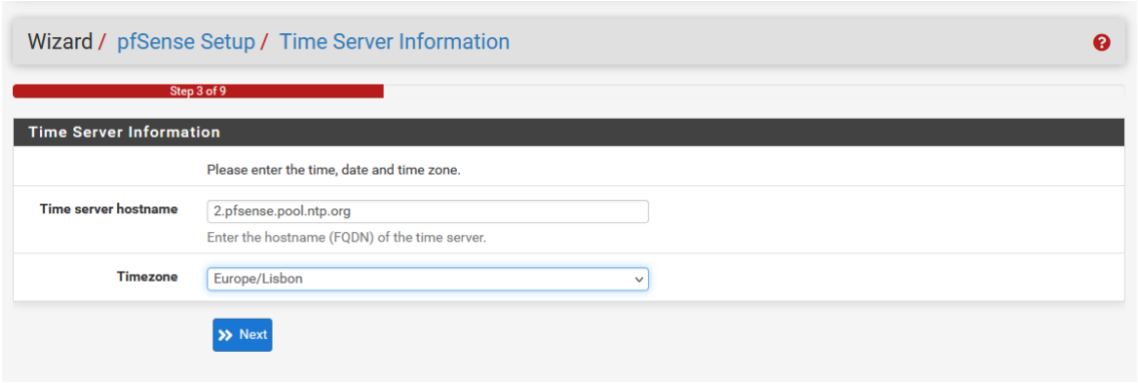
- Prosseguir com a informação inicial, clicando no botão azul-escuro Next:



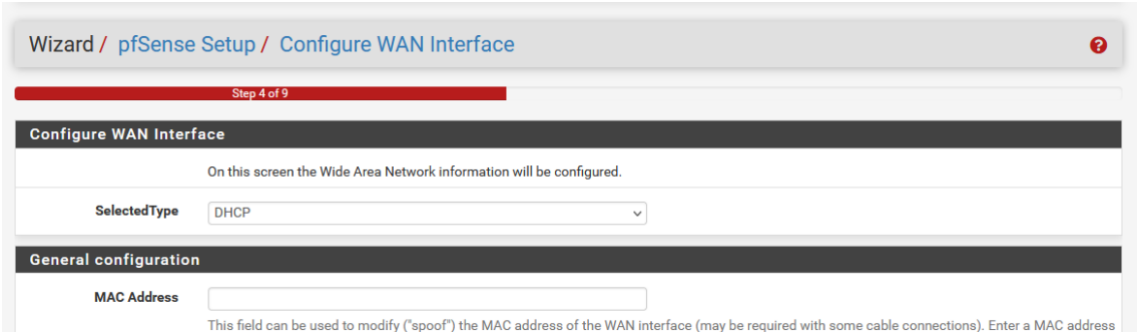
- Dar um nome a vossa máquina, como por exemplo “pfSense01”
- Deixar o domínio (domain) como home.arpa;
- Primary DNS: 8.8.8.8
- Secondary DNS: 4.4.4.4
- Override DNS: Selecionado



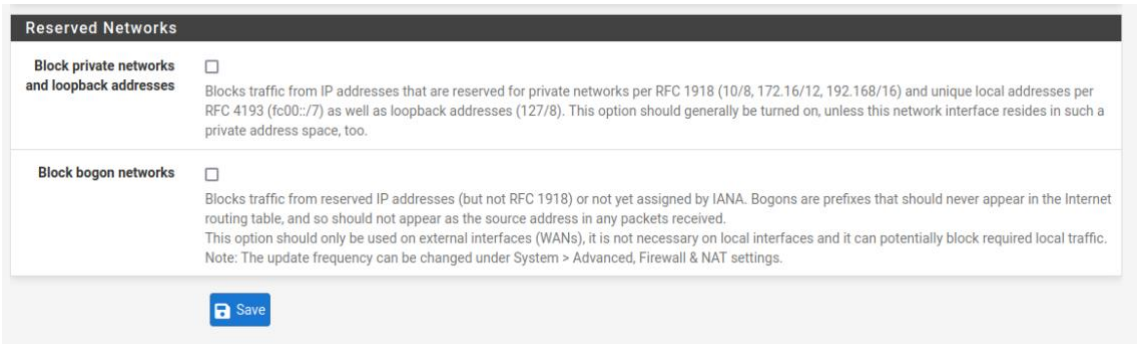
- Definir o fuso horário TimeZone como Europe/Lisbon:



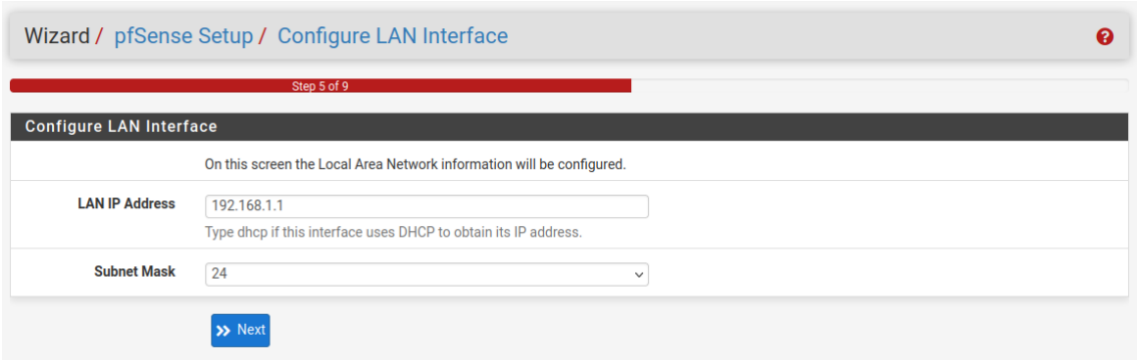
- Na configuração da Interface WAN (ligação exterior), vamos deixar que este tenha um IP dinâmico (mas somente neste caso). Num ambiente de configuração mais avançado, devem ter um IP estático para que este não mude as configurações de deteção dos equipamentos nas redes informáticas:



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

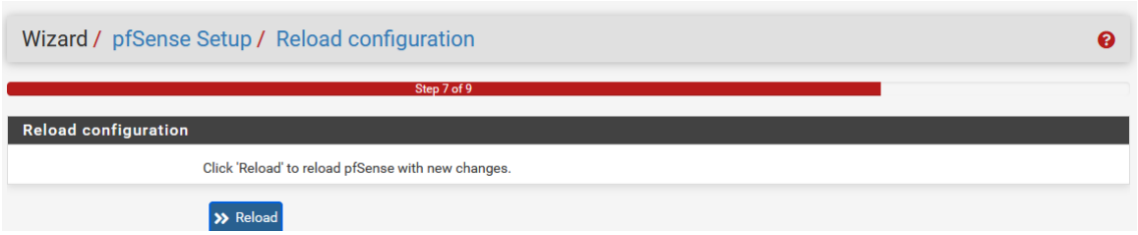


- Na configuração da Interface LAN (rede interna que está depois da firewall), vamos indicar que o servidor vai ser acessível no endereço 192.168.1.1 que tem uma máscara 24:

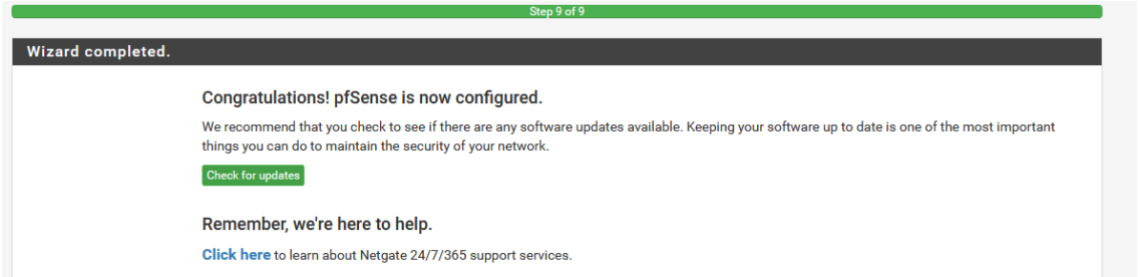


- Definir a senha do admin, que é utilizada para aceder a interface web e também os serviços SSH (quando habilitados):

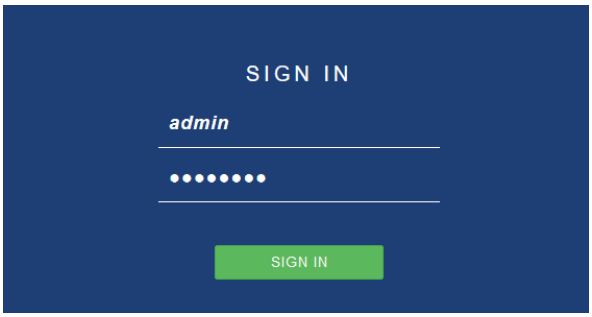
- Pedir para reiniciar o serviço e aplicar as novas modificações:



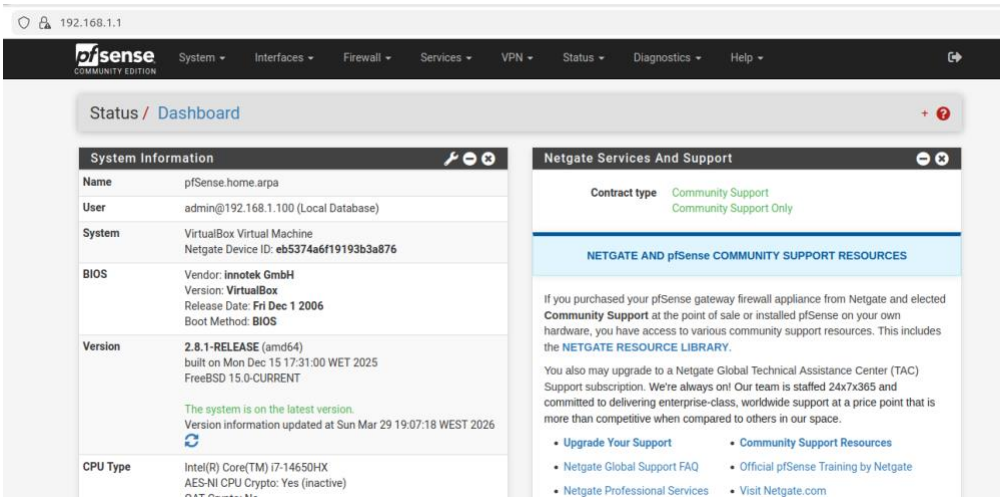
Se tudo correr bem, será exibida a seguinte janela:



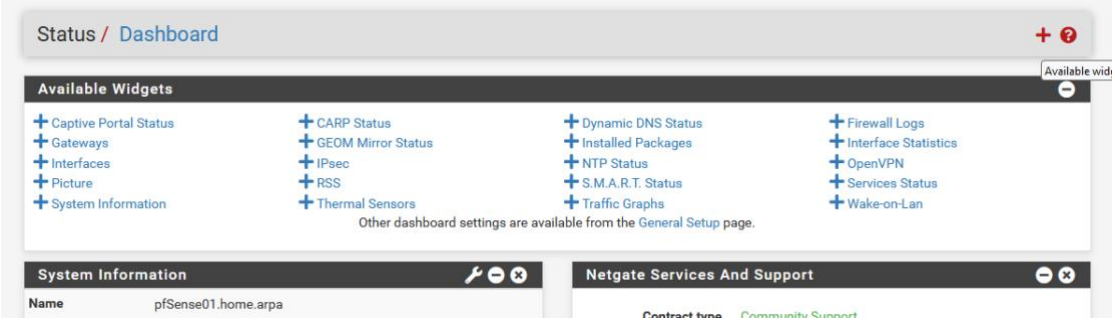
Passo 25 - Faça o logout na aplicação e insira a nova password que acabou de definir.



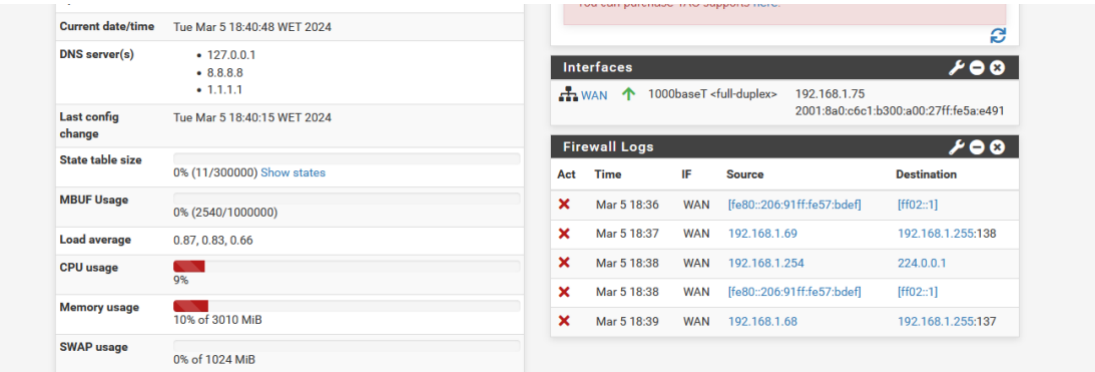
Visualização da tela inicial:



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

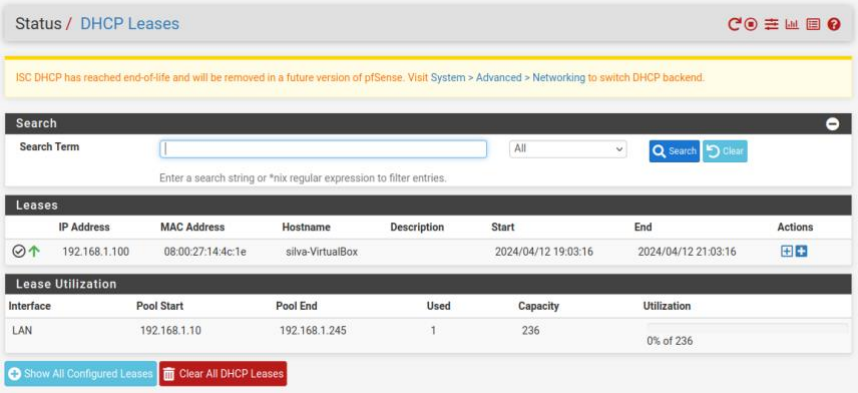


Exemplo de implementação dos logs da firewall:

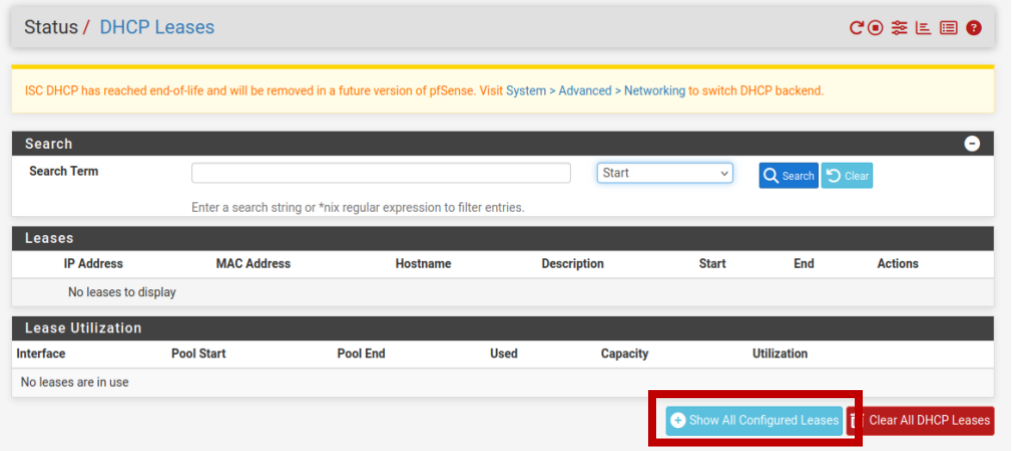


Parte 3 – DHCP Leases (deteção de equipamentos na rede)

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

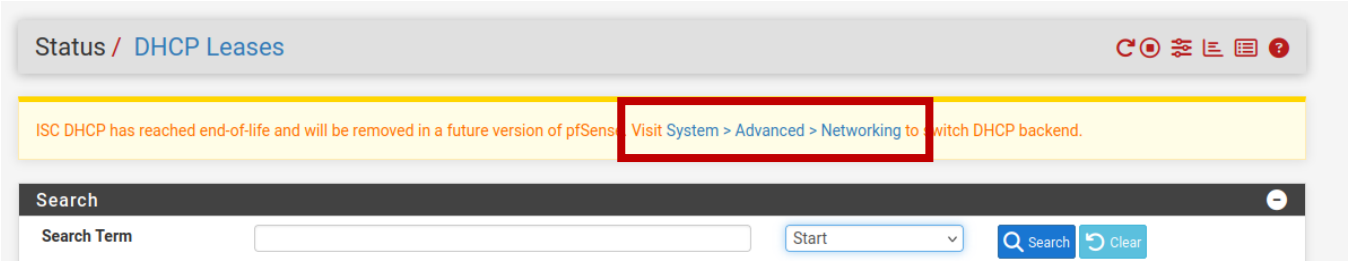


Para ver todas as ligações detetadas (leases), vamos clicar no botão azul-claro "Show All Configured Leases":

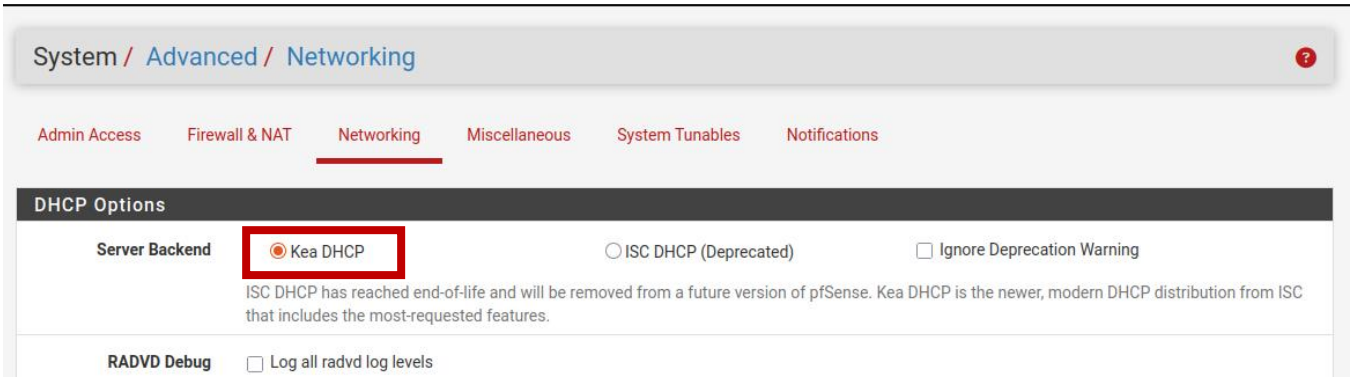


Para verificar a deteção de equipamentos na rede com DHCP, inicie a máquina virtual do Windows com o adaptador da rede na opção rede interna e dentro do sistema operativo, a placa de rede tem de estar a obter o IP automaticamente:

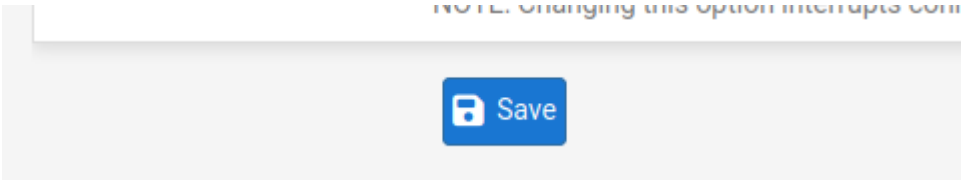
No entanto, como pode ver no início da página, aparece um aviso a dizer que a tecnologia ISC DHCP está a chegar ao fim e que será removido nas próximas atualizações. Para precaver esta situação, vamos começar por clicar na hiperligação azul que irá remeter para as configurações de deteção da rede (Networking):



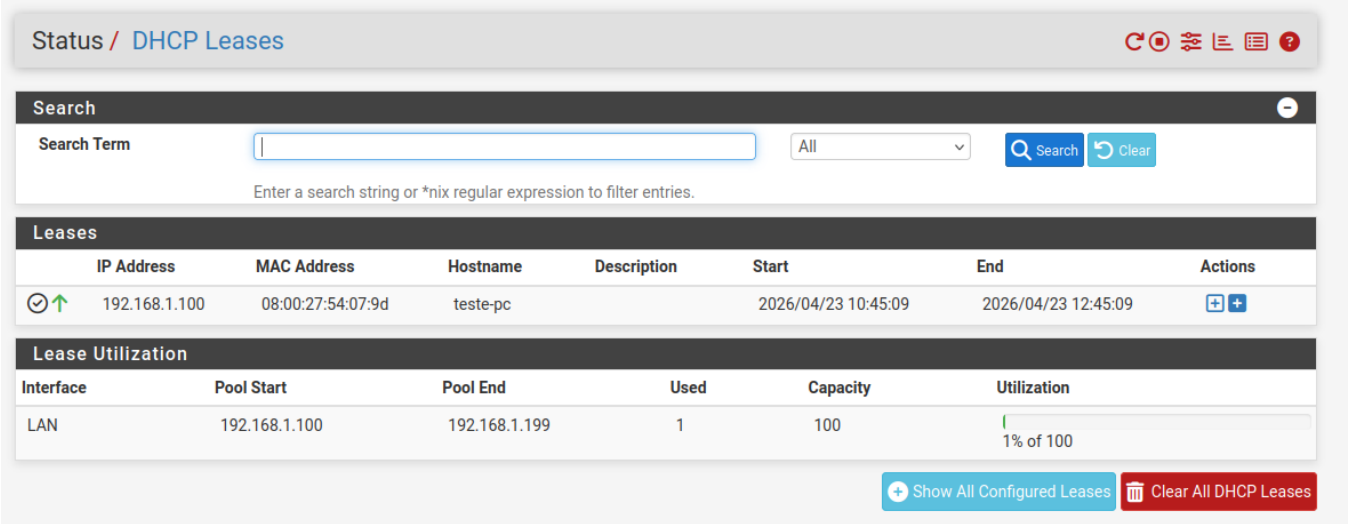
Nas configurações da nova página "Networking", vamos selecionar a tecnologia "Kea DHCP" que é o sistema de deteção mais moderno:



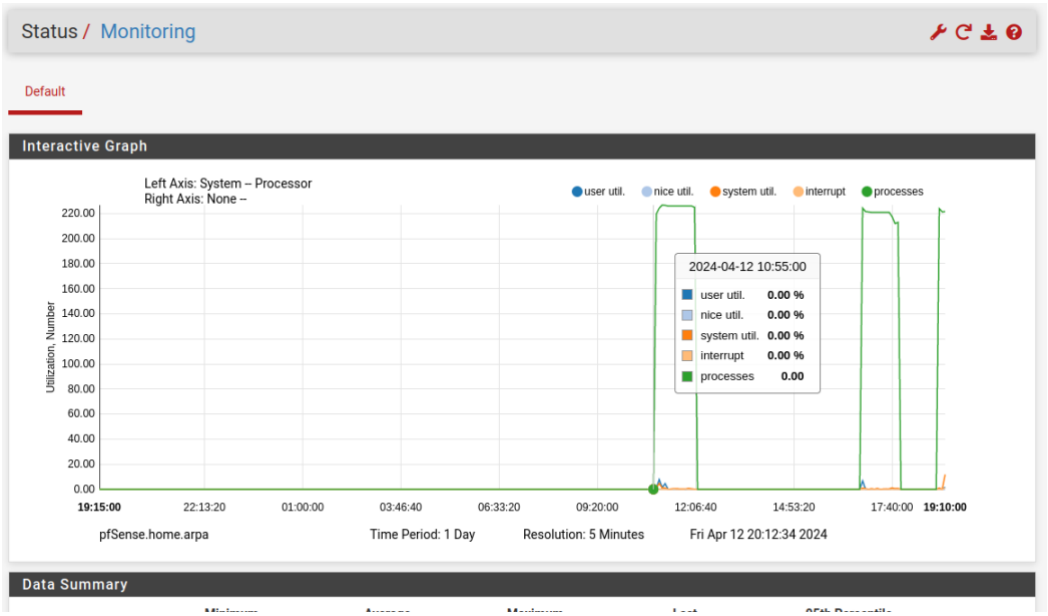
No final, deve ir até ao final da página e clicar no botão azul "Save" para guardar as novas alterações.



