UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

FILIPE CAMPOS DAS NEVES
LEONARDO ALVES MACHADO
RODRIGO DA FONTOURA CENTENARO

IMPLANTAÇÃO DE FIREWALL PFSENSE

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2014

FILIPE CAMPOS DAS NEVES
LEONARDO ALVES MACHADO
RODRIGO DA FONTOURA CENTENARO

IMPLANTAÇÃO DE FIREWALL PFSENSE

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2014

TERMO DE APROVAÇÃO

FILIPE CAMPOS DAS NEVES
LEONARDO ALVES MACHADO
RODRIGO DA FONTOURA CENTENARO

IMPLANTAÇÃO DE FIREWALL PFSENSE

Este trabalho de conclusão de curso foi apresentado no dia 09 de outubro de 2014, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
UTFPR

_____
Prof. MsC. Lincoln Herbert Teixeira
UTFPR

_____
Prof. Dr. Augusto Foronda
Orientador - UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

Às nossas famílias muito obrigado pela paciência, incentivo, força e carinho.

AGRADECIMENTOS

A Deus por ter nos dado saúde e força para superar as dificuldades.

Ao nosso orientador Prof. Dr. Augusto Foronda, pelo suporte e dedicação prestados, pelas suas correções e incentivos, e por meio dele nos reportamos a toda comunidade da Universidade Tecnológica Federal do Paraná (UTFPR) pelo apoio oferecido.

Aos nossos pais e familiares, pelo amor e incentivo incondicional, pois acreditamos que sem o apoio deles seria muito difícil vencer esse desafio.

E a todos que diretamente ou indiretamente fizeram parte da nossa formação, o nosso muito obrigado.

RESUMO

NEVES, Filipe Campos das, MACHADO, Leonardo Alves, CENTENARO, Rodrigo da Fontoura. Implantação de Firewall pfSense. 2014. 66 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Este trabalho apresenta pesquisas e aplicações necessárias para a implementação de um *Firewall* em *software* livre chamado pfSense em empresas que possuam menos receita para gastos na área de segurança, mas que mesmo assim necessitem de certa segurança para que seus dados sejam mantidos internamente ou trafeguem de forma segura para o ambiente externo. Esta aplicação se faz necessária devido à grande evolução das comunicações do mercado corporativo, que trouxe junto consigo, pessoas mal-intencionadas que se utilizam de mecanismos para furtos de informações e até mesmo de serviços e produtos. Este documento traz o resultado da implementação do *Firewall* pfSense definida para o atendimento da demanda de segurança de empresas utilizando mecanismos de prevenção de ataques e furtos de informações.

Palavras chave: *Firewall*. *Software* Livre. Segurança. pfSense.

ABSTRACT

NEVES, Filipe Campos das, MACHADO, Leonardo Alves, CENTENARO, Rodrigo da Fontoura. Deployment of pfSense Firewall. 2014. 66 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

This work presents research and applications necessary for implementing a Firewall in an open source software called pfSense in companies that have less revenue to spending in the area of security, but still need the security of your data either internally or even to external environment. This application is necessary due to the great development of the corporate communications market that brought with it malicious people that make use of mechanisms for the theft of information or even services and products. This document contains the result of the implementation of the pfSense Firewall set to meet the demand of companies using security mechanisms to prevent attacks and information theft.

Keywords: Firewall. Open Source software. Security. pfSense.

LISTA DE ILUSTRAÇÔES

LISTA DE SIGLAS

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
CPU	Central Processing Unit
DNS	Domain Name System
DMZ	Zona Desmilitarizada
DHCP	Dynamic Host Configuration Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
L2PT	Layer 2 protocol tunneling
LAN	Local Area Network
MAC	Media Access Control
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2
MTU	Maximum transmission unit
NAT	Network Address Translation
PHP	Personal Home Page
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RRD	Round-robin database
SGSI	Sistema de Gestão de Segurança da Informação
SNMP	Simple Network Management Protocol
SSH	Secure Shell
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

Com a grande evolução das comunicações do mercado corporativo, a transferência de informações se torna mais rápida a cada dia, e isso traz grande ganho às empresas que fazem uso desses mecanismos, porém junto com essa evolução, pessoas mal-intencionadas se utilizam de mecanismos para furtos de informações e até mesmo de serviços e produtos.

Com o crescimento das comunicações cliente-servidor, faz-se necessária a utilização de mecanismos de prevenção de ataques e furtos de informações. A partir dessa demanda, foi desenvolvido o *firewall*, um dispositivo, ou conjunto de dispositivos ou programas, incumbido de realizar a proteção da rede interna. Ele funciona como uma espécie de porta de entrada e saída e faz com que todos os fluxos de dados passem por ele.

É importante salientar que o *firewall* não faz toda a segurança da rede por si só, ele é somente uma das várias ferramentas necessárias para a segurança de uma rede. Também é importante diferenciá-lo das demais soluções de segurança, como por exemplo, conexões VPN, mecanismos antivírus, *anti-spyware*, entre outros. O *firewall* faz a chamada segurança de perímetro, impedindo conexões não desejadas e filtrando-as, permitindo somente o acesso devido à rede.

Desta forma, foi apresentada uma solução baseada em *software* livre, para empresas que possuam menos receita para gastos com segurança, mas que mesmo assim necessitem da segurança de seus dados seja ela interna ou até mesmo para o ambiente externo.

1.1 PROBLEMA

Invasões em sistemas internos de empresas há muito tempo preocupam os profissionais da área de segurança da informação, porém, ataques que antes tinham muitas vezes somente a intenção de realizar a autoafirmação de *hackers*, hoje se mostram muito mais perigosos e danosos às empresas que não utilizam de uma proteção adequada.

Diante desses problemas expostos acima, a demanda por segurança no mercado atual é de suma importância, e com isso foram propostos alguns questionamentos. Quais sistemas de segurança devem ser aplicados? Onde, dentro da rede corporativa, devem ser implantadas soluções de segurança? E quais seriam os ganhos reais desse sistema?

Para expor de forma mais concreta, foi abordado um estudo sobre o *firewall* pfSense*,* assim como sua importância no sistema corporativo. O *firewall,* apesar de não ser o único componente de segurança em uma rede, é um dos mais importantes deles, realizando a segurança de perímetro da rede.

Através do estudo de configurações e funcionamento do *firewall* podem ser respondidos os questionamentos sugeridos acima e também pode ser demonstrado porque sua implantação é fundamental no mercado atual.

1.2 JUSTIFICATIVA

Com base das informações colhidas acima, foi proposta uma solução de *firewall* aconselhado para pequenas empresas que não possuam muita verba para investimento na área de segurança da informação. Apesar de ser uma solução baseada em *software* livre, a ferramenta possui muitos recursos e apresenta grande grau de segurança a um custo mais acessível.

Este projeto visa à implantação de um *firewall pfSense*, para expor serviços como:

- Filtragem de origem e destino IP, protocolo IP, portas de origem e destino para tráfegos de protocolos UDP e TCP;
- Habilidade de limitar através de uma política de regras, conexões simultâneas;
- Opção de realizar ou não os relatórios baseados somente em regras selecionadas;
- Habilidade de criação de grupos de endereços, redes e portas visando à facilidade de gerenciamento e a clareza das regras criadas;
- Capacidade de gerenciamento de tabela de estados;
- Interface WEB de extrema facilidade de gerenciamento;

1.3 OBJETIVOS

1.3.1 Geral

Através da demonstração dos aspectos técnicos e de sua importância, apresentar uma solução de *firewall* que garanta a segurança e o gerenciamento das redes corporativas, com um custo de implantação extremamente baixo e confiável.

1.3.2 Objetivos Específicos

Apresentar fatos que intensificaram esforços na criação de meios de segurança para redes corporativas.

- Expor vulnerabilidades que novas tecnologias podem vir a trazer;
- Descrever características, conceitos e a importância de um *firewall* em redes corporativas;
- Demonstrar as configurações da tecnologia pfSense e apresentar um projeto de segurança utilizando a mesma;
- Simular um ambiente de rede, utilizando ferramentas de virtualização, utilizando o *firewall* pfSense;

1.4 PROCEDIMENTOS METODOLÓGICOS

A implantação do projeto será guiada por manuais, normas, e guias que tratem do tema.

O projeto será desenvolvido em quatro etapas, na primeira etapa será realizado uma contextualização sobre o tema segurança e mostradas as motivações que levaram ao desenvolvimento do *firewall*, será apresentado a importância, seus principais conceitos e os principais equipamentos utilizados no mercado.

Na segunda parte do projeto, será apresentada a tecnologia pfSense, suas funções, configurações e maneiras de implantação. Esse estudo será guiado por

apostilas, livros de estudo e o próprio *site* do pfSense, que oferece grande quantidade de informações e detalhes da solução.

Em sua terceira parte, será realizada uma simulação que demonstrará na prática o funcionamento do *firewall* e os principais atributos necessários para a implantação dessa tecnologia.

A última etapa visa vincular o conhecimento obtido nas simulações ao conhecimento teórico, para demonstrar os reais benefícios desta tecnologia.

2 FUNDAMENTAÇÃO TEÓRICA

Com a evolução nos sistemas de comunicações, o acesso à informação se torna cada dia mais democrático e universal, e a *internet* tem papel fundamental na evolução do mercado corporativo atual. Com esse amplo acesso a informações, se tornou essencial o desenvolvimento de equipamentos com capacidade de prover a segurança das informações trafegadas pela rede. Esses equipamentos são responsáveis por uma série de competências, como por exemplo, o controle de acessos, para evitar acessos nocivos ou não autorizados às informações.

A segurança da informação é regulamentada pelas normas ISO/IEC 27000 e ISO/IEC 27001 que consistem em definir um propósito para o desenvolvimento de um Sistema de Gestão e Segurança da Informação (SGSI) nas organizações, algo imprescindível tendo em conta a quantidade de informação produzida atualmente nas grandes corporações (ISO/IEC 27000, 2013).

Com esse novo ambiente de desenvolvimento de segurança, novos campos de estudo têm se destacado, como por exemplo, a segurança das redes. Essa área é marcada pela constante evolução, ou seja, é necessário o desenvolvimento de novas técnicas conforme novas formas de ataques são criadas.

Com base nesses argumentos, foram considerados alguns pontos importantes para estudo:

- Entendimento da forma como são constituídas as formas de invasão, que normalmente se dão através da exploração da implantação de novos sistemas corporativos, falhas na implantação de sistemas de segurança e novos sistemas de conectividade;
- A facilidade de acesso à *internet* possibilita a criação de novas formas de ataque, e por consequência a necessidade de desenvolvimento de novas formas de defesa aos mesmos. Pelo fato de um ataque precisar identificar somente uma falha para que possa servir ao seu propósito, a defesa tem de mitigar todas as formas de ataque e falhas no sistema de segurança. Com isso pode ser tomado como base que a defesa de um sistema de informação é muito mais complexa e trabalhosa que um ataque;

- Entendimento das mais variadas formas de ataque a um sistema facilita muito na criação de métodos de proteção aos mesmos. Os ataques a uma rede corporativa podem ter os mais diversos motivos, como por exemplo, interromper serviços da empresa, comprometendo a confiabilidade de dados e programas ou até mesmo a desestabilização de uma rede, com o objetivo de coletar informações que podem ser usadas no futuro para invasões com finalidades mais específicas, como o roubo de informações sensíveis e até mesmo para corromper sistemas vitais à empresa concorrente.

Com base neste contexto, foi desenvolvido uma das formas para mitigar esses ataques, o *firewall,* que realiza controle de acessos devidos a uma determinada rede. É possível interpretar um *firewall* fazendo uma analogia com a forma mais antiga de segurança medieval, criar um fosso ao redor de um castelo e forçar todos que quiserem entrar a passar por uma ponte levadiça, nessa analogia, o *firewall* seria a ponte levadiça, a única porta de entrada de uma rede (TANENBAUM, 2003).

O conceito de *firewall* começou a ser utilizado no final da década de 80, quando somente roteadores separavam pequenas redes corporativas. Desta forma, as redes poderiam instalar seus aplicativos da forma como lhes fosse conveniente sem que as demais redes fossem prejudicadas por lentidões.

Os primeiros *firewalls* a trabalharem com segurança de redes surgiram no início dos anos 90. Consistiam de mecanismos que com pequenos conjuntos de regras como, por exemplo: Alguém da rede A pode fazer acesso à rede B, porém a rede C não pode realizar acessos à rede A e B. Eram mecanismos bastante efetivos, porém extremamente limitados. A segunda geração de *firewalls* utilizava filtros, pacotes e aplicativos, além de trazer uma interface de gerenciamento de regras, um grande salto evolutivo.

Em 1994, a Check Point lançou o produto chamado Firewall-1, introduzindo uma amigável interface gráfica de gerenciamento, que continha cores, *mouse* e ambiente gráfico X11 simplificando a instalação e a administração dos *firewalls*.

Atualmente existem várias soluções de *firewalls* muito mais modernas, as principais empresas do ramo são: Cisco, Juniper, Check Point entre outras.

Firewall é uma solução de segurança baseada em *hardware* ou *software*, que a partir de um conjunto de regras ou instruções, analisa o trafego da rede para diferenciar operações válidas ou inválidas dentro de uma rede corporativa. Um *firewall* analisa o tráfego de rede entre a *internet* e a rede privada ou entre redes privadas. Com base nessas definições, é possível compreender que o *firewall* é mais que uma simples barreira de proteção contra ataques, ele pode ser utilizado para proteção dentro de uma rede controlando o tráfego de dados á servidores específicos.

2.1 TIPOS DE FIREWALL

Os três principais tipos de *firewall* são:

- *Firewall* em nível de pacote: O filtro de pacotes tem como objetivo permitir ou não a passagem de pacotes pela rede baseando-se em regras pré-definidas. Normalmente estes estão situados em roteadores, representando o ponto de acesso entre duas redes, permitindo que serviços controlem o trafego, mantendo a rede protegida.

Este é o *firewall* mais implementado atualmente, pois é a proteção básica da rede, ao deixar portas de comunicação nocivas abertas e permitir o tráfego livre de pacotes, a rede fica suscetível à ataques (Camy, 2003).

- Serviços *Proxy*: Os servidores de serviço *proxy* são especializados em aplicações ou programas servidores que executam um *firewall*. Os *proxies* pegam a solicitação e requisição dos usuários para o serviço da *internet*, verificam se as solicitações serão aceitas dentro do conjunto de regras preestabelecidas e em seguida passam ou não a solicitação adiante para o serviço específico solicitado (Stato Filho, 2009).

Estes servidores estão entre o usuário da rede interna e a *internet* e atuam como o próprio nome diz, como um mediador. É comum utilizarem transparência nesses servidores, como o nome sugere, ele fica transparente para o usuário, sendo imperceptível, porém atuando como filtro de pacotes.

- *Circuit-Level Gateway*: Este tipo de *firewall* cria um circuito entre o cliente e o servidor e não interpreta o protocolo de aplicação. Atua monitorando o

handshaking (troca de informações para estabelecimento de comunicação) entre pacotes, objetivando determinar se a sessão é legítima (Stato Filho, 2009).

O principal objetivo de um *firewall* é fazer com que todas as informações trafegadas entre duas redes diferentes passem por ele. Para que isso aconteça, é necessário que haja um estudo sobre a arquitetura da rede que se deseja proteger.

2.2 ARQUITETURAS DE IMPLANTAÇÃO DE FIREWALL

As principais arquiteturas de implantação de *firewalls* são:

- *Dual-homed host*: Nessa arquitetura o equipamento deve possuir duas interfaces de rede, uma interface que se liga a LAN, que representa a rede interna, e uma interface WAN, que representa a rede externa, se tornando uma espécie de porta única de saída e entrada da rede. De acordo com os principais pesquisadores, esta arquitetura é ideal para redes com pequeno tráfego de informações para a *internet* e cuja importância não seja vital.
- *Screened host*: Nesta arquitetura as conexões podem ser abertas da rede interna para a *internet*, bem como das redes externas para a rede interna de forma exclusivamente controlada pelos *Bastion hosts*. A filtragem de pacotes acontece no *firewall* que permite apenas poucos tipos de conexões, como por exemplo, consultas de DNS (*Domain Name System*). O *Bastion host* deve manter um alto nível de segurança pelo fato dele ser o ponto de falha dessa arquitetura. Esta arquitetura é apropriada para redes com poucas conexões vindas da *internet* e quando a rede sendo protegida tem um nível de segurança relativamente alto.
- *Screened Subnet*: Nessa arquitetura, também conhecida como arquitetura de sub-rede com triagem, é adicionada uma nova rede de perímetro que isola os *bastion hosts*, máquinas vulneráveis na rede. Também são encontrados roteadores de triagem com várias placas de rede. Neste caso, o *bastion host* fica confinado em uma área conhecida como Zona Desmilitarizada (DMZ), aumentando o nível de segurança, uma vez que, para ter acesso à rede interna o atacante deverá passar por mais de um processo de filtragem. O *firewall* externo deve permitir que os usuários externos tenham acesso somente à área

DMZ e o *firewall* interno deve permitir requisições apenas aos usuários da rede interna (Stato Filho, 2009, p.37).

Existem mais possibilidades de arquiteturas e uma flexibilidade no modo de configuração, devem ser avaliados os requisitos de proteção e de orçamento para poder atender as necessidades de proteção da rede em questão.

2.3 DHCP (*DYNAMIC HOST CONFIGURATION PROTOCOL*)

O DHCP é um servidor de endereços IP que ao receber uma solicitação de um dispositivo de rede por um IP atribui a este um endereçamento. Cada máquina que é conectada na rede transmite um pacote de DHCP *DISCOVER* para o agente de retransmissão DHCP da rede interceptar, ao então o agente envia este pacote em unidifusão ao servidor DHCP, possuindo apenas o endereço IP do servidor.

O DHCP distribui endereços de rede que são atribuídos fixamente ou dinamicamente para os *hosts* e dispositivos de rede (TANENBAUM, 2003, p. 349). A figura 1 mostra este processo DHCP.

