aiyo NETWORKS

www.centralit.com

pfSense

Sumário

Créditos

Autor: Leonardo Damasceno
Correção: Leonardo Damasceno
Arte: Gustavo Brandão
Contato: damasceno.lnx@gmail.com / leonardo.damasceno@centralit.me
Website: **www.centralit.me**

1. Introdução

A utilização de um firewall em uma rede de computadores possui o objetivo básico de proteção relacionado a entrada e saída de dados.

Ao iniciar uma auditoria ou um breve levantamento de dados relacionados a integridade e segurança destes, deve-se pensar em uma alternativa para a seguranã dos ativos envolvidos em uma empresa ou em qualquer ambiente organizacional.

1.1 Segurança

Os fatores básicos para a aquisição de um firewall independente de qual seja, são representados pela proteção da rede local relacionado a parte lógica com o tráfego de dados. Muitos estudiosos dizem que uma rede segura é uma rede de computadores sem usuários. Geralmente, os usuários ajudam a abrir brechas que até então não existem, e isso é feito de várias formas, como acessando e-mail com vírus, onde este abrirá uma porta no computador do usuário em questão.

Existem várias falhas em softwares, que podem comprometer a rede de computadores como um todo, para isso várias combinações de segurança podem ser feitas, como a adição de um firewall junto a um sniffer de rede, onde a rede de computadores estará protegida com regras pré-definidas e com um farejamento com ação de bloqueio para ameaças detectadas. Estas não são as únicas formas de manter o foco da segurança em um ambiente, pois vários cases de sucesso possuem apenas um simples firewall (Simples no nome, e poderoso na configuração), onde quem fará o isolamento cada vez mais forte entre a rede local e a internet será o próprio administrador da rede, definindo as políticas e regras necessárias para manter o ambiente.

É impossível manter 100% (Cem por cento) de disponibilidade para qualquer sistema ou hardware, mas o que deve-se pensar é que pode-se chegar perto disso, e quando maior o potencial da rede de computadores maior a preocupação, então a disponibilidade da mesma necessita de uma atenção com a segurança da informação tornando a integridade dos dados um fato.

1.2 pfSense

O pfSense é um firewall e roteador utilizado para a restrição e liberação de dados na entrada e saída de uma rede de computadores. Este é um front-end para o pf (Packet Filter), firewall padrão de sistemas operacionals da família BSD.

O projeto pfSense teve seu início em 2004 (Dois mil e quatro) como um fork do projeto m0n0wall, porém mais focado em instalações feitas em PC (Personal Computer). Ao longo destes anos, o pfSense vem ganhando conhecimento do público da área e atualmente encontra-se na versão 2.x.

Este firewall é executado sobre o sistema operacional FreeBSD, e possui uma interface web que torna o gerenciamento deste simples.

2. Instalação

2.1 Plataformas (LiveCD, Full Install, Embedded)

Live CD
A versão Live CD, dá a opção para que você utilizar o CD no boot, de modo que você vai acessar, configurare utilizar o PFSense, sem ter a necessidade de instalar o sistema em seu HD ou Cartão de memória. Isso é útil, principalmente para iniciantes que querem migrar de firewall, pois eles podem conhecer melhor o sistema antes de instalar. O CD não é utilizado após o boot completo, porém não é recomendado que você tire o CD enquanto o sistema estiver funcionando.

Full Install
Quando o Live CD é utilizado, existe uma opção para que o sistema seja instalado, essa opção é conhecida como “Full Install”. Após escolher essa opção, todo o seu HD será sobrescrito, portanto se você deseja instalar o PFSense em um HD ou Cartão de memória, verifique antes se o mesmo encontra-se vazio, ou com dados importantes. Até hoje, não é suportada a instalação de outro sistema operacional no mesmo dispositivo em que o PFSense esteja, pois, Dual Boot não é suportado.

Embedded
É recomendado a instalação embedded para cartões de memória, e outros dispositivos flash. Esse tipo de instalação foi otimizada para executar o mínimo de escrita para o disco. Você pode instalar essa versão tanto no Microsoft Windows quanto no Gnu/Linux. Também tem a possibilidade de instalar no próprio FreeBSD ou em qualquer derivado do Unix.

2.2 Requisitos

Os requisitos mínimos de hardware para instalação do pfSense, são:

- CPU - 100 MHz Pentium
- RAM - 128 MB

Requisitos mínimos para cada tipo de instalação:

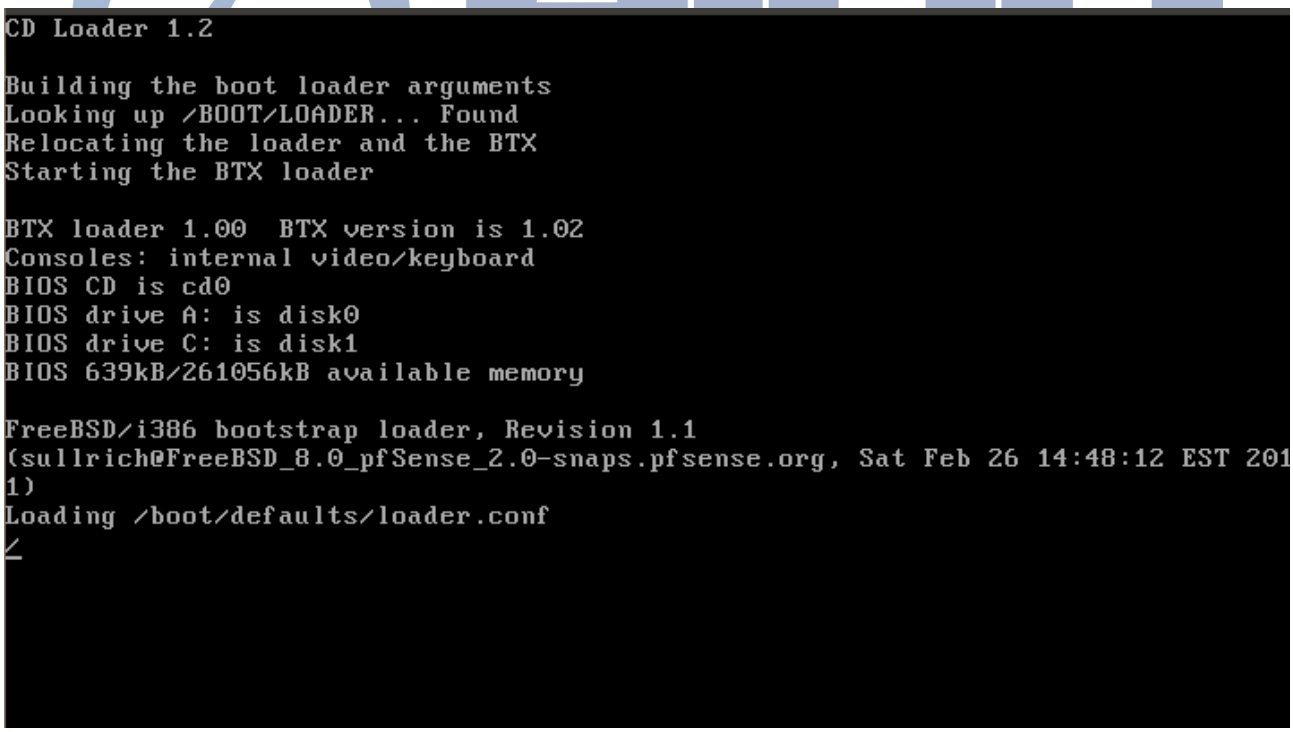
- **Live CD**
  - Unidade de CD-ROM
  - Unidade flash USB ou unidade de disquete para armazenar o arquivo de configuração

- **Instalação em HD**
  - CD-ROM para a instalação inicial
  - 1 GB HD
- **Embedded**
  - 128 MB Cartão Flash
  - Porta serial para o console

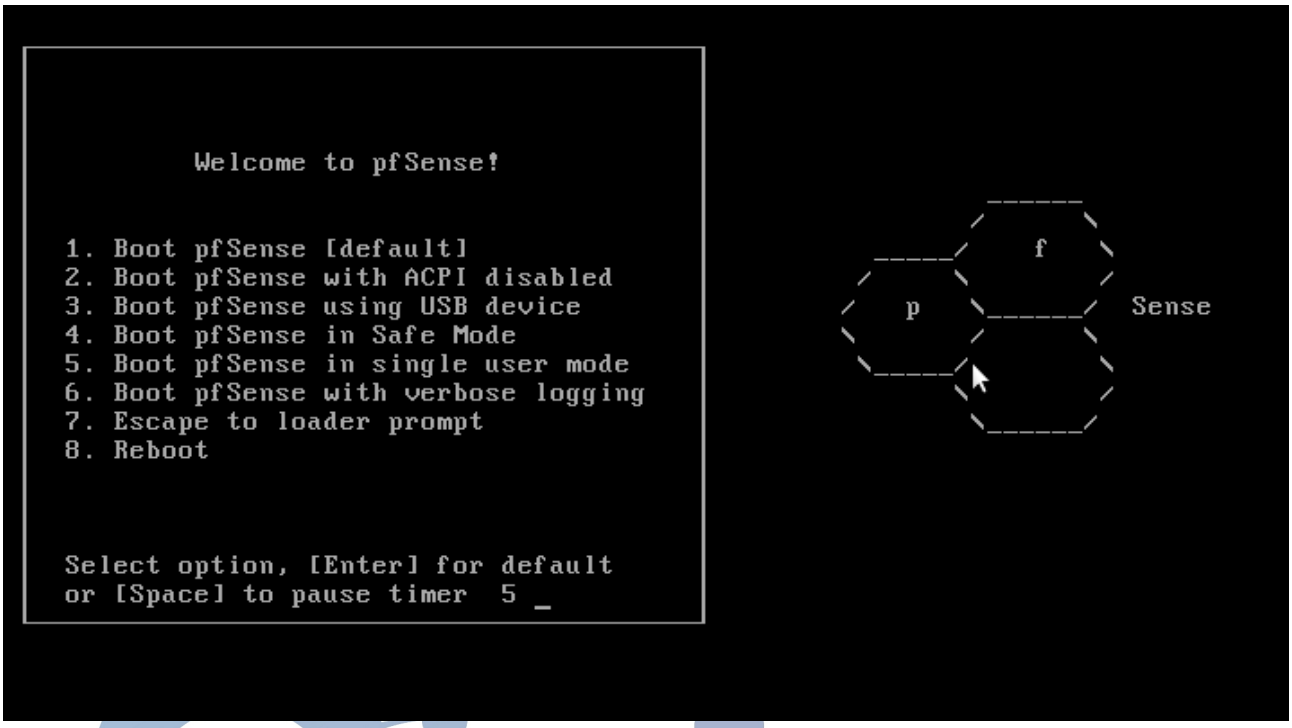
Já na questão de compatibilidade de hardware, o PFSense suporta qualquer hardware que é suportado pela versão do FreeBSD em uso. Arquiteturas como PowerPC, MIPS, ARM, SPARC não são suportadas até o momento. Atualmente, o PFSense trabalha com versões de 32 bits, porém na versão 2.0, será suportado 64 bits.

2.3 Processo de instalação

Ao inserir o CD de instalação do pfSense, a tela abaixo será visualizada dando início ao carregamento do CD Loader:

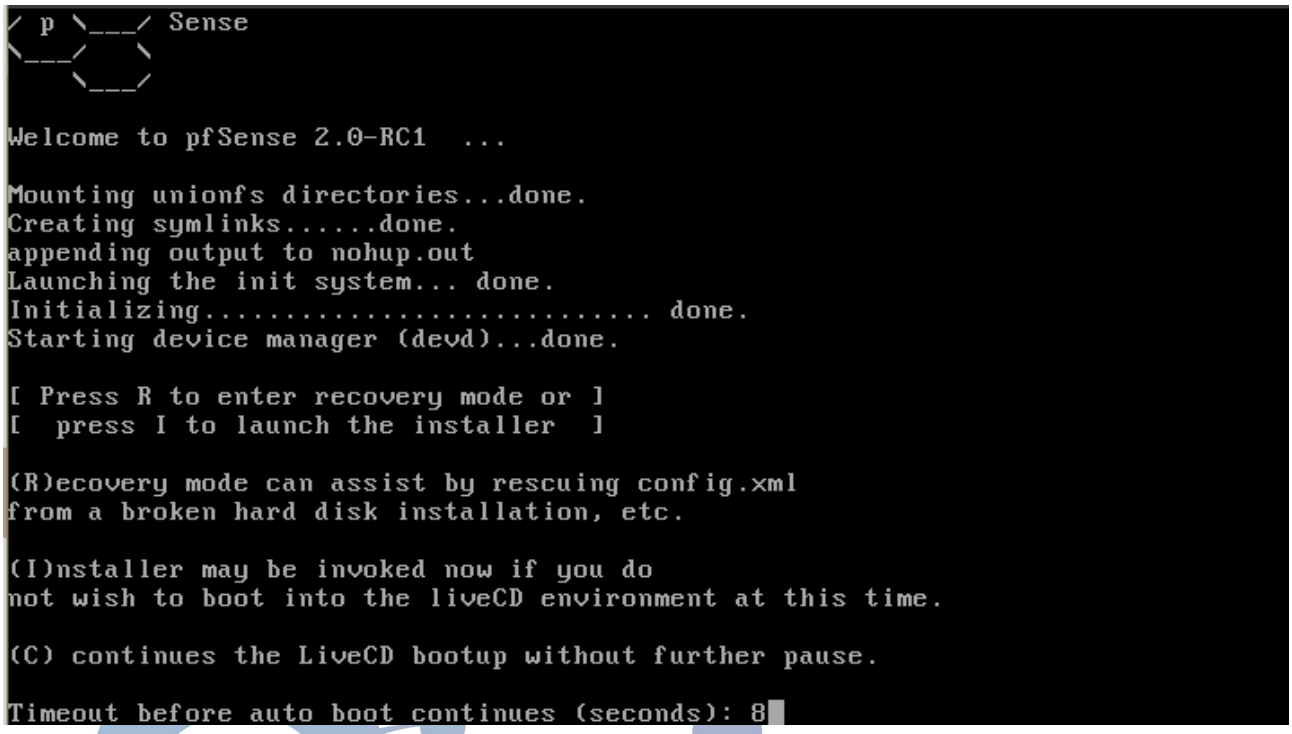


Ao aguardar alguns segundos para o carregamento do CD, a tela abaixo será visualizada:



Por default a opção 1 (Um) será utilizada se nenhuma outra for escolhida durante os 10 (dez) segundos de prazo. Caso seja teclado 1 (Um) também será carregada a opção default. Existem outras opções como por exemplo, é possível carregar o pfSense sem o suporte ACPI, ou iniciá-lo em modo seguro (Safe Mode).

Ao carregar as pontuações da opção escolhida na imagem acima, será perguntado se é desejada a instalação do pfSense ou a utilização dele através do próprio CD sem necessidade de realizar nenhuma instalação:



Nesta parte, existem três possibilidades de escolha:

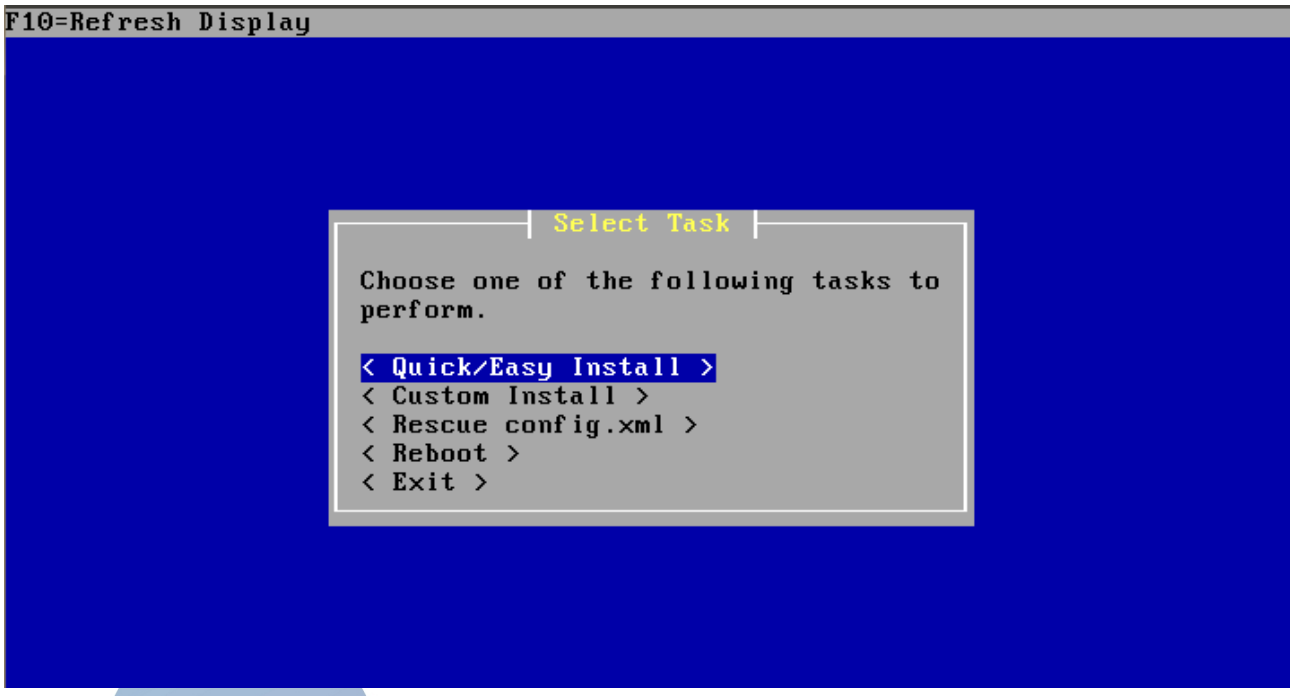
- **R**
  - Com essa opção é possível entrar no modo de recuperação.
- **I**
  - Utilizando essa opção (geralmente a mais utilizada) o sistema será instalado no H.D existente no computador ou outro dispositivo escolhido.
- **C**
  - Essa opção é utilizada para continuar no modo Live CD, ou seja, o sistema não será instalado, continuará executando a partir do CD.

Uma alternativa a opção **C** é simplesmente deixar o tempo acabar de espera, então o CD continuará a executar sem instalar nada.

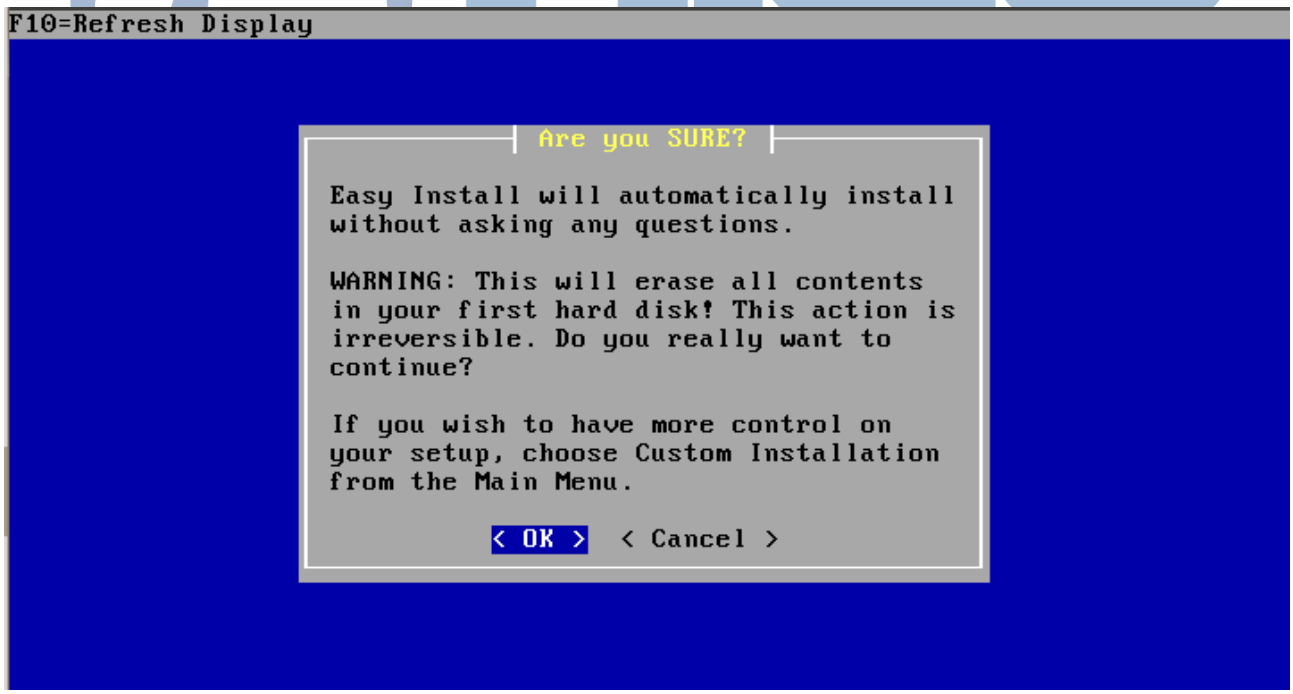
Se a opção **I** for escolhida, a tela a seguir será exibida para iniciar a instalação do pfSense:

Por padrão, o pfSense deixa uma configuração básica e funcional que em quase todos os casos o usuário que está instalando o sistema não necessita alterar nada. Então, ao iniciar a instalação, escolha a opção **Accept these Settings**.