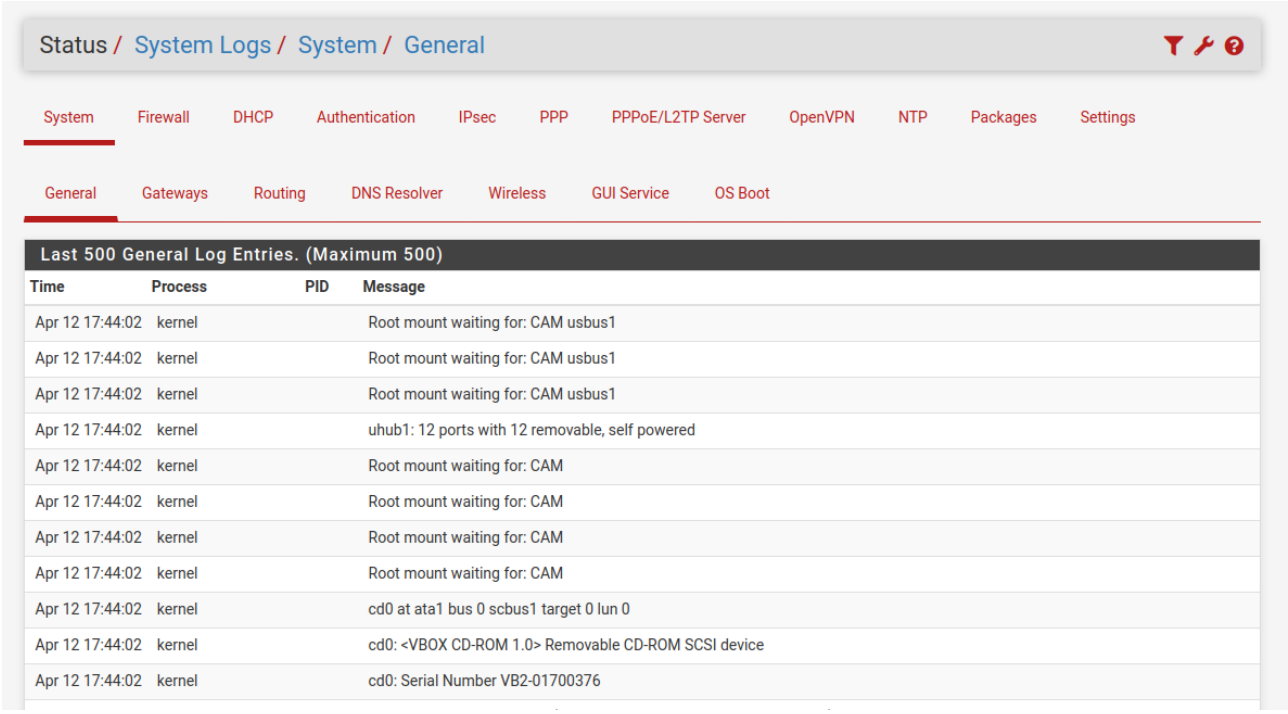
Ative uma máquina Windows 7 e veja a deteção a acontecer em tempo real:



Parte 4 – Monitoring (Monitorização de atividades na rede)



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



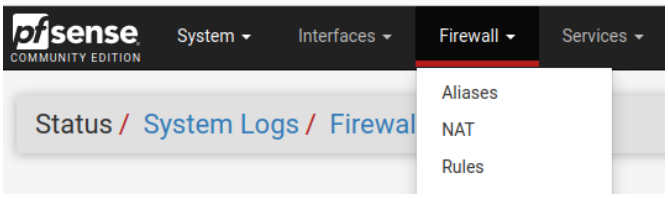
Parte 6 – Regras da Firewall Pfsense

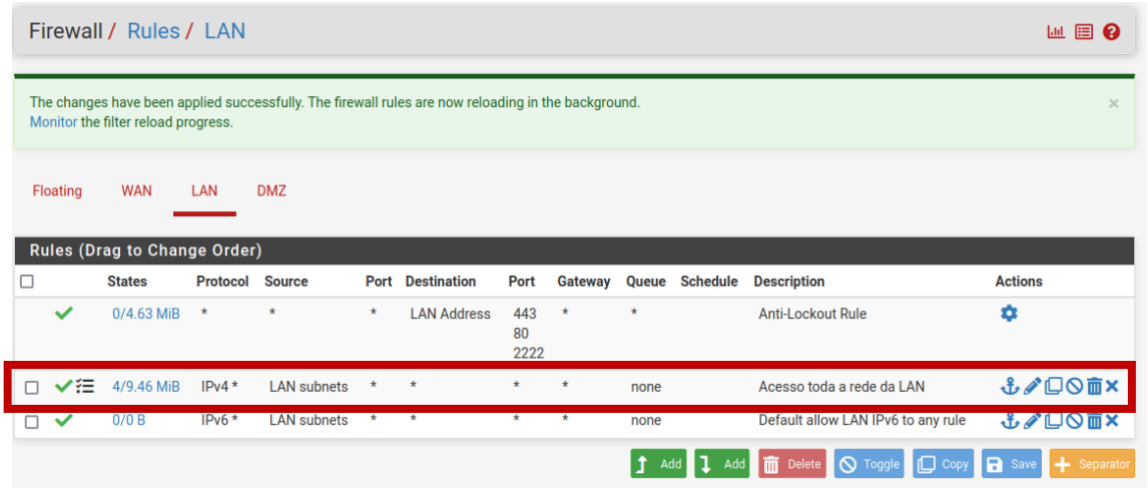
As regras, permitem estabelecer um conjunto de definições para que a firewall possa identificar e resolver os planos delineados para a nossa rede.

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*.

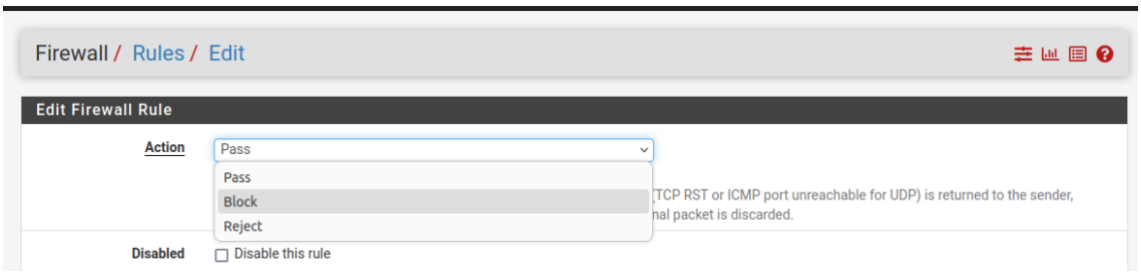
6.1 - Regras de bloqueio de internet geral na LAN

- 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:

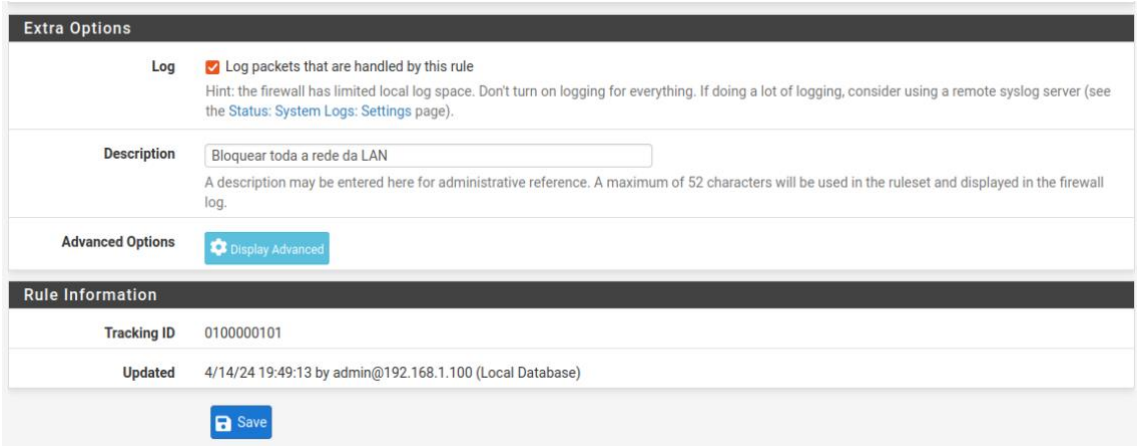




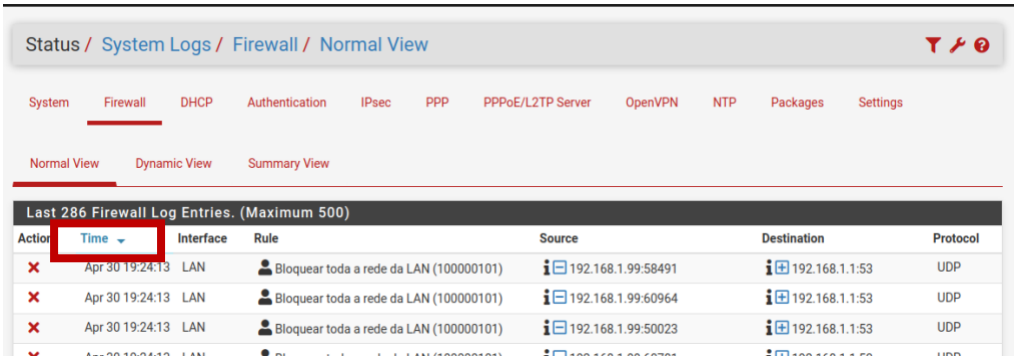
- Coloque a propriedade Action como Block:



- 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":



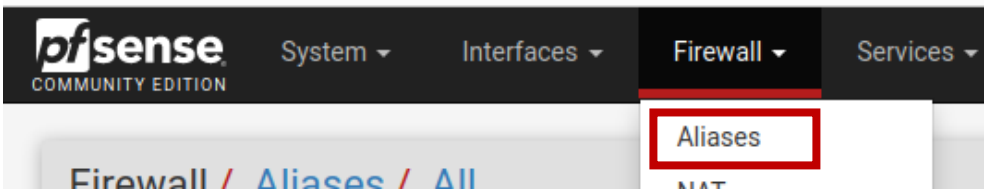
- Tente abrir um navegador e ver se consegue aceder a algum website. Se tudo correr como o que foi especificado, será bloqueado e nos eventos da firewall (Status → System Logs), irá visualizar a seguinte informação:



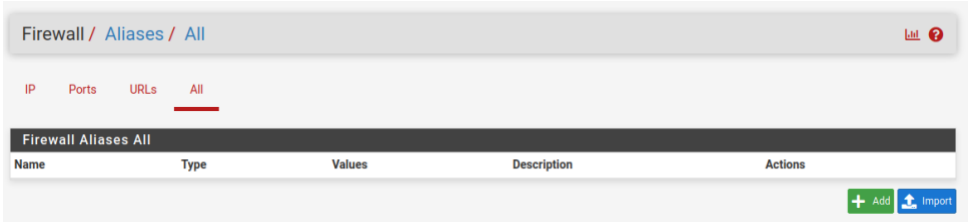
NOTA IMPORTANTE: Verifique o separador ***Time***, pois a ordenação da firewall mostra os dados por ordem crescente. ***Clique em cima no nome duas vezes separadas e veja a ordenação de forma decrescente.***

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 selecionar as opções Firewall → Aliases:

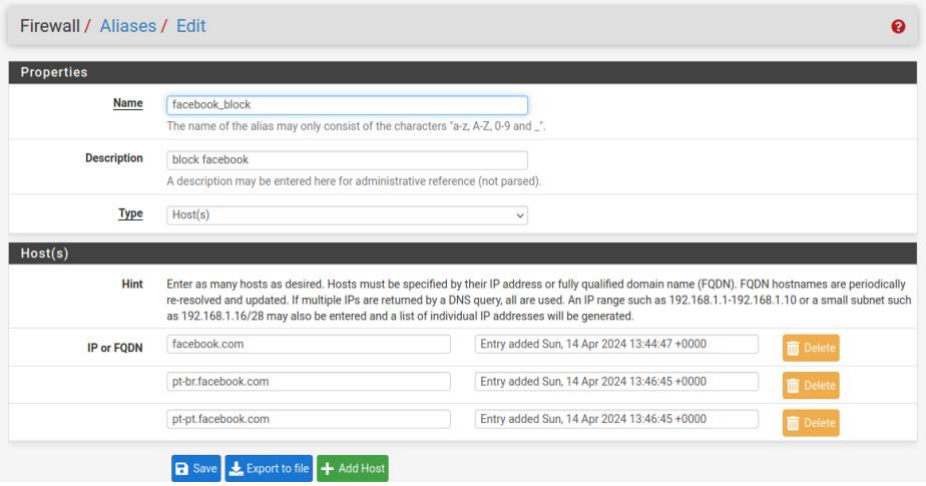


- Clique no botão verde ADD:

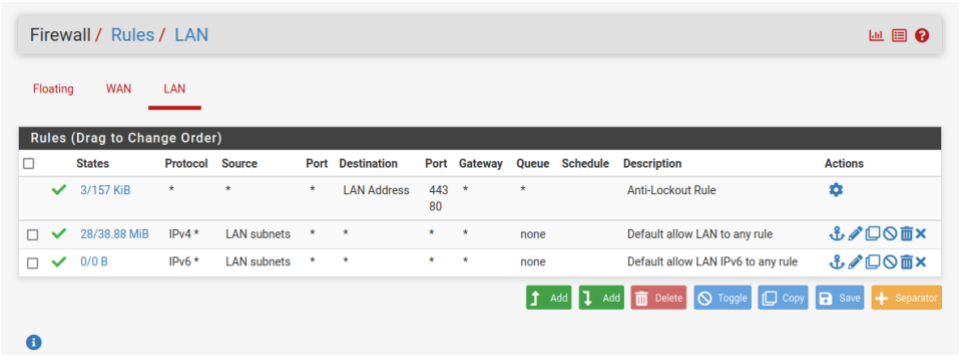


Indique as seguintes informações:

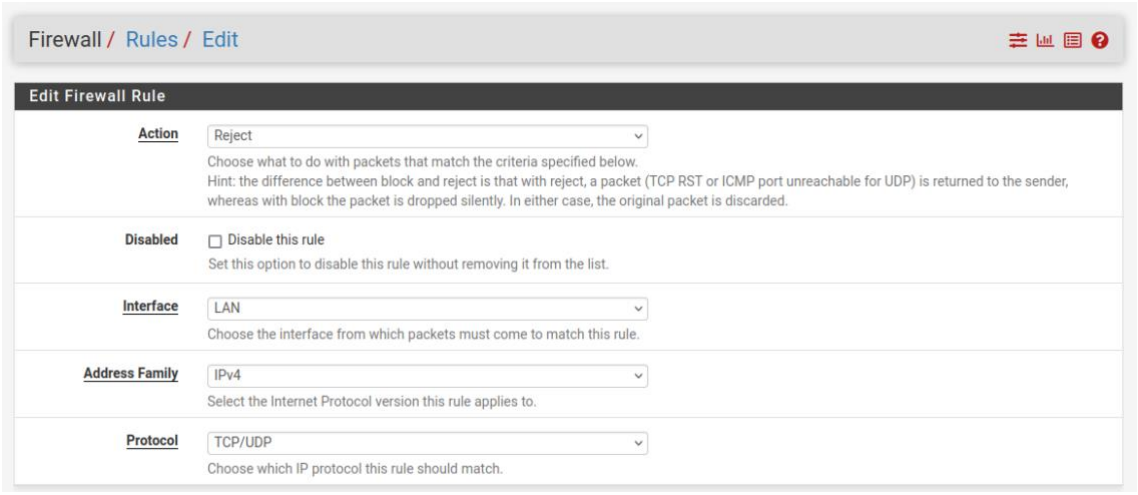
- *Nome*: Facebook_block;
- *Descrição*: Block_facebook (depois vamos importar este nome nas regras);
- *Tipo*: Host (domínio);
- Para tal, não podemos esquecer, que os websites e aplicações podem ter várias maneiras de acesso, como por exemplo, o Facebook, tem o acesso normal (Facebook.com), mas também,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

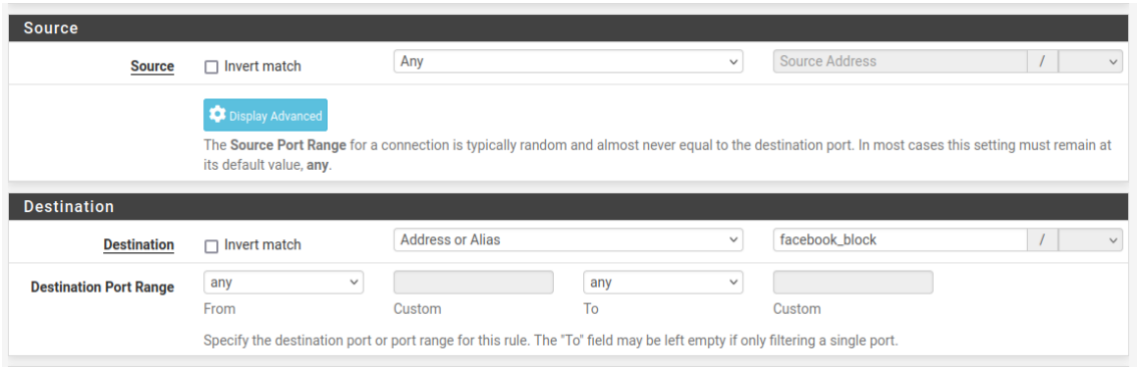


- Volte ao separador das regras da firewall e vamos definir uma regra para que qualquer computador na LAN não possa aceder ao website Facebook. Como tal, clique no botão ADD com seta para cima (para indicar que esta regra é a primeira a ser implementada, antes de qualquer regra que já exista):

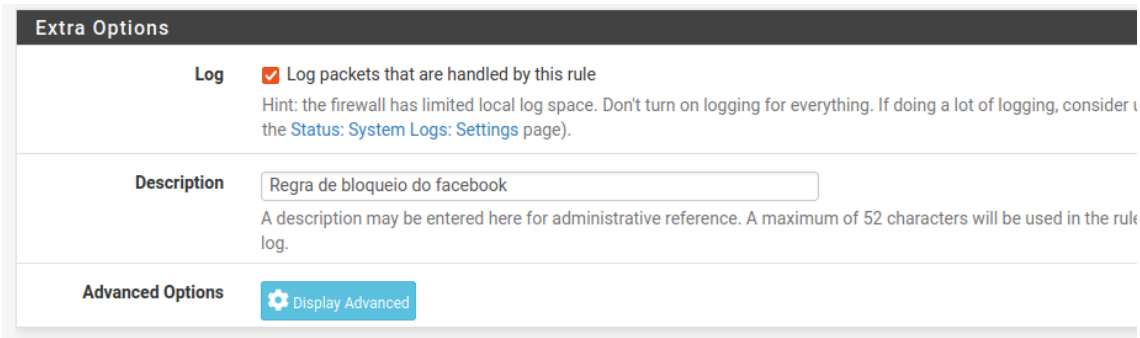


- Coloque os valores:
  - ***Ação***: Reject;
  - ***Interface***: LAN;
  - ***Address Family***: apenas IPv4;
  - ***Protocolo***: UDP/TCP;
  - ***Origem***: Any;
  - ***Destino***: selecione a opção Address or Alias e no campo mais a frente coloque o nome que deu na descrição dos passos anteriores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

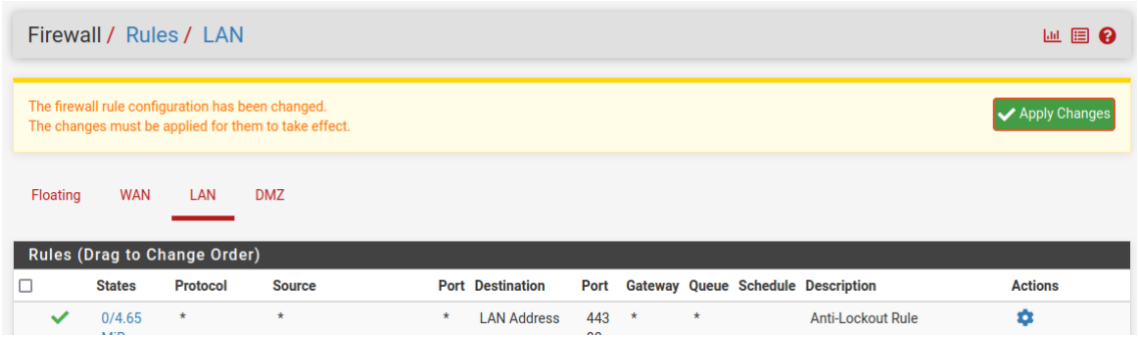




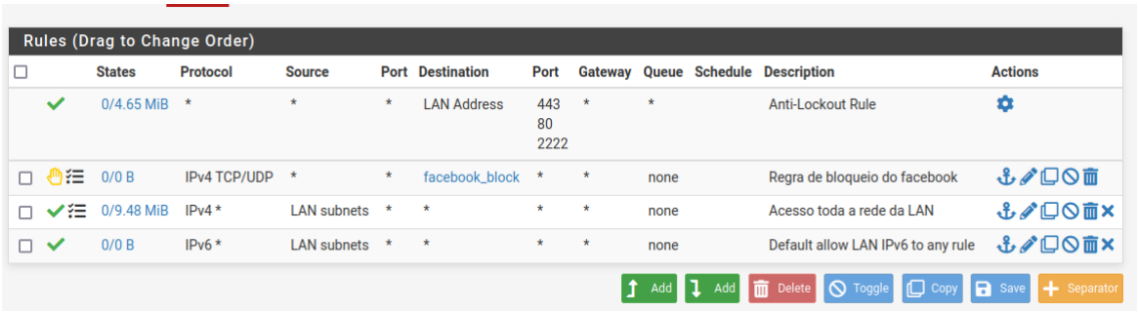
- Mais abaixo, ative a opção Log (para aparecer a regra de bloqueio nos logs da firewall), e coloque a descrição “Regra de bloqueio do facebook”:



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 "Aplly 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:

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.

