INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

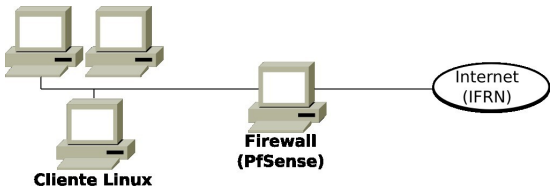
Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 11: Firewall com PfSense

Olá turma, na aula de hoje iremos compreender o papel de um firewall na segurança de redes, entender as funcionalidades do pfSense como firewall, realizar a instalação e configuração básica do pfSense e Criar regras de firewall para controlar o tráfego de rede interna. Vamos lá? Preparados?

Configurando o Ambiente

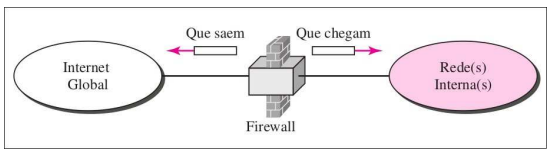
Para estudarmos estes conceitos e ferramentas iremos utilizar duas máquinas virtuais. Uma será a máquina com Firewall (PfSense) e outra máquina de teste com Kali Linux (cliente interno) para testarmos as as configurações.

A máquina Firewall deverá ter duas placas de Rede (uma em NAT e outra em Rede Interna). A máquina Kali com uma placa de rede em modo Rede Interna.



Firewall

O firewall é um dos principais mecanismos de segurança utilizados em redes de computadores. Seu principal objetivo é proteger redes e sistemas contra acessos não autorizados, ataques cibernéticos e tráfego indesejado, ao mesmo tempo que permite o tráfego legítimo e necessário. Em outras palavras, ele funciona como uma barreira entre redes, controlando o tráfego de entrada e saída com base em regras de segurança definidas pelo administrador.



Um firewall monitora e filtra pacotes de dados que trafegam entre redes, como a rede local (LAN) e a internet (WAN). Ele verifica informações como:

- Endereço IP de origem e destino;
- Portas de origem e destino;
- Protocolo utilizado (TCP, UDP, ICMP, etc.);
- Estado da conexão (nova, estabelecida, inválida).

e com base nessas informações, o firewall decide se o pacote deve ser permitido (*allow/pass*) ou bloqueado (*deny/block*).

Além de bloquear ou permitir pacotes, o firewall pode desempenhar as seguintes funções:

- NAT (Network Address Translation): oculta IPs internos, permitindo que uma rede privada acesse a internet.
- Port Forwarding: redireciona acessos externos para serviços específicos dentro da rede interna.
- VPN Pass-through: permite tráfego de redes privadas virtuais (VPNs).
- Registros e Logs: mantém histórico dos acessos permitidos e bloqueados.

Existem diversos tipos de firewall, classificados de acordo com seu modo de operação e sua posição na rede, os principais são:

- Filtro de Pacotes (Packet Filtering): ele analisa pacotes individualmente e toma decisões baseiado em regras simples de IP, porta e protocolo. Ele é rápido, mas com pouca capacidade de inspeção.
- Inspeção de Estado (Stateful Inspection): mantém registro das conexões ativas, permitindo decisões com base no estado da conexão (ex: permitir apenas pacotes de resposta). Ele é mais seguro que o filtro de pacotes simples.

- Aplicação (Application Layer Firewall): opera na camada 7 do modelo OSI, ta,também chamado de firewall proxy. Ele inspeciona o conteúdo dos pacotes na camada de aplicação (ex: bloqueio de palavras-chave em e-mails ou URLs específicas).

- Pessoal: instalado em computadores individuais, controlando o tráfego de rede do próprio sistema. A maioria dos sistemas operacionais atualmente possuem firewall pessoal, tais como Windows e Linux.

PfSense

O pfSense é um sistema operacional de código aberto baseado no FreeBSD, amplamente utilizado como firewall e roteador. Ele é administrado pela empresa Netgate. O pfSense possui vários pacotes de software livre para estender suas funcionalidades, tais como Snort e Suricata para detecção e prevenção de intrusão, OpenBGPD, Squid com cache e proxy reverso com SquidGuard, antivírus com ClamWin, além de vários outros pacotes de monitoramento e estatísticas.