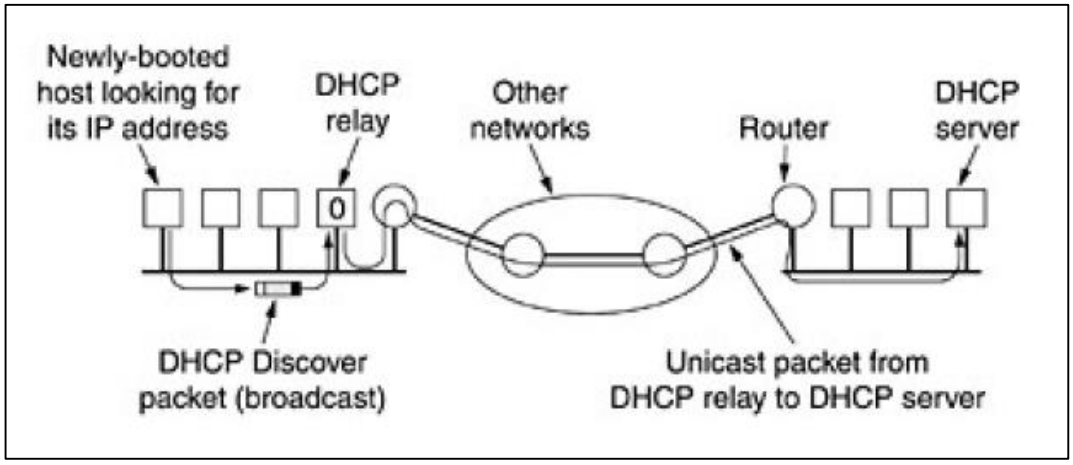


Figura 1 – Operação do DHCP
Fonte: TANENBAUM (2003)

2.4 DNS (*DOMAIN NAME SYSTEM*)

O DNS consiste na criação de um processo de atribuição de nomes baseados no domínio e em um sistema de bancos de dados distribuídos que implementam esse esquema de nomenclatura organizando e mantendo as informações. É utilizado para mapear nomes de *hosts* e destinos de correios eletrônicos em endereços IP, tendo também outras utilizações (TANENBAUM, 2003, p. 439).

O processo do DNS consiste em procurar o endereço IP correspondente ao nome de domínio do site especificado pela requisição (ex.: o endereço IP do site www.google.com pode ser resolvido pelo DNS como 173.194.118.51). A figura 2 traz um exemplo do esquema de resolução DNS.

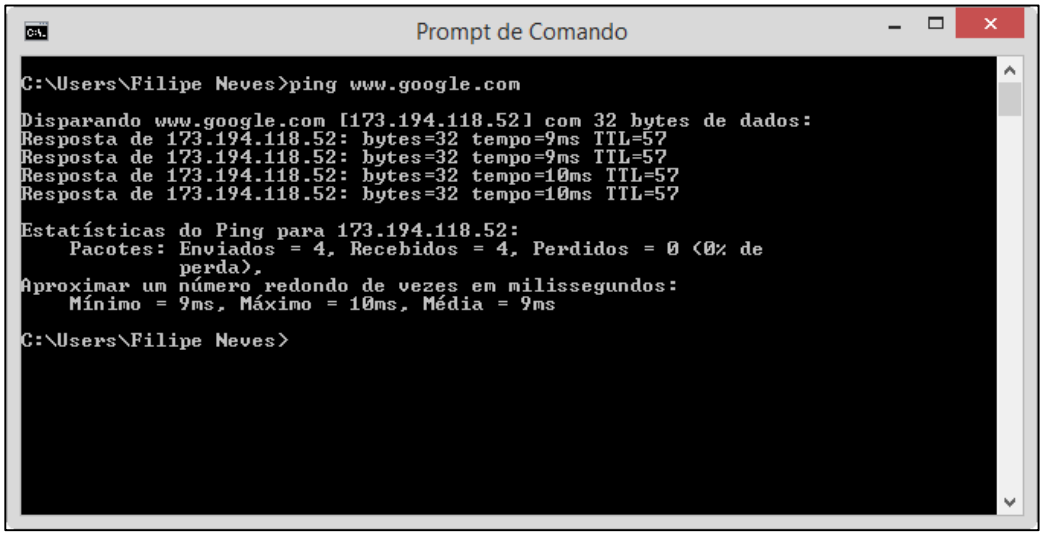


Figura 2 – Resolução DNS
Fonte: Autoria própria

2.5 NAT (*NETWORK ADDRESS TRANSLATION*)

O NAT tem como idéia básica a utilização de um único endereço IP para determinada empresa trafegar na *internet* (IP roteável), possibilitando assim cada computador da rede interna ter um endereço IP exclusivo, para roteamento do trafego interno. Quando um pacote de dados sai da rede interna para trafegar na *internet* é efetuada uma conversão de endereçamento para o endereço único da empresa para acesso a *internet*. Para que esse sistema fosse possível foram separadas três classes

de endereços IP que podem ser utilizadas para trafego interno, porém não podem ser utilizadas para o trafego na *internet* (TANENBAUM, 2003). A Tabela 1 apresenta os endereços privativos e suas classes.

Tabela 1 - Padrão de endereçamento na Internet (IPv4)

		Endereço IP			
Classe A	Início	1	0	0	0
	Fim	126	255	255	254
		rede	host	host	host
	Máscara	255	0	0	0
Classe B	Início	128	0	0	0
	Fim	191	255	255	254
		rede	rede	host	host
	Máscara	255	255	0	0
Classe C	Início	192	0	0	0
	Fim	223	255	255	254
		rede	rede	rede	host
	Máscara	255	255	255	0

Fonte: Teleco (2007)

Outra função do NAT muito utilizada pelas empresas provedoras de acesso à *internet* serve como uma alternativa para escassez de endereços IP que são destinados para os usuários de ADSL. A empresa atribui a seus clientes endereços 10.x.y.z, e então quando os clientes saem da rede do provedor para acessar a *internet* os pacotes passam pelo processo de NAT que efetua a conversão dos endereços internos para endereços IP roteáveis, e na volta desses pacotes eles sofrem o processo inverso (TANENBAUM, 2003, p. 343-344).

2.6 *PORT FORWARDING* (ENCAMINHAMENTO DE PORTA)

O encaminhamento de portas é uma funcionalidade que consiste na associação de numeros de portas de comunicação a dispositivos da rede local onde estes dispositivos atendem as requisições nestas portas de serviços vindas da internet. Quando são feitas requisições da internet, essas requisições são tranferidas para um endereço IP da rede local. Desta forma o dispositivo que é responsável por receber as requisições para essas determinadas portas deve permancer com um endereço IP estático (Intelbras, 2013). A figura 3 ilustra o processo de encaminhamento de porta vindo de um computador externo à rede local.

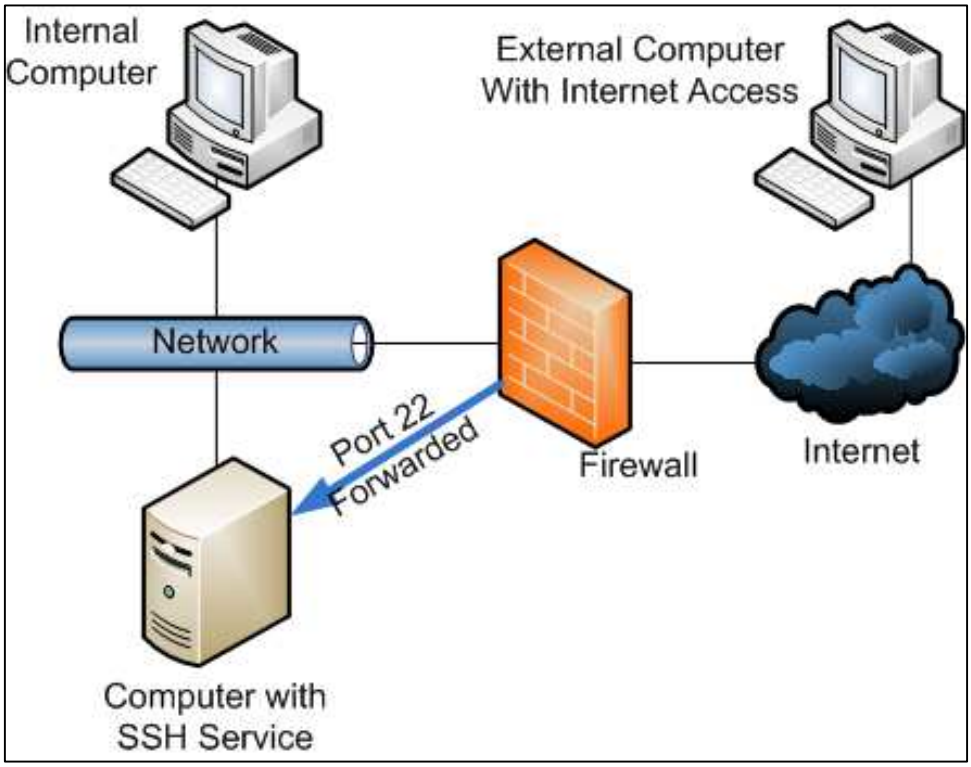


Figura 3 – Encaminhamento de Porta
Fonte: LeGauss (2012)

2.7 *LOAD BALANCING* (BALANCEAMENTO DE CARGA)

O balanceamento de carga torna os servidores altamente disponíveis e adaptáveis com a utilização de dois computadores disponibilizando seus recursos em conjunto. Para quem utiliza esses servidores o *cluster* (aglomerado de computadores)

é transparente, ou seja, o usuário não percebe que está alternando entre duas maquinas diferentes. O balanceamento de carga pode oferecer um serviço ininterrupto, já que mesmo com uma máquina falhando a outra máquina pode continuar oferecendo o serviço (TechNet, 2014). A figura 4 mostra como o balanceamento de carga pode ser feito.

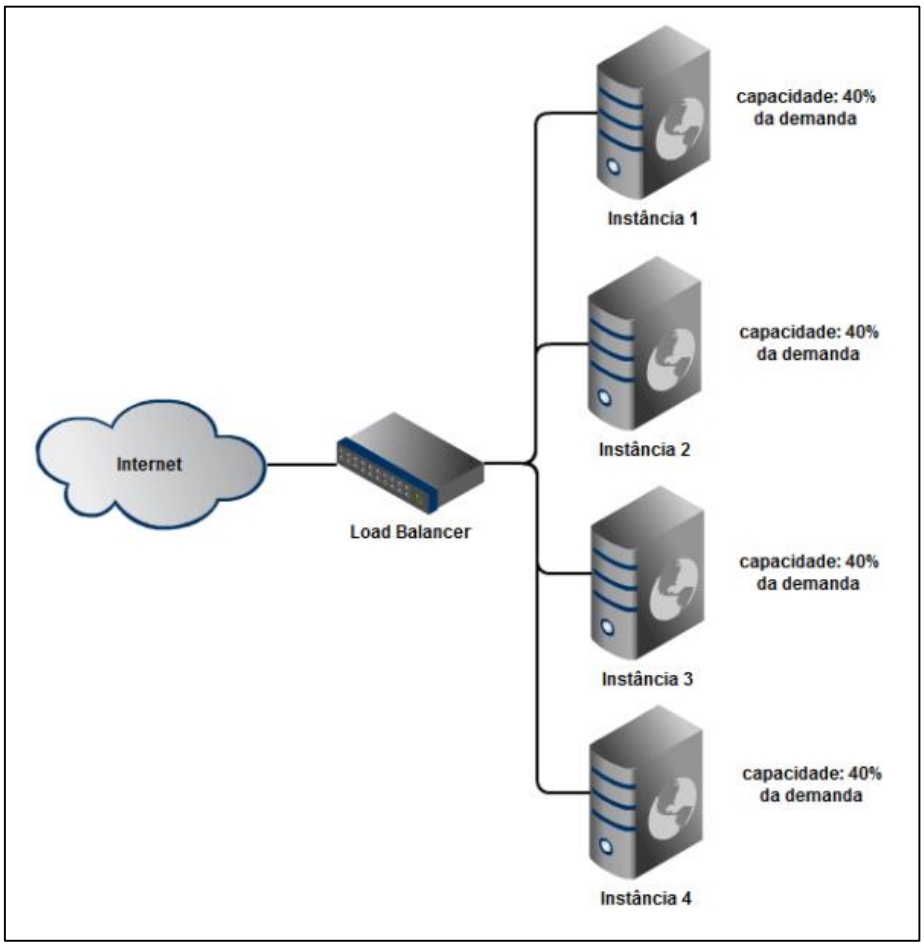


Figura 4 – Balanceamento de carga
Fonte: Planeta Tecnologia (2012)

2.8 APRESENTAÇÃO DO *FIREWALL* PFSENSE

O pfSense é um *software* livre customizado da distribuição do FreeBSD, sendo adaptado para uso como *firewall* e roteador, que é inteiramente gerenciado via interface WEB. Além de ser um poderoso *firewall*, e uma plataforma de roteamento, ele possui uma variada lista de recursos que podem ser adicionadas através de *downloads* de pacotes permitindo assim a adição de funcionalidades de acordo com a necessidade do usuário. O projeto do pfSense começou em 2004 se diferenciando de outro projeto o *m0n0wall*, por ser um projeto para ser instalado completamente em um pc (PFSENSE, 2014).

Recursos do pfSense:

- *Firewall;*
- *State Table* (Tabela de Estados);
- NAT;
- Alta Disponibilidade;
- *Load Balancing* (Balanceamento de carga);
- VPN;
- PPPoE *Server;*
- *Reporting* e *Monitoring* (Relatório e Monitoramento);
- Dynamic DNS (DNS Dinâmico);
- *Captive Portal;*
- *DHCP Server and Relay;*

3 IMPLANTAÇÃO DO *FIREWALL* PFSENSE

Este capítulo apresenta os materiais e os passos da instalação do *Firewall* pfSense utilizados na realização deste trabalho. Os materiais se referem às ferramentas utilizadas nos testes de laboratório, para a análise e comparação dos resultados. Não será abordada a instalação do sistema operacional Linux *Debian*, Linux *Ubuntu* e *Windows* 7, utilizados respectivamente para o servidor e as duas máquinas da LAN.

3.1 MATERIAIS

Para o desenvolvimento dos testes de instalação e configuração do pfSense e de suas funcionalidades foram utilizadas quatro máquinas virtuais no programa *VirtualBox*, duas máquinas como computadores de usuários para análise de funcionalidades na LAN, sendo uma máquina instalada com *Windows* 7 e uma com *Ubuntu*, uma máquina como servidor para análise de funcionalidades na DMZ sendo instalada com Debian, e uma máquina para instalação e configuração do *firewall* pfSense. A máquina que simulou os acessos à rede interna vindos da WAN, tanto para a LAN quanto para a DMZ, foi a própria máquina física onde estão hospedadas as quatro máquinas virtuais. A topologia da rede consiste na WAN para acesso à *internet*, na LAN para estações de trabalho e na DMZ para o servidor WEB, cada rede em sua interface e conectadas todas diretamente ao *firewall* pfSense como pode ser visualizado na figura 5.

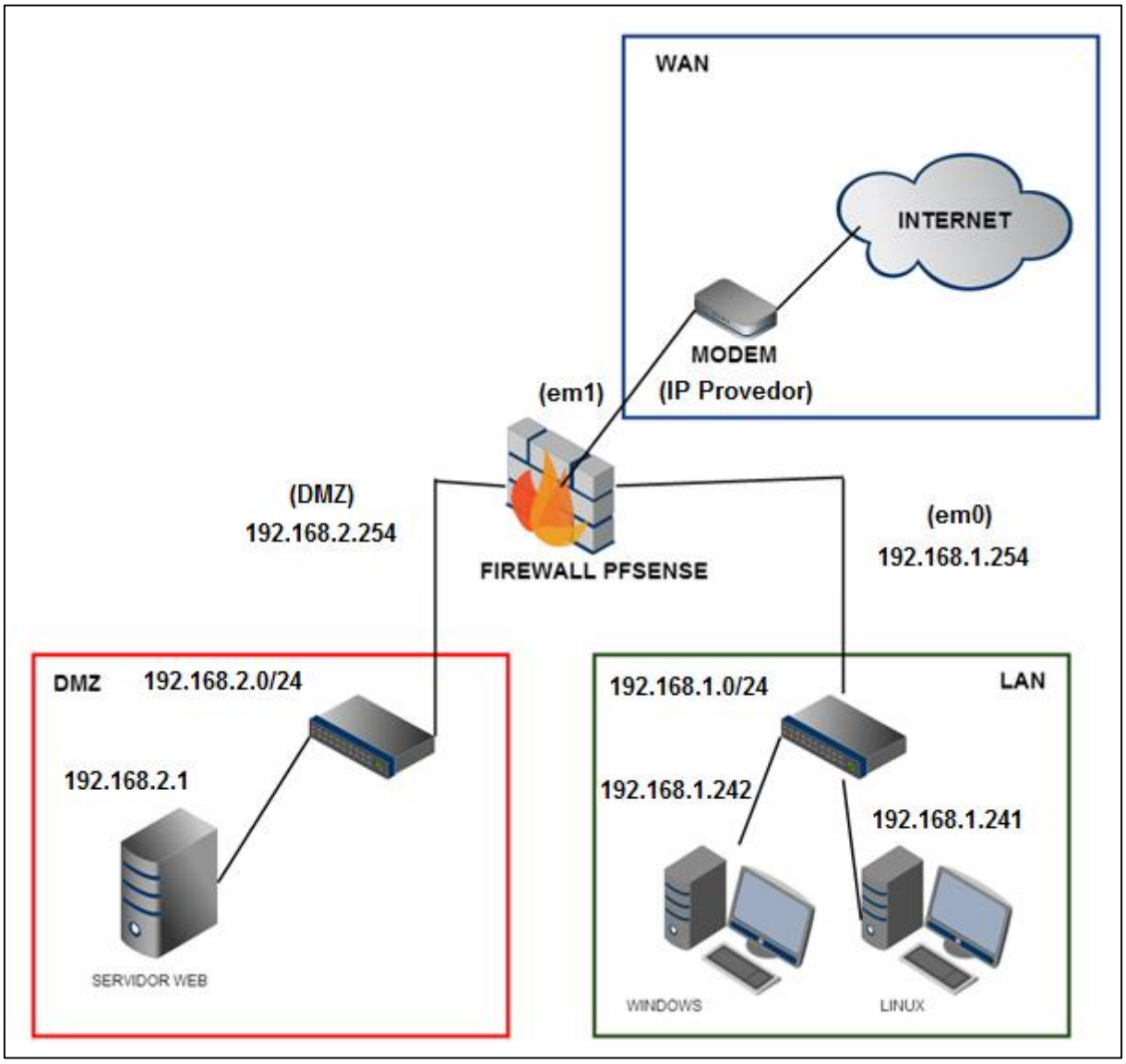


Figura 5 – Topologia da rede
Fonte: Autoria Própria

3.2 INSTALAÇÃO DO FIREWALL PFSENSE

O pfSense foi instalado em uma máquina virtual com a qual foi testada as funcionalidades e as configurações deste firewall juntamente as outras máquinas virtuais que estarão nas redes LAN e DMZ, também com a máquina física que simulou acessos da WAN. A versão do *pfSense* instalada foi a 2.1 através da ISO pfSense-LiveCD-2.1-RELEASE-i386-20130911-1815.iso.