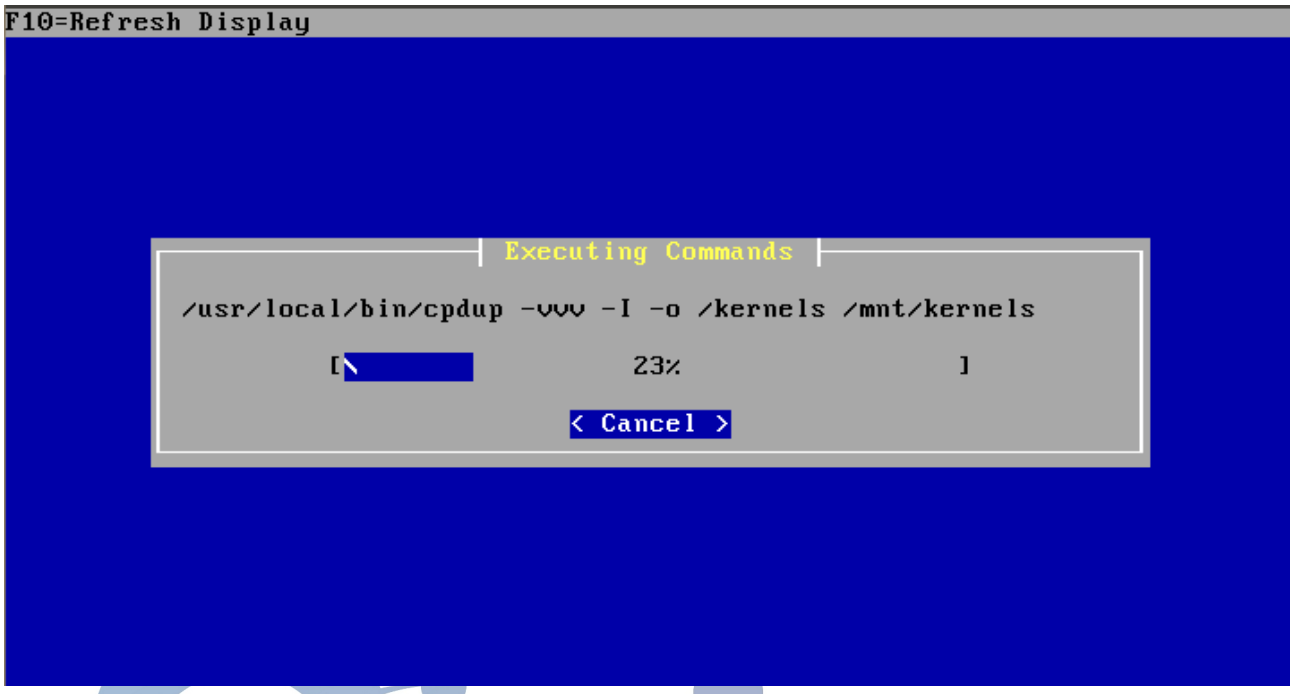
A próxima tela refere-se ao tipo de instalação, que pode ser customizada ou padrão (Sendo essa fácil e rápida). Esse tipo de instalação, fácil e rápida, é representada pela opção **Quick/Easy Install** como mostrado abaixo:



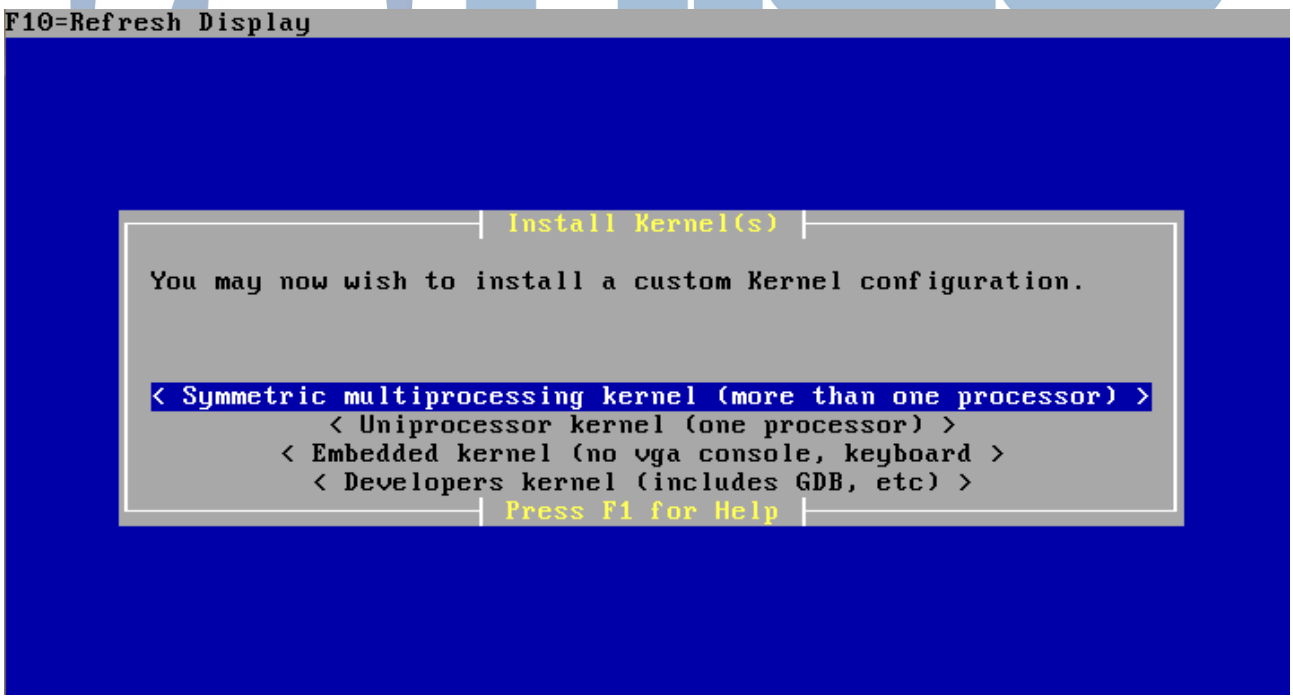
Um aviso é exibido após a tela acima ser mostrada, explicando que todos os dados serão deletados do dispositivo (geralmente o H.D):



Neste ponto, basta escolher **OK** para prosseguir com a instalação, desta forma o pfSense será instalado, e pode-se acompanhar o andamento como na imagem abaixo:

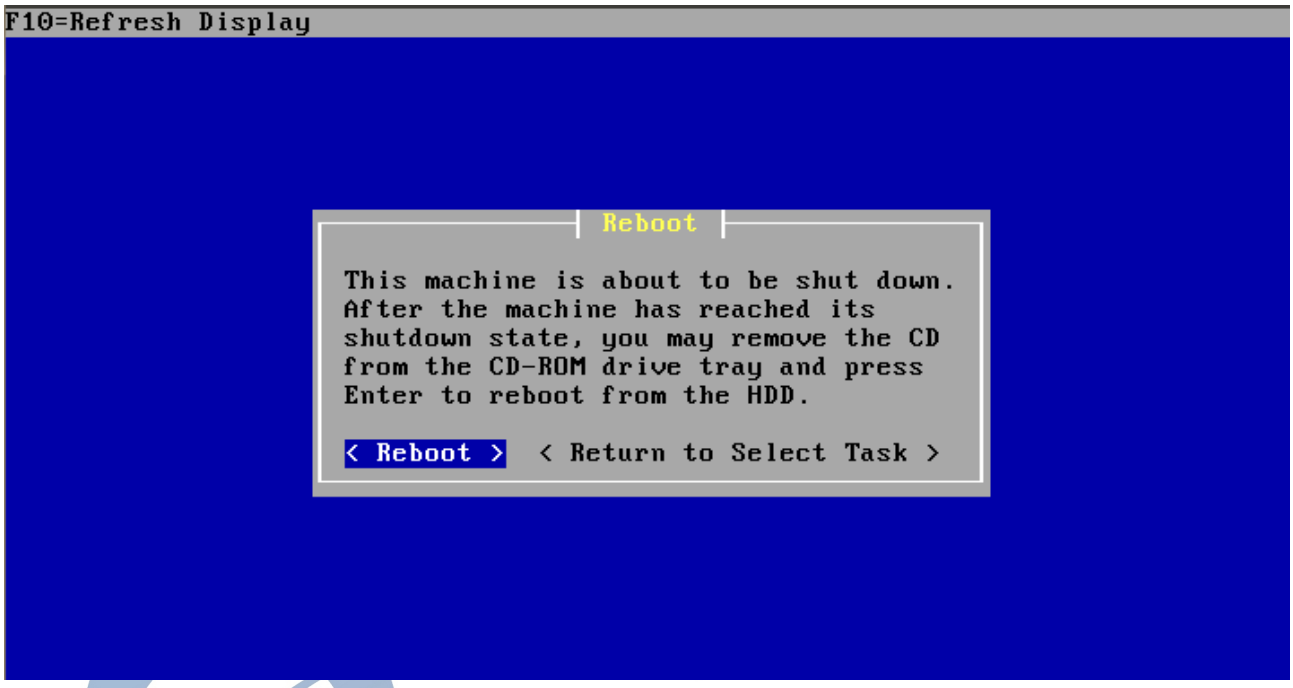


Antes de finalizar a instalação, é necessário especificar uma informação sobre o processador do computador em questão, pois é customizado a utilização do processamento por parte do pfSense, então a tela abaixo será exibida:

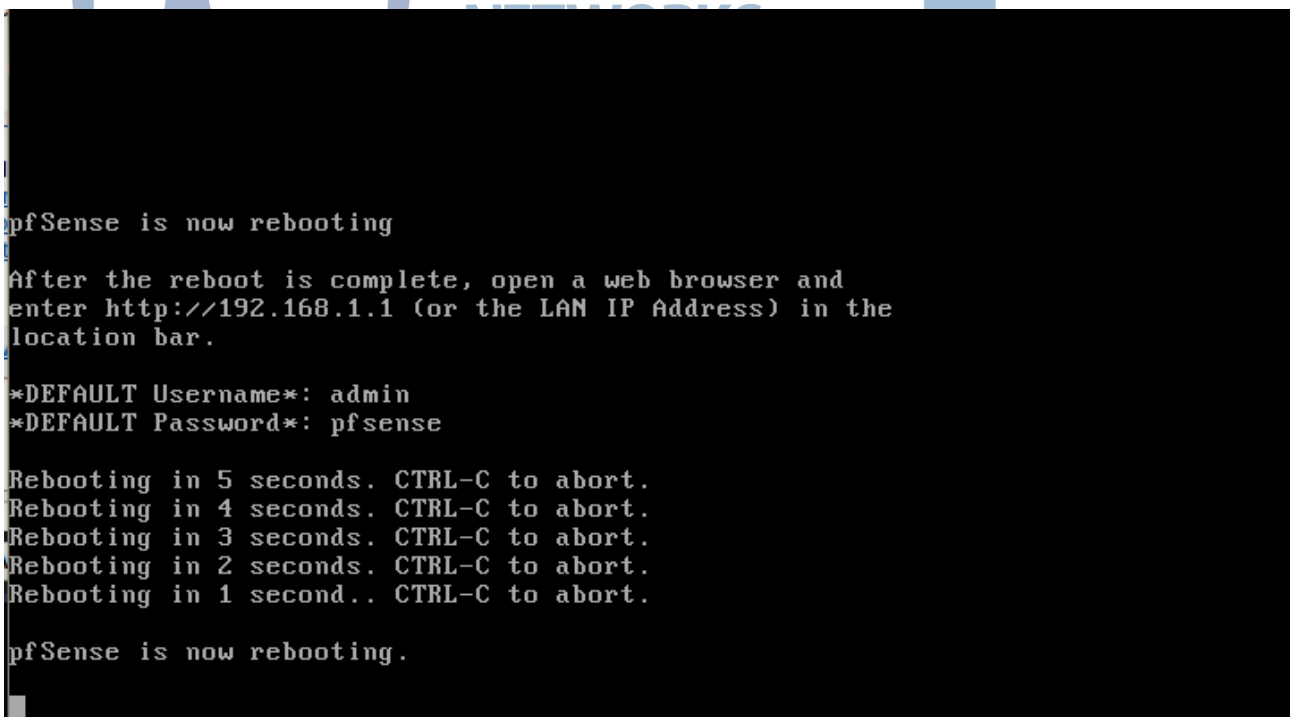


Na maioria dos casos, a primeira opção é escolhida **Symmetric multiprocessing kernel (more than one processor)**, onde está diz que existe mais de um núcleo para processar (Como em um Core 2 Duo). Para finalizar, é exibida a tela onde é possível realizar o a

reinicialização do computador, e já começar a utilizar o pfSense:



Ao escolher a opção **Reboot** o computador será reiniciado, e o pfSense será carregado, mas antes é necessário visualizar as informações para o primeiro acesso, que são exibidas na tela abaixo antes de reiniciar:

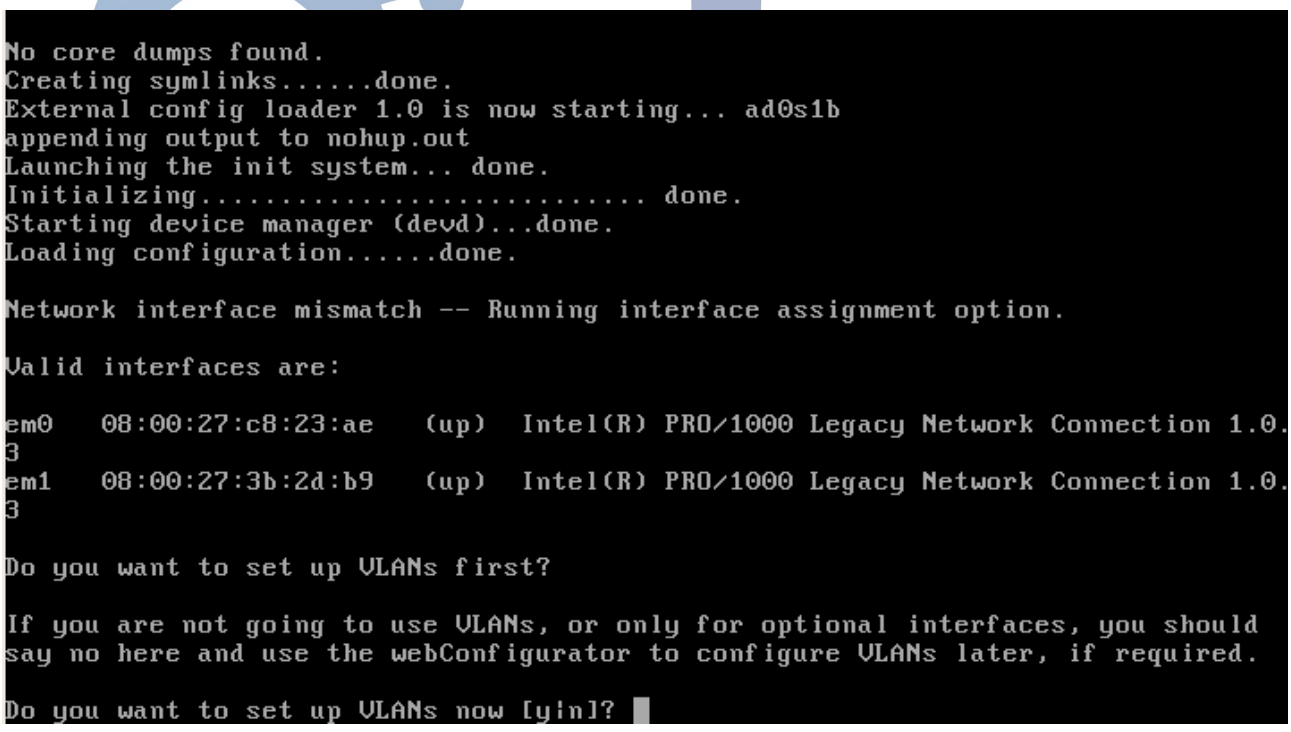


Ao visualizar a tela acima, as seguintes informações são válidas:

- IP de acesso
  - O IP de acesso por padrão é 192.168.1.1, então antes de inserir o firewall na rede local, é recomendado verificar se este IP não está em uso para que não haja nenhum conflito de rede.
- Usuário e senha
  - O usuário para o acesso via web é **admin** tendo a senha **pfsense**.

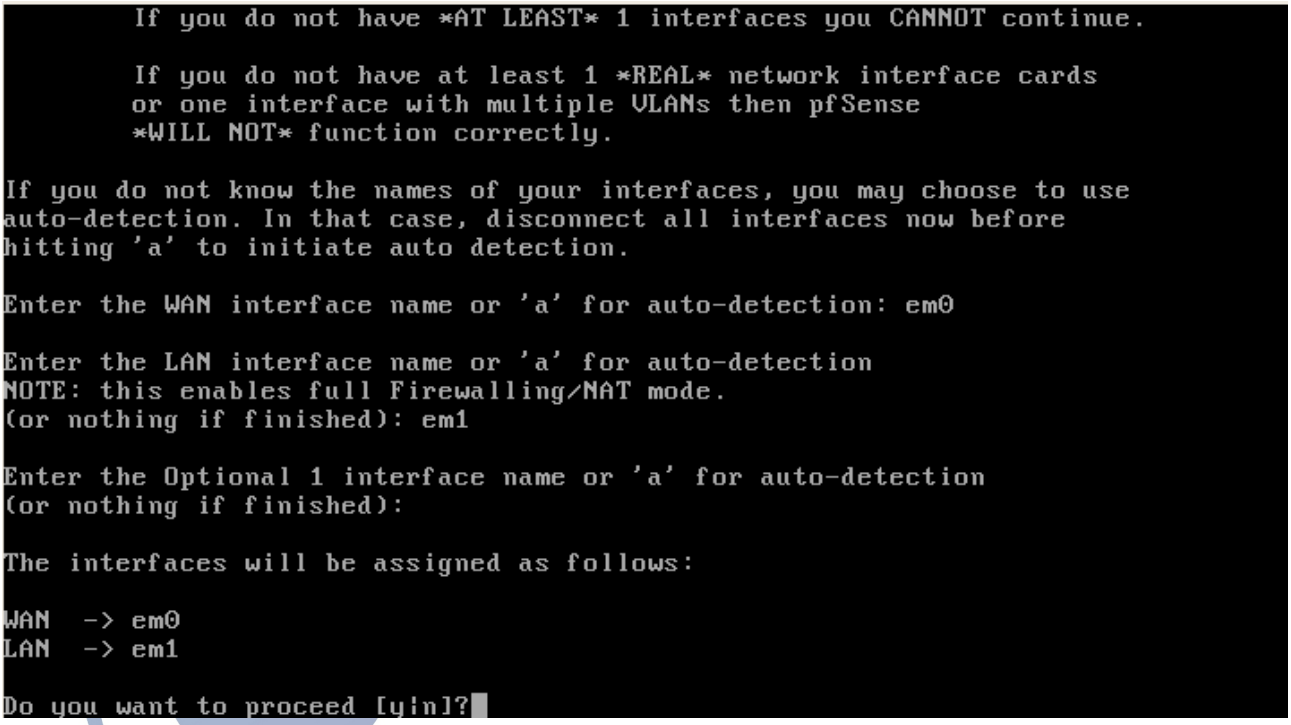
3. Análise inicial

Ao iniciar pela primeira vez, é feita uma análise inicial pelo pfSense. São feitas algumas perguntas iniciais, como por exemplo, qual placa de rede do computador em questão será voltada para a interface da rede local (LAN) e qual será voltada para internet (WAN) e ainda existe a opção de utilizar outras interfaces como WAN2, WAN3, DMZ e mais. Também é feita a pergunta, se é desejável a utilização de VLAN, onde não é recomendada a utilização desta inicialmente. Pode-se visualizar a questão das placas de rede abaixo:

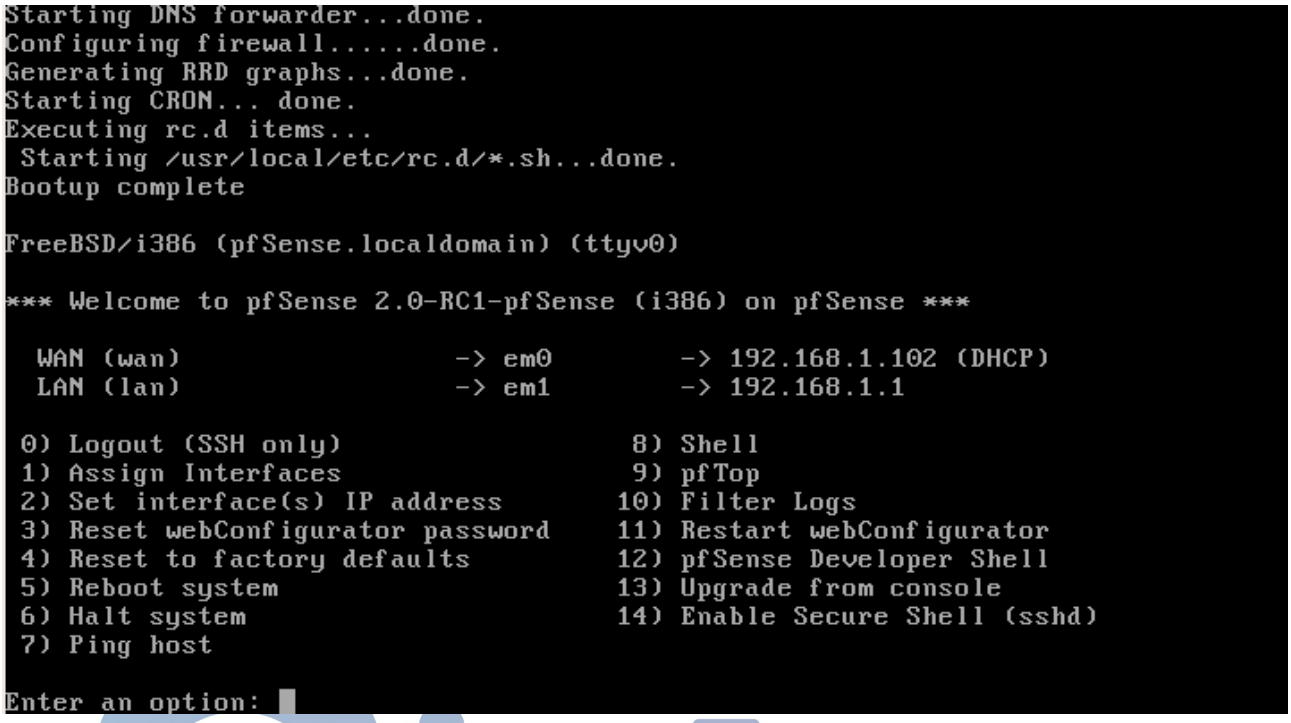


No caso exibido acima, duas placas foram detectadas e reconhecidas como **em0** e **em1** com suas respectivas descrições de cada uma. Logo, é feita a pergunta sobre a utilização de VLANs, o que recomenda-se que seja respondido **n** (No).

Depois de definir quais placas de rede serão alocadas para cada interface inicial, é feita uma revisão, em caso de erro basta teclar **n** (No) para voltar e refazer a configuração, ou teclar **y** (Yes) para confirmar:



Depois de confirmar, a tela inicial com todos os menus será exibida:



Essas opções são descritas abaixo:

- Logout (SSH only)
  - Faz o logout, deixando o acesso liberado via SSH. É importante frisar que após concluir os primeiros passos, você não terá o SSH habilitado, é necessário acessar o PFSense via web, criar a configuração básica (Com o Setup Wizard), para então liberar o acesso através de SSH.

