

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

JULIO CESAR BOFF

**ANÁLISE DAS DISTRIBUIÇÕES PFSENSE E ENDIAN PARA
IMPLANTAÇÃO DE FIREWALL EM REDES SOHO**

TRABALHO DE CONCLUSÃO DE CURSO

**PATO BRANCO
2015**

JULIO CESAR BOFF

**ANÁLISE DAS DISTRIBUIÇÕES PFSENSE E ENDIAN PARA
IMPLANTAÇÃO DE FIREWALL EM REDES SOHO**

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Fábio Favarim

**PATO BRANCO
2015**

TERMO DE APROVAÇÃO

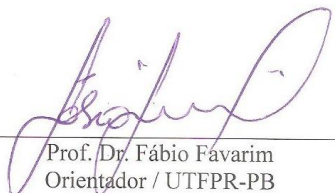
Análise das distribuições pfSense e Endian para implantação de firewall em redes SOHO

por

Julio Cesar Boff

Esta monografia foi apresentada às 18h30min do dia 20 de outubro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

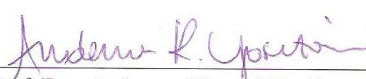
Banca Examinadora



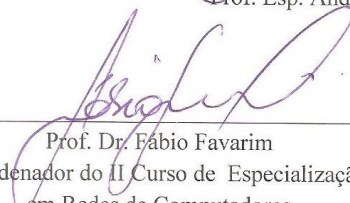
Prof. Dr. Fábio Favarim
Orientador / UTFPR-PB



Prof. M.Sc. Adriano Serckumecka
UTFPR-PB



Prof. Esp. Anderson Kiyoshi Yoshitome



Prof. Dr. Fábio Favarim
Coordenador do II Curso de Especialização
em Redes de Computadores

DEDICATÓRIA

Dedico este trabalho a Deus e a minha família, minha esposa Naraiana e ao meu filho Murilo que me apoiaram em todos os momentos necessários para cursar este curso e a elaboração do trabalho final.

AGRADECIMENTOS

Gostaria de agradecer ao professor Dr. Fábio Favarim por sua orientação, pela sua compreensão e apoio para a elaboração deste trabalho, juntamente aos demais professores.

O Senhor é o meu pastor e nada me faltará. Deita-me em verdes pastos e guia-me mansamente em águas tranquilas. Refrigera a minha alma, guia-me pelas veredas da justiça, por amor do seu nome. Ainda que eu ande pelo vale da sombra da morte, não temerei mal algum, porque Tu estás comigo, a Tua vara e o Teu cajado me consolam. Prepara-me uma mesa perante os meus inimigos, unges a minha cabeça com óleo, o meu cálice transborda. Certamente que a bondade e a misericórdia me seguirão todos os dias da minha vida e habitarei na casa do SENHOR por longos dias.

Salmo 23

RESUMO

BOFF, Julio Cesar. Análise das Distribuições pfSense e Endian para Implantação de Firewall em redes SOHO. 2015. 54 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores) Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015

Redes SOHO se caracterizam principalmente por possuírem poucos dispositivos e poucos usuários em uma pequena área, normalmente, em um pequeno escritório, uma casa ou apartamento. O uso de dispositivos para acesso à Internet para diversos fins como uso corporativo, uso pessoal, acesso a bancos, redes sociais está crescendo a cada dia, e a segurança dos dados trafegados pela rede torna-se essencial. O uso de soluções que permitam aumentar a segurança desses os dados é fundamental, no entanto muitas soluções existentes são complexas de implantar e configurar, assim como na maioria das vezes são pagas. Existem distribuições gratuitas e de fácil configuração, que auxiliam na prevenção de diversos incidentes e aumentam a segurança dos dados. Neste trabalho é reportada a análise, instalação, configuração e comparação entre Endian Firewall Community e o pfSense, ambos gratuitos para uso em redes SOHO.

Palavras-chave: Firewall, Segurança da Informação, Redes Domésticas, Pequenos Escritórios.

ABSTRACT

BOFF, Julio Cesar. Analysis of pfSense and Endian Firewall Distributions for implantation in SOHO networking. 2015. 54 f. Working monograph of Course (II Specialization Course in Computer Networks) Academic Department of Informatics, Federal Technological University of Paraná, Campus Pato Branco. Pato Branco, 2015

SOHO networks are mainly characterized by having few devices and few users in a small area , usually in a small office , a house or apartment . The use of devices to access the Internet for various purposes as business use , personal use , access to banks , social networks is growing every day, and security of data traffic over the network becomes essential . The use of solutions that will enhance the security of the data is critical , however many existing solutions are complex to deploy and configure , and most often are paid . There are free and easy to configure distributions , which help in preventing various incidents and increase data security . This paper reported the analysis , installation, configuration and comparison of Endian Firewall Community and pfSense are free for use in SOHO network .

Key-words: Firewall, Information Security, Home Network, Small Offices.

LISTA DE FIGURAS

Figura 1 – Proporção de Domicílios com Acesso à Internet.....	19
Figura 2 – Atividades Realizadas pela Internet	20
Figura 3 – Atributos Básicos da Informação.....	21
Figura 4 – Estrutura Básica de um Firewall.....	22
Figura 5 – Tecnologias de Firewall.....	22
Figura 6 – Arquitetura Dual-Homed Host	25
Figura 7 – Arquitetura Screened Host	26
Figura 8 – Arquitetura Screened Subnet	26
Figura 9 – Arquitetura do Ambiente Cooperativo	27
Figura 10 – Tela principal da Ferramenta Wireshark.	29
Figura 11 – Ambiente de Teste.	35
Figura 12 – Wireshak Tela Inicial.	36
Figura 13 – Tela Inicial do Endian Firewall Community.....	37
Figura 14 – Acesso ao Endian pelo Browser	38
Figura 15 – Configuração da Regra 1 no Endian.	38
Figura 16 – Configuração da Regra 2 no Endian.	39
Figura 17 – pfSense – Tela Inicial.....	40
Figura 18 – pfSense – Tela Principal / Menu.....	40
Figura 19 – pfSense – Tela de Login.	41
Figura 20 – pfSense – Tela Principal pelo browser.	41
Figura 21 – pfSense – Alterar Idioma.....	42
Figura 22 – pfSense – Criação de Aliases.	43
Figura 23 – pfSense – Regras de Firewall.	43
Figura 24 – pfSense – Configuração do Snort.	44
Figura 25 – Endian – Primeira Regra Desabilitada.	44
Figura 26 – Endian – Acesso liberado com a Regra Desabilitada.....	45
Figura 27 – Endian – Primeira Regra Habilitada.	45
Figura 28 – Endian – Bloqueio da Primeira Regra.	46
Figura 29 – pfSense – Regra Desabilitada.....	46
Figura 30 – pfSense – Acesso Permitido ao Facebook.....	47
Figura 31 – pfSense – Regra Habilitada	47
Figura 32 – pfSense – Acesso Bloqueado ao Facebook.....	48
Figura 33 – pfSense – Registro de Log de Tentativas de Acesso.....	48
Figura 34 – Wireshark – Monitoramento de Pacotes antes de ativar o Firewall.....	49
Figura 35 – Wireshark – Monitoramento de Pacotes com Firewall Ativado.	49
Figura 36 – pfSense – Dashboard.....	50
Figura 37 – Endian – Informações de Hardware.	51

LISTA DE TABELAS

Tabela 1 - Proporção de Domicílios que Possuem Equipamentos TIC – 2014.....	18
Tabela 2 - Proporção de Domicílios com Acesso à Internet - 2014.....	19

LISTA DE QUADROS

Quadro 1 - Endian Firewall - Especificações por Versões	31
Quadro 2 - Especificações Computador Usuário	32
Quadro 3 - Especificações Computador para os Firewall	33

LISTA DE ABREVIATURAS E SIGLAS

ABNT	<i>Associação Brasileira de Normas Técnicas</i>
ARM	<i>Advanced RISC Machine</i>
CA	<i>Certification Authority</i>
CD-ROM	<i>Compact Disc - Read Only Memory</i>
DMZ	<i>Demilitarized Zone</i>
FTP	<i>File Transfer Protocol</i>
GPL	<i>General Public License</i>
GUI	<i>Graphical User Interface</i>
HD	<i>Hard Disk</i>
HTTP	<i>HyperText Transfer Protocol</i>
ICMP	<i>Internet Control Message Protocol</i>
IDS	<i>Intrusion detection system</i>
IEC	<i>International Electrotechnical Commission</i>
IP	<i>Internet Protocol</i>
ISO	<i>Organização Internacional de Normalização</i>
LAN	<i>Rede Local</i>
NAT	<i>Network Address Translation</i>
NBR	<i>Norma Brasileira</i>
nic.br	<i>Núcleo de Informação e Coordenação do Ponto BR</i>
P2P	<i>Peer-to-peer</i>
PC	<i>Computador Pessoal</i>
PCAP	<i>Packet Capture</i>
PKI	<i>Public Key Infrastructure</i>
SM	<i>Salário Mínimo</i>
SO	<i>Sistema Operacional</i>
SOHO	<i>Small Office, Home Office</i>
SPAM	<i>Sending and Posting Advertisement in Mass</i>
TCP	<i>Transmission Control Protocol</i>
TIC	<i>Tecnologia da Informação e Comunicação</i>
URL	<i>Uniform Resource Locator</i>
UTM	<i>Unified Threat Management</i>
VPN	<i>Virtual Private Network</i>
WAN	<i>Rede de Área Extensa</i>

SUMÁRIO

1 INTRODUÇÃO	14
1.1 CONSIDERAÇÕES INICIAIS	14
1.2 OBJETIVOS	15
1.2.1 Objetivo Geral.....	15
1.2.2 Objetivos Específicos.....	15
1.3 JUSTIFICATIVA	15
1.4 ESTRUTURA DO TRABALHO	16
2 REFERENCIAL TEÓRICO.....	17
2.1 REDES DE COMPUTADORES.....	17
2.2 REDES DOMÉSTICAS	17
2.3 SEGURANÇA DA INFORMAÇÃO	20
2.4 FIREWALL	21
2.4.1 ARQUITETURA DE FIREWALL.....	25
3 MATERIAIS E MÉTODO.....	28
3.1 MATERIAIS.....	28
3.1.1 Wireshark.....	28
3.1.2 Endian: Internet Security	29
3.1.2.1 Endian <i>Firewall Community</i>	31
3.1.3 pfSense	32
3.1.4 Computadores.....	32
3.2 MÉTODO.....	33
4 RESULTADOS.....	35
4.1 APLICAÇÃO PRÁTICA	35
4.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO WIRESHARK.....	36
4.1.2 INSTALAÇÃO E CONFIGURAÇÃO DO ENDIAN.....	37
4.1.3 INSTALAÇÃO E CONFIGURAÇÃO DO PFSENSE	39
4.1.4 TESTES DAS REGRAS E ANÁLISE NO WIRESHARK	44
4.1.4.1 TESTES NO ENDIAN.....	44
4.1.4.2 TESTES NO PFSENSE	46
4.1.4.2 TESTES NO WIRESHARK.....	49
4.2 COMPARAÇÃO ENTRE FIREWALL.....	50
5 CONCLUSÃO	52
REFERÊNCIAS.....	53

1 INTRODUÇÃO

Este capítulo apresenta as considerações iniciais do trabalho, os objetivos, a justificativa de realização do mesmo e a organização do texto.

1.1 CONSIDERAÇÕES INICIAIS

A utilização da Internet é indispensável nos dias atuais no trabalho ou lazer, ambiente cooperativos ou doméstico. SOHO é uma abreviatura para *Small Office / Home Office*, definição para redes de computadores de pequeno porte, escritórios montados em casa em uma rede doméstica, destinados para realização de atividades profissionais, e juntamente atividades pessoais.

O número de domicílios com acesso à tecnologia da informação e a Internet está crescendo a cada dia. Dados do NIC.br (2014) indicam que 49% dos domicílios no Brasil tem computador e 43% tem acesso à Internet.

A maioria dos usuários de redes SOHO que acessam os serviços que estão disponíveis pela Internet, apenas estão preocupados em acessar o serviço e que este esteja disponível a qualquer momento. Ao acessar um serviço, dados do usuário são enviados pela rede, estando sujeito a interceptação por terceiros, ou ainda o computador estando conectado à rede está também sujeito a infecção por vírus ou até mesmo a invasão por usuários externos, podendo resultar em prejuízos tanto financeiros, como à imagem e reputação das pessoas.

No entanto, os usuários na maioria das vezes não se importam com a segurança de sua rede até que tenha tido um incidente relacionado. Desta forma, faz-se necessário esses usuários terem alguma solução para aumentar a segurança de sua rede de modo a reduzir os riscos com ataques, infecção de vírus, vazamento ou perda de informação.

Para aumentar a segurança, a maioria dos usuários faz uso de programas antivírus. Porém, apenas ter um antivírus instalado em um computador não implica em ter a garantia que o computador estará livre de acessos não autorizados.

Uma ferramenta que, em conjunto com os antivírus, permite para aumentar a segurança em redes de computadores é o firewall. O firewall tem como principal objetivo analisar os pacotes que trafegam em uma rede, barrando as entradas ou saídas de pacotes não autorizados na rede.

1.2 OBJETIVOS

Este trabalho de conclusão de curso se refere ao estudo referente a segurança de redes SOHO e a seguir são descritos seu objetivo geral e seus objetivos específicos. O objetivo geral está relacionado ao resultado principal obtido com o desenvolvimento deste trabalho e os objetivos específicos o complementam.

1.2.1 Objetivo Geral

Analisar as funcionalidades e características de duas distribuições de firewall gratuitas (pfSense e Endian) para uso em redes SOHO.

1.2.2 Objetivos Específicos

Como forma de complementar o objetivo geral foram definidos os seguintes objetivos específicos:

- Definir políticas de segurança mínima a ser aplicada em redes SOHO;
- Verificar o comportamento das distribuições gratuitas de firewall aplicando em redes SOHO.
- Relatar os resultados obtidos das ferramentas de acordo com as políticas de segurança definidas.

1.3 JUSTIFICATIVA

De modo a aumentar a segurança em redes SOHO, sem que seus usuários tenham que se preocupar diretamente com a questão da segurança, este trabalho visa propor a utilização de distribuições gratuitas de firewall. A implantação de um firewall na rede, além de reduzir a possibilidade de invasão da rede por usuários externos, também permite o bloquear o acesso a sites indevidos (pornografia, pedofilia, pirataria). Regras podem ser definidas de modo a especificar o que pode e o que não pode ser acessado na Internet. Essas regras podem ser utilizadas de várias maneiras e aplicadas para cada dispositivo e para cada usuário na rede de forma diferente. Por exemplo, poderia ser restringido totalmente o acesso a sites impróprios ou ainda pode ser restringido o horário de acesso a determinados sites.

1.4 ESTRUTURA DO TRABALHO

Este capítulo apresentou as considerações iniciais, os objetivos e a justificativa para o desenvolvimento deste trabalho. No Capítulo 2 está o referencial teórico apresentando conceitos relacionados a redes de computadores, redes domésticas, segurança da informação e Firewall. O Capítulo 3 apresenta as ferramentas e o método utilizados no desenvolvimento do trabalho juntamente com suas características. No Capítulo 4 estão os resultados. Esse capítulo contém a descrição dos testes, instalação, configuração e comparação entre as distribuições de firewall. Por fim, no Capítulo 5 está a conclusão com as considerações finais.

2 REFERENCIAL TEÓRICO

Este capítulo contém o referencial teórico do trabalho apresentando conceitos sobre redes de computadores, redes domésticas, segurança da informação e firewall.

2.1 REDES DE COMPUTADORES

Redes de computadores são estruturas físicas (equipamentos) e lógicas (programas, protocolos) que permitem que dois ou mais computadores possam compartilhar suas informações entre si. Quando um computador está conectado a uma rede de computadores, ele pode ter acesso às informações que chegam a ele e às informações presentes nos outros computadores ligados a ele na mesma rede, o que permite um número muito maior de informações possíveis para acesso através daquele computador.

Segundo Douglas Rocha Mendes (2007), Redes de computadores estabelecem a forma-padrão de interligar computadores para o compartilhamento de recursos físicos ou lógicos. Esses recursos podem ser definidos como unidades de CD-ROM, diretórios do disco rígido, impressoras, scanners, placa de fax modem entre outros. Saber definir que tipo de rede e que sistema operacional deve ser utilizado, bem como efetuar a montagem deste tipo de ambiente, é um pré-requisito para qualquer profissional de informática que pretende uma boa colocação no mercado de trabalho.

Segundo Kurose (2010), a Internet pública é uma rede de computadores mundial, uma rede que interconecta milhares de dispositivos computacionais ao redor do mundo. Existem cada vez mais dispositivos conectados à Internet, como TVs, laptops, consoles para jogos, telefones celulares, webcams, automóveis, dispositivos de sensoriamento ambiental, quadro de imagens, sistemas internos elétricos e de segurança. Isso põe o fim na limitação que a até pouco tempo ficava entre computadores, estações de trabalho e servidores, acesso a páginas da web e trocas de mensagens de e-mail.

2.2 REDES DOMÉSTICAS

Redes domésticas se caracterizam principalmente por fazer parte de um grupo de dispositivos em uma pequena área. O uso doméstico de dispositivos para acesso

à Internet para diversos fins como uso pessoal, acesso a banco, redes social está crescendo a cada dia, e sua segurança de dados e conteúdo é fundamental.

O número de domicílios que possuem dispositivos que se comunicam entre si, dando origem as redes domésticas já consta com um alto percentual, dados mostrados na Tabela 1, demonstram a proporção de domicílios que possuem computador portátil, computadores de mesa e tablet.(NIC.br - 2014).

Tabela 1 - Proporção de Domicílios que Possuem Equipamentos TIC – 2014

Percentual (%)		Computador portátil	Computador de mesa	Tablet
TOTAL		30	28	17
Área	Urbana	33	31	19
	Rural	13	11	4
Região	Sudeste	34	36	21
	Nordeste	21	19	11
	Sul	42	27	15
	Norte	21	16	8
	Centro-Oeste	28	28	16
Renda familiar	Até 1 SM (Salário Mínimo)	6	9	5
	Mais de 1 SM até 2 SM	19	20	10
	Mais de 2 SM até 3 SM	36	30	18
	Mais de 3 SM até 5 SM	49	45	25
	Mais de 5 SM até 10 SM	73	57	41
	Mais de 10 SM	83	53	51
Classe social	A	92	73	55
	B	60	51	32
	C	25	26	13
	DE	5	6	3

Fonte: TIC Domicílios – Acesso às Tecnologias da Informação e da Comunicação (NIC.br, 2014).

Segundo NIC.br os números referente a domicílios que tem conexão com a Internet muda um pouco conforme representado na Tabela 2.

Tabela 2 - Proporção de Domicílios com Acesso à Internet - 2014

Percentual (%)		Sim	Não	Não sabe / Não respondeu
TOTAL		43	56	0
Área	Urbana	48	52	0
	Rural	15	85	0
Região	Sudeste	51	48	0
	Nordeste	30	69	0
	Sul	51	49	0
	Norte	26	74	0
	Centro-Oeste	44	54	2
	Até 1 SM	11	88	0
Renda familiar	Mais de 1 SM até 2 SM	27	73	0
	Mais de 2 SM até 3 SM	52	48	0
	Mais de 3 SM até 5 SM	70	30	1
	Mais de 5 SM até 10 SM	84	16	0
	Mais de 10 SM	91	9	0
	Classe social	A	98	2
B		80	20	0
C		39	61	0
DE		8	91	1

Fonte: TIC Domicílios – Acesso às Tecnologias da Informação e da Comunicação (nic.br, 2014).

Esses números mudam gradativamente a cada ano, tendo um aumento de mais de 100% entre o ano de 2008 a 2013 conforme mostra a Figura 1 (NIC.br, 2014).

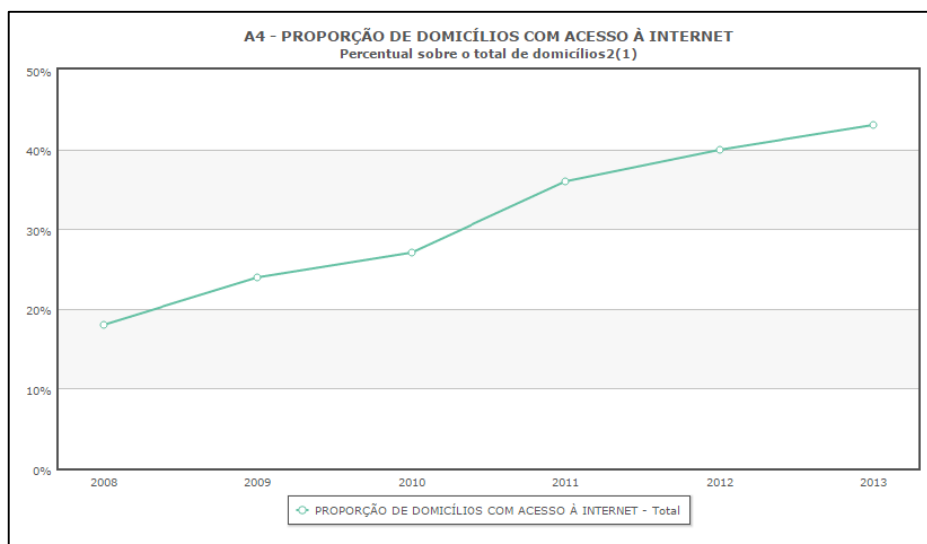


Figura 1 – Proporção de Domicílios com Acesso à Internet
Fonte: NIC.br (2014).

As atividades realizadas na Internet variam bastante, algo cada vez mais comum na vida das pessoas, fazendo parte das atividades do dia-a-dia, tanto para

lazer ou trabalho, na Figura 2 mostras as atividades realizadas na Internet pelo percentual total de usuários de Internet.

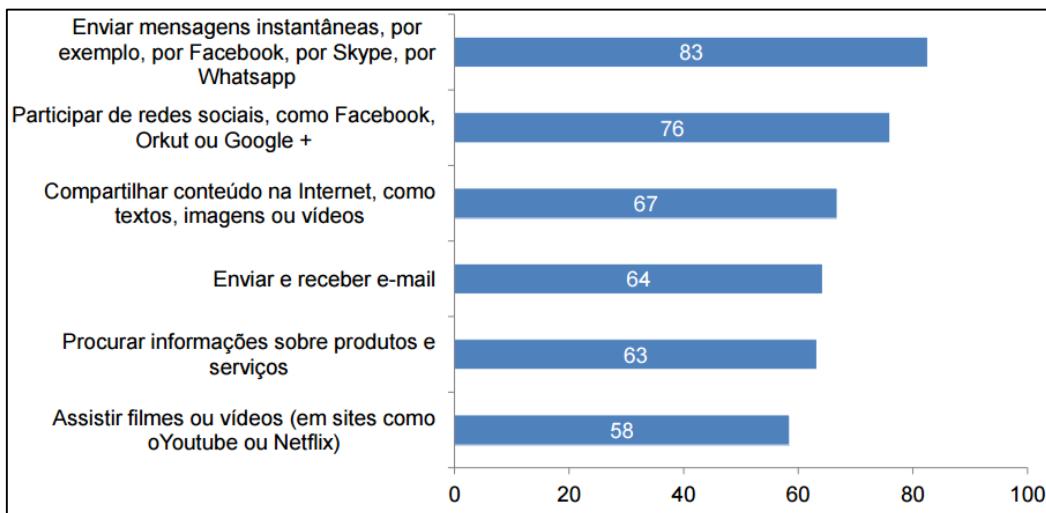


Figura 2 – Atividades Realizadas pela Internet
Fonte: NIC.br (2014).

As redes domésticas conectadas à Internet precisam de uma segurança diferenciada, dados dos usuários, dados pessoais e até mesmo acesso a dados corporativos, podem se tornar um empecilho, abrindo um vulnerabilidade dos dados e pondo em risco a integridade das informações acessadas e compartilhadas.

2.3 SEGURANÇA DA INFORMAÇÃO

Segundo as Normas de ABNT NBR ISO/NBR ISO/IEC 17799:2005 (2005), informação “é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida”.

Devido a importância da informação, sua proteção é crucial. Conforme a norma ISSO/IEC 17799 (2005), a segurança da informação é definida pela seguinte forma:

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

O site Oficina da NET relaciona segurança da informação com a proteção de um conjunto de dados, preservando o valor que a possuem. É a proteção existente sobre as informações de uma determinada pessoa ou empresa, ou qualquer conteúdo ou dado que tenha valor, sendo para uso restrito ou exposta ao público para consulta ou aquisição. Seguindo o padrão internacional existem 3 atributos básicos conforme mostra a Figura 3:

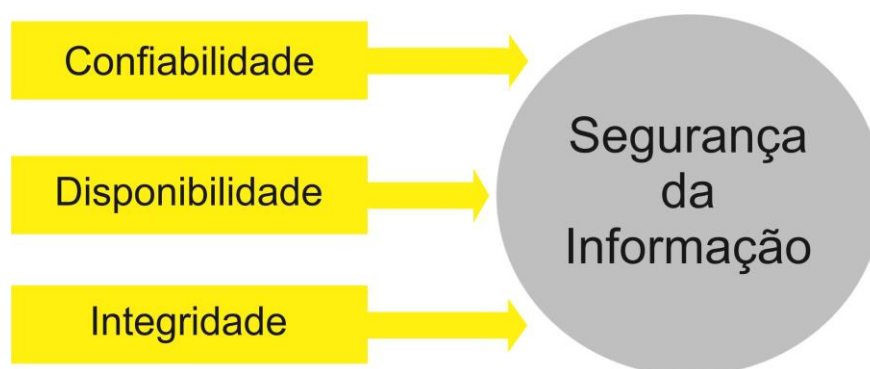


Figura 3 – Atributos Básicos da Informação
Fonte: Autoria Própria.

- Confiabilidade: O acesso a informação apenas as entidades autorizadas pelo proprietário ou dono da informação.
- Integridade: A informação deve manter todas as características originais estabelecidas pelo proprietário.
- Disponibilidade: A informação deve estar sempre disponível para uso quando usuários autorizados necessitarem.

2.4 FIREWALL

Um firewall pode ser definido como um mecanismo de controle de acesso para uma rede em particular ou mesmo um conjunto de redes. A função do firewall é separar uma rede protegida, como uma rede SOHO, de uma rede desprotegida, como a Internet, filtrando os pacotes que entram e/ou saem de uma rede protegida com destino a uma rede desprotegida. O firewall quando instalado adequadamente em uma rede garante que o acesso a uma rede desprotegida a partir da rede protegida, e vice-versa, somente possa acontecer passando pelo firewall, assim aumentando a segurança na rede. A Figura 4 ilustra um firewall em uma rede, sendo que 1 (um)

identifica uma rede protegida, 2 (dois) o firewall e 3 (três) a rede desprotegida, neste caso a Internet.

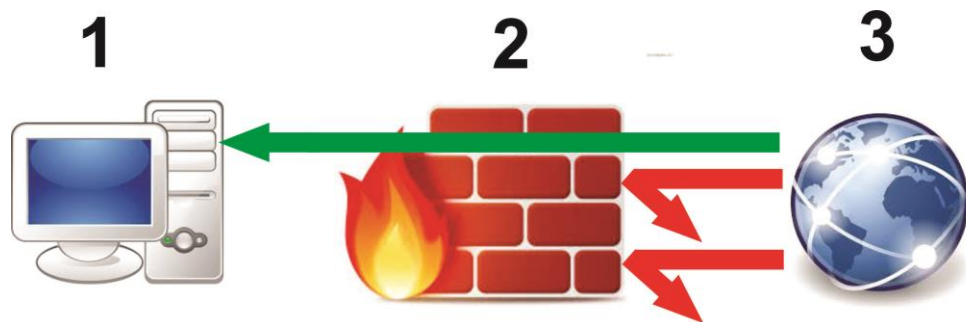


Figura 4 – Estrutura Básica de um Firewall
Fonte: Autoria Própria.

Segundo Nakamura (2007) o firewall está em um constante processo de evolução, o aumento da complexidade das redes das organizações, necessita cada vez mais características e funcionalidades a serem protegidas. Entre esses outros serviços de rede e de segurança passaram a ser incorporados como:

- Autenticação.
- Criptografia (VPN).
- Qualidade de Serviço.
- Filtragem de Conteúdo.
- Antivírus.
- Filtragem de URL.
- Filtragem de palavras-chave para e-mail.
- Filtragem de spam.

A integração entre o firewall e as novas funcionalidades deve ser bem configuradas, mantendo o objetivo de aumentar a segurança e não compromete-la. Nakamura (2007) destaca as principais tecnologias de firewall conforme representada na Figura 5.

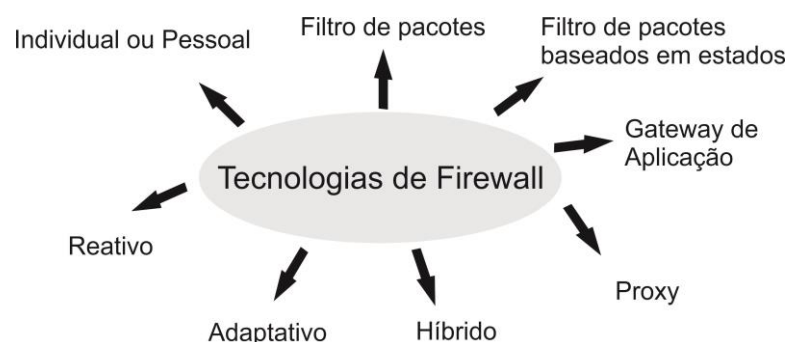


Figura 5 – Tecnologias de Firewall
Fonte: Autoria Própria.

As tecnologias tem características e funções distintas uma das outras, cada uma completa a outra. Com o aumento na necessidade do nível de segurança em algumas situações já é necessário utilizar mais de uma tecnologia ao mesmo tempo para manter a segurança. Nakamura (2007) aborda as tecnologias de firewall com as seguintes definições e características:

- Filtro de Pacotes: Funciona na camada de rede e de transporte, filtrando conforme informações do cabeçalho dos pacotes (endereço de origem, endereço de destino, porta de origem, porta de destino, direção das conexões). As regras são estáticas e definidas de acordo com endereços IP ou com o serviços permitidos ou proibidos, também conhecido como static packet filtering. Para pacotes ICMP (*Internet Control Message Protocol*) a filtragem é feita por código e por tipo de mensagem de controle ou erro.

- Filtro de Pacotes Baseados em Estados: São filtros dinâmicos (dynamic packet filter) que tomam as decisões de filtragem em relação a dois elementos. O primeiro elemento é as informações dos cabeçalhos dos pacotes de dados, filtrando os pacotes. O segundo elemento é uma tabela de estados, onde guarda os estados de todas as conexões. Todas as conexões são monitoradas, permitindo o pacote apenas se ele fazer parte da tabela dos estados.

- Proxy: O proxy é um mecanismo que quando o usuário se conecta a uma porta TCP no firewall, ele abre outra conexão com o mundo exterior. Ele pode trabalhar tanto na camada de sessão ou de transporte, quanto na camada de aplicação. Ou seja, não permite uma conexão direta entre o usuário interno e o servidor externo, todo o tráfego fica registrado como originado no Proxy. Ele possibilita a autenticação do usuário para a conexão. O Proxy pode ser modificado, originando o servidor Transparente que permite que o navegador cliente não saiba da sua existência.

- Firewalls Híbrido: É a mistura das tecnologias apresentadas anteriormente, garantindo maior proteção. Atualmente a maioria dos firewall é híbrido, ou seja, aproveita as melhores características dos filtros de pacotes, filtro de pacotes baseados em estados e proxies para cada um dos serviços específicos. Vários serviços podem necessitar de um firewall ao mesmo tempo, como por exemplo o Telnet utiliza o filtro de pacotes, enquanto o FTP utiliza o Proxy, pois necessita de filtragem no nível de aplicação.

- Proxies Adaptativos: Utiliza mecanismos de segurança em série trazendo benefícios para o nível de segurança da rede. Duas características diferem ele dos outros tipos de firewall: Monitoramento bidirecional e mecanismo de controle entre o Proxy adaptativo e o filtro de pacotes baseados em estados. Controle de pacotes que passam pelo Proxy adaptativo, o qual divide o processamento do controle e dos dados entre a camada de aplicação e a camada de rede. Esse Proxy por meio de suas características direcionam o controle dos pacotes de acordo com as regras por ele definida.

- Firewalls Reativos: Eles incluem funções de detecção de intrusão e alarmes, tornando a segurança mais ativa, policiando acessos e serviços e com característica de ser capaz de mudar a configuração de suas regras de filtragem de modo dinâmico, e enviar mensagens aos usuários e ativar alarmes.

- Firewalls Individuais: Também definido com firewall pessoal, tem seu foco em tecnologias P2P e VPN. Com o crescimento de uso de VPN em computadores pessoais para acessos a rede interna da organização a partir de qualquer lugar, a qualquer momento, o uso de firewall é aplicado no próprio equipamento do usuário e não na borda da rede da organização. Este é capaz de controlar o acessos aos recursos, bloquear determinadas conexões, monitorar todo o tráfego, gerar regras e criar logs de todos os acessos do sistema. Isso significa um aumento no nível de segurança de uma organização, e não uma garantia da segurança da rede, tendo como complemento uma eficiente política de atualização e utilização de antivírus.

Kurose (2010) aborda outra tecnologia de firewall, a qual aborda um nível mais refinado de segurança. Essa tecnologia é conhecida como:

- Gateway de Aplicação: Servidor Específico de Aplicação que através do qual todos os dados da aplicação devem passar. Um firewall pode executar vários gateway de aplicação, com servidor e processos separados, como gateways para Telnet, HTTP, FTP, e-mail e cache web. Cada tipo de aplicação, tem um gateway de aplicação, isso acaba se tornando uma desvantagem, como o desempenho que cai por causa da passagem de todos os dados.

A escolha de qual tecnologia de firewall utilizar é muito relativa ao ambiente a ser aplicado. Sendo assim, a melhor tecnologia é aquela que melhor se adaptar as necessidades do ambiente, da empresa ou da residência, que anda em paralelo com o grau de segurança requerido e a disponibilidade de recursos para sua implantação.

2.4.1 ARQUITETURA DE FIREWALL

Os firewall possuem uma grande variedade de tipos, podem ser implementados de diversas formas com diversas características, tendo outra diferenciação por meio de sua arquitetura, ou seja, como ele é projetado e implementado. A arquitetura pode ser definida de acordo com as necessidades da estrutura, segundo Nakamura (2007) existem três tipos de arquitetura clássicas:

- Dual-Homed Host: representado pela Figura 6, sua estrutura se define em um computador (1) que fica entre a rede interna (2) e a rede externa (Internet) (3), cada uma ligada em uma interface de rede, sendo um separador entre as duas redes. Filtram todas as conexões que por ele passam, usado em situações de baixo fluxo de tráfego. As comunicações são por meio de proxies ou por conexões de duas etapas, o usuário conecta primeiro ao host dual-homed, para depois se conectar ao servidor externo.

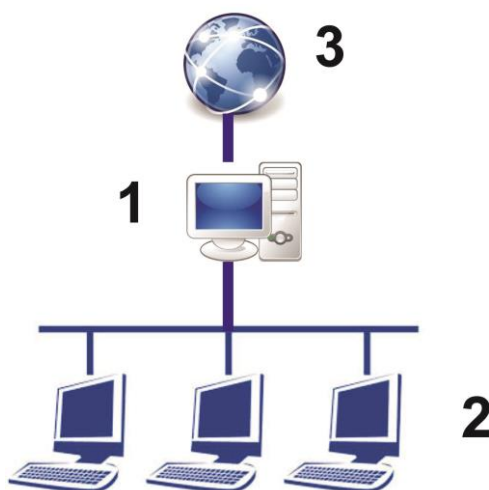


Figura 6 – Arquitetura Dual-Homed Host
Fonte: Autoria Própria.

- Screened Host: Representado pela Figura 7, sua estrutura se define em dois computadores (1) que ficam entre a rede interna (2) e a externa (3), um faz o papel de roteador (screening router) e o outro bastion host (entre o roteador e a rede interna). O bastion host é o único computador da rede interna aonde os hosts da Internet podem abrir conexões. A filtragem dos pacotes é realizada pelo roteador e posteriormente a validação encaminhados ao bastion host, o qual precisa ter um alto nível de segurança, pois todas as conexões vindas da Internet passam por ele. A zona de risco é limitada ao bastion host e o roteador.

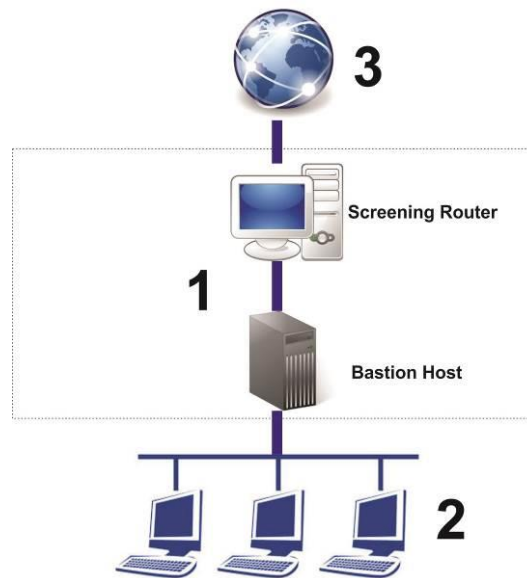


Figura 7 – Arquitetura Screened Host
Fonte: Autoria Própria.

- Screened Subnet: Representado pela Figura 8, sua estrutura se define em uma arquitetura mais complexa e mais cara, criando uma sub-rede chamada de DMZ (rede desmilitarizada) (1), isolando a rede interna(2) da rede externa(3), tendo ainda o bastion host(4). Essa arquitetura isola mais a rede interna da Internet, tendo uma maior proteção ao bastion host, o qual sofre mais ataques externos, criando uma sub-rede. Existem dois roteadores conectados, um conectado a DMZ e a Internet, e o outro conectado a DMZ e a rede interna.

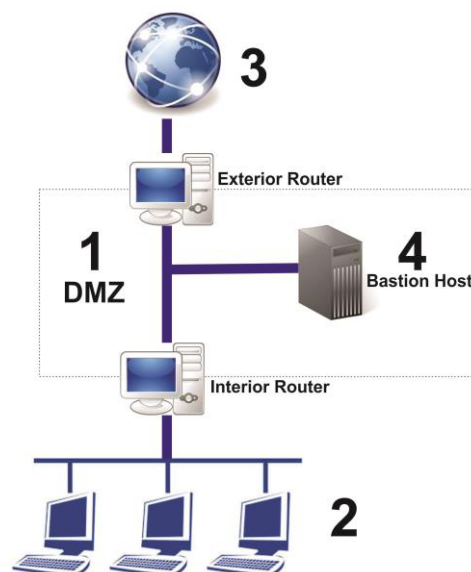


Figura 8 – Arquitetura Screened Subnet
Fonte: Autoria Própria.

Uma nova arquitetura mais recente surge, criando uma extensão das arquiteturas clássicas. A quarta arquitetura é a do firewall cooperativo, a qual é destinada para ambientes organizacional, ambiente de empresas, governo entre outros. Segundo Nakamura (2007) é uma arquitetura nova a qual é inserida novos componentes, como VPN, o IDS e a PKI. Diferente das clássicas, há uma extensão maior as situações encontradas em ambientes cooperativos. Seu objetivo tornar mais simples a administração da segurança em ambiente cooperativo.

- Firewall Cooperativo: Representado pela Figura 9, sua estrutura se define em uma arquitetura destinada ao meio cooperativo. Sua estrutura básica, mas flexível, contém agora uma VPN (1) que atua junto com a CA(2) para autenticar os usuários ao acesso a rede interna (3). Para recursos a serem de acesso por meio da Internet (4) é criada uma DMZ (5) específica para serviços como E-mail, FTP e servidor Web. Para recursos com maior grau de segurança, sem acesso direto de usuários por meio da Internet, como por exemplo o banco de dados (6) que é acessado por meio de uma aplicação, surge uma segunda DMZ (7).

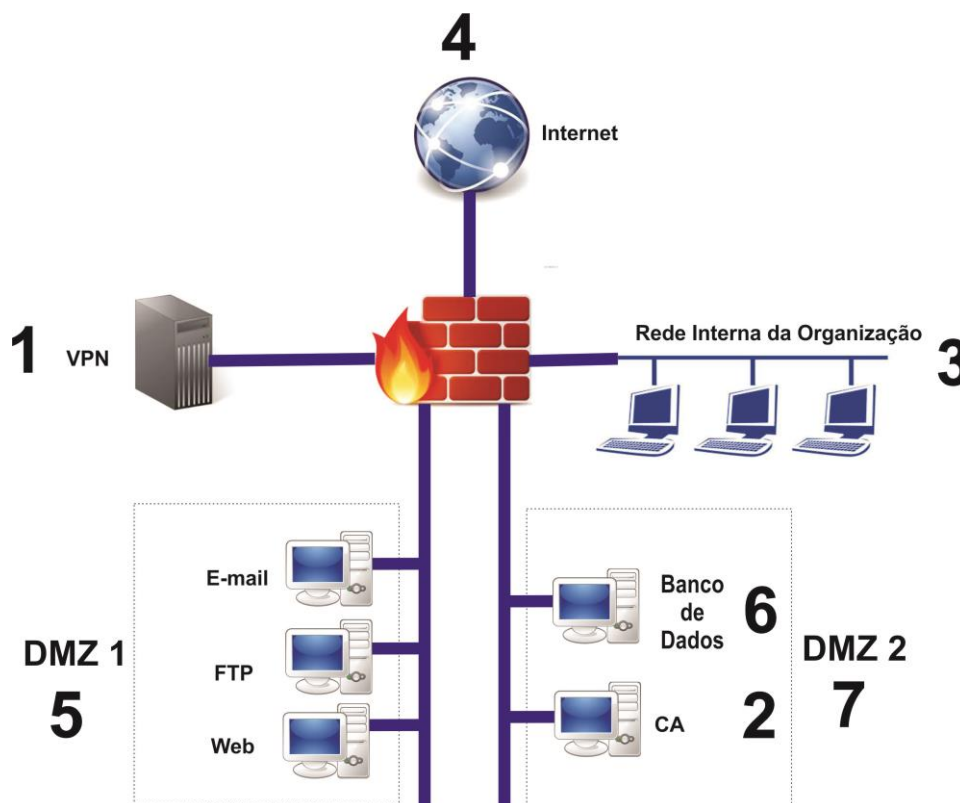


Figura 9 – Arquitetura do Ambiente Cooperativo
Fonte: Autoria Própria.

3 MATERIAIS E MÉTODO

Neste capítulo são apresentadas as ferramentas e tecnologias utilizadas para o estudo e elaboração da solução de rede.

3.1 MATERIAIS

Foram utilizadas as seguintes ferramentas e tecnologias:

- a) Wireshark – Software gratuito que analisa pacotes de rede.
- b) Endian Firewall Community – Distribuição gratuita de segurança para SOHO.
- c) pfSense – Distribuição gratuita de segurança para SOHO.

d) Computadores: O ambiente testado utilizou 02 computadores. Um simulando o dispositivo do usuário, e o outro os firewall, primeiramente foi instalado o Endian, que após a instalação, testes e levantamento dos resultados, foi instalado o pfSense, dando assim uma igualdade de hardware para as duas distribuições.

As distribuições Endian Firewall Community e pfSense seguem o mesmo padrão, apresentam características técnicas e operacionais bem parecidas, com as mesmas funcionalidades, versões gratuitas, processo de instalação, ambas ferramentas UTM, compatibilidade com hardware necessário justificam a comparação entre elas, existindo outras distribuições conforme consta no site Wikipedia (2015). A escolha destas distribuições é o reaproveitamento de computadores já sem uso, que já foram substituídos e estão sem utilidade e destino, entretanto, existem outras distribuições que possam ser mais customizadas, mas que necessitam de hardwares específicos como Roteadores ou Dispositivos ARM.

3.1.1 Wireshark

Wireshark (2015) é um software analisador de protocolo de rede, o qual permite ver o que está acontecendo na rede minuciosamente, monitora os pacotes de dados, um dos mais utilizados em indústrias e instituições educacionais. Ele captura os pacotes da rede e tenta mostrar os dados do pacote o mais detalhado possível.

Wireshark é composto de diversos recursos como: multi-plataforma, análise das leituras off-line, análise de VoIP, análise profunda de protocolos, pesquisar ou filtrar pacotes em vários critérios, entre outros.

Um software de código aberto disponível para download, usado por administradores de rede (solucionar problemas de rede), engenheiros de segurança de rede (examinar problemas de segurança), desenvolvedores (depurar implementações de protocolo) e pessoas que querem usá-lo para aprender protocolos de rede internas. Tem uma interface gráfica de fácil utilização conforme a Figura 10.

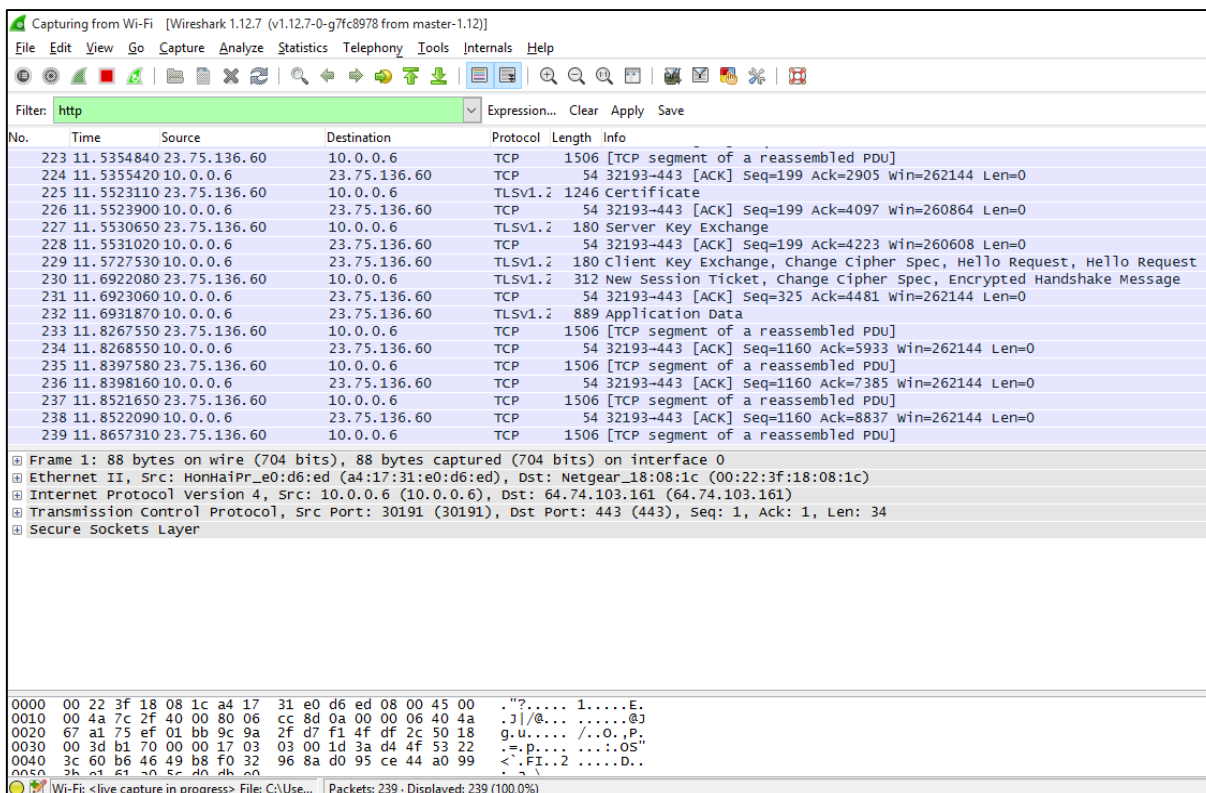


Figura 10 – Tela principal da Ferramenta Wireshark.
Fonte: Autoria Própria.

3.1.2 Endian: Internet Security

O Endian (2015) é desenvolvido pela empresa italiana Endian Srl e pela comunidade e consistem em uma distribuição Linux de gerenciamento de Firewall. Com configuração fácil em interface web, reduz o tempo de gerenciamento de rede e custos. O Endian é uma distribuição que necessita de uma máquina específica para ser instalada, não podendo dividir o HD com outro software ou SO. O Endian possui quatro versões, a Virtual Appliance, Software Appliance, Hardware Appliance e a EFW Community.

Segundo as especificações do site do fabricante as diferenças são:

- Virtual Appliance: Versão on-line, que protege redes virtuais e infraestrutura, suporta todas as principais plataformas de virtualização.

- **Software Appliance:** Versão do software que pode ser aplicada em qualquer hardware, podendo redimensionar os recursos e configurações do hardware, transformando em um UTM cheio de recursos.
- **Hardware Appliance:** Conjunto de hardware e software específico para UTM, atendendo todas as necessidades de segurança destinado para grandes redes.
- **EFW Community:** Versão do software que pode ser aplicada em qualquer hardware, podendo redimensionar os recursos e configurações do hardware, algumas funcionalidades a menos que a Software Appliance e é mantida pela comunidade, sem suporte e específica para redes SOHO.

O Quadro 1 mostra detalhadamente as diferenças de cada versão.

General	EFW Community	Virtual Appliance	Software Appliance	Hardware Appliance
Open Source License (GPL)	Sim	Sim	Sim	Sim
Commercial support options	Não	Sim	Sim	Sim
Ticket System Support	Não	Sim	Sim	Sim
Direct support from Endian	Não	Opcional	Opcional	Opcional
Phone Support	Não	Opcional	Opcional	Opcional
Live/Remote Support (hands on)	Não	Opcional	Opcional	Opcional
Instant Hardware Replacement	Não	N/A	N/A	Opcional
Industrial Grade Hardware	Não	N/A	N/A	Sim
DynDNS support	Sim	Sim	Sim	Sim
Network Security	Sim	Sim	Sim	Sim
Application Control	Não	Sim	Sim	Sim
Advanced Content Security	Não	Sim	Sim	Sim
CYREN URL Filter	Não	Sim	Sim	Sim
CYREN Anti-spam	Não	Sim	Sim	Sim
Panda Anti-virus	Não	Sim	Sim	Sim
Web Security	Sim	Sim	Sim	Sim
URL Filter	1.8 milhões URLs	150 milhões URLs	150 milhões URLs	150 milhões URLs
Mail Security	Sim	Sim	Sim	Sim
Anti-spam	Motor Individual	Dois Motores	Dois Motores	Dois Motores
Quarantine Management	Não	Sim	Sim	Sim
Anti-virus	Sim	Sim	Sim	Sim
Anti-virus	Motor Individual	Dois Motores	Dois Motores	Dois Motores
Virus disinfection	Não	Sim	Sim	Sim
User Authentication	Sim	Sim	Sim	Sim

Local User Authentication	Sim	Sim	Sim	Sim
HTTP Remote User Authentication	Sim	Sim	Sim	Sim
VPN Remote User Authentication	Não	Sim	Sim	Sim
Virtual Private Networking	Sim	Sim	Sim	Sim
IPsec	Sim	Sim	Sim	Sim
L2TP	Não	Sim	Sim	Sim
XAuth	Não	Sim	Sim	Sim
OpenVPN	Sim	Sim	Sim	Sim
WAN Failover	Sim	Sim	Sim	Sim
BYOD and Hotspot	Não	Sim	Sim	Sim
Network Address Translation	Sim	Sim	Sim	Sim
Routing	Sim	Sim	Sim	Sim
Bridging	Sim	Sim	Sim	Sim
High Availability	Não	Sim	Sim	Sim
Event Management	Sim	Sim	Sim	Sim
Email Notifications	Sim	Sim	Sim	Sim
SMS Notifications	Não	Sim	Sim	Sim
Python Scripting Engine	Não	Sim	Sim	Sim
Logging and Reporting	Sim	Sim	Sim	Sim
Live Network Monitoring	Sim	Sim	Sim	Sim
Event Reporting	Não	Sim	Sim	Sim
Management	Sim	Sim	Sim	Sim
Management Interface	Sim	Sim	Sim	Sim
Full System Access	Sim	Sim	Sim	Sim
Updates and Backup	Sim	Sim	Sim	Sim
Centralized Management	Não	Sim	Sim	Sim

Quadro 1 - Endian Firewall - Especificações por Versões
 Fonte: Site oficial do fabricante Endian (Endian, 2015).

3.1.2.1 Endian *Firewall Community*

Endian *Firewall Community* é uma distribuição de segurança de rede pronta para ser usado em uma rede SOHO, que pode transformar um equipamento que já não se encontra em uso em uma ferramenta UTM (*Unified Threat Management*), uma central unificada de gerenciamento de ameaças. Ele se torna uma evolução do firewall tradicional, que abrange diversas funções de segurança como firewall, prevenção de intrusões, antivírus, VPN (Virtual Private Network), filtragem de conteúdo, balanceamento de carga e relatórios em tempo real do tráfego da rede, uso e acessos.

3.1.3 pfSense

O pfSense (2015) é uma distribuição de software livre de firewall que foi criada em 2004 por Chris Buechler e Scott Ullrich, baseado no sistema operacional FreeBSD, foi adaptado para a função de um firewall e/ou roteador de redes. Ele possui pacotes adicionais transformando-se em um UTM.

Destinado para redes pequenas ou em grandes corporações é composto de diversos serviços como VPN, balanceamento de carga, regras de NAT, regras de Firewall, geração de chaves RSA, monitoramento de tráfego, entre outros.

O site oficial oferece a opção de comprar um hardware pré-definido que garante total compatibilidade, simplificando o processo de seleção de hardware certo para as necessidades e com suporte pelo período de um ano. A opção de download para utilizar em um hardware distinto, pode ser feita do site oficial, tendo opção de executar direto do CD para testes ou instalar direto no disco, o qual não pode ser compartilhado com outro sistema operacional.

3.1.4 Computadores

O ambiente de teste é composto por 2 computadores, um simulando o usuário final e o outro, os dois os firewall.

O primeiro computador é um notebook com as especificações técnicas contidas na Quadro 2, o qual foi instalado o Wireshark e simula o usuário final usando a Internet que será filtrada pelos firewall que estão sendo aplicadas as regras pré-definidas.

Características	
Processador	Intel Core I5 - 3230
Memória RAM	8 GB
HD	120 GB - SSD
Placa de Rede 1	1 Gbps

Quadro 2 - Especificações Computador Usuário
Fonte: Autoria Própria.

O segundo computador é uma máquina já sem uso no dia a dia, pois as distribuições de firewall utilizadas não requerem grande poder de processamento e de memória, podendo reaproveitar um computador sem utilidade, no entanto, a única alteração de hardware foi a adição de uma segunda placa de rede para a separação

física das redes WAN e LAN. As especificações técnicas do computador estão contidas no Quadro 3.

Características	
Processador	Intel Celeron 2.66GHz
Memória RAM	2 GB
HD	160 GB - SATA
Placa de Rede: 2	1 Gbps
	100 mbps

Quadro 3 - Especificações Computador para os Firewall
Fonte: Autoria Própria.

3.2 MÉTODO

Inicialmente foi necessário estudar as tecnologias envolvidas nas redes de computadores, tanto teórico como prático. Esse estudo envolveu uma ferramenta de monitoramento de redes para efetuar medições do tráfego e acesso da rede e duas distribuições de softwares de segurança para redes SOHO as quais serão comparadas seus resultados.

O estudo da ferramenta de monitoramento Wireshark teve como objetivo o entendimento do seu funcionamento e o monitoramento do tráfego de dados da rede, antes e depois de regras configuradas no Endian e no pfSense.

O estudo das distribuições gratuitas de segurança Endian Firewall Community e pfSense teve como objetivo o entendimento do seus funcionamentos e configurações e testes no mesmos.

Para o firewall por sua finalidade foi escolhido a arquitetura Dual-Homed host e tecnologia híbrida, tecnologia Proxy e Gateway de Aplicação, levando em consideração suas necessidades e ambiente a ser aplicado.

Devido ao estudo das tecnologias e o ambiente de pequeno porte, duas regras foram definidas para se testar as ferramentas e obter um resultado comparativo entre os mesmos. As regras definidas foram:

- 01- Proibir o acesso a rede social Facebook.
- 02- Bloquear acessos oriundos da rede externas à rede interna.

Essas regras formam a base de testes a serem usadas na prática para se obter um exemplo de configuração e de utilização, essas regras podem ser modificadas conforme a necessidade para efetivação da segurança da rede. Novas regras podem dar origem a um esquema de segurança da rede a ser protegida conforme as

necessidades dos usuários no seu dia a dia. Para aplicar as regras deve-se seguir as características e meios de configuração em cada distribuição.

A instalação e configuração dos firewalls cria um ambiente simulado, com o objetivo de recriar a situação real de uma rede SOHO.

4 RESULTADOS

Este capítulo apresenta o que foi obtido como resultado da realização deste trabalho que é estudar as funcionalidades, características e diferenças entre o Endian Firewall Community e o pfSense, distribuições gratuitas de segurança para serem utilizado em redes SOHO.

4.1 APLICAÇÃO PRÁTICA

A aplicação prática foi executada utilizando dois computadores, um computador simulando o usuário (1), o qual foi instalado o Wireshark que fará a comparação do antes e o depois do uso das regras em cada firewall testado. O outro computador(2), teve um firewall instalado, um de cada vez, aplicando as mesmas regras e acompanhando a usabilidade e os resultados obtidos. A Internet(3) foi conectada em uma das interfaces do computador com o firewall(2), dando origem a rede externa, conforme representado na Figura 11.

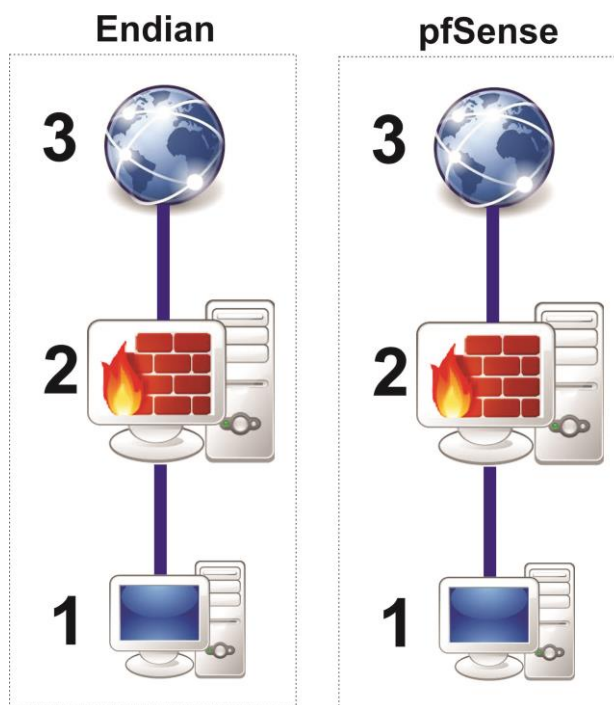


Figura 11 – Ambiente de Teste.
Fonte: Autoria Própria.

4.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO WIRESHARK

O computador utilizado simulando o usuário foi instalado o Wireshark, para fazer as leituras antes e depois de aplicar todas as regras, e também foi utilizado para configurar via browser os firewall.

Este computador em um ambiente real, poderá ser qualquer dispositivo que tenha conexão a Internet, tanto PC, Laptop, Celular ou Tablet, pois toda a conexão externa irá passar pelo firewall antes de sair ou entrar da Internet.

O Wireshark foi obtido no site do fabricante, e sua instalação é bastante simples, não necessitando de nenhuma configuração específica. Após sua instalação, ao executar, para iniciar o monitoramento, deve selecionar a interface(1) e clicar em Start(2), para fazer as análises pode inserir um filtro(3) específico conforme a necessidade para verificar cada regra aplicada conforme a Figura 12. A versão instalada é a 1.12.7.

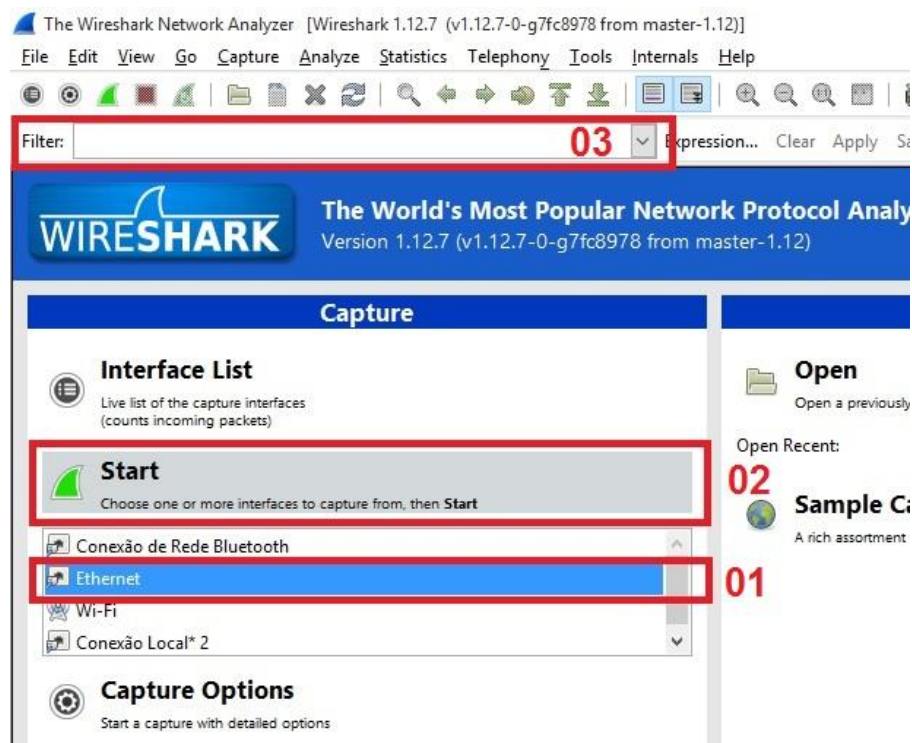
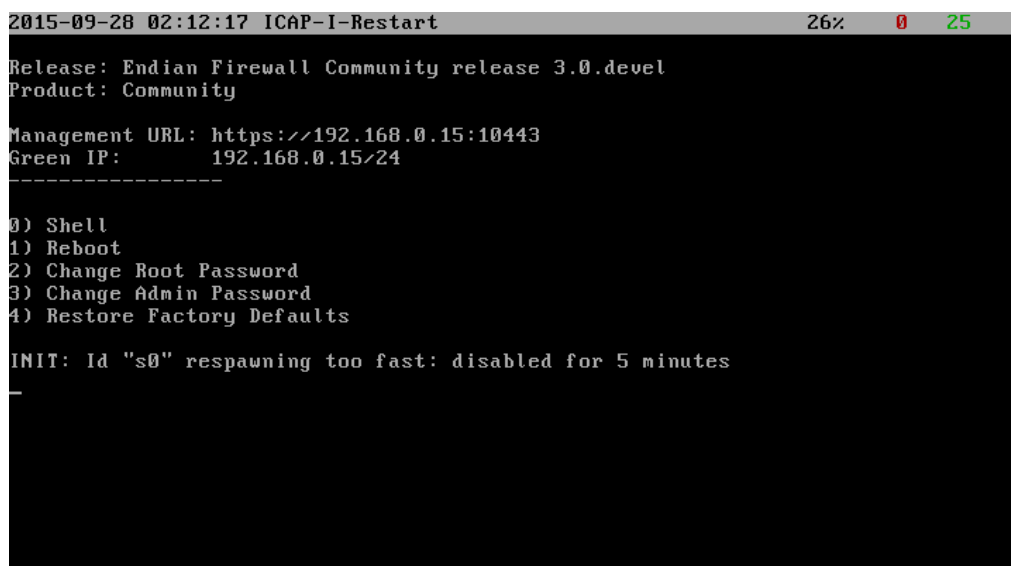


Figura 12 – Wireshak Tela Inicial.
Fonte: Autoria Própria.

4.1.2 INSTALAÇÃO E CONFIGURAÇÃO DO ENDIAN

Para a aplicação das regras na distribuição Endian, foi utilizado um computador conforme citado nos materiais para instalação do mesmo. O instalador do Endian encontra-se na página oficial para download gratuito, o qual deve ser gravado em uma mídia de CD-ROM, e em sequência instalado na máquina. A instalação não permite a divisão do HD com outro SO, forçando o disco ao uso total pelo Firewall. A instalação também é um processo bem simples, e após a finalização o computador fica em uma tela inicial, para efetuar as configurações iniciais, que pode ser feita pelo Shell ou por outro computador da rede por um browser conforme Figura 13. A versão instalada é a 3.0.devel.



```
2015-09-28 02:12:17 ICAP-I-Restart 26% 0 25
Release: Endian Firewall Community release 3.0.devel
Product: Community

Management URL: https://192.168.0.15:10443
Green IP: 192.168.0.15/24
-----
0) Shell
1) Reboot
2) Change Root Password
3) Change Admin Password
4) Restore Factory Defaults

INIT: Id "s0" respawning too fast: disabled for 5 minutes
```

Figura 13 – Tela Inicial do Endian Firewall Community.
Fonte: Autoria Própria.

Após a instalação do Endian, por meio de outro computador conectado na rede, é possível efetuar a configuração do mesmo por meio do browser pelo endereço <https://192.168.0.15:10443>, o qual aparece na tela inicial ao ligar o micro com ele instalado conforme a Figura 13. Esse IP vem padrão, mas pode ser alterado, juntamente com seu usuário e senha que vem por padrão “admin” e “endian” sucessivamente. A configuração é bem simples de ser efetuada, com uma interface bem amigável para o usuário mais leigo conforme mostra a Figura 14.

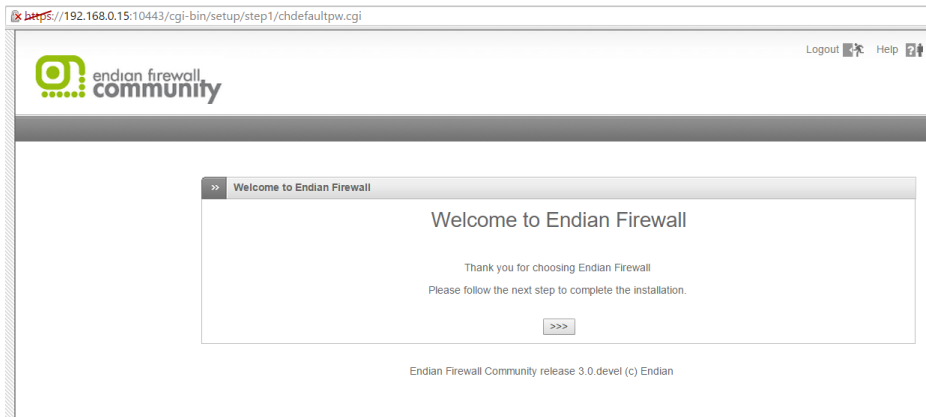


Figura 14 – Acesso ao Endian pelo Browser
Fonte: Autoria Própria.

Nas primeiras configurações pode ser selecionado o idioma português o qual facilita bastante as configurações e usabilidade. A Senha tanto do acesso da administração web ou por meio do SSH pode ser alterada.

A primeira regra configurada é o bloqueio ao acesso ao Facebook, o qual utiliza protocolo HTTPS para o acesso, tendo uma necessidade de configuração específica para efetuar esse bloqueio no Endian, pois utiliza uma porta diferente, a 443 em vez da 80. No menu Firewall, na Opção Tráfego de Saída, é necessário criar uma nova regra, a qual deve informar a Origem que é a Interface do Firewall, e o Destino que é a rede do Facebook, que por causa do HTTPS precisa ser bloqueada pelo endereço IP do domínio, que pode ser descoberta pelo comando *nslookup* no DOS ou em sites de fórum, e o protocolo que tem informar as portas 80 e 443 e colocar em uma posição antes dos protocolos HTTP e HTTPS para garantir que a regra seja acessada antes de liberar o acesso conforme a Figura 15. Após criar a regra e aplicar as configurações para as alterações serem efetivadas.

 A screenshot of the 'Editor de regra do firewall de saída' (Outgoing Firewall Rule Editor) in Endian Firewall. The form is divided into several sections:

- Origem (Source):** Tipo is 'Zona/Interface'. A list of interfaces is shown, with 'Interface 1 (Zona: VERDE)' selected.
- Destino (Destination):** Tipo is 'Rede/IP'. A list of IP ranges is shown, with '69.171.0.0/16' and '31.13.0.0/16' selected.
- Serviço/Porta (Service/Port):** Serviço is 'Definido pelo utilizador'. Protocolo is 'TCP + UDP'. Porta de destino (un por linha) has '80' and '443' entered.
- Política (Policy):** Ação is 'BLOQUEAR'. Observações is 'Bloqueando o Facebook'. Posição is 'Primeira'. There are checkboxes for 'Habilitado' and 'Registrar todos os pacotes aceitos', both of which are unchecked.

 At the bottom, there are buttons for 'Atualizar regra' and 'Cancelar', and a note: '* Este campo é obrigatório.'

Figura 15 – Configuração da Regra 1 no Endian.
Fonte: Autoria Própria.

A outra regra testada no Endian é o bloqueio de acessos externos a rede, o qual já consta com um serviço pré configurado, o qual apenas precisa ser ativado em suas configurações, que se encontram no menu Serviços, Prevenção a Intrusão, e em sequência, alterar o botão para habilitar o serviço conforme a Figura 16.

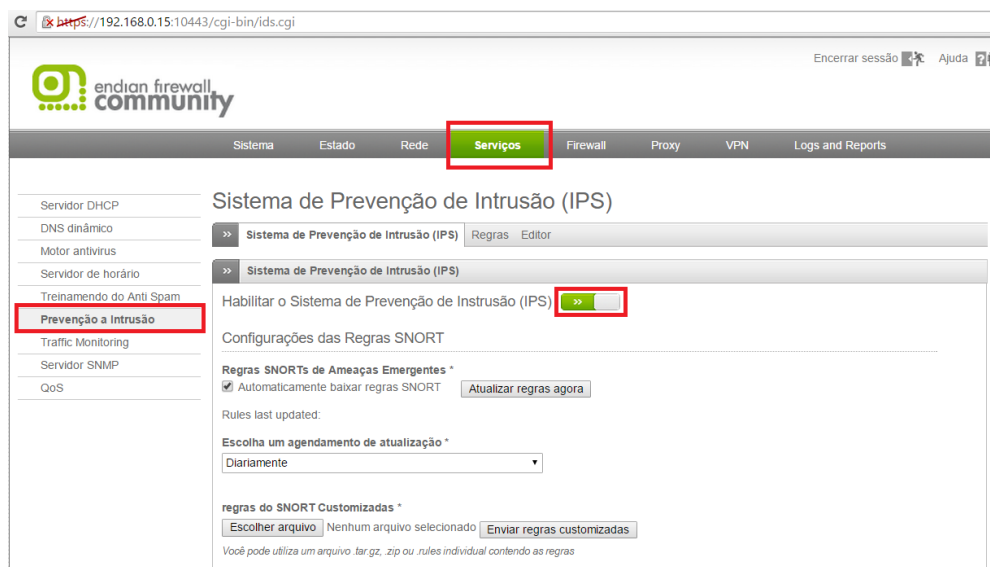


Figura 16 – Configuração da Regra 2 no Endian.
Fonte: Autoria Própria.

4.1.3 INSTALAÇÃO E CONFIGURAÇÃO DO PFSense

O pfSense foi instalado no segundo computador citado nos materiais, após o uso do Endian, o qual será instalado de forma como um sistema operacional específico. O instalador do pfSense encontra-se para download na página oficial gratuitamente, que como o Endian, precisa de uso exclusivo do HD para seu uso. A versão instalada é a 2.2.4-Release.

O processo de instalação também é bastante simples, bem parecido com o Endian, mas com algumas características e configurações diferentes. A interface web para configuração do mesmo após a instalação é acessada pelo endereço 192.168.1.1. Interface amigável para uso de usuários intermediários. Esse IP vem padrão, mas foi alterado para 192.168.1.15 para os testes, e seu usuário e senha que vem por padrão “admin” e “pfsense” sucessivamente, os quais foram mantidos. A tela inicial é mostrada na Figura 17.



Figura 17 – pfSense – Tela Inicial.
Fonte: Autoria Própria.

A instalação do pfSense por ser feita pelo CD no HD do computador, ou utilizar versão que roda por Pen Drive, ou Rodar direto do CD. A configuração é um pouco mais detalhada comparada com o a do Endian, necessitando alguns passos detalhistas, como por exemplo a configuração das duas placas de rede, que nessa distribuição é obrigatória, configurando uma placa para a rede WAN e a outra para a LAN. A configuração deve ser feita obedecendo uma sigla que é reconhecida pela instalação, essa sigla gera a partir do fabricante da placa, gerando nomes como em0, re0, ae0, onde por exemplo re0 significa que a placa é da Realtek, a Figura 18 mostra a placas utilizadas para o teste.

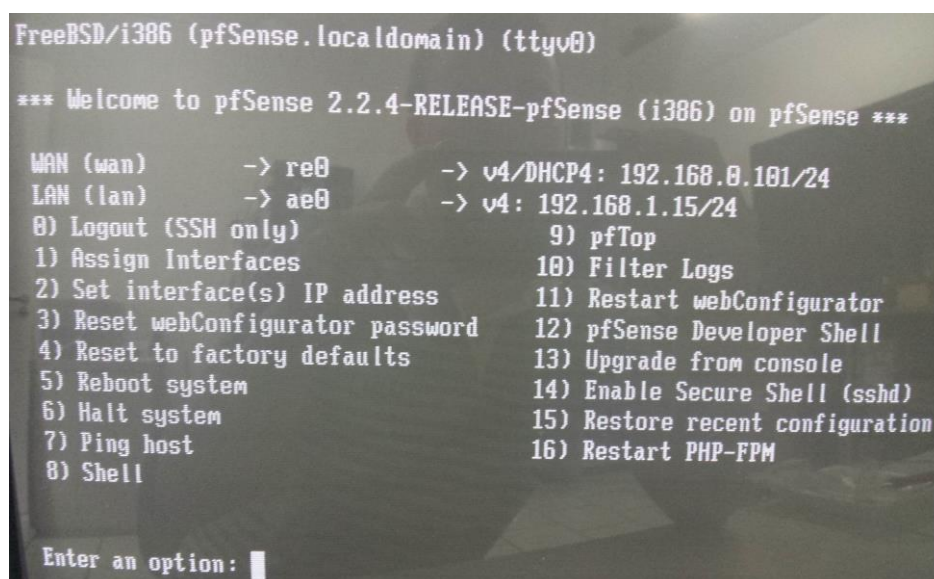


Figura 18 – pfSense – Tela Principal / Menu
Fonte: Autoria Própria.

A Figura 18 mostra o menu de opções para configuração que pode ser configurada diretamente pelo computador que está instalado o pfSense. O usuário é indicado acesso pelo browser de outra máquina em rede para acesso e configuração, o acesso é feito pelo endereço 192.168.1.15, o qual foi configurado na rede LAN. A Tela de login do pfSense mostrada na Figura 19 pede login e senha para o acesso, o qual foi mantido o padrão.



Figura 19 – pfSense – Tela de Login.
Fonte: Autoria Própria.

Após o login, abre a tela principal do firewall, uma interface em inglês, o que pode ser um pouco mais complicada de ser configurada pelo usuário, mas a mesma é completa com diversos serviços e ferramentas que podem ser usadas conforme a Figura 20.

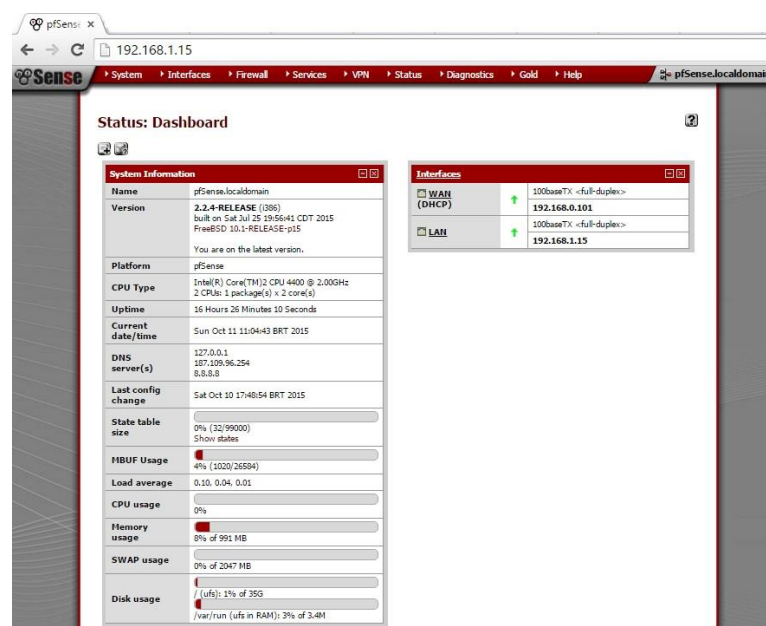


Figura 20 – pfSense – Tela Principal pelo browser.
Fonte: Autoria Própria.

Para facilitar o uso, pode se alterar a linguagem para Português do Brasil e o tema para facilitar o uso, essas configurações estão contidas no menu System, General Setup conforme Figura 21.

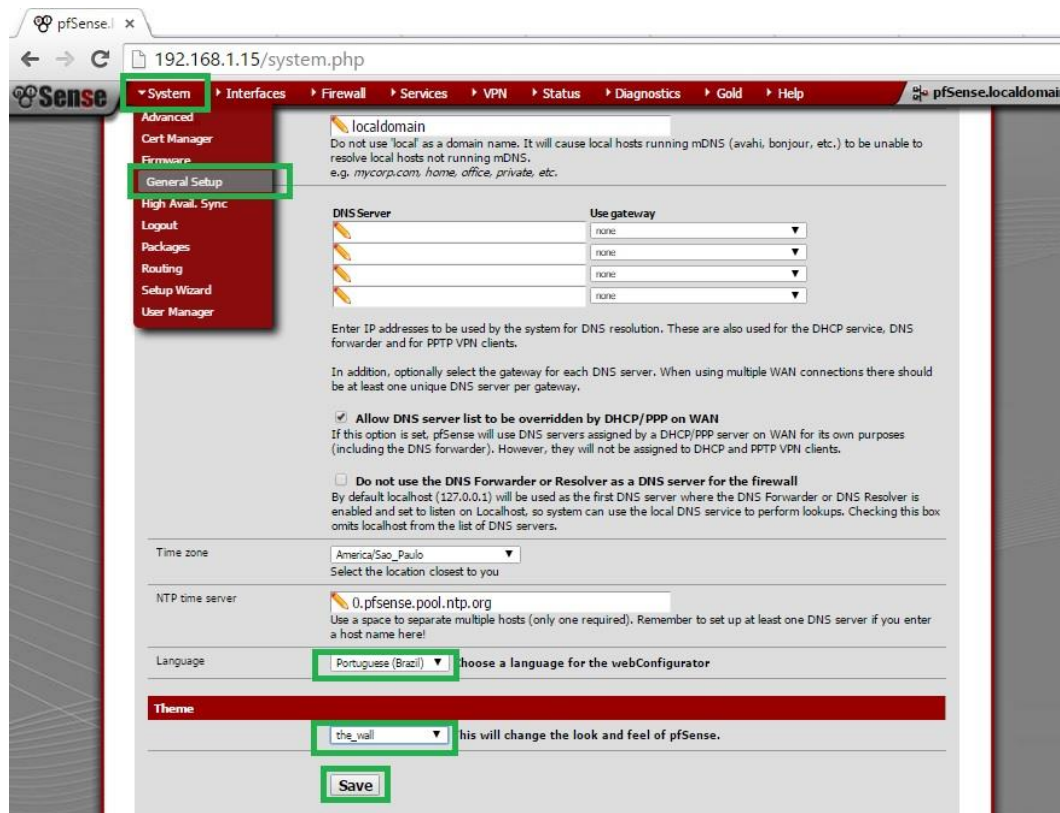


Figura 21 – pfSense – Alterar Idioma.
Fonte: Autoria Própria.

Para configurar e colocar em pratica as regras é necessário o uso de Proxy no pfSense, é necessário a instalação de pacote adicionais para este serviço, o qual tem acesso pelo menu Sistema, Pacotes, Pacotes Disponíveis, onde seleciona os seguintes pacotes: squid, squidGuard, e adiciona o pacote um de cada vez. Esses pacotes instalam os serviços de Proxy no firewall.

A primeira regra ser configurada é bloquear o acesso ao Facebook, mas tem alguns procedimentos necessários para o funcionamento, o primeiro é a criação de uma Aliases, ou seja, adicionar um grande números de IPs em uma lista com um nome a ser definido pelo usuário para facilitar as configurações, para sua criação deve-se ir em menu Firewall, Aliases, e adicionar com um nome e os IPs conforme Figura 22. Esses IP são os do site a ser bloqueado.

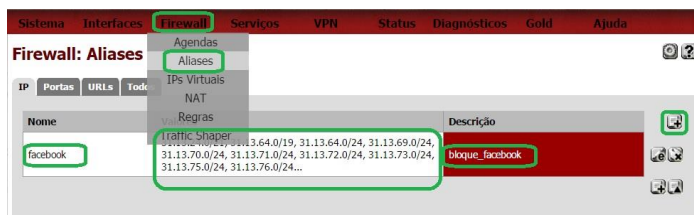


Figura 22 – pfSense – Criação de Aliases.
Fonte: Autoria Própria.

Em seguida deve se criar uma regra, no menu Firewall, Regras, na aba LAN, e adiciona uma nova regra para rejeitar, seleciona todos os protocolos com destino aliases criada anteriormente e posteriormente salva conforme a Figura 23.

Figura 23 – pfSense – Regras de Firewall.
Fonte: Autoria Própria.

A outra regra é o bloqueio de acessos externos a rede, para isso no pfSense é necessário a instalação de um pacote adicional para este serviço, o qual se acesso no menu Sistema, Pacotes, Pacotes Disponíveis, seleciona os seguinte pacote Snort e adiciona ele. Este é um serviço que detecta e previne Intrusão. Após sua instalação deve ativar o serviço, em menu Serviços, Snort, adiciona uma Interface, no caso a WAN e ativa o serviço conforme a Figura 24.

Services: Snort 2.9.7.5 pkg v3.2.8.2



Interface	Snort	Performance	Block	Barnyard2	Descrição
WAN	ENABLED	AC-BNFA	DISABLED	DISABLED	WAN

Figura 24 – pfSense – Configuração do Snort.
Fonte: Autoria Própria.

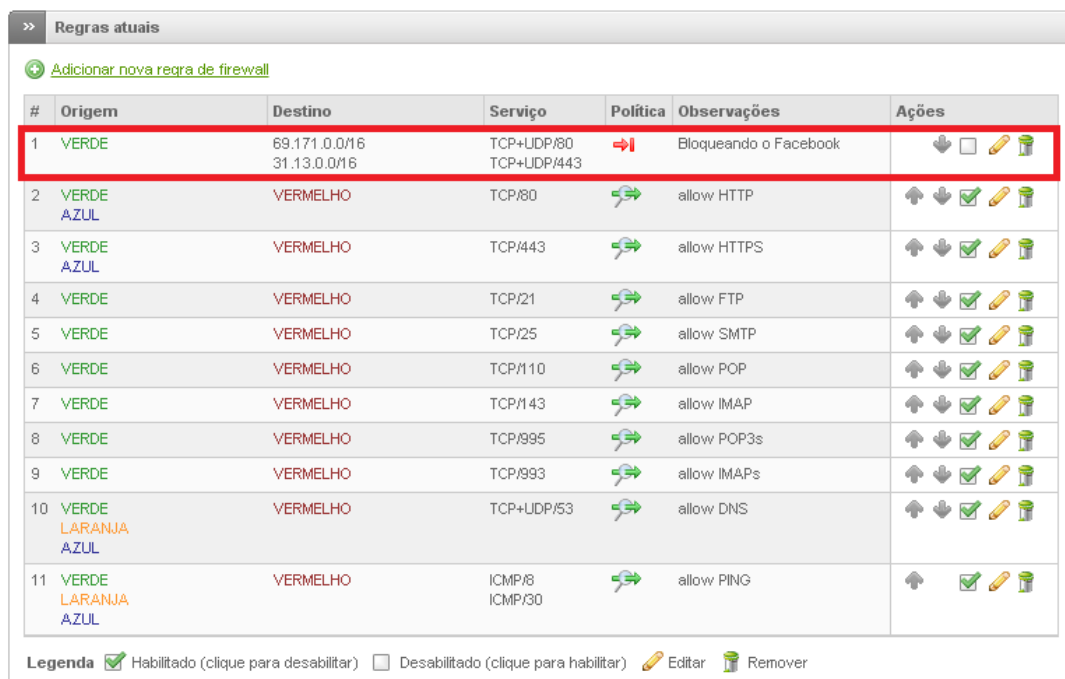
4.1.4 TESTES DAS REGRAS E ANALISE NO WIRESHARK

Para finalizar a parte prática foi necessário efetuar os testes e comprovar se as regras configuradas nos firewall estão funcionando, e verificar no Wireshark o tráfego de pacotes na rede.

4.1.4.1 TESTES NO ENDIAN

O primeiro teste é efetuado no Endian foi para verificar a primeira regra, que bloqueia o acesso ao Facebook. A Figura 25 mostra que a regra se encontra desabilitada e a Figura 26 mostra que o acesso continua liberado.

Configuração do firewall de saída



#	Origem	Destino	Serviço	Política	Observações	Ações
1	VERDE	69.171.0.0/16 31.13.0.0/16	TCP+UDP/80 TCP+UDP/443	→❌	Bloqueando o Facebook	↓ □ ✎ 🗑️
2	VERDE AZUL	VERMELHO	TCP/80	→✅	allow HTTP	↑ ↓ ✅ ✎ 🗑️
3	VERDE AZUL	VERMELHO	TCP/443	→✅	allow HTTPS	↑ ↓ ✅ ✎ 🗑️
4	VERDE	VERMELHO	TCP/21	→✅	allow FTP	↑ ↓ ✅ ✎ 🗑️
5	VERDE	VERMELHO	TCP/25	→✅	allow SMTP	↑ ↓ ✅ ✎ 🗑️
6	VERDE	VERMELHO	TCP/110	→✅	allow POP	↑ ↓ ✅ ✎ 🗑️
7	VERDE	VERMELHO	TCP/143	→✅	allow IMAP	↑ ↓ ✅ ✎ 🗑️
8	VERDE	VERMELHO	TCP/995	→✅	allow POP3s	↑ ↓ ✅ ✎ 🗑️
9	VERDE	VERMELHO	TCP/993	→✅	allow IMAPs	↑ ↓ ✅ ✎ 🗑️
10	VERDE LARANJA AZUL	VERMELHO	TCP+UDP/53	→✅	allow DNS	↑ ↓ ✅ ✎ 🗑️
11	VERDE LARANJA AZUL	VERMELHO	ICMP/8 ICMP/30	→✅	allow PING	↑ ✅ ✎ 🗑️

Legenda Habilitado (clique para desabilitar) Desabilitado (clique para habilitar) ✎ Editar 🗑️ Remover

Figura 25 – Endian – Primeira Regra Desabilitada.
Fonte: Autoria Própria.



Figura 26 – Endian – Acesso liberado com a Regra Desabilitada.
Fonte: Autoria Própria.

Após a ativação da regra conforme a Figura 27 o bloqueio acontece com sucesso conforme a Figura 28.

Configuração do firewall de saída

#	Origem	Destino	Serviço	Política	Observações	Ações
1	VERDE	69.171.0.0/16 31.13.0.0/16	TCP+UDP/80 TCP+UDP/443	→	Bloqueando o Facebook	↓ ✓ ✎ 🗑
2	VERDE AZUL	VERMELHO	TCP/80	→	allow HTTP	↑ ↓ ✓ ✎ 🗑
3	VERDE AZUL	VERMELHO	TCP/443	→	allow HTTPS	↑ ↓ ✓ ✎ 🗑
4	VERDE	VERMELHO	TCP/21	→	allow FTP	↑ ↓ ✓ ✎ 🗑
5	VERDE	VERMELHO	TCP/25	→	allow SMTP	↑ ↓ ✓ ✎ 🗑
6	VERDE	VERMELHO	TCP/110	→	allow POP	↑ ↓ ✓ ✎ 🗑
7	VERDE	VERMELHO	TCP/143	→	allow IMAP	↑ ↓ ✓ ✎ 🗑
8	VERDE	VERMELHO	TCP/995	→	allow POP3s	↑ ↓ ✓ ✎ 🗑
9	VERDE	VERMELHO	TCP/993	→	allow IMAPs	↑ ↓ ✓ ✎ 🗑
10	VERDE LARANJA AZUL	VERMELHO	TCP+UDP/53	→	allow DNS	↑ ↓ ✓ ✎ 🗑
11	VERDE LARANJA AZUL	VERMELHO	ICMP/8 ICMP/30	→	allow PING	↑ ✓ ✎ 🗑

Figura 27 – Endian – Primeira Regra Habilitada.
Fonte: Autoria Própria.

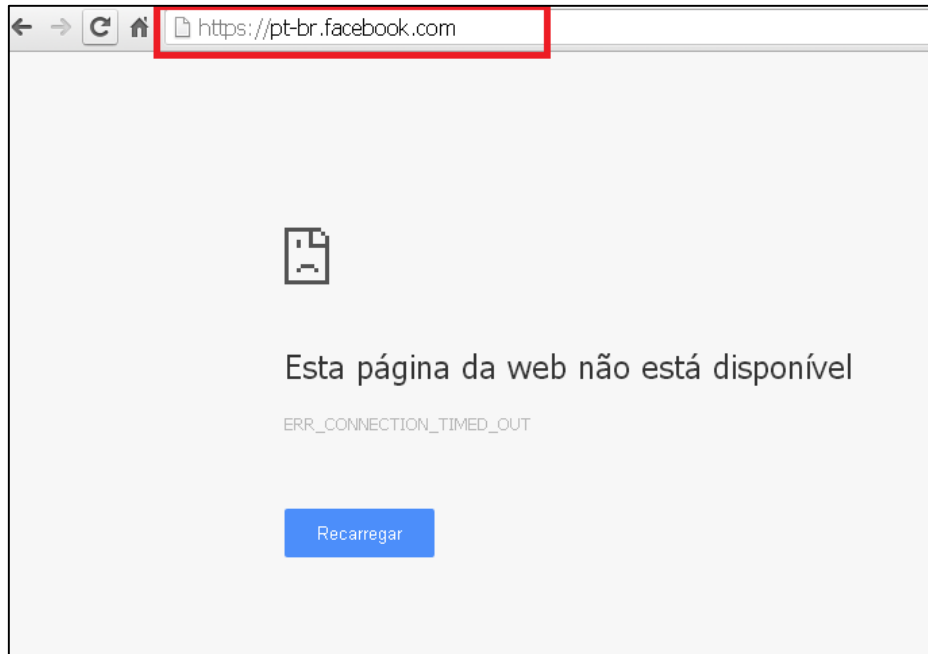


Figura 28 – Endian – Bloqueio da Primeira Regra.
Fonte: Autoria Própria.

A outra regra não foi testada, devido ser apenas uma prevenção para invasão externa, serviço que já vem padrão na instalação do Endian, e que precisa apenas ser ativado para funcionar.

4.1.4.2 TESTES NO PFSENSE

Os testes no pfSense foram efetuados da mesma maneira que no Endian, na Figura 29 mostra a regra ainda desabilitada e que o acesso ainda é permitido ao Facebook conforme a Figura 30.

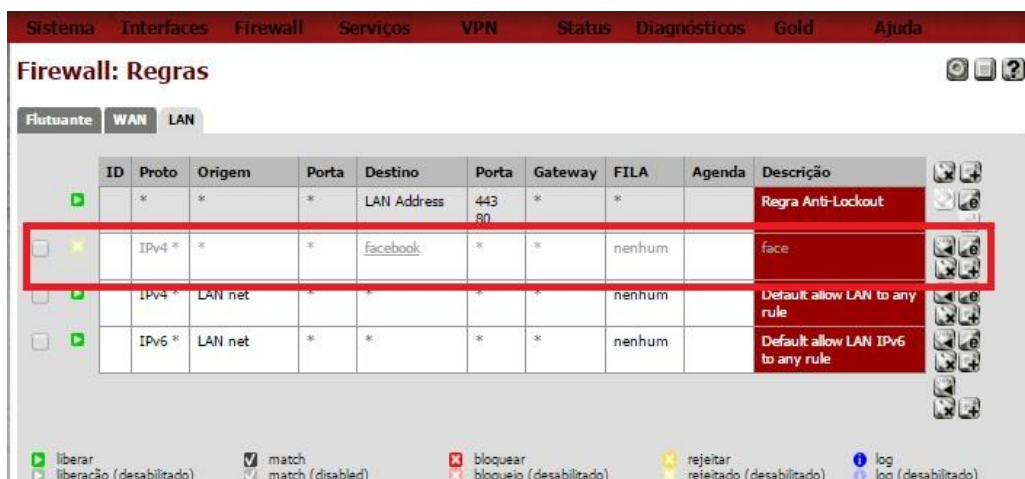


Figura 29 – pfSense – Regra Desabilitada
Fonte: Autoria Própria.



Figura 30 – pfSense – Acesso Permitido ao Facebook
Fonte: Autoria Própria.

Na Figura 31 mostra a regra habilitada e o bloqueio com sucesso na Figura 32 e na Figura 33 mostra o log das tentativas de acesso no momento que a regra está habilitada

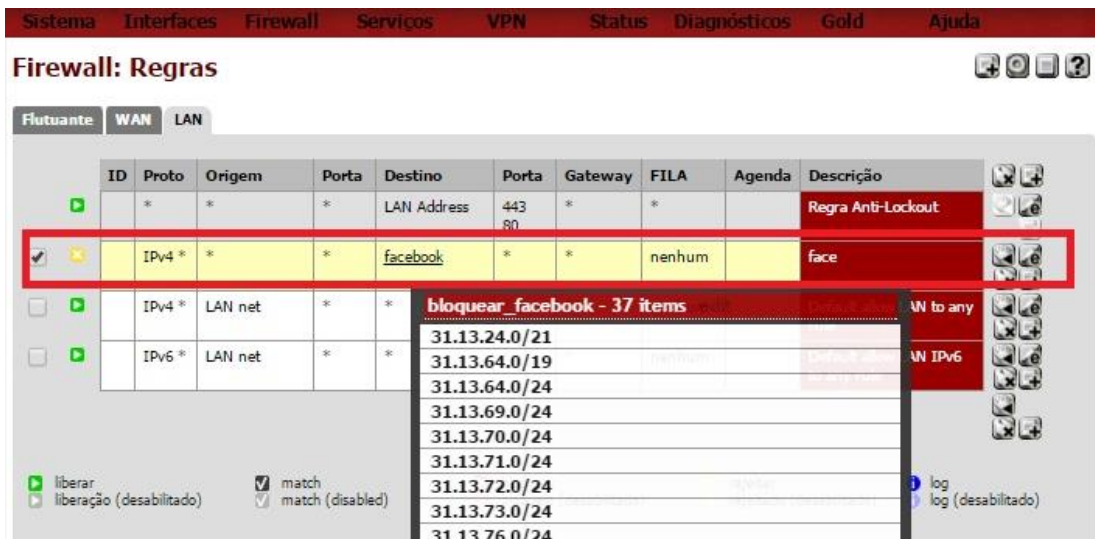


Figura 31 – pfSense – Regra Habilitada
Fonte: Autoria Própria.

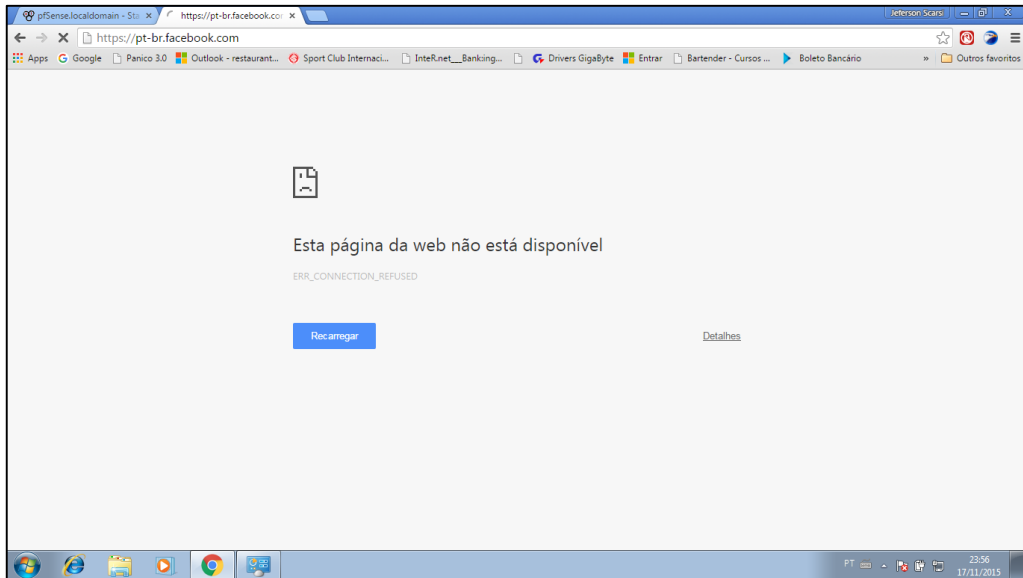


Figura 32 – pfSense – Acesso Bloqueado ao Facebook
Fonte: Autoria Própria.

Status: Registros do sistema: Firewall

Sistema Firewall DHCP Portal Autorização IPsec PPP VPN Balanc. Carga OpenVPN NTP Configurações

Visão Normal Visão Dinâmica Ver resumo

Pass
 Block

Interface: _____ Endereço IP de Destino: _____
 Porta de Origem: _____ Porta de destino: _____
 Protocolo: _____ Protocolos Marcados: _____

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

Últimos 8 logs de entrada do firewall.Máximo(50)

Ação	Tempo	Se	Origem	Destino	Proto
✗	Nov 17 23:53:33	WAN	192.168.0.106:17500	255.255.255.255:17500	UDP
✗	Nov 17 23:53:33	WAN	192.168.0.106:17500	192.168.0.255:17500	UDP
✗	Nov 17 23:54:03	WAN	192.168.0.106:17500	255.255.255.255:17500	UDP
✗	Nov 17 23:54:03	WAN	192.168.0.106:17500	255.255.255.255:17500	UDP
✗	Nov 17 23:54:03	WAN	192.168.0.106:17500	192.168.0.255:17500	UDP
✗	Nov 17 23:54:33	WAN	192.168.0.106:17500	255.255.255.255:17500	UDP
✗	Nov 17 23:54:33	WAN	192.168.0.106:17500	255.255.255.255:17500	UDP
✗	Nov 17 23:54:33	WAN	192.168.0.106:17500	192.168.0.255:17500	UDP

Limpar log

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, W - CWR

Figura 33 – pfSense – Registro de Log de Tentativas de Acesso.
Fonte: Autoria Própria.

A outra regra não foi testada, devido ser apenas uma prevenção para invasão externa, serviço que precisa de um pacote adicional Snort, após instalar o pacote, deve-se ativá-lo.

4.1.4.2 TESTES NO WIRESHARK

Antes de aplicar as regras nos dois firewall, foi feito um teste para verificar o acesso aos sites e conteúdo que serão bloqueados pelas regras, o resultado foi o mesmo nas duas regras, a primeira que bloqueia o acesso ao endereço <https://www.facebook.com/>, e a outra a conteúdos impróprios, os quais abriram sem nenhum problema e foram monitorados pelo Wireshak conforme Figura 34.

24	5.222263000	192.168.0.1	239.255.255.250	SSDP	370 NOTIFY * HTTP/1.1
25	5.326428000	192.168.0.1	239.255.255.250	SSDP	380 NOTIFY * HTTP/1.1
69	13.894944000	192.168.1.199	72.21.91.29	OCSF	511 Request
74	14.041088000	72.21.91.29	192.168.1.199	OCSF	842 Response
241	15.707434000	192.168.1.199	186.235.31.184	OCSF	524 Request
245	15.707571000	192.168.1.199	186.235.31.184	OCSF	524 Request
247	15.707710000	192.168.1.199	186.235.31.184	OCSF	524 Request
257	15.715322000	186.235.31.184	192.168.1.199	OCSF	542 Response
260	15.715509000	186.235.31.184	192.168.1.199	OCSF	542 Response
263	15.718076000	186.235.31.184	192.168.1.199	OCSF	542 Response
521	16.706144000	192.168.1.199	23.50.75.27	OCSF	506 Request
528	16.887986000	23.50.75.27	192.168.1.199	OCSF	388 Response
1147	25.078382000	192.168.0.1	239.255.255.250	SSDP	306 NOTIFY * HTTP/1.1
1154	25.181863000	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
1164	25.286451000	192.168.0.1	239.255.255.250	SSDP	378 NOTIFY * HTTP/1.1

Figura 34 – Wireshark – Monitoramento de Pacotes antes de ativar o Firewall.
Fonte: A autoria Própria.

Após a ativação das regras nos firewall, o Wireshark foi executado e verificado a diferença no tráfego de pacotes, o que sinaliza que os bloqueios obtiveram sucesso, obtendo diferenças nos resultados conforme mostra a Figura 35.

189	23.910796000	192.168.0.1	239.255.255.250	SSDP	306 NOTIFY * HTTP/1.1
190	24.014234000	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
193	24.118390000	192.168.0.1	239.255.255.250	SSDP	378 NOTIFY * HTTP/1.1
194	24.222469000	192.168.0.1	239.255.255.250	SSDP	370 NOTIFY * HTTP/1.1
195	24.326548000	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
198	24.430407000	192.168.0.1	239.255.255.250	SSDP	354 NOTIFY * HTTP/1.1
199	24.534417000	192.168.0.1	239.255.255.250	SSDP	386 NOTIFY * HTTP/1.1
202	24.638536000	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
203	24.742988000	192.168.0.1	239.255.255.250	SSDP	374 NOTIFY * HTTP/1.1
204	24.846620000	192.168.0.1	239.255.255.250	SSDP	368 NOTIFY * HTTP/1.1
209	24.954425000	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
210	25.054311000	192.168.0.1	239.255.255.250	SSDP	370 NOTIFY * HTTP/1.1
216	25.158969000	192.168.0.1	239.255.255.250	SSDP	380 NOTIFY * HTTP/1.1

Figura 35 – Wireshark – Monitoramento de Pacotes com Firewall Ativado.
Fonte: A autoria Própria.

Os resultados no Wireshak foram iguais entre os dois firewall nas duas regras, a terceira regra não foi testada na pratica, apenas ativada para prevenção.

4.2 COMPARAÇÃO ENTRE FIREWALL

A utilização dos dois Firewall definiu uma breve comparação entre as distribuições, suas características, usabilidade, desempenho e funcionalidade, em que ambos possuem ferramentas de segurança.

A usabilidade em ambos as distribuições é fácil, pois se tratando de ambientes de pequenos portes, a alteração para o idioma Português facilita muito o uso. A interface gráfica pelo browser também ajuda nos processos de configuração, monitoramento e uso em geral.

O desempenho do pfSense é bastante alto pois mesmo após as regras habilitadas e com o armazenamento de LOG, ele utiliza pouco memória, pouco processamento e pouco uso em disco conforme a Figura 36 que mostra os dados contidos no Dashboard do pfSense.

System Information	
Nome	pfSense.localdomain
Versão	2.2.4-RELEASE (i386) built on Sat Jul 25 19:56:41 CDT 2015 FreeBSD 10.1-RELEASE-p15 Update available. Click Here to view update.
Platform	pfSense
CPU Type	Intel(R) Core(TM)2 CPU 4400 @ 2.00GHz 2 CPUs: 1 package(s) x 2 core(s)
Uptime	00 Hour 53 Minutes 12 Seconds
Data/hora atuais	Tue Nov 17 23:46:05 BRST 2015
DNS server(s)	127.0.0.1 187.109.96.254 8.8.8.8
Last config change	Tue Nov 17 23:43:19 BRST 2015
State table size	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0% (120/99000) Show states
MBUF Usage	<div style="width: 4%;"><div style="width: 4%;"></div></div> 4% (1020/26584)
Load average	0.97, 0.52, 0.31
CPU usage	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%
Memory usage	<div style="width: 13%;"><div style="width: 13%;"></div></div> 13% of 991 MB
SWAP usage	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0% of 2047 MB
Disk usage	<div style="width: 2%;"><div style="width: 2%;"></div></div> / (ufs): 2% of 35G <div style="width: 3%;"><div style="width: 3%;"></div></div> /var/run (ufs in RAM): 3% of 3.4M

Figura 36 – pfSense – Dashboard
Fonte: Autoria Própria

O desempenho do Endian é bastante alto pois mesmo após as regras habilitadas e com o armazenamento de LOG, ele utiliza pouco memória, pouco processamento e pouco uso em disco conforme a Figura 37 que mostra os dados contidos nas Informações de Hardware na tela principal.

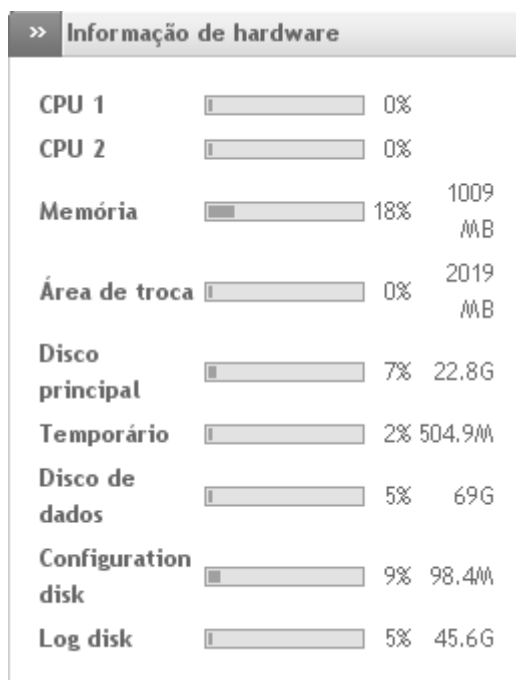


Figura 37 – Endian – Informações de Hardware.
Fonte: Autoria Própria

Analisando as Informações de Hardwares das duas distribuições, o baixo consumo de processamento e de memória de ambas, propõe uma igualdade, deixando a critério do usuário a escolha entre elas.

Material de suporte dos dois firewall podem ser encontrados no site dos fabricantes, mas em Inglês, o que pode dificultar a interpretação por um usuário leigo, entretanto vários fóruns e blog não oficiais contemplam grande conteúdo que pode ajudar.

5 CONCLUSÃO

A utilização do Endian Firewall Community e do pfSense, distribuições gratuitas de segurança para redes SOHO é importante devido a necessidade da segurança da informação, pois cada vez mais a tecnologia é usada para operações importantes, até em operações bancárias que necessitam de proteção. Esses dados podem ser captados por programas maliciosos que estão cada vez mais presentes no nosso dia a dia.

Outra funcionalidade bastante importante é o controle de acesso, onde um dispositivo ou um grupo deles, por meio de regras tem acesso a certos conteúdos bloqueados, como por exemplos sites pornográficos, de jogos e até mesmo em redes sócias, tendo o controle total de acessos a Internet por meio da rede.

A Internet tem um grande e amplo número de sites com conteúdo impróprios para certos usuários, e até mesmo abrem porta para invasão e roubos de dados e informações.

O uso do Endian e do pfSense se mostraram adequadas para alcançar os objetivos propostos. Todo o processo de configuração e uso alcançou as expectativas, abrindo uma ampla forma de criar novos mecanismo e configurações de segurança.

Ferramentas completas de segurança para utilização em redes SOHO que de forma gratuita podem facilitar o controle do uso da rede e da Internet de forma segura e com monitoramento.

Permitindo, assim, alcançar o objetivo geral de analisar as funcionalidades e características de duas distribuições de firewall gratuitas (pfSense e Endian) para uso em redes SOHO.

REFERÊNCIAS

MENDES, Douglas Rocha. **Redes de Computadores: Teoria e Prática**. São Paulo: Editora Novatec. 2007.

KUROSE, James F. **Redes de Computadores e a Internet: uma abordagem top-down / James F. Kurose e Keith W. Ross**. 5. ed. São Paulo: Editora Pearson. 2010.

NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambientes Cooperativos / Paulo Licio de Geus e Emilio Tissato Nakamura**. São Paulo: Editora Novatec. 2007.

NIC.br. **Pesquisas e Indicadores de TIC 2013**. Disponível em: <http://www.cetic.br/pesquisa/domicilios/indicadores>. Acesso em: 18 abril. 2015.

Oficina da Net. **Segurança da Informação**. Disponível em: http://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos. Acesso em: 17 maio. 2015.

Microsoft. **Firewall**. Disponível em: <http://windows.microsoft.com/pt-br/windows/what-is-firewall#1TC=windows-7>. Acesso em: 17 maio. 2015.

Tec Mundo. **Firewall**. Disponível em: <http://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.html>. Acesso em: 23 maio. 2015.

Blog Starti. **Firewall**. Disponível em: <http://www.starti.com.br/blog/quais-os-tipos-de-firewal-e-suas-diferencas/>. Acesso em: 23 maio. 2015.

Info Wester. **Arquitetura dos Firewalls**. Disponível em: <http://www.infowester.com/firewall.php>. Acesso em: 30 maio. 2015.

Wireshark. Site do fabricante. Disponível em: <https://www.wireshark.org/>. Acesso em: 14 março. 2015.

Wikipedia. **Lista de distribuições de Firewall**. Disponível em: https://en.wikipedia.org/wiki/List_of_router_and_firewall_distributions. Acesso em: 30 maio. 2015.

Endian Firewall Community. Site do fabricante. Disponível em: <http://www.endian.com/community/overview/>. Acesso em: 30 maio. 2015.

pfSense. Site do fabricante. Disponível em: <https://www.pfsense.org/>. Acesso em: 31 julho. 2015.

Comunidade Brasileira pfSense. **O que é pfSense**. Disponível em: <http://www.pfsense-br.org/blog/o-que-e-o-pfsense/>. Acesso em: 31 julho. 2015.

Blog Seja Livre. **Conhecendo e Configurando o pfSense**. Disponível em: <http://sejalivre.org/conhecendo-configurando-pfsense/>. Acesso em: 31 julho. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/NBR ISO/IEC**

17799:2005: Informação e Documentação - Referências - Elaboração. Rio de Janeiro, 2005.