3.3 CONFIGURAÇÕES DE INSTALAÇÃO

Na instalação do pfSense foram configuradas as Interfaces da LAN e WAN do firewall, foi feita a configuração dos endereços IP e o range do DHCP, simulando-se um *gateway* em uma rede corporativa de pequeno ou até mesmo médio porte.

3.3.1 Configuração das interfaces de rede

Ao iniciar o pfSense a tela inicial de configuração é mostrada, onde podem ser visualizadas as placas de rede instaladas, sendo elas em0 e em1, as interfaces possuem esses nomes devido ao fato do pfSense ser baseado um sistema operacional *FreeBSD*, no qual as interfaces possuem determinados nomes de acordo com seu fabricante. Foi perguntado sobre a configuração das VLANs, como não cabe em nossa proposta, foi respondido não (n) como pode ser visualizado na figura 22.

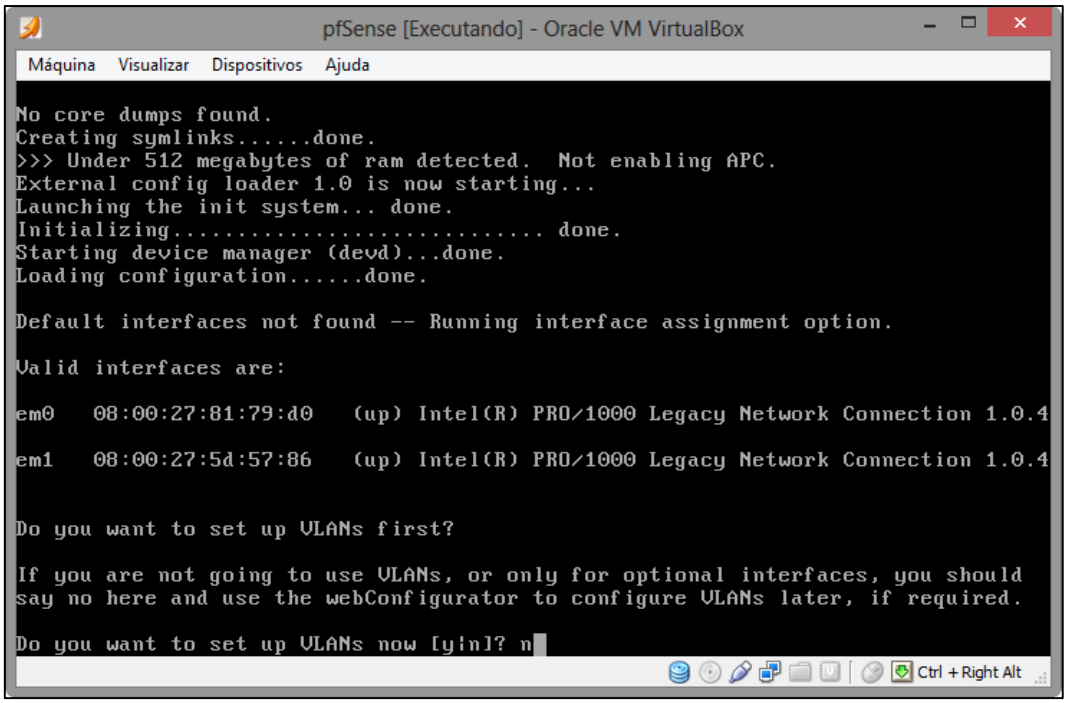


Figura 6 – VLANs
Fonte: Autoria Própria

Após a etapa da configuração de VLAN foi perguntado o nome da interface WAN. No caso a interface WAN esta em1, a interface que simularia a saída para a rede externa no servidor do cliente como pode ser visualizado na figura 23.

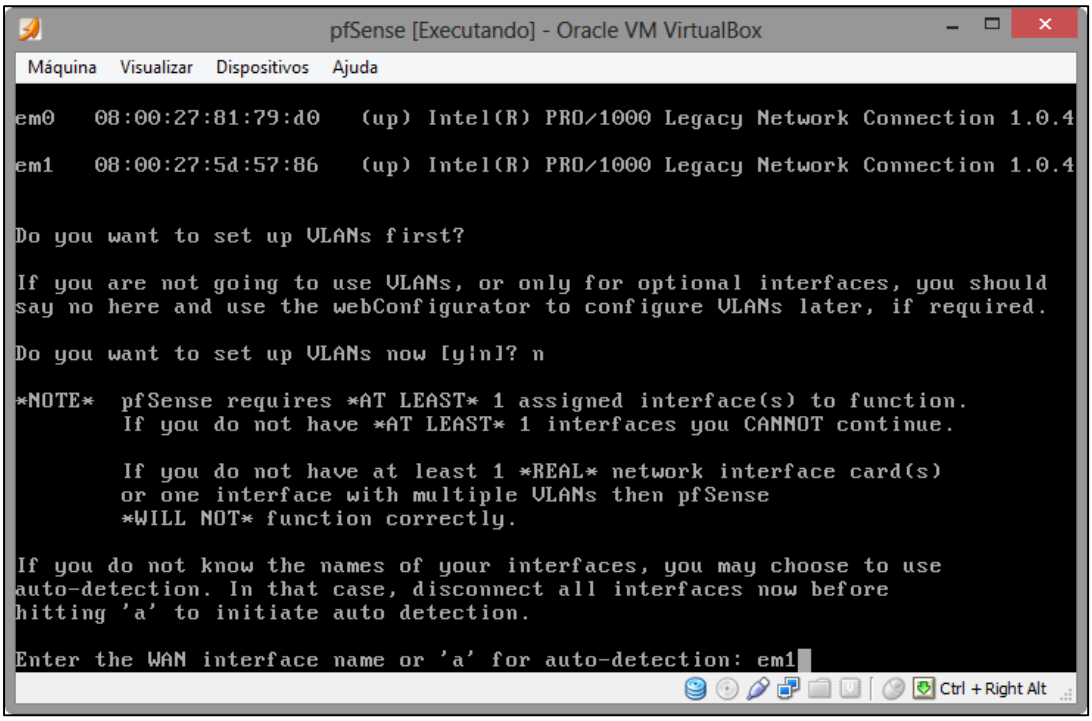


Figura 7 – Interface WAN
Fonte: Autoria Própria

A interface LAN será representada por em0. Será informada essa interface no momento que for solicitada, como foi demonstrado abaixo na figura 24. Essa interface representará a interface que pertence a uma das redes internas do nosso cliente.

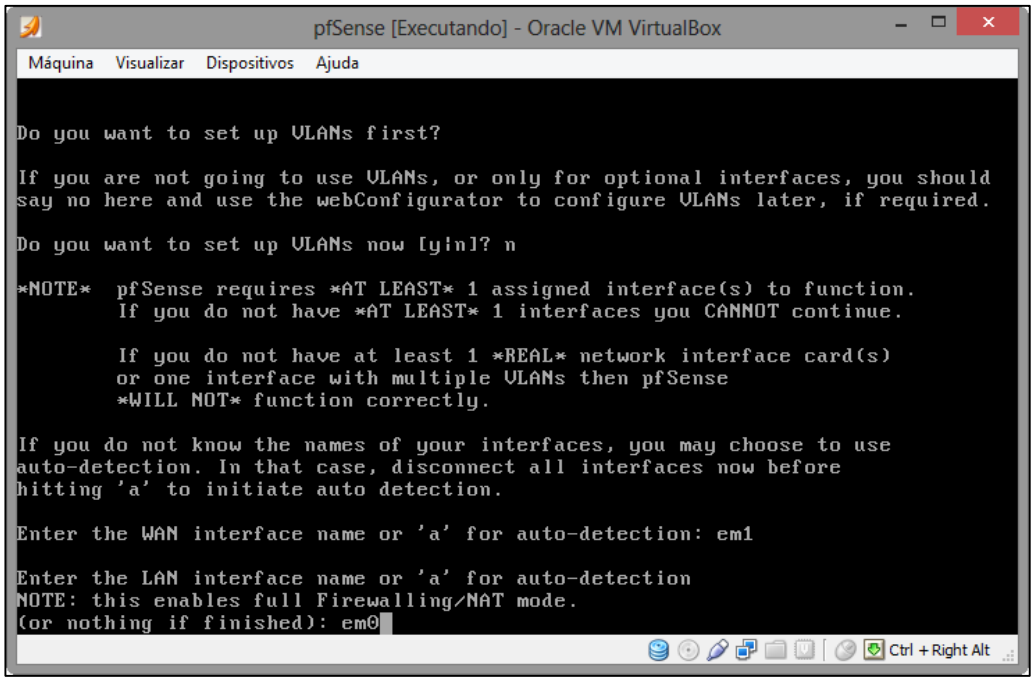


Figura 8 – Interface LAN
Fonte: Autoria Própria

A terceira interface de rede a qual irá representar a rede DMZ do nosso cliente, não foi configurada agora, este assunto foi abordado durante a configuração WEB do nosso firewall, então no momento a tecla *enter* pula esta etapa, conforme demonstrado na figura 25.

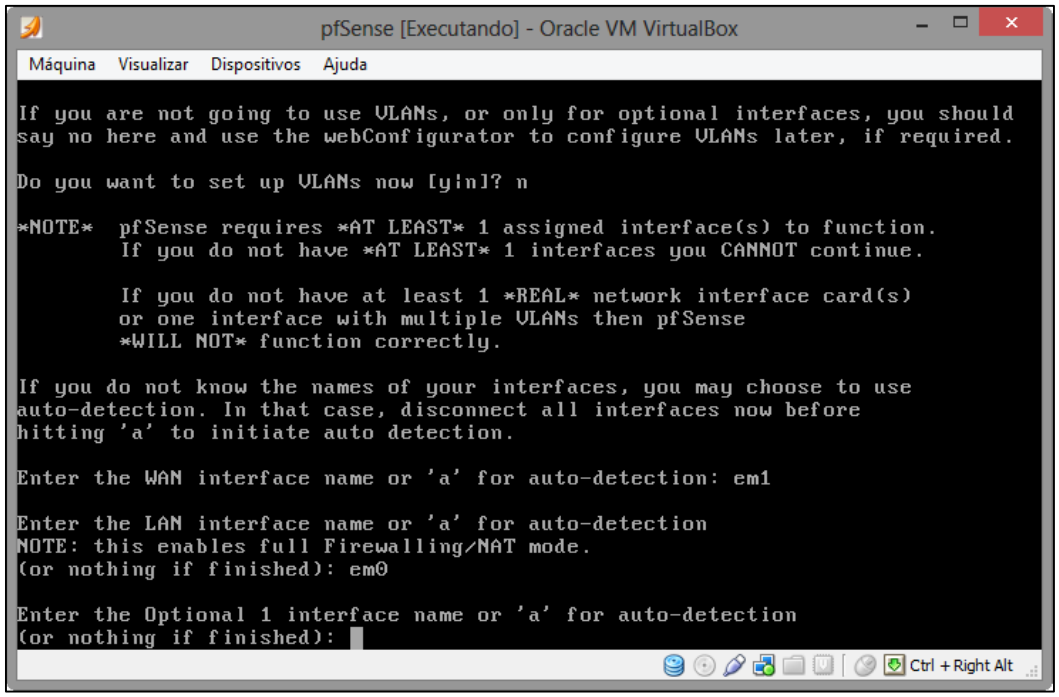


Figura 9 – Interfaces configuradas
Fonte: Autoria Própria

Foi mostrada na tela a configuração das Interfaces para confirmação, da forma como configuramos acima, com em1 representando a saída para a rede externa e em0 representando uma das redes internas, a figura 26 ilustra a situação explicada acima, através da tecla y que representa a opção *yes* continua-se o processo.

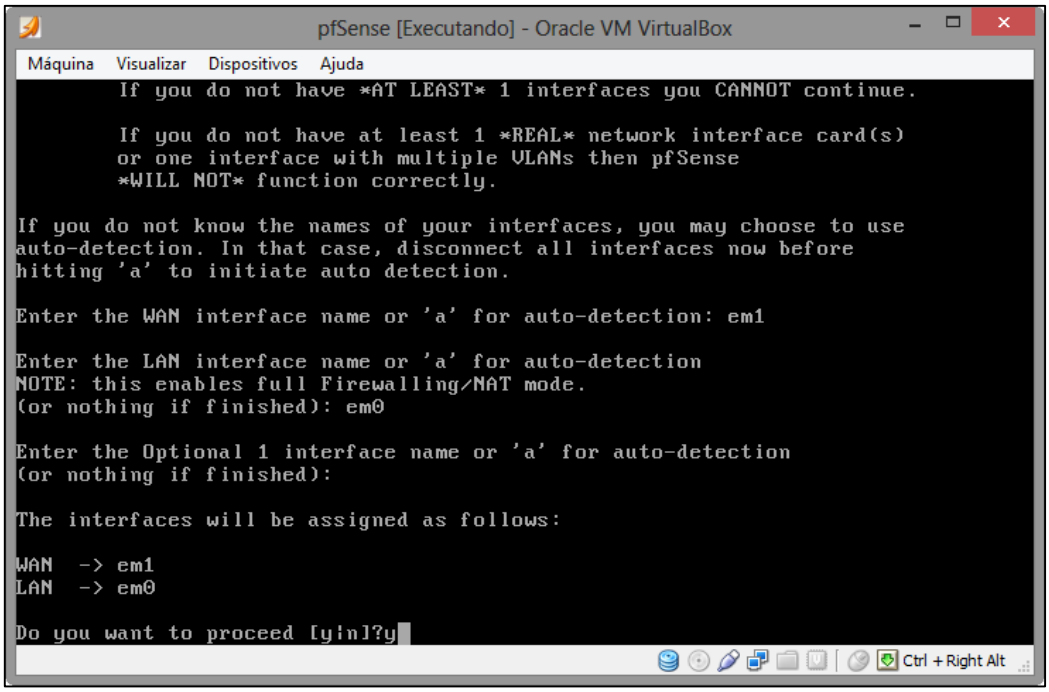


Figura 10 – Confirmação Interfaces configuradas
Fonte: Autoria Própria

A configuração foi gravada e então pode ser continuada a configuração, conforme é mostrado na figura 27.

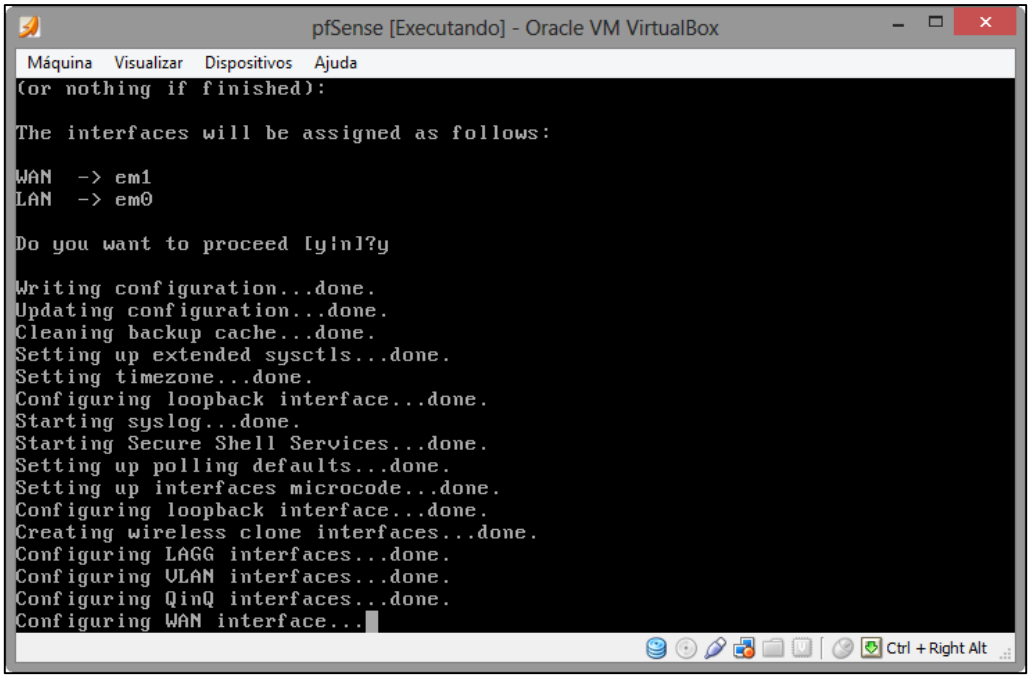


Figura 11 – Gravando as configurações
Fonte: Autoria Própria

3.3.2 Configuração do endereçamento IP

A configuração dos endereços IP, inicialmente foi feita somente na interface LAN, onde pode ser escolhido o endereço, a máscara de rede e o *gateway*, que simulam o *range* de endereços da rede interna do cliente, a interface WAN utiliza o endereço IP cedido pelo servidor DHCP do roteador de acesso a *internet*, que simularia um endereço externo da rede com o qual o cliente se conecta com a *internet*, este endereço pode também ser configurado de maneira fixa através de um link PPPoE ou um endereço fixo fornecido pela operadora, tema que foi abordado na etapa de configuração WEB do pfSense.

Na tela inicial de configuração, foi escolhido a opção para configuração dos endereços IP das interfaces com a opção “2” conforme figura 28.

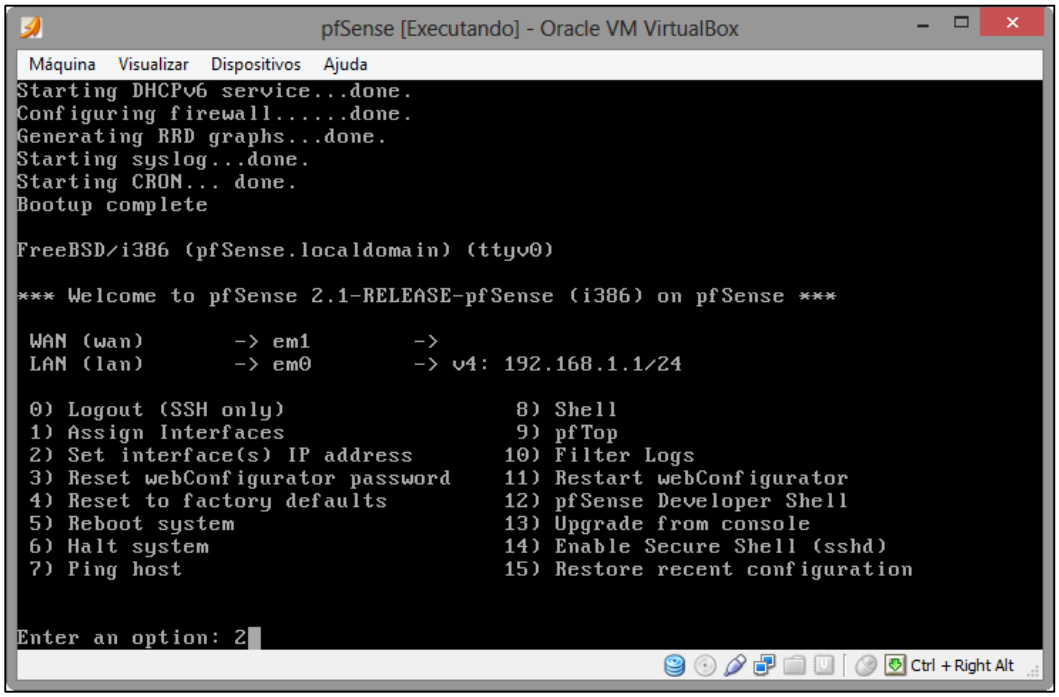


Figura 12 – Configuração de IPs
Fonte: Autoria Própria

Foi selecionado a opção “2” novamente, assim foi configurada a interface LAN, na qual estarão os computadores da rede interna do usuário como vide figura 29.