Existem duas versões do PfSense são elas: CE (Community Edition) e pfSense Plus. Utilizaremos a versão CE do pfSense, voltada para a comunidade de usuários, com todos os recursos essenciais disponíveis sem custo.

O pfSense CE é gratuito com código fonte abeto e pode ser instalado em um computador comum, em um servidor ou até em uma máquina virtual. Depois de instalado, a configuração é feita através de uma interface web acessível por um navegador. Ele oferece recursos profissionais mesmo em ambientes de baixo custo, sendo ideal para escolas, empresas, órgãos públicos ou laboratórios de estudo.

A ISO de instalação poderá ser obtida no link: `https://www.pfsense.org/download`.

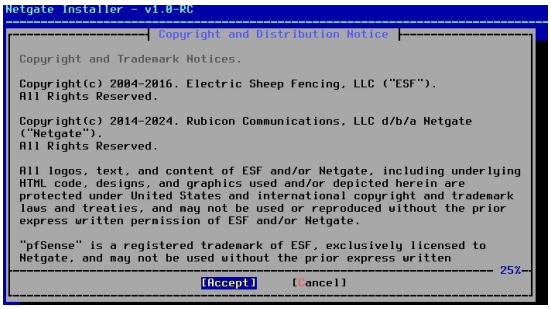
Instalação

1. Inicie o VirtualBox e crie uma nova máquina virtual com as seguintes características:

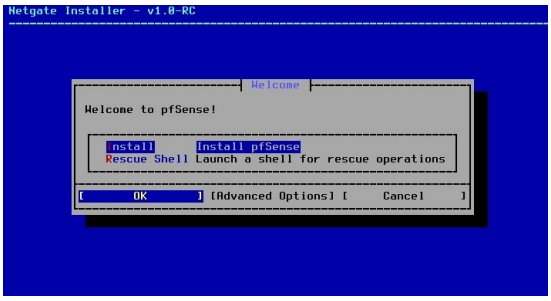
- Tamanho da memória : 2048MB
- Duas placas de Rede: NAT e Rede Interna;
- Tipo do SO: BSD;
- Versão do SO: FreeBSD 64 bits.

2. Monte a ISO de instalação e inicialize a máquina virtual.

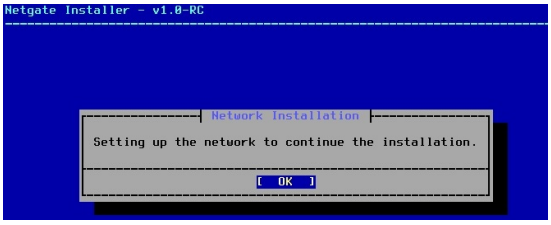
3. Após terminar todo processo de "boot" a primeira tela de opções de instalação será apresentada uma tela relacionada aos direitos autorais. Selecione a opção "Accept".



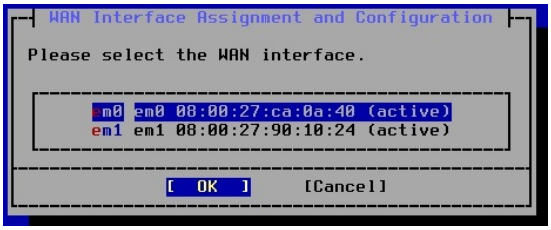
4. Na tela de Boas Vindas, selecione "Install" para instalar o sistema na máquina virtual, e clique em "Ok".



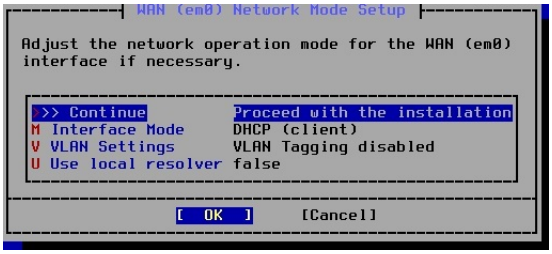
5. Será informado que as placas de redes serão consfigurada, clique em "Ok".