- Assign Interfaces
  - Essa opção dá a possibilidade de configurar novamente as interfaces (Lembrando que elas foram configuradas ao longo da inicialização do Live CD).

- Set interface(s) IP address
  - O PFSense geralmente utiliza o IP 192.168.1.1 para a interface LAN, com a máscara 24 (255.255.255.0). Porém, com essa opção é possível definir o ip e máscara para LAN e para a WAN (O que não era possível em versões anteriores para a interface WAN, apenas via web), para então acessar via web o endereço http://IPDEFINIDO e efetuar a configuração básica. Atenção para o final da configuração da LAN, onde é perguntado se deseja configurar o DHCP para essa interface, que no momento é recomendado que você responda não, utilizando a tecla “n”. Então, ele irá mostrar como acessar o firewall, com o endereço informado, como no formato citado acima.

- Reset webConfigurator password

  - Com essa opção o password para acesso à interface web do PFSense será resetado. O password padrão é “pfsense”, assim, se você acabou de instalar o PFSense, utilize esse password para acessar, e usuário “admin”. Ao final do Setup Wizard, é recomendado que você modifique o password (como é pedido).

- Reset to factory defaults
  - Para zerar as configurações feitas até o momento, basta utilizar essa opção. Tudo voltará para o ponto inicial, inclusive a senha de acesso.

- Reboot system
  - Opção utilizada para reiniciar o sistema (Na interface de gerenciamento via web, você também tem essa opção)

- Halt system
  - Para desligar o sistema, pode utilizar essa opção (Correspondente ao comando **halt** do Gnu/Linux)

- Ping host
  - Você pode utilizar o teste de ping. Basta colocar o ip, após escolher essa opção

- Shell
  - Utilizando essa opção, você tem acesso a linha de comando. Será mostrado o prompt, para que você de fato acesse o sistema utilizando comandos do FreeBSD. Porém, vale lembrar de que o PFSense é um FreeBSD modificado, então caso você não consiga utilizar um comando, provavelmente é porque o comando foi retirado pela equipe do PFSense

- PFtop
  - Aqui, você pode ter a visualização em tempo real do estado do firewall, a quantidade de dados enviados e recebidos e muito mais

- Filter Logs
  - Com o filtro de logs, você pode analisar o que acontece com o firewall (Também existe essa opção na interface web, Status > System logs). Nesta opção é utilizado o software tcpdump, conhecido de muitos administradores de redes, e bastante utilizado no Gnu/Linux

- Restart webConfigurator
  - Essa opção vai resetar toda a sua configuração, mas apenas da parte do gerenciador web Qualquer configuração feita no início, como por exemplo: Configuração do IP (LAN), Máscara. São as configurações que são feitas via terminal

- pfSense Developer Shell
  - Linha de comando utilizada para a linguagem PHP. É utilizada por desenvolvedores e usuários experientes. Você poderá executar códigos em PHP no contexto do sistema que está funcionando

- Upgrade from console
  - Você pode fazer um update da versão do seu PFSense, basta ter uma URL ou o arquivo para atualização

- Enable Secure Shell (sshd)
  - Habilita o acesso via SSH (Obviamente, se ele foi ativado). Vale lembrar, de que o PFSense não utiliza o SSH ativo como default. Você tem que acessar o menu *System* > *Advanced* para ativar a utilização do SSH

4. Configuração inicial (web)

Depois de realizar a configuração inicial o firewall estará funcionando, porém é recomendado que também seja feita a configuração via web, que pode completar algo que tenha sido feito via modo texto. Para acessar o pfsense, basta digitar https://IPDOFIREWALL então será apresentada a tela de login:

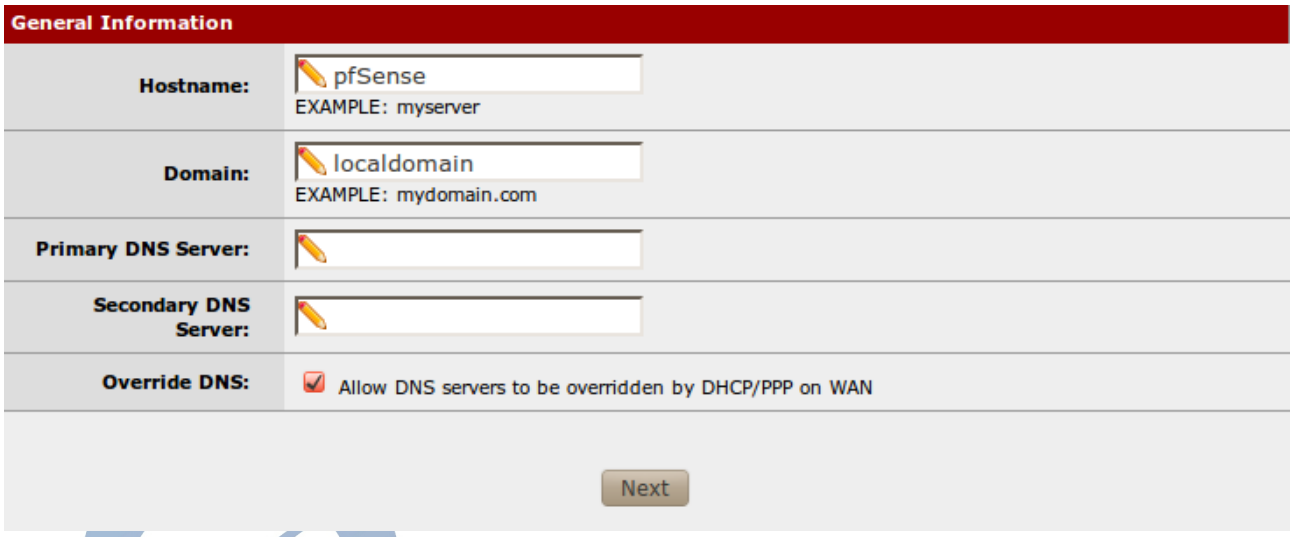
Como explicdo anteriormente, o login pode ser efetuado com o usuário **admin** e senha **pfsense**, feito isso basta clicar em **Login**.

Ao efetuar login, o painel inicial será exibido, mostrando informações dos sistema, e seus menus. Algumas das informações mostradas no painel inicial são: Cpu, memória e utilização de disco, status das interfaces de rede e outros.

4.1 Setup Wizard

Para realizar o setup via web, existe o submenu **Setup Wizard** que localiza-se no menu **System**. Este submenu irá guiar o usuário a realizar a configuração básica, lembrando que algumas opções já estarão preenchidas pois foram feitas no início do pfSense.

Para iniciar, basta clicar em **Next** após escolher o submenu **Setup Wizard**, então a primeira tela será exibida:

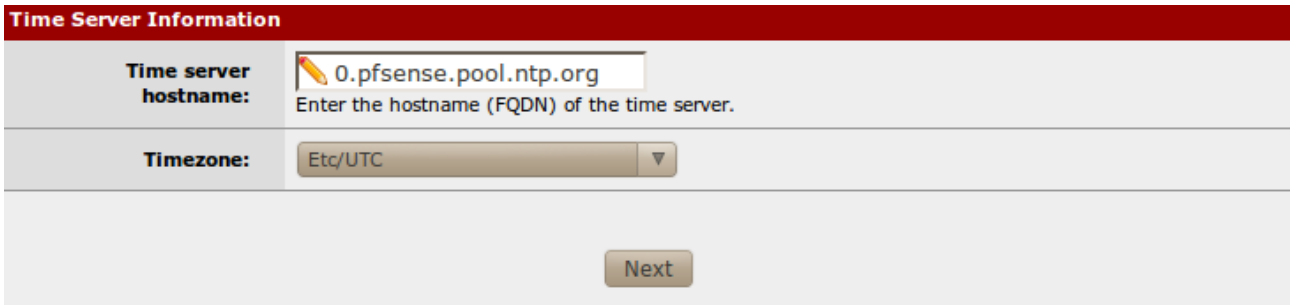


As seguintes opções precisam ser preenchidas:

- **Hostname**
  - Defina o nome para o seu firewall
- **Domain**
  - Defina em qual domínio o firewall vai estar
- **Primary DNS e Secondary DNS Server**
  - Defina o DNS primário e secundário. Neste caso, geralmente apenas o DNS primário é preenchido, como em nosso caso

O campo **Secondary DNS Server** não necessita ser preenchido, porém caso exista um DNS secundário pode-se utilizar esse campo para especificar este.

A próxima tela refe-se a configuração do servidor de tempo, definindo data e hora do pfSense:



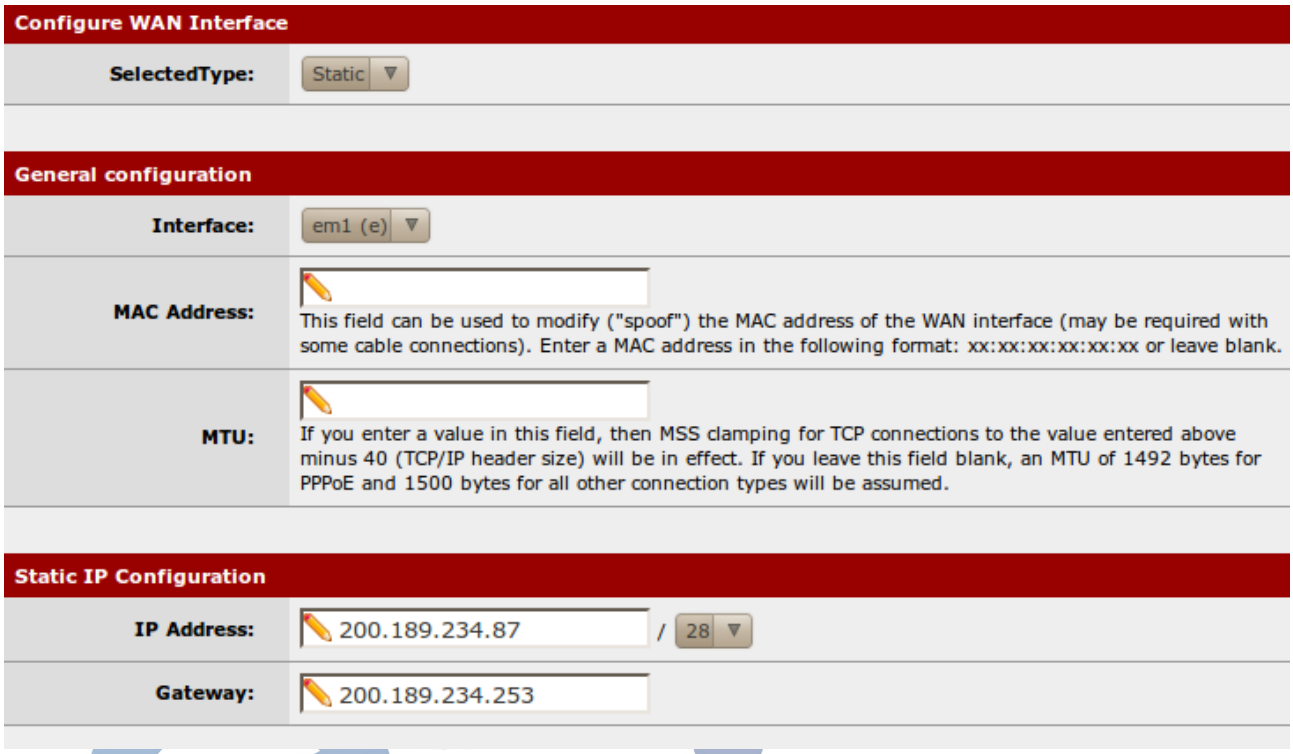
O campo **Time server hostname** não precisa ser alterado, já o campo **Timezone** necessita de alteração para o local onde o servidor se encontra. Como por exemplo **America/Maceio**.

Depois desta etapa, um dos passos mais importantes para o funcionamento do pfSense, que é a configuração da iterface WAN (Que foi definida qual placa de rede seria a interface WAN na interface em modo texto, alocando cada placa de rede para ser WAN e LAN). É necessário o entendimento sobre a interface WAN que é utilizada para a saída até a internet de sua rede local, portanto configure o IP correto e máscara correta.

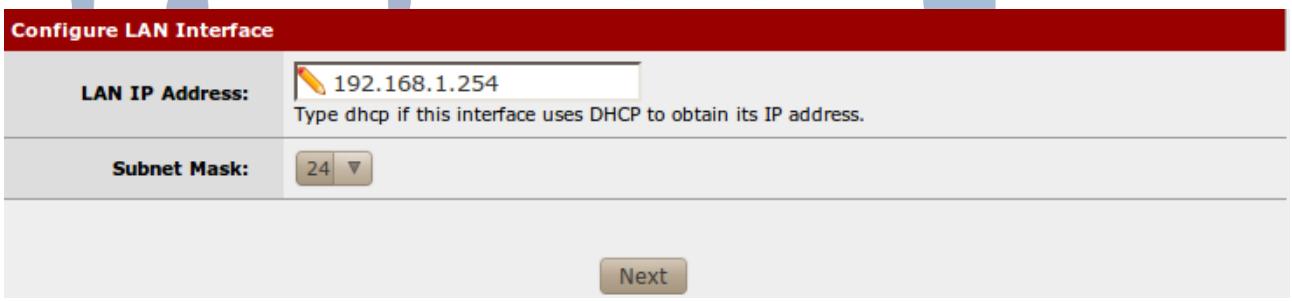
É necessário preencher dois campos, e selecionar um. É necessária a escolha, se a interface será DHCP, PPPoE, PPTP ou Static. Então, para isso precisa-se conhecer como trabalha a internet que chega até o firewall, que em nosso caso possui um IP fixo, então em **SelectedType** escolhe-se *"Static"*. Existe uma grande quantidade de campos, mas precisa-se escolher apenas o Tipo da interface, o IP/Máscara e também o gateway, que no exemplo abaixo ficaram da seguinte forma:

- SelectedType: Static
- IP Address: 200.189.234.87
- Máscara: 28
- Gateway: 200.189.234.253

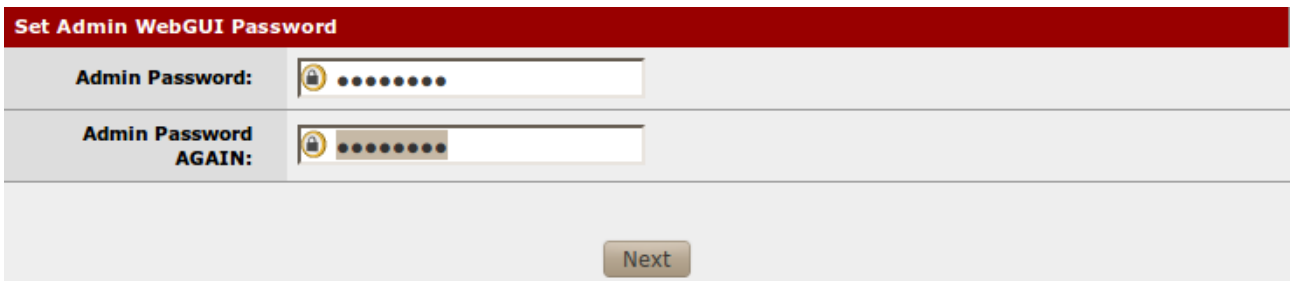
A imagem ilustra a configuração aqui feita:



Ao finalizar a configuração e clicar em **Next**, é possível configurar o IP da interface LAN caso alguma modificação seja necessária (É válido lembrar que esta opção também pode ser modificada no modo texto):



No exemplo acima, o IP 192.168.1.254 foi utilizado com a máscara 24 (255.255.255.0). Um dos últimos passos é redefinir uma senha, pois a senha **pfsense** logicamente não é confiável pois é a padrão:



Depois de definir a senha e repetir, ao clicar em **Next**, o último passo é clicar em **Reload** para que as configurações sejam aplicadas. Depois disso, basta agurdar 120 segundos ou simplesmente acessar o endereço via web novamente.

5. Reconhecimento dos menus

Inicialmente, o reconhecimento dos menus se dá através da primeira visualização, onde a barra superior é exibida com estes:

5.1 Detalhamento dos menus

Com a visualização destes, é possível detalhar os menus da seguinte forma:

- System
  - Utilizado para configurações relacionadas ao sistema (Como por exemplo, SSH, nome, domínio, HTTPS, e outras possíveis configurações do sistema).
- Interfaces
  - É possível definir quais placas de rede serão as interfaces de rede, e também realizar a configuração destas, definindo IP, gateway e outras opções.
- Firewall
  - Este é o menu principal do pfSense, onde é possível definir quais regras serão aplicadas, assim como a criação de conjunto de IPs, realização de NAT (Em três tipos), controle de banda e outros.
- Services
  - Todos os serviços são alocados neste menus, tais como DHCP, redirecionador de DNS e também grande parte dos pacotes instalados posteriomente como Squid, Snort e outros.
- VPN
  - Aqui são definidas como submenus as VPNs suportadas pelo pfSense, como OpenVPN, PPTP e outros.
- Status
  - Este menu é bastante importante, pois relata o status de serviços e do próprio sistema.
- Diagnostics
  - Os diagnósticos do sistema, de rede e de serviços podem ser realizados através deste menu, como a utilização do Traceroute, Backup e até mesmo a visualização dos processos do sistema.
- Help

- O menu de Ajuda provê uma vasta documentação sobre o sistema.

6. Interfaces de rede

Uma placa de rede é reconhecida como uma interface de rede na maioria dos sistemas derivados do Unix. No Gnu/Linux (Derivado do Minix), uma placa de rede é considerada uma interface de rede, que é nomeada de várias formas, como eth0, wlan0 e outros tipos.

O pfSense considera uma placa de rede da mesma forma, sendo uma interface de rede, logo a nomenclatura da mesma depende do fabricante. O reconhecimento das placas de rede mais comuns, são detalhados abaixo:

- Fabricante: Realtek
  - Modelo: 8129/8139
  - Reconhecida como: rl
  - Exemplo: Três placas de rede adicionadas ao pfSense, são reconhecidas como: rl0, rl1, rl2.
- Fabricante: Intel
  - Modelo: Pro/100
  - Reconhecida como: fxp
  - Exemplo: Três placas de rede adicionadas ao Pfsense, são reconhecidas como: fxp0, fxp1, fxp2.
- Fabricante: Intel
  - Modelo: Pro/1000
  - Reconhecida como: em
  - Exemplo: Três placas de rede adicionadas ao Pfsense, são reconhecidas como: em0, em1, em2.
- Fabricante: Broadcom
  - Modelo: Vários
  - Reconhecida como: bge
  - Exemplo: Três placas de rede adicionadas ao Pfsense, são reconhecidas como: bge0, bge1, bge2.

6.1 Adicionar uma interface

Ao adicionar uma placa de rede no computador onde o pfSense está instalado, pode-se adicionar uma placa de rede de duas formas:

- No modo texto
  - Ao escolher a opção 1 (Um), as interfaces serão alocadas de acordo com sua escolha. A tela é igual a primeira imagem da análise inicial, porém existe uma placa de rede a mais. Então, é feita a pergunta sobre a utilização de VLANs, que como foi dito anteriomente, o indicado é responder que não, com a opção **n**. Logo, as interfaces serão alocadas de acordo com as escolhas, como por exemplo WAN, LAN e OPT1.
- Via web
  - No menu **Interfaces** existe um submenu chamado **(assign)**, onde é possível modificar as placas de rede de acordo com as interfaces, e também é possível adicionar uma nova interface se uma nova placa de rede foi inserida através do botão 

6.2 Editar uma interface

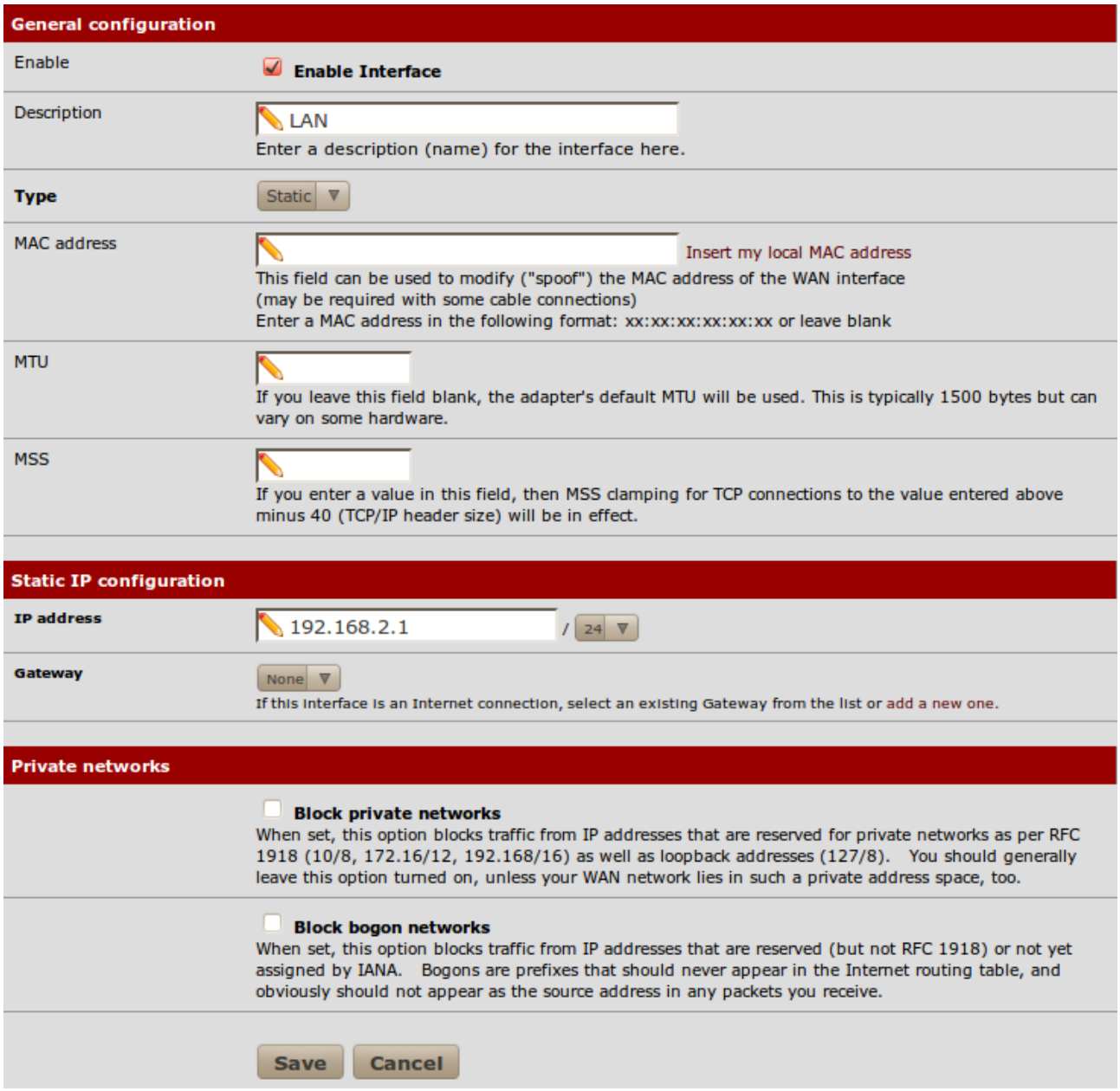
Para editar uma interface, basta ir ao mesmo menu citado anteriomente (**Interfaces > (assign)**) para então, alocar qual placa de rede será a WAN, LAN e assim por diante caso existam mais interfaces de rede.