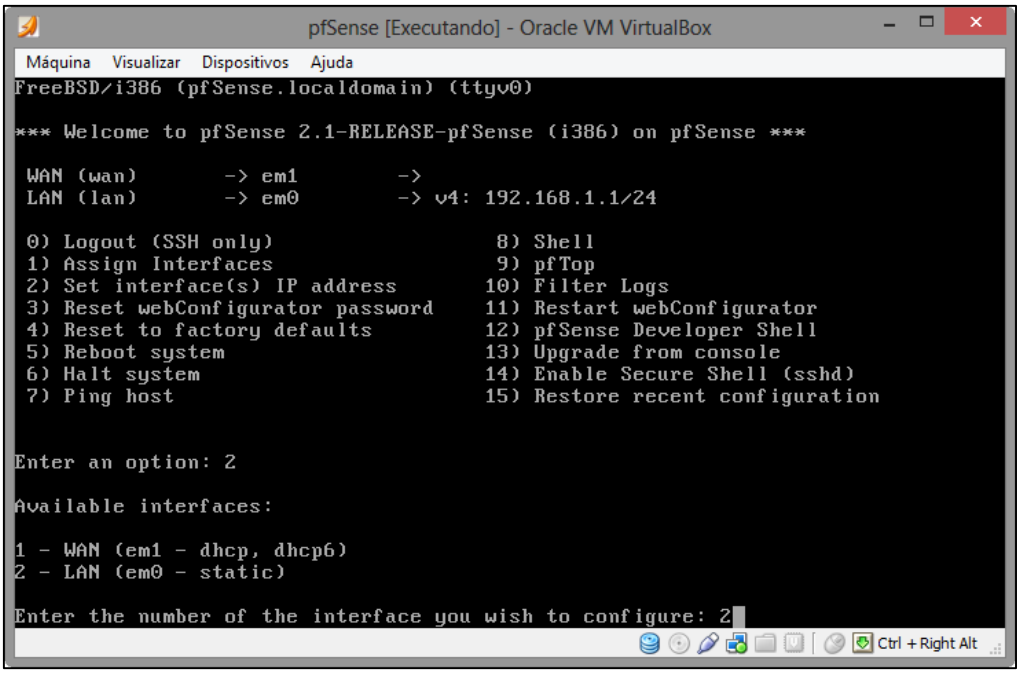


Figura 13 – Configurar LAN
Fonte: Autoria Própria

A interface LAN foi configurada com o endereço IP 192.168.1.254, último da rede 192.168.1.0, utilizada para simular a rede interna do nosso cliente, conforme demonstrado abaixo.

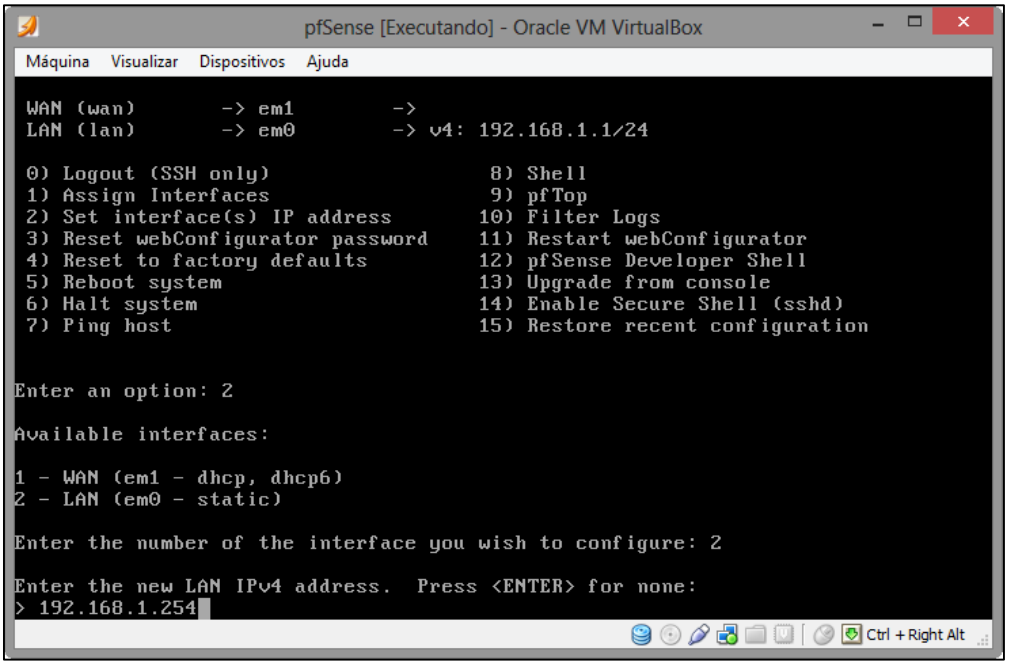


Figura 14 – IP da interface LAN
Fonte: Autoria Própria

A máscara para o endereço IP da LAN escolhida foi 255.255.255.0 (/24), o que possibilitou 254 endereços para a rede interna de computadores conforme demonstrado na figura 31.

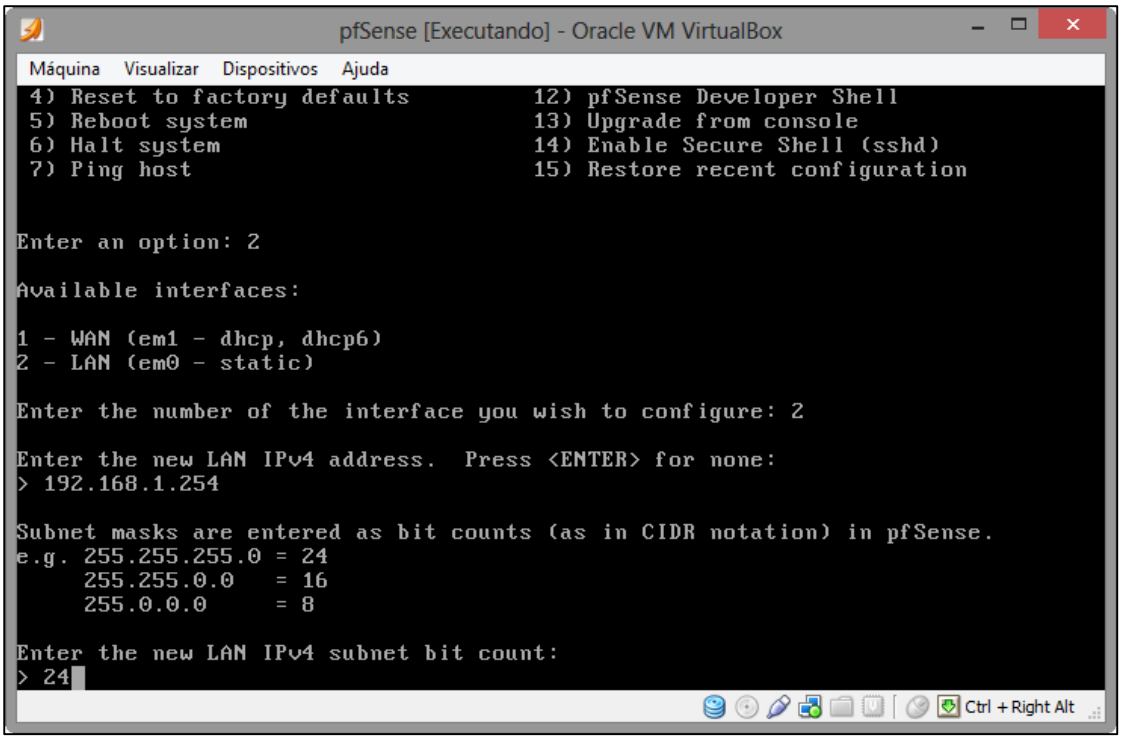


Figura 15 – Máscara da LAN
Fonte: Autoria Própria

O Gateway da LAN foi configurado com o endereço da interface da rede LAN do pfSense, conforme ilustrado na figura 32.

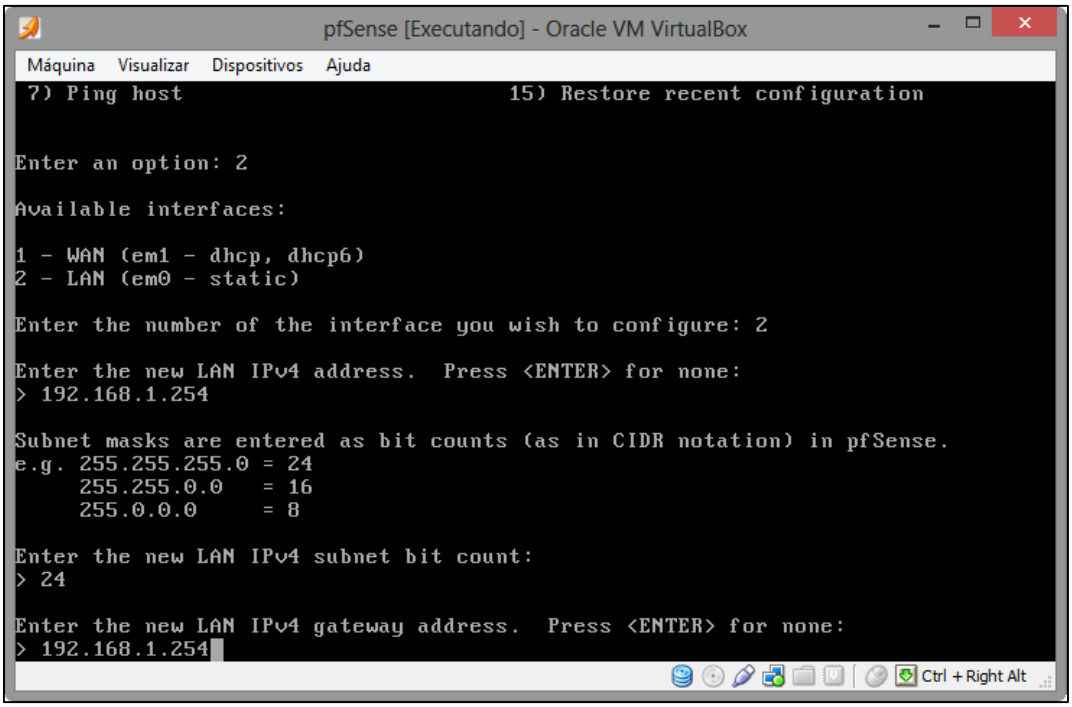


Figura 16 – Gateway da LAN
Fonte: Autoria Própria

Para a provisão de endereços para a rede em que ficaram os *hosts* do cliente foi ativado um servidor DHCP. O range de endereços contemplou os endereços de 192.168.1.10 até 192.168.1.220. Os endereços restantes foram utilizados para a configuração de equipamentos que por ventura não aceitem endereços distribuídos por DHCP, como por exemplo, impressoras, aparelhos de fax, entre outros. Caso haja necessidade de endereços fixos para *hosts* eles seriam fixados no servidor, tópico que será abordado durante a configuração WEB do pfSense. A figura 33 demonstra a configuração do DHCP.

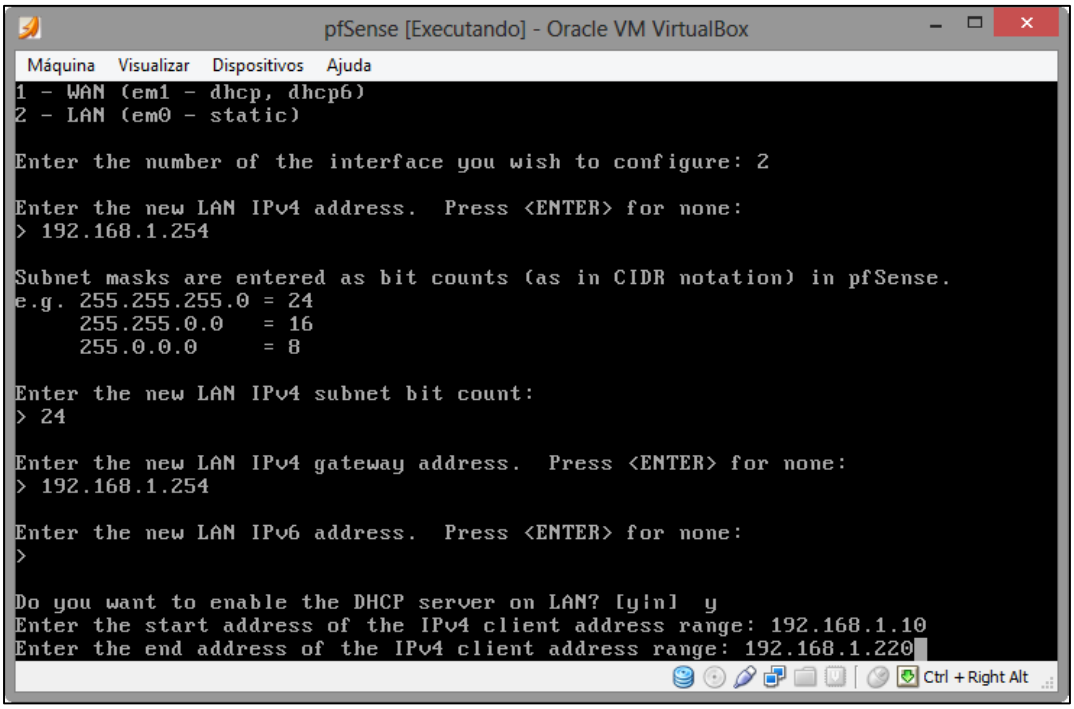


Figura 17 – DHCP da LAN
Fonte: Autoria Própria

A configuração dos endereços IP foi concluída. Agora o pfSense já pode ser acessado pela interface WEB através do IP 192.168.1.254 conforme figura 34. Neste momento o pfSense só pode ser acessado através de máquinas da rede LAN.

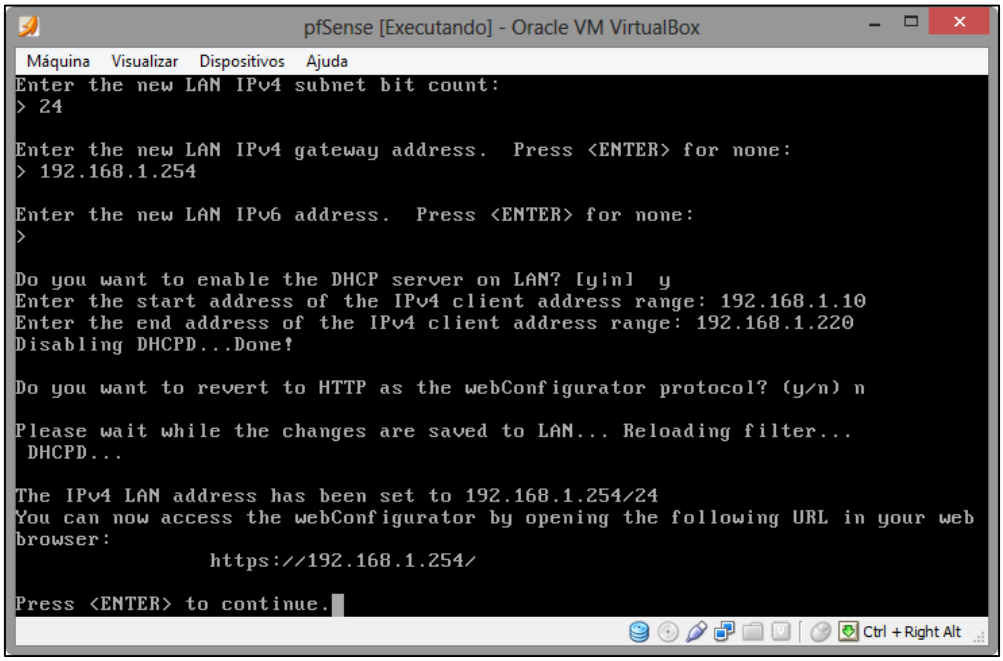


Figura 18 – IP Interface WEB
Fonte: Autoria Própria

3.4 FUNCIONALIDADES DO PFSENSE

Nesta etapa foi demonstrada as funcionalidades do pfSense através de sua interface de configuração WEB e algumas configurações em linha de comando. A interface de gerenciamento WEB proporciona muitas facilidades na configuração e no gerenciamento de nosso *firewall* permitindo ao administrador desde a configuração de interfaces de forma simplificada, até o estudo e verificação de falhas através de leitura de *logs* do sistema e gráficos de utilização de banda. Como pode ser visualizado na figura 19, a tela inicial de gerenciamento mostra uma série de informações sobre o *firewall*, como por exemplo, os estados das interfaces conectadas, os servidores DNS, tabela de estados, uso de CPU e memória entre outras informações muito úteis para o administrador de redes encarregado pelo gerenciamento do *firewall*.