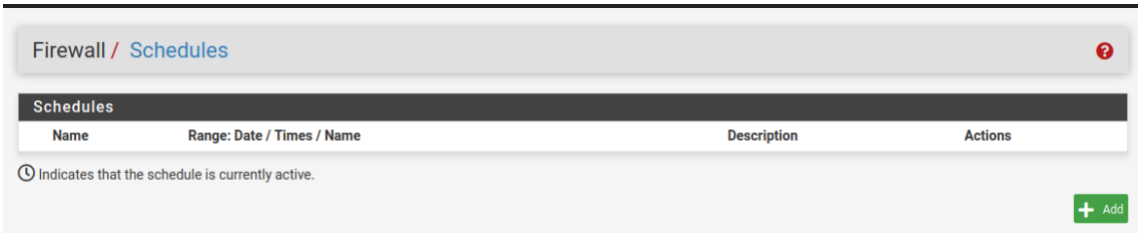
Para realizar esta tarefa, temos de trabalhar 3 seções:

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).

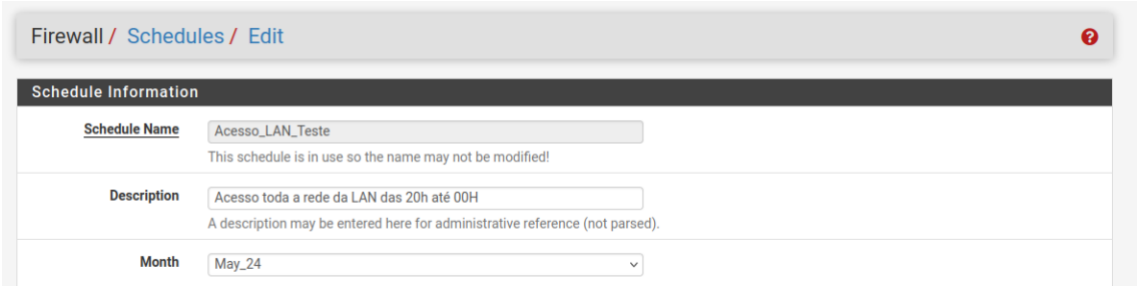
1. Criar agendamento de serviços (Firewall → Schedules);

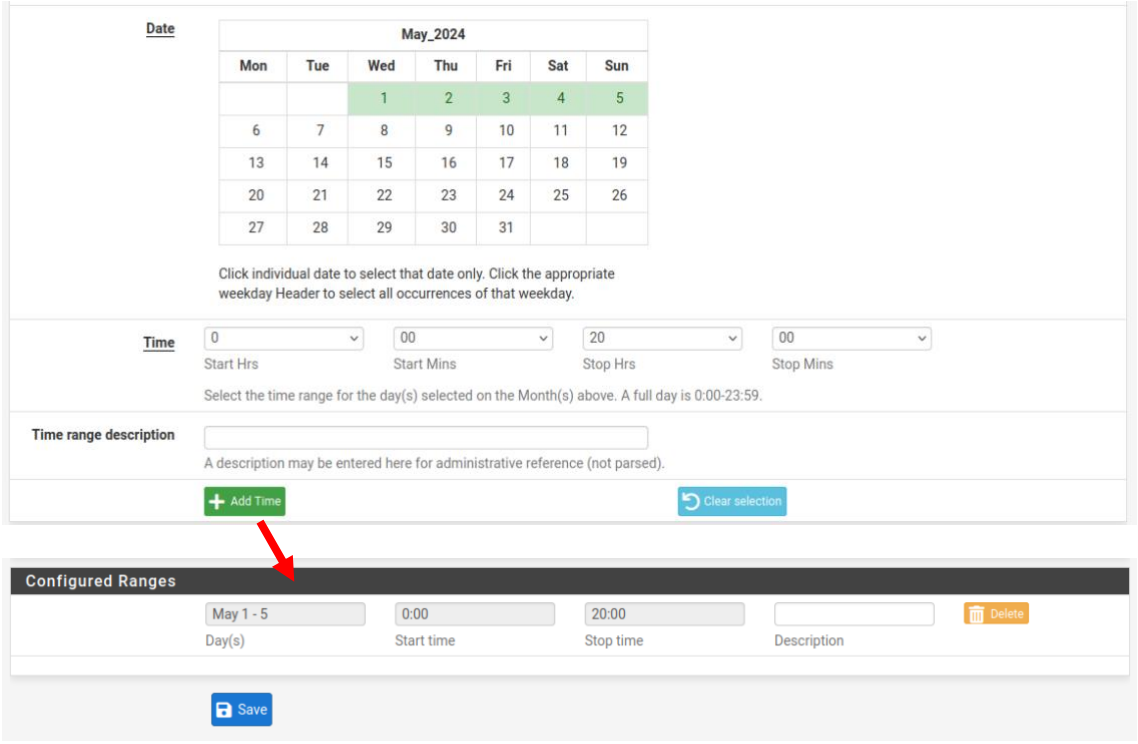
Clicar no botão ADD:



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":

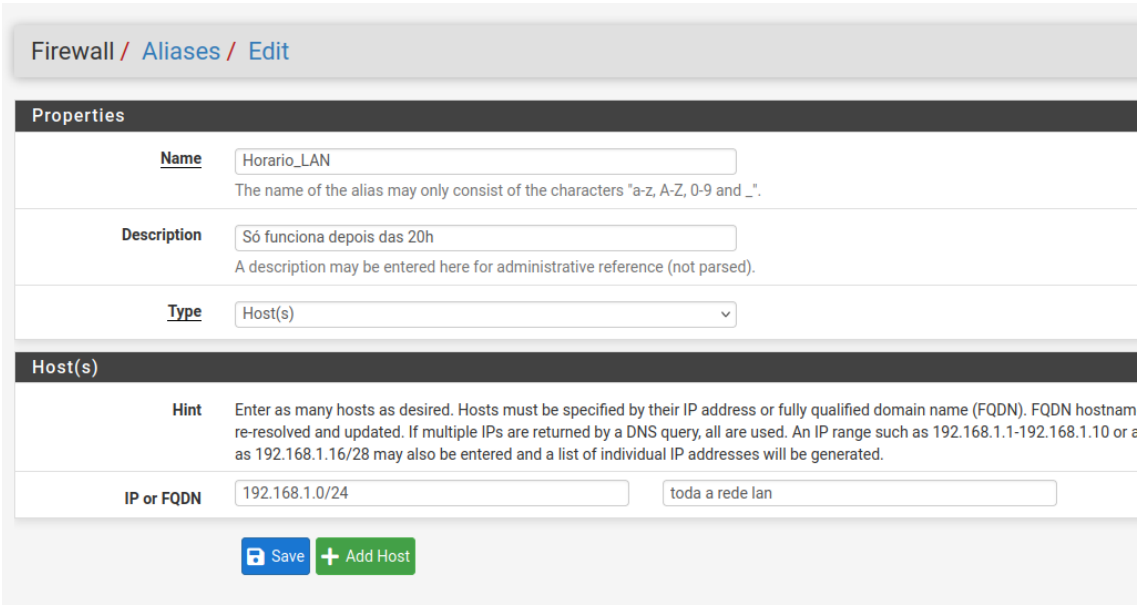




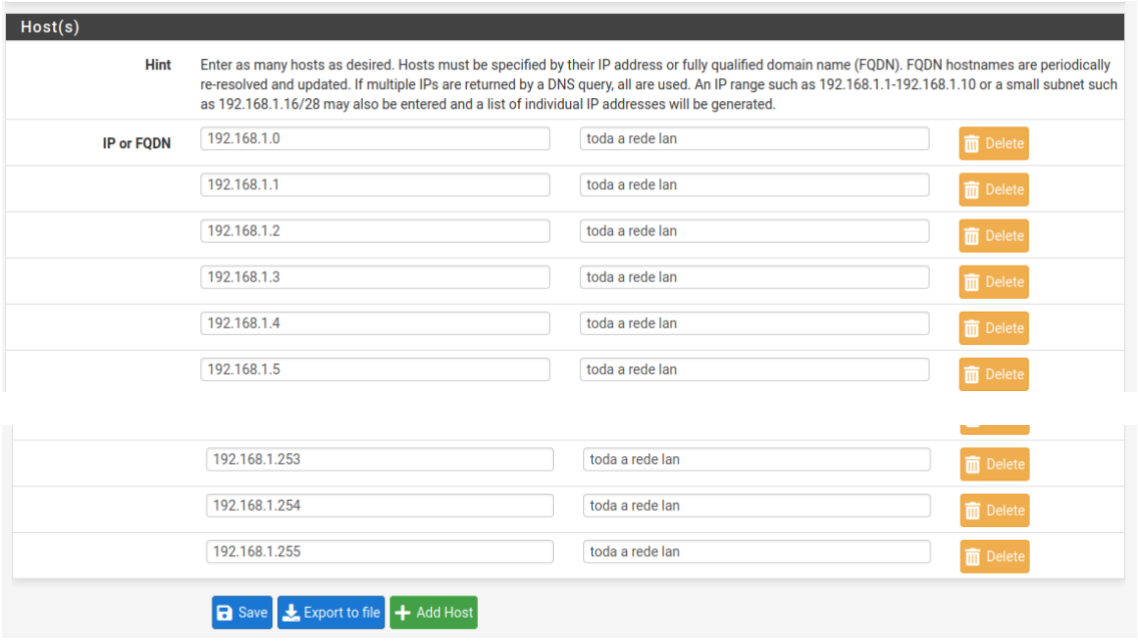
Gravar as novas informações.

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*



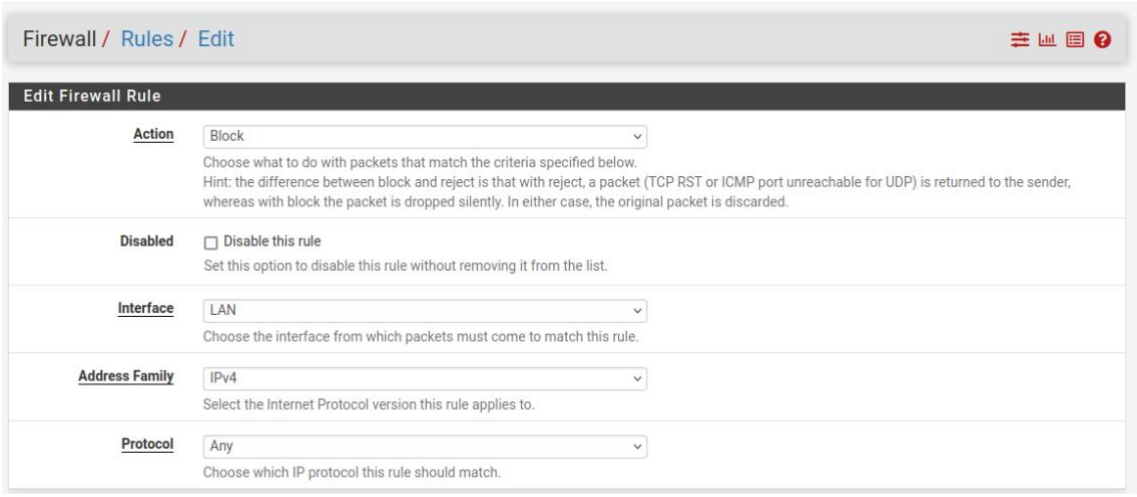
Depois de gravar as novas alterações, e voltar a editar o alias, repare que este colocou todos os hosts do domínio:



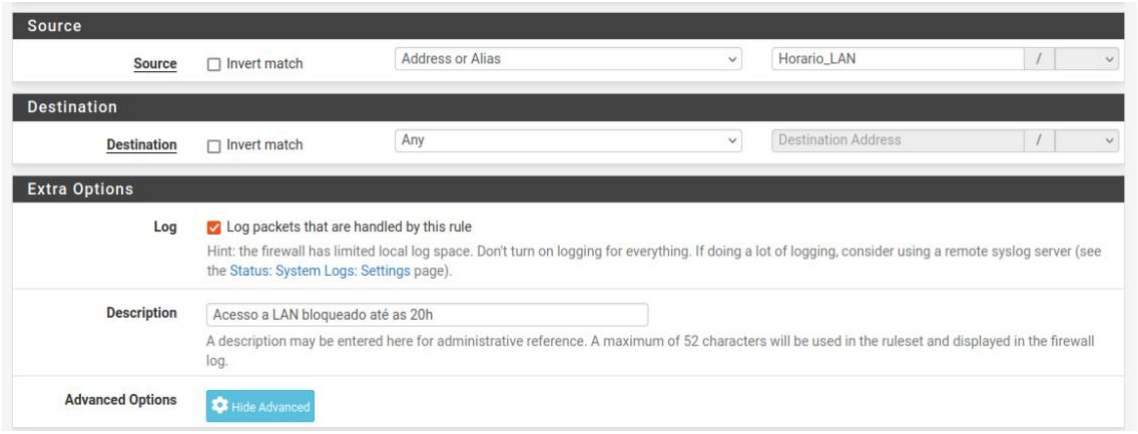
3. Criar regra e implementar os dois passos anteriores;

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):

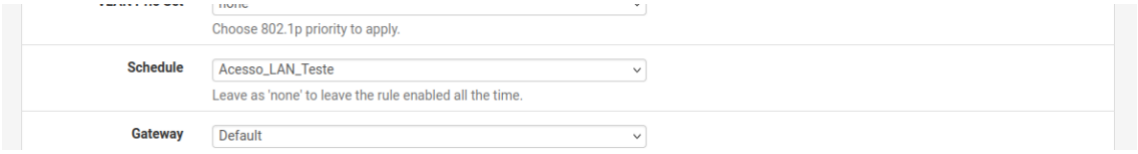
- *Action*: Block;
- *Interface*: LAN;
- *Address Family*: IPv4
- *Protocol*: Any



- *Source*: Address or Alias e escrever o nome Horario_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;

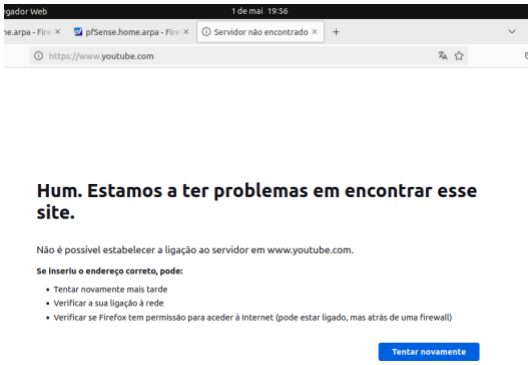


- *Clicar no botão azul com o nome "Show Advanced"* e perto do final, vamos ter uma opção para indicar a regra do agendamento (que foi feito no passo 1):



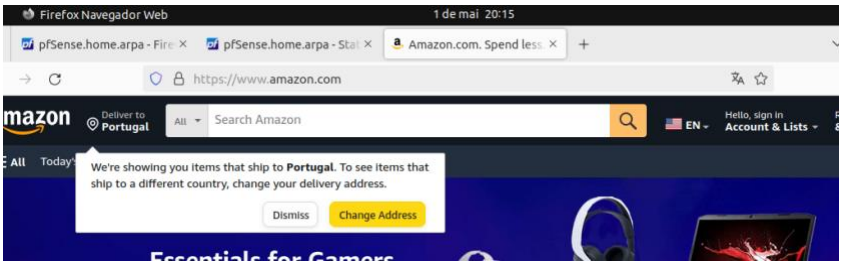
Testes de implementação:

- *Resultado <u>antes</u> das 20H no dia 1 de Maio:*

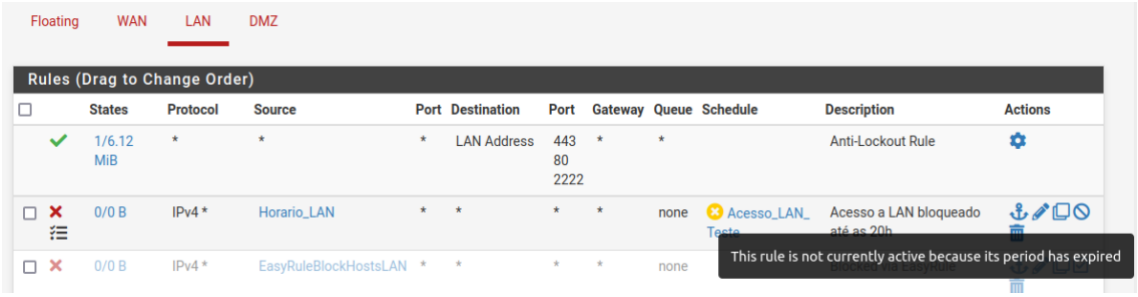


- *Resultado da regra <u>antes</u> das 20H:*

- *Resultado <u>depois</u> das 20H no dia 1 de Maio:*



- *Resultado da regra <u>depois</u> das 20H:*

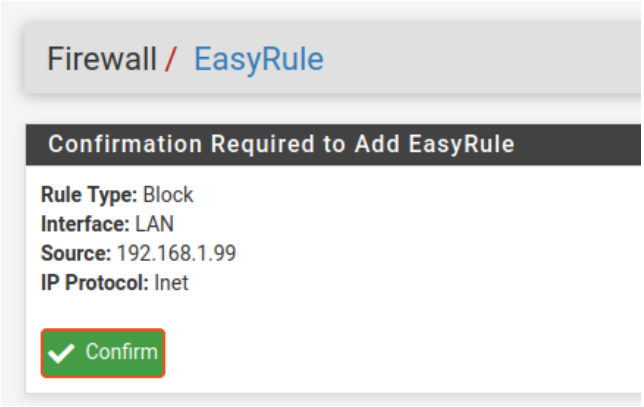


6.4 - EasyRule - Regras de bloqueio por deteção e identificação

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

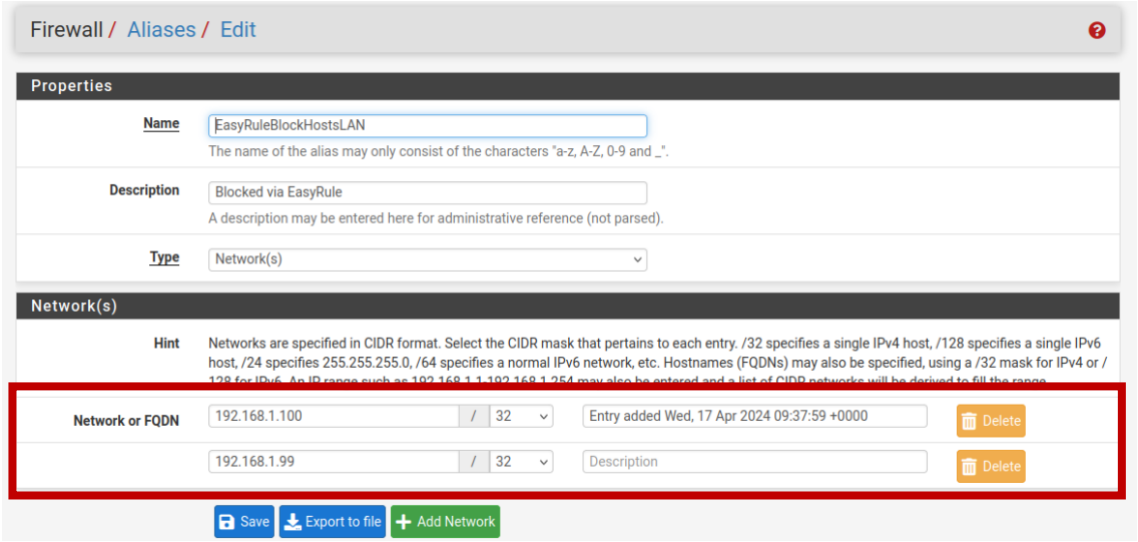
Caso queira bloquear um computador nas regras da firewall, basta clicar na opção – (menos) atrás do endereço IP (normalmente até aparece uma caixa a indicar a mensagem "EasyRule: Add to Block List"):

Este vai abrir uma nova janela para confirmar esta opção.