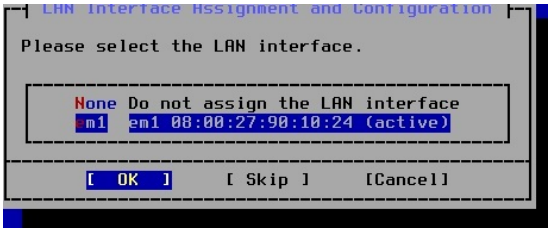
6. Selecione a placa de rede da interface WAN. Para isso, verifique o endereço das placas de rede no VirtualBox.



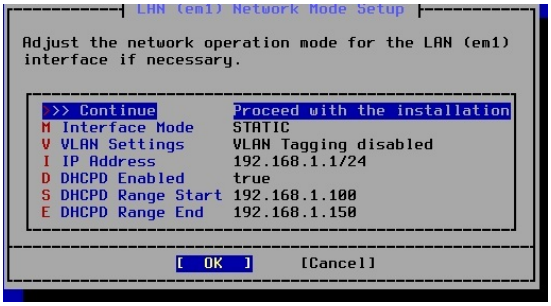
7. A nossa interface WAN deverá ser configurada por DHCP, sem VLAN e sem servidor DNS local. Deixe as opções padrões e clique em “Ok”.



8. Na sequência será questionado a respeito da interface LAN. Selecione a mesma e clique em “Ok”.

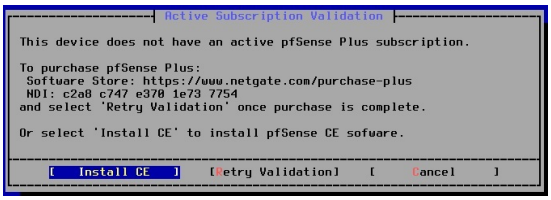


9. A nossa interface LAN será configurada de forma estática com o endereço IP 192.168.1.1/24 e com servidor DHCP da LAN ativado. Pode deixar as configurações padrões e clique em “Ok”.



10. Na sequência será solicitado que você confirme as interfaces. clique em “Continue”.

11. Selecione a versão gratuita CE, selecionando “Install CE”.



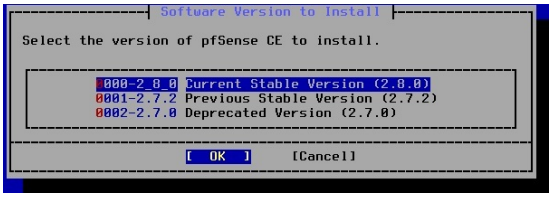
12. Quando questionado sobre o sistema de arquivos, pode selecione “Proceed with the installation” para utilizar a configuração padrão e “Ok”.

13. Na sequência será informado que o sistema de arquivo será o ZFS sem redundância. Clique em “Ok” para dar andamento.

14. Na próxima tela, será mostrado o disco que será instalado o sistema. Clique em “Ok”.

15. Será informado que o disco será apagado para criar o sistema de arquivos e copiar os sistema. Selecione “Yes” para dar andamento.

16. na sequência será mostrado as versões do PfSense CE disponíveis para instalação. Selecione “Current Stable” e em “Ok”.



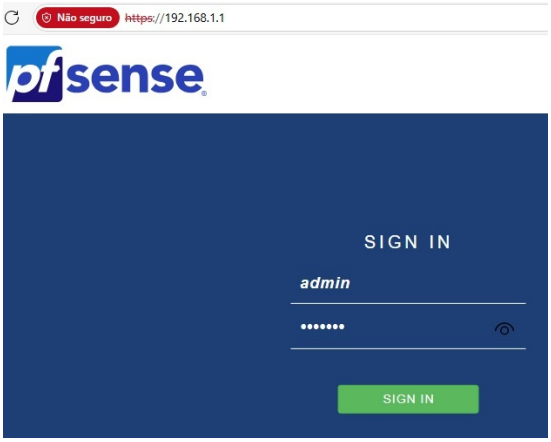
17. Agora será instalado o sistema. Após um tempo será solicitado a reinicialização da máquina virtual. Entretanto, antes de reinicar é preciso remover a imagem de instalação, caso contrário, o pfSense será inicializado na rotina de instalação novamente.