6.3 Remover uma interface

A remoção de uma interface é tão fácil quanto adicionar uma, pois para realizar essa tarefa basta clicar no botão  ao lado da interface desejada (Por exemplo, OPT1, OPT2).

6.4 Configuração da interface LAN

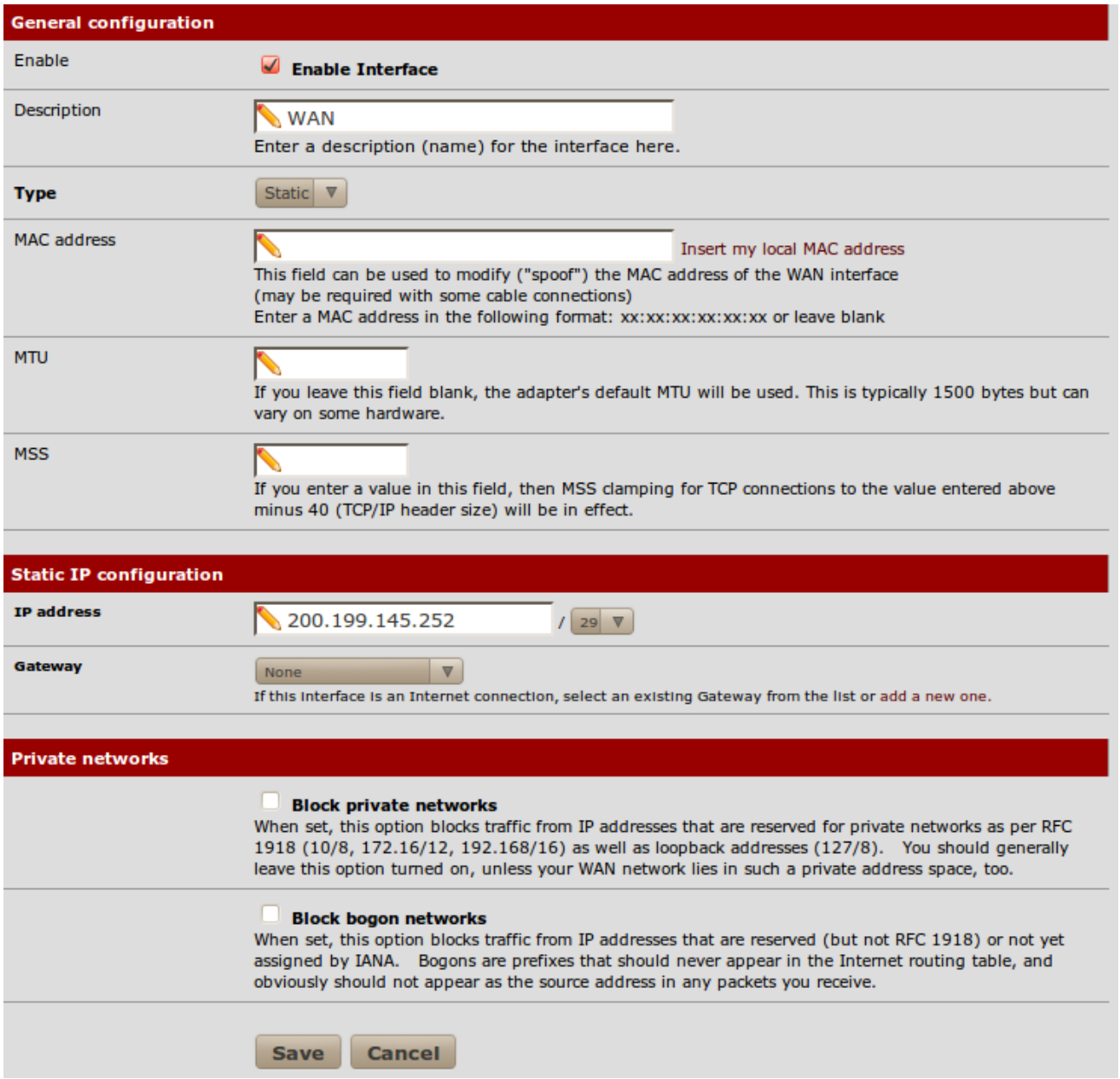
Essa interface é utilizada para a rede local. Em um caso prático simples, a rede ficaria por trás dessa interface, assim, as regras de acesso para a rede e bloquei para a rede local seriam configuradas nessa interface. No caso da configuração desta, são poucas opções, sendo assim, percebe-se que não é necessária uma configuração complexa bastando escolher o IP da LAN, a máscara e depois confirmar, clicando em **Save**. Ao finalizar a configuração inicial do Setup Wizard, a imagem mais abaixo mostra como é exibida a tela de configuração posterior, onde os campos mais importantes são preenchidos e explicados mais abaixo:



- Enable
  - Se esta opção estiver desmarcada, a interface não estará em funcionamento.
- Description
  - Descrição da interface, que geralmente é definida como LAN
- Type
  - Na interface da rede local (LAN), geralmente é definida como Static, mas existem outras opções, tais como DHCP, PPPoE e outras.
- IP address
  - Este é o IP do firewall, onde este será o gateway dos demais computadores da rede local. Além disso, existe a opção ao lado que é utilizada para a definição da máscara de rede.

6.5 Configuração da interface WAN

A interface WAN é utilizada como saída padrão para a internet, logicamente esta também pode ser utilizada para uma determinada saída até outra rede. A configuração dela existe alguns campos que serão explicados mais abaixo de acordo com a imagem a seguir:



- Enable

    - Se esta opção estiver desmarcada, a interface não estará em funcionamento.
- Description
    - Descrição da interface, que geralmente é definida como LAN
- Type
    - O tipo da interface depende do link de internet utilizado. Se por algum motivo um link com PPPoE seja utilizado, pode-se definir este tipo neste campo Type, onde será necessário especificar um usuário e senha para a conexão. Além deste, existem outros tipos de conexão como por DHCP. Porém, a opção mais utilizar é a Static, onde esta necessita da especificação do IP, máscara de rede e o gateway respectivo.
- IP address
    - Este é o IP do firewall utilizado pela interface WAN. Caso seja liberado o acesso externo através da internet, e uma regra libere este acesso, o IP utilizado será o que está sendo definido aqui. Além do IP, é necessário definir a máscara.
- Gateway
    - Este será o responsável direto por encaminhar qualquer requisição da LAN para a internet. O gateway é definido na configuração inicial (Setup Wizard), pois se este não for definido a opção None (Nenhum gateway) será a escolhida por default, e consequentemente não irá realizar o encaminhamento para a internet das requisições internas. Caso necessite adicionar um gateway ou mais, pode-se utilizar o menu **System > Routing**, onde a aba **Gateways** lista, adiciona e remove os possíveis gateways.
- Private Networks (É recomendado não selecionar as opções abaixo)
    - Block RFC1918 Private Networks
        - Esta opção adicionar uma regra na interface WAN para bloquear qualquer acesso com destino a WAN vindo de redes privadas registradas, como 192.168.x.x ou 10.x.x.x.
    - Block bogon Networks
        - Quando essa opção é marcada, existirá um bloquei do tráfego vindo de endereços IPs reservados (Mas não da RFC 1918) ou ainda não definidos pela IANA (Internet Assigned Numbers Authority).

7. Regras de acesso e bloqueio

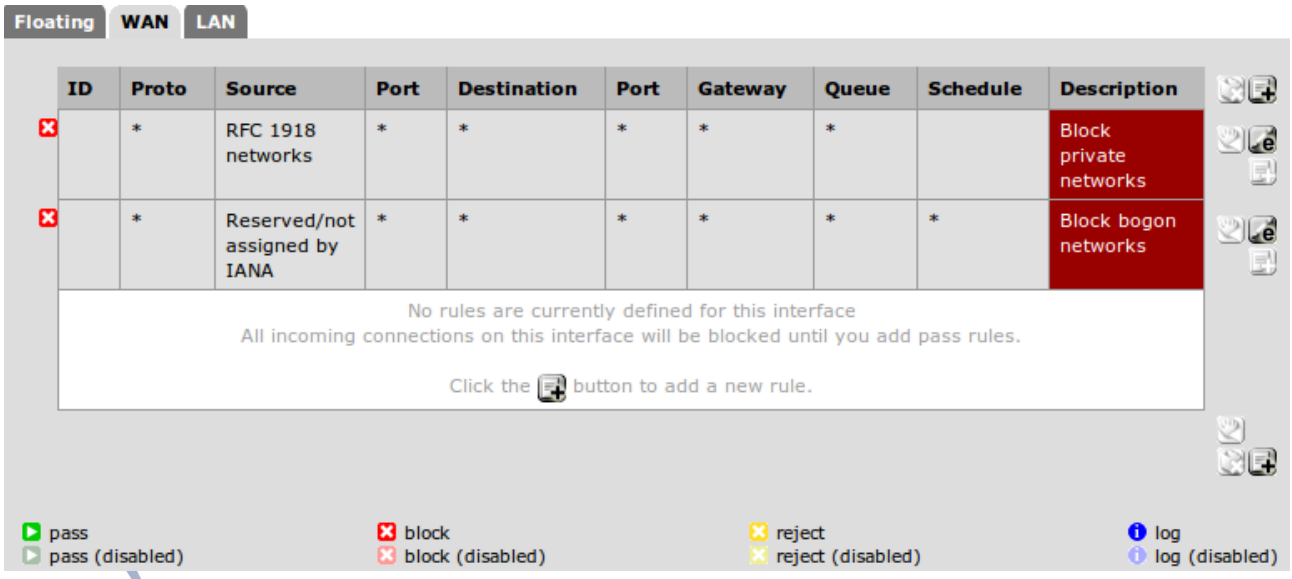
As regras são um meio de controle do que pode e não pode ser acessado relacionado a dados. Pode-se definir uma regra para cada caso, por exemplo, se é necessário que a rede local não tenha acesso ao IP 200.200.187.20 apenas na porta 80, basta criar uma regra específica para isso.

Com o pfSense é fácil criar, editar e remover regras pois este faz uma listagem básica e clara, lógico que isso irá depender do administrador do firewall em questão. Quando se tem

várias regras, é importante utilizar o campo **Description**, preenchendo com o texto bem explicativo da funcionalidade de cada regra.

Em resumo, pode-se pensar em regras de firewall e associar automaticamente à seguinte frase: “É necessário definir o que pode e o que não pode ser acessado nesta rede de computadores”.
Ao tratar diretamente com regras de acesso e bloqueio, o menu utilizado é o **Firewall > Rules**, onde neste é possível visualizar as regras existentes pelas interfaces, desta forma a visualização segmentada das regras se torna fácil. Neste mesmo menu, é possível criar uma regra, editar ou até mesmo excluir.

Ao acessar o menu citado acima, a tela abaixo exibe o conteúdo padrão deste menu (Se existem apenas a interface WAN e LAN):



Se as opções ao final da página de configuração da WAN (Block RFC1918 Private Networks e Block bogon networks) não foram desmarcadas, estas regras serão criadas. Note que estas regras são da interface WAN, ou seja o que tiver origem da internet ou de onde a WAN esteja.

Note que existe uma diferença das outras versões do pfsense para a 2.0 (Versões anteriores 1.2.2 e 1.2.3) sobre as abas para utilização de regras. A aba Floating foi criada com o objetivo de criar tipos especiais de regras, onde estas podem ser aplicadas em qualquer interface (Apenas uma interface, duas, três...) e também em qualquer direção (Entrada/Saída) para configurações de filtros mais complexos, porém quase nunca essa aba será utilizada.

Existem outras observações a serem feitas, como por exemplo a questão dos sinais e dos botões.

Na tela das regras, é possível observar vários sinais na barra inferior com a explicação, e estes são aplicados na esquerda das regras. Existe o sinal de pass (Regra feita para liberar), block (Regra feita para bloquear), reject (Regra feita para rejeitar), log (Regra feita com a intenção de armazenar log sobre a utilização desta). Quando a respectiva cor de cada sinal está mais fraco do que o normal ao lado das regras, significa que elas estão desabilitadas.

Já os botões ficam na direita, e estes são utilizado para adicionar, mover, editar e remover uma regra.

7.1 Criação de regra

Antes de criar uma regra, é necessário entender como funciona o método de criação e a lógica através do pfsense. Por padrão, o pfSense já cria a saída através do NAT e uma regra para que a LAN realmente consiga sair para qualquer local, inclusive para a internet.

Deve-se realizar um levantamento de informações sobre a regra, como por exemplo em sua funcionalidade de onde vem, para onde vai, quais são as portas, e qual o gateway.

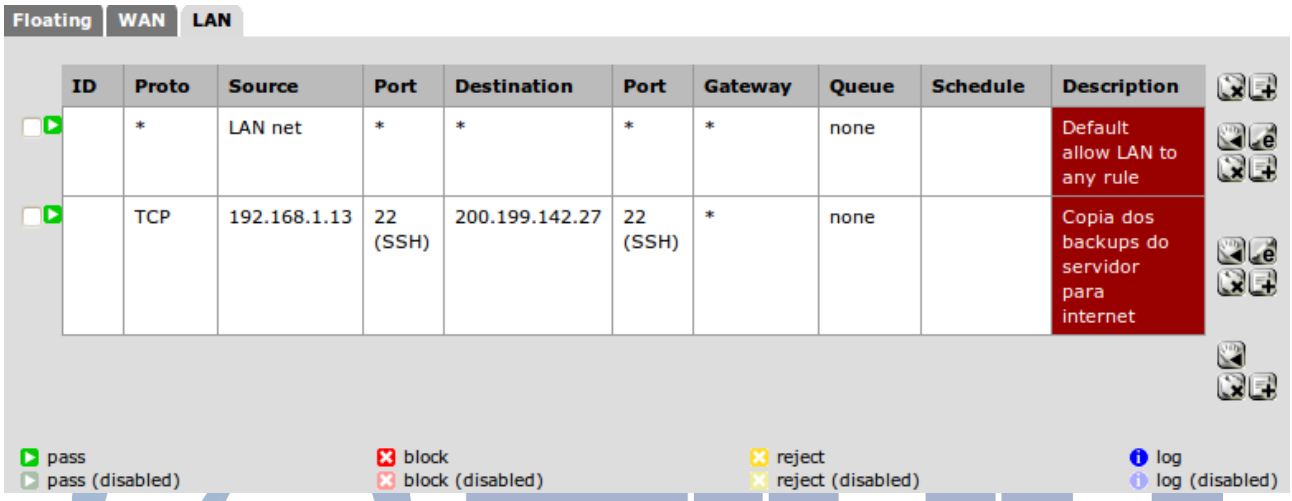
Um exemplo básico de uma lógica de regra, seria:

- Protocolo
  - É necessário definir um protocolo para a regra, mesmo que esse protocolo seja any (Todos os protocolos)
- Origem
  - A regra pretende liberar o servidor de Backup para enviar cópia destes para um local na internet, como forma de segurança. Logo, a Origem da regra será 192.168.1.13 (IP do servidor de backup).
- Porta de origem
  - Ao enviar a cópia dos backups a porta utilizada é a 22 (Vinte e dois), onde neste exemplo a cópia está sendo feita através do software scp do Gnu/Linux.
- Destino
  - O servidor que recebe as cópias de Backup encontra-se na internet com o IP 200.199.142.27, então este IP será utilizado como destino.
- Porta de destino
  - A porta de destino será a mesma, mas é válido lembrar que este servidor precisa aceitar conexões nesta porta, logo, se existir um firewall no destino a porta 22 precisa estar liberada para aceitar conexões nesta.
- Gateway
  - Geralmente o gateway utilizado é o default, de saída para a internet.

Ao recolher essas informações, a lógica começa a ser construída, mas então pode surgir a

dúvida relacionada as abas. Bom, existem três abas atualmente, Floating, WAN e LAN, e qual deve-se usar? Para responder essa questão, lembra-se sempre da origem, então qual é a origem? De onde virá o pacote? O servidor encontra-se na LAN, então deve-se criar essa regra na aba LAN, mas se a regra fosse por exemplo, parar liberar que uma máquina na internet tivesse acesso a rede local do firewall teria então que criar uma regra para a liberação na aba WAN.

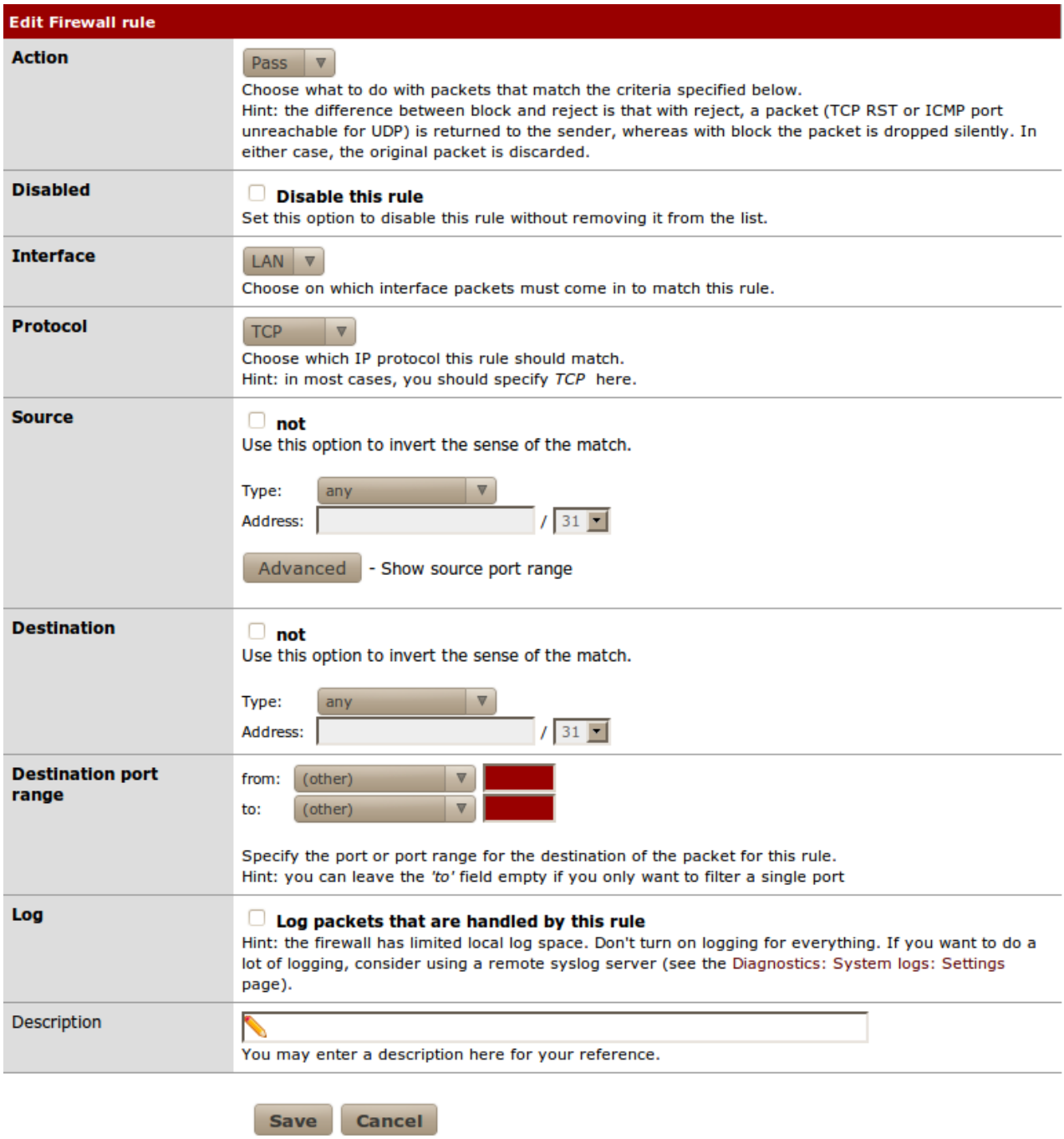
Esta regra seria visualizada da seguinte forma:



Os sinais anteriomente explicados podem ser visualizados a esquerda, onde a ação das duas regras existentes é de pass (Liberar).

A primeira regra é default, e foi explicada anteriomente, onde esta tem o intuito de liberar todo o acesso da LAN para qualquer lugar, e recomenda-se que esta seja removida. Já a segunda regra foi adicionada seguindo o exemplo citado acima.

Com toda a teoria, será iniciada a prática com a criação de uma regra, onde a explicação e imagens serão divididas em duas partes, pois no pfSense 2.0 existem algumas configurações e o tipo de organização diferente para a criação de uma regra quando comparado as versões antigas:



A imagem acima ilustra exatamente como é a primeira parte da criação de uma regra, os campos e opções são explicados abaixo:

- **Action**
  - Deve-se definir se a utilização da regra será para habilitar o acesso, bloquear ou rejeitar. É recomendado que se utilize a opção **Block** quando deseja-se bloquear o acesso, pois essa opção irá “dropar” o acesso de forma silenciosa, enquanto a opção **Reject** irá enviar uma resposta de negação TCP e UDP. Já para liberar o

acesso, existe apenas uma opção, **Pass**.

- **Disabled**
  - Se deseja-se que a regra seja adicionada, porém, não seja habilitada, pode-se marcar essa opção.

- **Interface**
  - Aqui pode-se definir a qual interface a regra será aplicada.

- **Protocol**
  - Defina qual o protocolo que será utilizado para a regra. Pode-se utilizar **any** para todos os protocolos.

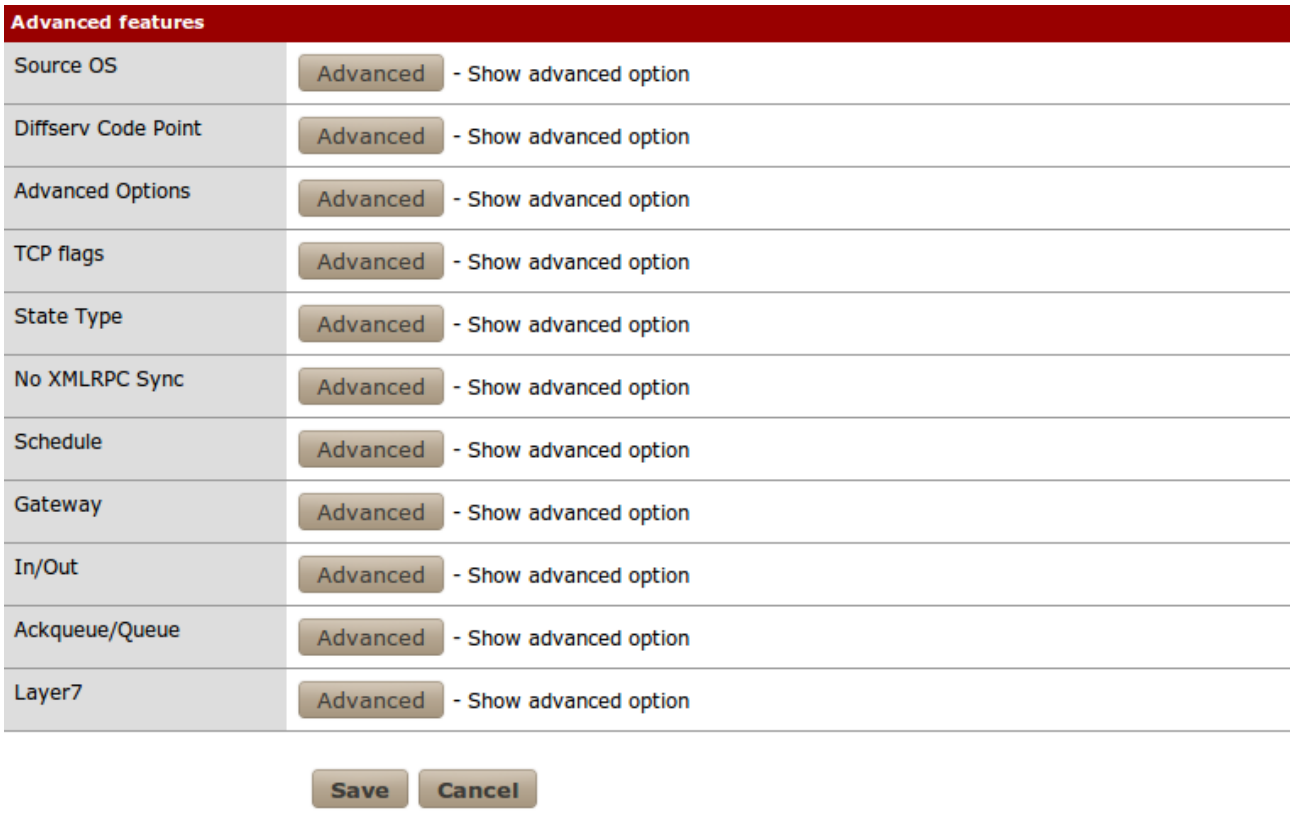
- **Source**
  - Precisa-se definir a origem da requisição, de onde vem o acesso. Pode-se definir uma rede, apenas um host, o endereço da interface, a subnet de uma interface, e até mesmo a opção **any**, para qualquer origem. Em Advanced pode-se definir qual a porta de origem.

- **Destination**
  - É necessário definir tanto uma origem como um destino para cada regra, mesmo que seja any. Assim como na opção Source, você também pode definir uma rede, apenas um host, o endereço da interface, e a subnet de uma interface. Em Advanced pode-se definir qual a porta de destino.

- **Log**
  - Habilitando essa opção, qualquer pacote que passe por esta regra, será direcionado para o log do pfSense.

- **Description**
  - Essa opção é uma das mais importantes, pois se você tem um firewall com várias regras, é sempre bom definir uma descrição clara. Portanto neste campo de texto, defina uma descrição para a sua regra. Você pode utilizar até 52 caracteres.

A segunta etapa (Opções avançadas) não é necessária, pois a maior parte da configuração é feita pelas opções definidas acima, mas é de extrema importância o conhecimento destas:



- **Source OS**
  - Você também pode definir que a regra será aplicada, apenas para o sistema operacional selecionado nessa opção.
- Diffserv Code Point
  - É utilizado como mecanismo para provê qualidade de serviço (QoS) do tráfego de rede.
- Advanced Options
  - Opção utilizada para uma maior especificação sobre as opções avançadas do IP.
- TCP flags
  - Uma definição segundo o site oficial do pfSense é: As subopções aqui são controles de bits que indicam estados de conexões diferentes ou informações sobre como o pacote deve ser suportado.
- State Type
  - Especifica um mecanismo de rastreamento de estado particular.
- No XMLRPC Sync
  - Evita uma regra de sincronizar com outros membros CARP.
- Schedule
  - Pode-se realizar um agendamento para a aplicação dessa regra, definindo os dias e as horas.
- Gateway
  - Pode-se definir o gateway para esta regra, onde este geralmente não é alterado, determinado por padrão o gateway default.

- In/Out
  - Defini-se filas alternativas e interfaces virtuais nesta opção.
- Ackqueue/Queue
  - Especifica o reconhecimento alternativo de filas.
- Layer7
  - Utilizado para identificar tráfego na camada 7 (sete) do modelo OSI. Pode ser acessado através dos menus Firewall > Traffic Shaper > Layer7.

7.2 Editar, mover e desabilitar regras

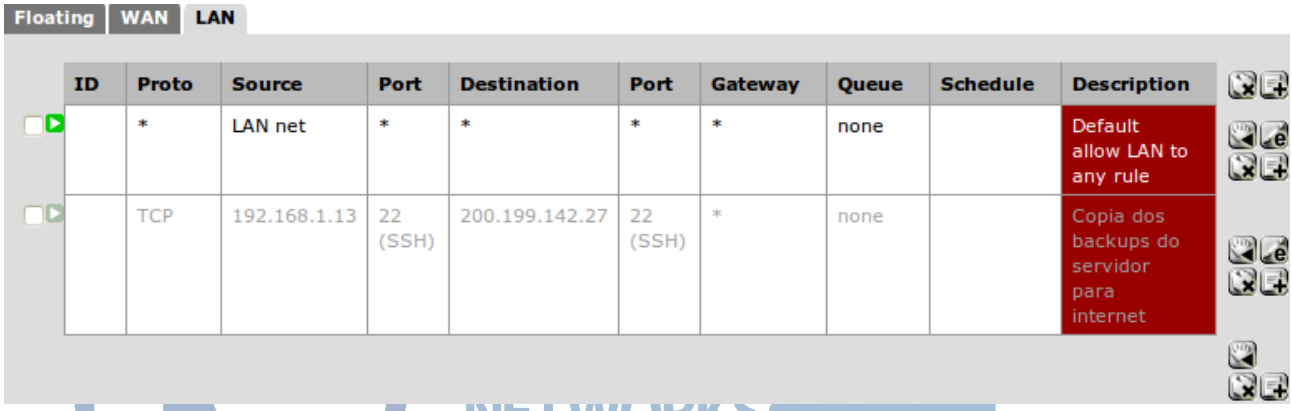
A edição de regras pode ser feita através do botão Editar, que é representado pela letra E. Para um melhor entendimento da utilização de regras percebe-se os seguintes botões:

Os botões representam ações, e ficam ao lado das regras criadas. Acima de qualquer regra, existem dois botões, Remover (Representado pela letra x) e adicionar (Representado pelo sinal de +), abaixo vêm os botões referêntes as respectivas regras, que neste caso são duas. É utilizado um conjunto de quatro ações para cada regra como:

- Mover
  - É utilizada para mover uma regra para cima ou para baixo, sabendo que as regras são interpretadas em ordem crescente.
- Editar
  - Opção utilizada para editar a regra, sendo possível modificar os campos definidos na criação da mesma.
- Remover
  - Remove uma regra existente.

- Adicionar
  - Adicionar uma regra abaixo desta que foi utilizada com o conjunto de botões.

Ao final, existem mais três botões, Mover, Remover, e Adicionar, onde estes são utilizados para ações relacionadas ao final ou a todas regras. Ao clicar em adicionar, uma regra será adicionar ao final de todas as outras. Se o botão escolhido for o de remover, é necessário selecionar a regra ou as regras. Para mover para baixo, utiliza-se esse botão do útimo conjunto.
Ao criar uma regra, a opção **Disable this rule** não é selecionada, pois as regras são criadas para entrarem em funcionamento. Ainda sim, se não foi desativada na criação, pode-se desativar uma regra clicando no sinal de habilitado que é representado por uma seta branca com fundo verde a esquerda, e ao clicar a regra ficará cinza e seu sinal também, significando que esta foi desabilitada:



Para habilitar a regra, basta clicar no ícone que agora está cinza (pois a regra está desabilitada) ao lado da regra. É possível notar também, que a regra acima (a primeira regra) está habilitada.

8. Aliases

Aliases são utilizados como um nome para um conjunto de IPs, redes, portas, usuários OpenVPN, urls e tabela de urls.

Um exemplo de sua utilização seria criar um aliase com o nome bancos, onde seria criada uma regra para liberação da LAN sem passar pelo proxy com destino ao alias bancos, onde neste existiram vários IPs dos sites dos bancos mais acessados, pois se não utilizar um alias , várias regras serão criadas, sendo uma para cada endereço de cada respectivo banco. O menu para criação, edição e remoção de aliases pode ser acessado através dos menus Firewall > Aliases.

8.1 Criar aliase

Ao acessar o menu citado acima, pode-se criar um aliase clicando no botão com um sinal “+”. Então, as seguintes opções são exibidas para a escolha e preenchimento:

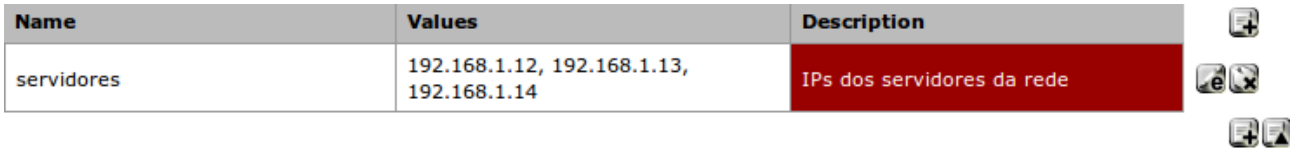
- Name
  - Defini-se um nome para a utilização deste, pois ao criar uma regra é necessário especificar apenas o nome do aliase.
- Description
  - É indicado que a descrição do aliase seja bem definida e clara.
- Type
  - Esta opção irá definir a opção abaixo, onde é possível criar um conjunto de:
    - Hosts
      - Pode-se especificar hosts para a aplicação de determinada regra. Um exemplo seria a criação de um aliase com este tipo, especificando os IPs dos servidores, pois estes não necessitam passar pelo proxy, então teriam acesso direto se na regra de criação a origem (Source) fosse especificada com o aliase aqui citado.
    - Network
      - Utilizado para criar um conjunto de redes. Se deseja-se que a rede local tenha acesso por exemplo a outras redes, pode-se especificar as possíveis redes neste aliase, e então utilizar uma regra de liberação com origem (Source) a partir da LAN e destino (Destination) para o aliase aqui citado.
    - Ports
      - Também é possível criar um conjunto de portas, como por exemplo se da internet (Source) é possível acessar o firewall (Destination) nas portas 22,80,21, então serão criadas três regras, uma para cada porta se não for utilizado um aliase.
    - OpenVPN Users
      - Pode-se criar um conjunto de usuários OpenVPN com apenas um nome.
    - URL
      - É possível criar um conjunto de URLs para a aplicação de regras através de um alias.
    - URL Table
      - Também é possível especificar uma URL contendo vários hosts, ou qualquer outro tipo aqui permitido.
- Campo de escolha
  - O campo de escolha varia com a opção selecionada em **Type**, logo os campos abaixos são exibidos de acordo com a seleção feita:
    - Hosts
      - IP
        - Definição do IP que o alias irá representar
      - Description
        - Descrição do IP definido.

- Network
  - Network
    - Neste campo é definida a rede utilizada, como por exemplo 192.168.3.0.
  - CIDR
    - É necessário definir a máscara da rede definida no campo anterior.
  - Description
    - Descrição da rede definida.
- Ports
  - Port
    - Porta utilizada na criação do Alise. Pode-se definir um range de portas preenchendo este campo da seguinte forma 300:399, logo as portas consideradas irão iniciar de 300 até 399.
  - Description
    - Descrição da porta definida.
- OpenVPN Users
  - Username
    - Especifica-se o usuário utilizado na VPN neste campo.
  - Description
    - Descrição do usuário preenchido.
- URL
  - URL
    - Este campo é utilizado para definir qual a url que será utilizada para as regras futuramente criadas. Um exemplo seria www.google.com.br.
  - Description
    - Descrição da URL definida.
- URL Table
  - URL
    - Defini-se uma URL com uma larga lista de endereços.
  - Update Freq.
    - É definido neste campo de quanto em quantos dias será feito um update na URL especificada.
  - Description
    - Descrição da URL utilizada.

Depois de definir as opções para a criação de um aliase, basta clicar em **Save** e depois aplicar.

8.2 Editar Aliase

Após criar um aliase, a visualização pode ser feita através do mesmo (Firewall > Aliases):



Name	Values	Description
servidores	192.168.1.12, 192.168.1.13, 192.168.1.14	IPs dos servidores da rede

Existem os botões ao lado direito que realizam ações como adicionar, editar e remover aliases. Para editar basta clicar em editar que possui a letra “e”. Após clicar no botão, a mesma tela de adição de aliases será aberta para a edição deste.

8.3 Remover Aliase

Clicando no botão com a letra “x”, o aliase ao lado do botão será excluído, portanto é importante ter noção do que está sendo feito para que um aliase com grande quantidade de informação não seja deletado acidentalmente.

9. Network Address Translator (NAT) no pfSense

A utilização do NAT em redes de computador é algo bastante frequente, pois além do protocolo de internet Ipv4 não possuir IPs públicos suficientes para todos os computadores que hoje acessam a internet, os provedores nem sempre disponibilizam vários IPs ao finalizar um contrato e quando fornece o valor é alto o suficente para fazer com que o cliente prefira não ter esses IPs públicos.

Qualquer computador que necessite acessar a internet precisa de um IP público, onde através deste é possível se comunicar com outros computadores também na internet, porém, como explicado anteriomente, existe uma dificuldade em suprir a necessidade de que todo computador necessita de um IP público, pensando nisso foi criado o NAT, onde este realiza uma tradução de endereços de rede para a saída até a internet e vice-versa.

Através do NAT, uma rede de computador 192.168.1.0 na máscara 255.255.255.0 pode utilizar apenas um IP público para que por exemplo, 50 (cinquenta) computadores possam acessar a internet sem a necessidade da utilização de 50 (cinquenta) IPs públicos.

Como dito anteriomente, o NAT trabalha em duas formas, saída e entrada. A saída é utilizada para a comunicação da LAN com qualquer computador existente na internet, e a entrada (essa precisa ser configurada) diz que um IP público pode ser redirecionado para um IP interno, um exemplo disso seria que um usuário na internet precisa acessar o site que está hóspedado na rede local em um servidor com o IP 192.168.1.5, sabendo que este IP não é público na internet, cria-se um NAT dizendo que por exemplo, o IP 200.199.145.20 será utilizado para redirecionar o usuário da internet para o IP interno.

9.1 Utilização do NAT no pfSense

O pfSense automaticamente cria a saída padrão (Outbound), desta forma só é necessário configurar a entrada e quando preciso. Pode-se criar qualquer tipo de NAT no menu Firewall > NAT, onde neste são visualizadas três abas:

- Port Forward
  - Pode-se efetuar um redirecionamento de portas através deste tipo de NAT. Assim, especifica-se o IP externo (público) juntamente com a porta de acesso, o IP interno com a porta interna. Um exemplo de utilização seria com o IP 200.188.199.20 sendo acessado na porta 33, porém será redirecionado para a rede local, especificamente para o servidor de IP 192.168.1.19 na porta 22 (SSH).
- 1:1
  - Pronuncia-se um para um, onde é necessário especificar apenas um IP externo (público) com sua respectiva máscara, e o IP interno. Então todo tráfego que chegue até o IP público especificado, será encaminhado para o IP interno definido.
- Outbound
  - É possível criar uma regra para a saída da LAN nesta aba, porém, como explicado anteriormente, o pfSense já possui uma opção padrão que serve justamente para isso. É recomendado que nada seja alterado nesta aba, mas caso seja necessário criar uma saída mais específica.

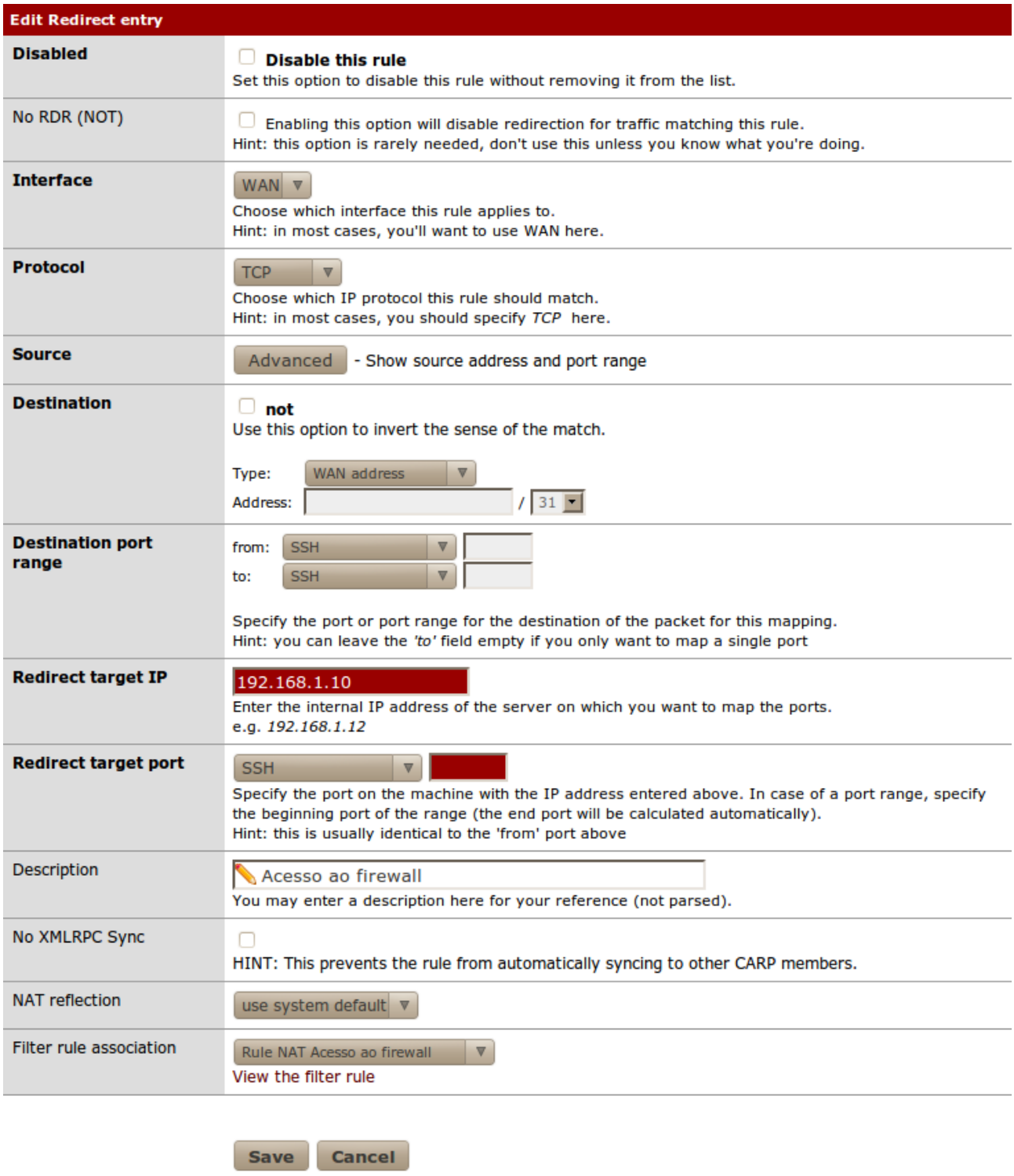
9.2 Redirecionamento de portas (Port Forward)

Ao acessar o menu Firewall > NAT a aba Port Forward já é selecionada por padrão. Nesta aba pode-se criar um redirecionamento clicando no botão add (com o sinal “+”), e as seguintes opções serão exibidas para a escolha e preenchimento:

- **Interface**
  - Selecione a interface onde a regra será aplicada, geralmente sua interface de saída, que é por onde as requisições feitas pela internet chegam.
- **Protocol**
  - Nesta opção, geralmente é selecionado **TCP**, mas existem outras alternativas, como **UDP**, **TCP/UDP**, **GRE**, **ESP**.
- **Source**
  - É possível definir a origem da requisição através deste campo, assim como na criação de uma regra.
- **Source port range**
  - Pode-se definir a porta de origem ou um range de portas com início e fim.
- **Destination**
  -
- **Destination port range**
  -

- **Redirect target IP**
  - Preencha este campo definindo qual o IP local. Lembrando que ao tentar acessar o IP externo, a requisição será encaminhada para esse IP.
- **Redirect target port**
  - Defina para qual porta a requisição será encaminhada.
- **Description**
  - Opção utilizada para inserir uma breve e clara descrição sobre a regra NAT criada.
- **No XMLRPC Sync**
  - Previne essa regra de ser aplicada a qualquer firewall redundante usando CARP.
- **NAT reflection**
  - Essa opção é utilizada para habilitar o redirecionamento de portas da interface WAN para outras interfaces como a LAN. Geralmente é utilizada a escolha padrão **use system default**.
- **Filter rule association**
  - Com a escolha padrão **Add associated file rule**, uma regra será criada e associada a esta regra NAT.

Um exemplo para criação é mostrado na tela abaixo, onde foi determinado o destino como 192.168.1.10 que neste caso é um servidor que poderá ser acessado pela porta 22 (SSH) através da internet. Foi utilizada o IP da interface WAN para o acesso:



9.3 Criação de NAT 1:1

Para este tipo de NAT são utilizados apenas dois IPs, um público e um privado sem a necessidade de especificar qualquer porta.

As opções para a criação da regra NAT 1:1 são explicadas abaixo:

- **Interface**
  - Interface utilizada para o NAT. Geralmente essa opção fica como WAN.
- **Source**
  - Pode-se especificar a origem da requisição, porém, na maioria dos casos está opção é definida como any.
- **Destination**
  - O destino é definido como o IP interno para qual a requisição será redirecionada.
- **External subnet**
  - Neste campo é definido o IP público. Os clientes na internet irão acessar este IP para então serem redirecionados para o IP interno.
- **Description**
  - Este campo é utilizado para definir uma breve e clara descrição sobre a regra criada.
- **NAT reflection**
  - Utilizada para o redirecionamento de portas, que neste caso não é utilizado.

9.4 NAT Outbound

Para qualquer visualização ou configuração de saída, pode-se acessar a aba Outbound que fica no menu Firewall > NAT. Por padrão, a saída é feita automaticamente pelo próprio pfSense, e possui a opção marcada por padrão **Automatic outbound NAT rule generation (IPsec passthrough included)**.

Para realizar uma configuração manual de saída, a opção **Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)** é marcada, logo é necessário salvar e aplicar essa alteração. Pode-se visualizar abaixo em **Mappings** se existe alguma configuração, onde também é possível adicionar uma nova clicando no botão add (com simbolo “+”). As opções a serem definidas são as seguintes:

- Interface
  - Interface utilizada para a tradução de endereço, geralmente esta opção é utilizada como WAN.
- Protocol
  - Protocolo utilizado na regra para determinar que tipo de protocolo será utilizado pela origem, na maioria dos casos é selecionada a opção any.
- Source
  - Na origem pode-se definir uma rede, IP (utilizando a opção como Network e máscara de rede 32) e any para qualquer origem.
- Destination
  - É necessário especificar o tipo de destino, mesmo que esse seja any (qualquer destino).
- Translation

    - A tradução pode ser feita para o IP da interface em questão, ou para um IP Virtual definido.
- No XMLRPC Sync
    - Evita uma regra de sincronizar com outros membros CARP.
- Description
    - Descrição da regra de NAT Oubound criada.

Depois de realizar a configuração basta clicar em Save para salvar a regra.

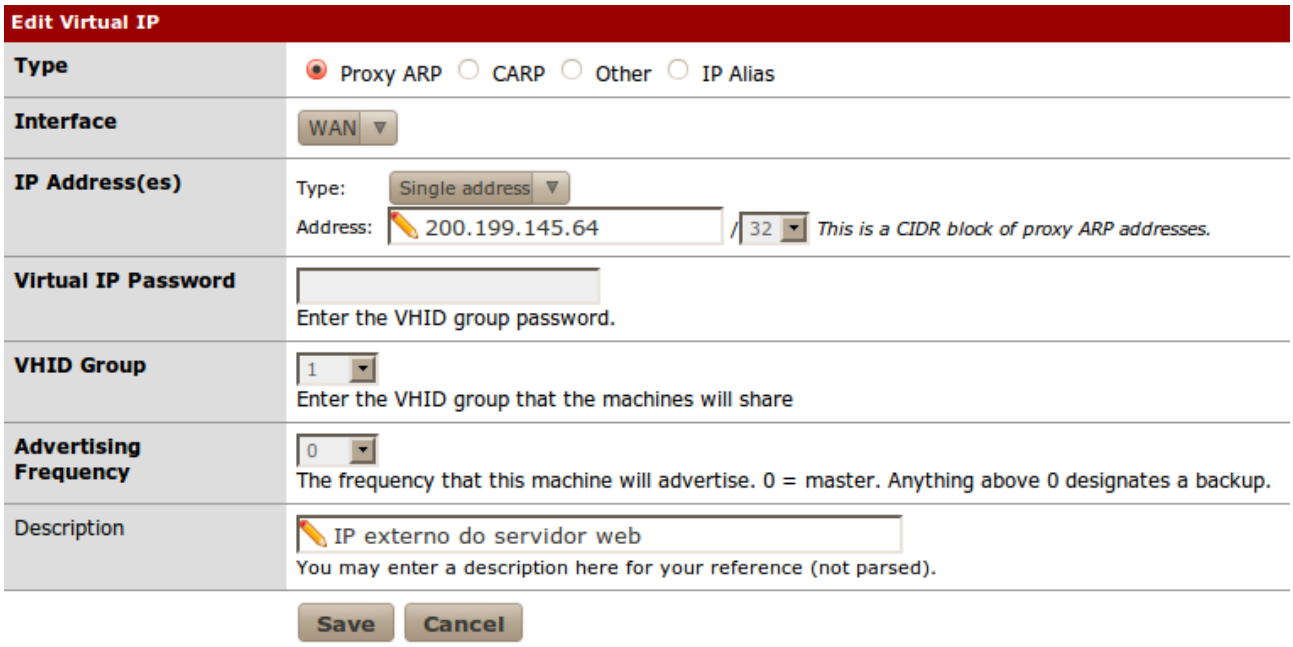
10. IP Virtual

Ao utilizar um IP público, geralmente este precisa ser associado a uma interface de rede, logo se necessita-se utilizar três IPs públicos será necessária a utilização de três placas de rede. Ao utilizar o pfSense não é necessário ter uma placa de rede para cada IP para utilizar este como saída ou entrada de dados, existe uma opção conhecida como IP Virtual que faz esta função sem ter a necessidade de alocar uma interface de rede a um IP público.

O acesso ao menu de configuração é feito através de Firewall > Virtual IPs, e a partir deste pode-se visualizar a aba padrão Virtual IPs e os IPs existentes, também é possível criar, editar e remover qualquer um que esteja listado alí. Atualmente existem três tipos de IP Virtual que podem ser criados:

- Proxy ARP
  - Utiliza a camada 2 (dois) de tráfego.
  - Pode ser redirecionado apenas pelo firewall.
  - Pode estar em uma subrede diferente da interface.
  - Não responde a requisições ICMP.
- CARP
  - Utiliza a camada 2 (dois) de tráfego.
  - Pode ser utilizado ou redirecionado pelo firewall.
  - Deveria ser utilizado em cenários FailOver ou Load Balance
  - Responde a requisições ICMP se configurado de forma correta.
- Other
  - Pode ser redirecionado apenas pelo firewall.
  - Pode estar em uma subrede diferente da interface.
  - Não responde a requisições ICMP.
- IP Alias
  - Pode ser redirecionado apenas pelo firewall.
  - Permite adicionar endereços IP extras a uma interface.

Geralmente o primeiro tipo (Proxy ARP) é o mais utilizado. Pode-se visualizar uma simples configuração abaixo:



No caso acima, foi especificado um único endereço, mas também pode-se utilizar uma rede como por exemplo 200.199.145.0/28.

Todos os outros tipos de IP Virtual são configurados da mesma forma com exceção do CARP, porém só possuem a opção de determinar um IP e não uma rede. Ao configurar um IP Virtual do tipo CARP é necessário especificar um password para a utilização deste no campo **Virtual IP Password**, o número que é compartilhado no campo **VHID Group** e a frequencia em **Advertising Frequency**.

11. Serviços

Por padrão o pfSense oferece alguns serviços que são disponibilizados a partir da própria instalação do firewall, estes são conhecidos como serviços integrados. Com esta integração de serviços o pfSense disponibiliza não só a função básica de um firewall e router mas também um gerenciador de serviços de rede, onde estes estão protegidos através das regras criadas no firewall.

11.1 Pacotes

O pfSense disponibiliza diversos pacotes para serem instalados e integrados ao firewall, como por exemplo:

- Squid
  - Serviço para proxy de rede.
- LightSquid
  - Emite relatórios de utilização do proxy.

- Snort
  - Sniffer utilizado para verificação de ameaças.
- FreeRadius
  - Utilizado para criação de autenticação centralizada.
- Nmap
  - Pacote utilizado para realização de scanners de portas e informações sobre o alvo.

A visualização dos pacotes disponíveis só é possível se o acesso a internet está devidamente configurado, e pode-se acessar estes através do menu **System > Packages**.

11.2 Portal Captive

Este serviço provê um portal de autenticação para acesso web dos hosts da rede. Este serviço é integrado ao firewall na instalação do pfSense. Pode-se acessar o portal de autenticação Captive Portal através do menu **Services > Captive Portal**.

A aba principal e padrão é a Captive Portal, nesta são configuradas as opções para o devido funcionamento do portal de autenticação, e suas opções são descritas abaixo:

- **Enable captive portal**
  - Habilita a utilização do portal de autenticação Captive Portal.
- **Interfaces**
  - Nesta opção é selecionada a interface na qual o portal de autenticação irá trabalhar. Na maioria dos casos a interface LAN é selecionada.
- **Maximum concurrent connections**
  - Pode-se definir a quantidade de conexões por IP neste campo, o padrão são 4 (quatro) conexões, desta maneira o cliente com o IP em questão não irá consumir recursos desnecessários do firewall.
- **Idle timeout**
  - Com esta opção um usuário inativo pode ser automaticamente desconectado.
- **Hard timeout**
  - O valor deste campo irá desconectar de forma forçada um cliente conectado através do portal de autenticação.
- **Pass-through credits allowed per MAC address**
  - Essa opção permite passar pelo portal de autenticação sem a necessidade de autenticar com um número limitado de vezes por endereço MAC.
- **Waiting period to restore pass-through credits**
  - Os clientes terão seus **pass-through credits** disponíveis restaurados para a contagem original depois dessa quantidade de tempo desde a primeira utilização.
- **Reset waiting period on attempted access**
  - Se esta opção for habilitada, o periodo de espera é resetado para a duração original se o acesso for tentado quando todos **pass-through credits** estiverem

esgotados.

- **Logout popup window**
  - Pode-se habilitar essa opção para abrir um pop-up com ação de logout. É válido lembrar que a maioria dos navegadores bloqueiam qualquer tipo de pop-up.
- **Redirection URL**
  - Ao efetuar o login o cliente pode ser redirecionado para uma url ao utilizar essa opção. Um exemplo é redirecionar o cliente após o login para http://www.google.com.br (Essa opção só irá funcionar se existir o http:// antes do site).
- **Concurrent user logins**
  - Com essa opção, o portal de autenticação irá limitar um login por conta de usuário.
- **MAC filtering**
  - Com essa opção é possível desabilitar o filtro de MAC.
- **Pass-through MAC Auto Entry**
  - **Enable Pass-through MAC automatic additions**
    - É possível criar um tipo de passe livre após a primeira autenticação com essa opção, desta forma o cliente que autenticar a primeira vez não precisará autenticar novamente pois uma entrada com seu MAC será criada.
  - **Enable Pass-through MAC automatic addition with username**
    - O usuário será salvo após a autenticação será salvo.
- **Per-user bandwidth restriction**
  - Pode-se definir um limite de banda para a utilização do portal de autenticação com esta opção. É utilizado 0 (zero) quando essa opção é marcada mas não existe limite.
- **Authentication**
  - Pode-se utilizar o portal sem autenticação ou com autenticação. São possíveis três opções:
    - **No Authentication**
      - O portal ficará sem autenticação quando essa opção for selecionada.
    - **Local User Manager**
      - Existe a possibilidade de utilizar o portal com uma autenticação local, no próprio pfsense pode-se gerenciar todas as contas.
    - **RADIUS Authentication**
      - Também é possível integrar o portal a um tipo de autenticação centralizada com essa opção como o RADIUS.
- **MAC address format**
  - Essa opção só pode ser utilizada quando na opção Authentication for selecionada como RADIUS. Essa opção irá modificar o formato do endereço MAC de todo o sistema RADIUS.
- **HTTPS login**
  - Se esta opção for habilitar o usuário e senha serão transferidos para o servidor de autenticação via HTTPS.
- **HTTPS server name**

    - É necessário especificar o nome do servidor HTTPS, geralmente neste campo é utilizado o nome da empresa.
- **HTTPS certificate**
    - Pode-se definir o certificado HTTPS neste campo.
- **HTTPS private key**
    - Neste campo a chave privada é definida.
- **HTTPS intermediate certificate**
    - Neste campo é definido o certificado de intermediação HTTPS.
- **Portal page contents**
    - É possível realizar o upload de uma página para a autenticação do usuário ao tentar acessar a internet, desta forma a página de acesso do portal seria personalizada.
- **Authentication error page contents**
    - Ao tentar efetuar o login, caso algum dado esteja errado no login ou senha essa página pode ser exibida indicando erro.
- **Logout page contents**
    - Ao efetuar o login é possível exibir uma página para o cliente através desta opção.

11.3 DHCP Server

Para criação de um servidor que distribua dinamicamente IPs de forma automática pode-se acessar o menu Services >DHCP Server, onde é possível configurar diversos servidores DHCP de acordo com a quantidade de interfaces.

Basicamente um servidor para distribuição de IPs é configurado na aba LAN (Onde este será aplicado de fato para a rede local) e ao clicar nesta as seguintes opções para configuração do servidor são possíveis:

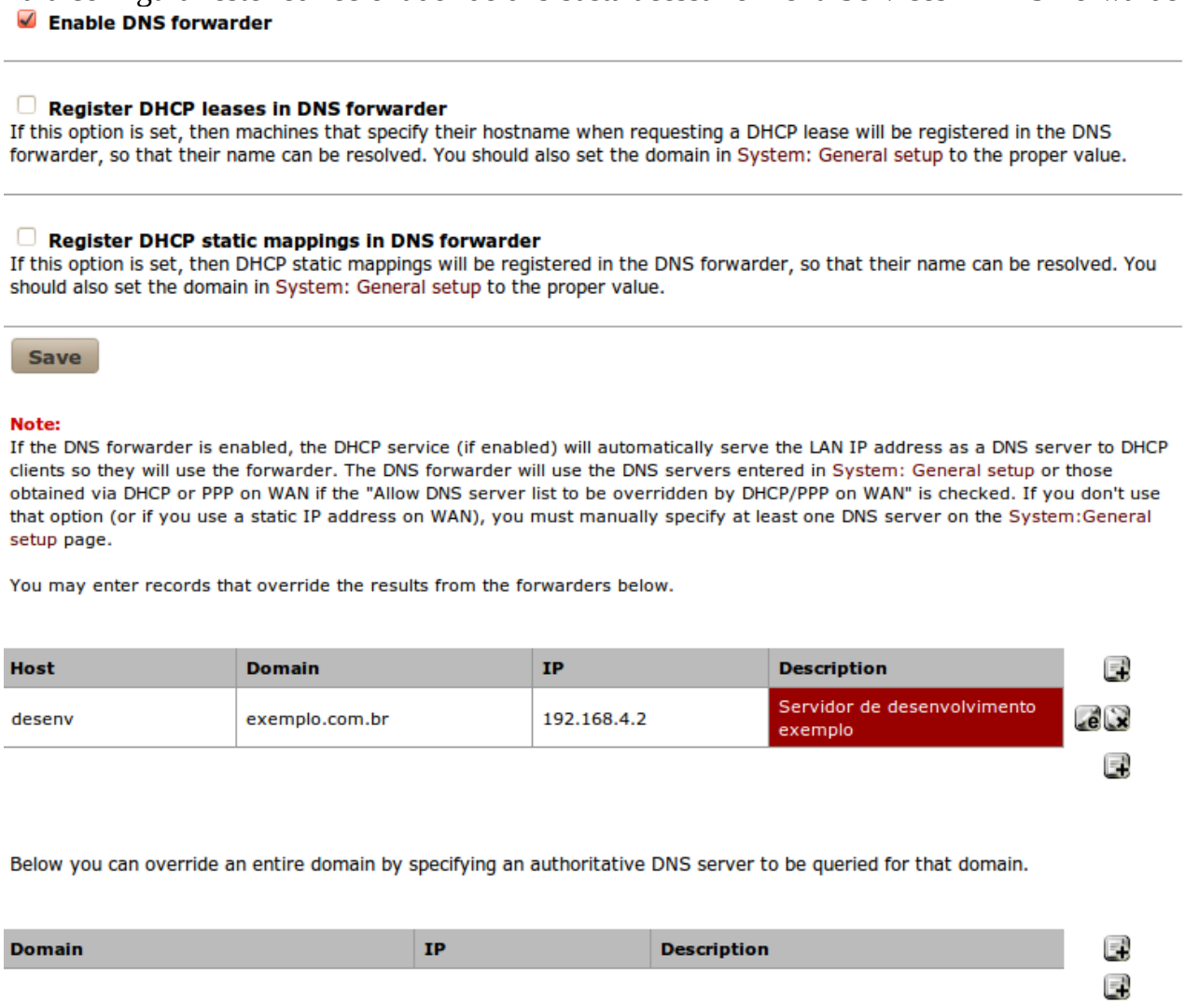
- **Enable DHCP server on LAN interface**
    - Essa opção habilita a utilização do servidor DHCP na respectiva interface.
- **Deny unknown clients**
    - Com esta opção habilitada apenas os clientes “fixos” com MAC e IP cadastrados mais abaixo irão receber “DHCP leases”.
- **Range**
    - Esta opção define o range de IPs disponíveis para a distribuição. É importante observar os campos acima **Subnet**, **Subnet mask** e **Avaiable range** que mostram as informações para a definição desta opção.
- **WINS servers**
    - Esta opção é utilizada para definir o servidor WINS (Windows Internet Name Service) da rede local (se existir um).
- **DNS servers**
    - Pode-se utilizar essa opção com dois DNS's ou deixar em branco. Se os campos não forem preenchidos o DNS que será distribuído para os clientes será o IP do firewall, que quando o cliente realizar uma consulta essa requisição irá para o

firewall e o firewall redirecionará a consulta para o DNS real, logo seria um tipo de encaminhamento.

- **Gateway**
  - Essa opção é utilizada para definir um gateway que será distribuído para os clientes. Se nenhum gateway for especificado o IP da interface (No caso aqui exemplificado, da LAN).
- **Domain name**
  - Pode-se definir o domínio de rede que será distribuído para os clientes através desta opção.
- **Domain search list**
  - O servidor DHCP pode provê uma lista de pesquisa de domínios com essa opção.
- **Default lease time**
  - Controla o tempo de renovação dos IPs. O tempo definido neste campo será utilizado para uma verificação constante dos minutos ou segundos definidos, desta forma, se o computador com o IP não estiver mais em uso, este será disponibilizado para qualquer outro computador da rede local.
- **Maximum lease time**
  - Esta opção controla o tempo máximo que um cliente pode ficar com um IP.
- **Failover peer IP:**
  - Essa opção é utilizada para manter um servidor pfsense com dhcp ativo como backup. Essa opção é útil apenas quando utiliza-se CARP.
- **Static ARP**
  - Essa opção funciona de forma similar ao negar endereços MAC desconhecidos de obter “dhcp leases”.
- **Dynamic DNS**
  - É possível utilizar um DNS dinâmico de domínio que será utilizado para registrar nomes de clientes no servidor DNS com essa opção.
- **NTP servers**
  - Para inserir um ou mais servidores NTP (Network Time Protocol Servers) basta utilizar essa opção clicando no botão Advanced.
- **TFTP server**
  - Caso exista algum servidor TFTP, pode-se especifica-lo neste campo.
- **LDAP URI**
  - Pode-se integrar o serviço de DHCP com o LDAP através dessa opção. É necessário especificar o caminho completo (LDAP URI, Uniform Resource Identifier) como por exemplo ldap://ldap.exemplo.com/dc=exemplo,dc=com
- **Enable network booting**
  - Pode-se utilizar essa opção para inserir os endereços IP das imagens de boot disponíveis e o nome da imagem de boot.
- **Additional BOOTP/DHCP Options**
  - Qualquer outra opção para o servidor DHCP pode ser adicionada neste campo. A lista dessas opções é encontrada neste endereço http://www.iana.org/assignments/bootp- dhcp-parameters/bootp-dhcp-parameters.xml

11.4 DNS Forwarder

Pode-se utilizar um redirecionador de DNS para consultas a nomes. A utilização do DNS forwarder geralmente se faz presente quando um cliente da rede local necessita consultar um nome de outra rede que possui uma ligação com a que o cliente se encontra. Desta forma, ao consultar por exemplo desenv.exemplo.com.br o IP retornado é 200.199.140.22, mas sabendo que existe uma ligação desta rede com a outro que o servidor desenv.exemplo.com.br pertence pode-se adicionar um redirecionamento de DNS e desta forma o nome seria resolvido por exemplo para 192.168.4.2. Logo, sua função é resolver o DNS e coloca em cache.
Para configurar este redirecionador de dns basta acessar o menu Services > DNS Forwarder:



Antes de qualquer explicação é importante notar que a opção Enable DNS Forwarder está marcada para a utilização do mesmo.

Neste caso foi adicionado o host junto ao domínio. Também é possível adicionar um domínio inteiro mais abaixo.

Ao clicar no botão para adicionar o host junto ao domínio existem as seguintes opções de configuração:

- **Host**
  - Host que faz parte do domínio. Também considerada a primeira parte antes do ponto no nome, como por exemplo desenv em desenv.exemplo.com.br ou www em www.exemplo.com.br.
- **Domain**
  - Domínio no qual o host se faz presente, no citado acima exemplo.com.br.
- **IP address**
  - Endereço IP para o qual o nome será resolvido. No caso citado acima 192.168.4.2.
- **Description**
  - Uma breve descrição sobre o redirecionamento criado.

11.5 Load Balance

Uma prática muito utilizada quando se têm dois links de internet é criar um balanceamento de carga para que a rede local não se torne lenta com o consumo de banda. O pfSense disponibiliza uma ferramenta integrada para isso. Em suas versões anteriores a criação do Load Balance era feita através do menu Services > Load balance, mas em sua versão 2.0 a configuração é feita em System > Routing, segmentado qualquer configuração com este fim para uma melhor utilização.

Existem três abas para a utilização no menu citado acima, Gateways, Routes e Groups. As abas utilizadas para a criação de um balanceamento de carga são descritas abaixo:

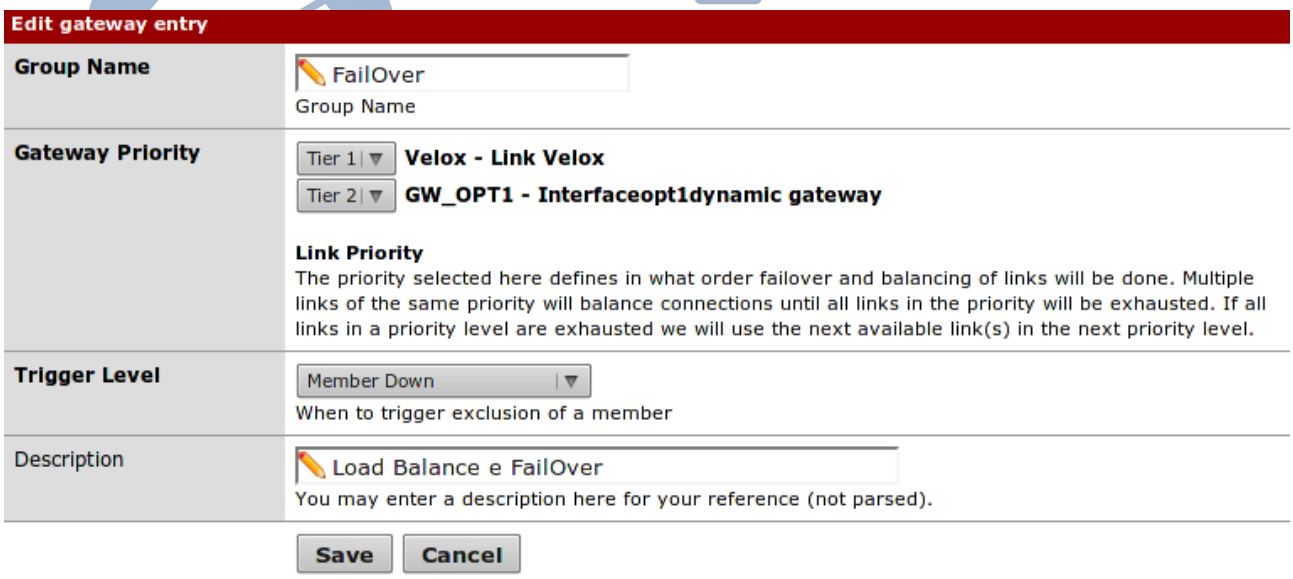
- **Gateways**
  - Aba utilizada para a criação dos gateways a serem utilizados pelas interfaces de saída (WAN, WAN2, e outras). São utilizados no mínimo dois links para a realização de um balanceamento de carga, logo são necessários dois gateways. Para a criação de um gateway deve-se clicar no botão add para então preencher e selecionar as seguintes opções:
    - Interface
      - É utilizada nesta opção a interface correspondente ao link de internet em questão.
    - Name
      - Pode-se definir um nome para o gateway em questão nesta opção.
    - Gateway
      - Nesta opção deve-se definir de fato o gateway do link de internet.
    - Default Gateway

        - Pode-se marcar essa opção para que este seja o gateway padrão.
    - Monitor IP
        - Para a verificação do link de internet, se este está ativo ou não é realizado um teste de ping (utilizando o protocolo ICMP) para o IP de verificação aqui definido, se este não responder a requisição o link será considerado como inativo.
    - Advanced
        - Pode-se definir opções avançadas para a configuração do gateway, um exemplo seria a definição da possível latência.
    - Description
        - Nesta opção defini-se uma breve descrição do gateway.
- **Groups**
    - Um grupo de gateways pode ser utilizado para uma junção de links de internet com o objetivo de criar um Load balance ou um FailOver. Para a criação de um grupo de gateways basta clicar no botão add, e em seguida preencher e selecionar as opções:
        - Group Name
            - Deve-se definir um nome para este grupo, como por exemplo LoadBalance.
        - Gateway Priority
            - A prioridade a ser definida para o Load Balance deve ser de 1 (um) para os dois gateways.
        - Trigger Level
            - Existem quatro possibilidades nesta opção para a realização de uma ação:
                - Member down
                    - Quando um dos gateways estiver offline.
                - Packet Loss
                    - Quando houver uma perda significativa de pacotes.
                - High Latency
                    - Quando uma alta latência for detectada em um dos gateways.
                - Packet Loss or High Latency
                    - Quando uma perda de pacote ou uma alta latência for detectada.
        - Description
            - Deve-se definir uma breve descrição do grupo de gateways em questão.

11.6 FailOver

Esta técnica é utilizada para efetuar uma redundância de links de internet, desta forma o segundo link de internet irá servir como uma espécie de backup. O FailOver pode ser configurado através do menu System > Routing.

A configuração do FailOver é feita da mesma forma que a configuração do balanceamento de carga com exceção da opção Gateway Priority que é selecionada na criação do grupo de gateways. Após efetuar a criação dos gateways (A criação de gateways pode ser visualizada no tópico 11.5) deve-se criar o grupo de gateways (Também pode ser visualizado no tópico 11.5), porém nesta opção deve definir a prioridade dos gateways, onde o gateway principal ficará com a prioridade 1 (Um) e o gateway secundário (Gateway respectivo do link de internet utilizado como backup) deverá ficar com prioridade 2 (Dois), para um melhor entendimento pode-se visualizar a parte da criação de um grupo de gateways para a utilização do FailOver abaixo:

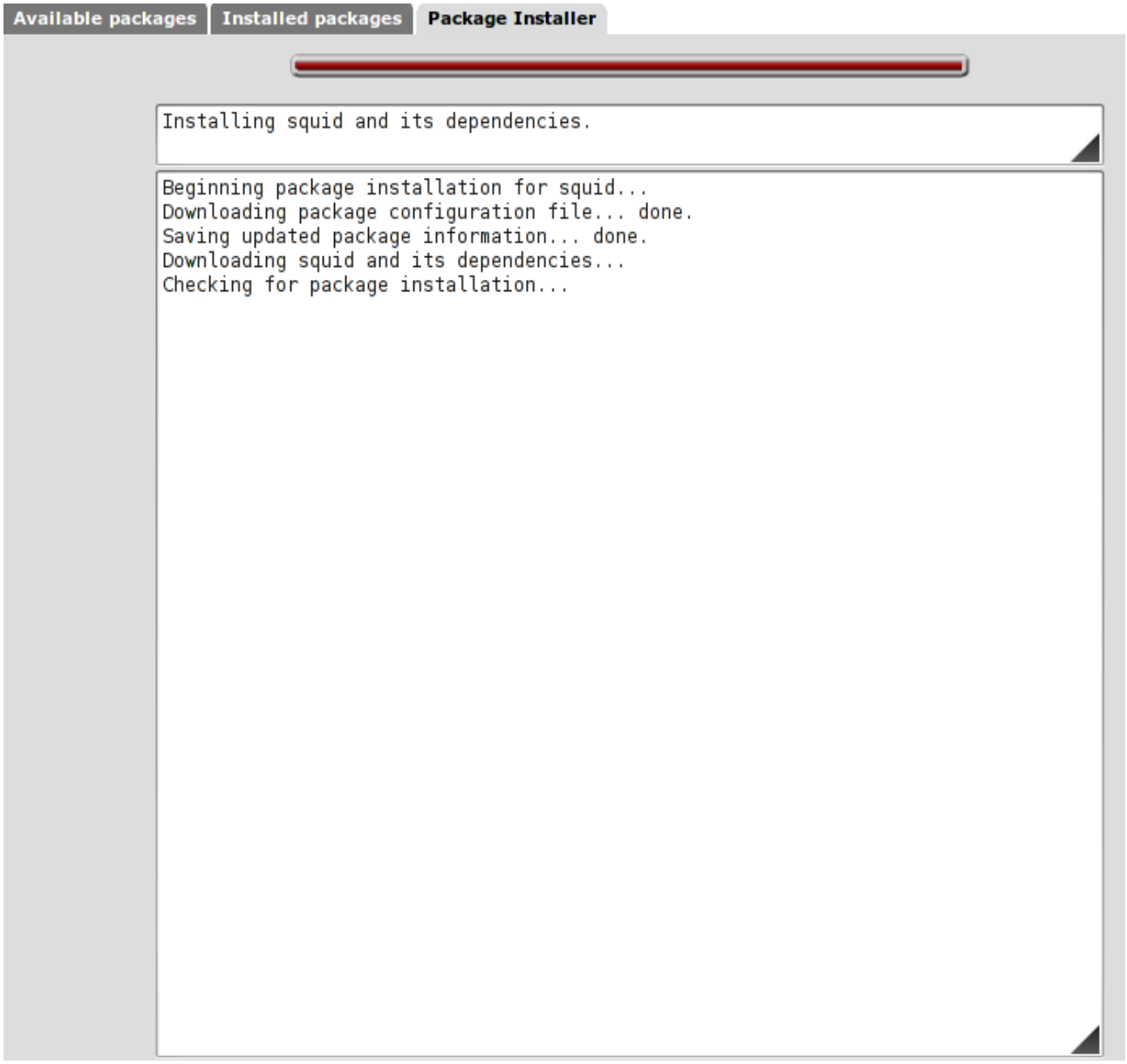


É possível perceber a prioridade dos gateways como 1 (Tier 1) e 2 (Tier 2) e ainda o Trigger Level que foi definido como Member Down, ou seja, quando o primeiro link estiver com status offline o segundo irá assumir.

11.7 Proxy Server

Para efetuar a instalação do serviço proxy integrado ao pfSense basta acessar o menu System > Packages e localizar o pacote squid. Ao localizar o pacote squid deve-se clicar no botão add ao lado do pacote para efetuar a instalação do mesmo, logo será feita a pergunta

Do you really want to install this package? Para continuar basta clicar no botão de resposta OK. Iniciando a instalação será visualizado o progresso:



Após efetuar a instalação do pacote Squid o mesmo será encontrado para configuração no menu Services > Proxy Server. Ao acessar o menu para configuração do servidor proxy, a aba General será visualizada por padrão, porém existem outras abas para configuração onde estas são descritas abaixo:

- **General**
  - Esta é a aba principal de configuração para o funcionamento do servidor proxy. Nesta aba são definidas várias opções importantes, por exemplo em qual interface o proxy irá trabalhar, onde os logs serão armazenados ou se o proxy será transparente, etc.

- **Upstream Proxy**
  - Se é utilizado um servidor de upstream essa aba irá ser útil a partir da primeira opção que trás uma boa descrição de sua funcionalidade: This option enables the proxy server to forward requests to an upstream server (Essa opção habilita o servidor proxy encaminhar requisições para um servidor upstream).
- **Cache Mgmt**
  - Essa aba é utilizada para o gerenciamento de cache do servidor proxy.
- **Access Control**
  - O controle de acesso é configutado nessa aba, desta forma pode-se definir qual a rede que poderá utilizar o servidor proxy, assim como os Ips que serão excluídos de qualquer regra de bloqueio. Pode-se também definir uma whitelist ou uma blacklist.
- **Traffic Mgmt**
  - O gerenciamento de tráfego é feito nesta aba, várias opções são possíveis como por exemplo definir o tamanho máximo de download ou o máximo de upload por parte dos usuários do proxy.
- **Auth Settings**
  - Caso não seja marcada a opção Transparent Proxy da aba General, a autenticação é possível de três formas:
    - Local
    - LDAP
    - RADIUS
    - NT Domain
- **Local Users**
  - Se a autenticação selecionada for Local, essa aba é utilizada para definir os usuários e suas respectivas senhas de acesso.

Para um melhor entendimento serão explicadas as opções mais utilizadas em um servidor proxy no pfSense:

- **Aba General**
  - Proxy interface
    - É necessária a escolha da interface que o proxy irá trabalhar. Na maioria dos casos esta opção é selecionada como LAN.
  - Allow users on interface
    - Essa opção geralmente é marcada, pois esta libera o uso de clientes nesta interface.
  - Transparent proxy
    - Existe a possibilidade da utilização do proxy sem autenticação. Este tipo de proxy é reconhecido como proxy transparente, onde esta opção é marcada para esta utilização.
  - Enabled logging

        - Essa opção habilita a criação e armazenamento de logs de acesso.
    - Log store directory
        - Pode-se definir nesta opção um outro diretório de armazenamento para os logs, sabendo que o padrão é /var/squid/logs.
    - Proxy port
        - A porta padrão do proxy é 3128, mas é possível alterar esta.
    - Visible hostname
        - Essa é a opção referente a URL que é exibida nas mensagens de erro do proxy.
    - Administrator e-mail
        - Esse é o e-mail fornecido para contato nas mensagens de erro.
    - Language
        - Idioma utilizado para a visualização do Proxy.
    - What to do with requests that have whitespace characters in the URI
        - Essa opção geralmente é deixada como padrão (strip), para o tratamento de caracteres com espaços.
    - Use alternate DNS-servers for the proxy-server
        - Pode-se definir um servidor DNS alternativo para o proxy com esta opção.
    - Custom Options
        - Caso seja necessário definir alguma opção no arquivo de configuração do proxy, basta digitar as opções nesta caixa de texto.

- **Aba Access Control**
    - Allowed subnets
        - É necessário preencher quais redes terão acesso para a utilização do proxy nesta opção.
    - Unrestricted Ips
        - Pode-se excluir da filtragem do proxy alguns IPs nesta opção.
    - Banned host addresses
        - Com esta opção é possível definir os IPs que não terão acesso ao proxy, serão banidos.
    - Whitelist
        - Pode-se definir domínios liberados para acesso dos usuários. Por padrão o squid já libera todos os domínios, logo só é necessário utilizar a opção abaixo, para bloquear determinados domínios.
    - Blacklist
        - Essa opção é utilizada para especificar os domínios proibidos. Geralmente são utilizados domínios de acordo com a política da empresa, como sites adultos, sites com vídeos, onde estes irão consumir boa parte da banda se os usuários estiverem acessando.

- **Aba Auth Settings**
    - Authentication method

        - Essa opção irá definir quais campos mais abaixo serão utilizados. Existem algumas opções como: None, Local, LDAP, RADIUS, NT Domain.
    - Authentication server
        - IP do servidor de autenticação.
    - Authentication server port
        - Porta utilizada para a comunicação com o servidor de autenticação.

- **Local Users**
    - Username
        - Usuário para utilização do proxy.
    - Password
        - Senha para o usuário do proxy.
    - Description
        - Breve descrição sobre o usuário.

11.8 Snort

O snort é um sniffer que pode ser integrado ao pfSense se tiver seu pacote instalado através do menu System > Packages. A função de um sniffer é observar o tráfego da rede agindo de forma silenciosa para a coleta de dados. Ao efetuar a instalação, este poderá ser encontrado em **Services > Snort**. Porém, antes de acessar o menu para efetuar a configuração é notável a mensagem que é exibida ao finalizar a instalação:

"Please visit the Snort settings tab and enter your oinkid code. Afterwards visit the update rules tab to download the snort rules."

Logo, deve-se efetuar a configuração incial que a mensagem recomenda. Acesso o menu citado acima para a configuração do Snort e então clique na aba **Global Settings**. As seguintes opções são exibidas:

- **Install Snort.org rules**
    - É necessário obter o Oinkcode, onde este é utilizado para conhecimento de quem está utilizando as regras do snort, logo, é necessário criar um login no site www.snort.org para então conseguir um Oinkcode. Com o código em mãos, como este: d53ab786f11cdd347889f05f9b15f2611e5aa979, basta adicionar este no campo **Code**, e depois selecionar se serão instaladas as regras básicas ou premium, onde este é o recomendado, caso não tenha interesse basta deixar a opção default marcada **Do NOT Install**.
- **Install Emergingthreats rules**
    - Essa opção é utilizada se além das regras default desejá-se instalar as regras Emergingthreats, essas são criadas pela comunidade e possuem várias opções de filtro.
- **Update rules automatically**
    - É possível definir a atualização automática das regras através desta opção. Por padrão, as

regras nunca são atualizadas.

- **Log Directory Size Limit**
  - É possível definir o limite de tamanho do diretório utilizado para armazenar o log nesta opção. Por padrão o tamanho definido é correspondente a 20% do tamanho total do disco rígido.
- **Remove blocked hosts every**
  - Essa opção é utilizada para desbloquear hosts que tiveram seu acesso negado e bloqueado pois caíram em algum filtro das regras existentes e selecionadas na configuração.
- **Alerts file description type**
  - Por padrão a opção **FULL** é selecionada e recomendada, pois essa opção define como a descrição do alerta será exibida no arquivo de alertas. Ao selecionar a opção default a descrição terá uma melhor visualização, pois esta será completa. Se a outra opção **SHORT** for selecionada, o alerta não será totalmente exibido, ao invés disto será exibido um pequeno alerta, como um resumo do fato ocorrido.
- **Keep snort settings after deinstall**
  - Com está opção selecionada, ao desinstalar o pacote snort as opções definidas serão salvas. Caso este pacote seja instalado novamente as configurações serão restauradas.

Ao finalizar a configuração desta aba, basta clicar em **Save** para salvar as configuraões feitas até então. É necessário dar um update nas regras para que estas sejão de fato instaladas e disponibilizadas. Para efetuar este passo clique em **Updates** e no botão **Update rules**, logo será iniciado o download destas.

O próximo passo é clicar na primeira aba, **Snort Interfaces**, onde esta é utilizada para especificar em qual interface de rede o snort irá trabalhar. Para adicionar as informações necessárias clique no botão utilizado para adição com o ícone "+". As opções abaixo serão exibidas:

- **Enable**
  - Habilita o uso da interface que será definida na opção abaixo.
- **Interface**
  - Nesta opção defini-se em qual interface o Snort irá trabalhar. Geralmente definise a interface de saída (WAN) ou qualquer outra que trabalhe diretamente com a saída para a internet.
- **Description**
  - Este campo é utilizado para definir uma breve descrição sobre a interface que será monitorada.
- **Block offenders**
  - Habilitando essa opção, qualquer alerta gerado pelo snort será automaticamente bloqueado através do firewall. É necessário ter cuidado com o filtro definido pelo o snort, pois qualquer alerta gerado mesmo que por engano terá um efeito de bloqueio.

Existem outras opções, porém estas são as mais utilizadas para a definição da interface que será utilizada pelo Snort.

12. VPN

A conectividade através de VPNs tem o objetivo de interligar redes e hosts. Basicamente existem três métodos de interligação de redes e/ou hosts através de VPN, onde estes podem ser definidos pelas possibilidades apresentadas de cada tipo de VPN:

- **Host-Host**
  - Neste tipo, é criada uma conexão entre dois hosts para uma melhor comunicação.
- **Host-Rede**
  - Neste modelo, é criada uma conexão onde um host irá ter acesso até uma rede. Desta forma, um host na internet pode criar uma conexão, e através de uma autenticação ou não, este irá conseguir acesso até a rede de computadores lógica alvo.
- **Rede-Rede**
  - Este modelo é muito utilizado em organizações, onde estas possuem filiais. Desta forma, duas filiais podem estar conectadas 24 (Vinte e quatro) horas por dia, sem a necessidade de criar conexão.

O pfSense já disponibiliza após suas instalação alguns tipos de VPN, estes serão abordados nos respectivos subtópicos abaixo.

12.1 PPTP

Point-to-Point Tunneling (PPTP) é utilizado para a criação de uma VPN mais simples, pois esta não disponibiliza uma alta segurança como em outros protocolos, pois só é possível configurar uma criptografia de 128 bits. Basicamente, o usuário cria uma conexão do tipo VPN PPTP, e então conecta utilizando um usuário e senha.

A configuração é feita através do menu **VPN > PPTP**, e as opções de configuração da aba *Configuration*:

- **PPTP redirection**
  - Através desta opção é possível encaminhar uma requisição de VPN PPTP para outro servidor VPN, bastando definir o IP do servidor em questão.
- **No. PPTP users**
  - Ao habilitar a utilização da VPN PPTP através da opção Enable PPTP server, é possível definir um número de usuários para a VPN, onde por padrão o número de usuários é igual a 16.
- **Server address**
  - Esta opção é utilizada para definir um gateway para os clientes da VPN PPTP.
- **Remote address range**
  - Utiliza-se esta opção para definir qual será o primeiro IP disponibilizado para clientes da VPN.
- **PPTP DNS Servers**
  - É possível utilizar um ou dois servidores DNS que serão distribuídos para os clientes da VPN.
- **WINS Server**

  - Se houver algum servidor WINS, esta opção é utilizada para especificar este.
- **RADIUS**
  - A autenticação pode ser centralizada com a utilização de um servidor RADIUS em rede, seja ele em um servidor remoto ou no próprio firewall com este serviço (pacote) instalado.
- **Require 128-bit encryption**
  - Ativa a criptografia de 128 bits.

12.2 OpenVPN

Este tipo de VPN é considerada como Rede-Rede, onde é possível interligar unidades, como uma filial e sua matriz. É considerado um tipo seguro de transmitir dados com uma alta criptografia, este tipo de VPN pode ser considerado uma ótima opção para utilização em ambientes corporativos.

Para efetuar a configuração de uma VPN OpenVPN no modelo aqui apresentado, dois firewalls pfSense serão utilizados, onde um fará o papel da matriz e o outro da filial respectivamente. A matriz será o servidor OpenVPN, enquanto a filial será apenas um cliente, desta forma é possível integrar várias filiais nesta VPN. Para iniciar, a configuração pela parte da matriz tem início com acesso ao menu **VPN > OpenVPN**, então a aba a ser utilizada será *Server*, clicando no botão para adicionar o servidor, as seguintes opções estarão disponíveis:

- **Disabled**
  - É possível desabilitar o servidor mesmo na criação deste marcando esta opção.
- **Server Mode**
  - O modo do servidor geralmente é definido como Peer to Peer (Shared key), onde este irá compartilhar uma chave gerada pelo próprio pfSense, com o cliente. Então, estes dois irão se comunicar. Pode-se selecionar outro modo como Peer to Peer (SSL/TLS), Remote Access (SSL/TLS).
- **Protocol**
  - É necessário definir um protocolo (UDP ou TCP), onde geralmente o protocolo UDP é selecionado.
- **Device Mode**
  - Esta opção por padrão já esta definida como tun, pois na maioria dos casos é utilizada desta forma.
- **Interface**
  - Esta opção geralmente é definida como WAN, pois esta interface precisa ter conexão direta com a interface de saída do cliente.
- **Local port**
  - A porta local pode ser modificada, porém é utilizada por padrão 1195.
- **Description**

    - Pode-se definir uma descrição para a utilização da VPN utilizando esta opção.
- **Shared Key**
    - Ao selecionar a opção Server Mode como Peer to Peer (Shared key) algumas opções não estarão mais disponíveis, logo a opção shared key é exibida, onde esta pode ser definida como Automatically generate a shared key. Desta forma, o pfSense irá gerar automaticamente uma chave de segurança.
- **Encryption algorithm**
    - Uma boa criptografia é selecionada por padrão, AES-128-CBC (128-bit), porém existem várias outras opções para seleção.
- **Hardware Crypto**
    - É possível definir criptografia de hardware para o dispositivo através desta opção.
- **Tunnel Network**
    - É necessário definir uma rede para a comunicação privada através do túnel. Pode-se definir esta rede através desta opção.
- **Local Network**
    - Nesta opção, defini-se a rede local, especificando a faixa e a máscara de rede.
- **Remote Network**
    - A definição da rede remota é feita nesta opção, onde se a rede cliente é representada por 192.168.10.0/24, esta precisa ser especificada no campo desta opção.
- **Concurrent connections**
    - Esta opção é utilizada para especificar o número máximo de clientes permitidos para conectar ao mesmo tempo no servidor.
- **Compression**
    - É possível utilizar a compressão no túnel utilizando o algorítimo LZO.
- **Type-of-Service**
    - Define um cabeçalho no pacote que irá passar pelo túnel para comparar de forma correta com o valor dos pacotes encapsulados.
- **Duplicate Connections**
    - Permite várias conexões ao mesmo tempo dos clientes que utilizam o mesmo nome.
- **Advanced**
    - Pode-se definir opções avançadas nesta opção, onde estas serão inseridas no arquivo de configuração da VPN.