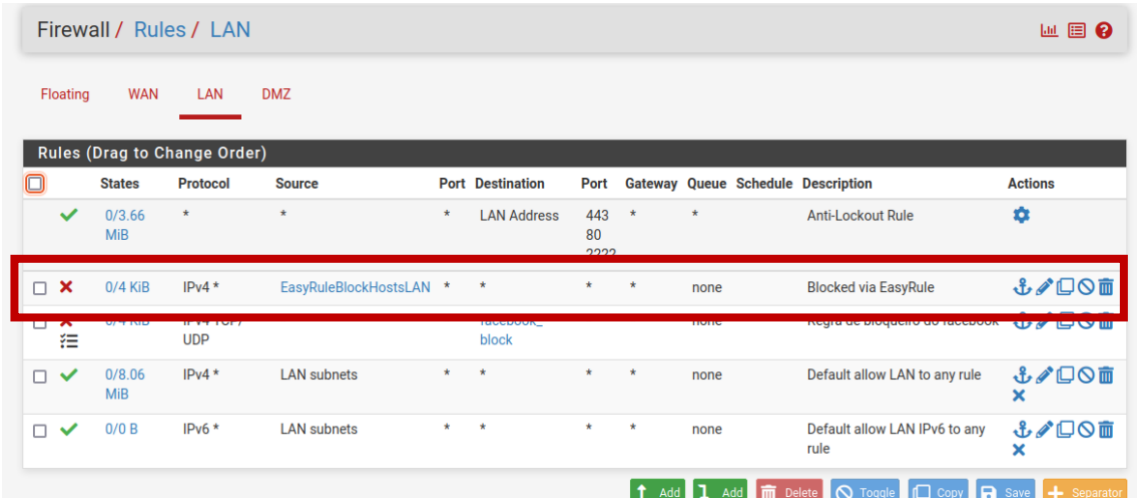


Ao confirmar, o EasyRule vai fazer duas operações:

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



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



Parte 7 – Ativar DMZ no Pfsense

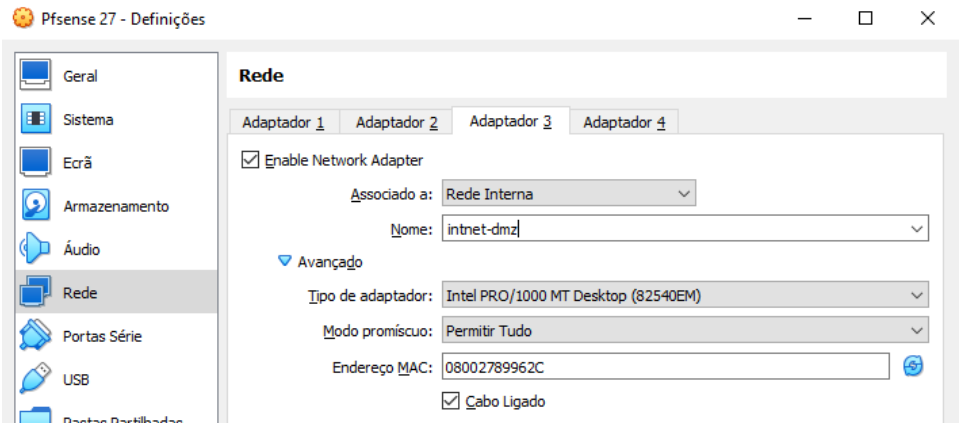
Para adicionar uma nova interface, mais especificamente, incluir a interface DMZ (Zona desmilitarizada), vamos ter de adicionar uma placa de rede adicional nas propriedades da máquina virtual.

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

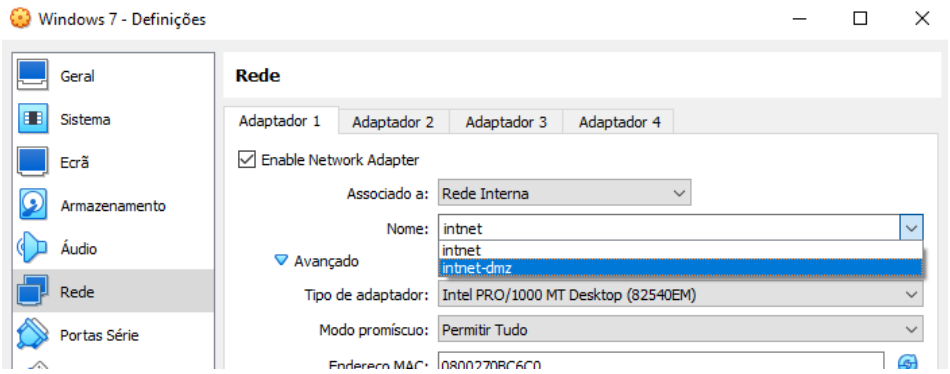
- Interface WAN
- Interface LAN
- Interface DMZ

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

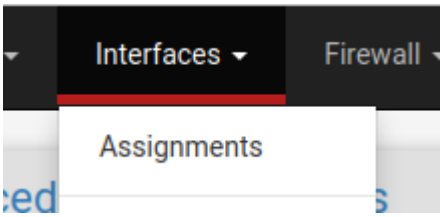
Passo 2 – Dentro das definições da máquina virtual, vamos clicar na opção rede e adicionar um novo adaptador (em rede interna) e na opção do nome, vamos dar um nome diferente, para que este crie duas redes diferentes com o nome "intnet-dmz":



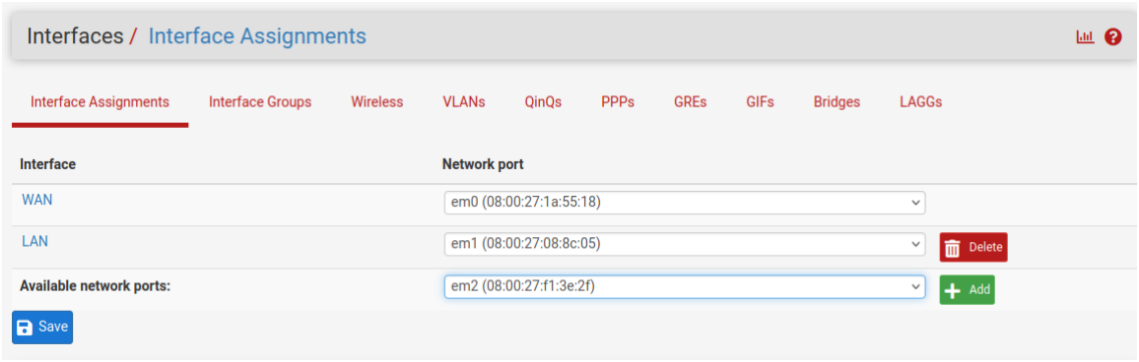
Passo 3 - Vamos colocar a máquina virtual do Windows 7 dentro da interface DMZ. Para tal, deve ir as propriedades de rede da máquina virtual e mudar o adaptador de rede para a rede interna e no nome deve colocar a nova interface que foi criada no passo anterior:



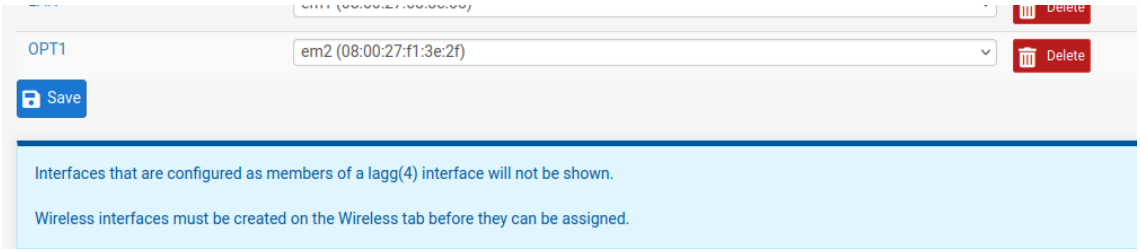
Passo 4 – Entrar na plataforma online do pfsense e no menu superior deve selecionar as opções ***Interfaces → Assignments***



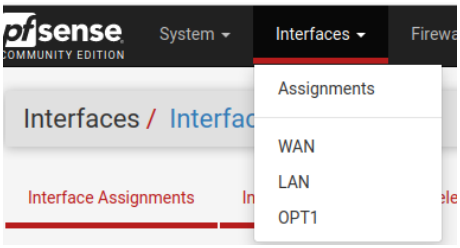
Passo 5 – Se tudo correr bem, será disponibilizada a nova interface da DMZ:



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):

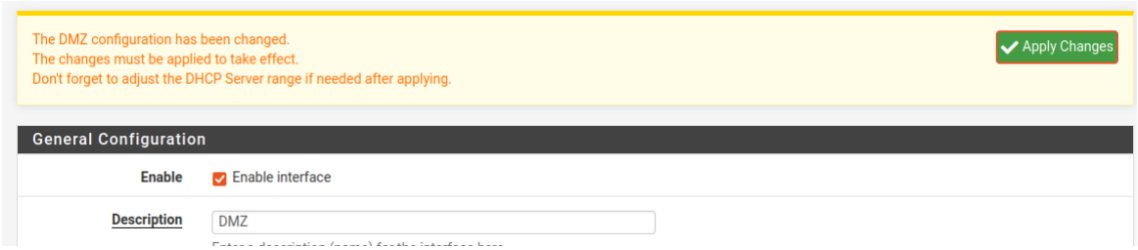


Passo 7 – Dentro da interface da DMZ, deve realizar os seguintes passos:

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

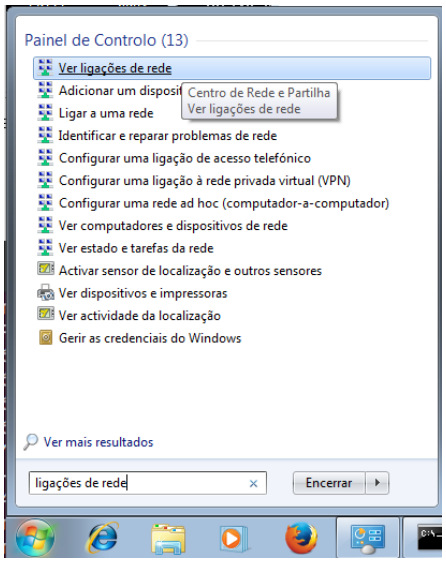
- Configuração IPv4 deve ser: Static IPv4;
- Mais abaixo no separador "Static IPv4 Configuration", vamos indicar que queremos a rede da DMZ na interface com o IP 192.168.2.254/24:

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:

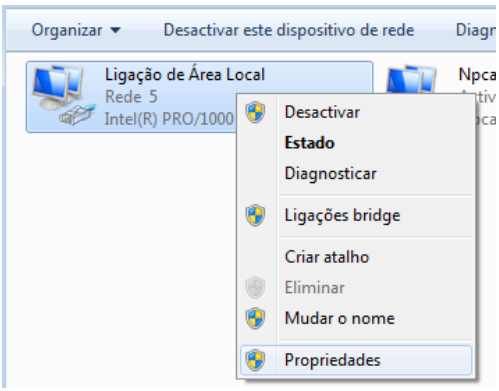


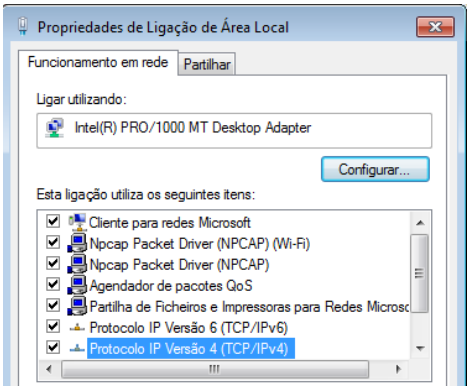
Passo 8 – Inicie a máquina virtual do Windows 7 e quando esta estiver operacional, devemos alterar os dados da placa de rede para atribuir um IP estático (tal como definido anteriormente). Para tal, faça os seguintes passos:

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

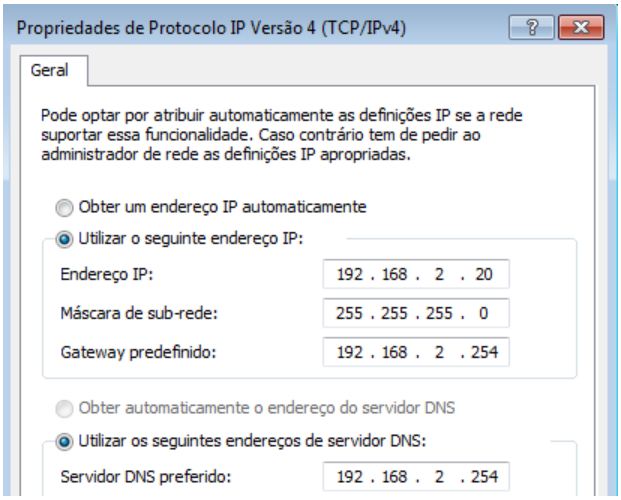


- Na opção ligação de rede local, deve clicar com o lado direito do rato em cima da opção e selecionar "Propriedades" e selecionar a opção Protocolo IP Versão 4 (TCP/IPv4):

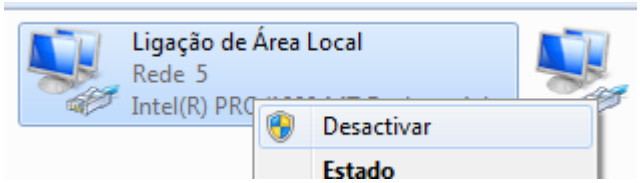




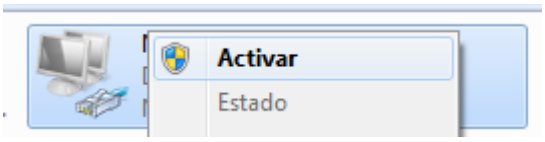
- Alterar a gama de endereço IP para um IP estático e colocar as seguintes propriedades:



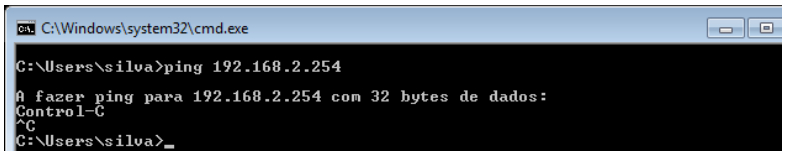
Guarde as novas alterações de seguida, deve reiniciar a interface de rede no Windows:



E voltar a ativar:

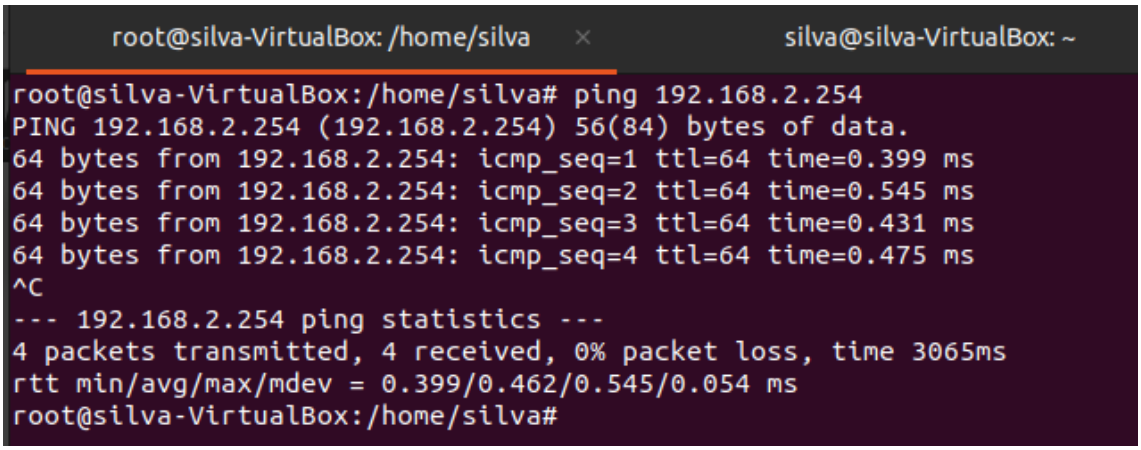


Quando a interface for reiniciada e se tentar fazer ping na interface DMZ da firewall PFsense, este ainda não vai funcionar:

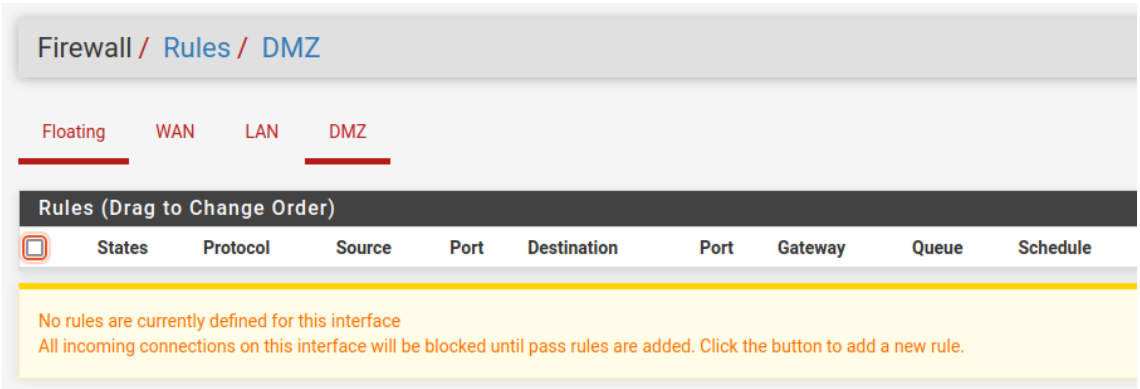


Isto acontece, pois ainda não existe nenhuma regra padrão para trabalhar nessa interface.

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



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:



<u>Adicione as seguintes regras:</u>

Regra DNS:

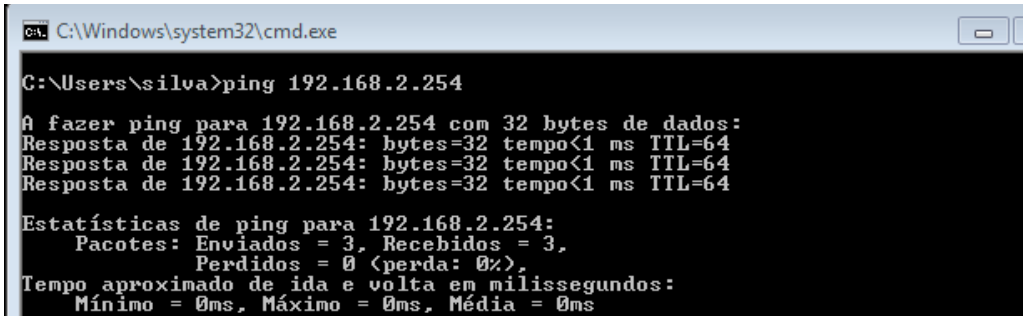
- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: UDP
- Source: DMZ subnets
- Destination: DMZ address

  - 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:



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:

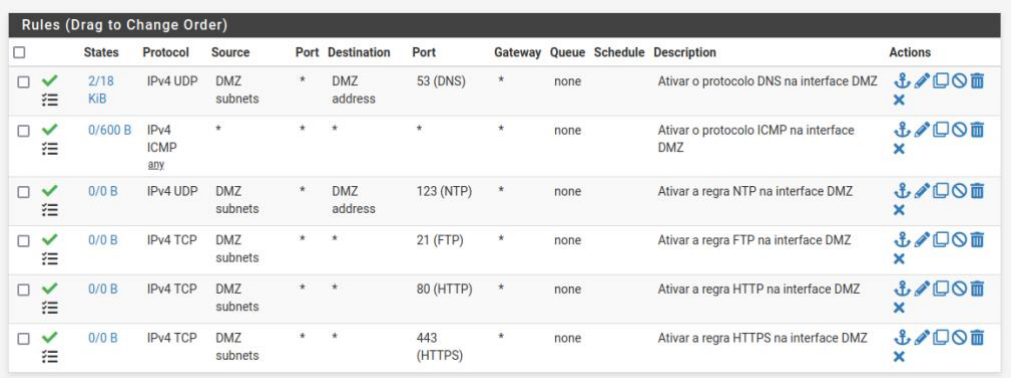
- Action: Pass
- Interface: DMZ (já deve estar automaticamente);
- Address Family: IPv4
- Protocol: TCP
- Source: DMZ subnets
- Destination: any
  - Porta FROM: 80 (HTTP)
  - Porta TO: 80 (HTTP)
- Extra Options:
  - Ativar a opção Log;
  - Description: Ativar a regra HTTP na interface DMZ

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:



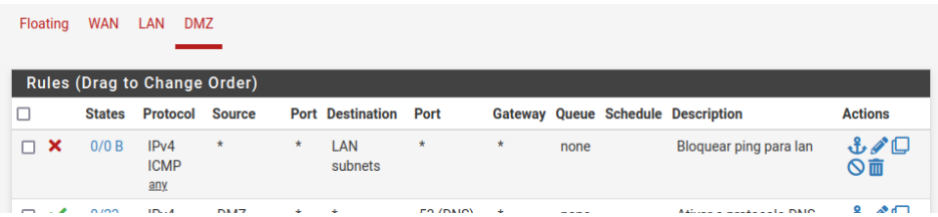
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2/18 KiB	IPv4 UDP	DMZ subnets	*	DMZ address	53 (DNS)	*	none		Ativar o protocolo DNS na interface DMZ	
✓	0/600 B	IPv4 ICMP any	*	*	*	*	*	none		Ativar o protocolo ICMP na interface DMZ	
✓	0/0 B	IPv4 UDP	DMZ subnets	*	DMZ address	123 (NTP)	*	none		Ativar a regra NTP na interface DMZ	
✓	0/0 B	IPv4 TCP	DMZ subnets	*	*	21 (FTP)	*	none		Ativar a regra FTP na interface DMZ	
✓	0/0 B	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	none		Ativar a regra HTTP na interface DMZ	
✓	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:

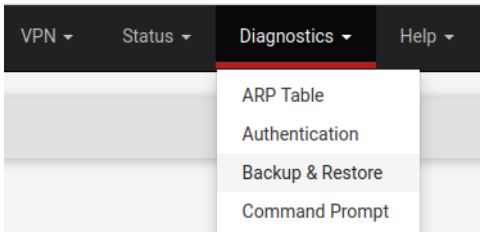


Parte 8 – Backup e Restore

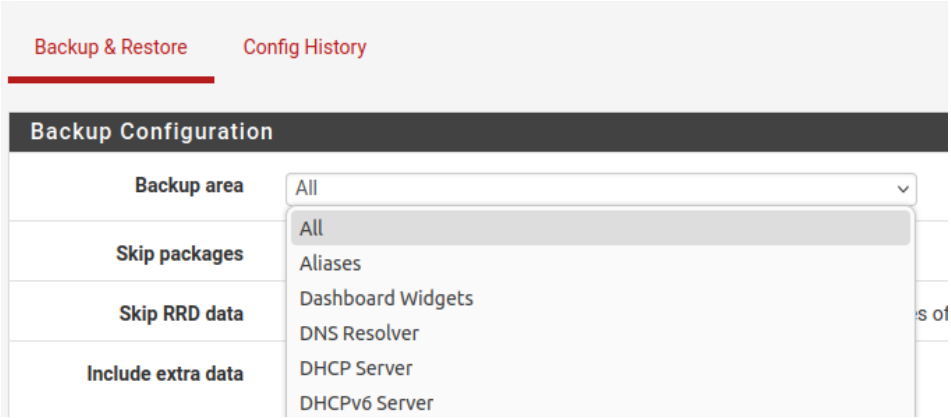
O sistema de backup do pfSense é muito importante para usar em eventuais problemas de hardware ou atualizações que não tenham sido efetuadas com sucesso. Como tal, vamos ver como fazer o backup e eventualmente o restore (restaurar).