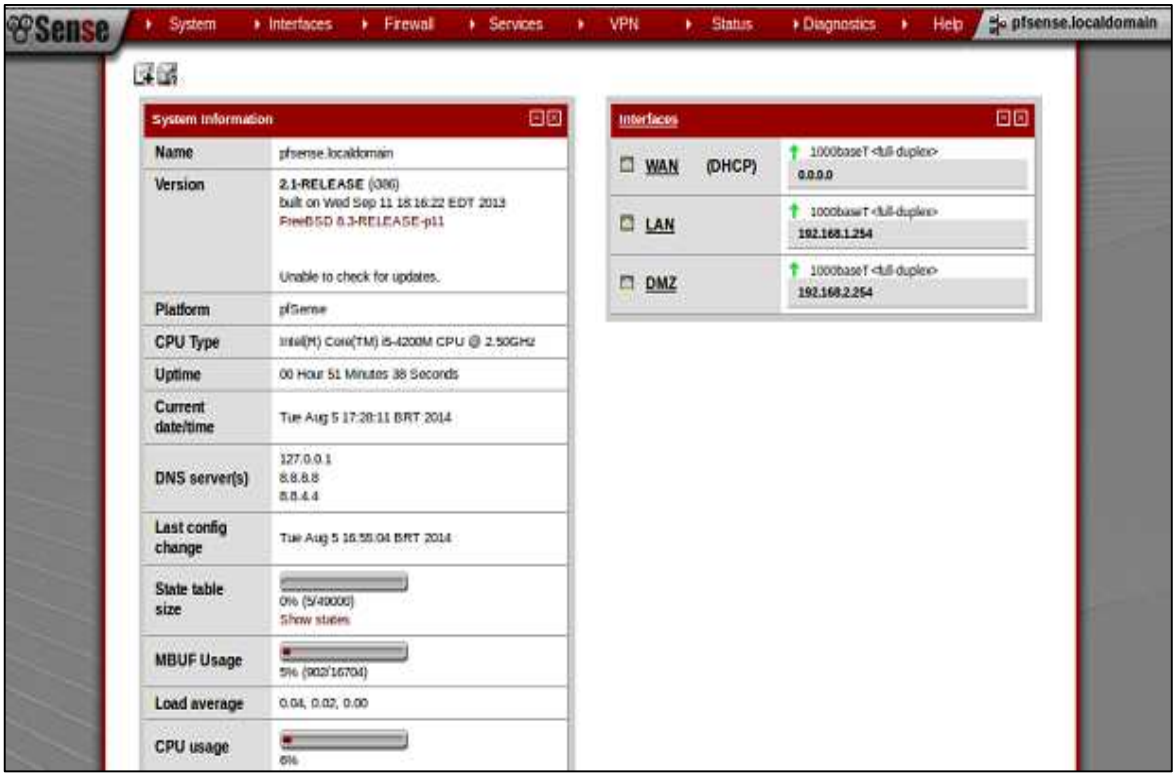


Figura 19 – Tela inicial pfSense
Fonte: Autoria Própria

3.4.1 Interface WEB

A interface WEB do pfSense é dividida em abas de configuração de diferentes tipos de serviço, abaixo foi listado detalhadamente cada uma das abas com as configurações que são consideradas mais importantes para o desenvolvimento de um *firewall* para empresas de pequeno e até mesmo médio porte.

3.4.2 Configurações de sistema

Na aba *system* é possível configurar opções avançadas do *firewall*, como por exemplo, o acesso remoto via SSH, que será tratado com mais detalhes na parte final deste capítulo, alterar a forma de acesso à interface WEB utilizando uma conexão HTTPS, alterar a porta para conexão HTTP/HTTPS, configurar diferentes formas de otimização do *firewall* para *links* com menor capacidade ou redes com maior latência. Pode ser também utilizada a tecnologia IPv6, uma nova forma de endereçamento IP mais segura e robusta. Existem várias configurações possíveis nesta aba de configuração, porém somente algumas foram utilizadas neste projeto.

3.4.3 Configuração de Interfaces

Na aba *interfaces* é possível realizar a configuração das interfaces de rede como o próprio nome sugere, é possível também adicionar novas interfaces caso haja necessidade de ampliar a rede, assim poderíamos dividir nossa rede em um número maior de domínios de *broadcast*, porém esse assunto foge do escopo do trabalho. A figura 20 demonstra a configuração de uma nova interface de rede que foi utilizada para configurar a interface DMZ.

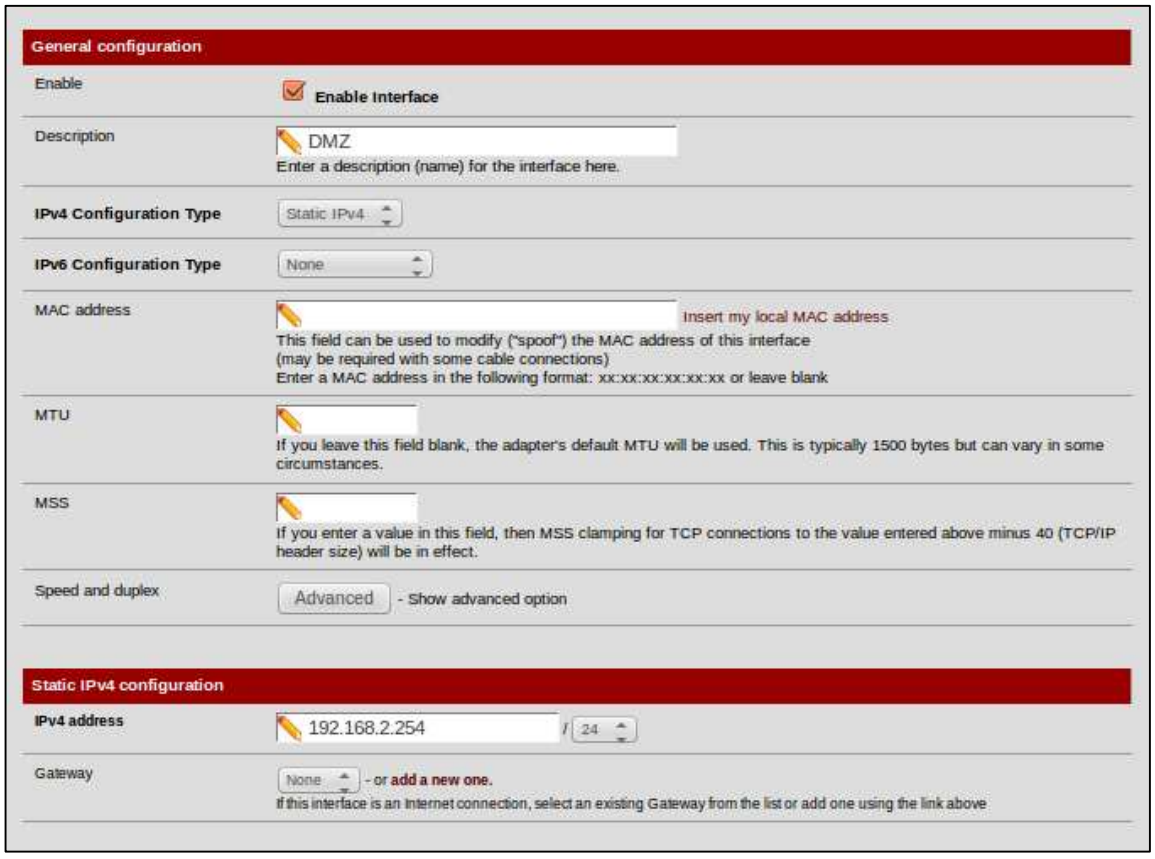


Figura 20 – Tela Interface DMZ
Fonte: Autoria Própria

Como pode ser observado na figura 20, é possível realizar algumas configurações na interface, a primeira seria a ativação da mesma através do *checkbox* "*Enable Interface",* logo abaixo a configuração de uma descrição para a interface, o tipo de endereçamento, neste caso IPv4 com configuração estática, assinalar um novo endereço MAC, alterar o tamanho dos pacotes que trafegam na interface através da opção de MTU e configurar a velocidade e forma de tráfego das informações na opção "*Speed and Duplex".* A configuração do endereço de IP encontra-se logo abaixo de onde configura-se a interface.

3.4.4 Regras de *Firewall* e NAT

Na aba *firewall* podem ser configuradas as regras de acesso a rede interna e quais requisições são possíveis de serem efetuadas para a rede externa. Na tela de configuração das regras é possível verificar que as abas permitem a configuração de

regras dividas por interfaces. Nesta aba também são realizadas as configuração de *aliases*, que são grupos de *hosts*, redes ou portas que facilitam a administração de regras de acesso e NAT, tema que também é tratado nesta mesma aba de configuração, através de *port forwarding*.

Primeiro foi abordada a criação de *aliases*, dentro da opção tem-se 3 tipos de agrupamentos que demonstram grupos de endereços IP, portas de rede e URLs, e existe uma quarta opção que mostra todos os agrupamentos juntos, como pode ser verificado na figura 21.

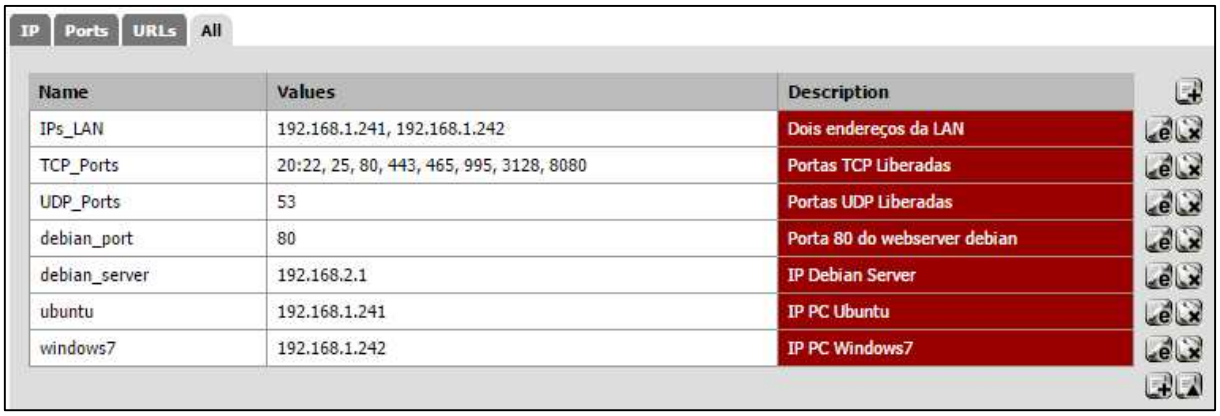


Figura 21 – *Aliases*
Fonte: Autoria Própria

Através do botão que contêm a letra “e”, é possível editar o *alias* e a letra “x” exclui o mesmo. Para adicionar novos *aliases* basta clicar no pequeno “+” que existe logo acima.

Então foi abordada a segunda parte desta aba de configurações, as regras de NAT e *port forwarding*, que se trata de um redirecionamento de portas de conexões vindo da rede externa para a rede interna. No exemplo, como foi demonstrado na figura 22, consiste em redirecionar requisições partindo para o endereço IP externo, o endereço da interface WAN, através da porta 80, para um servidor de página WEB dentro da rede, assim acessando o servidor na rede interna.

Port Forward | 1:1 | Outbound | NPt

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
	WAN	TCP	*	*	*	80 (HTTP)	debian_server	80 (HTTP)	Encaminhamento HTTP para o debian webserver
	WAN	TCP	*	*	*	222	debian_server	22 (SSH)	Encaminhamento SSH para o debian webserver

Figura 22 – *Port Forwarding*
Fonte: Autoria Própria

As demais formas de NAT, 1:1, *outbound* e NPt, não foram abordadas nesse trabalho.

A opção de regras de *firewall*, são divididas por interfaces, como pode ser visualizada na figura 23. Foram abordadas somente as regras específicas de nossas interfaces.

Floating | WAN | LAN | DMZ

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		IPv4 TCP	*	*	debian_server	80 (HTTP)	*	none		NAT Encaminhamento HTTP para o debian webserver
		IPv4 TCP	*	*	WAN address	8080	*	none		Regra para acesso servidor pfSense WAN
		IPv4 TCP	*	TCP_Ports	LAN net	*	*	none		Regra acesso TCP Ports
		IPv4 UDP	*	UDP_Ports	LAN net	*	*	none		Regra acesso UDP Ports
		IPv4 TCP	*	*	debian_server	22 (SSH)	*	none		NAT Encaminhamento SSH para o debian webserver
		IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Regra acesso SSH pfSense
		IPv4 *	*	*	*	*	*	none		Bloqueio total de requisições vindas da WAN

pass / pass (disabled) | block / block (disabled) | reject / reject (disabled) | log / log (disabled)

Figura 23 – Regras de *Firewall*
Fonte: Autoria Própria

Podem ser criadas regras específicas para cada interface, por exemplo, que endereços da rede local acessem somente determinadas portas, para filtrar, por exemplo, somente páginas WEB, bloqueando tráfego para outros serviços. Podem ser também definidas regras que liberem o acesso somente a endereços IP conhecidos da empresa. As regras podem filtrar o endereço de origem, as portas de origem, os endereços de destino e as portas de destino, pode ser também filtrado o protocolo da camada de transporte a ser utilizado, TCP ou UDP. Ao criar-se uma regra de NAT, como foi descrito a pouco, automaticamente o pfSense cria uma regra liberando o acesso ao servidor para o qual o redirecionamento foi criado.

A última parte que foi abordada no trabalho trata dos agendamentos do pfSense. Esse tipo de funcionalidade pode ser utilizada quando necessita-se que os funcionários não tenham determinados acessos durante o horário comercial, porém durante o horário de almoço ou após o expediente seja permitido que o usuário tenha acesso a algumas páginas ou serviços que em horário comercial não tenha possibilidade de usufruir. Pode ser utilizado o agendamento para acessos que possam ser realizados somente em determinados dias ou horários do mês, assim impedindo que usuários acessem determinados serviços em horários errados, como por exemplo, um serviço de ponto.

O pfSense possui serviços de *traffic shaping* e *Virtual IPs*, que são configurados nesta mesma aba, porém esses serviços não foram abordados nesse projeto.

3.4.5 Serviços de Rede

O pfSense possui uma série de serviços de rede que podem ser configurados dentro deste mesmo servidor, assim facilitando o gerenciamento da rede através da centralização destes serviços. Neste trabalho foram abordados somente os serviços de DHCP *server* e *proxy server.*

3.4.6 DHCP Server

O servidor DHCP faz parte do sistema pfSense, ele auxilia na configuração da rede interna provendo endereços para os *hosts* da rede. Neste exemplo habilitou-se o servidor somente na interface LAN. Este servidor possibilita definir o *range* de endereços dinâmicos que será distribuído pelo nosso *firewall*, nesse caso serão os endereços compreendidos no intervalo de 192.168.1.10 até 192.168.1.220 como foi demonstrado na figura 24.

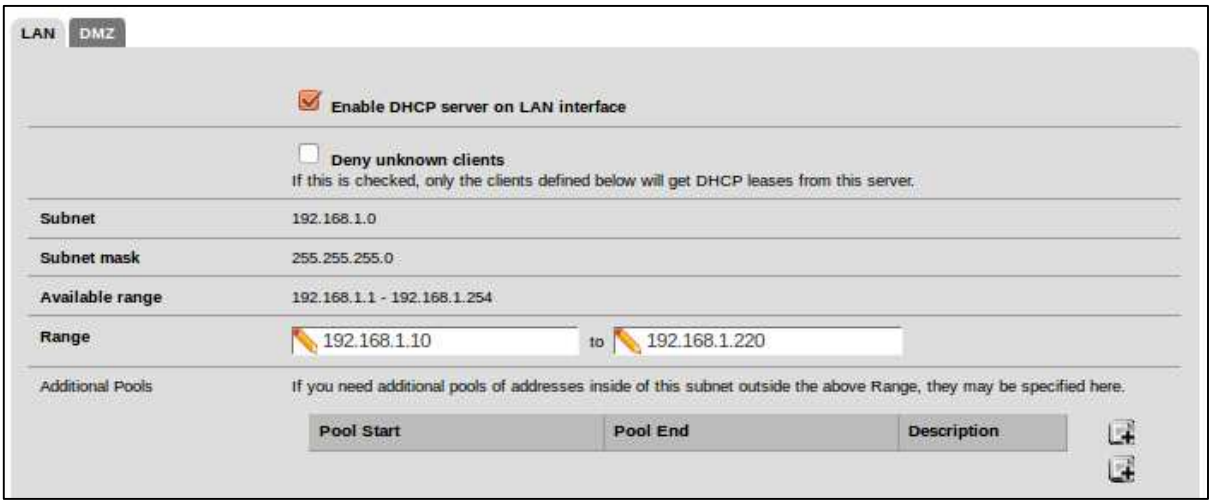


Figura 24 – *Range* DHCP
Fonte: Autoria Própria

Na figura 24 pode ser visualizado que é possível adicionar outros *ranges* de endereço para dividir espaços no mesmo *pool* de endereços para determinadas funcionalidades. Podem ser configurados servidores WINS e DNS específicos para as máquinas, o tempo do *lease*, ou empréstimo de endereço, entre outras funcionalidades. Pode ser controlado o acesso das máquinas através do controle de endereços MAC, endereço físico das placas de rede, para que somente máquinas da rede interna recebam endereços do servidor DHCP.

Caso existam alguns *hosts* que necessitem receber sempre o mesmo endereço IP, pode ser fixado o endereço através do mapeamento de um endereço IP específico para um determinado endereço físico como pode ser verificado na figura 25.

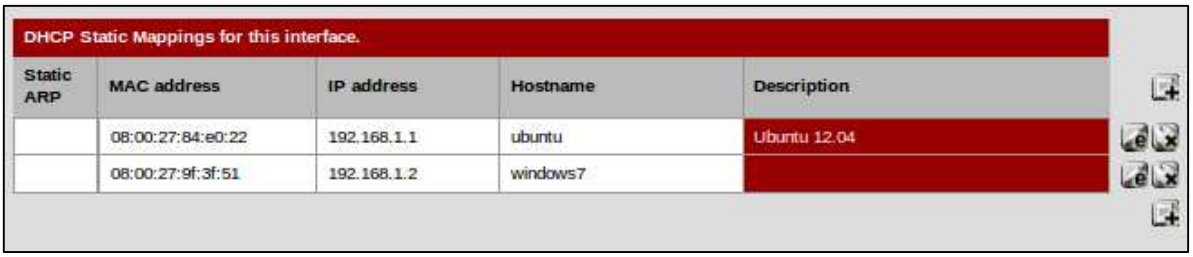


Figura 25 – Mapeamento Fixo DHCP
Fonte: Autoria Própria

3.4.7 Proxy Server

O pfSense pode operar juntamente com servidor *proxy*, assim facilitando e muito o gerenciamento das configurações. O servidor proxy utilizado por este *firewall* é o *squid*, um servidor *proxy* de código aberto muito utilizado em diversas empresas, para sua operação é necessário adicionar o pacote através da aba de configurações vista anteriormente nesse capítulo na opção *packages*. Depois de instalado, o servidor fica habilitado para operar, podendo ser configurado na aba de serviços de rede e possuirá as mesmas funcionalidades de um *squid* configurado diretamente em um sistema operacional Linux ou Unix. Como pode ser verificado na figura 26 existem diversas abas de configuração para o servidor *proxy*, neste projeto foram abordadas somente as abas *general*, *cache managment* e *access control.*

Figura 26 – Abas Configuração *Proxy*
Fonte: Autoria Própria

Foi utilizada a primeira aba para configurar a interface na qual nosso servidor irá operar, no caso foi a interface LAN, de onde virão mais requisições para acessos WEB, foi utilizado a opção de *proxy* transparente para não haver necessidade de configuração no navegador do *host*, em *proxies* transparentes não é possível realizar a autenticação de usuários para um melhor relatórios de acessos, mas como esse não é o escopo do projeto não foi tratado o assunto em detalhes. São possíveis alterações

de diretórios de *log* para acesso às informações do *proxy* nesta mesma aba. Na configuração de *cache*, podem ser realizadas as configurações de tamanho de *cache*, diretórios em que os arquivos serão salvos, formas de substituição de conteúdo gravado, informações que não devem ser salvas para acessos posteriores e um modo *off-line*, para que o servidor não valide as informações em *cache*, assim diminuindo o *overhead* da rede, porém também diminuindo a confiabilidade das informações.

Foi finalizada a configuração do proxy abordando-se os controles de acessos, através destas configurações é possível configurar subredes que possam realizar acesso ao *proxy*, endereços IP irrestritos, os quais as regras do *proxy* não surtirão efeito, *hosts* banidos, listas tanto de endereços permitidos, denominadas *whitelists*, e de endereços proibidos, denominadas *blacklists*. Existem algumas configurações de ACLs que não foram abordadas neste projeto.

3.4.8 Configuração de VPNs

O pfSense pode operar como um servidor de VPNs, utilizando as tecnologias IPsec, L2PT, OpenVPN e PPTP, pelo fato da tecnologia PPTP utilizar algoritmos de criptografia MS-CHAPv2 e este não ser mais considerado seguro é recomendado que esta não seja utilizada. Esta tecnologia não faz parte do escopo do projeto então não foi detalhada a fundo.

3.4.9 Ferramentas de *Status*

Nesta etapa foi demonstrada as ferramentas de *status* do pfSense, elas não foram totalmente descritas, somente as mais importantes para o projeto. A *dashboard*, que é mostrada na tela inicial do *firewall*, pode ser acessada através do *menu* com este nome, nela ficam listadas uma série de informações sobre o servidor, a dashboard pode ser customizada adicionando-se as informações que julgarem essenciais, entre elas pode-se citar por exemplo, o *status* dos *gateways*, que demonstra informações sobre o estado do link, a porcentagem de banda utilizada e o

endereço referente à interface, também utiliza-se os *logs* de acesso do *firewall*, como demonstrado na figura 27.

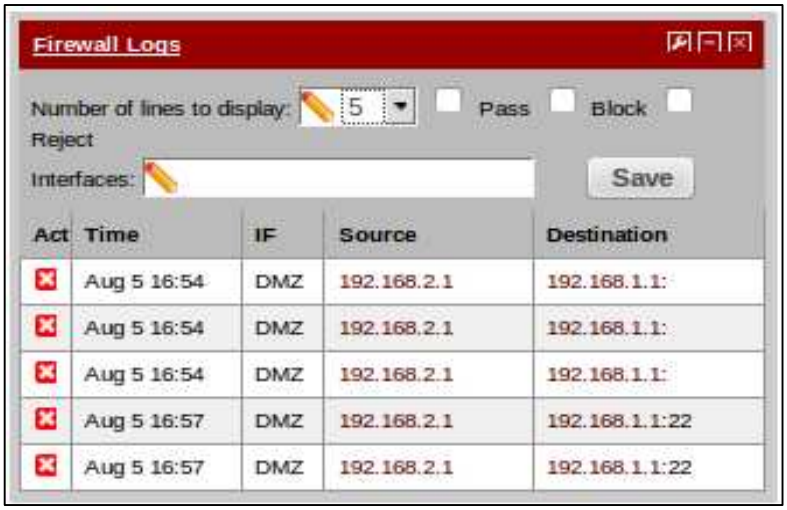


Figura 27 – *Widget* com *Logs* de *Firewall*
Fonte: Autoria Própria

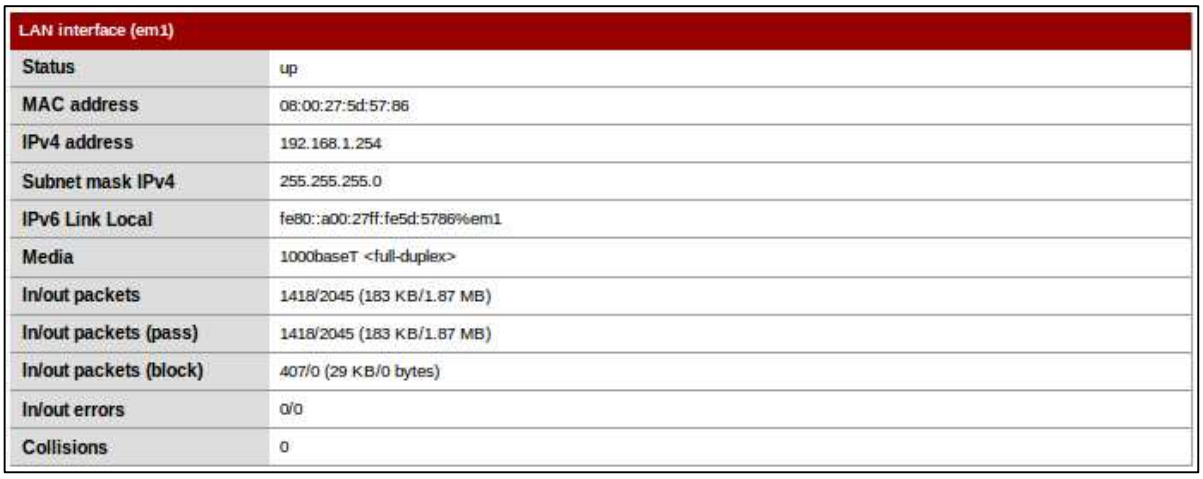
Como pode ser verificado, pode ser escolhida a quantidade de registros a ser exibido, o tipo de regra, seja ela de bloqueio ou permissão, e também pode ser escolhidas as regras de qual interface se deseja verificar, uma ferramenta que facilita a visualização dos registros de acesso.

Como diagnóstico do servidor DHCP, podem ser verificados todos os *leases* realizados pelo servidor através da opção DHCP *leases*. Pode ser verificado tanto *leases* que estão ativos no momento como máquinas que estão desligadas. Pode ser utilizada a opção *WakeOnLan* para ativar os terminais desligados, tema que não foi abordado no projeto.

Através do *menu filter reload* podem ser recarregadas as regras do servidor, em caso de alguma alteração que ainda não tenha sido aplicada automaticamente.

Na opção *gateways* podem ser verificadas as mesmas informações que podem ser visualizadas no *widget* que foi configurado no *dashboard* tema tratado anteriormente neste mesmo capítulo.

Os estados das interfaces podem ser visualizados através do *menu Interfaces*, que lista uma série de informações, como podemos verificar na figura 28.



LAN interface (em1)	
Status	up
MAC address	08:00:27:5d:57:86
IPv4 address	192.168.1.254
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe5d:5786%em1
Media	1000baseT <full-duplex>
In/out packets	1418/2045 (183 KB/1.87 MB)
In/out packets (pass)	1418/2045 (183 KB/1.87 MB)
In/out packets (block)	407/0 (29 KB/0 bytes)
In/out errors	0/0
Collisions	0

Figura 28 – *Status* da Interface LAN
Fonte: Autoria Própria

Também foi demonstrado, o estado da interface, neste caso *up,* o endereço MAC da interface de rede, o endereço IP, neste caso estático, porém quando atribuído via DHCP pode-se realizar o release do mesmo através desta tela, a máscara de rede e um endereço IPv6 são mostrados abaixo. Pode ser também verificada a velocidade atribuída à interface, a contagem de pacotes, tanto os que chegaram ao destino como os que foram bloqueados devido a alguma regra de *firewall* ou erros e o número de colisões que ocorreram naquela interface.

No *menu RRD Graphs* pode ser visto uma série de gráficos do sistema, estes gráficos podem ajudar o administrador do servidor a verificar uma série de informações sobre o *status* do servidor, como mostrado na figura 29.

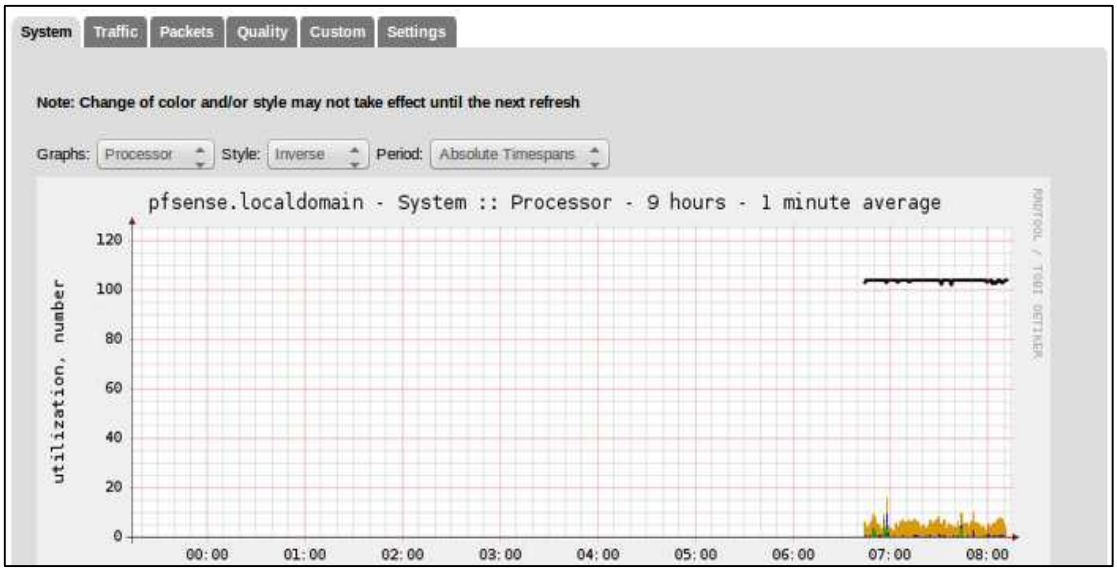


Figura 29 – Gráficos RRD
Fonte: Autoria Própria

Podem ser visualizados gráficos de sistema, que são divididos em uso de CPU, uso de memória e controle de estados, mostrando ao administrador informações referentes ao servidor em si. Podem ser também verificados gráficos de tráfego, específicos ou não de cada interface, tráfego de *streams* de saída da rede e gráficos de IPsec, uma tecnologia VPN. Gráficos de pacote são divididos da mesma forma que os de tráfego, e gráficos de qualidades são divididos por interfaces.

No *menu system logs* podem ser verificados os logs de sistema do pfSense, ferramenta essencial para resolução de possíveis problemas durante a operação. Através dos logs pode ser identificada a origem dos problemas e criar soluções para os mesmos, na figura 30 podem ser verificadas como são organizados os *logs* do sistema pfSense.

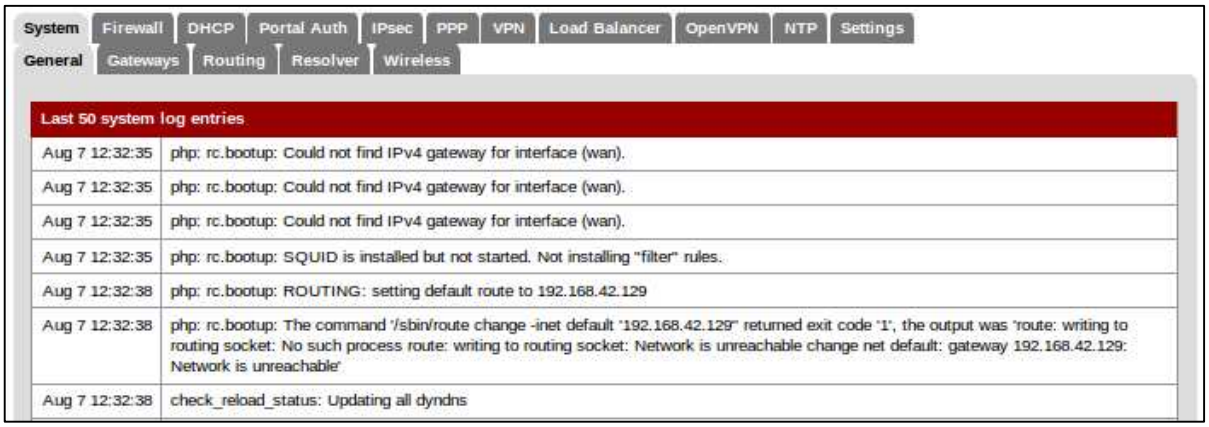


Figura 30 – *Logs* do Sistema
Fonte: Autoria Própria

Podem ser obtidas informações referentes a praticamente todos os serviços em operação no servidor, desde mensagens do sistema, que envolvem serviços rodando no sistema operacional, informações de *gateways*, roteamento e até mesmo *wireless*, se este estiver habilitado. Podem ser retiradas informações referentes às regras de *firewall*, desta forma consegue-se verificar que pacotes estão entrando na rede ou sendo bloqueados, relatórios com informações sobre o servidor DHCP e uma série de outras informações.

3.4.10 Ferramentas de Diagnóstico

Nesta aba de configurações são encontradas diversas funcionalidades de diagnóstico e outras funções de extrema importância para uma melhor segurança e desempenho do *firewall*. Foram exploradas somente algumas das funcionalidades desta aba, como por exemplo, *backup/restore* de configurações do pfSense, um *prompt* de comando para executar comando *shell* e php, ferramentas de DNS *lookup* entre outras. Na figura 31 foram listadas algumas das opções de diagnóstico, foram tratadas todas as opções que podem ajudar um administrador de sistemas a operar da melhor maneira o *firewall.*

Figura 31 – Ferramentas de diagnóstico
Fonte: Autoria Própria

A opção *backup/restore* é uma opção de segurança extremamente útil, ela serve para realizar o *backup* de diversas configurações das funcionalidades do pfSense. Como pode ser verificado na figura 32, estão listadas as opções de *backup* das configurações.

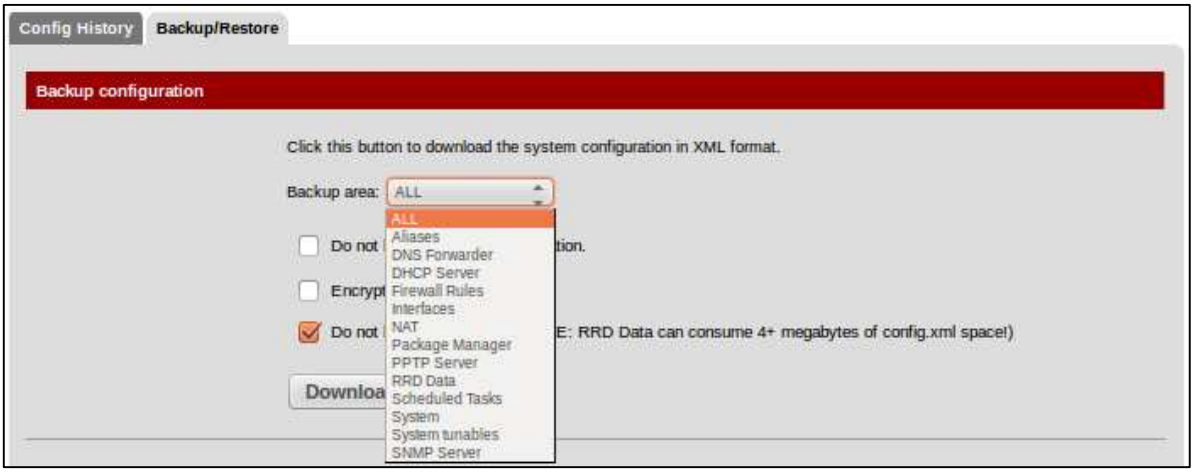


Figura 32 – *Backup* de Sistema
Fonte: Autoria Própria

Pode ser realizado o *backup* de todas as configurações, de *aliases*, de regras de DHCP, regras de *firewall*, configurações de interfaces, regras de NAT, opções de pacotes salvos no sistema, dados obtidos para gráficos RRD, tarefas agendadas e até mesmo informações de um servidor SNMP rodando dentro do servidor. Após selecionada a opção e realizado o *backup*, é gerado um arquivo de configuração com as informações específicas, esse arquivo deve ser guardado em local seguro para um possível problema e restaurado na opção *restore.*

A opção de *restore* funciona de forma inversa ao *backup*, ao invés de gerar um arquivo, será selecionado o arquivo que contem os dados salvos, depois selecionada a opção a qual o arquivo faz parte e então serão restauradas as configurações. É necessário ter cuidado ao restaurar essas informações pois as configurações atuais serão sobrescritas, assim perdendo-se regras que podem não estar salvas nos *backups* atuais.

A opção *command prompt* serve para utilizar comandos em um *shell* Linux ou comandos PHP para algumas funcionalidades específicas. Esta opção não tem suporte por parte do pfSense, então deve ser utilizada somente por usuários que tenham o devido conhecimento nessas linguagens de programação.

Podem ser resolvidos nomes ou endereços IP através da opção DNS*lookup*, ferramenta muito útil para verificação de problemas com servidores DNS ou para encontrar nomes de *hosts* ou endereços através de nomes como pode ser verificado na figura 33.

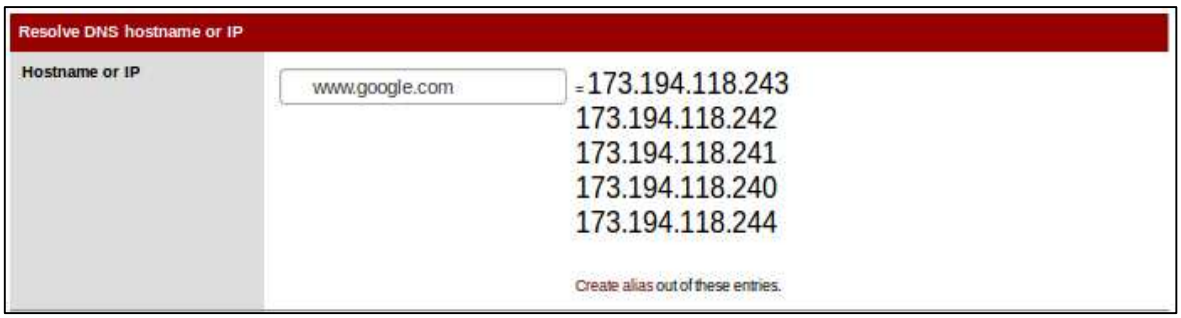


Figura 33 – DNS*lookup*
Fonte: Autoria Própria

Ao tentar resolver o nome de uma página como o *google* por exemplo, o *lookup* resolve o nome e mostra os endereços associados que podem ser utilizados para acessar esta pagina.

É possível efetuar a reinicialização do pfSense através da opção *reboot* ou realizar o desligamento da máquina através da opção *halt.* Também podem ser apagadas as configurações efetuadas no pfSense retornado aos valores padrões do *firewall* através da opção *factory defaults*.

Através da opção *packet capture* pode ser realizada a captura de pacotes de uma determinada interface. É possível filtrar a quantidade de pacotes, a porta pela qual os pacotes estão trafegando, o tamanho dos pacotes, o protocolo da camada de transporte sendo utilizado e filtrar entre pacotes IPv4 e IPv6. Isto ajuda o administrador a verificar se existem alguns pacotes que não deveriam estar trafegando na rede.

Por último foi tratada a opção *traceroute* do pfSense, que funciona igual ao comando *traceroute* do Linux ou *tracert* do Windows. Este comando tem a finalidade de descobrir o caminho que o pacote está fazendo para chegar ao destino, desta forma consegue-se encontrar pontos de falha no trajeto do pacote. Isto é possível da seguinte maneira, é executado um comando de *ping* para cada roteador no caminho do pacote e a cada *hop* no caminho é recebida uma confirmação, então é impresso o nome do roteador, assim quando não houver resposta de determinado roteador consegue-se diagnosticar onde está o problema.

3.4.11 Acesso SSH

Além do acesso WEB, é possível realizar o acesso ao pfSense pela sua interface de gerenciamento via linhas de comando, por acesso remoto através de conexões SSH como demonstrado na figura 34.

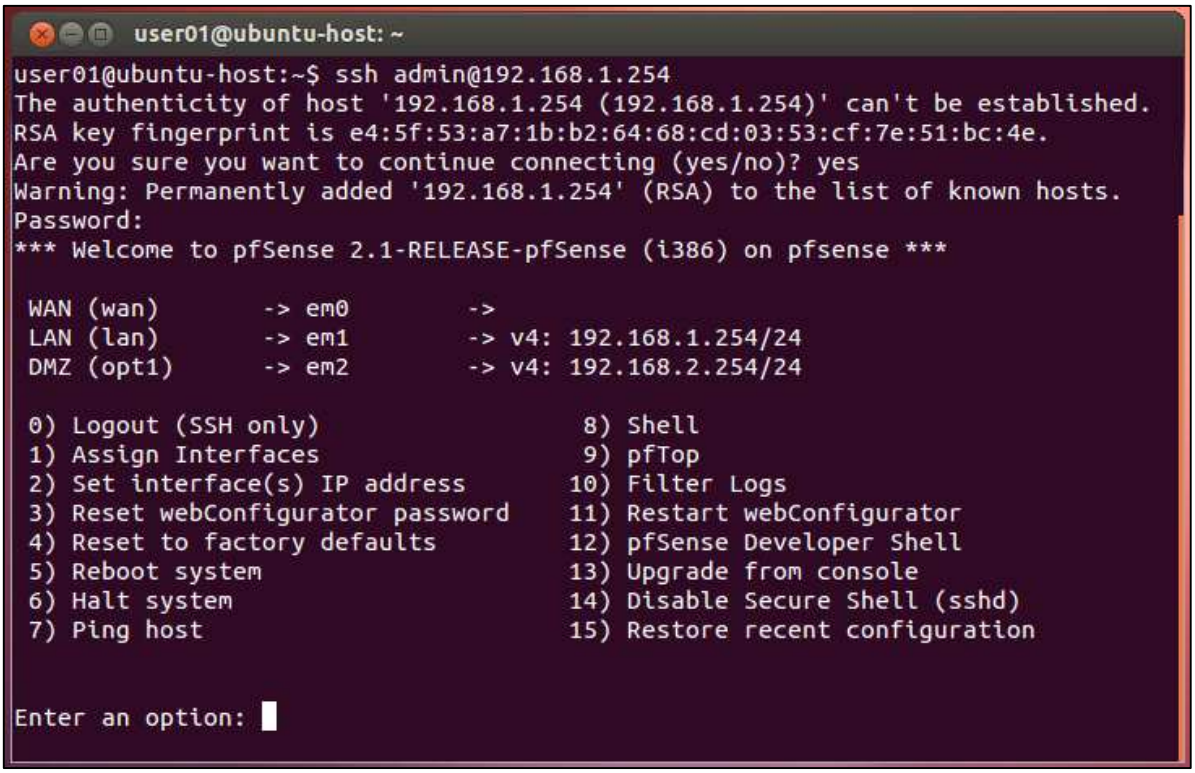


Figura 34 – Acesso SSH
Fonte: Autoria Própria

Na figura 34, foi realizado o acesso ao servidor através de uma conexão SSH vinda de um dos *hosts* da rede interna com o sistema operacional Linux, é importante salientar que somente computador com sistemas operacionais Unix *based,* como Mac OS e Linux possuem conexões SSH em seu sistema operacional por padrão, para realizar esse tipo de conexão em computadores com Windows é necessário um *software* adicional. O acesso via SSH permite que o administrador acesse ao servidor exatamente como se estivesse em frente ao servidor com um monitor conectado ao mesmo. Através desse tipo de acesso pode ser realizada uma série de operações de administração que foram descritas a seguir.

A primeira opção serve para realizar *logout*, podem ser assinaladas interfaces para dividir nossa rede em novas subredes, configuração dos endereços IP das interfaces assinaladas, alteração de senha do administrador de acesso WEB, retorno as configurações padrão do *firewall*, reinicialização do sistema, desligamento do sistema, realização de *ping* para outros *hosts* para verificação de disponibilidade, uma opção para acesso ao *shell* do servidor e acesso as funcionalidades do sistema

operacional FreeBSD do nosso servidor, a ferramenta *pfTop* utilizada para verificar conexões e estados, *logs* dos filtros do *firewall*, opção para reinicialização da interface de configuração WEB, acesso a um *shell* do pfSense no qual é possível realizar alguns comandos como desativar o DHCP e SSH, realizar o *upgrade* de versão do sistema, desativar o acesso remoto via SSH e realizar o *restore* de configurações recentes.

3.5 CONFIGURAÇÕES DA SIMULAÇÃO DE REDE

Neste tópico foram abordadas as configurações que foram realizadas na simulação de rede para o cliente, foram demonstradas configurações de serviços como regras de *firewall,* redirecionamentos NAT, finalização da configuração do servidor DHCP fixando endereços para determinados *hosts* para exemplificar essa funcionalidade, configuração de um servidor *proxy* e demonstração de *logs* de alguns tipos de serviço de modo à exemplificar como funcionaria esse servidor.

3.5.1 Configurações gerais do pfSense

Primeiramente foi configurada a forma de acesso WEB, através da aba opção *advanced* na aba *system* para acessar via HTTP pela porta 8080 para a não utilização da porta padrão, assim a porta 80 do servidor poderia ser utilizada para outra aplicação caso fosse necessário, porém isso não foi abordado no projeto, logo após na mesma tela de configurações foi habilitado o acesso SSH ao servidor através da opção *enable secure shell* e mantida a porta padrão 22 deixando em branco a opção SSH *port.* As figuras 35 e 36 demonstram essas configurações com mais clareza.

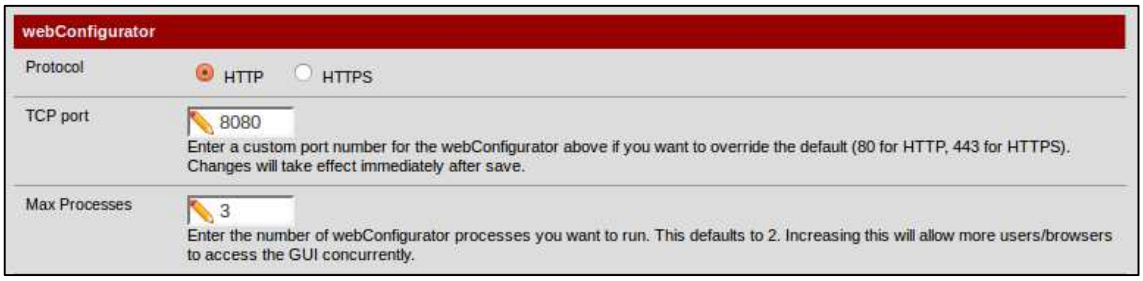


Figura 35 – Configuração de acesso WEB
Fonte: Autoria Própria

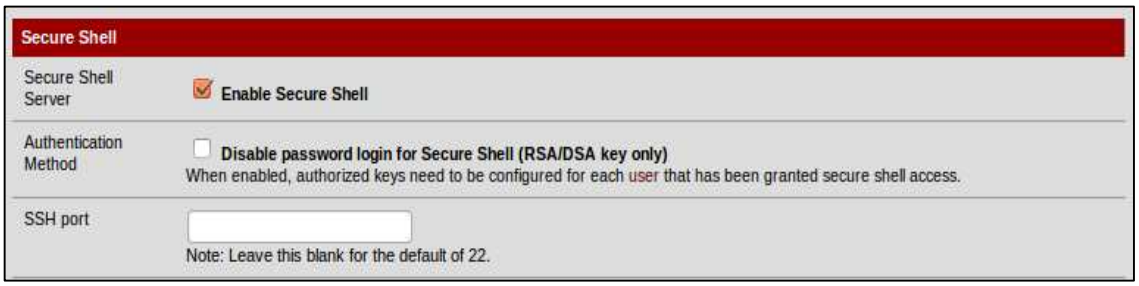


Figura 36 – Habilitando o acesso SSH
Fonte: Autoria Própria

Após esta primeira etapa foi instalado o pacote do servidor *proxy* através da opção *packages* desta mesma aba. Dentro da aba é necessário pesquisar pelo nome do pacote, neste caso será o servidor *squid*, um famoso serviço de *proxy opensource* baseado em sistemas *Unix-like,* após encontrado o pacote solicitado na lista de opções de pacotes clicamos na opção de adicionar que fica do lado direito do pacote, então o sistema pergunta se realmente se deseja instalar e então clica-se em sim para continuar, então o sistema realiza o *download* e instala o pacote automaticamente em uma nova aba chamada *packet installer*, após finalizada a instalação é demonstrado que o pacote já foi instalado. Neste trabalho foi instalado também o pacote Bandwidthd, uma ferramenta para verificar o status do *firewall*. A figura 37 demonstra o pacote instalado.

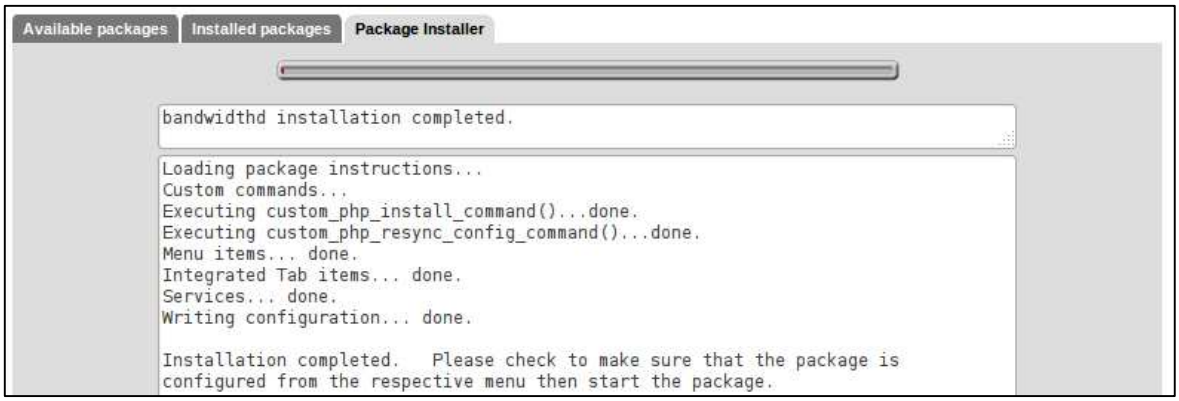


Figura 37 – Instalação de pacote finalizada
Fonte: Autoria Própria

Os pacotes já instalados são listados na aba *installed packages* e através dessa aba eles podem ser reinstalados ou excluidos, somente o pacote, ou todos seus componentes.

3.5.2 Configuração de interfaces

As configurações inicias de interfaces já foram realizadas logo após a instalação do *firewall* pfSense, nesta etapa realizamos a configuração da interface DMZ na qual estão localizados os serviços utilizados pelo cliente, estes serviços estão hospedados em no servidor Linux que utiliza sistema operacional Debian.

A interface DMZ inicialmente era nomeada OPT1, pode ser acessada através da aba de configuração de interfaces, após acessada a tela de configurações de interface pode ser habilitada a interface através da opção *enable interface* e configurado seu nome, nesse caso DMZ. Após estas configurações iniciais foi realizada a configuração do endereço IP desta interface, que será o *gateway* desta mesma rede. O endereço atribuído foi 192.168.2.254 referente à rede 192.168.2.0/24 no campo IPv4 *address*. As figuras 38 e 39 ilustram as duas configurações explicadas acima.

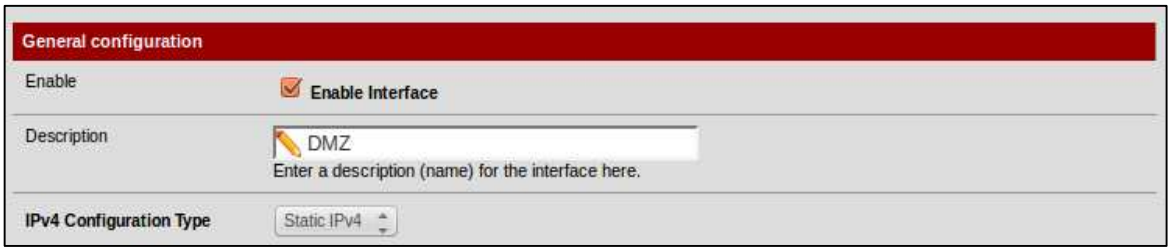


Figura 38 – Habilitando interface DMZ e configurando descrição
Fonte: Autoria Própria

Figura 39 – Habilitando interface DMZ e configurando IP
Fonte: Autoria Própria

3.5.3 Configuração de regras de *Firewall* e NAT

Nesta etapa foram configurados os *aliases*, regras de NAT, regras de *firewall* e regras de agenda ou *schedules.*

Foi iniciada a configuração pelos *aliases*, que nada mais são do que nomes dados a agrupamentos de endereços e portas de redes. Foram agrupados endereços de IP da LAN, os dois endereços que simulam as máquinas da rede, o servidor Debian Linux de nossa rede DMZ e também foi separado as 2 máquinas da rede LAN de forma a interpretá-las como nomes e não como endereço, assim facilitando o entendimento e compreensão das regras de *firewall* e NAT. Os agrupamentos de portas criados foram divididos em TCP_ports, que são as portas que os *hosts* podem acessar para a rede externa, e Debian_ports as portas de acesso ao servidor Debian Linux. Na figura 40 pode ser visualizada essa configuração.

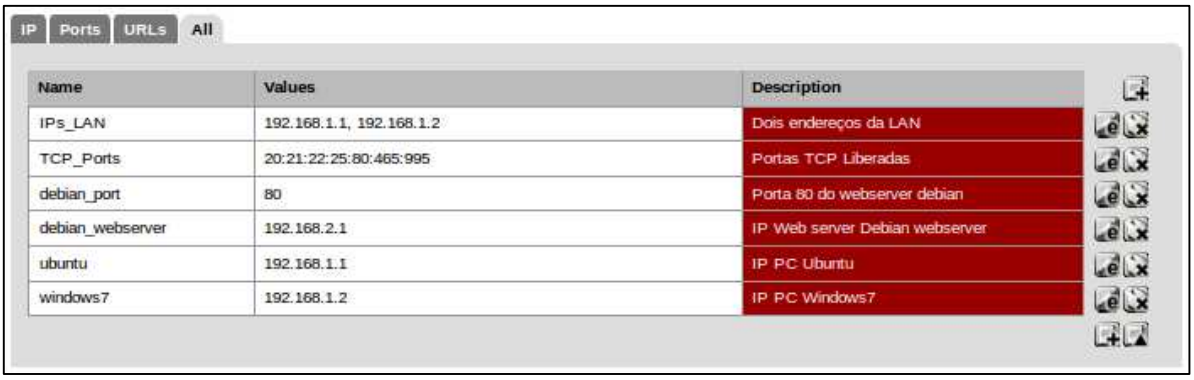


Figura 40 – *Aliases*
Fonte: Autoria Própria

Foi explicado também os redirecionamentos de NAT criados para simular o ambiente de um cliente. Esses redirecionamentos ficam divididos em abas dentro da opção NAT conforme explicado no capítulo anterior, no exemplo foi realizada a configuração de dois redirecionamentos, um utilizado para acessar o servidor Debian através da porta HTTP, assim possibilitando o acesso ao serviço WEB no servidor, e outro redirecionamento da porta 222 para a porta SSH, pois assim é possível realizar acesso SSH externo tanto ao servidor Debian, pela porta 222 como para o *firewall* pfSense através da porta padrão do SSH. A figura 41 demonstra como foram configuradas as regras de redirecionamento no projeto.

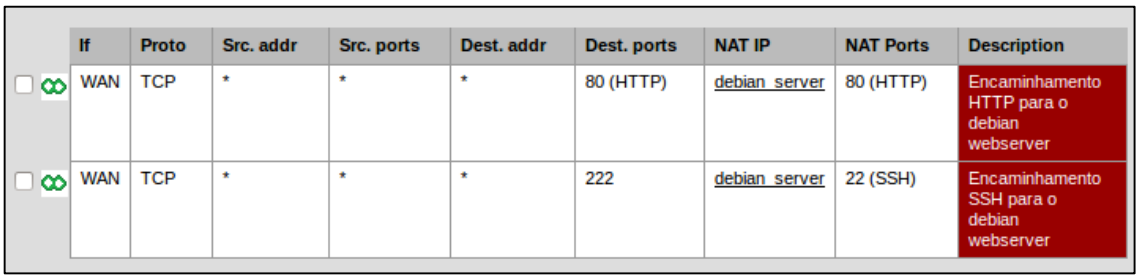


Figura 41 – Redirecionamentos
Fonte: Autoria Própria

Depois de configurado o NAT, foram configuradas as regras de *firewall* do servidor através da opção *rules* da aba *firewall*. Inicialmente foi percebido que foram criadas regras automaticamente para os redirecionamentos NAT, assim evitando que

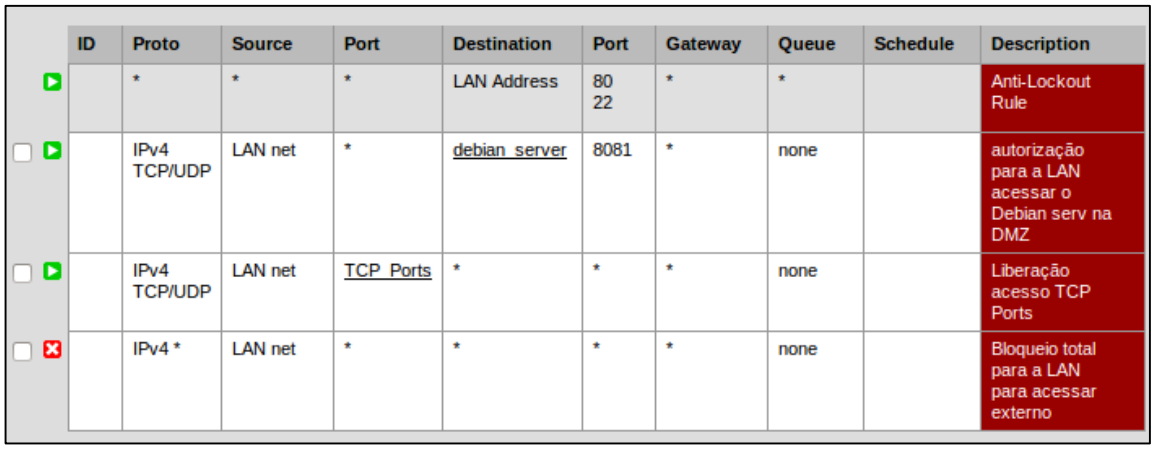
apesar de realizado o redirecionamento, que o pacote seja bloqueado por uma regra de proibição. As regras são divididas por interface como foi demonstrado no capítulo anterior, na figura 42 estão as regras que foram criadas no projeto na interface WAN.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐ ▶		IPv4 TCP	*	*	debian_server	80 (HTTP)	*	none		NAT Encaminhamento HTTP para o debian webserver
☐ ▶		IPv4 TCP	*	*	WAN address	8080	*	none		Regra para acesso servidor pfSense WAN
☐ ▶		IPv4 TCP	*	TCP_Ports	LAN net	*	*	none		Regra acesso TCP Ports
☐ ▶		IPv4 TCP	*	*	debian_server	22 (SSH)	*	none		NAT Encaminhamento SSH para o debian webserver
☐ ▶		IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Regra acesso SSH pfSense
☐ ✖		IPv4 *	*	*	*	*	*	none		Bloqueio total de requisições vindas da WAN

Figura 42 – Regras interface WAN
Fonte: Autoria Própria

A primeira regra que pode ser observada na figura 44 é a liberação NAT, regra criada automaticamente conforme informado a pouco, a segunda regra representa a liberação de acesso à interface WEB do pfSense da rede externa, a terceira regra é um regra utilizada para liberação das portas TCP para a rede LAN, essa regra também demonstra uma forma de utilização dos *aliases* demonstrada a pouco neste capítulo, as duas próximas regras representam uma liberação de SSH para a regra de NAT e uma liberação para acesso SSH vindo da internet para o servidor pfSense e a última regra proíbe o acesso de qualquer coisa que venha da internet para a rede interna, como as regras são ordenadas, tudo o que não esteja compreendido nas regras acima será bloqueado.

Na figura 43 estão listadas as regras da interface LAN.



	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule
		IPv4 TCP/UDP	LAN net	*	debian_server	8081	*	none		autorização para a LAN acessar o Debian serv na DMZ
		IPv4 TCP/UDP	LAN net	TCP_Ports	*	*	*	none		Liberação acesso TCP Ports
		IPv4 *	LAN net	*	*	*	*	none		Bloqueio total para a LAN para acessar externo

Figura 43 – Regras interface LAN
Fonte: Autoria Própria

A primeira regra da figura 43 é uma regra automática do pfSense, uma regra para que a rede LAN não seja excluída do acesso, ela pode ser desabilitada através da opção *advanced*, no mesmo lugar onde pode ser configurada a forma de acesso e o acesso SSH ao servidor. A segunda regra é uma regra de acesso a algum serviço que possa ser utilizado da rede interna através de uma porta que não está nas portas liberadas no servidor Debian Linux, pode ser um serviço de ponto por exemplo. A terceira regra é a liberação de acesso da rede local para qualquer lugar através das portas que foram consideradas necessárias, conforme citado no tópico sobre *aliases*. A última regra bloqueia todos os acessos não liberados nas regras acima, da mesma forma que na interface WAN.

Por finalizar esse tópico foram abordadas as configurações de *schedules* (agendamentos) ou horários específicos. No projeto foi criado somente um *schedule* para horário de expediente, com essa regra, por exemplo, pode ser limitada a conexão HTTP externa somente para horário de almoço ou limitar qualquer outro tipo de serviço. O agendamento foi configurado na opção *schedule* e selecionado durante a criação das regras de *firewall* através da opção *schedules*. Na figura 44 estão demonstradas como ficam listados os horários programados ou *schedules* na opção com o mesmo nome, aqui estão listados o nome do *schedule*, os horários compreendidos nele, note que eles são divididos em opções, podem ser divididos da forma como o administrador preferir.

Name	Time Range(s)			Description
Horario_Comercial	Tues - Sat Tues - Sat	8:00-12:00 13:30-17:30	Manha Tarde	

Figura 44 – *Schedules*
Fonte: Autoria Própria

3.5.4 Servidor DHCP

Neste tópico foi mostrado como foi configurado o servidor DHCP no projeto. As configurações iniciais foram realizadas logo após a instalação do *firewall* como demonstrado anteriormente neste trabalho, agora foram abordadas as configurações através da interface WEB, onde podem ser configurados os hosts que serão fixados para sempre receberem o mesmo endereço, foi demonstrado que o DHCP pode ser configurado em outras interfaces, entre outras funcionalidades. As figuras 45 e 46 demonstram a configuração realizada no servidor DHCP.

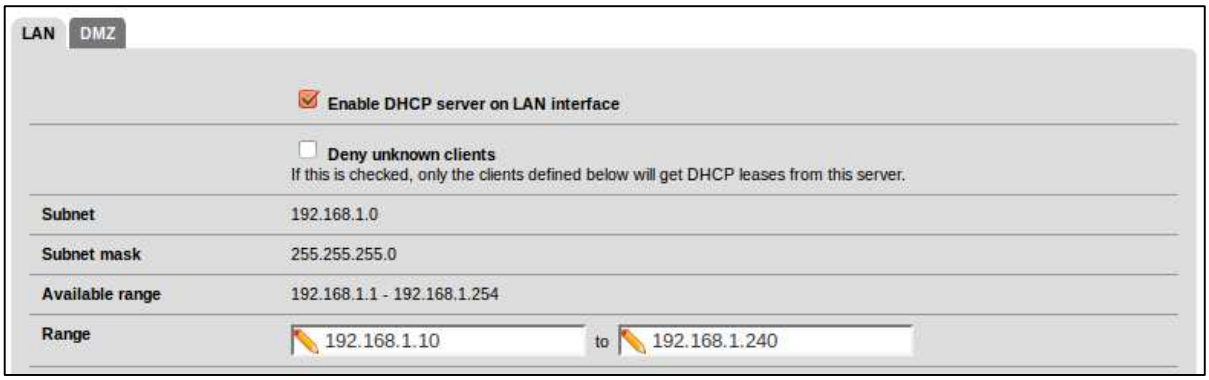


Figura 45 – Configuração *range* DHCP
Fonte: Autoria Própria

DHCP Static Mappings for this interface.

Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:84:e0:22	192.168.1.241	ubuntu	Ubuntu 12.04
	08:00:27:9f:3f:51	192.168.1.242	windows7	Windows 7

Figura 46 – Mapeamento estático de endereços IP
Fonte: Autoria Própria

Pode ser observado que na rede LAN o DHCP está habilitado através da opção *enable DHCP server on Lan interface*, e seu range para empréstimo de endereços vai do endereço 192.168.1.10 até 192.168.1.240. Para ilustrar como é feito o mapeamento estático foram mapeadas as duas máquinas que representam os hosts da rede LAN, uma é a máquina com Windows *7* e outra a máquina com Ubuntu.

3.5.5 Servidor *Proxy*

Para finalizar as configurações da rede, foi configurado um servidor *proxy* para realizar funções de filtragem de acesso WEB e para realizar *cache* de páginas WEB. As figuras 47 e 48 ilustram as configurações aplicadas no *firewall*.

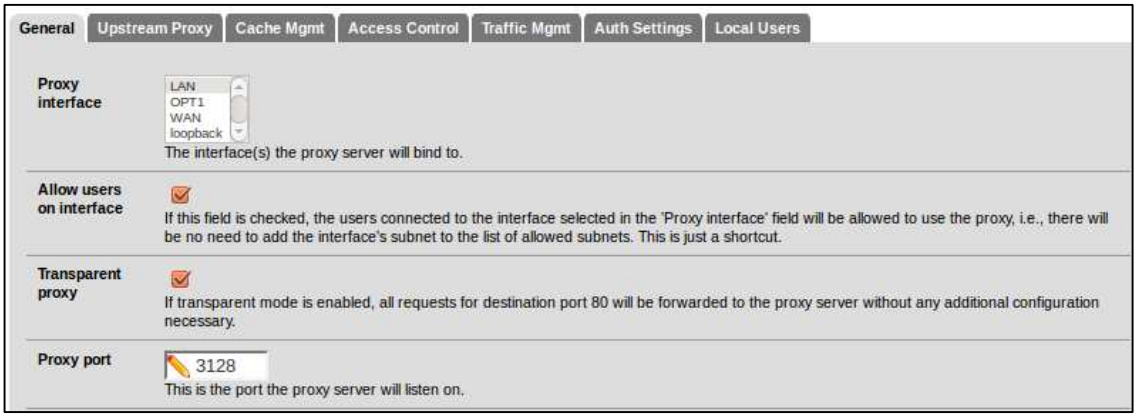


Figura 47 – Configurações gerais *proxy*
Fonte: Autoria Própria

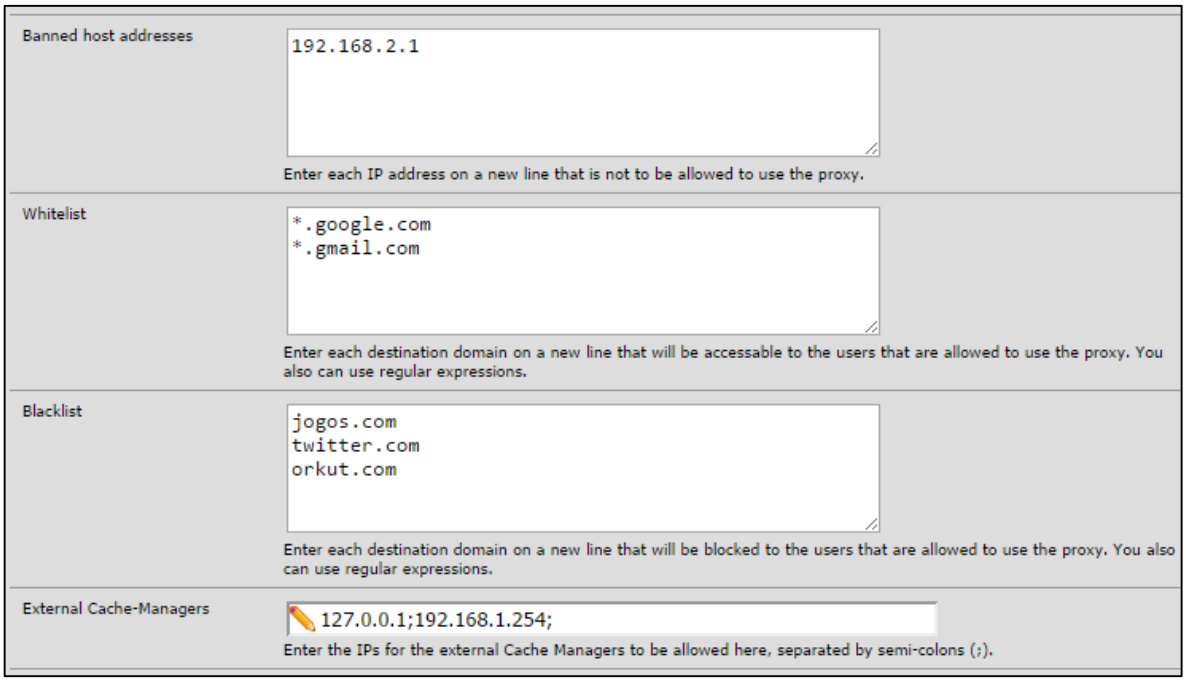


Figura 48 – Configurações acesso *proxy*
Fonte: Autoria Própria

A figura 47 ilustra as configurações básicas do servidor *proxy*, tais como a interface na qual o proxy foi habilitado, no exemplo foi a interface LAN. No projeto foi utilizada a porta 3128, a padrão de servidores *proxy* e foi habilitado o *proxy* para ser transparente ao usuário, não necessitando de nenhuma configuração no navegador, isso facilitou muito a configuração da rede porém impediu de configurar autenticação.

Na figura 48 podem ser visualizadas as configurações de acesso WEB do servidor, foi configurado um *host* banido para propósitos de demonstração, uma *whitelist* com alguns hosts de acesso liberado, nesse tipo de lista são inseridos endereços WEB que podem ser acessados sem a filtragem do proxy. Foi também configurada uma *blacklist*, que contém endereços que serão bloqueados pelo proxy, representa o contrário da *whitelist*.

Nas configurações de *cache* de páginas WEB foram mantidos os valores padrões, como ilustra a figura 49. Em caso de necessidade de alterações para determinadas demandas é possível acessar o manual do servidor *proxy squid* para mais informações.

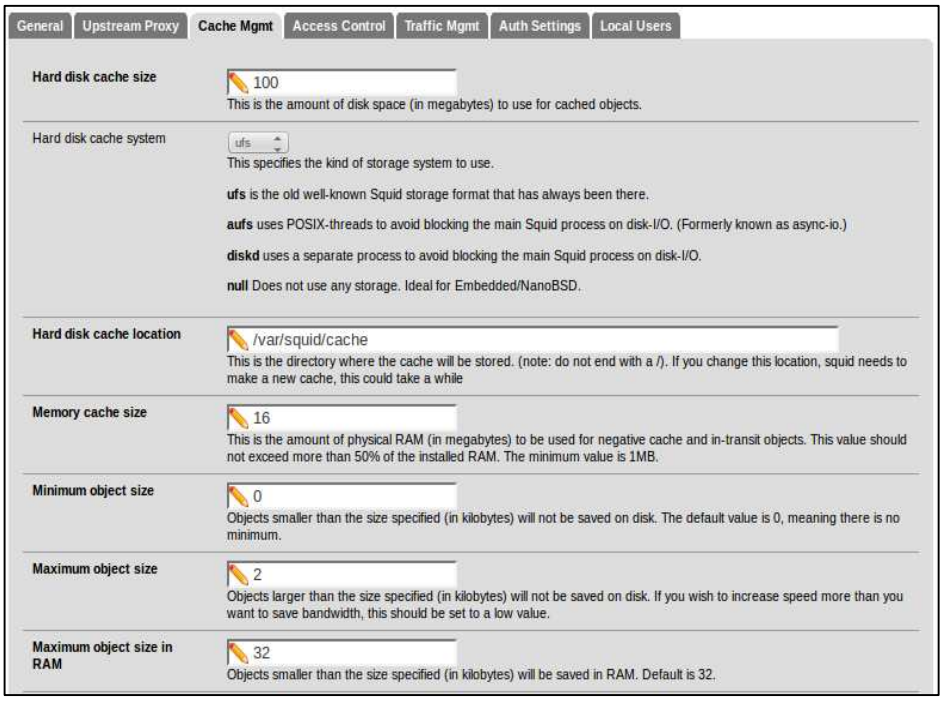


Figura 49 – Configurações cache
Fonte: Autoria Própria

4 CONSIDERAÇÕES FINAIS

Neste projeto foi colocado em prática uma série de aprendizados adquiridos durante o curso em diversas matérias, foram mais utilizados os conhecimentos de redes de computadores adquiridos de disciplinas como redes de acesso, redes de longa distância, comunicação de dados, gerência e programação de redes, entre outras.

O projeto do *firewall* pfSense foi muito útil para a aplicação de uma série de conhecimentos na montagem de um projeto de utilidade profissional. Com os estudos investidos sobre a ferramenta foi descoberto que o pfSense pode ser mais do que uma solução de *firewall* para uma pequena empresa, mas sim uma solução de gerência de redes com diversas funções como servidor DHCP e *proxy* integrado, além de possuir uma fácil interface de gerenciamento e manutenção através de telas de *status e debugging.* Pelo valor que teria de ser investido na tecnologia o pfSense seria uma excelente solução para pequenas e até em alguns casos para médias empresas. Com isso pode ser concluído que o projeto do *firewall* pfSense é viável e a melhor solução *Open Source* pesquisada pela equipe atendendo a demanda por segurança e assim o objetivo deste trabalho.

REFERÊNCIAS

CAMY, Alexandre Rosa; Silva, Evandro R. N.; RIGUI, Rafael. **Seminário de firewalls.** 2003. 27 f. Seminário – Curso de Pós-Graduação em Ciência da Computação, UFSC, Florianópolis.

INTELBRAS. **Redirecionamento de Portas**. Disponível em: < http://www.intelbras.com.br/simuladores/wig240/portfw.html >. Acesso em: 25 abr. 2014.

ISO/IEC 27000. **Norma ISO/IEC 27000.** Disponível em: www.iso27000.com.br. Acesso em: 01 nov. 2013.

LEGAUSS. **SSH - Dicas, truques e um tutorial sobre o protocolo**. Disponível em: < http://legauss.blogspot.com.br/2012/07/ssh-dicas-truques-e-um-tutorial-sobre-o.html >. Acesso em: 25 abr. 2014.

PFSENSE. **pfSense.** Disponível em: < www.pfsense.org.br >. Acesso em: 28 out. 2013.

PLANETA TECNOLOGIA. **Configurando elastic load balancing amazona web-services**. Disponível em: < http://planetatecnologia.com/wp-content/uploads/2012/01/elastic-load-balancer-cenario-1.png > Acesso em: 30 jul. 2014.

STATO FILHO, André. **Linux Controle de Redes.** 1ª ed. Florianópolis: Editores Visuais Books, 2009.

TANENBAUM, Andrew S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Elsevier, 2003.

TECHNET. **Como funciona o balanceamento de carga de rede.** Disponível em: < http://technet.microsoft.com/pt-br/library/cc738894%28v=ws.10%29.aspx >. Acesso em: 29 abr. 2014.

TELECO. **Endereçamento IP.** Disponível em: < http://www.teleco.com.br/ip.asp >. Acesso em: 25 abr. 2014.