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

GIAN MARCEL DE SOUZA

IMPLANTAÇÃO DE FERRAMENTA LIVRE PARA CONTROLE E SEGURANÇA DE REDE LOCAL

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO
2018

GIAN MARCEL DE SOUZA

IMPLANTAÇÃO DE FERRAMENTA LIVRE PARA CONTROLE E SEGURANÇA DE REDE LOCAL

Monografia de especialização apresentada ao III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Anderson Luiz Fernandes

PATO BRANCO
2018

TERMO DE APROVAÇÃO

IMPLANTAÇÃO DE FERRAMENTA LIVRE PARA CONTROLE E SEGURANÇA DE REDE LOCAL

por

Gian Marcel de Souza

Esta monografia foi apresentada às 08h45min do dia 24 de novembro de 2018, como requisito parcial para obtenção do título de ESPECIALISTA, no III 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**.

Prof. M. Eng. Anderson Luiz Fernandes
Orientador / Faculdade Mater Dei

Prof. Dr. Fábio Favarim
UTFPR-PB

Prof. Dr. Eden Ricardo Dosciatti
UTFPR-PB

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

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

AGRADECIMENTOS

A minha família, pelo apoio constante durante a realização do curso, perseverando para a conclusão de mais esta etapa.

A Deus, pela dádiva concedida de todos os dias ter uma nova oportunidade para alcançar meus sonhos.

Aos colegas e professores, pela ajuda e conhecimento transmitidos durante todo o decorrer do curso.

Ao meu professor e orientador Anderson Luiz Fernandes, pela sabedoria e dedicação prestadas durante esta trajetória.

RESUMO

SOUZA, Gian Marcel de. Implantação de Ferramenta Livre para Controle e Segurança de Rede Local. 2018. 50 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2018.

A tecnologia revolucionou e vem facilitando cada vez mais a vida e os negócios de todos. A expansão e utilização dos mais diversos serviços de busca e geração de informações digitais ocorre de forma frenética, consumando uma dependência entre pessoas, corporações e a Tecnologia da Informação. Dessa forma, procurar alternativas de promover segurança e elevar a garantia da continuidade dos serviços e acesso a informação utilizados dentro de uma organização, restringindo o acesso a somente pessoas autorizadas, se tornou um quesito elementar, para todos os segmentos de negócios e dimensões de instituições. Assim, realizou-se um estudo de ferramentas de Firewall que pudessem prover camadas adicionais de segurança à rede local de uma empresa, para tornarem-se alvo de testes de funcionamento, finalizando na implantação e configuração desta técnica na rede da organização. Devido a empresa em estudo ser caracterizada como SOHO, de momento optou-se por uma solução de segurança que não envolvesse altos investimentos para aquisição de equipamentos, pré-requisito de viabilização para continuidade do projeto. As distribuições escolhidas para simulações foram o pfSense e Endian Firewall, ambas ferramentas gratuitas e empregadas em diversos cenários, conforme verificado durante o desenvolvimento do projeto. Durante os laboratórios, foi possível comprovar que as duas distribuições tem um desempenho muito bom, pacotes adicionais que auxiliam na configuração de serviços de rede, como *FailOver*, gerenciados através de painel administrativo disponibilizado em ambiente *web*. Finalizada a realização dos testes nas distribuições, houve a escolha do Endian Firewall para uso na rede da empresa. Com as devidas configurações nos módulos, evidenciadas na seção de resultados, promoveu-se um ambiente mais seguro e controlado para a empresa, atingindo êxito nos propósitos inicialmente identificados e que precisariam ser sanados com a implementação da ferramenta de segurança.

Palavras-chave: segurança. redes. firewall.

ABSTRACT

SOUZA, Gian Marcel de. Free Tool Deployment for Local Network Control and Security. 2018. 50 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2018.

Technology has revolutionized and made life and business easier for everyone. The expansion and use of the most diverse services of search and generation of digital information occurs in a frantic way, consuming a dependence between people, corporations and Information Technology. In this way, seeking alternatives to promote security and increase the guarantee of continuity of services and access to information used within an organization, restricting access to only authorized persons, has become an elementary question for all business segments and dimensions of institutions . Thus, a study of Firewall tools was carried out that could provide additional layers of security to the local network of a company, to become the target of functional tests, finalizing in the implantation and configuration of this technique in the network of the organization. Due to the company under study being characterized as SOHO, at the moment it was chosen a security solution that did not involve high investments for acquisition of equipment, prerequisite of feasibility for project continuity. The distributions chosen for simulations were pfSense and Endian Firewall, both free tools and used in several scenarios, as verified during the development of the project. During the labs, it was possible to prove that the two distributions have a very good performance, additional packages that help in the configuration of network services, like FailOver, managed through administrative panel made available in web environment. After completing the tests in the distributions, there was the choice of Endian Firewall for use in the company network. With the correct configurations in the modules, evidenced in the results section, a more secure and controlled environment for the company was promoted, achieving success in the purposes initially identified and that would need to be remedied with the implementation of the security tool.

Keywords: security. network. firewall.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

CD	*Compact Disc*
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DVD	*Digital Versatile Disc*
EFW	*Endian Firewall Community*
FEBRABAN	Federação Brasileira de Bancos
IBGE	Instituto Brasileiro de Geografia e Estatística
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
NAT	*Network Address Translation*
QoS	*Quality of Service*
RAM	*Random Access Memory*
RDP	*Remote Desktop Protocol*
SOHO	*Small Office Home Office*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
UTM	*Unified Threat Management*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

SUMÁRIO

2 INTRODUÇÃO

Já há algum tempo, praticamente todas as organizações possuem um vínculo muito forte com a Internet, seja para prover serviços para demais empresas, consumir e produzir informações, comunicação das mais diferenciadas formas, dentre inúmeras outras finalidades. A facilidade e agilidade se tornaram uma exigência para conseguir manter-se no mercado, deixando para trás o conservadorismo e burocracia antes fortemente impregnadas nas instituições. Assim, as informações digitais ganharam espaço, alastrando-se rapidamente, assumindo papel singular em todos os setores. Com esse protagonismo alcançado, tornaram-se uma das maiores riquezas das empresas, o que torna a proteção destas, um quesito obrigatório e de suma importância, asseguram Rossetti e Morales (2007).

Segundo Nakamura e Geus (2007), a necessidade de segurança transcendeu a produtividade e a funcionalidade. Velocidade e eficiência dos processos resultam em vantagem competitiva, e a falta de segurança nos meios que possibilitam velocidade e eficiência, tem capacidade de resultar em prejuízos e falta de oportunidades para novos negócios. Protocolos de segurança se fazem necessários hoje nas organizações, não importando o tamanho do estabelecimento. No entanto, essa não é a realidade ainda de muitos locais, principalmente em empresas de menor porte (BRODBECK, 2017).

Redes de pequenos escritórios/escritórios domésticos, conhecidas como SOHO (*Small Office/Home Office)* também são alvos de ataques cibernéticos. A conscientização para investimentos de prevenção muitas vezes é difícil de ser aceita pelos gestores/usuários, o que pode acarretar em perda de dados e consequentemente, perdas financeiras.

Um dos modos mais seguros para tentar evitar que ciberataques obtenham êxito e possam causar danos, é assegurar antes de mais nada, que seus pacotes não consigam entrar na rede. Para essa finalidade, são utilizados firewalls, dispositivos situados entre a rede a ser protegida e o restante do mundo, informam Kurose e Ross (2006). Ainda de acordo com Stallings (2008), um firewall tem capacidade de formar uma barreira, pela qual os pacotes de dados precisam passar. As políticas de segurança especificam qual tipo de tráfego é autorizado a transpor essa barreira. Em geral, os filtros de pacotes são fundamentados em tabelas definidas pelo administrador, que listam as origens e destinos aceitáveis/bloqueados, e as regras que orientam o que deve ser feito com pacotes recebidos de outras máquinas ou destinados a elas, corrobora Tanenbaum (2003).

Aliado ao uso do firewall, também se torna interessante o uso de sistemas denominados Proxy, que complementam a segurança interna das empresas. Através deles, é

possível definir diretrizes de acesso a *sites* e outros recursos da Internet, limitando a navegação dos colaboradores, evitando assim, possibilidade de alcançar locais que potencialmente contenham arquivos maliciosos ou julgados impróprios para o ambiente corporativo, bem como a otimização de recursos, como por exemplo, largura de banda.

Visando implementar estas rotinas de segurança e melhorar o gerenciamento dos serviços de rede em um cenário empresarial SOHO, deu origem a presente proposta de trabalho. Pretende-se alcançar os objetivos aqui definidos, implementando uma solução capaz de fortalecer e auxiliar o administrador de rede em seu cotidiano.

2.1 OBJETIVOS

2.1.1 Objetivo Geral

Realizar a implantação de uma ferramenta livre em ambiente SOHO, visando a segurança e melhor gerenciamento dos serviços de rede.

2.1.2 Objetivos Específicos

- Promover um ambiente mais seguro com a instalação da ferramenta livre, consistindo nas regras de entrada e saída da rede interna;
- Alcançar uma melhor gestão dos *links* de Internet disponíveis, através do monitoramento de banda consumida por cada dispositivo;
- Desenvolver um ambiente controlado de navegação para os usuários, através das restrições de acesso, tanto na matriz quanto nas filiais da empresa.

2.2 JUSTIFICATIVA

Como já apresentado previamente, a segurança da informação hoje exerce um papel fundamental, especialmente no âmbito corporativo. O uso de ferramentas que auxiliam a

proteção e melhor gerenciamento dos recursos relacionados a internet se tornou imprescindível.

Para atender essa demanda em uma rede empresarial de pequeno porte, foi realizada a implantação de uma ferramenta livre, que atue como firewall e forneça também possibilidade de gerir demais necessidades de rede, como entrega dinâmica de endereços IP de rede (DHCP), alteração automática de *link* em caso de quedas (*FailOver),* regras de roteamento, dentre outras. Também auxiliará na filtragem de conteúdo das filiais da empresa.

2.3 ESTRUTURA DO TRABALHO

A estruturação do texto deste trabalho se dará através da divisão de capítulos, sendo que o Capítulo 1 contextualizou o assunto ao leitor, bem como apresentou os objetivos pretendidos e a justificativa da proposta.

O Capítulo 2 contém o referencial teórico, que tem por finalidade apresentar os conceitos das tecnologias e também das áreas envolvidas no projeto, fazendo com que o leitor tenha o conhecimento para compreender os artefatos produzidos durante o desenvolvimento deste.

No Capítulo 3 estão os materiais e a metodologia empregados no desenvolvimento deste trabalho.

O Capítulo 4 contém o resultado do desenvolvimento do projeto, onde serão evidenciadas as aplicações práticas realizadas para o atingimento dos propósitos já informados.

Por fim, o Capítulo 5 apresenta a conclusão com as considerações finais, ofertando ao leitor um parecer dos resultados, bem como opiniões formadas das ferramentas a partir da realização desta proposta.

3 REFERENCIAL TEÓRICO

Neste capítulo, são apresentados os principais conceitos das áreas utilizadas para a realização do projeto.

3.1 REDES DE COMPUTADORES

Apresentando um conceito simplificado do que são redes de computadores, pode-se dizer que trata-se de uma estrutura de computadores e dispositivos, que estão conectados através de um sistema de comunicação, tendo como objetivo final o compartilhamento de informações e recursos entre eles (MENDES, 2007).

Em conformidade com a definição acima, é possível obter-se o fornecimento facilitado de diversos serviços através de uma rede computacional, como compartilhamento de arquivos digitais e impressoras, comunicação entre usuários através de mensageiros online ou mesmo e-mails.

Soares, Lemos e Colcher (1995) expõem que o sistema de comunicação se constitui de um arranjo topológico interligando os dispositivos através de enlaces físicos (meios de transmissão), juntamente com um conjunto de regras com a finalidade de organizar a comunicação através de protocolos. De acordo com a distância entre os dispositivos, é possível realizar uma distinção entre os tipos de redes, como será visto adiante.

Segundo Tanenbaum (2003), um critério utilizado para a classificação de redes é através da escala. Elas podem ser organizadas por seu tamanho físico, como descreve a Quadro 1. Redes pessoais, são destinadas a uma única pessoa. As redes de maior abrangência, subdividem-se em redes locais (LAN), metropolitanas (MAN) e geograficamente distribuídas (WAN). Finalizando, a conexão de duas ou mais redes denomina-se inter-rede, sendo a Internet pública mundial o exemplo mais marcante deste modelo.

Distância entre os dispositivos	**Dispositivos localizados no(a) mesmo(a)**	**Exemplo**
1 m	Metro quadrado	Rede pessoal
10 m	Sala	Rede Local
100 m	Edifício	
1 km	Campus	
10 km	Cidade	Rede

		metropolitana
100 km	País	Rede geograficamente distribuída
1.000 km	Continente	
10.000 km	Planeta	A Internet

Quadro 1 – Classificação de redes de acordo com seu tamanho físico
Fonte: Tanenbaum (2003)

A Internet pública trata-se de um vasto conjunto de redes que interconecta milhões de equipamentos de computação em todo o mundo. Inicialmente, esses dispositivos eram primordialmente concentrados em computadores tradicionais de mesa e servidores que armazenam e transmitem informações, como páginas *Web*. Contudo, com a explosão da disseminação de dispositivos finais que possuem conexão com a Internet, como *smartphones*, notebooks, *tablets*..., quebraram esse paradigma afirmam Kurose e Ross (2006).

3.2 SEGURANÇA DE REDES E DA INFORMAÇÃO

Como Tanenbaum (2003) apresenta, durante as primeiras décadas, as redes de computadores eram usadas principalmente por pesquisadores universitários e funcionários de empresas, tendo um uso basicamente formado por compartilhamento de impressoras e troca de mensagens eletrônicas. Neste cenário, a preocupação com segurança era quase nula. Porém, como o universo de dispositivos se propagou e uma enorme quantidade de serviços passaram a ser ofertadas pelas redes, a necessidade de proteção também ganhou grande enfoque.

No âmbito de segurança, todos os agentes envolvidos estão em constante evolução. A ação de novos tipos de ataques tem como reação medidas de prevenção, que levam ao desenvolvimento de novas técnicas de ataques, formando um ciclo ininterrupto. Assim, no mundo da informação, a segurança deve ser contínua e prover aperfeiçoamento para novos tipos de ameaças (NAKAMURA; GEUS, 2007).

Segundo os mesmos autores supracitados, a tecnologia de forma geral largamente utilizada hoje pelo homem, propõe realizar seus trabalhos de modo facilitado, com agilidade e eficiência, produzindo assim, melhores resultados. A rede é uma das principais tecnologias, permitindo a conexão entre todos os elementos, que vão desde roteadores até os servidores que hospedam banco de dados e sistemas gerencias.

Assim, a confidencialidade, integridade e disponibilidade dessa estrutura de rede passam a ser vitais para o bom andamento das organizações. Benetti (2015), explica que estes são os três pilares da segurança da informação, conforme a Figura 1. A confidencialidade garante que a informação não será conhecida por pessoas que não sejam autorizadas para tal. Integridade endossa que a informação está correta e é apresentada corretamente para quem a consulta. Já por sua vez, a disponibilidade assegura que a informação possa ser obtida sempre que for necessário.

Figura 1 – Os três pilares da segurança da informação
Fonte: Duarte (2012)

A importância da segurança pode ser destacada ainda mais quando se analisam números e oportunidades que surgem no meio digital. Em um estudo publicado no *site* Valor Econômico, realizado pelo Instituto Brasileiro de Geografia e Estatística (IBGE), Bôas (2018) retrata que as vendas online registraram uma receita bruta de R$ 43,84 bilhões em 2016, crescimento de 8,2% em relação ao ano anterior.

Já a Agência Brasil (2018), que faz parte do grupo Empresa Brasil de Comunicação, responsável por importantes veículos de comunicação do país (como exemplo o programa de rádio “A Voz do Brasil”), exibe que os clientes bancários estão migrando cada vez mais para os serviços de aplicativos de celular. A pesquisa da Febraban – Federação Brasileira dos Bancos, apontou um crescimento de 70% nas transações financeiras por aplicativos de celular no ano passado, projetado pelo pagamento de contas (85%), transferências (45%), contratação de crédito (141%) e investimentos/aplicações (42%). Essa pesquisa já é realizada há 26 anos e contou com a participação de 24 bancos.

Contudo, assim como há elevação nas oportunidades de novos serviços, há elevação em incidentes de ataques reportados. Em consulta ao site CERT.br - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, comprova-se o aumento de incidentes, analisando-se o período 2016-2017, como demonstra a Figura 2.

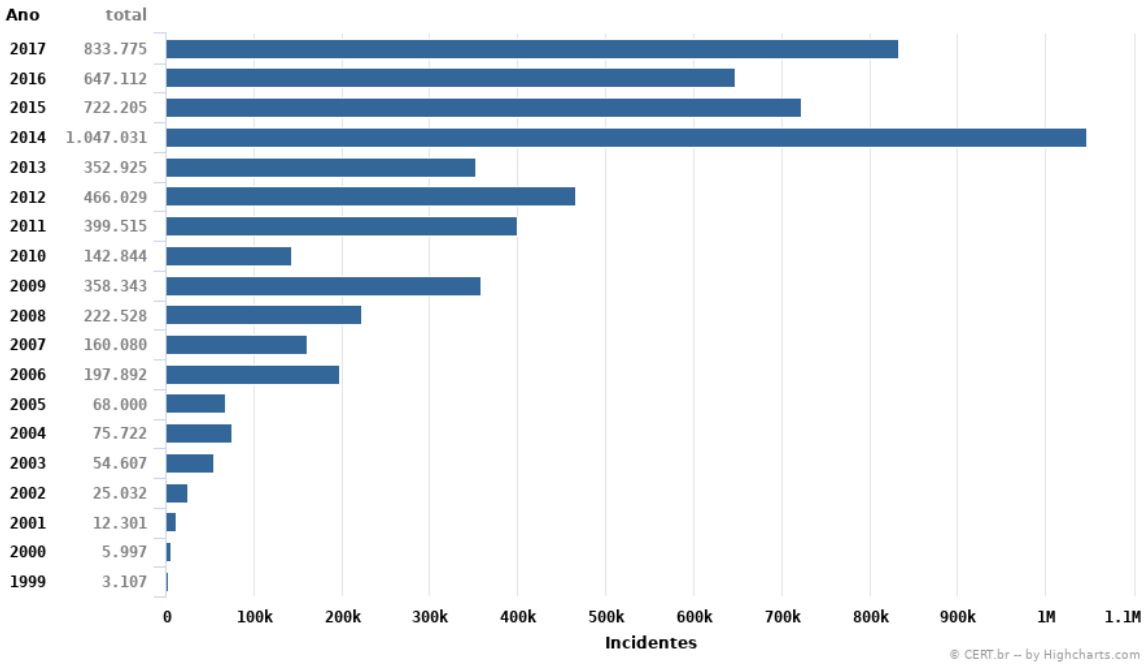
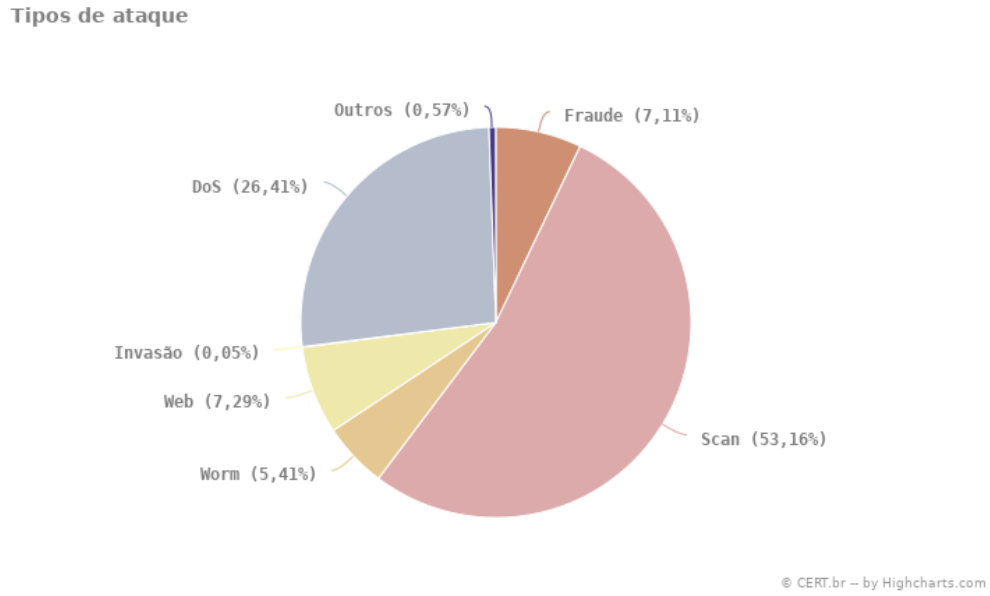


Figura 2 – Total de incidentes reportados ao CERT.br por ano
Fonte: CERT.br (2018)

Bem como, na Figura 3, são expostos os tipos de ataques registrados em 2017.



Legenda
worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
dos (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Figura 3 – Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2017
Fonte: CERT.br (2018)

Dessa maneira, a segurança deve ser visualizada como um elemento que permite a exploração de novos segmentos, protegendo os serviços que já estão em execução e os novos que irão surgir. Cabe as empresas e aos usuários se adequarem a esta demanda, para não sofrerem com eventuais consequências pela falta dela.

3.3 FIREWALL

Como já apresentado, a tecnologia está em constante evolução, trazendo novas possibilidades e oportunidades de negócios no meio digital. Porém, seja através de noticiários ou demais veículos de informação, mesmo as pessoas menos habituadas já detém o conhecimento que a Internet é um ambiente que pode ser perigoso. Assim, o uso de ferramentas de proteção ganhou destaque, tanto em esfera doméstica, quanto principalmente, nos meios corporativos, sendo o firewall, uma das principais alternativas.

Pode-se dizer que um firewall é um ponto entre duas ou mais redes, sendo um componente ou conjunto de componentes, através do qual passa todo o tráfego, possibilitando assim, que o controle e os registros de todo o tráfego sejam realizados, através das políticas definidas, afirmam Nakamura e Geus (2007).

Segundo Goodrich e Tamassia (2013), a utilização de firewalls é realizada tanto como medida preventiva para proteger os usuários de redes internas de atacantes, quanto meio de censura. Muitas empresas restringem o acesso de seus funcionários a certos protocolos ou visitem determinados sites por meio do emprego desta tecnologia.

De acordo com os mesmos autores, os firewalls podem ser implementados em hardware ou software, sendo geralmente adotados no perímetro de uma rede interna, no ponto onde esta se conecta com a Internet, como ilustra a Figura 4. Os pacotes que transpõem o firewall, podem ser aceitos, descartados ou rejeitados, respeitando as regras implementadas.

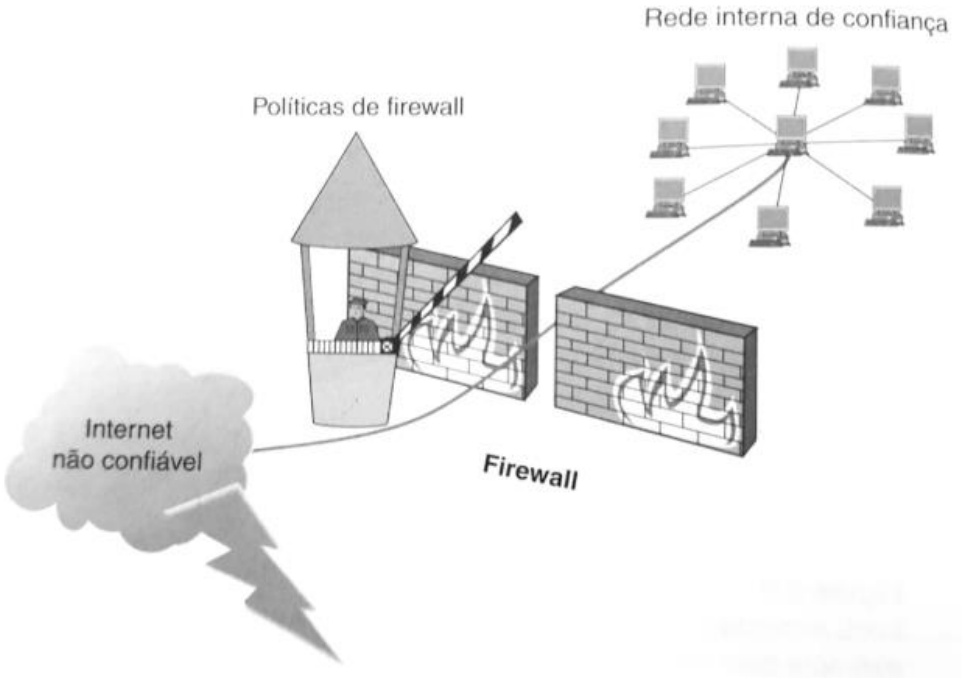


Figura 4 – Implementação de Firewall, separando a rede interna da Internet
Fonte: Goodrich, Tamassia (2013)

Nakamura e Geus (2007), explicam que com o passar do tempo, os firewalls foram agregando uma série de componentes e funcionalidades que influi diretamente no nível de segurança. Algumas dessas funcionalidades, tratam-se dos constituintes clássicos de um firewall, outras foram implementadas devido a evolução natural das necessidades de segurança. A Figura 5 ilustra as funcionalidades comumente desempenhadas por um firewall.

Figura 5 –Exemplos de componentes de um firewall
Fonte: Nakamura, Geus (2007)

A função de um firewall pode ser desempenhada de diferentes formas, o que justifica uma metodologia ou outra, são fatores como critérios do desenvolvedor, necessidades específicas do que será protegido, características do sistema operacional que mantém, estrutura de rede, e assim por diante, informa Alecrim (2013). Ainda, segundo este autor, é por isso que se encontram diferentes tipos de firewalls, sendo os mais conhecidos a seguir apresentados:

- Filtragem de pacotes: as primeiras soluções a surgirem na década de 1980, possuem uma metodologia simples, porém oferecem um significativo nível de segurança. Tem como objetivo permitir ou não a passagem dos pacotes pela rede, analisando informações do cabeçalho de cada pacote, como endereço IP de origem e destino, tipo de serviço..., regidos por diretrizes pré-estabelecidas que definem se serão aceitos os descartados.
- Firewall de aplicação ou *Proxy* de serviços: funciona por meio de retransmissões de conexões TCP, ou seja, o usuário se conecta a uma porta TCP no Firewall, que por sua vez, abre outra conexão com o mundo exterior. O proxy ainda consegue trabalhar nas camadas de sessão, transporte e aplicação, o que lhe fornece mais controle sobre a interação entre cliente e o servidor.
- Inspeção de estados: analisam todo tráfego de dados para constatar os estados, padrões aceitáveis por suas regras, que serão usados para manter a comunicação. Por exemplo, os pacotes de dados iniciais informam quais portas TCP serão usadas. Caso vertiginosamente o tráfego passe a ocorrer por portas não mencionadas previamente, o firewall pode detectar esta ocorrência como uma anormalidade e efetuar o bloqueio.

Nakamura e Geus (2007), ainda citam os firewalls híbridos, que misturam as três tecnologias anteriormente mencionadas, de modo a aproveitar as melhores características dos filtros de pacotes, filtros de pacotes baseados em estados e *proxies* para cada um dos serviços específicos.

3.4 ENDIAN FIREWALL

Fundada em Appiano, Itália, no ano de 2003, por uma equipe de especialistas em redes e entusiastas do Linux, o objetivo da empresa Endian logo ficou explícito: desenvolver um sistema de gerenciamento unificado de ameaças de código aberto mais potente e com uso facilitado que o mercado já ofereceu (ENDIAN, 2018).

Ainda segundo o site da fabricante, utilizando-se das melhores ferramentas de código aberto, a Endian lançou seus primeiros produtos, sendo um gratuito e outro profissional com custo para aquisição, em dois anos de existência. Desde então, a versão gratuita oferecida acumulou mais de 1,7 milhão de *downloads*, alcançando uma marca notória e se

estabelecendo como uma das distribuições mais populares de código aberto UTM (*Unified Threat Management).*

Os produtos Endian alteraram o cenário de segurança de rede, disponibilizando uma solução de UTM, com experiência de gestão única: implementar de forma rápida, gerenciar de forma fácil e permanecer flexível. Milhares de usuários espalhados pelo mundo estão utilizando produtos UTM Endian, mantendo suas organizações mais seguras contra vírus, *spyware*, *spam*, roubos de dados e outras ameaças da Internet. Isso é possível, graças a gama de funcionalidades incluídas na ferramenta, como *Proxy* HTTP, IPS, filtro de conteúdo, VPN, QoS, Firewall, agendamento de *backup*, dentre outras, conforme descrito por VirtualOne (2018).

3.5 PFSENSE

De acordo com o *site* do fabricante pfSense (2018), é uma distribuição personalizada de código aberto *FreeBSD*, adaptada especialmente para utilização como uma ferramenta de firewall e roteamento que pode ser inteiramente gerenciada via interface *web.*

Assim como o *Endian Firewall*, o *pfSense* também é considerado uma Central Unificada de Ameaças (UTM), pois é compreendido por um dispositivo com diversas funções, como: firewall, antivírus, *antispyware, antispam*, filtragem de conteúdo, detecção de intrusão, entre outros (DELFINO, 2018).

Delfino (2018) ainda complementa, que um UTM com tantas funções primordiais de segurança como o *pfSense*, pode funcionar com uma excelência comparável aos mais diversos produtos desse mercado. Além disso, outras vantagens dessa ferramenta, são a estabilidade, fácil utilização devido ao painel administrativo *web*, a exigência de recursos de *hardware* ser muito modesta e os excelentes recursos de filtragem.

4 MATERIAIS E METODOLOGIA

Neste capítulo são apresentadas as ferramentas e a metodologia utilizada para alcançar os objetivos propostos no trabalho. Para o projeto em questão, foram analisadas apenas ferramentas gratuitas e que possibilitam a implementação com um baixo custo de investimento em hardware, visando atender a o cenário da empresa escolhida para implantação.

4.1 MATERIAIS

Conforme já apresentado na seção anterior, as ferramentas que foram utilizadas neste projeto, são centradas nas distribuições Endian Firewall e pfSense. Estas foram base para os passos seguintes desta proposta, ofertando o cenário de testes para obtenção dos resultados, que culminaram na escolha em uma delas para implementação na empresa em estudo.

4.2 METODOLOGIA

Inicialmente, para conseguir atingir o objetivo deste trabalho, foi necessário a realização de uma pesquisa bibliográfica e levantamento de possíveis ferramentas que atendessem a demanda existente na empresa que era objeto de implantação.

Assim, analisando-se o cenário atual em artigos, fóruns e demais trabalhos disponíveis na Internet, foram elencadas duas ferramentas que ganharam destaque em diversas obras consultas, tratando-se do *Endian Firewall* e o *pfSense.* Estes oferecem uma solução gratuita, que é um dos pré-requisitos para o desenvolvimento deste trabalho, visando o baixo custo da implantação para uma rede SOHO.

Além disso, de acordo com as especificações encontradas, ambos conseguem oferecer serviços de Rede Particular Virtual (VPN), DHCP, múltiplas conexões com a Internet, além é claro, de prover segurança, utilizando-se das regras que serão definidas e ajustadas para o melhor funcionamento possível da tecnologia que será empregada. Juntamente a isto, o hardware mínimo solicitado pelas desenvolvedoras para a instalação, é compatível com máquinas já disponíveis na empresa, não havendo assim necessidade de investimento com novos equipamentos.

Durante o levantamento de informações sobre as tecnologias, foi possível montar o Quadro 2, que é um comparativo entre as distribuições, visando as funcionalidades que serão utilizadas desde o início da implantação, até aquelas que poderão ser implementadas posteriormente se assim desejar a empresa.

Serviços	Endian Firewall	Pfsense
Proxy	Sim	Sim
VPN	Sim	Sim
Antivírus	Sim	Sim
WAN *Failover*	Sim	Sim
Roteamento	Sim	Sim
DHCP	Sim	Sim
Alta disponibilidade	Não	Sim
Alerta de eventos	Sim	Sim
Relatórios de logs	Sim	Sim
Atualização	Sim	Sim
Backup	Sim	Sim
Firewall filtro de pacotes	Sim	Sim
Painel administrativo web	Sim	Sim
Gratuito	Sim	Sim

Quadro 2 – Características das distribuições Endian Firewall e PFSense
Fonte: Autoria própria (2018)

Como ambas as tecnologias apresentam muitos fatores em comum, para realizar a escolha foram implementados e testados tanto *Endian Firewall* como *pfSense* em um ambiente controlado, para assim verificar o real funcionamento destes. O ambiente controlado foi constituído por uma máquina física que conteve a distribuição de firewall, dois *links* de Internet e um notebook. As configurações do servidor e do notebook podem ser visualizadas no Quadro 3.

Hardware	Servidor	Notebook
Processador	Intel Pentium 4	Intel Core i5
Memória RAM	4 GB	8 GB
HD	500 GB	1000 GB
Placas de Rede	3 placas – Gigabit	1 placa - Gigabit

Quadro 3 – Configurações do Servidor utilizado para o UTM e Notebook
Fonte: Autoria própria (2018)

Por meio do computador portátil, foram realizados os testes simulando os usuários da rede, que tiveram seu acesso filtrado pela distribuição firewall em operação. Assim, nas diretrizes de acesso, foi efetuado o bloqueio de alguns sítios da Internet para validação do correto funcionamento esperado das distribuições. Bem como, realizado também o bloqueio

de portas utilizadas para conexão da área de trabalho remota. Há necessidade de bloqueio de portas de navegação (80 e 443), pois de acordo com os requisitos tratados com a empresa, será de mais valia do que realizar instalação de certificados em todas as máquinas, para tratamento de navegação segura. Outro aspecto, é a configuração de proxy não transparente, sendo necessário ajustar nas máquinas o endereço do servidor proxy e porta que funcionará.

Também foram realizados testes com a funcionalidade *FailOver* das ferramentas, a fim de comprovar sua eficácia em falhas em um dos *links* de Internet, buscando gerar o mínimo de transtorno possível para os colaboradores da empresa em possíveis desconexões durante o expediente.

5 RESULTADOS

Este capítulo apresenta o resultado da realização do trabalho. Todos os testes, etapas e a implementação da ferramenta em produção aqui serão discorridas.

5.1 TESTES COM PFSENSE - VERSÃO 2.4.4

Para iniciar a avaliação da distribuição pfSense, foi necessário realizar o *download* do *appliance*, disponível no site da desenvolvedora. Para obtenção do arquivo, é preciso apenas informar a arquitetura da máquina onde o mesmo será instalado, qual o tipo da imagem, podendo ser preparada diretamente para Pen Drive ou através de imagem ISO para CD/DVD e o local de onde será baixado o arquivo, como mostra a Figura 6.

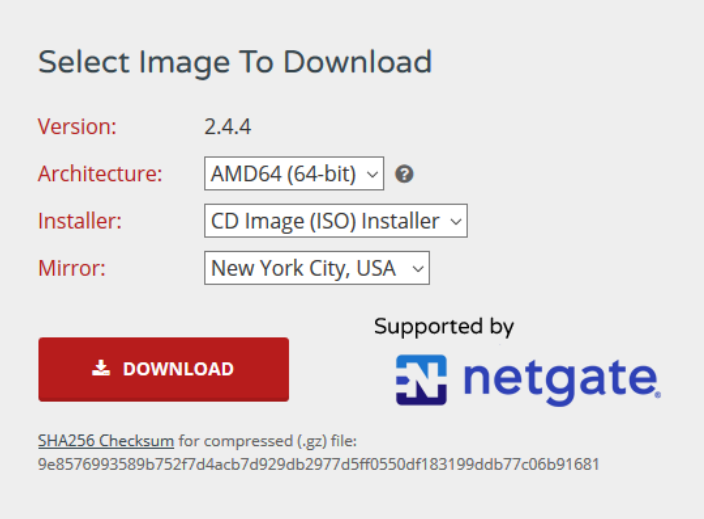


Figura 6 – Download da distribuição pfSense
Fonte: pfSense.org (2018)

Após os devidos processos de preparação de uma mídia inicializável, realizou-se a instalação do *appliance* na máquina já descrita na seção de materiais e métodos.

A instalação ocorre de maneira simplificada, e após o término dos processos automáticos, é solicitado ao usuário informar qual a placa de rede que será usada como WAN, e qual será utilizada como LAN, para a rede local. Para facilitar, o pfSense já informa primeiramente a nomenclatura usada para as placas de rede identificadas na máquina, ilustrado pela Figura 7, sendo assim, somente necessário direcionar corretamente as interfaces para cada situação.

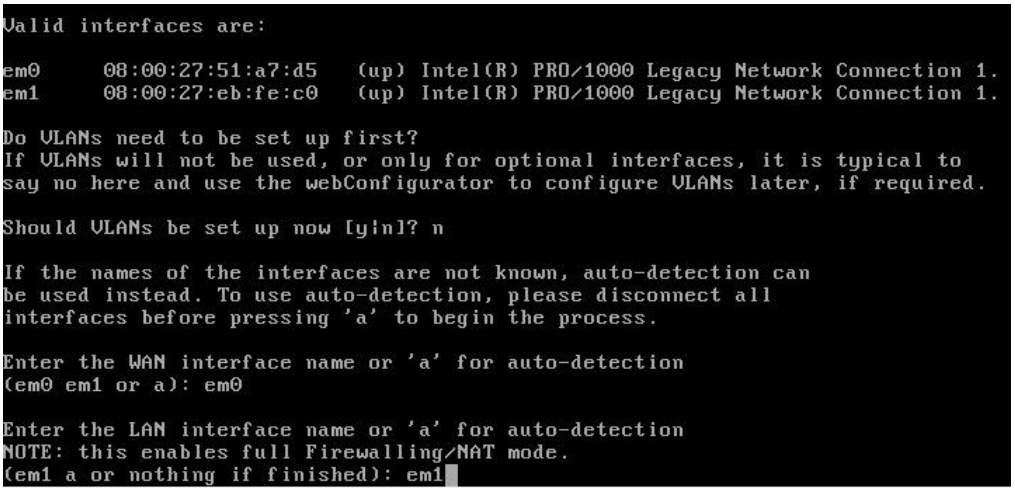


Figura 7 – Identificando as placas de rede do servidor
Fonte: Autoria própria (2018)

Realizada a ordenação das interfaces de rede, o pfSense exibirá as configurações iniciais, como endereço de IP para WAN e LAN, conforme Figura 8. O IP da LAN, também dará acesso ao painel administrativo web do *appliance*, provendo o gerenciamento de todas as funções disponíveis.

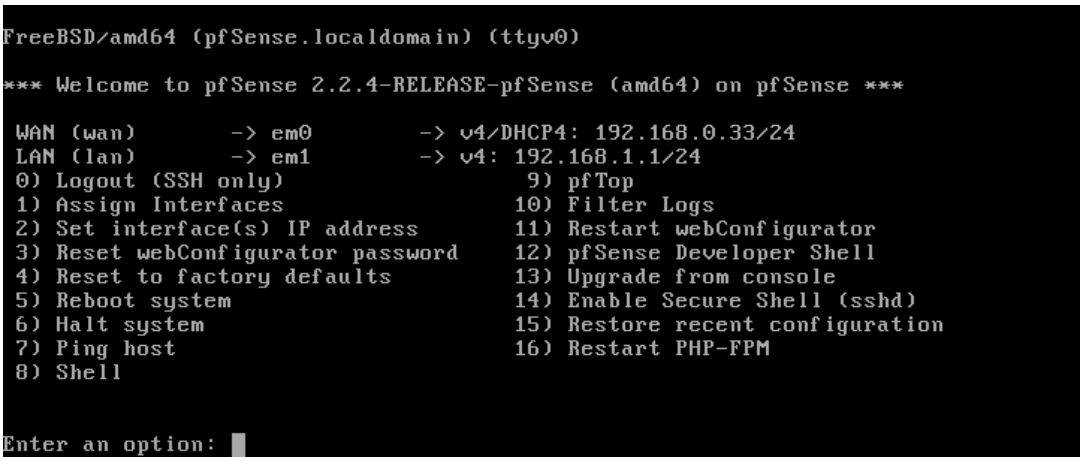


Figura 8 – Tela de Informações gerais do pfSense
Fonte: Autoria própria (2018)

Para acesso ao painel administrativo, basta informar o endereço de IP da LAN em um *browser*, neste caso https://192.168.1.1. O navegador irá direcionar para a página de login do pfSense, que por padrão tem o usuário admin e a senha pfsense, como exibido na Figura 9.

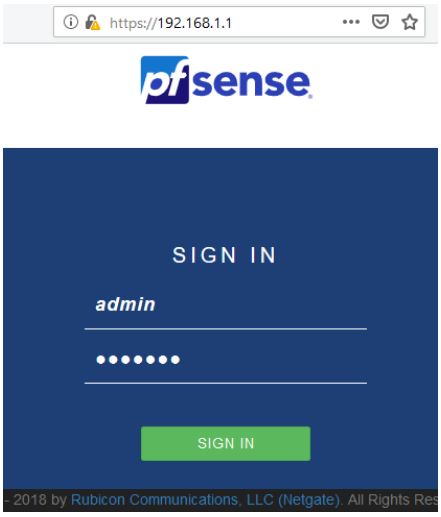


Figura 9 – Tela de Login para gerenciamento do pfSense
Fonte: Autoria própria (2018)

Através da página inicial do pfSense, é possível visualizar várias informações, como versão do próprio sistema, uso de memória e processador, uso do disco, dentre outras, demonstrado pela Figura 10. Isso é configurável, podendo ser adicionado ou removido informações desta seção inicial. Destaca-se também, avisos provenientes do sistema, como alteração da senha padrão após a instalação.

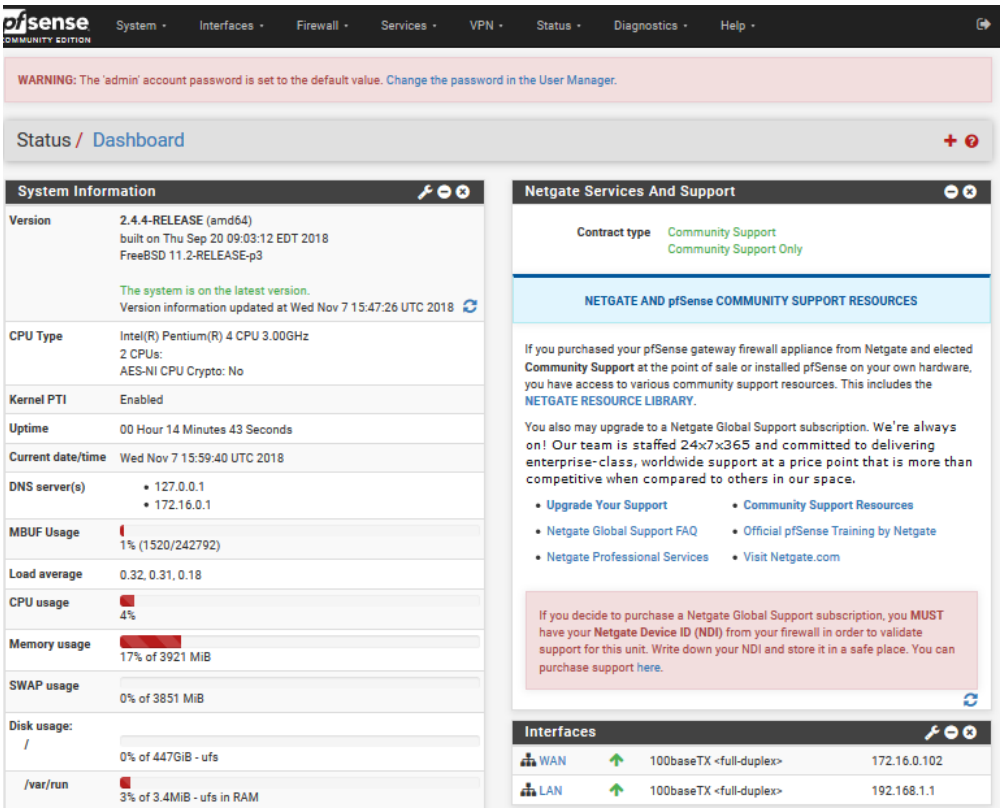


Figura 10 – Página inicial do configurador web do pfSense
Fonte: Autoria própria (2018)

Após reconhecimento e aprendizagem da ferramenta, iniciou-se então as tratativas para configuração dos módulos, de acordo com os aspectos para testes definidos no tópico de materiais e métodos.

Primeiramente, foram configuradas as regras de firewall para bloqueio de algumas portas específicas. A primeira regra definida pelo utilizador, bloqueia a porta TCP 3389, comumente usada para conexões da Área de Trabalho Remota do Windows, protocolo RDP, vide Figura 11. Para validação do funcionamento, no notebook com sistema operacional Windows usado para testes, houve a tentativa de uma conexão, como confirma a Figura 12.

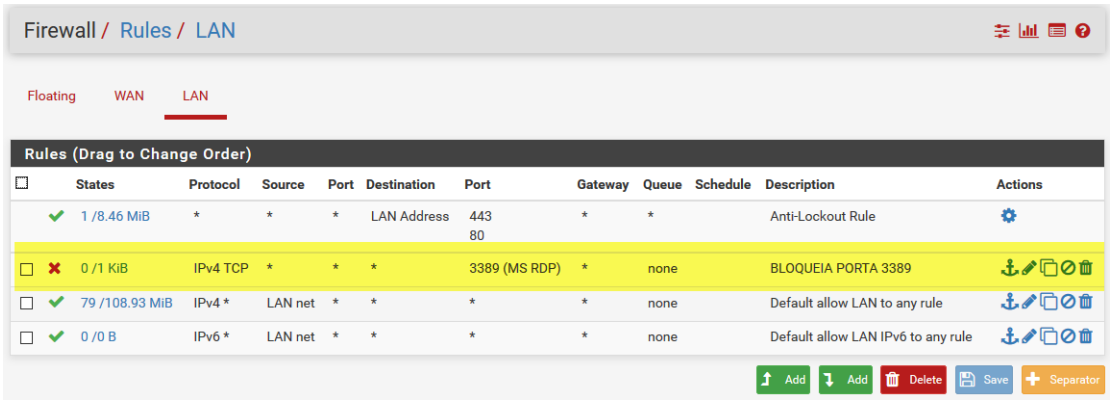


Figura 11 – Regra destacada em amarelo que faz o bloqueio da porta 3389
Fonte: Autoria própria (2018)

Tentativa de conexão através da Área de Trabalho Remota, sendo bloqueada pelo firewall pfSense.

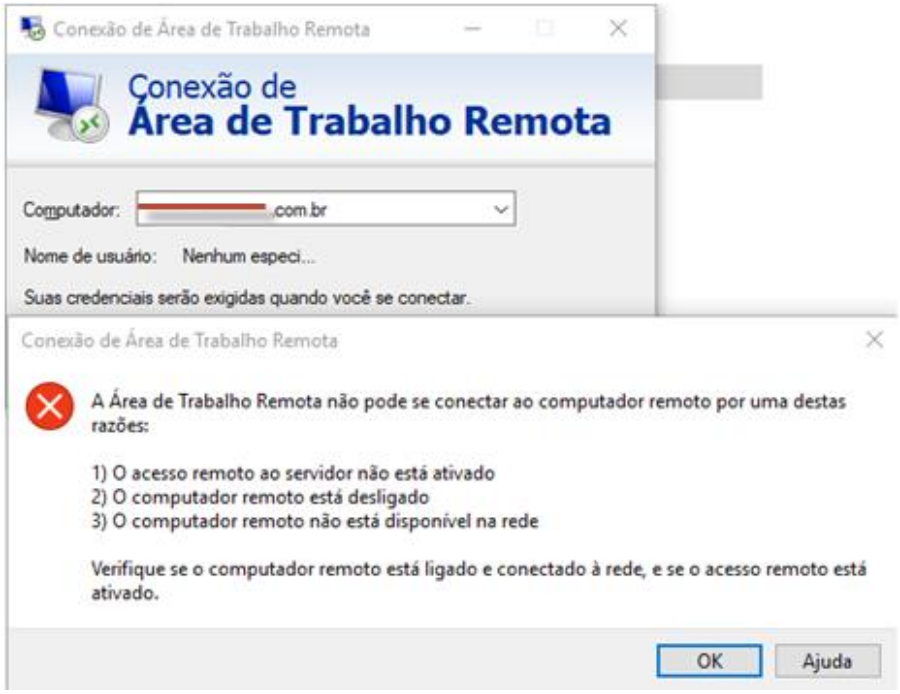


Figura 12 – Tentativa de conexão através de RDP (conteúdo oculto por segurança)
Fonte: Autoria própria (2018)

Imediatamente após, foi excluída a diretiva, fazendo com que a conexão voltasse a funcionar normalmente, exemplificado pelas Figuras 13 e 14.

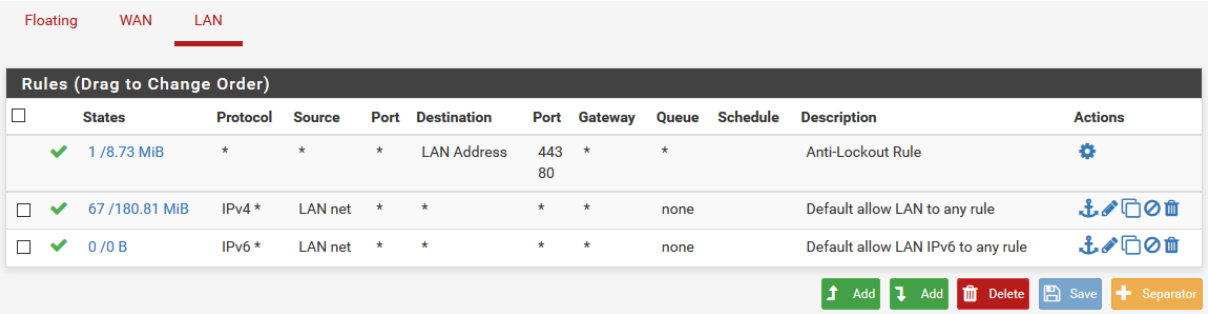


Figura 13 – Exclusão da regra anteriormente ilustrada
Fonte: Autoria própria (2018)

Nesta experiência, a conexão voltou a ser estabelecida, solicitando ao usuário os dados de login e senha para acesso à Área de Trabalho Remota.

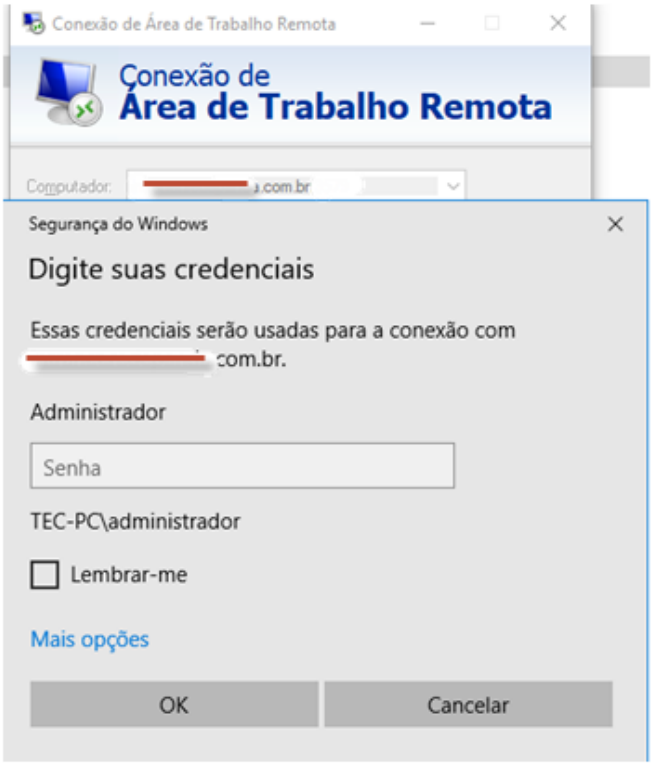


Figura 14 – Conexão estabelecida com o servidor (dados ocultos para segurança)
Fonte: Autoria própria (2018)

Continuando com as implementações de firewall, foram aplicadas duas novas regras, que ajudarão também no controle de acesso a sites dos usuários da rede. Para isso, foram incorporadas as diretrizes que bloqueiam as portas TCP 80 e 443, protocolos HTTP e HTTPS respectivamente, comprovado pela Figura 15.

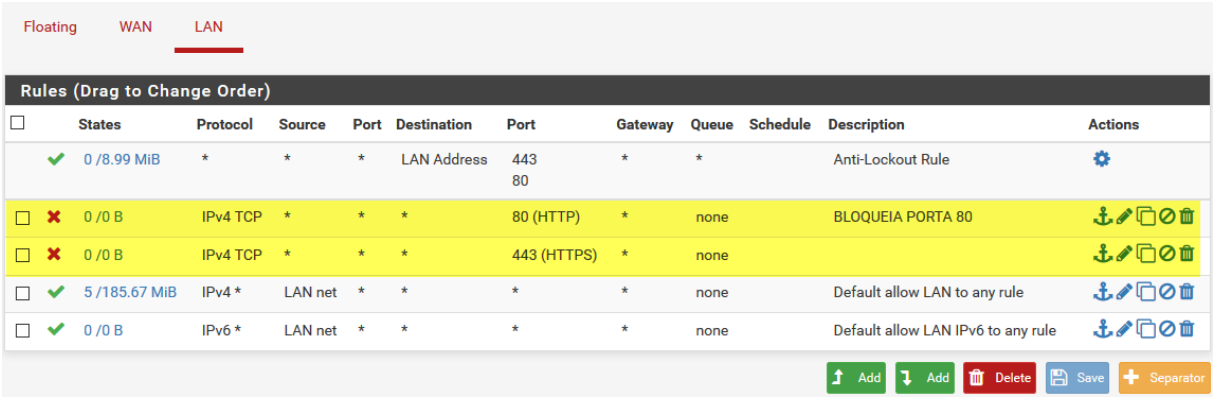


Figura 15 – Bloqueios das portas 80 e 443, conforme destacado
Fonte: Autoria própria (2018)

Assim, a navegação por *browser* fica impossibilitada, como evidencia a Figura 16.

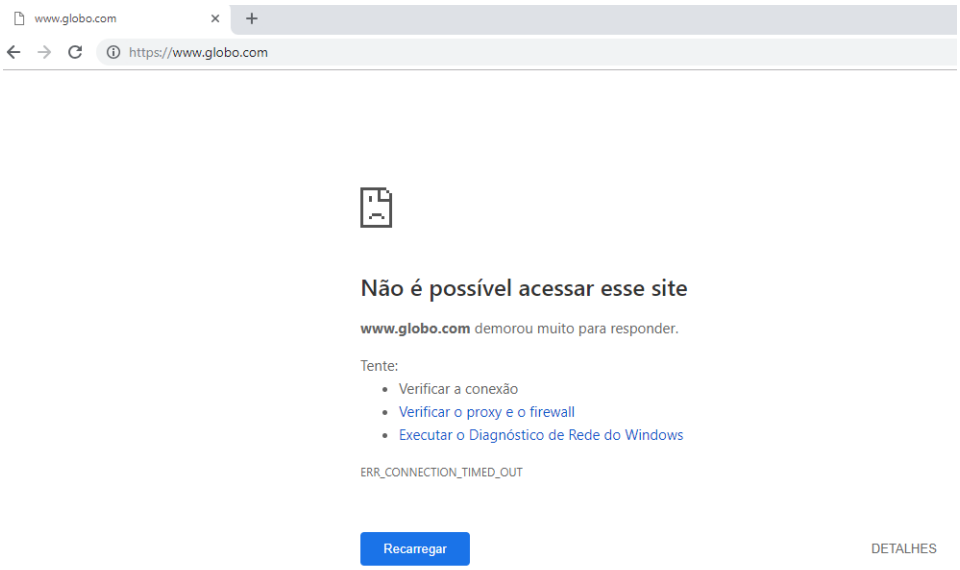


Figura 16 – Navegação dos usuários não sendo possível pelo bloqueio no pfSense
Fonte: Autoria própria (2018)

Para que a navegação volte a acontecer, de acordo com os critérios definidos pela empresa onde foi realizado a implantação do firewall, é imprescindível realizar a configuração do módulo *proxy* disponível no pfSense. Isso se faz necessário, para que o *Proxy* de Serviços efetue as retransmissões de conexões TCP para o mundo exterior, uma vez que as portas TCP 80 e 443 foram previamente bloqueadas. Assim, é habilitado o *Squid Proxy*, na interface LAN do pfSense, configurado para funcionar na porta 3128, como ilustra a Figura 17.

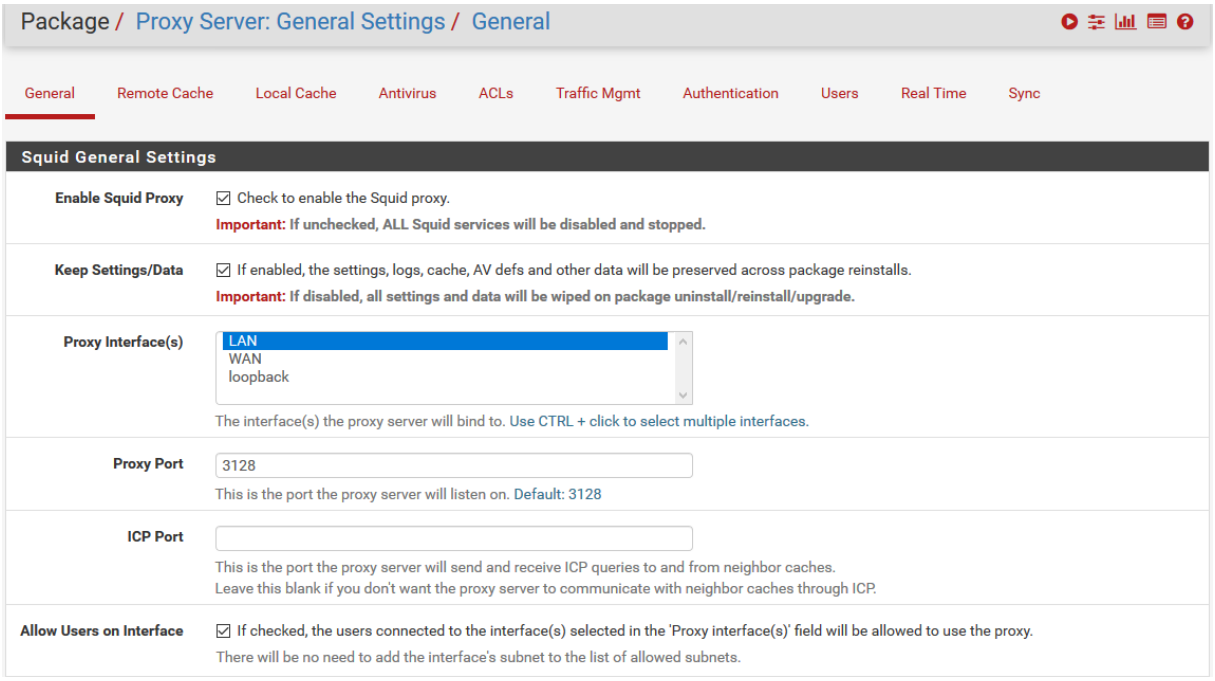


Figura 17 – Habilitando o módulo proxy do pfSense
Fonte: Autoria própria (2018)

Habilitado o módulo Proxy do pfSense, basta configurar no navegador do cliente, neste caso no notebook de testes, o endereço e a porta que o servidor proxy responderá, como mostra a Figura 18.

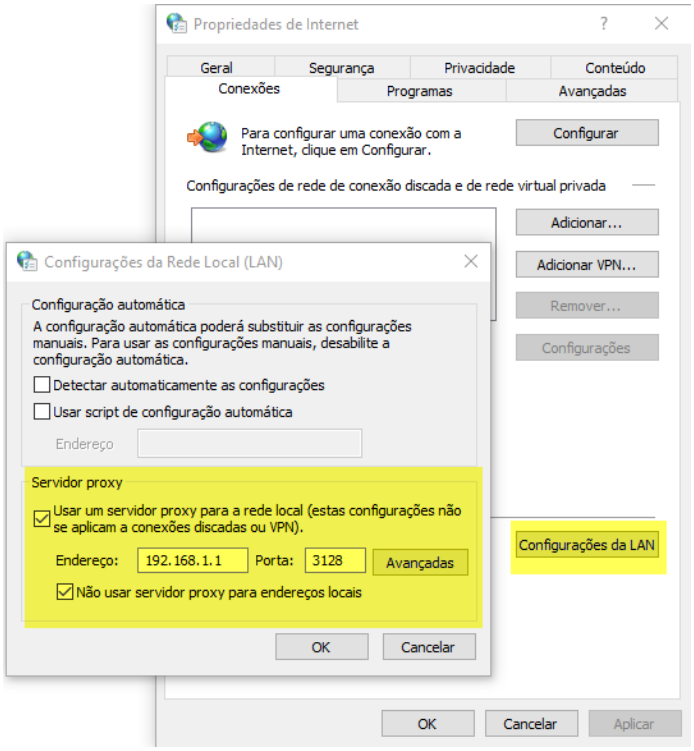


Figura 18 –Ajustando as configurações da LAN
Fonte: Autoria própria (2018)

Desta forma, a navegação será novamente possível, e também, haverá viabilidade de restringir sítios da Internet ainda através do módulo Proxy, bastando colocar os domínios no campo de *blacklist*, como demonstra a Figura 19. Isso atende outra demanda necessária na empresa de implantação.

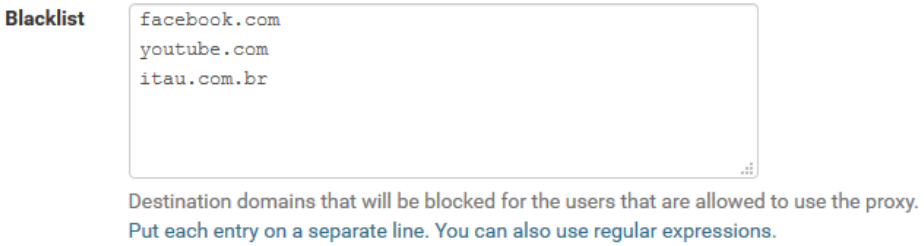


Figura 19 – Bloqueando sites através do proxy
Fonte: Autoria própria (2018)

Finalizada as configurações, os sites não listados serão exibidos quando requisitados pelos usuários, porém, ao tentar acessar um dos domínios da *blacklist*, aparecerá uma mensagem de falha ao acesso ao site, como exemplifica a Figura 20, onde o acesso a página da UTFPR é feito com sucesso, enquanto o Facebook demonstra não estar acessível.

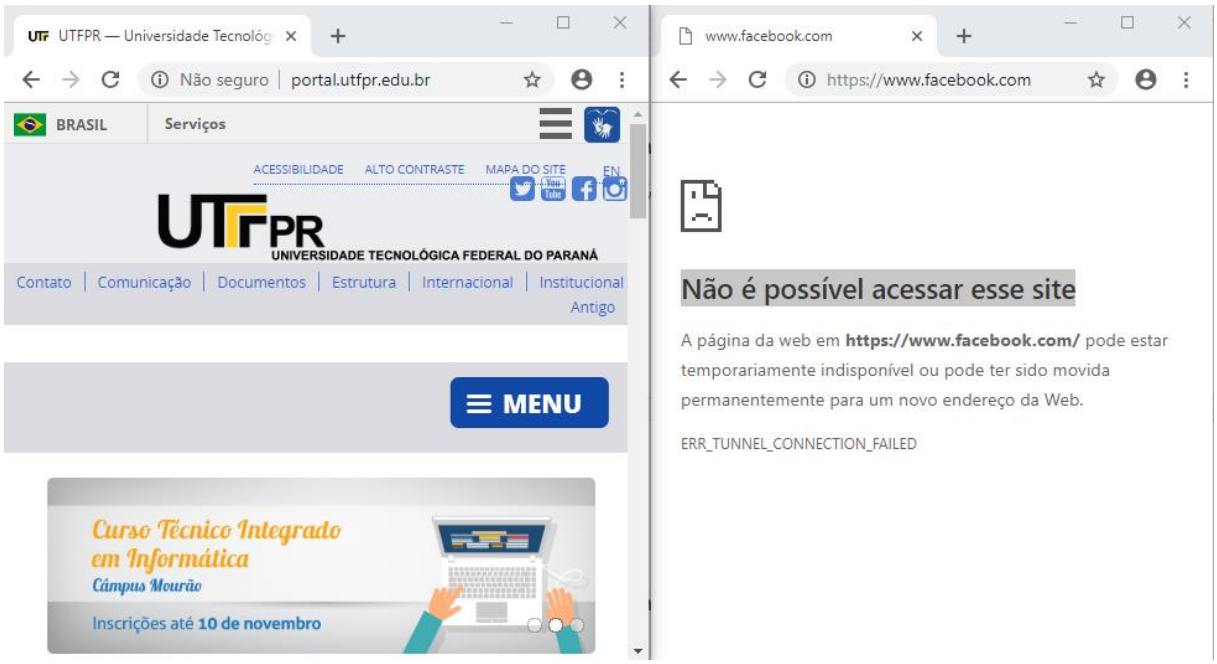


Figura 20 – Site da UTFPR funcional, enquanto o Facebook é bloqueado
Fonte: Autoria própria (2018)

Para validação também do *FailOver* possível no pfSense, foi realizada as tratativas no sistema para o funcionamento desta técnica. O pfSense possibilita a criação de grupos de *Gateway*, onde são apontados os *Gateways* de maior prioridade, bem como o gatilho que fará

o disparo da ação de troca de *link*, podendo ser um membro *off-line*, perda de pacotes, alta latência ou os dois últimos aliados, como ilustra a Figura 21.

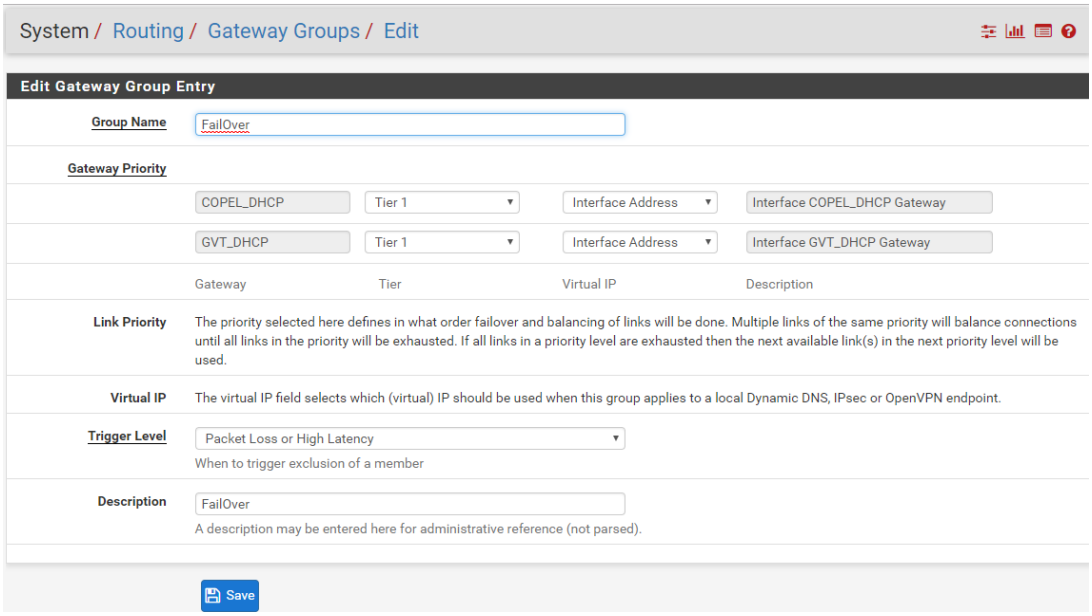


Figura 21 – Adicionando um grupo de *Gateway*
Fonte: Autoria própria (2018)

Aliado a prioridade de *Gateway*, há necessidade de informar o peso do *Gateway* na interface de rede (Figura 22), para que o pfSense possa administrar qual será *link* principal e o backup. No cenário de testes, o *link* da Copel ficou com peso 1, enquanto GVT recebeu o peso 2 (quanto mais próximo a zero, maior o peso).

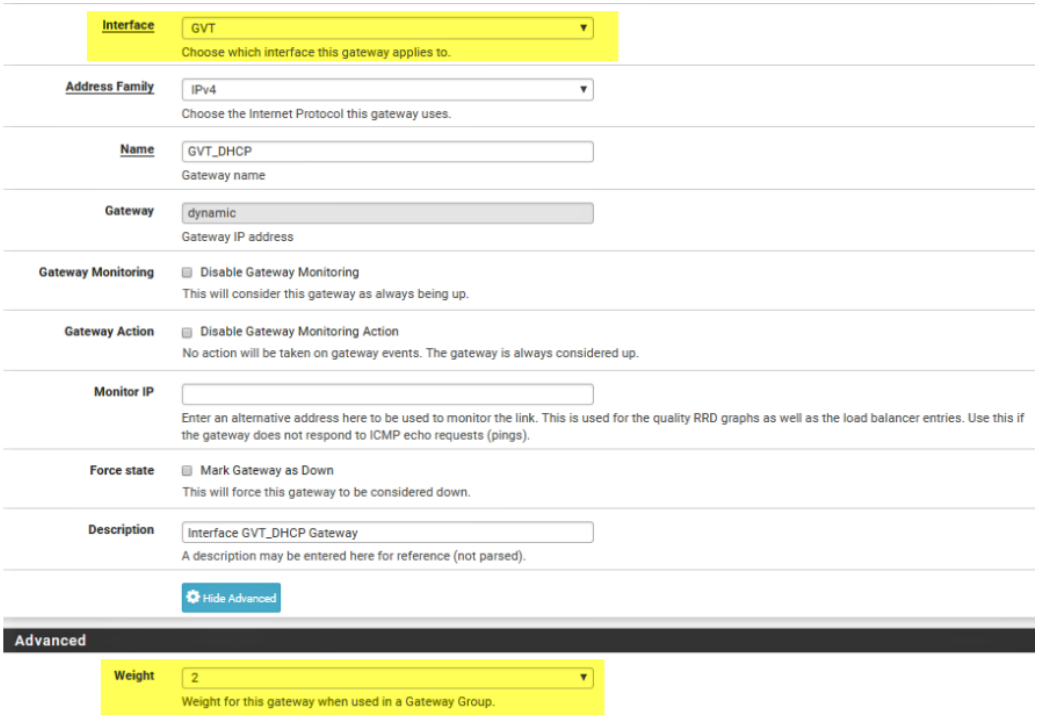


Figura 22 – Informando o peso do *Gateway*
Fonte: Autoria própria (2018)

Para finalizar, basta indicar que o *Gateway* padrão que será utilizado, é o grupo que foi acabado de criar, denominado neste caso *FailOver*, conforme Figura 23.

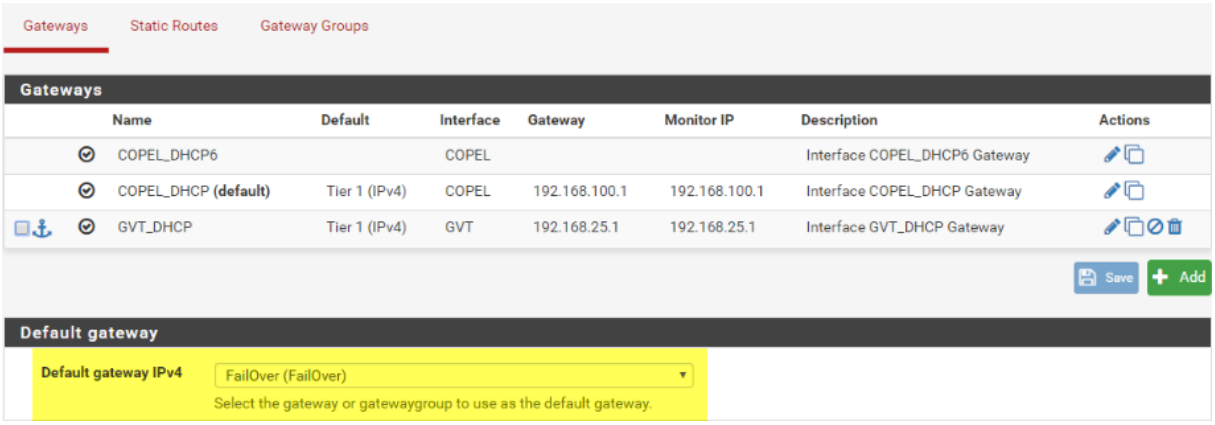


Figura 23 – Apontando o *Gateway* padrão
Fonte: Autoria própria (2018)

Concluída estas etapas, foi possível realizar o laboratório de teste, fazendo com que o *link* da Copel (primário), que estava em correto funcionamento, fosse desativado (através da remoção do cabo de rede) e a navegação em poucos segundos passou a ser realizada através da GVT. Passados alguns minutos, foi reestabelecida a conexão da Copel, fazendo com que os serviços voltassem a operar pelo canal principal, podendo ser comprovado pela Figura 24.

Seu Histórico de IPs e Provedores		
Dia - Hora	seu IP	Provedor
09/11/18 - 10:13:44	138.204.26.160	COPELFIBRA
09/11/18 - 10:08:28	.29	GVT
09/11/18 - 10:07:44	138.204.26.160	COPELFIBRA

Figura 24 – Consulta de histórico de Provedores
Fonte: Autoria própria (2018)

Mesmo após as configurações dos serviços de rede anteriormente demonstrados, o servidor que tem configurações consideradas básicas atualmente, apresenta uma utilização baixa dos recursos, o que viabiliza a implementação do pfSense, com um baixo custo para isto. A Figura 25, corrobora esta informação:

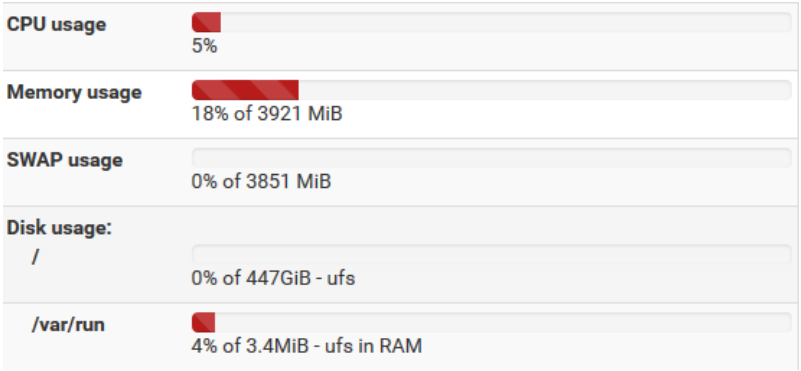


Figura 25 – Utilização dos recursos do servidor pfSense
Fonte: Autoria própria (2018)

5.2 TESTES COM ENDIAN FIREWALL – VERSÃO 3.2.4

Para obtenção da distribuição do Endian Firewall, é necessário ir até a página da fabricante. No momento do início dos testes, a versão mais atualizada disponível era a EFW-3.2.4. Realizado os procedimentos de preparação de mídia inicializável para instalação do *appliance*, notou-se que este processo também se dá de forma muito simplificada.

Após o término dos processos automáticos, é solicitado ao usuário o fornecimento do IP e máscara de rede da interface "Verde", que é como o Endian trata as redes LAN, visualizado na Figura 26.

Figura 26 – Informando o endereço IP para o Endian Firewall
Fonte: Autoria própria (2018)

Este mesmo IP também dará acesso ao painel administrativo web do Endian, onde é possível realizar as manutenções através de interface gráfica, assim como o pfSense. Informado o IP para a LAN, é exibida algumas informações, como o próprio endereço de gerenciamento, o IP da WAN (conhecida como interface vermelha), ilustrados na Figura 27.

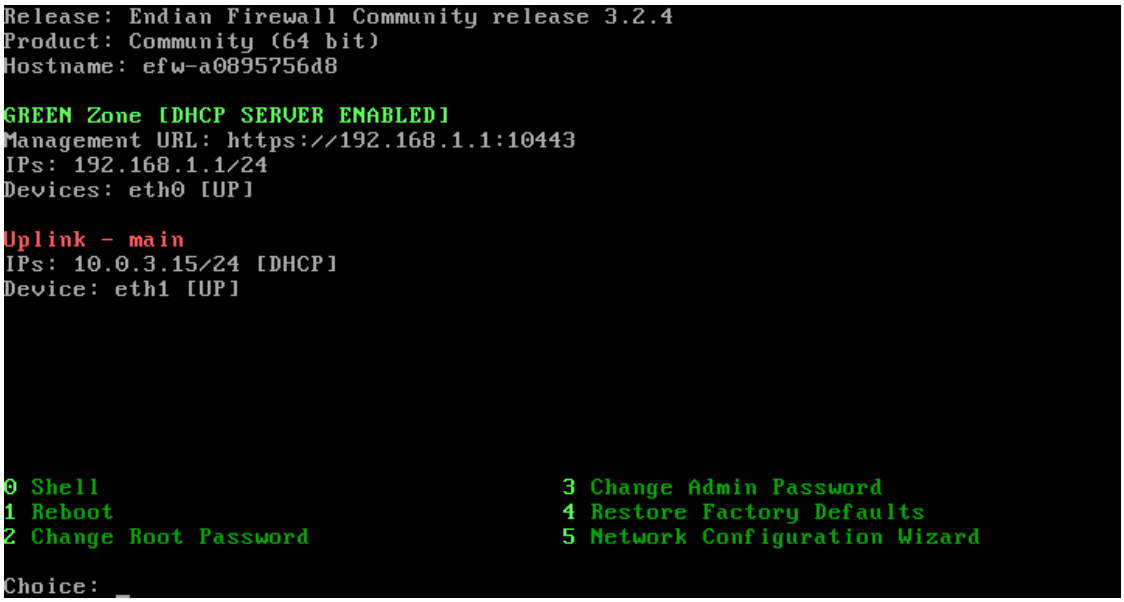


Figura 27 – Informações exibidas pelo Endian Firewall
Fonte: Autoria própria (2018)

No *browser*, após requisitar o endereço de gerenciamento, é solicitado a introdução do login e senha, que por padrão da distribuição, é admin e endian respectivamente. Fornecido os dados, é apresentada a tela inicial com alguns gráficos e informações úteis do sistema, como utilização dos recursos, serviços ativos, dentre outros identificados na Figura 28.

Figura 28 – Página inicial do web configurador do Endian Firewall
Fonte: Autoria própria (2018)

Bem como realizado no pfSense, os mesmos testes aplicaram-se no Endian Firewall. Nesta distribuição, há uma diretiva que habilita a filtragem do tráfego de saída, exemplificado na Figura 29. Habilitando a mesma, todas as portas são bloqueadas, exceto as que estiverem liberadas acima, uma vez que a leitura das regras é realizada de forma *top-down.* Assim, o bloqueio da porta TCP 3389, é realizada naturalmente ao acioná-la.

As portas 443 e 80 também foram bloqueadas (Figura 29), para seguir o modelo de controle de acesso a sites na empresa. Fazendo isso, a navegação fica suspensa, até a configuração do módulo proxy nos próximos passos.

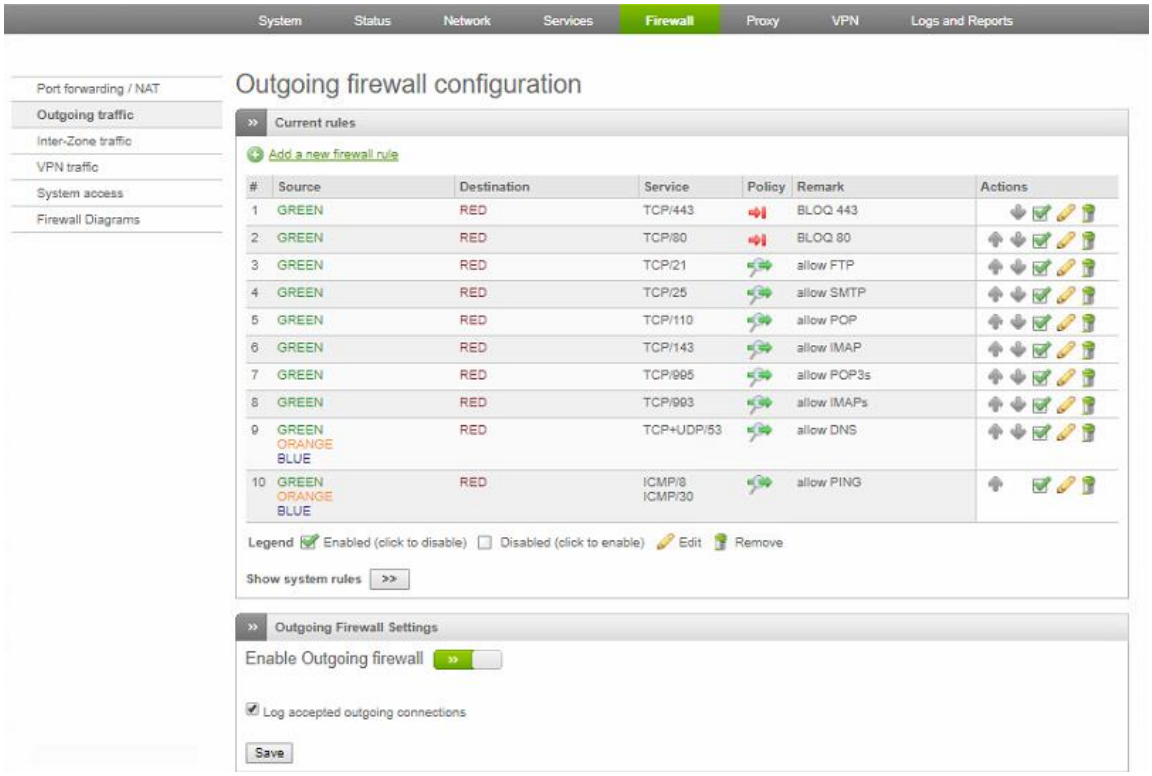


Figura 29 – Habilitando o Firewall de tráfego de saída e bloqueio de portas 80 e 443
Fonte: Autoria própria (2018)

Em sequência, ocorreu a habilitação do módulo Proxy no Endian. Foi informado que a porta que o mesmo responderá é na 3128, ilustrado pela Figura 30.

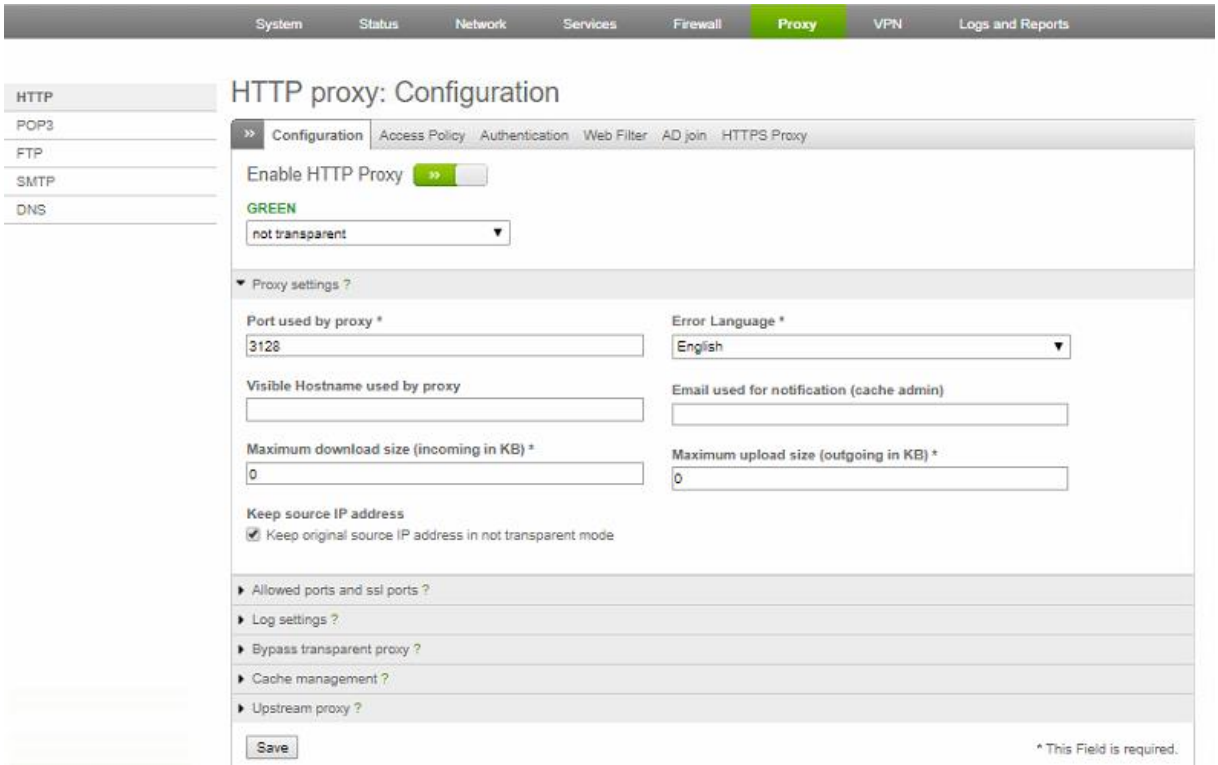


Figura 30 – Habilitando o módulo Proxy do Endian
Fonte: Autoria própria (2018)

Juntamente há esta configuração, realizou-se também a determinação de alguns sites bloqueados, exemplificado pela Figura 31. Essa regra foi incorporada então aos usuários da interface verde (LAN), limitando o acesso aos *sites* definidos.

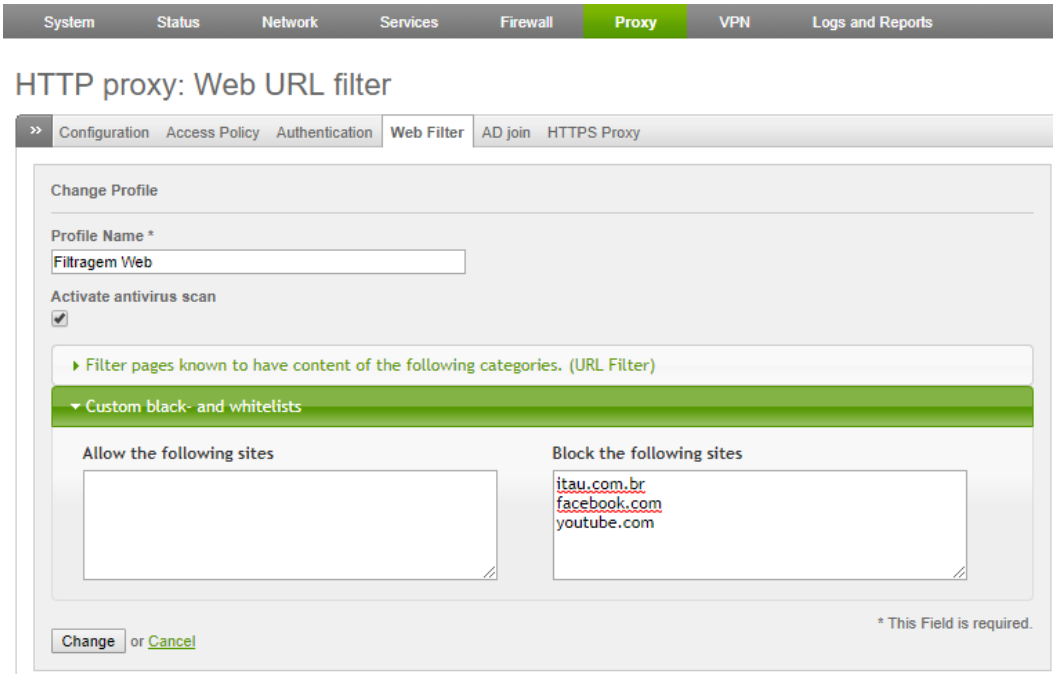


Figura 31 – Definido os sites bloqueados no Endian
Fonte: Autoria própria (2018)

Após a alteração das informações de proxy nas propriedades da Internet (ver Figura 18), a navegação é possível novamente, desde que não seja requisitado alguma página considerada imprópria e listada nos itens bloqueados, como mostra a Figura 32.

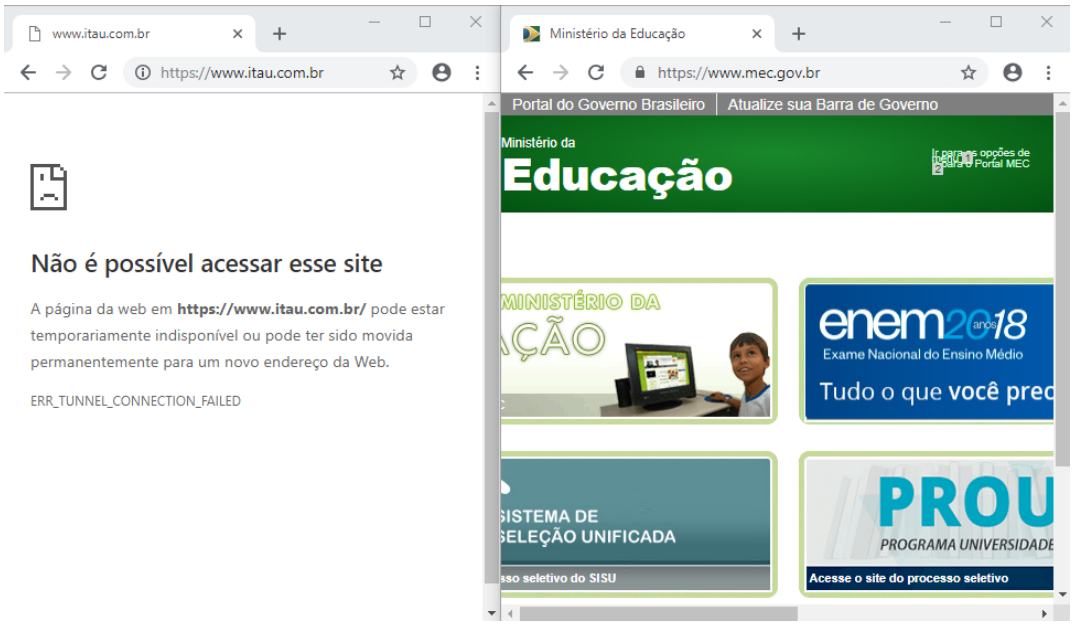


Figura 32 – Tentativa de acesso a sites
Fonte: Autoria própria (2018)

Por fim, realizou-se experiências com o *FailOver* do Endian. Para isso, nos cadastros das interfaces, há uma opção que faz a verificação se um destino é alcançável, configurado pelo utilizador. Caso essa validação não ocorra, o Endian faz a alteração para o *link* que for informado na opção “caso esta conexão falhe, ative determinada placa de rede”, neste caso, GVT, confirmado pela Figura 33.

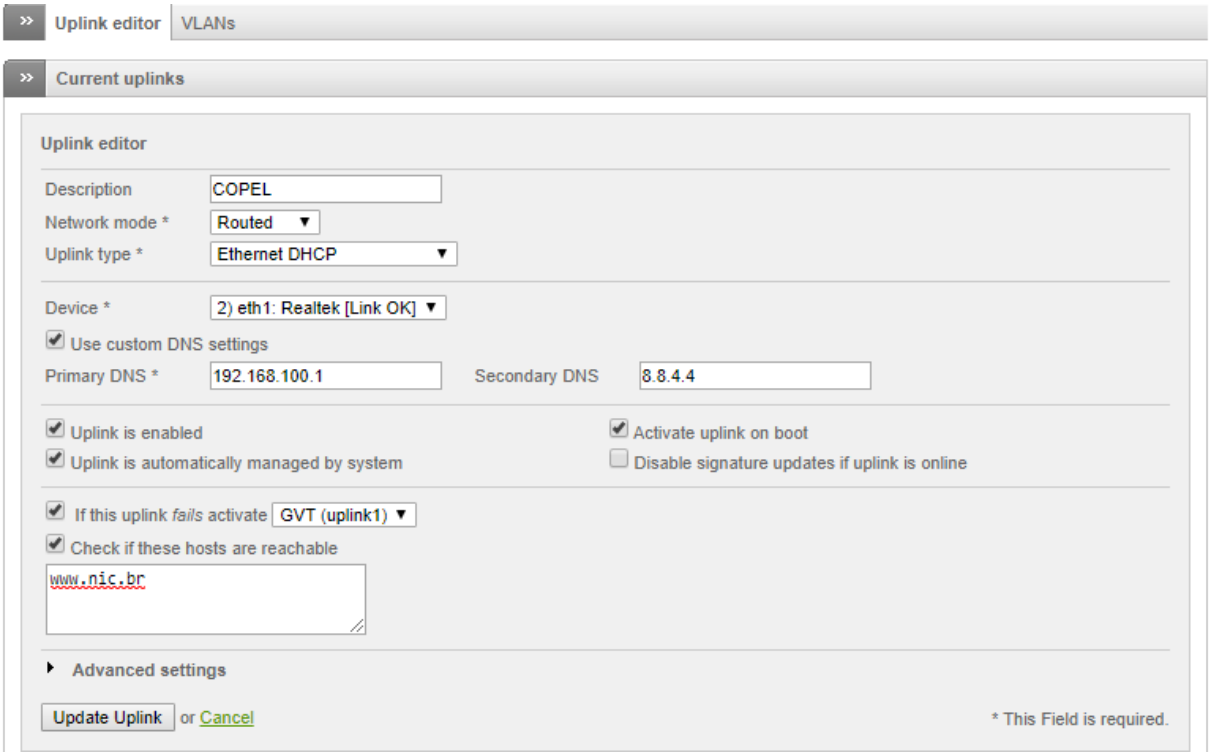


Figura 33 – Configuração de *FailOver* no Endian
Fonte: Autoria própria (2018)

Para comprovação, o mesmo teste do pfSense foi aplicado nesta situação, confirmando o funcionamento da técnica, identificado na Figura 34.

Seu Histórico de IPs e Provedores

Dia - Hora	seu IP	Provedor
10/11/18 - 14:07:04	138.204.26.103	COPELFIBRA
10/11/18 - 14:03:06	.29	GVT
10/11/18 - 14:02:00	138.204.26.103	COPELFIBRA

Figura 34 – Troca de *link* automática realizada pelo Endian
Fonte: Autoria própria (2018)

Após a configuração dos módulos no Endian, ele apresenta um uso pouco superior dos recursos, se comparado ao pfSense, demonstrado pela Figura 35.

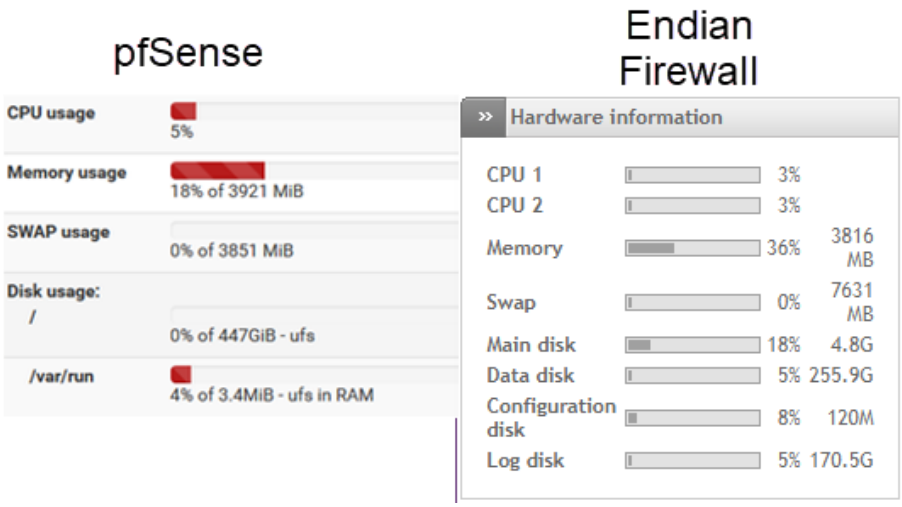


Figura 35 – Comparativo de utilização de recursos entre as distribuições pfSense x Endian
Fonte: Autoria própria (2018)

5.3 IMPLANTAÇÃO DA FERRAMENTA NA EMPRESA

Verificado ambas as distribuições conforme descrito anteriormente, percebeu-se que tanto Endian Firewall como pfSense, demonstram um funcionamento muito bom dos módulos que foram configurados. Bem como, o desempenho da rede se manteve em um nível alto, sem quaisquer percepções de lentidão por haver filtragem de pacotes. De acordo ainda com os gráficos de utilização de recurso, nenhum dos dois tem um consumo excessivo de hardware, conseguindo manter a viabilidade técnica para este projeto.

Assim, a escolha da distribuição (pfSense ou Endian) fica a critério de cada usuário que um dia possa se utilizar delas em futuras implementações, sendo neste projeto, adotado o Endian, observado a coleta de estatísticas e logs de maneira mais rápida e clara.

Dessa forma, se deu o início da implantação do Firewall, em uma rede SOHO que obedece a uma topologia que pode ser consultada na Figura 36. Todo o tráfego da rede passará pelo Firewall, propiciando assim, um controle maior dos pacotes que entram e saem da rede local.

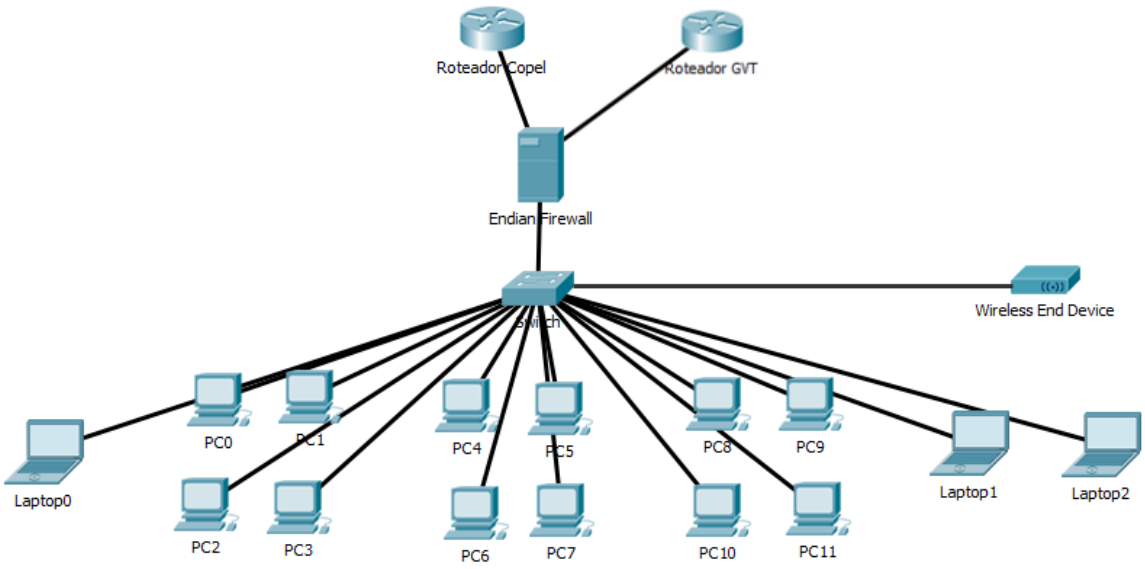


Figura 36 – Topologia da Rede SOHO de implantação do Firewall
Fonte: Autoria própria (2018)

Primeiramente, habilitou-se no Endian a realização da filtragem do tráfego de saída, para que se tenha controle do que será permitido transpor o Firewall, em sentido a WAN. Logo após, iniciou-se a configuração das regras de Firewall já conhecidas pelo setor de tecnologia, como portas de acesso remoto ao sistema gerencial, e-mail, e também foram aplicadas as mesmas regras de bloqueio para as portas 80 e 443 dos laboratórios de testes, obrigando aos usuários utilizarem-se das configurações de Proxy para obterem acesso à Internet.

No ambiente real, há algumas ressalvas no bloqueio das portas de navegação HTTP e HTTPS, onde por exemplo, a direção deve ter acesso ilimitado a Internet, sem nenhuma restrição. Para atender essa demanda, uma das maneiras possíveis, é criar regras no Firewall, que permitam acesso total a qualquer destino, dispositivos que tenham o endereço MAC associados a esta mesma regra, conforme Figura 37. Um detalhe que se deve observar, é que esta regra deve ir acima das regras de bloqueio, pois como já explicado, a leitura das definições ocorre de forma *top-down.*

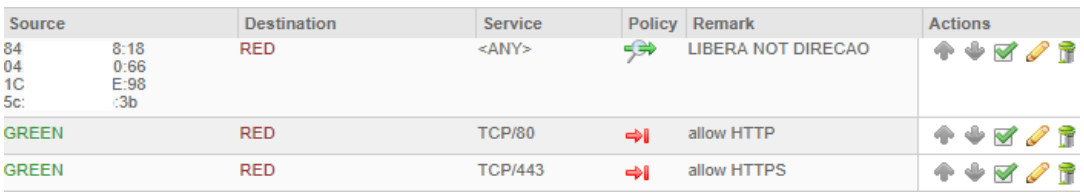


Figura 37 – MAC de origem sendo liberado no Endian Firewall
Fonte: Autoria própria (2018)

Os ajustes de proxy tornam-se semelhantes, alguns usuários do comercial precisam ter acesso ao WhatsApp Web para atendimento de clientes, enquanto os demais funcionários não podem conseguir acessá-lo. O Endian permite, a criação dos filtros web, como já mostrado na seção de testes, colocar domínios em bloqueio ou permissão. Assim, é necessário apenas associar a regra que libera o domínio, também associada aos MACs que deverão ter acesso, como pode-se observar na Figura 38.

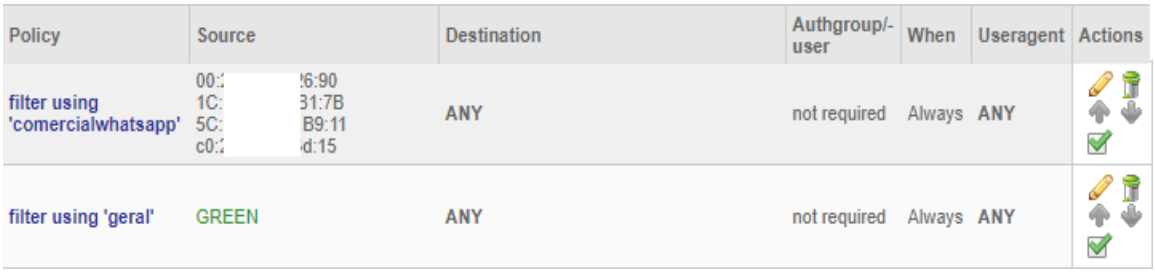


Figura 38 – Política comercialwhatsapp permitindo os MACs liberados no campo *Source*
Fonte: Autoria própria (2018)

Um grande facilitador no Endian para bloqueios de sites, é um filtro de páginas distribuídos em diversas categorias, que recebem atualização frequentemente (Figura 39). Assim, é possível realizar o bloqueio facilmente de grupos de páginas consideradas de acesso inadequado em ambiente de trabalho, aliando também os bloqueios personalizados que o utilizador mesmo pode efetuar.

Figura 39 – Categorias disponíveis para bloqueio no módulo Proxy do Endian
Fonte: Autoria própria (2018)

Como a empresa escolhida utiliza um sistema em nuvem, após as primeiras liberações no Firewall que foram repassadas pelo departamento de tecnologia, a implantação da ferramenta se encaminhou muito bem. Porém, mesmo assim, alguns softwares locais utilizados na empresa, tiveram seu funcionamento afetado, sendo necessário a investigação para identificação do problema que estava ocorrendo.

Um exemplo ocorrido foi com o software da Receita ValidaPR 5.2, que é utilizado pelos contribuintes para remeter informações da totalidade de suas operações a SEFA/PR. Ao tentar fazer o envio dos arquivos, o software dizia não ser possível comunicação com o servidor. Para essas situações, é possível utilizar-se dos *logs* em tempo real do Endian, que mostram estatísticas das conexões. A Figura 40, mostra que ao tentar comunicar com o servidor da receita na porta 22, houve o bloqueio do pacote, sendo necessário ajuste deste IP e porta nas regras do Firewall para correto funcionamento. Neste caso, o *site* da receita informa através de qual porta o arquivo será transmitido, mas em várias ocasiões, será necessário usar este recurso para conseguir ajustar o funcionamento dos sistemas.

Figura 40 – Monitorando o Endian Firewall
Fonte: Autoria própria (2018)

Em consulta ao *site* da Receita confirma a informação observada nos *logs*, na Figura 41.

Figura 41 – Instruções de instalação do ValidaPR
Fonte: Secretaria da Fazenda (2018)

Na empresa onde o Endian foi implantando, também há alguns serviços internos que devem ficar disponíveis para as filiais, como chat, acesso remoto a câmeras, dentre mais alguns. Da mesma forma que são definidas regras de saída, para estes casos devem ser instauradas regras de entrada, possibilitado também pela técnica de NAT (protocolo que faz a tradução dos endereços IPs e portas TCP da rede local para Internet), para que os serviços continuassem operantes e acessíveis para os interessados. Conforme a Figura 42, é possível ver essas regras determinas no Firewall.

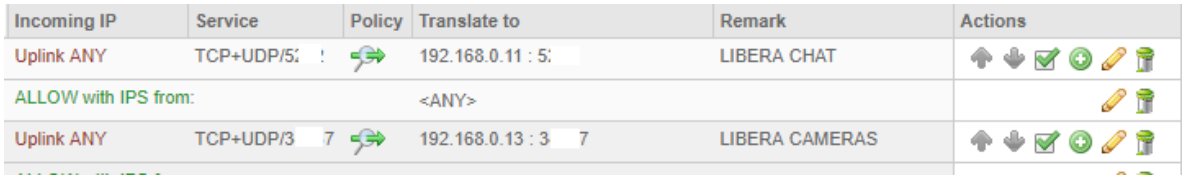


Figura 42 – Regras de entrada definidas no Firewall
Fonte: Autoria própria (2018)

Também foi utilizado o serviço de DHCP provido pelo Endian, para entrega de endereços automaticamente para os dispositivos da rede. Nas configurações, habilitou-se o servidor DHCP para a interface verde, informando os principais atributos para a funcionalidade do serviço, como intervalo de endereços disponíveis, *gateway*, servidor de DNS primário e secundário, expresso na Figura 43.

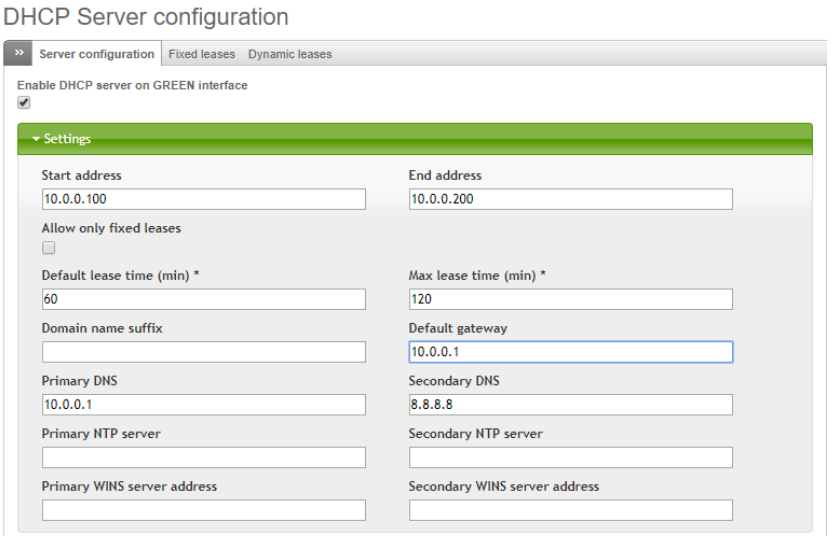


Figura 43 – Definições para o servidor DHCP
Fonte: Autoria própria (2018)

Com os principais serviços configurados para correto funcionamento e melhor desempenho, foram efetuas alguns outros ajustes de monitoramento do servidor. O primeiro deles, adicionar notificações por e-mail de determinadas ações que acontecem com o servidor, como exemplo, desligamentos, indisponibilidade de *links*, conexão via SSH, visualizados na Figura 44.

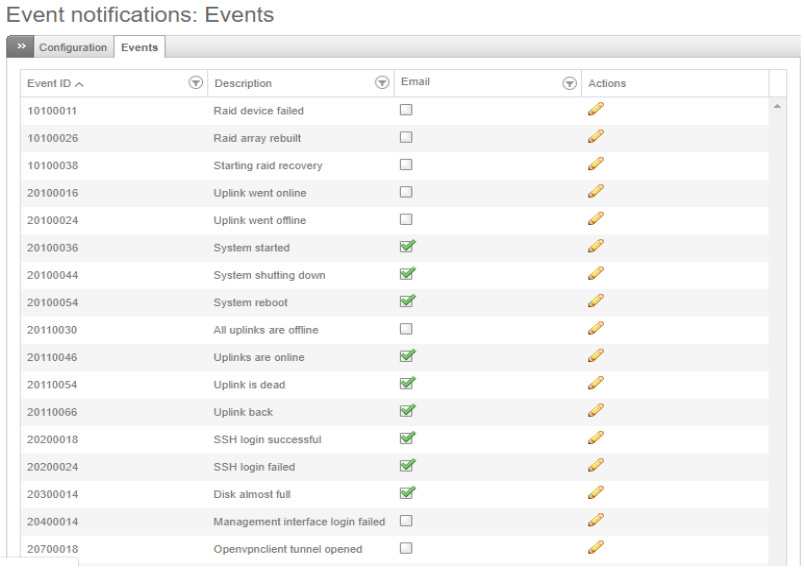


Figura 44 – Definições para notificações de eventos
Fonte: Autoria própria (2018)

Outro serviço muito interessante fornecido pelo Endian, é o monitoramento de tráfego através do ntopng, uma ferramenta que é capaz de analisar os pacotes que trafegam na rede, listar e ordenar o tráfego de acordo com os protocolos, expor estatísticas de tráfego, exibir a distribuição do tráfego IP entre vários protocolos da camada de aplicação (FERRARI, 2008). Ele é capaz de gerar gráficos destas informações coletadas, exemplificado pela Figura 45.

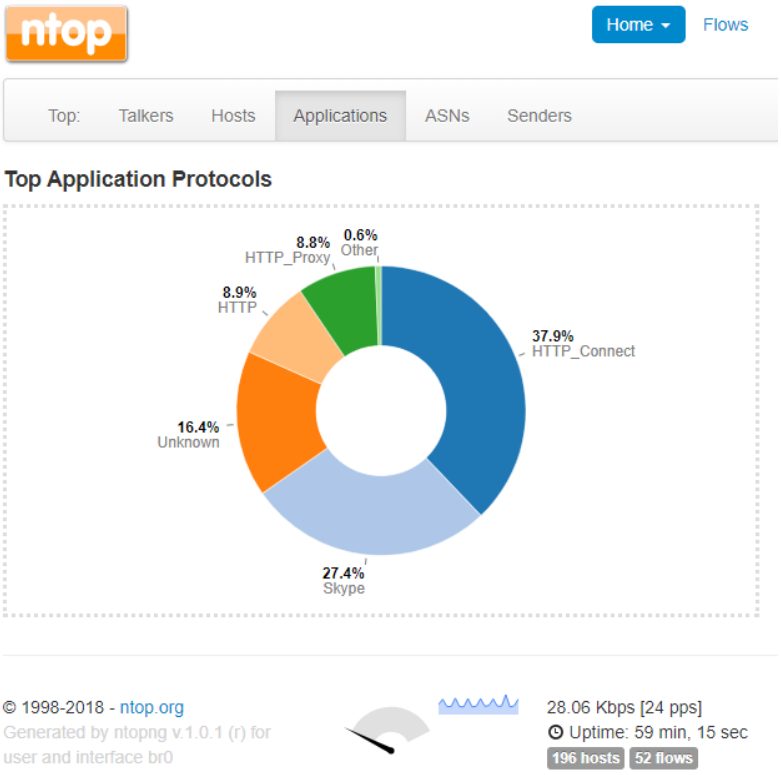


Figura 45 – Exemplo de gráfico gerado pelo ntop
Fonte: Autoria própria (2018)

O *FailOver* também foi definido na versão em produção, exatamente da mesma forma como demonstrado na sessão de testes com o Endian.

Para finalizar, após todas as modificações, foi implementada uma rotina de backup (Figura 46), que faz o envio diário das configurações do Endian para o e-mail do utilizador, a fim de prevenir perda de informações por quaisquer problemas de hardware que possam vir a ocorrer, garantindo assim a rápida restauração se um dia necessário.

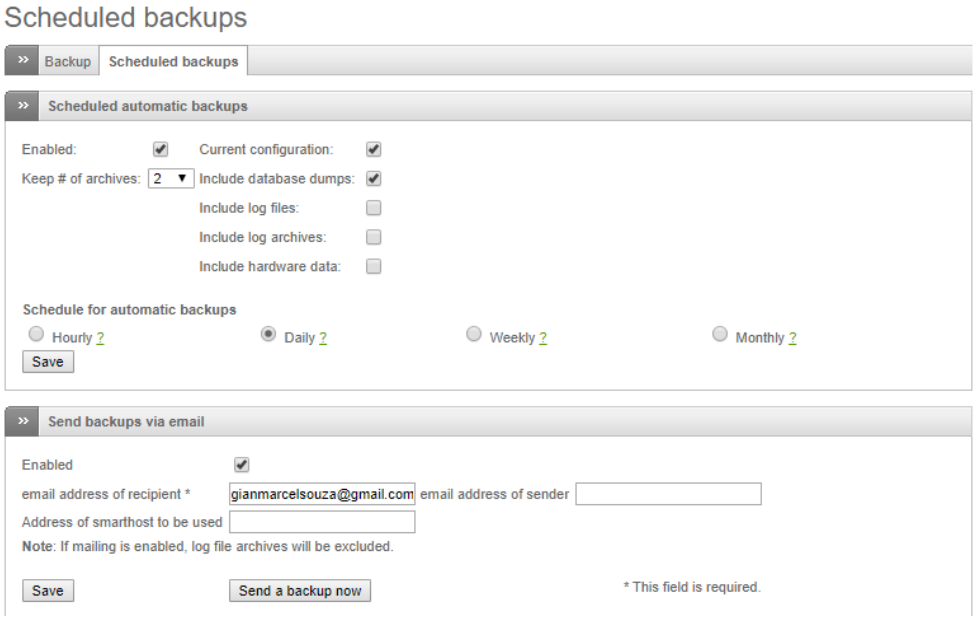


Figura 46 – Agendamento do envio de backups diários
Fonte: Autoria própria (2018)

6 CONCLUSÕES

Durante a realização do trabalho, foi possível perceber como a Segurança da Informação passou a ser fundamental. Os serviços ofertados hoje pela tecnologia, propiciam as empresas e usuários maior agilidade em diversos aspectos, seja na tomada de decisões, na captação de informações para gerir corretamente os negócios, funcionamento de sistemas gerenciais completos de organizações, dentre outros. Possíveis paradas destes serviços por ataques, resultam em perda de tempo, e por consequência, perda de dinheiro.

Uma das técnicas que se pode empregar para amenizar o risco de ataques cibernéticos, é o emprego de Firewalls, que foi estudo de caso e implantação durante este projeto. Analisou-se duas distribuições gratuitas desta ferramenta, para aplicação em uma rede SOHO de uma empresa. A implantação deveria se caracterizar, no momento, por um baixo custo de instauração do serviço, mas sem deixar de prezar qualidade e segurança.

Desta forma, foram examinados dois *appliances* gratuitos de Firewall, muito conhecidos e renomados na comunidade de Tecnologia da Informação, sendo eles pfSense e Endian Firewall. Durante os testes, pode-se perceber o funcionamento muito bom de ambas as distribuições, provendo segurança e serviços adicionais interessantes para gerência de redes locais, neste caso, optando-se pela instalação do Endian.

A implementação de uma nova ferramenta que afeta os usuários, sempre gera um pouco de desgaste inicialmente. Porém, isso em nenhum momento chegou a ser um empecilho da continuação do projeto, uma vez que os problemas foram verificados e solucionados de forma relativamente rápida, causando um mínimo impacto nas atividades dos demais colaboradores da instituição. Verificações de bloqueios/liberações serão contínuas, originadas de novas necessidades que possam aparecer aos usuários.

Como apresentado durante o trabalho, as UTMs apresentam inúmeras funcionalidades, além da segurança provida pelo Firewall. Como trabalhos futuros, é de interesse do departamento de Tecnologia da Informação, a configuração das demais aplicações disponíveis no Endian Firewall, como a utilização do serviço de *Virtual Private Network* (VPN), que possibilitará uma comunicação mais segura entre matriz e filiais da empresa. Há também, o módulo de prevenção a intrusões, que ainda precisa ser estudado e analisado, que proverá ainda mais segurança à rede local, aliado ao uso de Firewall já implementado. Outra técnica que poderá ser empregada, é a utilização de balanceamento de cargas, que possibilitará o uso de ambos os *links* ao mesmo tempo, por exemplo.

Por fim, de maneira geral, a implementação do Firewall obteve êxito e trouxe significativas melhorias para a empresa. Além de propiciar um melhor gerenciamento dos *links* de Internet disponíveis, com o monitoramento e as restrições de acesso realizadas, proporcionou principalmente, segurança reforçada contra ameaças que se alastram de forma intermitente no mundo virtual.

REFERÊNCIAS

ALECRIM, Emerson. **O que é firewall? Conceito, tipos e arquiteturas.** Disponível em: <https://www.infowester.com/firewall.php>. Acesso em: 03 set. 2018.

BENETTI, Ticiano. **Segurança da informação – confidencialidade, integridade e disponibilidade (CID).** Disponível em: <https://www.profissionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/>. Acesso em: 15 ago. 2018.

BÔAS, Bruno Villas. **IBGE: em meio à crise, vendas pela internet crescem e somam R$ 44 bi.** Disponível em: <https://www.valor.com.br/brasil/5624881/ibge-em-meio-crise-vendas-pela-internet-crescem-e-somam-r-44-bi>. Acesso em: 20 ago. 2018.

BRASIL, Agência. **Transações financeiras por aplicativos cresceram 70% em 2017, diz Febraban.** Disponível em: <https://economia.uol.com.br/noticias/redacao/2018/05/03/transacoes-financeiras-por-aplicativos-cresceram-70-em-2017-diz-febraban.htm>. Acesso em: 25 ago. 2018.

BRODBECK, Cassio. **Firewall corporativo, entenda a real importância para seu negócio.** Disponível em <https://ostec.blog/seguranca-perimetro/firewall-corporativo-importancia-negocio>. Acesso em: 08 ago. 2018.

CERT.br. **Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil.** Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em 07 set. 2018.

DELFINO, Pedro. **pfSense – principais vantagens e recursos dessa poderosa ferramenta de firewall.** Disponível em: <https://e-tinet.com/linux/pfsense-vantagens/>. Acesso em: 02 set. 2018.

DUARTE, Otto Carlos Muniz Bandeira. **Possíveis Ataques.** Disponível em: <https://www.gta.ufrj.br/grad/12_1/seg_smartgrid/possiveisataques.html>. Acesso em: 05 set. 2018.

ENDIAN. **History and Milestones.** Disponível em: <https://www.endian.com/company/history/>. Acesso em: 26 ago. 2018.

FERRARI, Sandro Roberto. **NTOP – Configurações gerais.** Disponível em <https://www.vivaolinux.com.br/artigo/NTop-Configuracoes-gerais>. Acesso em 10 nov. 2018.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Porto Alegre: Bookman, 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem top-down. 3 ed., São Paulo: Pearson Addison Wesley, 2006.

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

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

PFSENSE. **Take a tour of pfSense.** Disponível em: <https://www.pfsense.org/about-pfsense/>. Acesso em: 29 ago. 2018.

PORTAL GSTI. **O que são Redes de Computadores?** Disponível em <https://www.portalgsti.com.br/redes-de-computadores/sobre/>. Acesso em: 10 ago. 2018.

ROSSETTI, Adroaldo; MORALES, Aran Bey. **O papel da tecnologia da informação na gestão do conhecimento.** Disponível em: < http://revista.ibict.br/ciinf/article/view/1191/1362>. Acesso em 14 set. 2018.

SECRETARIA DA FAZENDA. **Processamento de Dados – Arquivos Magnéticos – ValidaPR.** Disponível em: < http://www.fazenda.pr.gov.br/modules/conteudo/conteudo.php?conteudo=209>. Acesso em: 10 nov. 2018.

SOARES, Luiz Fernando Gomes; Lemos, Guido; Colcher, Sérgio. **Redes de computadores: das LANs, MANs e WANs às redes ATM.** Rio de Janeiro: Elsevier, 1995.

STALLINGS, W. **Criptografia e segurança de redes:** Princípios e práticas. 4 ed., São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, Andrew S. **Redes de computadores.** Rio de Janeiro: Elsevier, 2003.

VIRTUALONE. **Endian Firewall Enterprise.** Disponível em: <http://www.virtualone.com.br/solucoes-servicos/endian-firewall/>. Acesso em: 26 ago. 2018.