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:

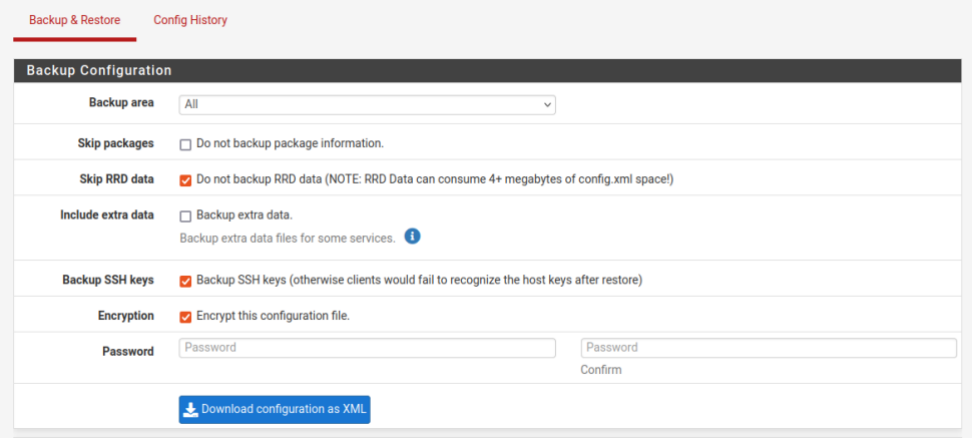


Passo 3 – Para além da opção Backup Area, temos os seguintes campos:

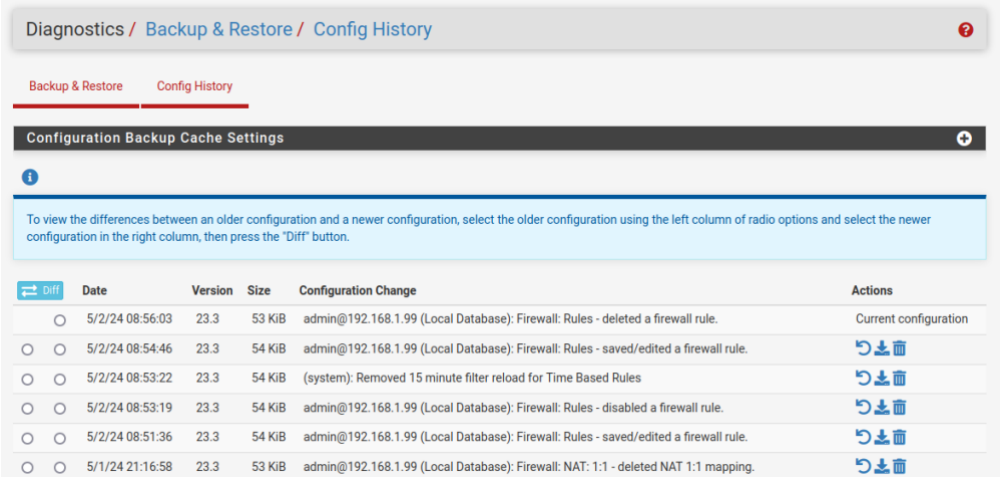
- ***Skip packages:*** não guardar informações de aplicações/pacotes que foram adicionados no pfSense. ***Não selecione esta opção***, pois pode ser importante preservar a informação das aplicações que foram instaladas na firewall;
- ***Skip RRD Data:*** O firewall coleta e mantém dados sobre o desempenho 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 selecione 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 selecionar 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":



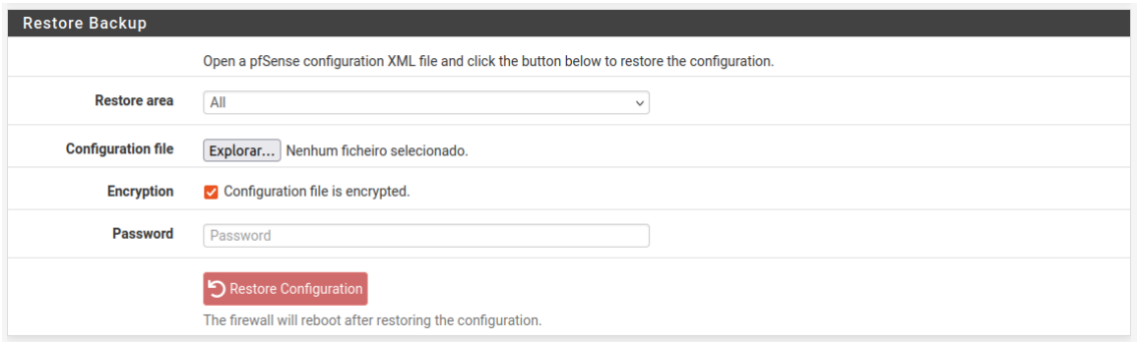
8.2 - Restore

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.

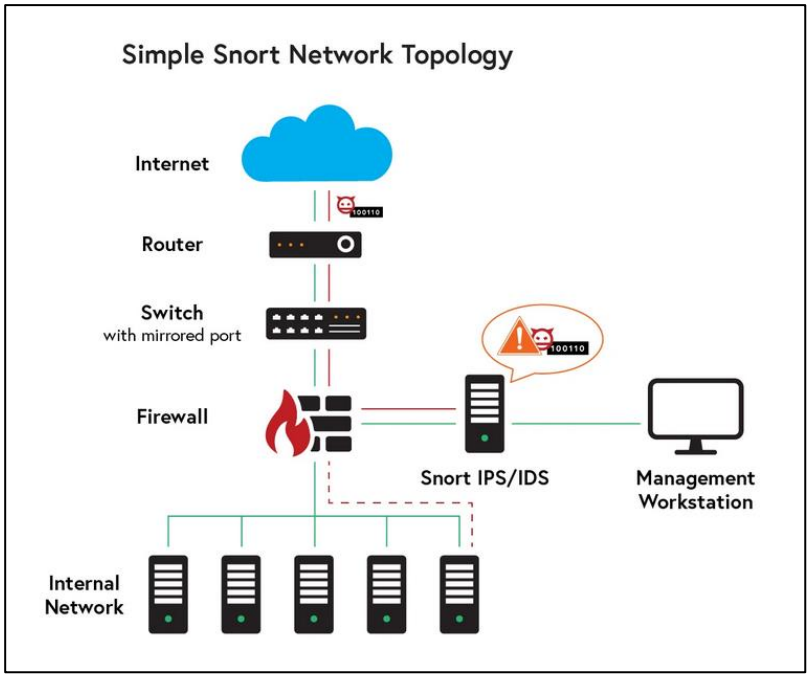
O pfSense vai pedir para reiniciar e após o processo para deixar tudo operacional.



Parte 9 - SNORT e PFSENSE

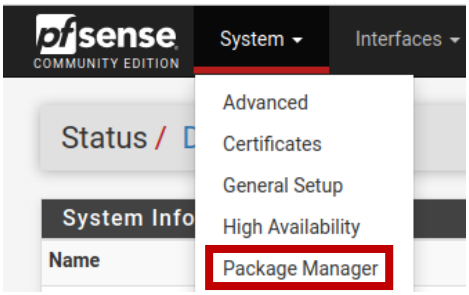
O Snort (https://www.snort.org/) é um sistema de deteção de intrusões (IDS) e de prevenção de intrusões (IPS) amplamente utilizado para monitorizar o tráfego de rede em tempo real e identificar atividades suspeitas ou maliciosas. Esta aplicação analisa pacotes de dados com base em regras e assinaturas, 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.

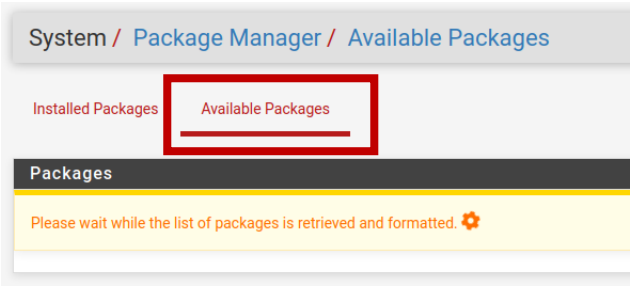


9.1 – Configuração e Instalação Snort

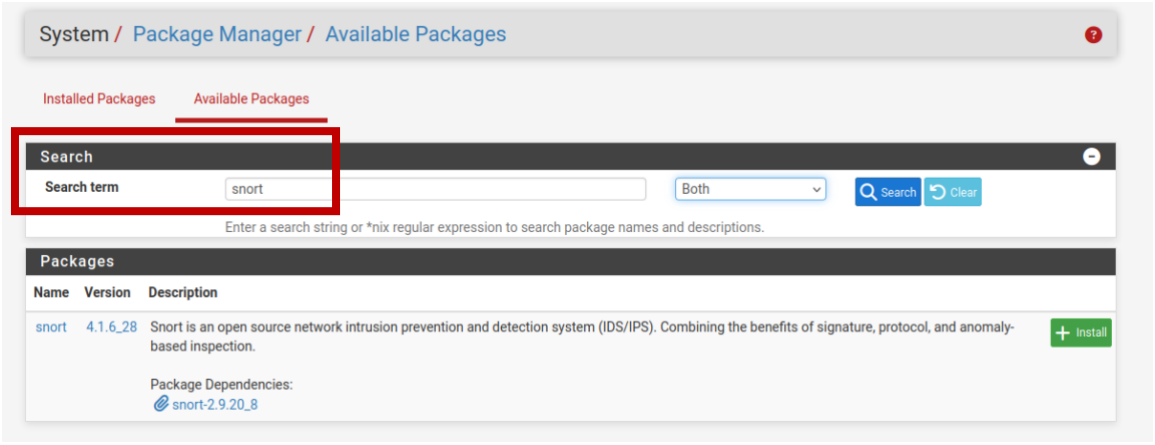
Passo 1 – Para realizar a instalação do Snort no PFSense, devemos ir ao menu superior da aplicação e clicar nas opções ***System → Package Manager:***



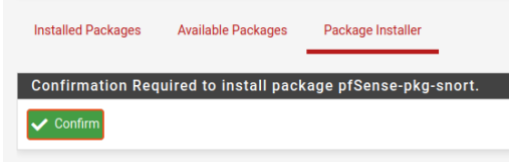
Passo 2 – Na nova página, vamos clicar no separador "Available Package":



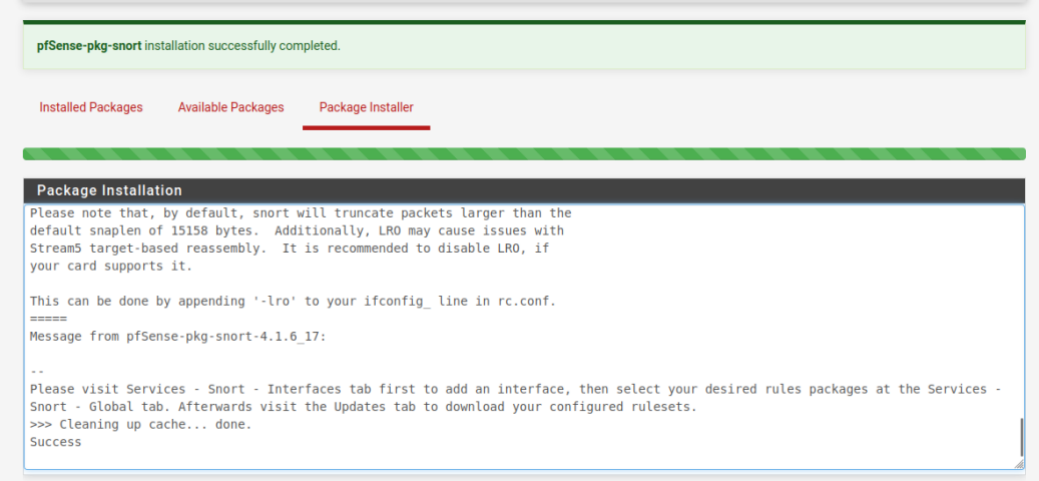
Passo 3 – Na caixa de pesquisa, procure pelo termo "snort":



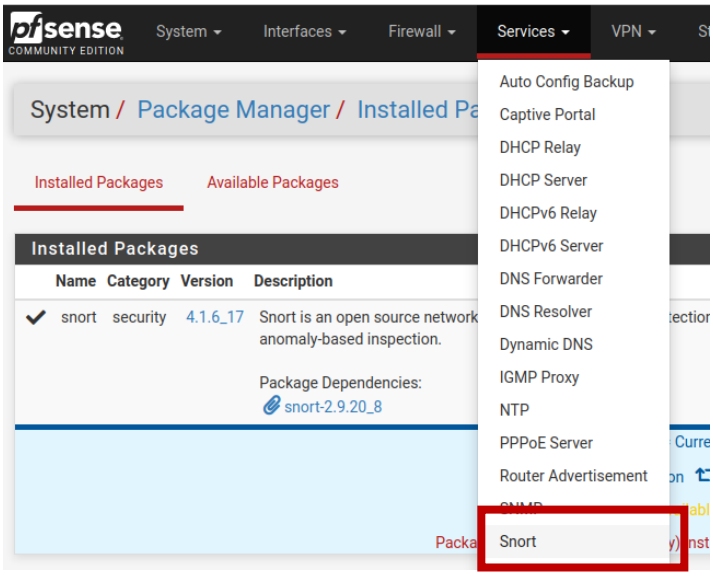
Passo 4 – Confirme o botão para continuar a instalação:



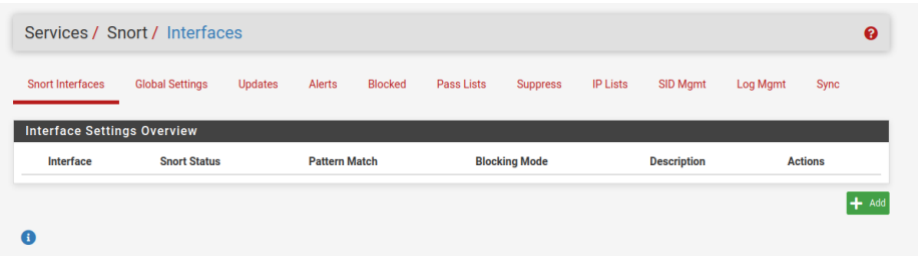
Passo 5 – Deve esperar que a instalação conclua todo o processo de instalação, e no final deverá aparecer a mensagem de sucesso:



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

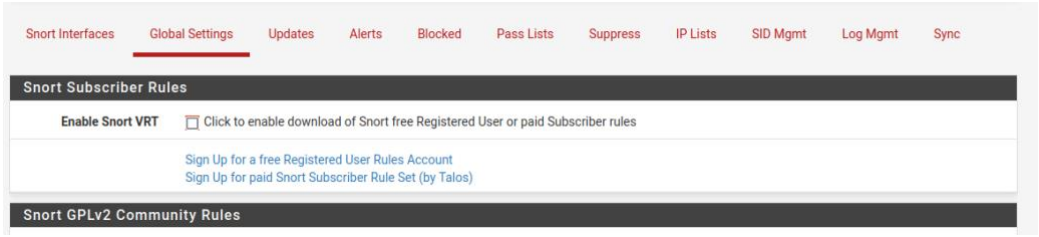


Quando abrir a nova janela, será exibida a informação das interfaces do Snort para realizar a configuração:



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 subescritores da plataforma (que tem as regras pagas).



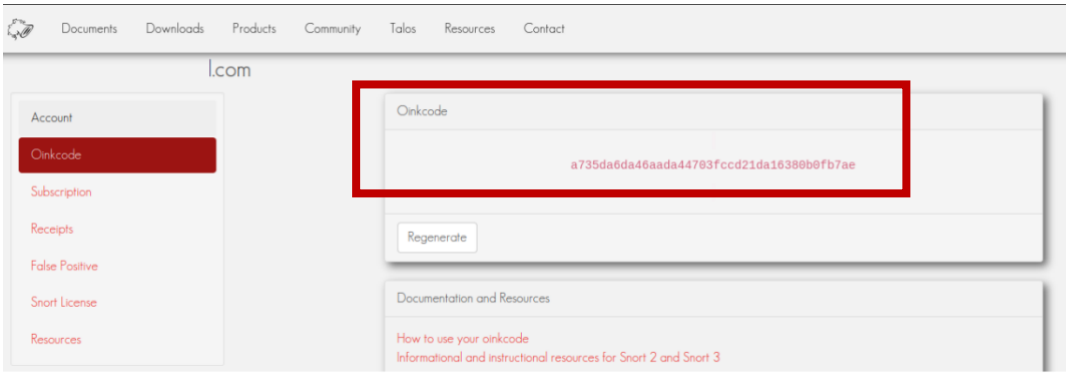
Ao ativar esta opção, temos de colocar o código de acesso ao serviço, conhecido como "**Snort Oinkmaster Code**" para autenticação dos utilizadores.

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.

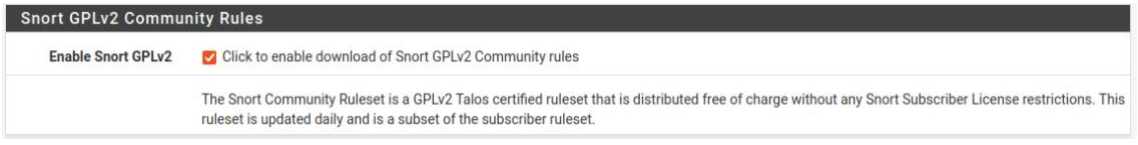
No pfSense, quando configuramos o pacote Snort, podes inserir esse Oinkcode em **Global Settings** para ativar:

- **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.

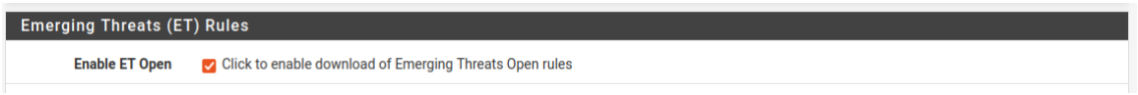
Faça o registo no portal do Snort e obtenha o OinkCode!



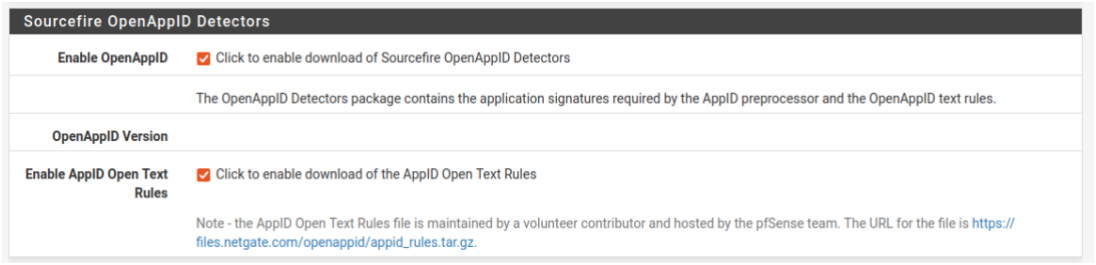
- **Enable Snort GPLv2:** permite fazer download das regras comunitárias dos servidores Snort (como falado mais acima).



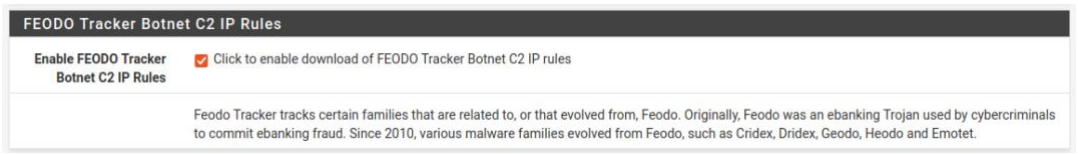
- **Enable ET Open:** permite ativar as prevenções contra ameaças externas;



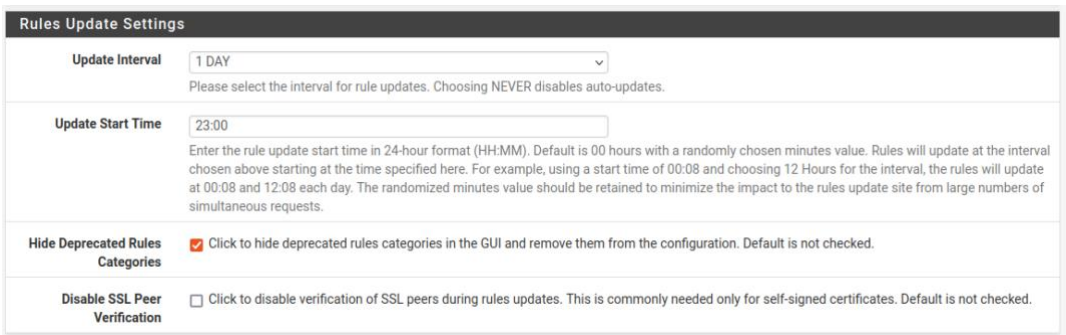
- Enable OpenAppID
  - **Enable AppID Open Text Rules:** permite ativar e verificar quais as aplicações que estão a utilizar;



- **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.

