CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA
REDES DE COMPUTADORES

ALECSANDRO JOSÉ DE ANDRADE
ANDRIO GONÇALVES CAMPOS
WALLISSON FRANCISCO DOS SANTOS

ESTUDO COMPARATIVO DE SOLUÇÕES CORPORATIVAS DE FIREWALL: SOFTWARE LIVRE E SOFTWARE PROPRIETARIO.

RECIFE
2020

ALECSANDRO JOSÉ DE ANDRADE
ANDRIO GONÇALVES CAMPOS
WALLISSON FRANCISCO DOS SANTOS

ESTUDO COMPARATIVO DE SOLUÇÕES CORPORATIVAS DE FIREWALL: SOFTWARE LIVRE E SOFTWARE PROPRIETARIO.

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo e Redes de Computadores.

Professor(a) Orientador(a): Mestre Ameliara Freire Santos de Miranda

RECIFE
2020

ALECSANDRO JOSÉ DE ANDRADE
ANDRIO GONÇALVES CAMPOS
WALLISSON FRANCSICO DOS SANTOS

ESTUDO COMPARATIVO DE SOLUÇÕES CORPORATIVAS DE FIREWALL: SOFTWARE LIVRE E SOFTWARE PROPRIETARIO.

Artigo aprovado como requisito parcial para obtenção do título de Tecnólogo em Rede de Computadores, pelo Centro Universitário Brasileiro - UNIBRA, por uma comissão examinadora formada pelos seguintes professores.

Ameliara Freire S. de Miranda

Prof.ª Mestre Ameliara Freire Santos de Miranda

Professor(a) Orientador(a)

Humberto C. Cardoso da Silva

Prof.º Doutor Humberto Caetano Cardoso da Silva

Professor(a) Examinador(a)

Diego Ribeiro Gomes

Prof.º Especialista Diego Ribeiro Gomes

Professor(a) Examinador(a)

Recife, 15/12/2020

NOTA: 9,0

“Nada grandioso entra nas vidas dos mortais sem uma maldição.”

Sófocles

RESUMO

O isolamento social fez com que a adesão ao trabalho remoto tomasse proporções não esperadas para os dias atuais. Adaptar rapidamente a essa mudança na forma de trabalho torna-se imprescindível. Os *cybers* ataques tornam-se cada dia mais comuns, trazendo não apenas prejuízo, como também a má reputação, ninguém vai confiar informações pessoais a uma empresa que teve dados vazados na internet. Encontrar meios de defesa para ataques cibernéticos é dever dos gestores e empresários, pessoas mal intencionadas estão em todos os lugares, procurando brechas ou falhas de segurança, fazem uso dessas falhas para obter de forma não autorizada informações sigilosas, tanto de pessoas comuns, quanto de corporações. O *firewall* é uma importante ferramenta de segurança dentro do ambiente corporativo e a escolha de uma tecnologia capaz de prover os recursos de rede e segurança é vital para manter a integridade, disponibilidade e confidencialidade dos dados. Este trabalho consiste no desenvolvimento de um estudo comparativo entre duas soluções de *firewalls* presentes atualmente no mercado para proteção de redes de computadores, o *firewall software* proprietário e o *software* livre.

Palavras-chaves: *Firewall*, Segurança, *software* livre e *software* proprietário.

ABSTRACT

Social isolation meant that adherence to remote work took on unexpected proportions today. Adapting quickly to this change in the way of working becomes essential. Cyber attacks are becoming more and more common, causing not only damage, but also a bad reputation, no one will entrust personal information to a company that had leaked data on the internet. Finding means of defense for cyber attacks is the duty of managers and entrepreneurs, malicious people are everywhere, looking for loopholes or security breaches, make use of these breaches to obtain unauthorized confidential information, both from ordinary people and corporations. The firewall is an important security tool within the corporate environment and the choice of a technology capable of providing the network and security resources is vital to maintain the integrity, availability and confidentiality of the data. This work consists of the development of a comparative study between two firewall solutions currently on the market to protect computer networks, the proprietary software firewall and free software.

Keywords: Firewall, Security, free software and proprietary software.

SUMÁRIO

1 INTRODUÇÃO

Observando o contexto da pandemia causada pelo Sars-CoV-2 (Covid-19), percebe-se que houve uma adesão significativa ao trabalho remoto dentro da configuração de home office no Brasil e no mundo, em um grande movimento de respeito às diretrizes de isolamento social, a colunista Futema (2020) do web site uol publicou “... o home office poderá ser o novo normal para sempre. O CEO do Twitter, Jack Dorsey, disse que os funcionários que desejarem poderão trabalhar em casa para sempre ...”.

Contudo gestores e empresário precisam tomar cuidado com a segurança das informações que estão indo para casa dos seus colaboradores, e esse é um dos maiores desafios enfrentados pelas empresas. Muitas organizações ainda não se atentaram ao fato de que seus dados podem estar em risco, segundo estudo da empresa de segurança da informação *Kaspersky*, houve um crescimento de 148% no número de ataques contra empresas em março, somando aproximadamente 1,6 bilhão de ataques cibernéticos no primeiro trimestre deste ano. E a tendência é que esse número cresça, visto que as informações corporativas estão sendo cada vez mais acessadas e compartilhadas de diferentes lugares. *Softwares* de antivírus não são suficientes para garantir a proteção dos dados corporativos. É preciso implementar políticas de segurança da informação (PSI), com o objetivo de minimizar riscos de perdas ou violação de quaisquer ativos da Rede. Combinada com tecnologias capazes de assegurar o perímetro onde as informações se encontram, como proteção contra *ransomware*. O *firewall* em conjunto com políticas de segurança da informação (PSI) é a melhor maneira de evitar vazamentos, roubos e sequestros de dados e acessos indevidos. (NACIF, 2020)

Firewall é um dispositivo ou um *software* ou os dois que funciona impondo política de controle de acesso entre duas redes, permitindo ou negando as transmissões de uma rede à outra. Um uso típico é como dispositivo de segurança para evitar que os intrusos possam acessar uma informação confidencial. Pode-se dizer, ainda que *firewall* é um componente ou um conjunto deles, que atua entre uma ou mais redes, por onde passa todo o tráfego, examina-se a comunicação que está entrando ou saindo, e dependendo da sua direção pode permiti-la ou não, sendo um dos elementos mais importantes e conhecidos em ambientes de computadores, a utilização dele na rede pode trazer importantes benefícios, como por exemplo,

proteção a serviços, acesso controlado, privacidade aumentada, logs de acessos e cumprimento das políticas de segurança da informação. (MOREIRA, 2011)

Atualmente pode-se encontrar no mercado diversas tecnologias de *firewall* e a escolha da melhor solução não é simples, pois deve ser levado em consideração vários fatores, tais como: suporte, profissionais capacitados na região onde a empresa fica localizada e custo. Segundo os autores Stallings e Brown (2013) "O *firewall*, assim provê uma camada de defesa adicional, isolando sistemas internos de redes externas. Isso segue a clássica doutrina militar da "defesa intensa" ...", dentre as tecnologias de *firewall* temos as opções comerciais e as não comerciais que são encontradas com licença de *software* livre. Abordaremos os critérios necessário que um *firewall* deve ter para ser usado como solução corporativa.

1.1 JUSTIFICATIVA

A reflexão acerca da efetividade do processo de segurança da informação, dentro do ambiente corporativo, a segurança é fundamental análoga à escolha de uma boa solução de *firewall*, hoje a tecnologia evolui a um ritmo exponencial, segundo Moraes (2015) pág. 10, "... os processos que desenvolvíamos de modo manual alguns anos atrás foram automatizados por algum sistema ou alguma aplicação. As empresas estão cada dia mais dependentes de processos de tecnologia da informação ...", e manter os sistemas seguro, é de urgente e extrema importância.

Mesmo hoje, em 2020, os casos de ataques cibernéticos são cada vez mais comuns, dados estatísticos retirados do site Convergência Digital (2020) mostra que "A maior parte das organizações brasileiras (96%) sofreu um ataque cibernético que afetou o negócio nos últimos 12 meses, segundo executivos de negócios e de segurança.". Essa realidade decorre de diversos fatores e ineficiência das ferramentas processuais para combater a invasão e apropriação sem autorização de dados. Essas dificuldades resultam em grande prejuízo para as organizações/corporações.

Com o objetivo de atrair atenção para o tema, o trabalho faz um estudo comparativo de soluções de *firewall*: *software* livre e *software* proprietário. Com intuito de esclarecer e desmitificar o software livre para analista, gestores e empresários, ao mesmo tempo que demostra com casos reais de uso, adquirir um *firewall* vai além, fatores tais como: preço, suporte, garantia e tempo de resolução de falhas devem ser levados em consideração.

1.2 OBJETIVO GERAL

Fazer um estudo comparativo de tipos de *firewall* entre as soluções *software* livre e código fonte fechado.

1.3 OBJETIVOS ESPECIFICOS

- Apresentar os conceitos básicos de *software* livre.
- Descrever a evolução das ferramentas de *firewalls* até os dias atuais.
- Analisar os requisitos necessários de uma ferramenta de firewall para uso corporativo.
- Comparar as soluções de *software* livre e *software* proprietário.

2 REFERENCIAL TEÓRICO

2.1 *SOFTWARE* LIVRE

O movimento *software* livre é em prol do compartilhamento do conhecimento tecnológico, tem seu início no ano de 1980 e se difundiu pelo mundo através da rede mundial de computadores à internet. Seus apoiadores são acadêmicos, cientistas, dentre outros. (SILVEIRA, 2004)

O software livre conta com uma grande comunidade de desenvolvimento espalhada por todo mundo, estima-se que cerca de 100 mil programadores e gerentes de projetos façam parte dessa comunidade, trabalhando voluntariamente para o crescimento do movimento. Empresas como IBM e Hewlet-Packard passaram a desenvolver *softwares* com o objetivo de serem distribuído livremente, bem como serviços para usuários de software livre. (A HEXSEL, 2002)

O *software* livre deve ser entendido como um software que respeita a liberdade e o senso de comunidade dos usuários, significa que possui a liberdade de ser executado, copiado, distribuído, estudado e até mesmo melhorado. (GNU, 2009-2019)

Hexsel (2002), da Universidade Federal do Paraná, descreve em seu relatório técnico RT-DINF 004/2002, o que é o movimento *software* livre:

> O movimento de publicação de *Software* Livre ganhou notoriedade nos últimos anos. Este modo de produção de software tem resultado em produtos de excelente qualidade e grande penetração em alguns setores do mercado mundial de *software*. A características mais importante do software livre é a liberdade de uso, cópia, modificações e redistribuição. Esta liberdade é conferida pelos autores do programa e é efetivada através da distribuição do código fonte dos programas, o que os transforma em bens públicos, disponíveis para utilização por toda a comunidade e da maneira que seja mais conveniente a cada indivíduo.
>
> A liberdade para usar, copiar, modificar e redistribuir *software* livre lhe confere uma serie enorme de vantagens sobre o *software* proprietário. A mais importante delas é disponibilidade do código fonte, porque isto evita que os usuários se tornem reféns de tecnologias proprietárias. Além desta, as vantagens técnicas são também consideráveis.

As quatro liberdades essenciais que garantem um *software* livre:

- A liberdade de executar como desejar.
- A liberdade de estudar como o programa funciona e poder adaptar.
- A liberdade de poder distribuir copias livremente.

- A liberdade de distribuir copias modificadas do *software*. Para tal acesso ao código-fonte é um pré-requisito.

A *Free Software* Foundation (FSF) fundada em 1985 por Richard Stallman, considerado o pai do *Software* Livre. Stallman é contra *softwares* proprietários, por não permitem alterar seu código fonte. Um dos projetos livre mais conhecido nos dias de hoje, é o projeto GNU, seu kernel foi desenvolvido por Linus Torvalds e Richard Stallman, fazendo parte da gênese do sistema operacional Linux. Foram criadas mais de 30 licenças para garantir o direito de distribuição entre os usuários, a mais usada é a GPL (*General Public License* - Licença Pública de Uso Geral), criada por Richard Stallman. A GPL possui uma regra que restringe a apropriação das modificações, garantindo que alterações feitas no *software* se tornem comum entre todos que o usam. (KUSZKA, 2020)

Software livre é uma alternativa economicamente e financeiramente viável devido ao seu tipo de licenciamento, Reis (2020) descreve em seu artigo na homepage DevMedia “o *software* sendo livre, não significa dizer que seja gratuito, e é válido considerar que o preço não precisa estar embutido apenas no produto em si, uma vez que se pode cobrar por uma modificação do *software* (manutenção) ou sua distribuição.”

2.2 *FIREWALL*

Os *firewalls* são datados da década de 80, foram criados com a finalidade de restringir o acesso entre redes e internet, inicialmente a internet era apenas usada por universidade e militares. Porém com o crescimento do uso doméstico, proteger os dados passou a ser uma necessidade **TECNOLOGIA DE *FIREWALL***. (COSTA, 2020)

Tanenbaum (2011) pág. 583, faz uma comparação alegórica para explicar o que é um firewall de forma simples:

> Os *firewalls* são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. Nas redes, é possível usar o mesmo artifício: uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou de entrada da empresa é feito através de uma ponte levadiça eletrônica (*firewall*).

Segundo a definição de Kurose e Ross (2013) pág. 538, entende-se que “um *firewall* é uma combinação de *hardware* e *software* que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros”. O mesmo afirma que “o *firewall* permite a um administrador de rede controlar o acesso entre o mundo externo e os recursos da rede que ele administra, gerenciando o fluxo de tráfego para esses recursos”.

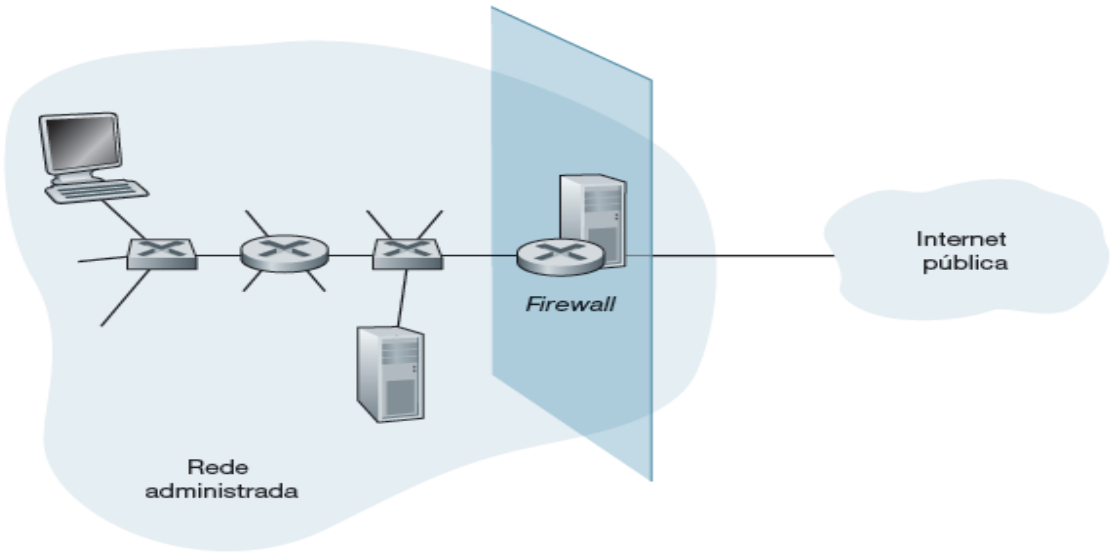
Um *firewall* possui três objetivos para Kurose e Ross (2013):

1. **Todo o tráfego de fora para dentro, e vice-versa, passa por um *firewall***. A Figura 1.0 mostra um *firewall*, situado diretamente no limite entre a rede administrada e o resto da Internet. Embora grandes organizações possam usar diversos níveis de *firewalls* ou *firewalls* distribuídos alocar um *firewall* em um único ponto de acesso à rede, conforme mostrado na Figura 1.0, facilita o gerenciamento e a execução de uma política de acesso seguro.

2. **Somente o tráfego autorizado, como definido pela política de segurança local, poderá passar.** Com todo o tráfego que entra e sai da rede institucional passando pelo *firewall*, este pode limitar o acesso ao tráfego autorizado.

3. **O próprio *firewall* é imune a penetração**. O próprio *firewall* é um mecanismo conectado à rede. Se não projetado ou instalado de modo adequado, pode ser comprometedor, oferecendo apenas uma falsa sensação de segurança (pior do que não ter nenhum *firewall*!).

Figura 1.0 Posição do *firewall* entre a rede administrada e o mundo exterior



Fonte: Kurose e Ross (2013)

2.2.1 TIPOS DE *FIREWALL*

A primeira geração do *firewall* tem sua origem em 1989 na Digital Equipment Corp (DEC) e a proposta veio de Jeff Mogul. Três anos depois, em 1991, Steve Bellovin e Bill Cheswick, da Bell Labs da AT&T, projetaram o primeiro conceito conhecido como o filtro de pacotes de estado, o *firewall stateful*, surgindo a segunda geração dos dispositivos de segurança. A terceira geração aparece pouco tempo depois com as vendas do DEC SEAL, que já tinham recursos de aplicação: os *proxy services*. Em 1994, a empresa Check Point lançou o *Firewall*-1, com grande relevância para o desenvolvimento da segurança digital. Na década de 90, com os projetos do Squid (1996) e o Snort (1998), essas soluções são disponibilizadas gratuitamente com a finalidade de gerar um amadurecimento no conceito de segurança digital. Nessa mesma década a VPN, *webfilter*, integração a antivírus e outras soluções foram incorporadas ao *firewall*. (COSTA, 2020)

Para o escritor do blog sobre segurança Pizzolato (2020) “A partir dos anos 2000, o conceito de *firewall* se tornou ainda mais completo. Em 2004, surgiu o termo Unified Threat Management (UTM), que denomina a evolução do dispositivo de segurança ao longo dos anos.”

- **Filtro de pacotes (*Packet filtering*)**

Tanenbaum (2011), descreve em seu livro que “o *firewall* inspeciona todo e qualquer pacote que entra e que sai. Os pacotes que atenderem a algum critério descrito nas regras formuladas pelo administrador serão remetidos normalmente, os falham no teste serão descartados.”

- **Filtros de pacote com controle de estado (*Stateful Firewall*)**

Os autores Kurose e Ross (2013), fazem uma comparação com o filtro de pacotes para explicar que “em filtro de pacotes tradicional, as decisões de filtragem são feitas em cada pacote isolado. Os filtros de estado rastreiam conexões TCP e usam esse conhecimento para tomar decisões sobre filtragem.”

- ***Firewall* de aplicação ou proxy de serviços (*proxy services*)**

O *firewall* de aplicação, conhecido como *proxy* de serviços é uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e

outra rede, externa ou a internet. *Firewalls* deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino. (ALECRIM, 2013)

2.3 TECNOLOGIA DE *FIREWALL*

Firewall de Gerenciamento Unificado de Ameaças ou *Unified Threat Management* (UTM), são dispositivos que fornecem melhor controle e segurança a rede, potenciais problema relacionados a tráfego de rede, comportamento do usuário e conteúdo de aplicativos, tendo uma maior capacidade de prever ameaças, com suporte a tecnologias de detecção e prevenção de intrusão, recursos esses não encontrados em *firewalls* comuns. (TITTEL, 2016)

Atualmente, pode-se encontrar no mercado diversas soluções de firewalls UTM, no entanto, será abordado o PFsense sendo a solução software livre e o FortiGate a comercial que são usadas nas empresas alvo desse estudo, sujeitos objetos do estudo utilizam em infraestrutura de rede essas tecnologias de firewall.

PfSense é um *software* livre usado para transformar um servidor(computador) em um *firewall*, sendo uma poderosa ferramenta de rede, capaz de desempenhar uma variedade de serviços de rede. É uma distribuição *FreeBSD* customizada e é um fork do *m0n0wall*, uma distribuição de *firewall* poderosa de baixo processamento computacional. Sendo baseado no *m0n0wall*, suas funcionalidades vão muito além, adicionando uma variedade de outros serviços de rede popularmente utilizados. (WILLIAMSON, 2011)

FortiGate é uma solução comercial que vem ganhando bastante espaço entre as empresas, segundo a Brasiline Tecnologia (2020) empresa com ênfase em soluções corporativas em Tecnologia da Informação (TI) “os produtos *FortiGate* são *appliances* de segurança com o conceito de UTM que consiste em uma solução de *firewall* com vários outros recursos de segurança já embarcados, que permite uma proteção mais ampla de sua rede corporativa.”

3. PERCURSO METODOLÓGICO

Este é um estudo descritivo comparativo e transversal sobre tecnologias de *firewalls*. Os sujeitos corporativos da pesquisa são:

- Sujeito Empresa 1 utiliza uma solução comercial de *firewall* o *FortiGate* 100D.
- Sujeito Empresa 2 usuária de uma solução de *firewall software* livre o *Pfsense* 2.4.

Essas empresas estudadas ambas são situadas na região metropolitana da cidade do Recife (RMR), e foram observadas para coleta de informações através de entrevista não estruturadas com os gestores de TI. Tal coleta de informações deu-se no período de três meses entre agosto e outubro de 2020.

Assim como supra citado, cada empresa estudada faz uso de uma tecnologia específica, tais tecnologias são de Gerenciamento Unificado de Ameaças ou *Unified Threat Management* (UTM). Ambas as empresas são escritórios de advocacia e precisam de um *firewall* capaz de centralizar várias funções de segurança, serviços de rede e com maior facilidade de gestão e implantação.

4 RESULTADOS E DISCUSSÕES

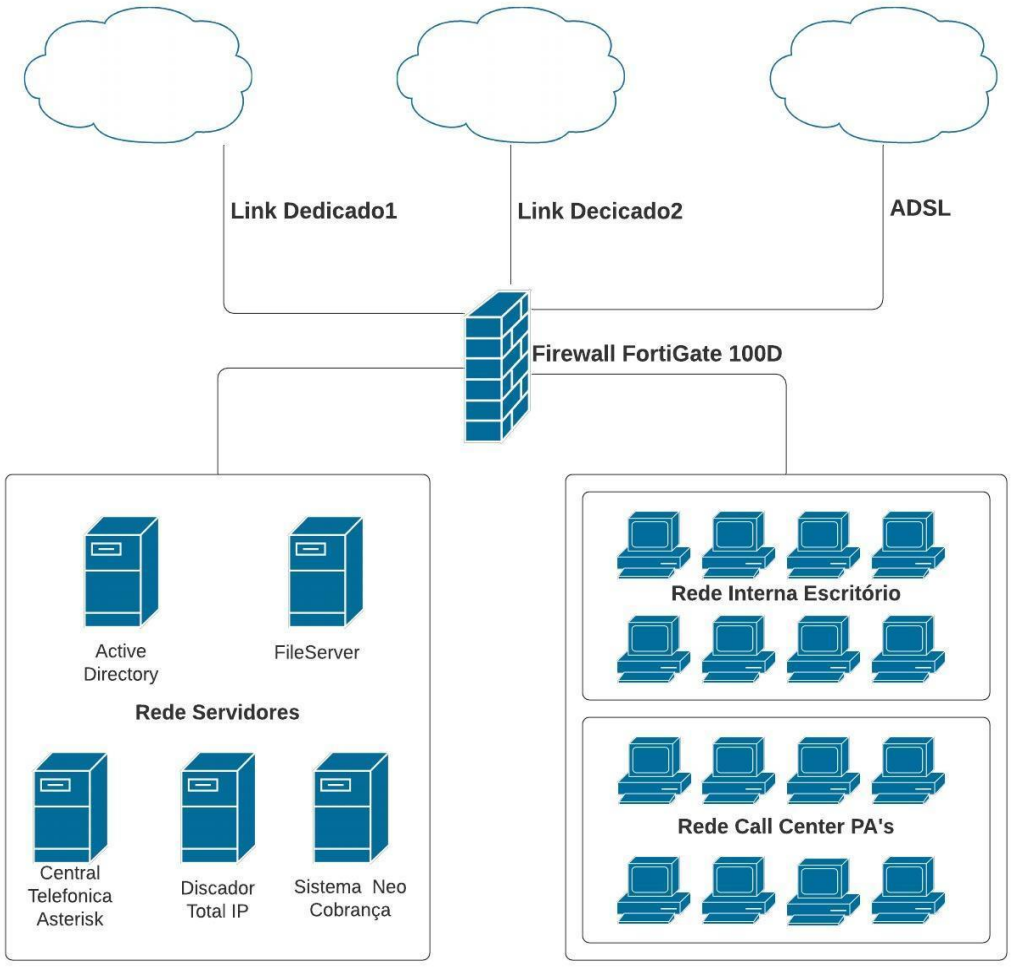
Dentro de cada instituição são necessários recursos de rede tais como: *Dynamic Host Configuration Protocol* (Protocolo de configuração dinâmica de host, ou simplesmente DHCP Server), *Domain Name System* (Sistema de Nomes de Domínios também chamado DNS Server), *WebFilter* (Filtro de conteúdo), *Virtual Private Network* (Rede Virtual Privada – VPN), *Load Balancing* (Balanceamento de carga), *Reporting* e *Monitoring* (Relatório e Monitoramento), IPS/IDS além de várias regras de *Firewall*.

4.1 SUJEITO EMPRESA 1

Sujeito Empresa 1, é um escritório de direito e cobrança que atende vários bancos e empresas. Suas operações compõem atividades que utilizam serviços de rede como central telefônica IP, compartilhamento de arquivos e impressoras em rede, filtro de conteúdo, serviço de controle de domínio, lista de controle de acesso, sistema de CRM de cobrança, balanceamento de carga de links, dentre outros. O *firewall FortiGate* 100D UTM usado na empresa citada, possui todos os serviços de rede usados na empresa. Com uma topologia de rede de complexidade média, o *firewall* escolhido pela empresa atende a todas as suas necessidades. O gestor de TI, fala que esse escolha se deu devido ao time de TI não possuir conhecimento em ferramentas de firewall, e com o crescimento dá empresa ter um firewall não era apenas uma opção mais uma necessidade, contratar um novo colaborador apenas para desempenhar essa tarefa foi uma opção, mas devido ao fato que de que uma pessoa não poderia dá conta da demanda, a escolha mais assertiva seria contratar uma empresa para prestar esse serviço tendo assim um suporte 24 por 7, tendo e uma equipe já treinada e pronta para solucionar problemas, não tirando essa atribuição dos suporte internos.

Na figura 2 consta a descrição topológica física da rede:

Figura 2: Topologia física da rede

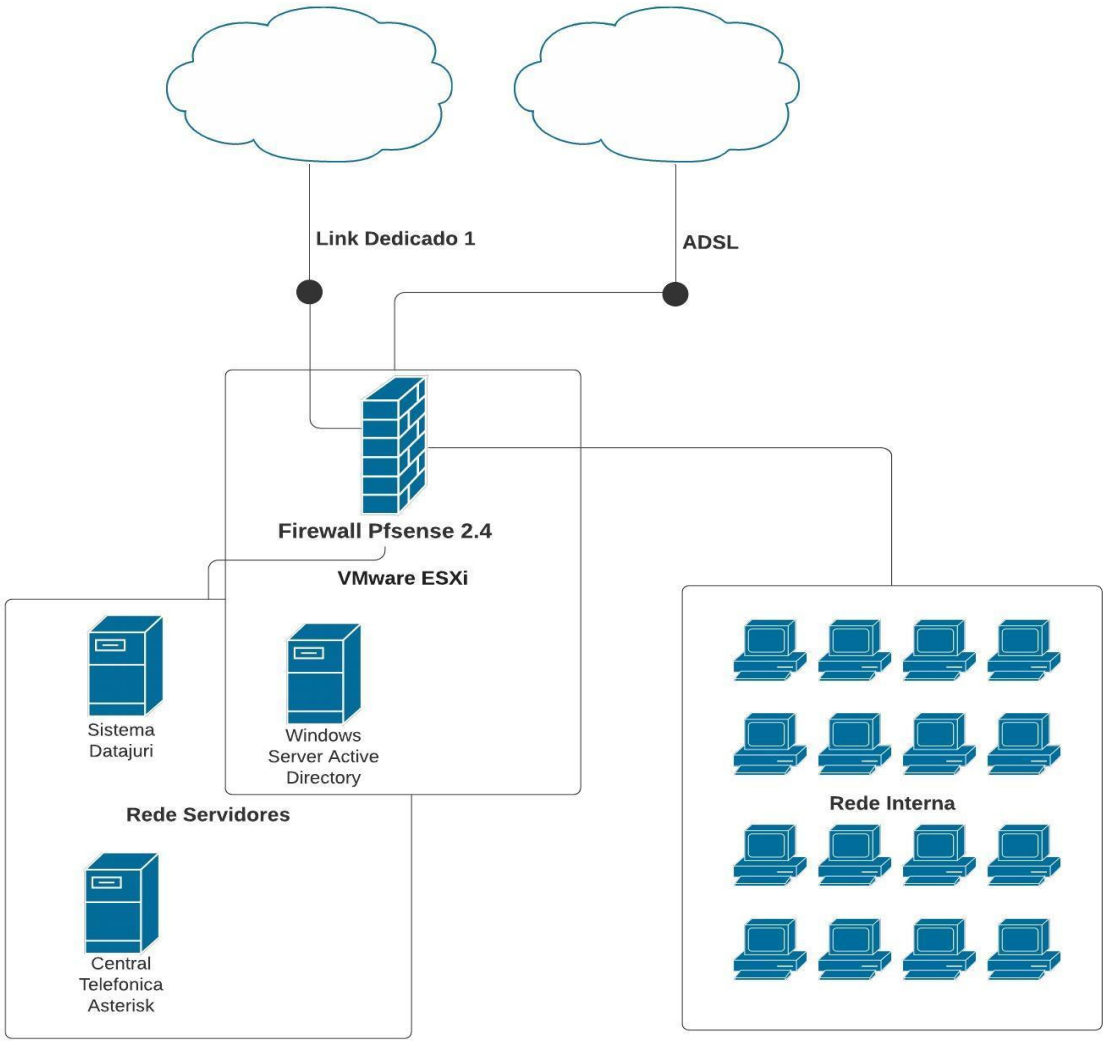


4.2 A SUJEITO EMPRESA 2

Sujeito Empresa 2 é um escritório de direito que atende a vários segmentos e com uma operação de cobrança pequena, faz uso em suas operações de serviços de rede como central telefônica IP, compartilhamento de arquivos e impressoras em rede, filtro de conteúdo, serviço de controle de domínio, lista de controle de acesso, sistema jurídico e balanceamento de carga de links. O *Pfsense* 2.4 *firewall* escolhido pelo gestor possui os recursos de rede e de segurança para manter sua operação em funcionamento e segura, mesmo possuindo uma topologia de rede de complexidade média, devido ao fato de usar virtualização. Estando o *Pfsense* virtualizado em sua estrutura de rede como apresentado da figura 3, tal solução possui os requisitos

necessário de rede e dispõe da possibilidade de instalar novos serviços, e aprimorar seus recursos computacionais, por se tratar de uma máquina virtual, recursos tais como memória, processador e até mesmo periféricos pode ser adicionado ou substituído facilmente como exemplo adaptadores de redes, HD dentre outros. Sendo uma ferramenta *software* livre faz uso das liberdades dessa licença.

Figura 3: Representação Topológica física da rede.



5 CONCLUSÃO

O desenvolvimento do presente estudo possibilitou uma análise de como o *software* livre pode ser usado no ambiente corporativo, provendo segurança e recursos de rede, do mesmo modo que *software* proprietário. Tal estudo também descreveu os tipos de licença de *software* livre e a gênesis do *firewall*. Permitiu através de entrevistas não estruturada conhecer as soluções de *firewall* e como cada uma das soluções contribui dentro das empresas alvo deste estudo. Pode-se perceber similaridade nos recursos de ambas as tecnologias de *firewall*, o que responde um dos objetivos específicos desta pesquisa.

A empresa sujeito 1 do estudo, segundo o gestor, optou por ter uma solução software proprietário, o *FortiGate* 100D, que é uma caixa fechada com recursos pré-definidos de fábrica e que usa o *FortiOS*, não permitindo ser manipulado para qualquer tido de alteração. Sua implantação e suporte se dá através de terceiros. a escolha de uma empresa terceirizada como mantenedora do *firewall* para configurações de maior complexidade se faz necessário para garantir uma equipe especializada e certificada na ferramenta.

A empresa sujeito 2, O administrador e gestor de TI informou que optou por uma solução *software* livre de *firewall* o *Pfsense* 2.4, implementado pelo próprio time de TI (Tecnologia da Informação) da empresa, que possibilita mais agilidade nas resoluções de problemas visto que o suporte é dado pela equipe interna. O *Pfsense* encontra-se virtualizado em sua infraestrutura de TI, flexibilizando alterações de *hardware*, tais como memória, processador e adaptadores de rede. O *software* por se tratar de uma licença livre conta com uma variedade de melhorias através de *software* de terceiros e modificações de acordo com as necessidades da empresa. O Administrador da rede e também gestor descreve que devido ao pouco recurso ofertado para a escolha da tecnologia que seria escolhida, por possuir conhecimento em ferramentas livres, e o firewall sendo uma ferramenta de gerência interna tornaria mais rápido e ágil a resoluções de problema, visto que o próprio time de TI poderia agir imediatamente quando o problema acontecer, por possuir conhecimento na ferramenta, treinou e capacitou a equipe para que pudesse atuar na resolução de problemas, tornando esse suporte parte da operação do time.

A escolha de um firewall, deve ser levada em consideração vários pontos tais como: investimento financeiro que a empresa está disposta a disponibilizar,

necessidade de proteção que o modelo de negócio exige, marca dos fornecedores, o tipo de suporte, atualizações do produto e como atende seus parceiros.

Tendo em vista esses critérios o que os fatores que foram levados em consideração pelos gestores da empresa foi o investimento e o suporte. Enquanto um opta por uma empresa para prestar esse serviço tornando assim esse suporte uma demanda externa e aguardar a solução por parte da empresa contratada. O outro tendo um investimento financeiro mais baixo, torna essa atividade parte da rotina interna do time de TI, e assim tornando mais ágil as resoluções dessa origem de demanda.

6 ANEXO

QUESTIONARIOS:

Gestor empresa sujeito 1:

1. Conhece sobre softwares livres?

Apenas conhecimento acadêmico do tempo de faculdade.

2. Por que usa a tecnologia de firewall atual?

Devido ao investimento financeiro não ser um problema, optamos por ter uma empresa terceirizada, para prestar esse serviço, tirando a carga que essas demandas poderiam causar a nossa equipe, com isso a continuar livre para o atendimento dos colaboradores.

3. Teria uma solução software livre em seu parque?

Sim, já pensamos em usar o Zabbix para monitoramento dos ativos, mas devido à falta de conhecimento dentro da equipe TI é apenas um projeto futuro.

Gestor empresa sujeito 2:

1. Conhece sobre softwares livres?

É usuário de sistemas operacionais unix, e já implementou vários tipos de serviço com software livre para backup, monitoramento dentre outros.

2. Por que usa a tecnologia de firewall atual?

Por conhecer as tecnologias livres, e não dispor de um orçamento que pudesse usar soluções proprietárias, a tecnologia de firewall livre usada se mostrou a melhor alternativa por possuir os mesmo recurso que os firewall proprietários do mercado.

3. Teria uma solução software proprietário em seu parque?

Não se aplica.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. **O que é firewall?**: conceito, tipos e arquiteturas. Conceito, tipos e arquiteturas. 2013. Disponível em: https://www.infowester.com/firewall.php. Acesso em: 05 nov. 2020.

COSTA, Matheus Bigogno. **O que é Firewall**. 2020. Disponível em: https://canaltech.com.br/internet/o-que-e-firewall/. Acesso em: 05 nov. 2020.

FUTEMA, Fabiana. **Home office para sempre vai ser o novo normal das empresas?** 2020. 6 Minutos - Notícias, entrevistas e vídeos de economia. Disponível em: https://6minutos.uol.com.br/carreira/home-office-para-sempre-vai-ser-o-novo-normal-das-empresas/. Acesso em: 13 nov. 2020.

GNU. Patrocinado Pela Free Software Foundation (org.). **O que é o software livre?**: a definição de software livre. A Definição de Software Livre. 2009-2019. Tradução: Rafael Beraldo e Rafael Fontenelle. Disponível em: https://www.gnu.org/philosophy/free-sw.pt-br.html. Acesso em: 30 out. 2020.

HEXSEL, Roberto. **Software Livre**: propostas de ações de governo para incentivar o uso de software livre. Curitiba: Universidade Federal do Paraná, 2002. Fonte: http://www.inf.ufpr.br/pos/techreport/RT_DINF004_2002.pdf

KUROSE, Jim F.; ROSS, Keith W.. **Redes de computadores e a internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013. 658 p.

KUSZKA, Boris. **A História do Software Livre**. Homepage Canal Tech. Disponível em: https://canaltech.com.br/software/A-Historia-do-Software-Livre/. Acesso em: 13 nov. 2020.

MORAES, Alexandre Fernandes de. **Firewalls**: segurança no controle de acesso. São Paulo: Editora Érica Ltda., 2015. 50 p.

MOREIRA, Paulo. **Política de Segurança da Informação e Firewall**. 2011. Revista Infra Magazine 2. Disponível em: https://www.devmedia.com.br/politica-de-seguranca-da-informacao-e-firewall-revista-infra-magazine-2/22234. Acesso em: 28 out. 2020.

NACIF, Luis Carlos. **Home office**: segurança da informação e trabalho remoto. segurança da informação e trabalho remoto. 2020. Disponível em:

https://www.cisoadvisor.com.br/security-room-posts/home-office-a-seguranca-da-informacao-e-o-trabalho-remoto/. Acesso em: 30 out. 2020.

PIZZOLATO, Rafael. **O Guia Definitivo sobre Firewall**. 2020. Disponível em: https://blog.starti.com.br/firewall/. Acesso em: 10 nov. 2020.

REIS, Daniel Fonseca. **Sobre o uso de Software Livre nas Micro e Pequenas Empresa no Brasil**. Homepage Canal Tech. Disponível em: https://www.devmedia.com.br/sobre-o-uso-de-software-livre-nas-micro-e-pequenas-empresa-no-brasil/10615. Acesso em: 13 nov. 2020.

SILVEIRA, Sérgio Amadeu da. **Software livre**: a luta pela liberdade do conhecimento. São Paulo: Editora Fundação Perseu Abramo, 2004. (1). Fonte: https://www.ufrgs.br/soft-livre-edu/arquivos/amadeu-livro-soft-livre.pdf

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores**: princípoos e práticas. 2. ed. Rio de Janeiro: Elsevier Editora Ltda, 2013. Citado paginas: 570;

TANENBAUM, Andrew S.. **Redes de computadores**. 5. ed. São Paulo: Editora Campus, 2011. 945 p. Tradução de: Vandenberg D. de Souza.

TECNOLOGIA, Brasiline (org.). **FortiGate**: o poder da segurança de alto desempenho. O Poder Da Segurança De Alto Desempenho. 2020. Disponível em: https://brasiline.com.br/blog/fortigate-o-poder-da-seguranca-de-alto-desempenho/#:~:text=Os%20produtos%20FortiGate%20s%C3%A3o%20appliances,ampla%20de%20sua%20rede%20corporativa.. Acesso em: 06 nov. 2020.

TITTEL, Ed. **Unified Threat Management For Dummies**: fortinet special edition. 2. ed. New Jersey: Wiley, 2016

WILLIAMSON, Matt. **PfSense 2 Cookbook**. Birmingham-Uk: Packt Publishing, 2011. 252 p.