18. Depois da reinicialização, o pfSense será inicializado em sua nova instalação. A primeira inicialização demora um pouco, mas depois ele apresenta um terminal com informações e um menu para interagir por terminal com o firewall.

Configurando o PfSense

Realizada a instalação iremos configurar o nosso firewall. Para isso, precisaremos utilizar uma outra máquina virtual (cliente Linux com o Kali) com interface de rede na “Rede interna”.

19. No navegador digite o endereço IP 192.168.1.1. No primeiro acesso será exibido uma mensagem alertando que a conexão não é segura, desconsidere a mensagem e clique para adicionar uma exceção de segurança.

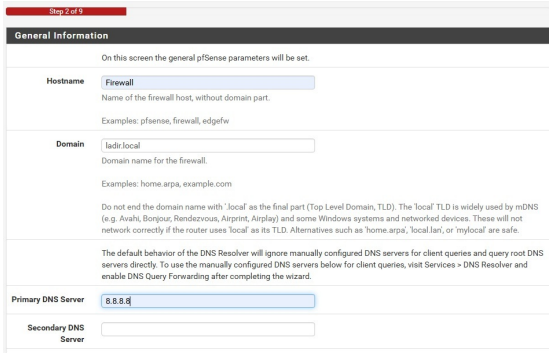


20. Utilize o usuário: **admin** e senha: **pfsense**

21. Em seguida, surgirá uma tela de boas vindas do assistente de configuração do “pfSense” apenas clique em “Next” para prosseguir.

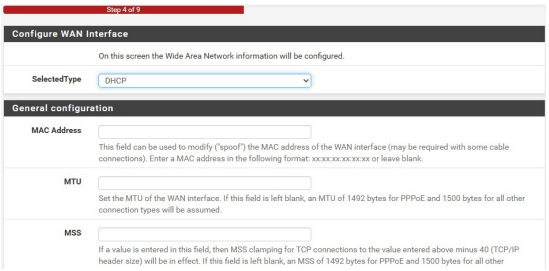
22. Será apresentado uma oferta para assinar o serviço “pfSense Gold” que fornece alguns benefícios como backup na nuvem, o E-book , acesso a videoconferências, entre outros. Clique em “Next”.

23. Na sequência, será solicitado que você informe parâmetros gerais do firewall. Insira os dados: hostname = Firewall, domínio = ladir.local, Servidor DNS = 8.8.8.8 e pode deixar marcada a opções de “Override DNS”. Por último clique em “Next”.

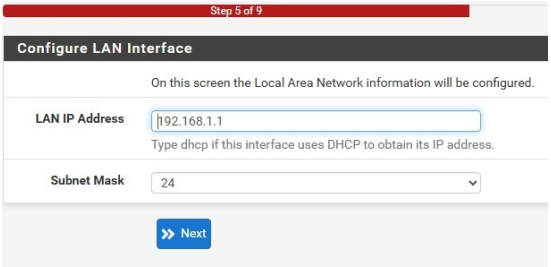


24. Informe o Timezone, selecione América/São_Paulo ou GMT-3. Time Server hostname pode deixar o padrão pfsense.pool.ntp.org. Por último, clique em “Next”

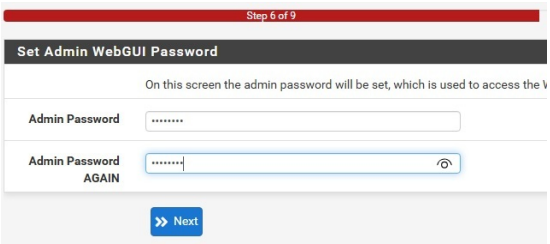
25. Será solicitado as configuirações da interface WAN do Firewall. Selecione “DHCP” e clique em “Next”



26. Será solicitado as configuirações da interface LAN do Firewall. Deixe os parâmetros padrões, IP 192.168.1.1/24, e clique em “Next”



27. Na sequência será solicitado a alteração da senha padrão para acessar a interface gráfica do Configurador Web e do SSH. Utilize a senha “ifrn@2025” e clique em “Next”



28. Na última tela, aparecerá link para atualização, suporte, informações sobre o produto e a empresa. Clique em “Finish” e aguarde o firewall reinicar.