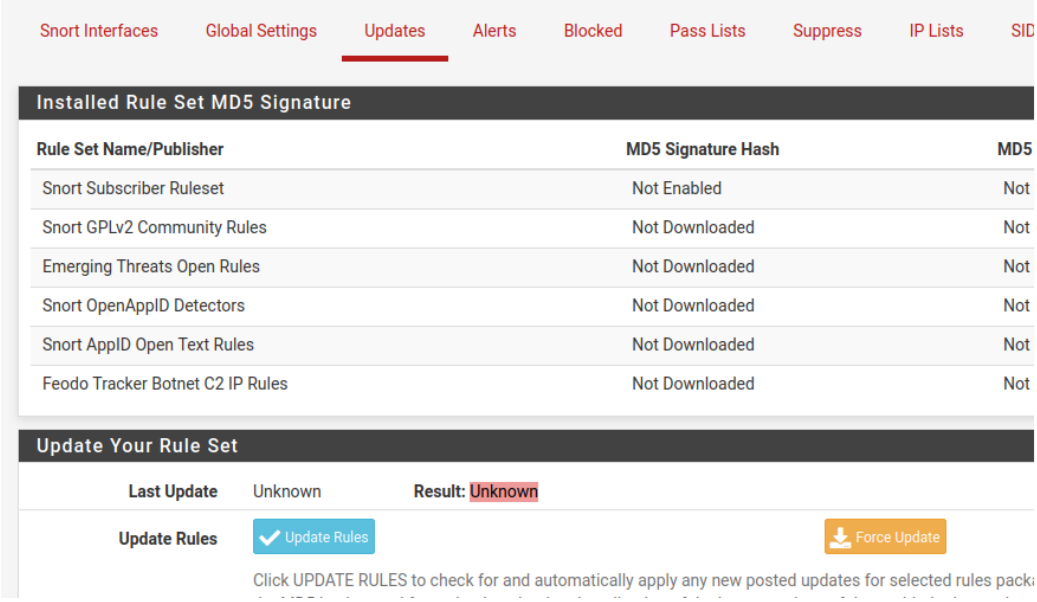


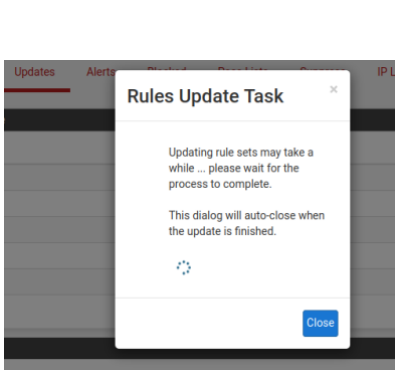
- Rules Update Interval
  - **Update Interval:** vai permitir fazer a atualização das regras em intervalos de tempo. Vamos configurar para atualizar as regras de 1 em 1 dia;
  - **Update Time:** indicar a que horas é que vai fazer a atualização das regras. Defina 23:00;
  - **Hide Deprecated Rules Categories:**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

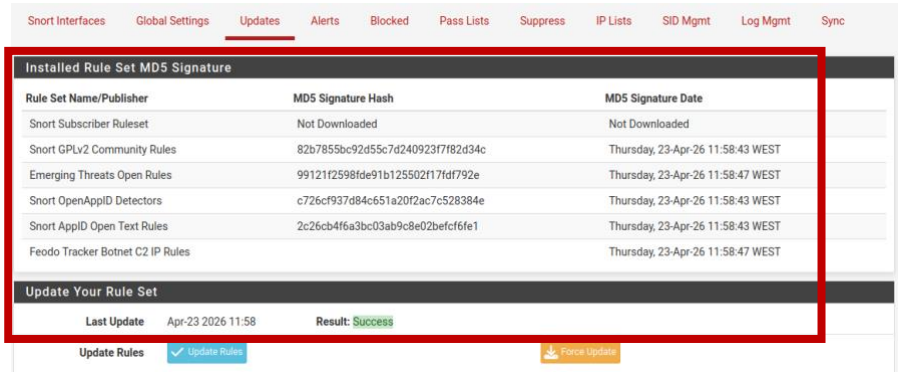


Passo 8 – Vamos selecionar o separador "Updates" e ativar as seguintes opções:

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

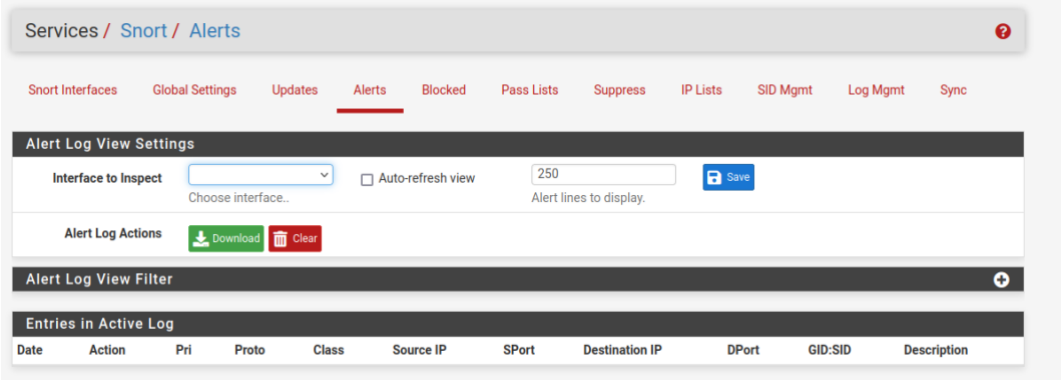




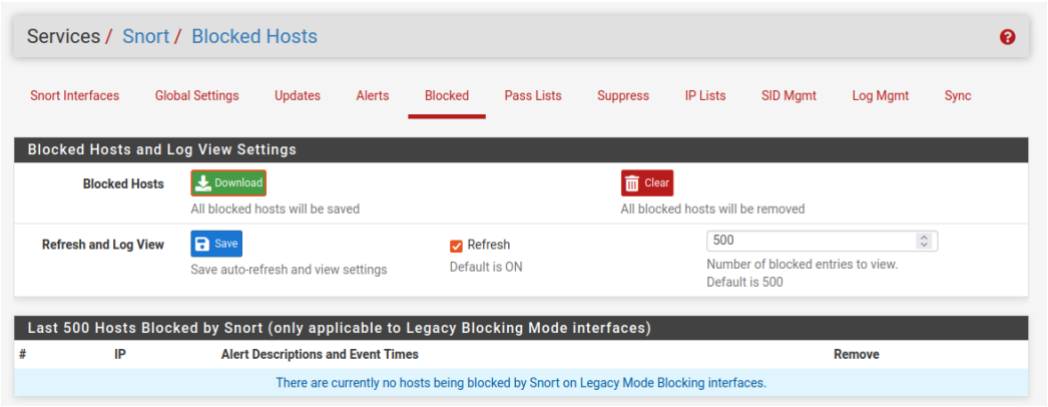


Vamos analisar os outros separadores:

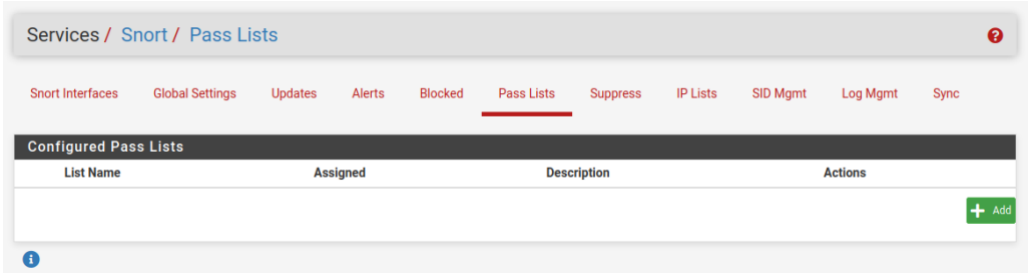
SNORT ALERTS



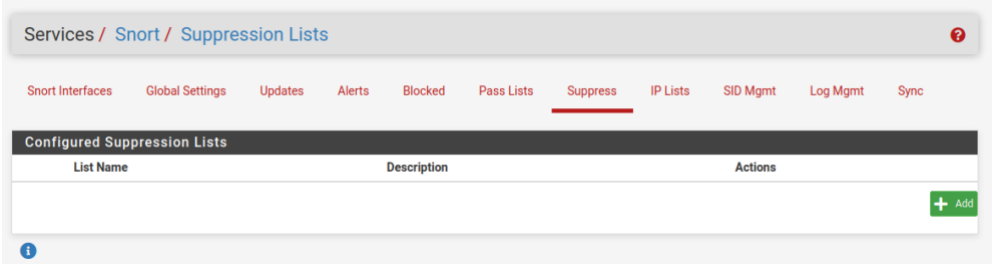
SNORT BLOCKED



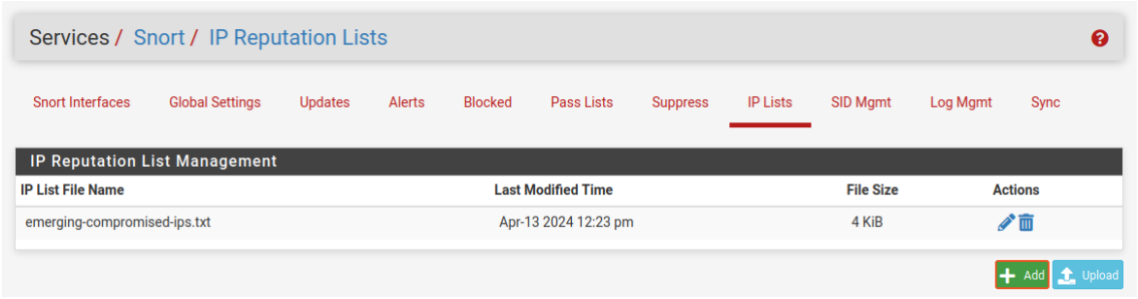
SNORT PASS LISTS



SNORT SUPRESS

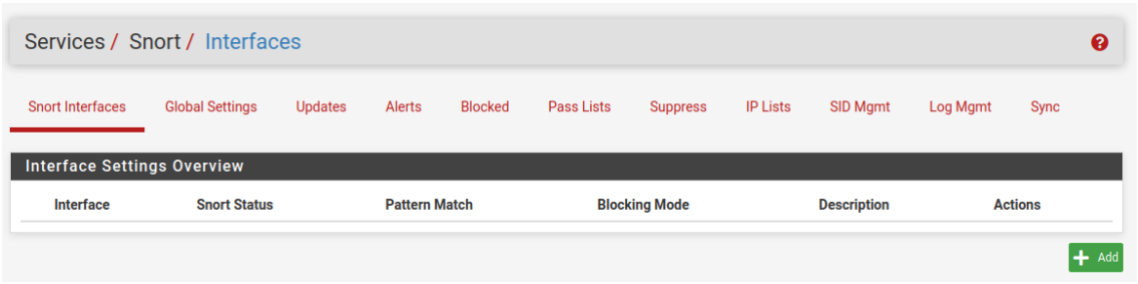


SNORT IP LISTS



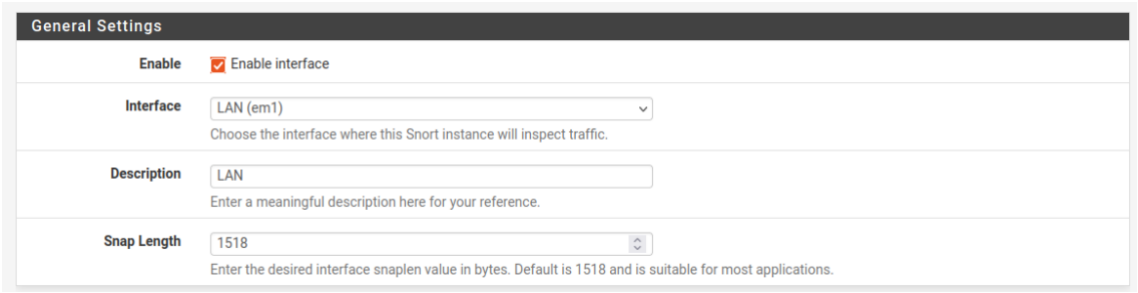
9.2 – Interfaces de captura Snort

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

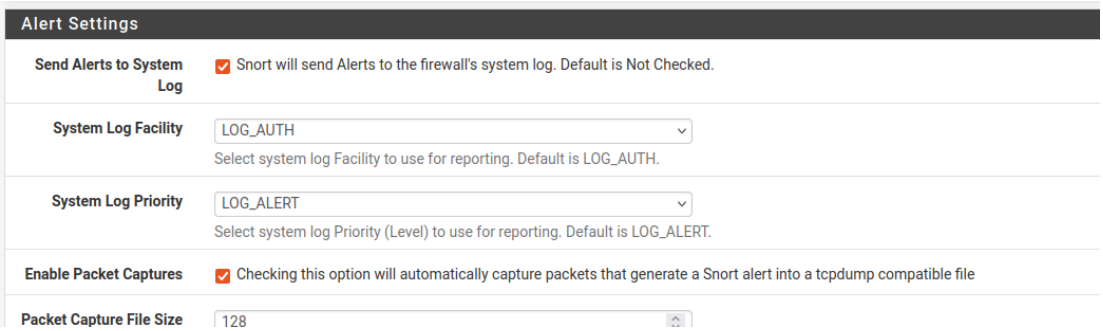


Definir interfaces (LAN Settings)

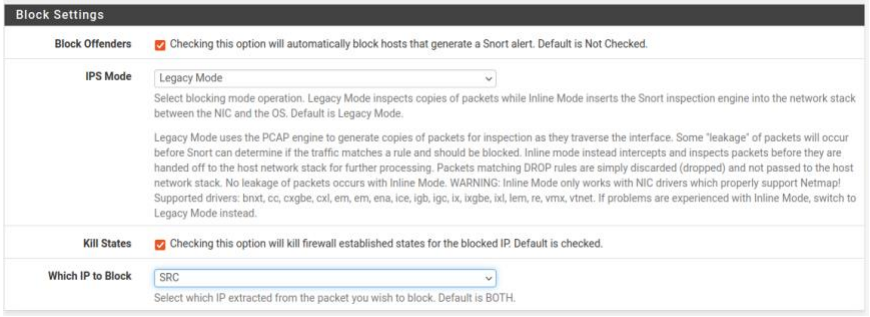
- Na interface, selecione a opção LAN (o campo da descrição muda automaticamente para o mesmo nome):



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



- Ativar a opção "Block Offenders"

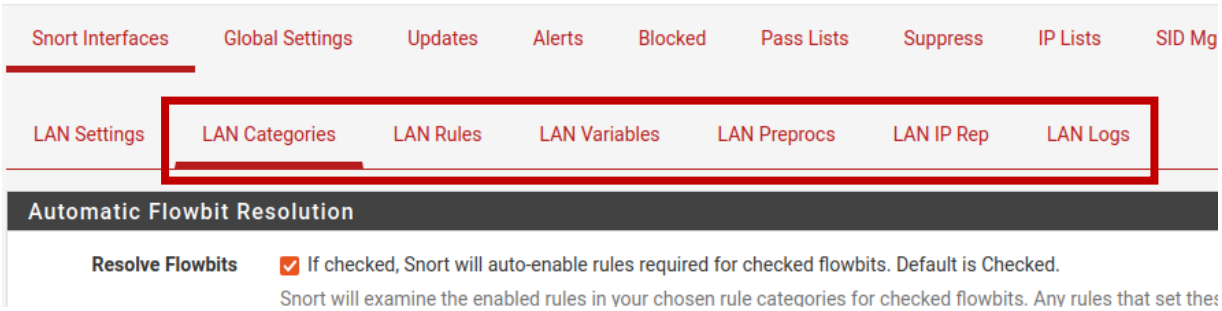


Muito importante: Na opção "**Which IP to Block**", vamos deixar a opção **BOTH**, bloqueando apenas a origem do tráfego de onde vem o ataque.

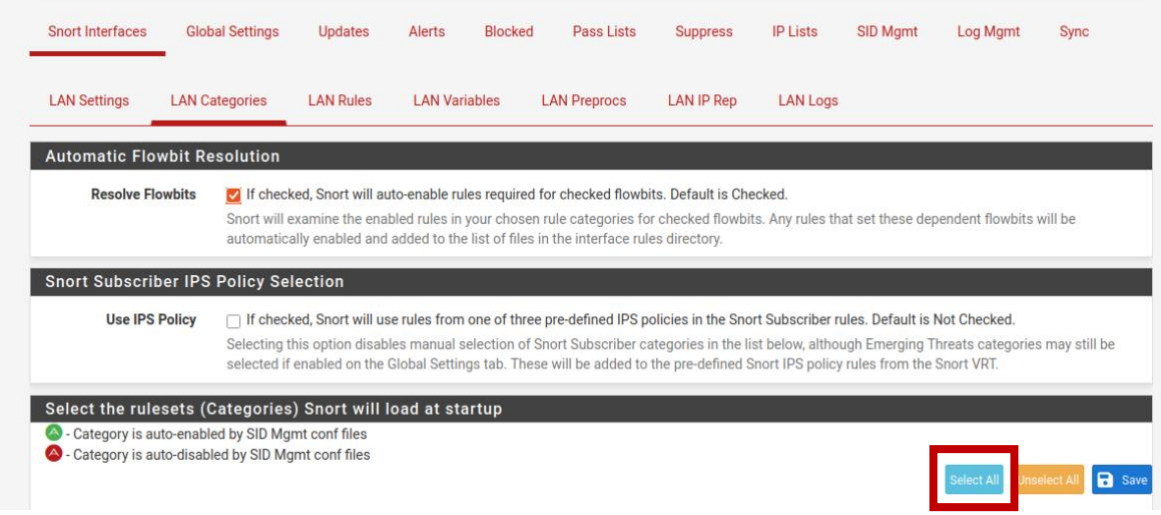
Se for selecionado BOTH, isto significa que, a origem do ataque e o destino vão ser bloqueados, se um hacker tentar entrar no vosso sistema e os destinos desejados pelo mesmo.

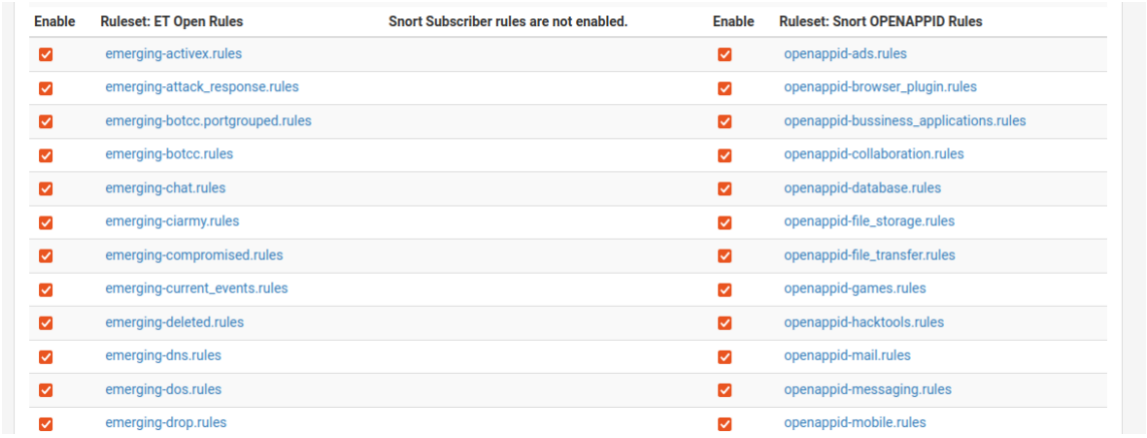
Categorias das interfaces (LAN Categories) e definição de regras

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

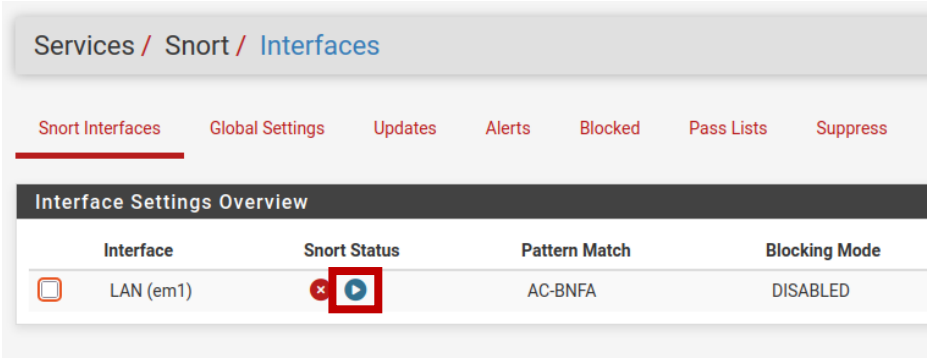


Neste ponto, vamos selecionar todas as regras que importou previamente, pois será uma mais-valia para a nossa análise (**mas não selecione a opção Use IPS Policy**):

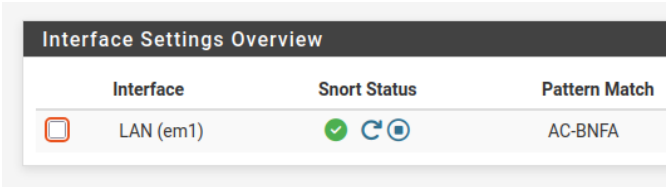




No final, deve ativar o serviço (pois ele está desativado), do qual deve clicar no botão azul (por debaixo do título "Snort Status" para arrancar a interface:



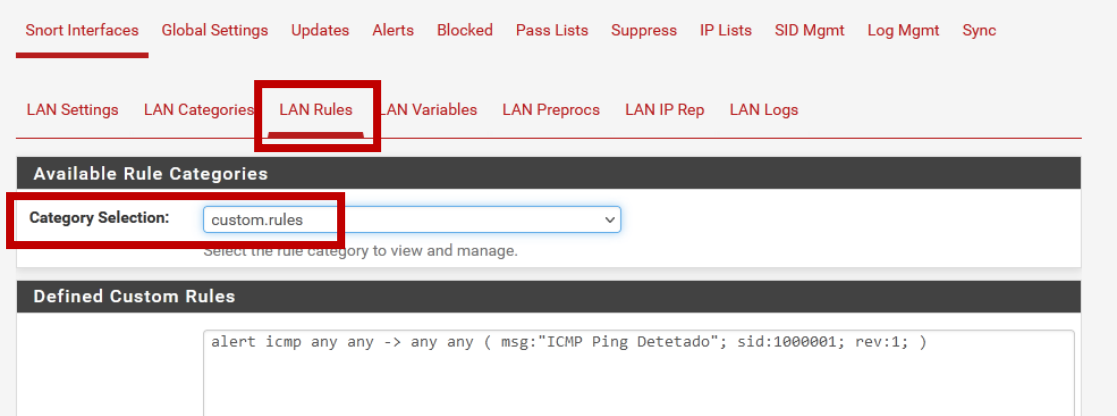
Quando o serviço ficar operacional, teremos a seguinte imagem com a confirmação:



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 especificas, vamos ter de selecionar o separador "**LAN Rules**";
- Na seção "**Available Rule Categories**" deve selecionar a opção "**custom.rules**";



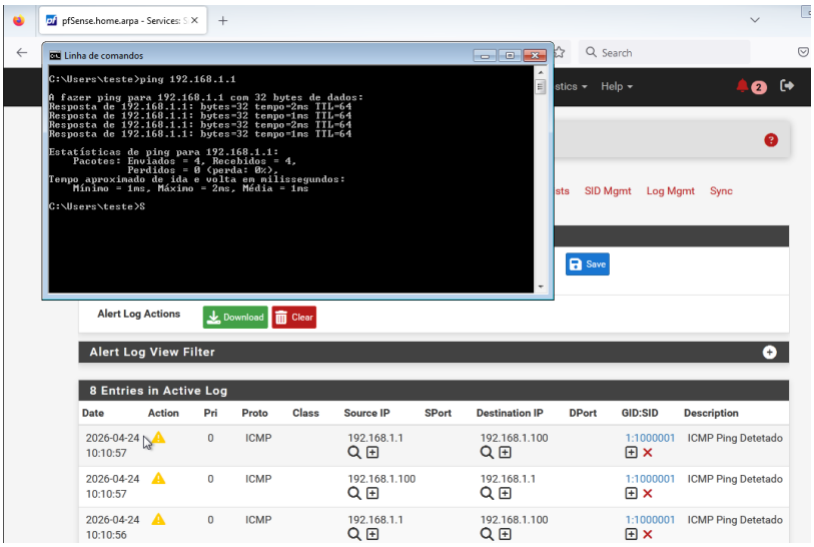
- **No final, deve gravar as novas alterações;**

1- Definir regras especificas 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;)

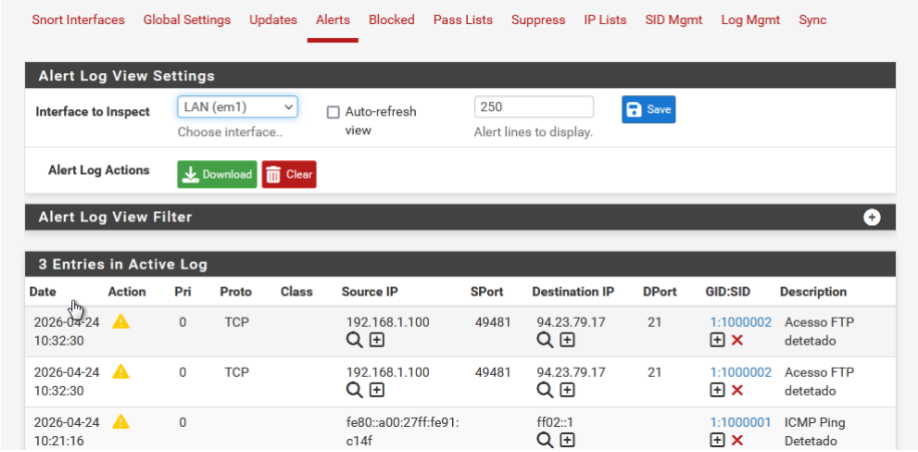
Grave as novas alterações e teste o alerta. Como tal, vamos a máquina virtual que esteja na rede LAN da firewall (netse caso o Windows 7) e fazemos ping para a firewall (ou pode ser para outro equipamento na rede):



Definir alertas para tentativa de acesso ao servidor FTP:

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

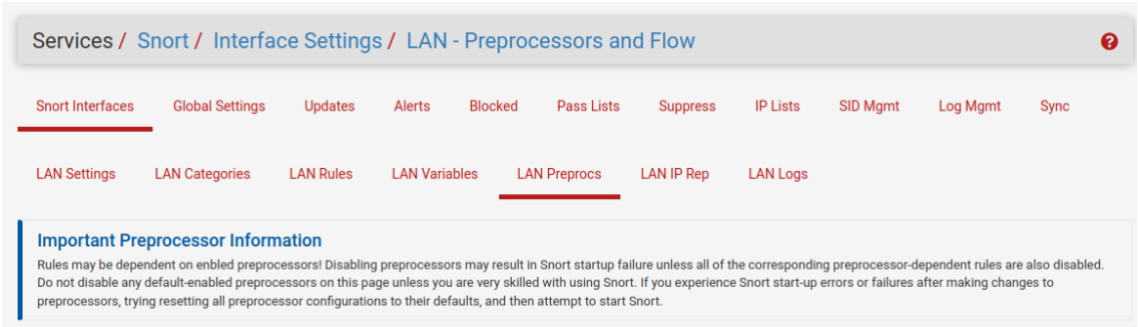
Grave as novas alterações e teste o alerta. Como tal, vamos utilizar o programa FileZilla para tentar ligar remotamente a uma máquina e ver a tentativa da ligação (mesmo sem efetuar a ligação com sucesso):



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 selecione a opção LAN Preprocs:

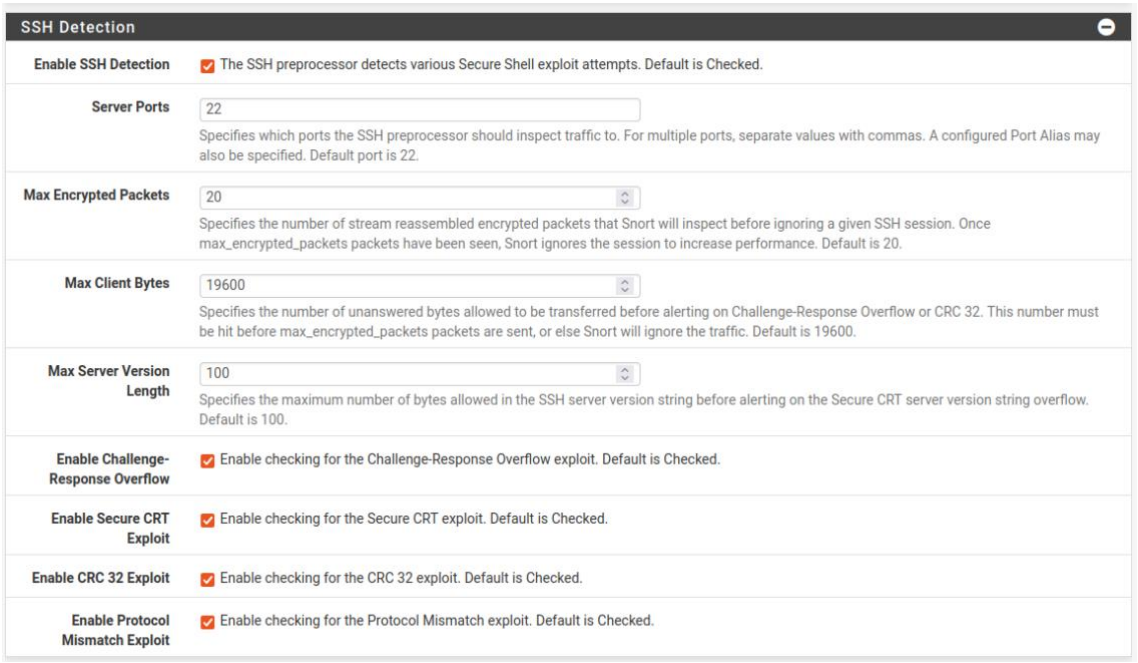


Deslize a janela para baixo até encontrar o separador (que está agrupado), com o nome "Portscan Detection" e clique no botão + que está no lado direito:

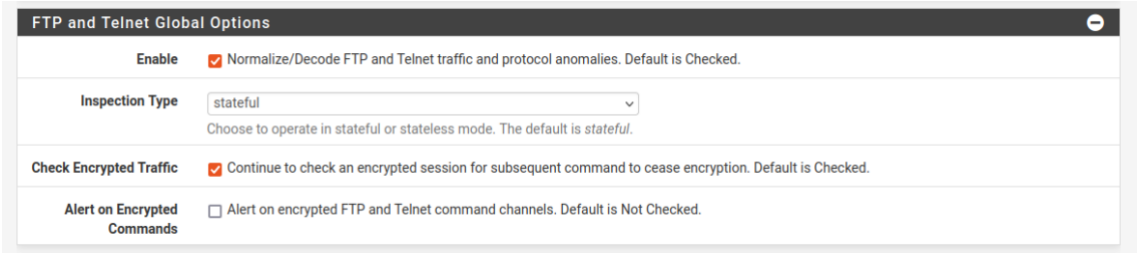
Procure pelo separador "SSH Detection" e:

*Verificar se a opção "*Enable SSH Detection" está ativada;

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

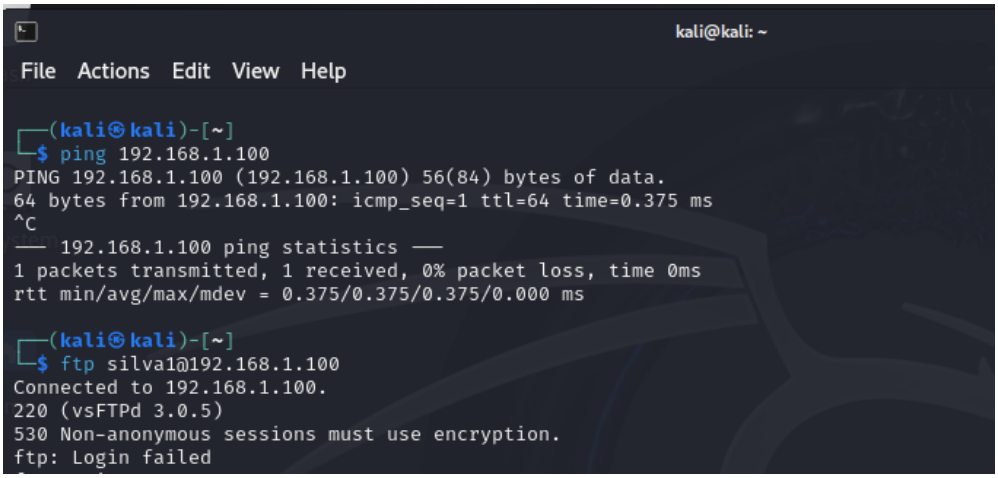


Por último, vamos abrir o separador "FTP and Telnet global options" e verificar se este grupo está ativo no enable:



Resultados:

Ping ICMP e conectar ftp

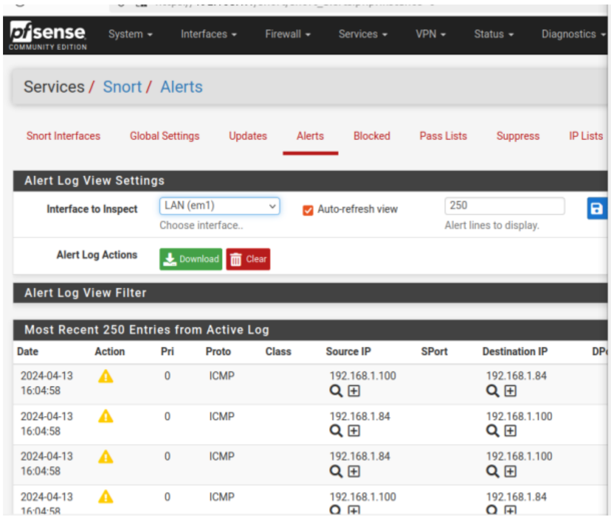


16 Entries in Active Log

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 15:32:06	⚠	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;)

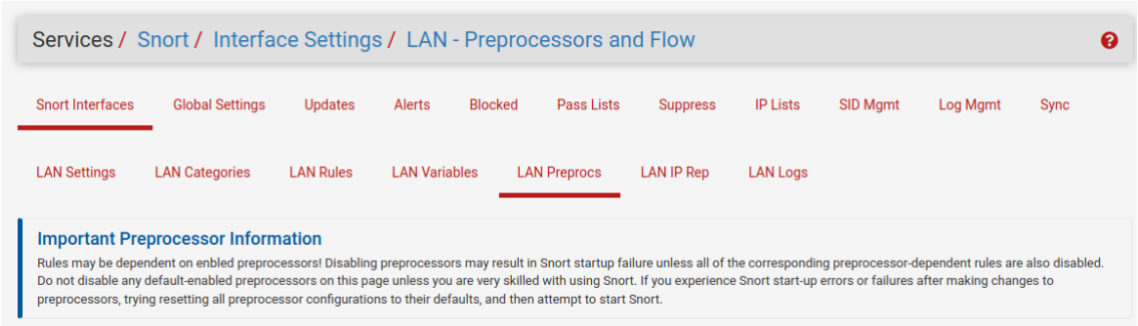


3 – Volte a colocar a primeira regra como alert:

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.

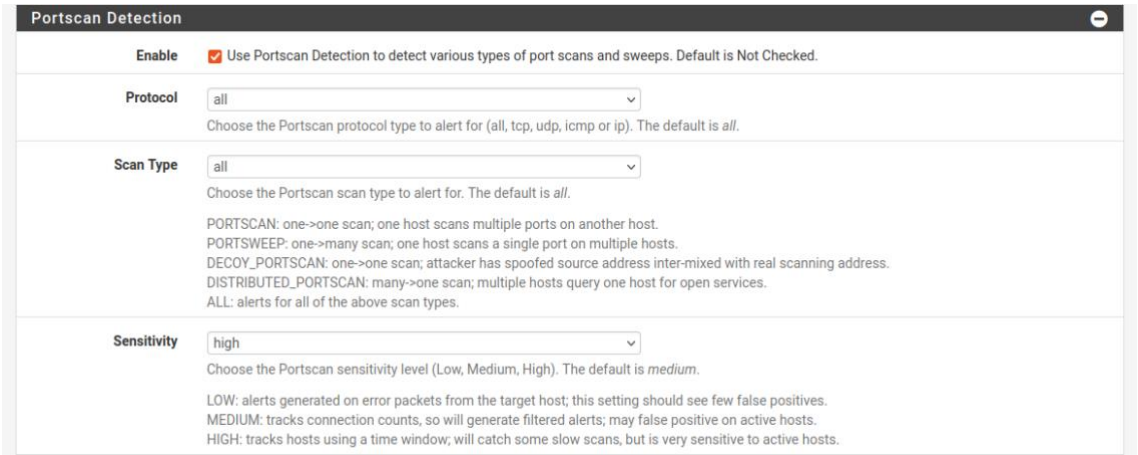
Volte a ir ao menu Snort Interface, edite as configurações dentro da interface que já está configurada e selecione a opção LAN Preprocs:



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:

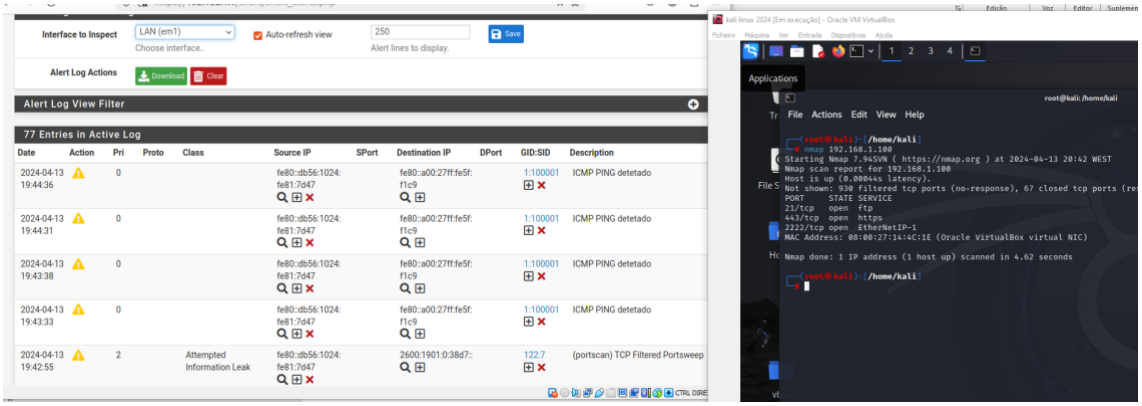
Dentro deste grupo:

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

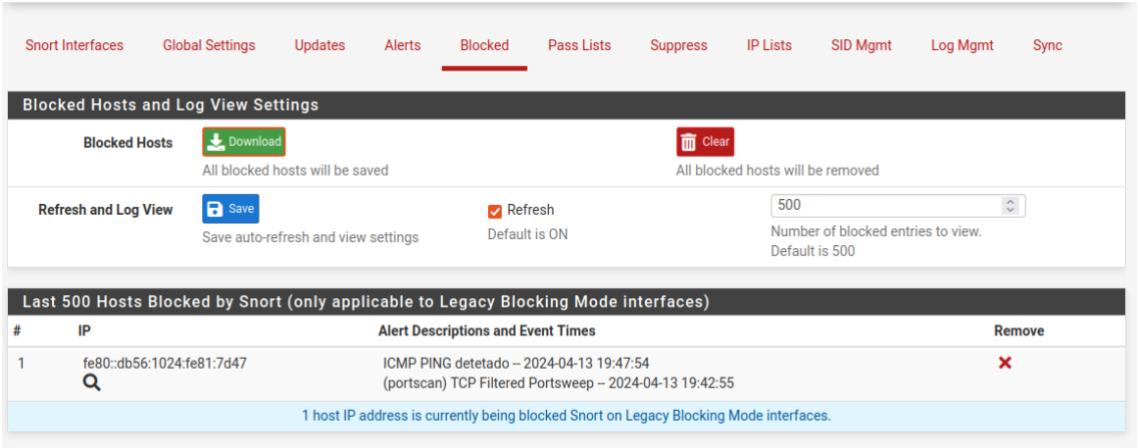


Volte a ir para a zona dos alerts do Snort e na máquina do atacante, faça o comando “nmap ip_da_vitima” (ex: nmap 192.168.1.100)

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



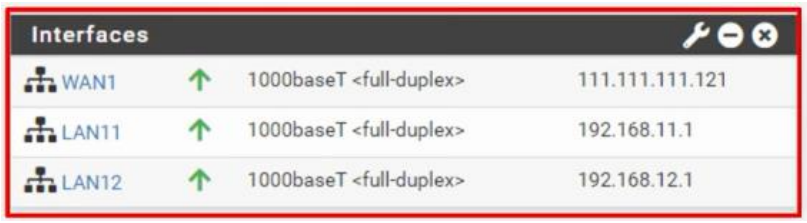
Como ativou as opções avançadas nas configurações para deteção máxima, o snort vai entender este tipo de ataque como malicioso e vai colocar o endereço como bloqueado, tal como demonstra a seguinte imagem do separador “Blocked”:



Parte 10 – Limitar velocidade dentro da firewall

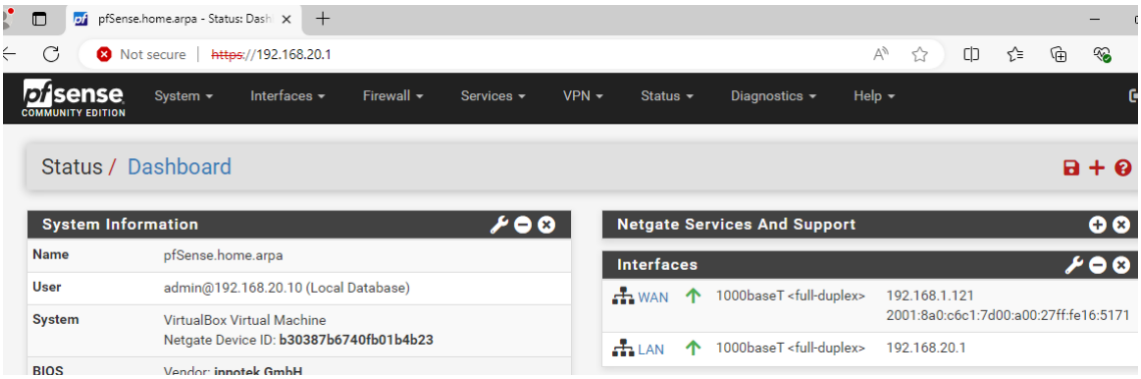
Imagine o seguinte cenário:

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 demostra a seguinte imagem:

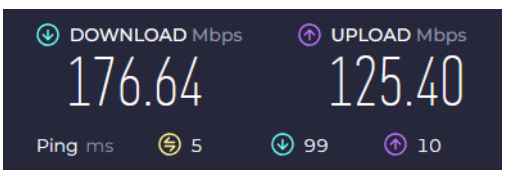


Como tal, podemos colocar limites no acesso a internet como uma norma de segurança adicional dentro da firewall.