O último passo seria criar uma regra na interface de saída do firewall onde o servidor VPN, onde seria liberada a porta 1194 no protocolo UDP (Origem).

12.3 IPSec

IPSec (IP Security Protocol) é uma extensão do protocolo IP, onde este provê segurança no nível da camada IP para comunicações através da Internet. Este é parte obrigatória do Ipv6, porém, no Ipv4 o uso é opcional. É considerada uma ótima opção, senão a melhor para a

interligação de unidades, utilização de VPN no modelo rede-rede.

Para iniciar a configuração da interligação entre matriz e filial, deve-se acessar o menu **VPN > IPSec**, e então clicar no botão adicionar na aba Tunnels para criar uma VPN IPSec. Logo, as opções necessárias para a criação e funcionamento da VPN são listadas abaixo:

- **Interface**
  - A interface aqui utilizada precisa ter conexão direta com a internet para a comunicação com a outra ponta da VPN, neste caso deve-se utilizar a interface WAN na maioria dos casos.
- **Remote gateway**
  - Este é definido pelo IP remoto do segundo firewall, onde é criada a conexão (ponte).
- **Description**
  - Este campo é utilizado para inserir uma breve descrição da VPN criada.
- **Pre-Shared Key**
  - Deve-se definir um password para a segurança na comunicação entre as pontas da VPN.

Após finalizar a primeira etapa da configuração da VPN do tipo IPSec, deve-se clicar no botão adicionar localizado abaixo da informação da VPN, desta forma deve-se clicar novamente no botão exibido de adição, desta forma serão exibidas as opções para a identificação da rede local e remota:

- **Mode**
  - O modo é definido como Tunnel, logo é criado um túnel entre a rede local do firewall atual e a rede local do firewall remoto.
- **Local Network**
  - A rede local pode ser definida digitando o endereço de rede com sua respectiva máscara ou simplesmente selecionando LAN subnet em Type.
- **Remote Network**
  - Defini-se em Network na seleção da opção Type, então deve-se definir o endereço de rede e a máscara da rede remota.
- **Description**
  - Deve-se inserir uma breve descrição sobre a rede remota que está sendo configurada.

Ao finalizar esta configuração, deve-se clicar em Save para salvar as alterações feitas. Para finalizar a configuração da VPN e então criar as regras necessárias é necessário habilitar a VPN marcando a opção Enable IPSec e então clicar em Apply changes.

Após configurar de forma correta a VPN IPSec, deve-se criar uma regra na aba IPSec, onde esta deverá ter a função de liberar a comunicação na interface. A configuração feita até

então tem que ser efetuada nas duas pontas do túnel (Nos dois firewalls). Após finalizar toda a configuração, tanto da matriz quanto da filial, deve-se checar o status em Status > IPSec, caso o sinal de funcionamento esteja diferente de verde, é necessário verficar a configuração e tudo feito até então, e então iniciar clicando no botão específico desta tela para tal ação.

13. QoS

QoS (Quality of Service), refere-se a vários aspectos ligados a telefonia e redes de computador. Este é extremamente utilizado na limitação da navegação de redes, onde é possível definir por exemplo a utilização da banda através do download e upload que a rede local poderá utilizar.

13.1 Traffic Shaper

Para utilizar o Traffic Shaper no pfSense basta acessar o submenu Firewall > Traffic Shaper, e efetuar a configuração para o controle de banda de acordo com a respectiva necessidade da rede local, desta forma priorizando os pacotes necessários. Geralmente a opção escolhida se encontra na linha da coluna Single Wan multi Lan, definida pelo nome traffic_shaper_wizard_multi_lan.xml. As opções por etapas são definidas abaixo:

- **Enter number of LAN type connections**
  - Deve-se definir o número de redes existentes, como por exemplo 2 (dois), LAN e DMZ.
- **Link Upload**
  - Deve-se informar o tamanho da banda que será utilizada para upload.
- **Link Download**
  - Deve-se informar o tamanho da banda que será utilizada para download.
- **LAN interface**
  - **Nesta opção deve-se definir a interface da rede local (LAN).**
- **VoIP**
  - As opções da próxima tela só são utilizadas quando se quer definir um QoS para VoIP. Então defini-se a velocidade de upload e download. Se não for o caso, basta clicar em Next para prosseguir até a próxima etapa.
- **Penalty Box**
  - Permite reduzir a prioridade de um endereço IP em particular ou de um alias.
- **Peer to Peer networking**
  - É possível ter controle também sobre o tráfego P2P nesta tela através das opções que são apresentadas.
- **Network Games**
  - Também é possível ter controle sobre jogos em rede através destas opções.
- Raise or lower other Applications
  - Esta tela é utilizada com a configuração respectiva da rede local para outras

aplicações que não foram listadas nas telas anteriores.

Por fim, o botão Finish é exibido para ao clicar, finalizar a configuração de QoS.

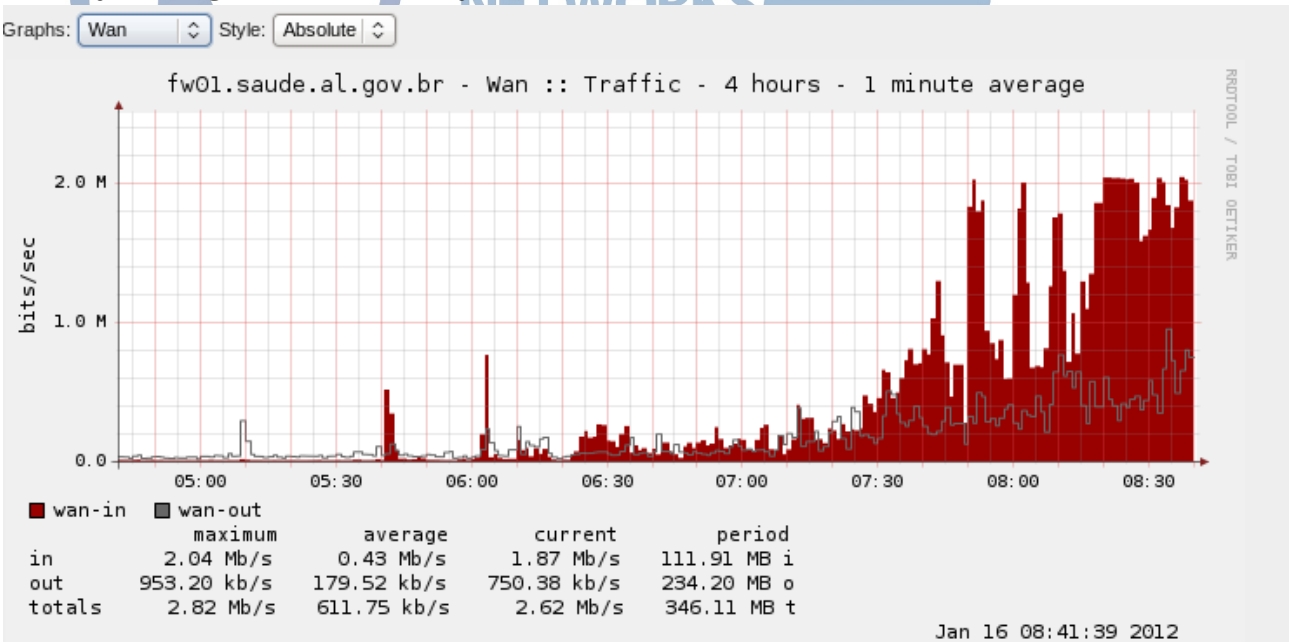
14. Monitoramento

É de extrema importância que exista um monitoramento via rede, mas também é muito importante que o administrador da rede responsável pelo firewall verifique os logs, acesso dos clientes, o status das interfaces e dos hosts, assim como os links de internet, porém mais importante que isso é saber por onde começar quando houver algum problema. Este tópico cobre os tipos possíveis de monitoramento com o pfSense.

14.1 Link

Os gateways criados no submenu *Routing* dentro do menu *System* podem ser visualizados com seus respectivos status através do menu *Status* > *Gateways*, além de exibir o status e outras informações como a qual interface este gateway pertence, e também qual o IP que está sendo utilizado para monitorar se o gateway está online ou não, outras abas são exibidas para mostrar informações das rotas e os grupos de gateways.

O pfSense também apresenta gráficos dos links, para uma melhor análise do tráfego. É possível visualizar como anda o tráfego relacionado ao upload e download de cada interface ou de todas através do menu *Status* > *RRD Graphs*. A aba Traffic deve ser selecionada para a exibição dos gráficos da utilização das interfaces:



O download é representado pela parte vermelha do gráfico, e o upload pela linha cinza exibida, onde outras informações podem ser visualizadas abaixo do gráfico.

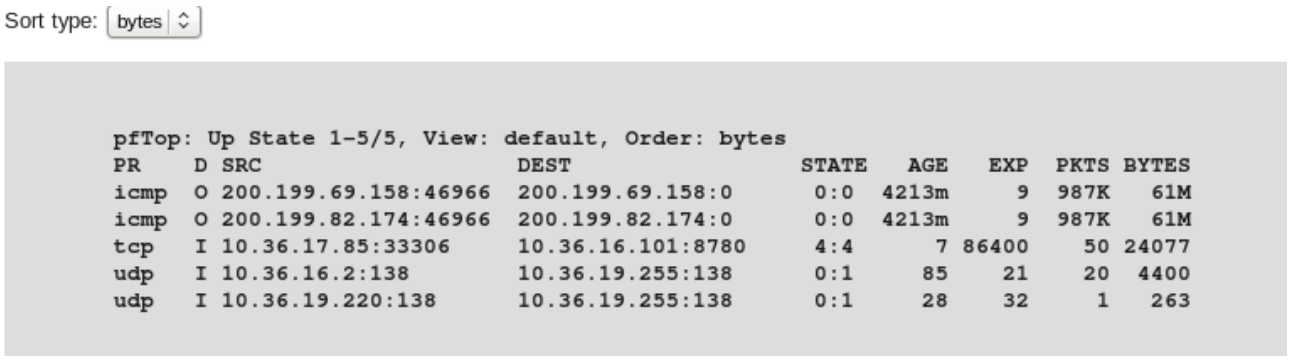
14.2 Interfaces

O submenu *Status>Interfaces* exibe informações sobre as interfaces reconhecidas pelo pfSense, onde através deste é possível virtualizar:

- **Status**
  - Mostra o status da interface, onde esta pode estar up ou down (no carrier).
- **MAC address**
  - O MAC da placa de rede sobre a interface em questão é exibido aqui.
- **IP address**
  - Aqui, o IP é exibido.
- **Subnet mask**
  - A máscara de rede da interface pode ser visualizada aqui.
- **Gateway**
  - O gateway é exibido neste campo.
- **ISP DNS servers**
  - Os servidores DNS são exibidos neste campo.
- **In/out packets**
  - É possível visualizar os pacotes que estão entrando e saíndo da rede de computadores através do firewall aqui.
- **In/out packets (pass)**
  - Neste campo o filtro com os pacotes que tiveram sua entrada permitida são exibidos aqui.
- **In/out packets (block)**
  - Neste campo são exibidos apenas os pacotes que tiveram sua entrada e/ou saída bloqueada.
- **In/out errors**
  - Se houver algum erro na entrada ou saída de pacotes, estes serão apresentados neste campo.
- **Collisions**
  - Se houver alguma colisão entre pacotes, esta opção irá exibir estes.

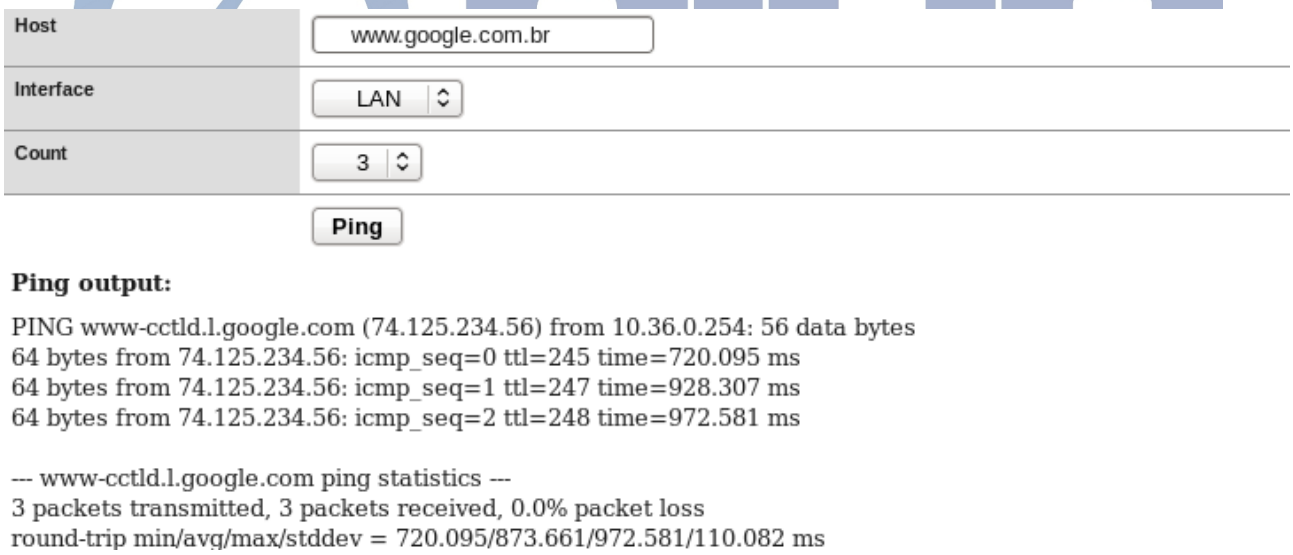
14.3 pfTop

Este é utilizado para monitorar a largura de banda e o tráfego de rede, onde é possível ver informações do tráfego com origem, destino, status, pacotes e mais. Existem várias opções para a visualização das informações, onde a padrão é representada por bytes. É interessante utilizar mais esta opção que o pfSense disponibiliza quando pretende-se obter informações de um IP em específico em uma visualização do tráfego da rede sem gráfico, pois todas informações são exibidas em tempo real, sem ter a necessidade de atualizar a página e/ou entrar e sair dos menus para visualizar os dados de forma atualizada:



14.4 Ping

O ping é uma ferramenta básica que dá um retorno com uma resposta positiva ou negativa. Este geralmente é utilizado para verificar se há ou não conectividade entre a comunicação do host de origem e o host de destino. Um exemplo básico, seria utilizar essa ferramenta para enviar pacotes ao google, desta forma se a resposta for positiva, significa que o firewall está conectado à internet. Para a utilização deste, deve-se acessar o menu *Diagnostics* > *Ping*. Este exemplo é exibido na imagem abaixo:



Na imagem acima é possível perceber que houve conectividade entre a origem (interface LAN do firewall) e o destino (Site do google). As opções para a utilização desta ferramenta no modo gráfico são definidas abaixo:

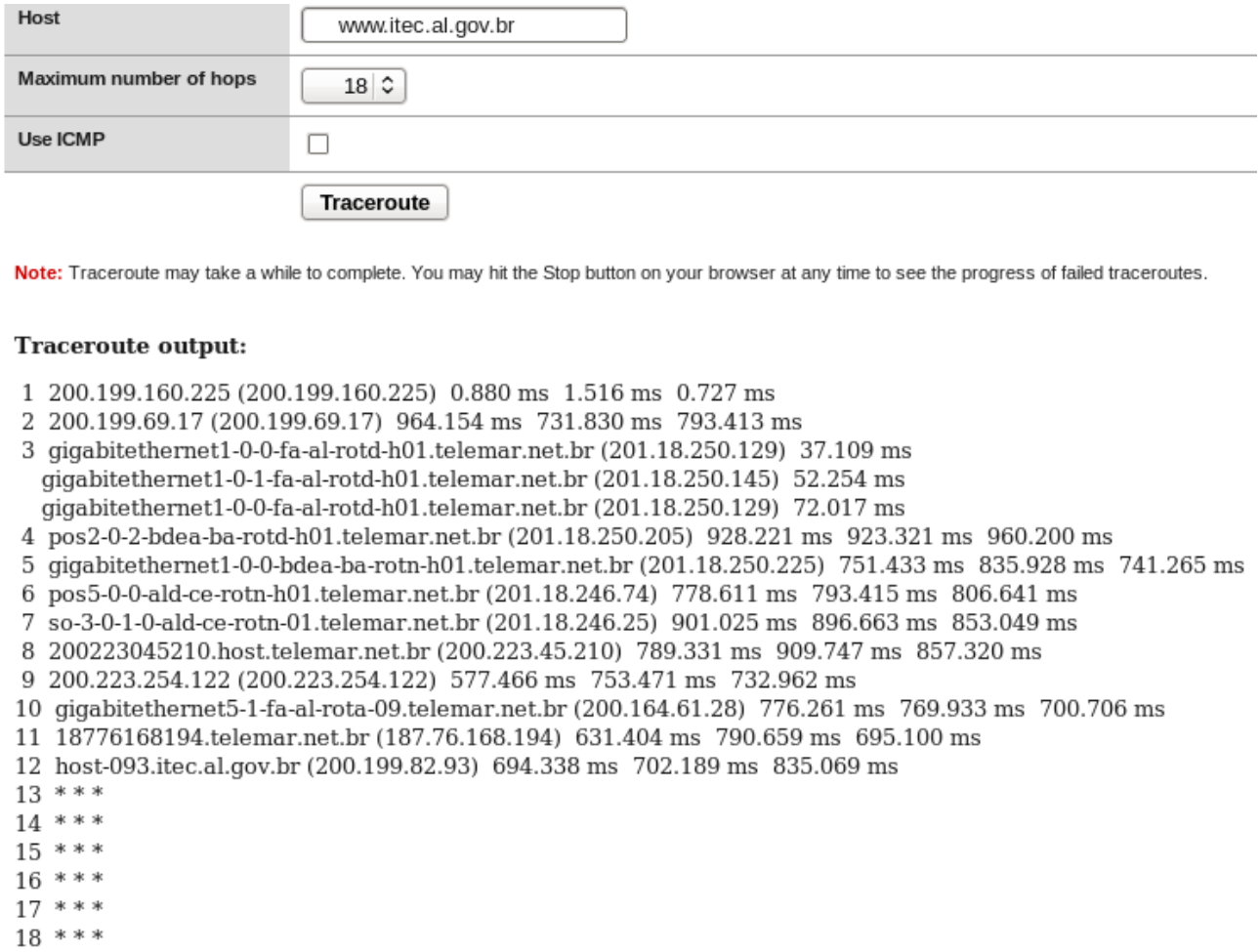
- **Host**
  - É o destino, para onde o firewall irá enviar pacotes para verificar se há retorno.
- **Interface**
  - Nesta opção defini-se qual interface será utilizar para verificar a conectividade entre esta e o destino especificado.

- **Count**
  - Esta opção especifica o número de saltos, a quantidade de pacotes enviados, que no caso da imagem acima foi definido o número 3 (três).

É válido lembrar que esta opção pode ser utilizada também na linha de comando com a opção 7 (sete), ou através da opção 8 (oito), digitando o comando ping.

14.5 Traceroute

Traceroute é utilizado para verificar o caminho, as rotas seguidas no caminho completo percorrido pelo pacote, este pode ser acessado através do menu *Diagnostics* > *Traceroute*, a imagem abaixo detalha um exemplo de utilização:



Neste exemplo é possível perceber que há uma perda de pacote após o host 200.199.82.93, logo isso pode ser causado por um bloqueio com um simples firewall ou o host pode não estar em funcionamento com conectividade.

15. Backup/Restore

O pfSense disponibiliza uma opção que pode ser acessada através do menu *Diagnostics* > *Backup/Restore*, onde através deste é possível efetuar um backup de toda configuração ou parte desta para então restaurar quando necessário. A utilização desta ferramenta é de extrema facilidade, e os subtópicos cobrem a utilização desta.

15.1 Backup

Ao acessar o respectivo menu, pode-se efetuar o backup da configuração atual do firewall clicando no botão Download Configuration, logo o backup poderá ser salvo no computador utilizado para acessar o firewall. Porém, existem algumas opções que pode customizar o backup:

- **Backup area**
  - Por padrão, o backup é feito de toda a configuração, porém é possível efetuar o backup por categorias, como por exemplo, backup apenas da configuração das interfaces, das regras NAT ou até mesmo apenas das informações do sistema. O ideal é que seja feito um backup geral, e outros de cada categoria.
- **Do not backup package information**
  - Essa opção geralmente é utilizada para diminuir um pouco o tamanho do backup, porém é interessante que esta não seja marcada, pois as informações dos pacotes são importantes para o sistema e para o administrador.
- **Encrypt this configuration file**
  - Com esta opção é possível criptografar o arquivo de configuração, logo o backup será bem mais seguro.
- **Do not backup RRD data**
  - Os gráficos geralmente ocupam uma grande parte do espaço utilizado no H.D, logo o backup deles não é recomendado pois aumentará o tamanho do arquivo de backup.

15.2 Restore

Após efetuar o backup da configuração do firewall, é possível restaurar este utilizando o mesmo menu: *Diagnostics* > *Backup/Restore*, utiliza-se as opções em Restore configuration, onde estas são explicadas abaixo:

- Restore area
  - Deve-se definir qual área será restaurada. Em caso de restauração de toda a configuração deve-se selecionar ALL (Que já é a opção padrão).
- Configuration file is encrypted
  - Se o arquivo de backup for criptografado, deve-se marcar esta opção.

Ao selecionar o arquivo, clicando em Browse, o próximo passo é clicar no botão Restore configuration, e logo as configurações serão restauradas.