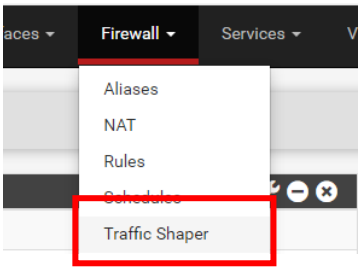
Como tal, vamos fazer os seguintes passos, mas neste caso prático, apenas vamos aplicar as regras numa rede LAN (com a máquina virtual da SEDE que temos trabalhado ao longo das fichas de trabalho):



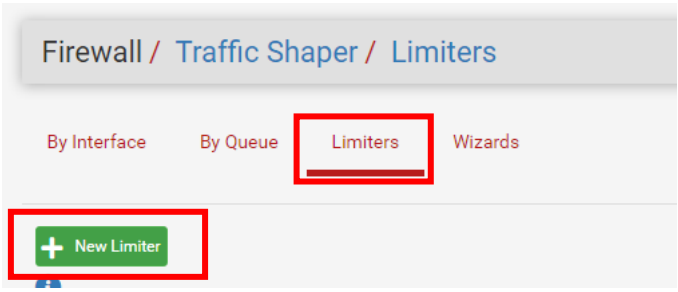
Suponha que estes são os valores da velocidade da sua Internet:



Passo 1 – Vamos até ao menu Firewall → Traffic Shaper

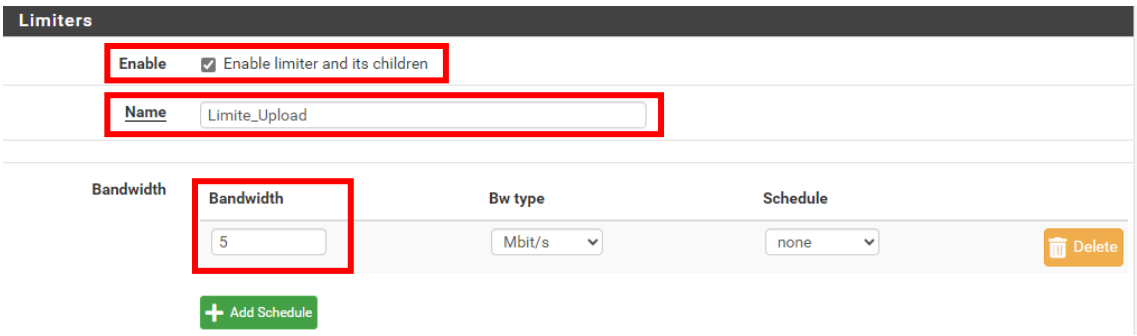


Passo 2 – Selecione o separador "Limiters" e depois carregue no botão New Limiter para adicionar uma nova limitação (neste passo apenas vamos dizer os parâmetros da configuração):



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

- **Enable**: ative esta opção
- **Name**: Limite_Upload
- **Brandwidth**: 5 (por defeito já vem Mbit/s)

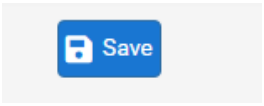


Passo 4 – No campo Mask, podemos escolher as opções "origem (source)" para definir que estamos a trabalhar o upload ou "destino (destiny)" para definir que estamos a trabalhar o download. Para tal, vamos:

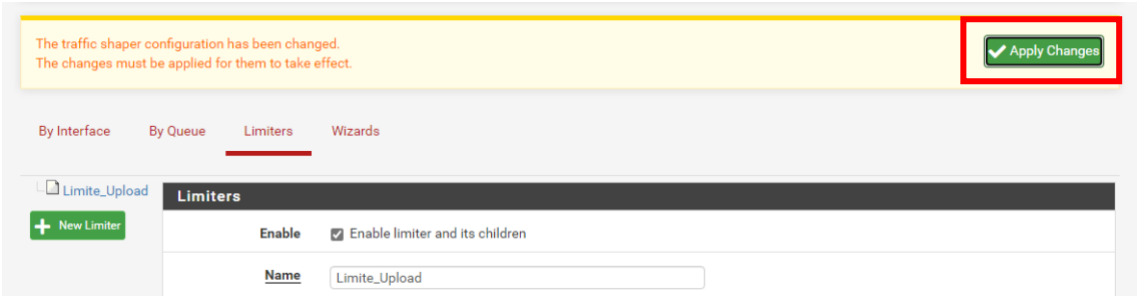
- **Mask**: selecionar a opção Source Address para indicar que quero trabalhar o Upload de dados;
  - Deixar os valores 32 e 128 para aplicar a regra em todos os hosts da LAN;

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

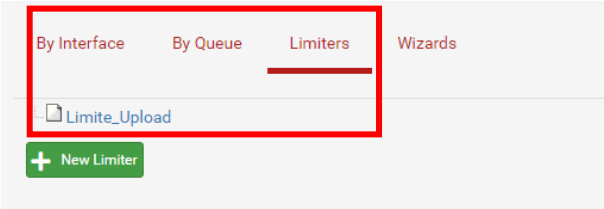
Passo 5 – Não esqueça de gravar as novas informações;



Passo 6 – Aplique as novas alterações:



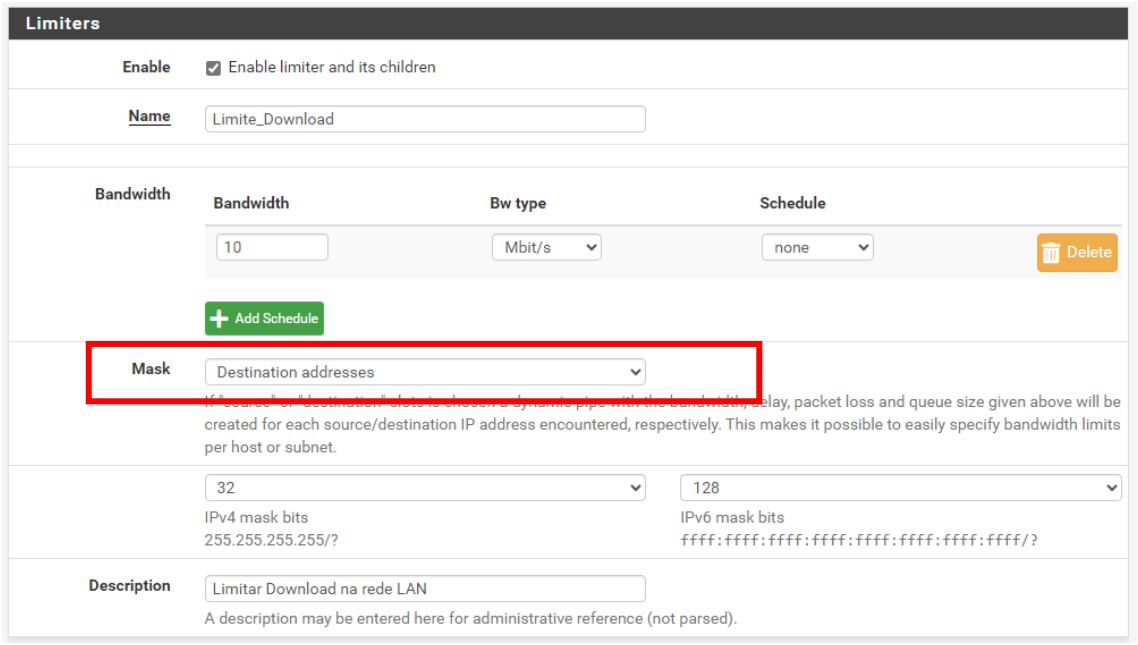
Resultado da criação do limite:



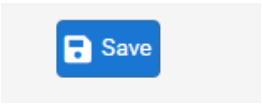
Passo 7 – Vamos fazer a mesma tarefa para o Download de ficheiros, mas com algumas modificações, em especial no campo Mask que ao contrário do Upload que usa Source Addresses o Dowload vai usar a opção Destination Addresses:

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

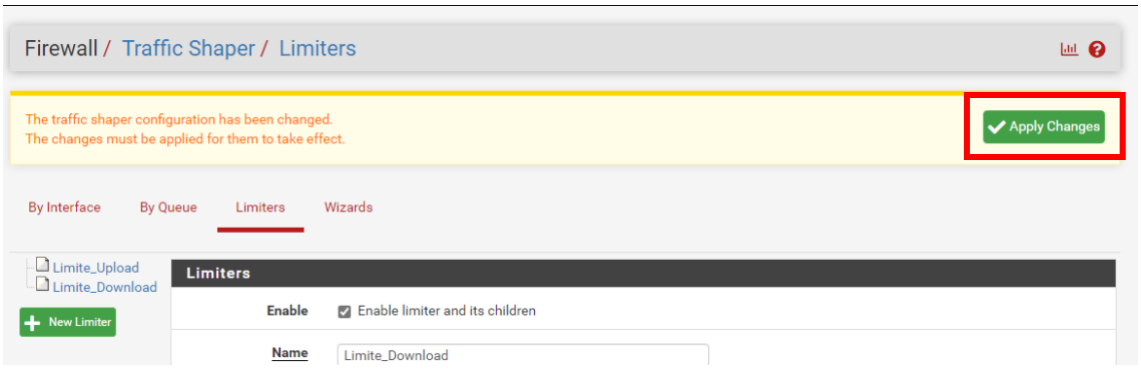
- **Enable**: ative esta opção
- **Name**: Limite_Download
- **Brandwidth**: 10 (por defeito já vem Mbit/s)
- **Mask**: selecionar a opção Destination Address para indicar que quero trabalhar o Download de dados;
    - Deixar os valores 32 e 128 para aplicar a regra em todos os hosts da LAN;
- **Description**: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



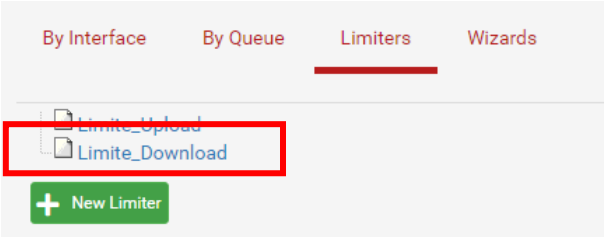
Passo 8 – Não esqueça de gravar as novas informações;



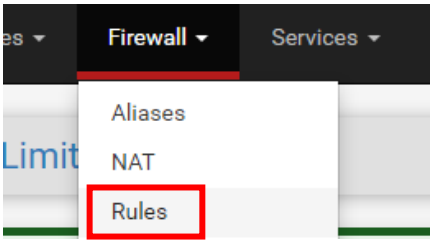
Passo 9 – Aplique as novas alterações:



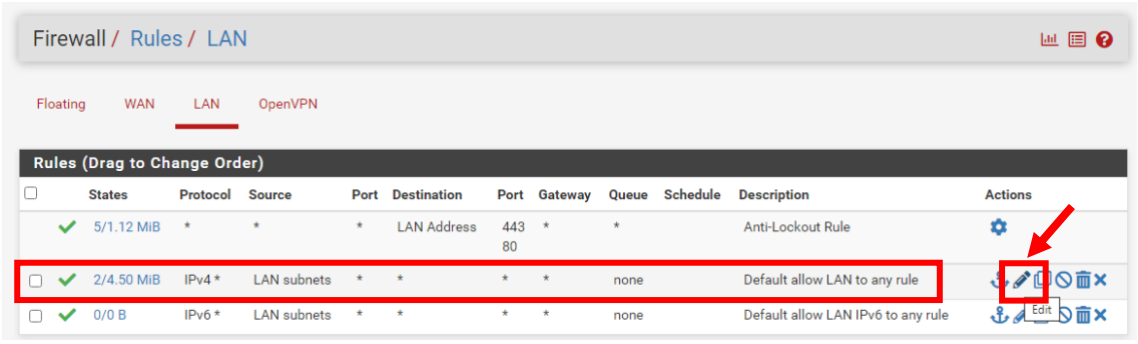
Resultado:



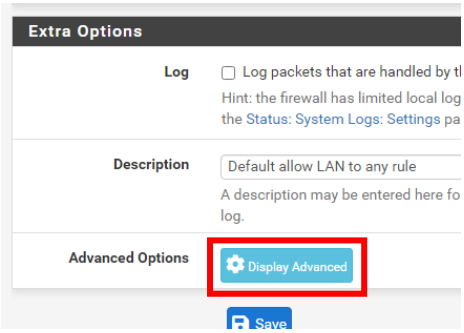
Passo 10 – No próximo passo, vamos associar a regra dos limites na rede LAN (pois apenas criamos as indicações, mas ainda falta associar as mesmas nas regras da firewall). Vamos ao menu **Firewall → Rules**:



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



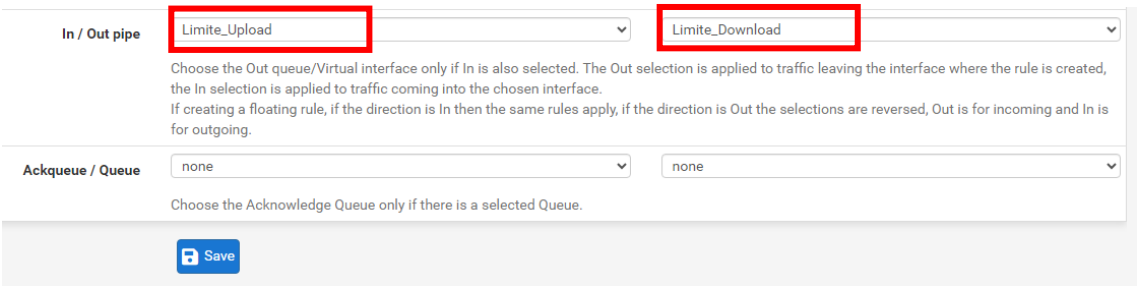
Dentro da regra, deve ir ao fundo da página e clicar no botão **Display Advanced** para aceder as propriedades avançadas das configurações da regra:



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:

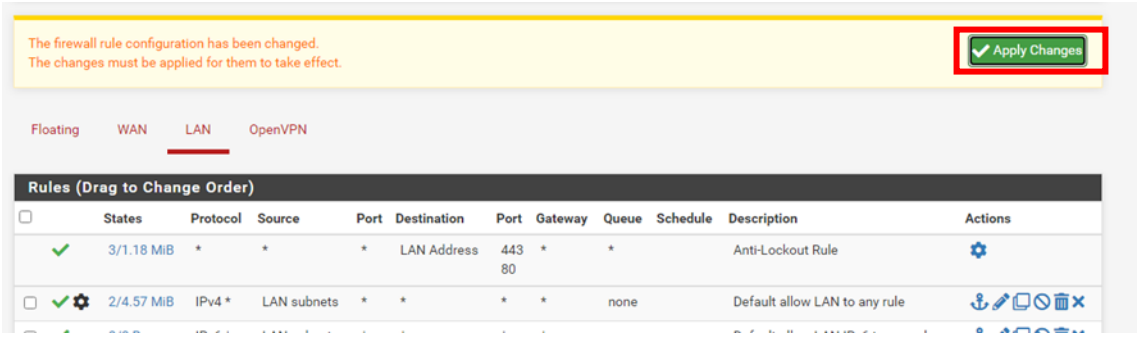
- 1º Campo → Colocar o limitador "Limite Upload"
- 2º Campo → Colocar o limitador "Limite Download"

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

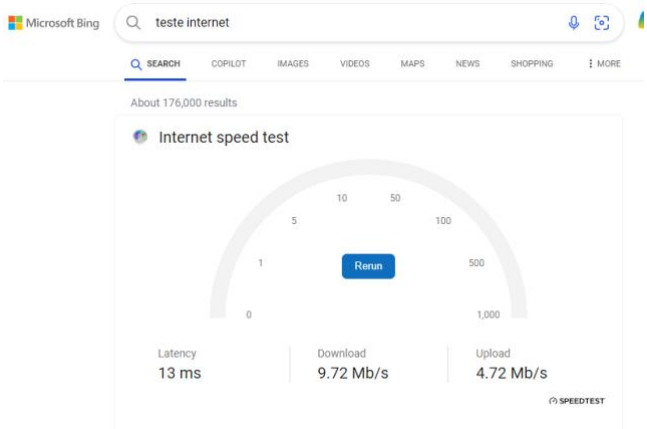


Não esquecer de gravar as novas alterações.

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



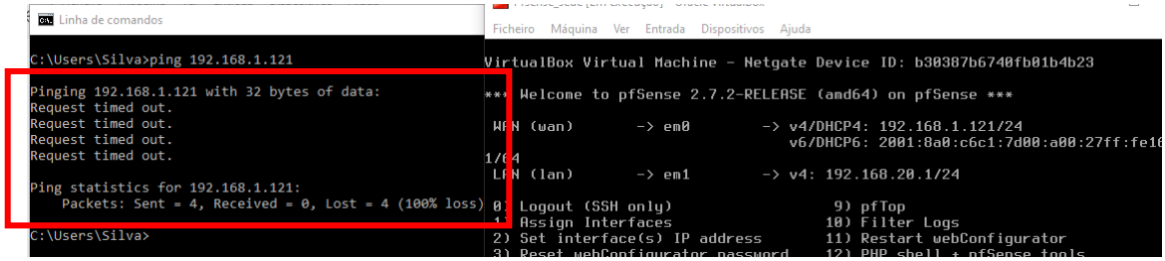
Passo 12 – Teste a ligação da LAN na máquina virtual (que esteja ligada na rede LAN):



Permitir ping na rede WAN

De notar que, por defeito a firewall do PFsense bloqueia rodos os pacotes "ping", incluídos protocolos ICMP, por razoes 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.

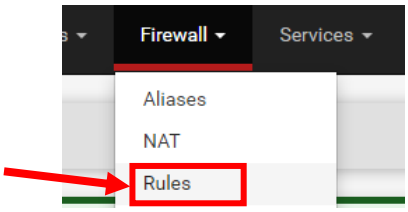
Passo 1 – Abra uma linha de comandos (cmd) e faça ping na firewall da sede (neste exemplo o IP é o 192.168.1.121):



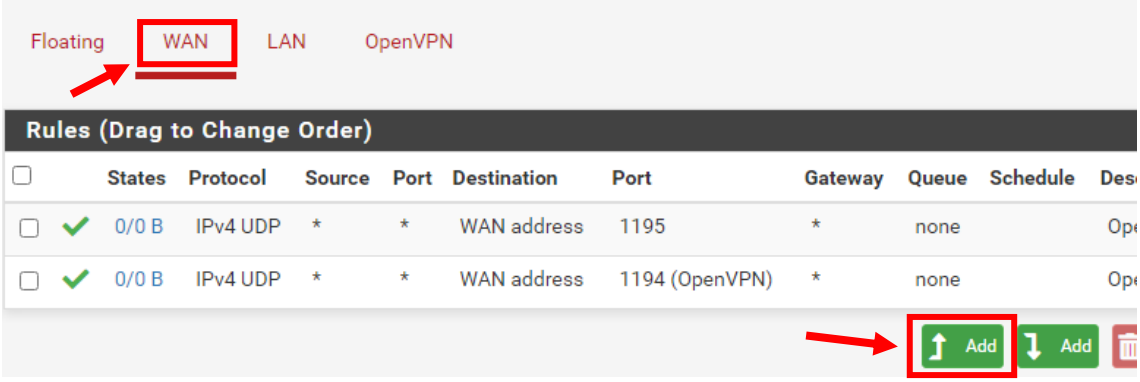
Repare que a resposta foi negativa e os pacotes não obtiveram qualquer resposta!

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

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

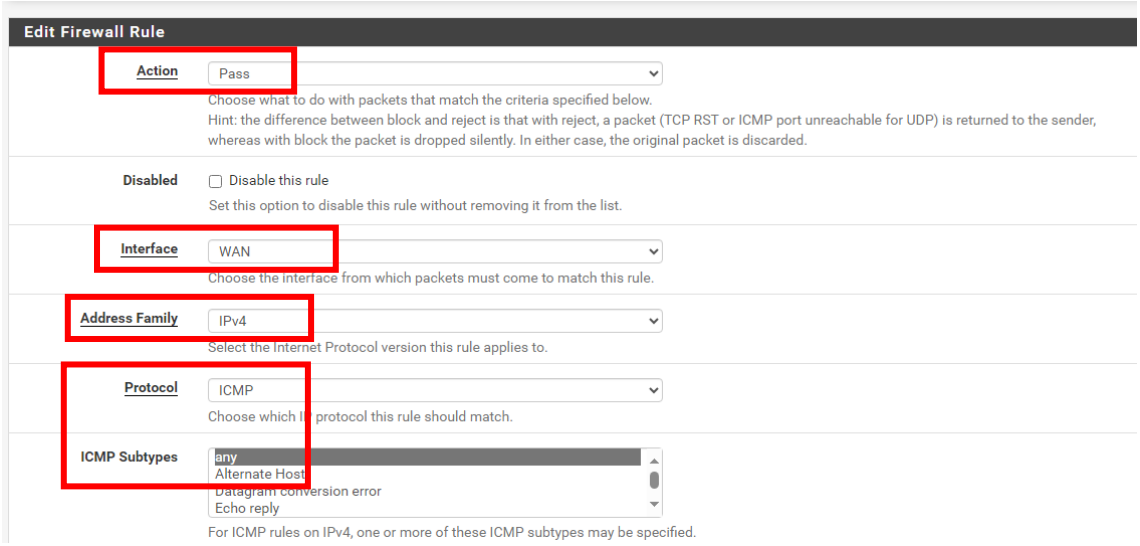


Passo 2 – Selecione o separador WAN e clique no botão ADD para adicionar nova regra:



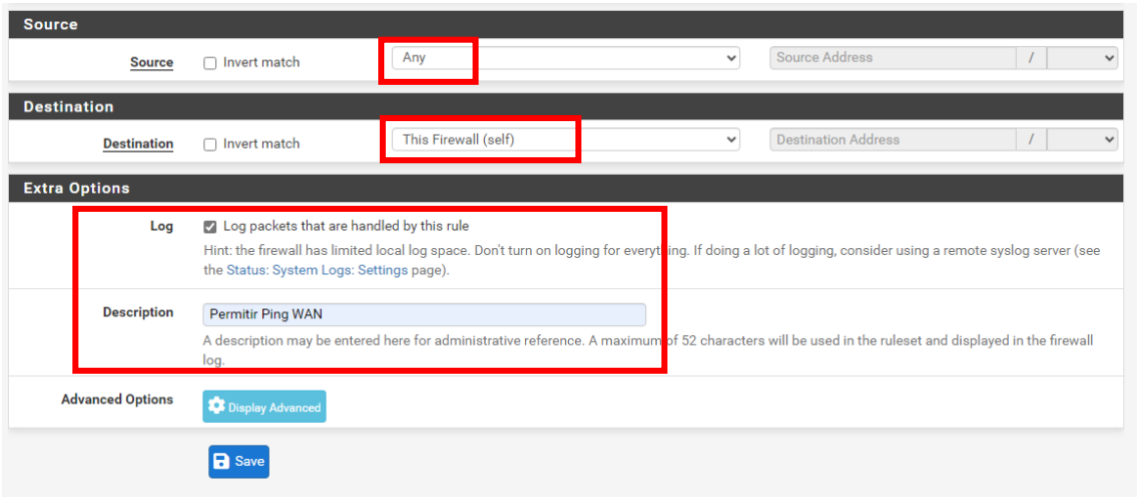
Passo 3 – Coloque as seguintes opções:

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



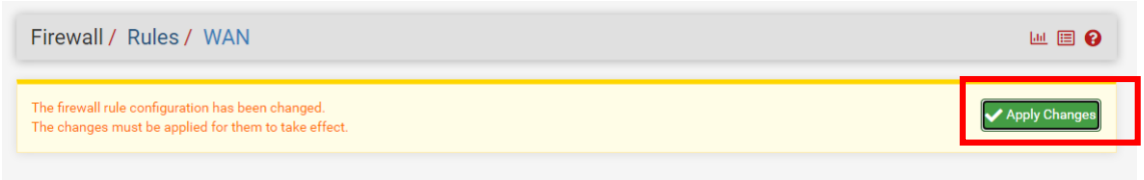
Passo 4 – Nas próximas seções deve fazer as seguintes ações:

- 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";



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: