SÃO LUCAS EDUCACIONAL DE JI-PARANÁ

ATHER JOSUÉ CORREA GONÇALVES

DEMONSTRAÇÃO DE VULNERABILIDADES NA SEGURANÇA DAS REDES EM COOPERATIVA DE CRÉDITO

Proposta para utilização de firewall

JI-PARANÁ
2021

SÃO LUCAS EDUCACIONAL DE JI-PARANÁ

ATHER JOSUÉ CORREA GONÇALVES

DEMONSTRAÇÃO DE VULNERABILIDADES NA SEGURANÇA DAS REDES EM COOPERATIVA DE CRÉDITO

Proposta para utilização de firewall

Projeto de Pesquisa apresentado à disciplina de trabalho de conclusão de curso, do 8 período do Curso de Sistemas de Informação, do Grupo Educacional São Lucas, sob a orientação da Prof. José Rodolfo M. Olivas.

JI-PARANÁ
2021

Dados Internacionais de Catalogação na Publicação - CIP

G635d Gonçalves, Ather Josué Correa.

Demonstração de vulnerabilidades na segurança das redes em Cooperativa de Crédito: Proposta para utilização de firewall. / Ather Josué Correa Gonçalves. – Ji-Paraná, 2021.
40 fls.; il.

Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2021.

Orientador: Prof. Esp. José Rodolfo Milazzotto Olivas

1. Segurança da Informação. 2. Redes de Computadores. 3. Firewall. 4. Cooperativa de Crédito. I. Olivas, José Rodolfo Milazzotto. II. Título.

CDU 004.7

Ficha Catalográfica Elaborada pelo Bibliotecário Giordani Nunes da Silva CRB 11/1125

RESUMO

Com o rápido avanço das tecnologias, a segurança da informação muitas vezes não acompanha essa demanda, dando espaço para que hackers possam acessar com facilidade os dados, sendo indispensável utilizar técnicas para garantir a segurança da rede. Ter privacidade e segurança nas informações em um ambiente corporativo só é possível com as ferramentas certas, aliadas a uma política de segurança bem elaborada e amplamente divulgada, praticada por cada um dos colaboradores. O objetivo deste trabalho é demonstrar quais ferramentas podem ser utilizadas na área de segurança de redes, demonstrando os conceitos de um sistema e o entorno das medidas a serem tomadas, delineando inclusive, como detectar as necessidades e brechas existentes na rede, através da metodologia de revisão de literatura. Facilitando o processo de decisões acerca da proteção. Para isso foi utilizado a aplicação de um Firewall de última geração em uma Cooperativa de Crédito X, afim de demonstrar como funciona a proteção dos dados.

Palavras-chave: Segurança da Informação. Redes de Computadores. Firewall. Cooperativa de Crédito.

ABSTRACT

With the rapid advancement of technologies, information security often does not keep up with this demand, providing space for hackers to easily access data, and it is essential to use techniques to ensure network security. Having information security and security in a corporate environment is only possible with the right tools, combined with a well-designed and widely publicized security policy, practiced by each of the employees. The objective of this work is to demonstrate which tools can be used in the area of network security, demonstrating the concepts of a system and the surroundings of the measures to be isolated, even outlining how to detect the need and gaps in the network, through the review methodology of literature. Facilitating the decision-making process about protection. For this, the application of a state-of-the-art Firewall in a Credit Cooperative X was used, in order to demonstrate how data protection works.

Keyword: Information security. Computer network. Firewall. Credit cooperative.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Indiscutivelmente, a maior preocupação hoje de empresas e colaboradores é a segurança das informações que as mesmas armazenam, disponibilizam e adquirem. A maioria das empresas pode considerar os riscos e os prejuízos que uma invasão causa, apesar disso, ainda não investem na segurança das informações.

Os riscos surgem quando as empresas vêem as ameaças cibernéticas como problemas puramente técnicos que podem ser resolvidos apenas pelo departamento de TI. Na verdade, as ameaças cibernéticas são e devem ser consideradas como uma questão de gerenciamento de riscos, e a gestão corporativa só pode enfrentar plenamente essa realidade quando a própria organização prioriza sua estrutura digital.

Além dos riscos conhecidos, novos desafios surgem a cada segundo, pois os criminosos estão sempre em busca de fragilidades em cada sistema. Com a pandemia, o mercado foi forçado a explorar cada vez mais o trabalho remoto, expandindo de maneira improvisada suas capacidades de TI, porém, esse despreparo já era notório e só foi agravado pela pandemia.

Ademais, antes mesmo dos acontecimentos de 2020, já sofríamos na mão dos criminosos cibernéticos, que criam por ano em torno de 120 milhões de tipos de malwares. (FILHO, Paulo. Revista PEGN, 2020)

Segundo a CERT.br, o número de incidentes reportados em 2010 foi de 142.844 e em 2011 (até junho) foi de 217.840, ou seja, um aumento de 65% comparando somente com o primeiro semestre de 2011.

De acordo com levantamentos mais recentes realizado pela Consultoria Mckinsey, apenas 16% das empresas no mercado norte-americano se encontram preparadas para lidar com os riscos cibernéticos da atualidade, e as brasileiras infelizmente se encontram ainda menos preparadas. (FILHO, Paulo. Revista PEGN, 2020)

É inegável que, os arquivos devem ser fortemente protegidos contra ataques mal intencionados, pois Hackers podem facilmente acessar os computadores caso os mesmos não possuam nenhum tipo de firewall que minimiza as possibilidades de

um ataque. Um firewall pode proporcionar um meio para que se crie uma camada de tal forma que haja um isolamento de redes externas.

Com o surgimento da Internet, vírus, malwares e a demanda pós pandemia de se utilizar a via remota, a cada dia aumenta a possibilidade de fraudes eletrônicas e ataques externos explorando as vulnerabilidades dos sistemas utilizados.

Por meio da revisão de literatura, esse trabalho tem como objetivo orientar sobre conceitos e tecnologias para alcançar a maior segurança possível dentro de uma rede de computadores especialmente de cooperativas de crédito, a fim de maximizar a integridade e segurança dos dados.

2 PROBLEMATIZAÇÃO

É inegável o avanço em massa das tecnologias, o descontrole sobre as informações processadas e o desconhecimento de como proteger dados que são armazenados em redes torna os ataques presentes e por vezes imperceptíveis, o domínio das redes sobre o controle da vida humana deveria ser um fator de preocupação quanto à segurança de dados, porém, o vazamento de informações demonstra quão vulneráveis e incapacitados estão os usuários.

O número de invasões principalmente em empresas como as cooperativas de crédito vem crescendo a cada dia e mostram o quanto estão despreparadas em questões de segurança de dados. Com isso, qual a importância de investir em segurança da informação empresarial e consequentemente pessoal? Quais prejuízos uma invasão pode causar? Como proteger a rede de maneira eficaz?

3 HIPÓTESES

No dia a dia, invasores se aproveitam do tráfego de entradas e saídas de dados para adentrar nos ambientes corporativos ou residenciais com a finalidade de subtrair dados na sua forma bruta ou mesmo informações, por meio de vírus e malwares, que são softwares invasores. Para isso, um firewall possui ferramentas de proteção oferecidas ao usuário, a fim de minimizar essas investidas.

4 OBJETIVOS

Analisar incapacidades ao proteger dados da rede de cooperativa de crédito, explicar e implementar o funcionamento de um firewall para uma cooperativa de crédito e aumentar a segurança da rede.

4.1 OBJETIVO GERAL

Apresentar informações e detectar vulnerabilidade nas redes, mostrar o processo das invasões e métodos de prevenção contra furto de dados, por fim, conceituar e instruir na aplicação de um firewall.

4.2 OBJETIVOS ESPECÍFICOS

Levantar informações sobre segurança em redes de computadores
Mostrar histórico de complicações em cooperativas de crédito
Informar sobre tipos de invasões e invasores
Capacitar para eventual prevenção de vazamento de dados
Orientar sobre a segurança de dados
Elaborar um guia prático para orientação dos colaboradores
Utilizar firewall de acordo com a necessidade da empresa

5 JUSTIFICATIVA

Com o aumento do uso de componentes de rede e Internet, o número de invasões e infecções por vírus pode aumentar significativamente, o que gera uma grande demanda por investimentos na área de segurança de rede. Para isso, é importante orientar empresas e colaboradores da proteção, evitando vazamento de dados e comprometimento das informações, visando um ambiente seguro ao trabalhar, seja na empresa ou em home office.

6 REFERENCIAL TEÓRICO

6.1 SOBRE REDES

Em tempos remotos, redes de computadores eram entendidas como vários computadores, dentro de uma empresa, que se comunicavam apenas localmente. Por padrão, redes de computadores eram entendidas como uma solução que distribuía cabos por toda a sala para que vários computadores utilizassem, por exemplo, a mesma impressora e ocasionalmente compartilhassem arquivos de um computador para outro, utilizando o conceito mais básico de Local Area Networks (LAN), sem ainda com o conceito de um servidor central (SOARES; LEMES; COLCHER, 1995; KIZZA, 2009).

A mobilidade consistia unicamente em utilizar o disquete para transferir informações de um local para outro. A Internet, mesmo que de forma restrita, já existia, e dispositivos móveis tais quais os celulares também, porém eram tratados como algo além da imaginação.(SOARES; LEMES; COLCHER, 1995; GALLO, 2003; KIZZA, 2009).

O primeiro conceito de extranet deu-se com a Advanced Research Project Agency Network (ARPANET), que era uma forma de comunicação a longa distância restrito para uso militar e acadêmico. Nesta época, a concepção de segurança da informação não ia além de memorizar senhas com poucos caracteres, tais como datas de aniversário ou simples nomes. A população em geral não tomava conhecimento dos riscos da falta de segurança justamente por estes riscos serem pequenos. O maior perigo seria alguém roubar fisicamente o computador, levando consigo as informações (GALLO, 2003; MORIMOTO, 2010).

Ao longo do tempo com a evolução da informática, a Internet e a tecnologia tornaram-se indispensáveis e necessárias. Com o rápido avanço das tecnologias, a segurança da informação não conseguiu acompanhar este avanço, tornando-se de certa forma ineficaz, dando espaço para que hackers conseguissem acessar com facilidade os sistemas e trazer prejuízos para as empresas.

De acordo com (HORTON; MUGGE, 2003), algumas consequências das invasões são: Monitoramento não autorizado, descoberta e vazamento de

informações confidenciais, modificação não autorizada de servidores e da base de dados da organização, negação ou corrupção de serviços e fraude ou perdas financeiras (QUEIROZ, 2007).

6.2 SEGURANÇA DAS REDES

A segurança em rede de computadores é o resguardo dos dados mantidos na rede, ou seja, na segurança das informações que estão sendo armazenadas em um determinado local (ZOTTO, 2012).

Segundo ARRUDA (2012), a evolução da segurança da informação é realizada simultânea ao dos sistemas computacionais, infelizmente isso não ocorre, as evoluções dos sistemas computacionais são muito mais rápidas, todos os dias novos sistemas são desenvolvidos e a maioria não é realizada os testes para identificar erros de segurança. Atualmente são raros os sistemas que não tenham falhas graves de segurança.

Visando o grande número de dispositivos e equipamentos com acesso à Internet e a falta de segurança principalmente em ambientes corporativos, o número de ataques de invasores e até mesmo de vírus implantados em uma máquina que se propaga através da rede possibilitando a invasão ou perda de dados (ERICSSON, 2015; PEREIRA, 2015).

Com o uso massivo de redes sem fio, prover segurança nas conexões é extremamente importante para que os usuários utilizem a tecnologia de forma segura. Porém em pontos de acesso a falta de segurança é o fator principal, tendo a possibilidade de perda ou roubos de informações. Aplicar técnicas e métodos de segurança é um fator primordial para qualquer segmento que utilize tecnologia (ASSUNÇÃO, 2013).

6.3 TIPOS DE INVASORES

O hacker é a pessoa que descobre a falha de segurança no sistema, informa a falha e desenvolve a correção para a falha encontrada para que a mesma não seja identificada por pessoas má intencionadas que possam realizar possíveis ataques àquele sistema (HIMANEN, 2001; RAYMOND, 2002).

O indivíduo que explora a deficiência na segurança de um sistema computacional ou produto sem qualquer intenção perversa, com o intuito de chamar a atenção dos desenvolvedores, é chamado de cracker é a pessoa que utiliza do conhecimento de segurança da informação para realizar invasão em sistemas, quebrar senhas, roubar informações, ou seja, é um vândalo virtual (MORIMOTO, 2005; CINTO, 2015).

Já o Lammer é um termo utilizado para as pessoas que não possuem nenhum ou pouco conhecimento sobre hack e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques. Conhecido atualmente também por "Script Kiddie" que utilizam exploits, trojan, entre outros. O Lammer foi um termo depreciativo utilizado com maior frequência no final da década de 80 e na década de 90, atribuído àqueles que realizam ataques da área de segurança da informação, mas não possuem conhecimento necessário para desenvolver suas próprias ferramentas para realizar ataques (CANALTECH, 2016c). Segundo Canaltech.

6.4 SOFTWARES GERALMENTE UTILIZADOS

6.4.1 VÍRUS

Vírus é um software que infecta o sistema, se replicando e tentando se espalhar rapidamente para outros computadores, via e-mail, redes sociais, rede, dispositivos plugados no computador como pen drive, discos rígidos externos, entre outros. Estes vírus têm como objetivo prejudicar o desempenho do computador podem causar danos ao sistema do computador, tais danos como, formatar o disco rígido, apagar arquivos do sistema ou arquivos do usuário e utilizar a memória do computador para torna-lo lento (STI, 2016).

6.4.2 MALWARE

Malwares é um termo utilizado para todos os softwares que se instalam nos computadores comandados para se infiltrar na máquina causar danos mais graves, como roubar informações e senhas divulgar serviços, entre outros (STI, 2016).

6.5 TÉCNICAS DE INVASÃO

“Após escolher o alvo os ataques são definidos de acordo com a coleta de informações e fragilidades dos sistemas” Welch A, Deamon D (2002).

Algumas taxonomias de ataque são:

6.5.1 Fin scan, ataque de captura o levantamento de informações do alvo

Esse tipo de scanner utiliza um recurso muito interessante que partir do princípio que as portas fechadas respondem com um RESET (reiniciar), E as portas abertas não enviam flag (sinalização) algum. Esta é uma das técnicas preferidas para o chamado modo estealh (oculto) de levantamento de informações. (SANTOS, 2007)

6.5.2 Ataque de paralisação ou sobrecarga de solicitações

Denial of service - de acordo com a definição CERT (Computer Emergency Response Team), os ataques Dos (Denial of service), também denominados ataque de negação de serviços, consistem em tentativas de impedir usuários legítimos de utilizar em um determinado serviço de um computador. Para isso, são usadas técnicas que podem: sobrecarregar uma rede até o ponto em que os verdadeiros usuários dela não consigo usá-la; derrubar uma conexão entre dois ou mais computadores; fazer tantas requisições é um site até que este não consiga mais ser acessado; negar acesso a um sistema ou a determinados usuários. (SANTOS, 2007)

6.5.3 Ataque de comprometimento

Buffer overflow, os programas que manipulam variáveis necessitam de buffers, que são áreas de memória onde são armazenados dados que estas mesmas variáveis recebem. Esta área normalmente é limitada e quando, em determinado momento, a um estouro dessa área por um excesso de informação ocorre o Buffer overflow. (SANTOS, 2007)

6.6 FIREWALL

“Um dos grandes riscos para uma rede interna é o próprio usuário”. Marcos A, Pitanga C (2003).

O usuário por não conhecer ou negligenciar os acessos da rede ou apenas leigo a como proceder com a segurança interna, expõe ao risco toda segurança da rede.

Entretanto, um firewall pode ajudar a impedir que hackers ou softwares mal-intencionados (worms) acessem computadores por meio da rede ou da Internet. Um firewall também pode ajudar a evitar que seu computador envie software malicioso para outros computadores.

Desenvolvido pela Bell Labs em meados de 1980, a pedido de uma das maiores empresas de telecomunicações do mundo a AT&T, o primeiro firewall do mundo foi desenvolvido com o objetivo de “filtrar” informações que entravam e saiam da sua rede empresarial, de forma que fossem flexíveis para a manipulação seguindo especificações presentes as regras definidas pelos cientistas e desenvolvedores da Bell Labs (NETO, 2004, p. 10).

Desde então, mesmo os meios tecnológicos estarem em crescente desenvolvimento, um firewall continua obtendo os mesmos conceitos, mas contendo alguns aprimoramentos.

Ademais, segundo NAKAMURA e GEUS (2007), é possível compreender que firewall vai além de uma simples barreira de proteção contra- ataques externos. O firewall pode ser utilizado como uma proteção dentro da rede, controlando de tráfegos a servidores específicos.

6.7 CLASSES DE FIREWALL

Existem basicamente três classes de firewall que são filtro de Pacotes, NAT e o Híbrido.

6.7.1 Firewall Filtro de Pacotes

É o tipo de firewall que filtra todo o tráfego direcionado a ele mesmo ou a rede local a qual ele isola, da mesma forma, é responsável por filtrar os pacotes que ele, ou a rede, emitem.

INPUT: Pacotes que chegam ao host;

OUTPUT: Pacotes que saem do host;

FORWARD: O que chega a um host e precisa ser redirecionado a um outro host ou outra interface de rede (NETO, 2004).

6.7.2 Firewall NAT

Tem a finalidade de manipular a rota do tráfego, aplicando a tradução de endereçamento sobre os pacotes. Isso possibilita a manipulação dos endereços de origem e destino entre outras coisas.

PREROUTING: Quando há necessidade de realizar alterações em pacotes antes serem roteados ao seu destino;

POSTROUTING: Quando há necessidade de realizar alterações depois que os pacotes forem roteados ao seu destino;

OUTPUT: Realiza a verificação em pacotes emitidos pelo host Firewall (NETO, 2004).

6.7.3 Firewall Híbrido

É a opção de Firewall que seria uma união entre as outras duas classes citadas anteriormente, ou seja, “agrega a si tanto funções de filtragem de pacotes quanto de NAT.” (NETO, 2004, p. 13).

PREROUTING: Modifica os pacotes antes de eles serem roteados;

OUTPUT: Modifica pacotes gerados localmente antes de serem roteados.

6.8 COOPERATIVA DE CRÉDITO

A sua finalidade é colocar os produtos e serviços de seus cooperados no mercado, em condições mais vantajosas do que eles teriam isoladamente. Desse

modo, a cooperativa pode ser entendida como uma “empresa” que presta serviços aos seus cooperados (SEBRAE, 2014, p. 11).

> “As Cooperativas de crédito são sociedades de pessoas, constituídas com o objetivo de prestar serviços financeiros aos seus associados, na forma de ajuda mútua, baseada em valores como igualdade, equidade, solidariedade, democracia e responsabilidade social. Além de prestação de serviços comuns, visam diminuir desigualdades sociais, facilitar o acesso aos serviços financeiros, difundir o espírito de cooperação e estimular a união de todos em prol do bem-estar comum (PAGNUSSATT, 2004 p.13)”.

Todavia, suas atividades estão sujeitas a riscos diversos. A ampliação da participação dessas organizações no Sistema Financeiro Nacional (SFN) pode impactar na competitividade do setor, o que poderia levar a uma maior tomada de risco por parte delas (FIORDELISI, MARQUES-IBANEZ e MOLYNEUX, 2011).

A preocupação com as situações de risco envolvendo instituições financeiras na década de 1970 levou ao surgimento do Comitê de Supervisão Bancária de Basileia (BCBS), que instituiu novos parâmetros de requerimento de capital regulamentar, considerando os riscos associados a exposições, governança e transparência das instituições financeiras (BANCO CENTRAL DO BRASIL, 2019a).

A falta de controle sobre os riscos afeta diretamente o nível de segurança e de garantias sobre as operações realizadas, levando-as a se afastar de sua finalidade principal, que é garantir eficiência na prestação de seus serviços (FREITAS, AMARAL e BRAGA, 2008**;** PEREIRA, 2006).

Nas cooperativas, os dados estão presentes de forma onipresente. São informações sobre os milhares de cooperados, processos internos e externos, resultados das produções e outros tantos que viajam do campo para a cidade graças à conexão existente nos dias de hoje. Sendo componentes essenciais para o funcionamento dos processos, incluindo em tomadas de decisão, os dados são um bem que precisa ser protegido. (CESAR, Leonardo. 2021)

De acordo com uma entrevista publicada no Mundo Coop, o entrevistador Leonardo Cesar questiona que "Com o aumento de dados online, o número de ataques cibernéticos também viu um crescimento. Num mundo baseado em dados, como garantir a segurança das informações compartilhadas?”

Em resposta, Bruno Lobo, gerente geral da Commvault para América Latina, assegura que é importante que a empresa adote algumas práticas, como a governança corporativa e uma boa política de segurança da informação, o

treinamento constante dos usuários, a segurança de redes Wi-Fi, a proteção de dados na nuvem, a segurança de dispositivos móveis, além de testes e atualizações constantes. Ele afirmou que sempre terá alguém responsável por acessar os dados, então qualquer descuido que aconteça, permitirá que o sistema seja invadido/ hackeado. Além disso, acrescentou que hoje, o ativo mais valioso de uma empresa são os dados que elas armazenam.

7 MATERIAIS E MÉTODOS

Após entender todo o processo de invasão, desde as técnicas utilizadas, até os tipos de invasores, bem como sobre firewall e suas classes, será abordado procedimentos de prevenção, e posteriormente sobre firewall e sua devida utilização. O objetivo deste trabalho é estabelecer o conhecimento sobre a segurança que um firewall lhes proporciona e sugerir alternativas ao aplicar os métodos de proteção.

Com o crescimento da utilização de tecnologias computacionais nas corporações e no meio doméstico aumentou-se, primeiramente, a necessidade de garantir a confidencialidade, integridade e disponibilidade dos recursos dispostos em rede. Estas medidas de prevenção se tornam necessárias devido ao grande número de informações confidenciais que trafegam em uma rede.

- Confidencialidade — parte do pressuposto que somente as pessoas autorizadas terão acesso aos dados ou recursos;
- Integridade — baseia-se no fato de que somente pessoas devidamente autorizadas terão acesso à alteração destes dados;
- Disponibilidade — é a garantia de que as pessoas devidamente autorizadas terão acesso aos dados quando desejarem.

Ademais, deve-se levar em conta a abordagem de segurança de rede que inclui firewalls para proteger os sistemas internos e redes. É possível usar um sistema de autenticação forte e encriptação para proteger dados particularmente importantes que transitam na rede. Com isso, um local pode obter um tremendo reforço de segurança usando um modelo de segurança de rede.

Além desses métodos, o firewall convém ser muito eficaz, este que é um componente ou um conjunto de componentes que tem como função analisar pacotes que trafegam entre redes, sendo tanto de uma rede interna para a internet, quanto entre redes internas.

Ao contrário do que muitos pensam um firewall não é um dispositivo único, mas sim um conjunto de ferramentas de segurança instaladas e configuradas de modo a trabalharem em conjunto, garantindo assim a aplicação dos parâmetros implementados pelo administrador de segurança para tratamento dos pacotes que trafegam pelas redes. (MITSHASHI, Roberto Akio. 2011. Pág 24)

7.1 GUIA DE INFORMAÇÃO PRÁTICO

7.1.1 Analisar a demanda e necessidades da sua rede

Entender o grau de necessidade mais especificamente é importante, pois existe firewall com suporte para a demanda da empresa, por exemplo, o firewall para rede simples, para empresas pequenas com poucos computadores e usuários, que é o fortinetfortigate 100e.

Em contrapartida, as empresas que possuem um grau de necessidades mais específicas, como vendedores externos e a utilização de sistema mobile, por exemplo, existem os firewallsutm (gerenciamento unificado de ameaças), esse tipo de ferramenta garante que todas as informações sejam criptografadas e que as ameaças sejam gerenciadas por um único dispositivo unificado, as empresas que possuem essa necessidade ou de médio porte é indicado utilizar um fortigate 600e.

Além disso, se a empresa trabalha em um ambiente misto, parte na nuvem e parte fisicamente, é recomendável usar uma arquitetura de firewall avançada que cubra servidores e aplicativos, dessa forma, é possível controlar melhor a segurança da informação, independentemente do ambiente em que esteja inserida.

7.1.2 Verificar questões de segurança

Para facilitar o entendimento dessa etapa, são 3 pontos relevantes que um firewall corporativo predica ter, primeiro o controle unificado de usuários e aplicação e navegação web, sendo que deve haver a limitação de pessoas e aplicativos no acesso as informações e dados, um bom firewall fornece esse recurso de controle unificado, permitindo o gerenciamento dos recursos em um único local com uma maior segurança ao sistema.

Segundo que muitas vezes o usuário é deixado de lado, para isso foi criado a tecnologia de controle em camada 8 que permite controlar e monitorar a “identidade humana” de um usuário como parte de um requisito de segurança, controlando suas atividades e criando relatórios detalhados com suas ações.

E terceiro vem a visibilidade instantânea, dando poder a um gestor ter acesso rápido a todas as informações que envolvem seu firewall, disponibilizando a

visualização do sistema em tempo real, além de outros parâmetros, com isso, o painel principal de controle do sistema precisa fornecer dados sobre o monitoramento de rede, fazendo com que o administrador seja capaz de solucionar problemas como ping, rotas, captura de pacotes e outros.

7.1.3 Conhecer os tipos de firewall disponíveis

Primeiramente, deve-se entender que esse produto está relacionado diretamente com a segurança da rede de computadores de uma empresa, ele funciona baseado no controle de tráfego da rede e monitora todas as ações que ocorrem no sistema.

Com isso, o firewall define os caminhos liberados para o tráfego de informações e quais os programas que poderão passar por eles, evitando por exemplo, furtos de dados confidenciais e invasões de programas maliciosos.

As duas formas básicas que um firewall pode ser encontrado são como software que normalmente já vem instalado em caso de aparelhos como Windows, por exemplo, mas como é uma solução básica, alguns vírus já são capazes de desativarem barreiras e causar danos ao sistema.

Outras formas são os hardwares, um dispositivo que fica fora do computador dos usuários, mais indicados para redes corporativas, por não compartilhar recursos ele consegue ser mais eficiente em tratar requisições, e não é atingido caso o sistema seja infectado por algum vírus.

7.1.3.1 Opções de firewall

Firewall Linux

Seu custo de aquisição é baixo, portanto, é utilizado quando não se tem um grande investimento financeiro para a tecnologia da informação, isso se deve ao fato da ferramenta ser construída em cima de um sistema operacional de código aberto, por isso não precisa de licença ao usar e os custos só ficam na mão de obra da instalação e configuração da estrutura de proteção.

Porém, esse firewall só consegue fazer um controle das portas e protocolos da rede, o que já não é o suficiente para garantir a segurança digital das empresas,

por causa disso, perdeu espaço para novas tecnologias e só é bastante utilizada em máquinas que já vem com este instalado de fábrica.

UnifiedThreatManagement (UTM)

O UTM (UnifiedThreatManagement ou Gerenciamento Unificado de Ameaças), trata-se de uma central que unifica todas as ferramentas de proteção que existem na rede, assim, em uma interface integrada ficam, por exemplo, soluções em segurança digital como o antivírus, anti-spyware, anti-spam, filtros de URL, proxy, entre outros. Dessa forma, em um único processo de atualização do sistema, é possível adequar todas as ferramentas de proteção e continuar o seu funcionamento sem nenhum comprometimento.

Além disso, para empresas com várias unidades, independentemente da distância, algumas soluções UTM apresentam outras vantagens e por meio desses sistemas, o encaminhamento remoto, tradução de endereço de rede e criação de redes virtuais privadas podem ser realizados.

NextGeneration Firewall (NGFW)

Os NGFW (NextGeneration Firewall ou Firewall da Nova Geração) são considerados os melhores firewalls corporativos, com uma performance de excelência na análise das demandas, além de de suprir as demandas das soluções tradicionais UTM, também atuam com tranquilidade quando há o aumento do tráfego de dados das redes.

Portanto, esse é o firewall mais indicado, pois o sistema garante máxima desguarneça do tráfego de informações, independente da demanda, além de atuar em complemento com as UTMs ativadas, sem a existência de perdas.

FortiGateFortinet

Com implantação flexível e um centro de dados avançado, FortiGate pode fornecer desempenho escalonável de serviços de segurança avançados. Nesse sentido, ele usa o processador de segurança de rede (SPU). Como um NGFW, ele também pode fornecer sistemas de maior visibilidade de aplicativos e conexões para os dispositivos IoT do sistema, a topologia ponta a ponta de toda a rede corporativa é gerada automaticamente. Esse aspecto fortalece toda a cadeia de proteção da rede para evitar ataques conhecidos e desconhecidos.

Ele está entre os melhores firewalls corporativos, pois oferece constantes atualizações para o aprimoramento do combate a ameaças que proporcionam uma proteção mais robusta, uma segmentação escalável e latência ultrabaixa para defender setores da estrutura, um compartilhamento de proteção das ameaças em toda a superfície de ataque digital para fornecer proteção rápida e automatizada, além da redução da complexidade do controle da malha de segurança e acesso à nuvem criptografada com todos os tipos de tráfego com inspeção (SSL).

7.2 RELEVÂNCIA DA PROTEÇÃO EM COOPERATIVAS

Para o gerenciamento de dados, é necessário um processo que envolve coletar, validar, armazenar e garantir a segurança de tais e assim poderem ser transformados em informações úteis. É importante ir além, analisando os detalhes da base de dados, tornando o processo de tomada de decisão qualificado, pois quando todas as informações estão organizadas e devidamente armazenadas, de forma integrada e ordenada, arquivos como projetos, balanços financeiros, prospecções de vendas e outros documentos importantes são encontrados com maior facilidade no sistema toda vez que você precisar analisá-los.

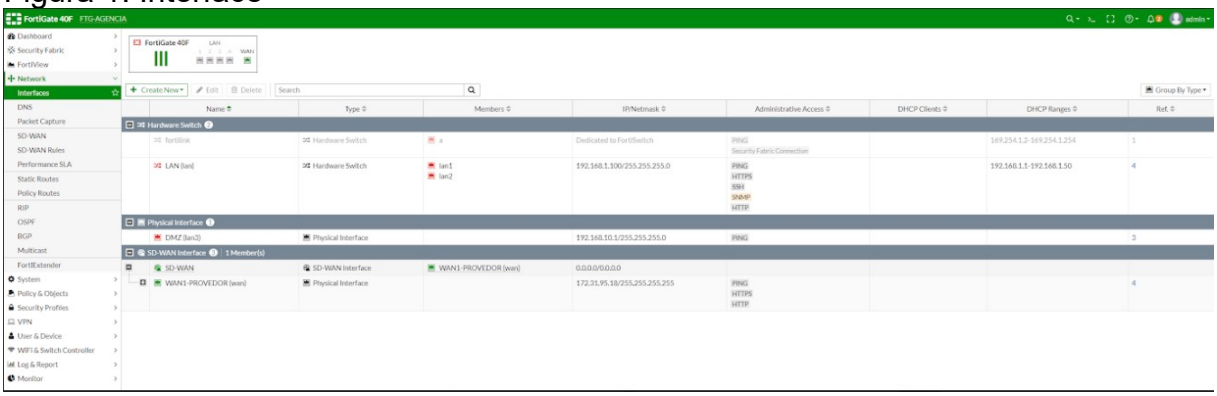
Dessa forma, com o reforço da segurança da informação e proteção da rede, evitaria situações adversas, como a que passou o Banco Inter, em maio de 2018, que sofreu vazamento de dados de quase 20 mil pessoas, entre correntista próprios e até mesmo de outros bancos. Vale a pena investir em ações preventivas e no cumprimento da legislação, evitando assim perdas financeiras e de credibilidade, muitas vezes irrecuperáveis. (MACEDO, KEDSON. COOP. 2019).

8 IMPLANTAÇÃO DE FIREWALL

Normalmente, em cooperativas e empresas com o layout de redes mais antigo utilizavam servidores que serviam como firewall, servidor de arquivos e como DHCP server. Porém, visando maior segurança, será implantado um firewall de última geração em uma Cooperativa X.

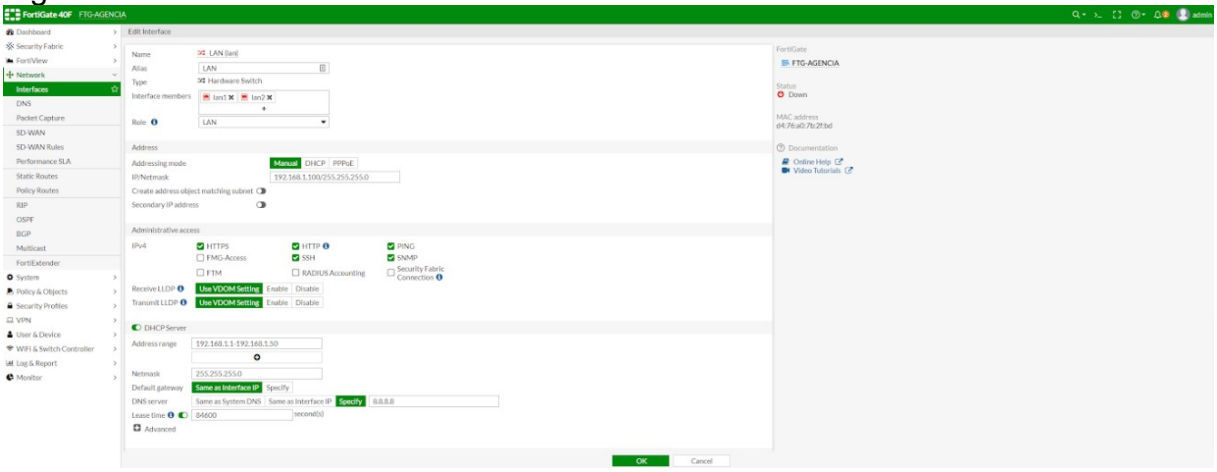
As figuras de 1 a 4 mostram as interfaces que serão usadas, o servidor antes utilizado como DHCP server, será substituído pelo FortiGate e terá o papel apenas de file server. Representado na figura 2, temos a INTERFACE LAN , foi retirado o cabo do servidor e inserido na porta do 01 FortiGate, além disso, as figuras adiante mostram as interfaces DMZ e WAN, por onde chega a internet.

Figura 1: Interface



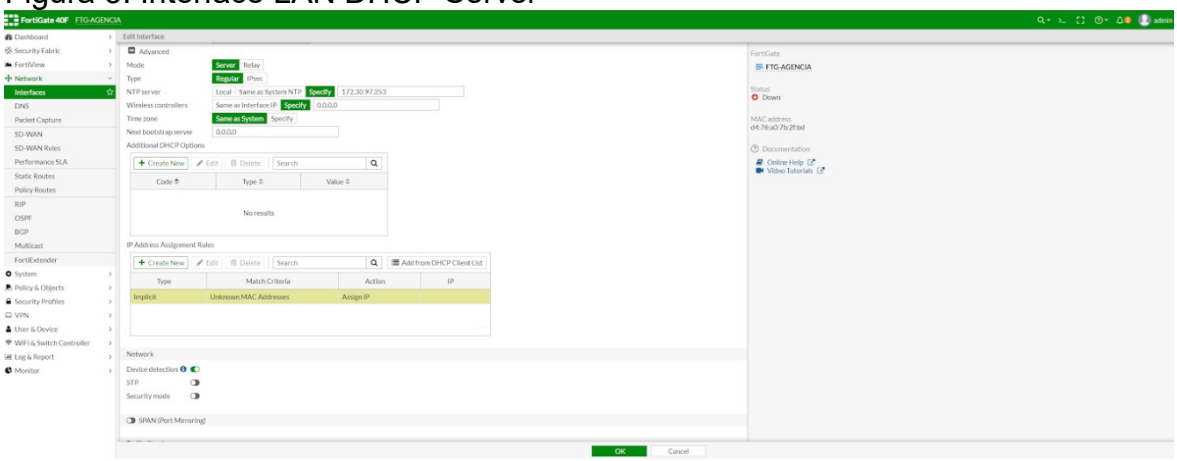
(Fonte: Do autor)

Figura 2: Interface LAN



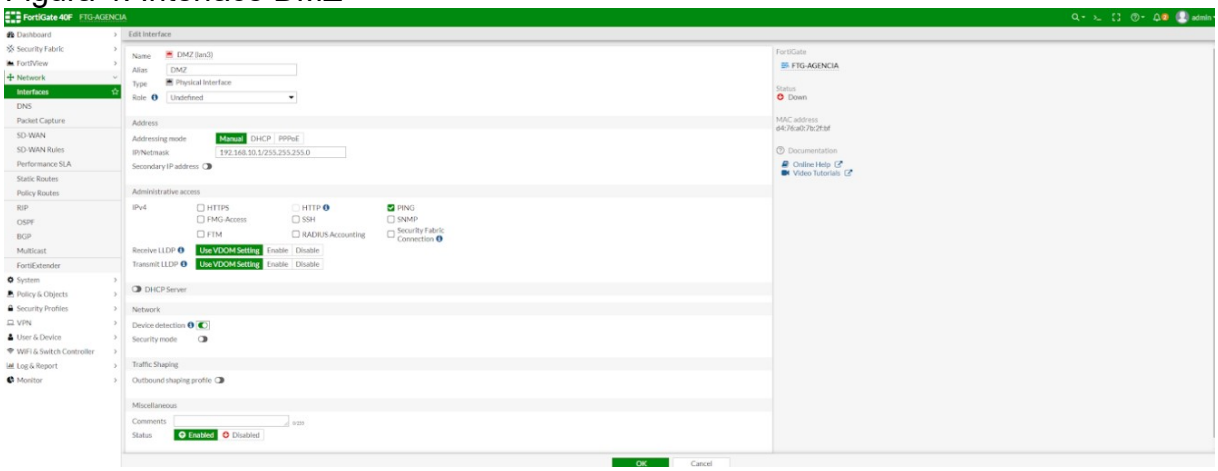
(Fonte: Do autor)

Figura 3: Interface LAN DHCP Server



(Fonte: Do autor)

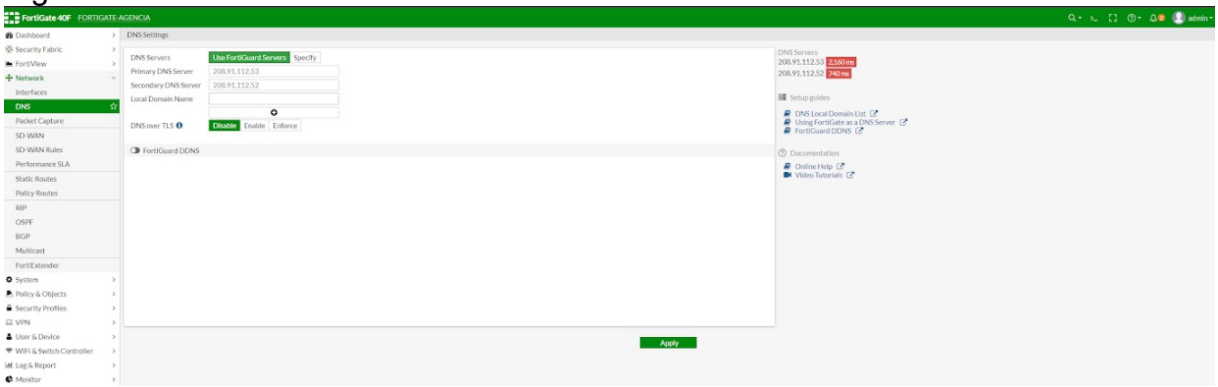
Figura 4: Interface DMZ



(Fonte: Do autor)

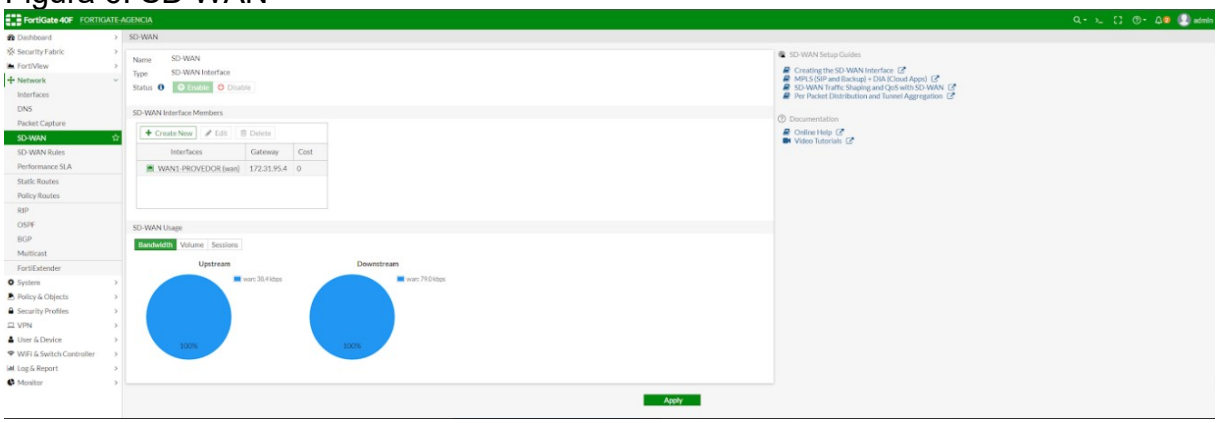
A partir da apresentação das interfaces, as figuras 5 e 6 apresentam as configurações de DNS e a configuração de SD-WAN.

Figura 5: DNS



(Fonte: Do autor)

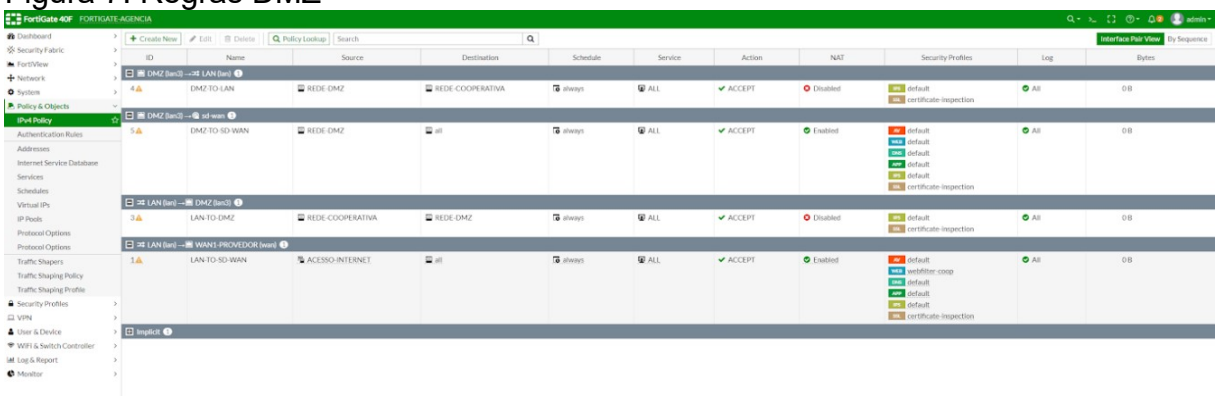
Figura 6: SD WAN



(Fonte: Do autor)

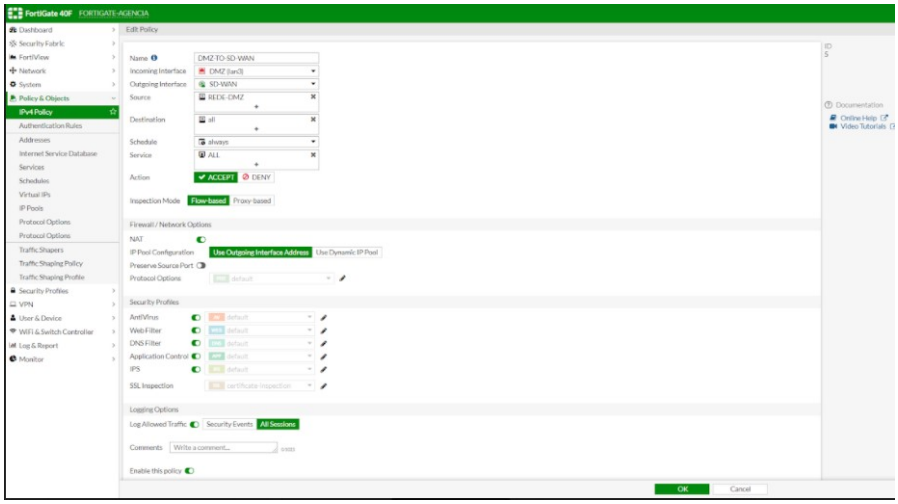
As figuras 7 a 11 apresentam as regras de firewall, que são responsáveis por fazerem a comunicação ou bloqueio entre interfaces, como também com a internet.

Figura 7: Regras DMZ



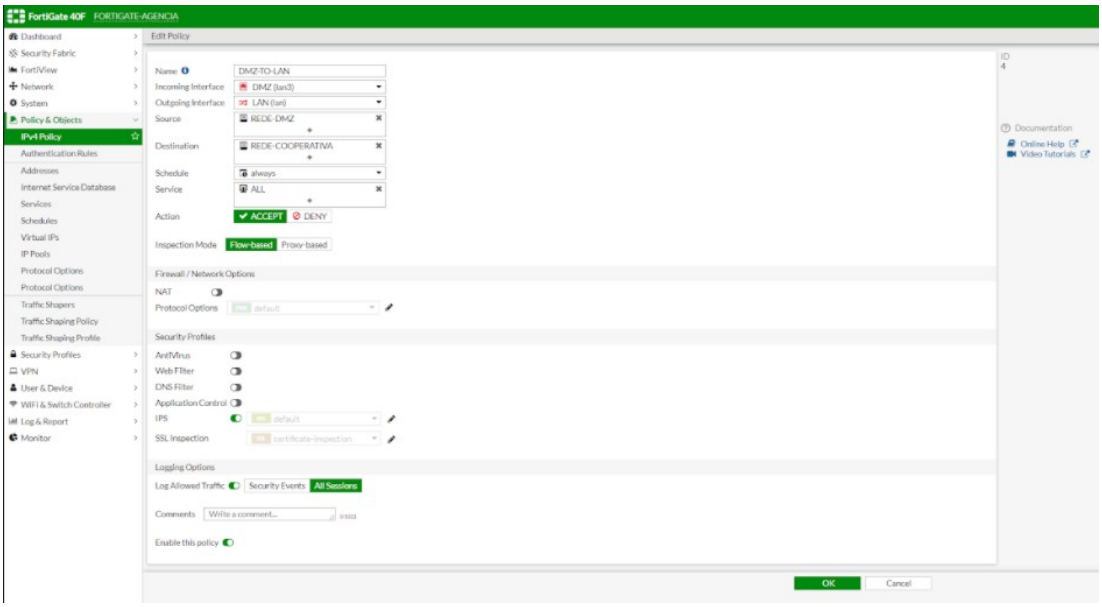
(Fonte: Do autor)

Figura 8: DMZ TO SD WAN



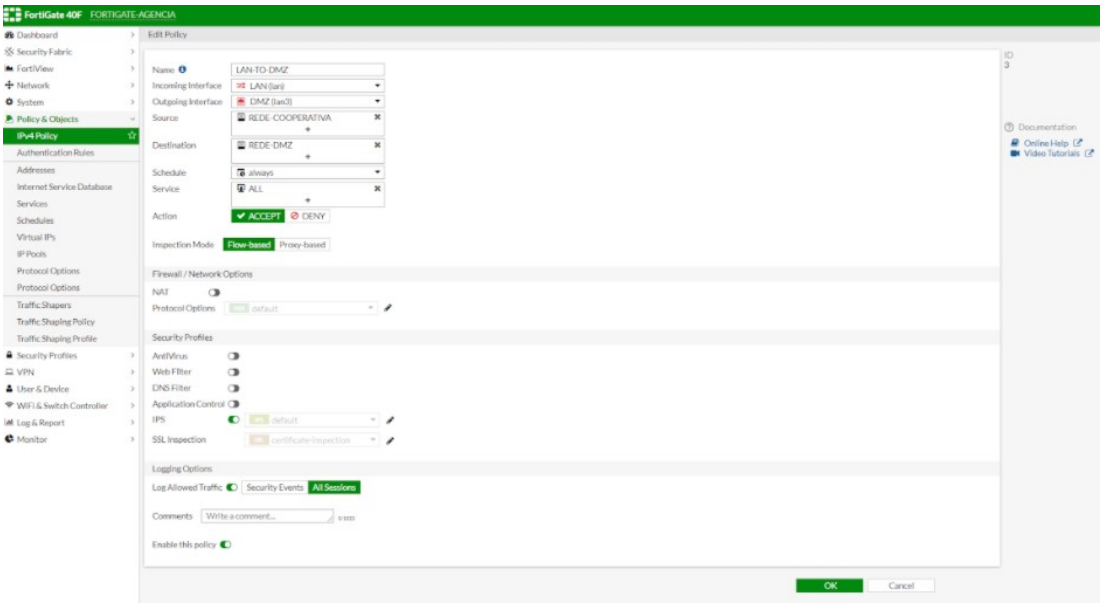
(Fonte: Do autor)

Figura 9: DMZ TO LAN



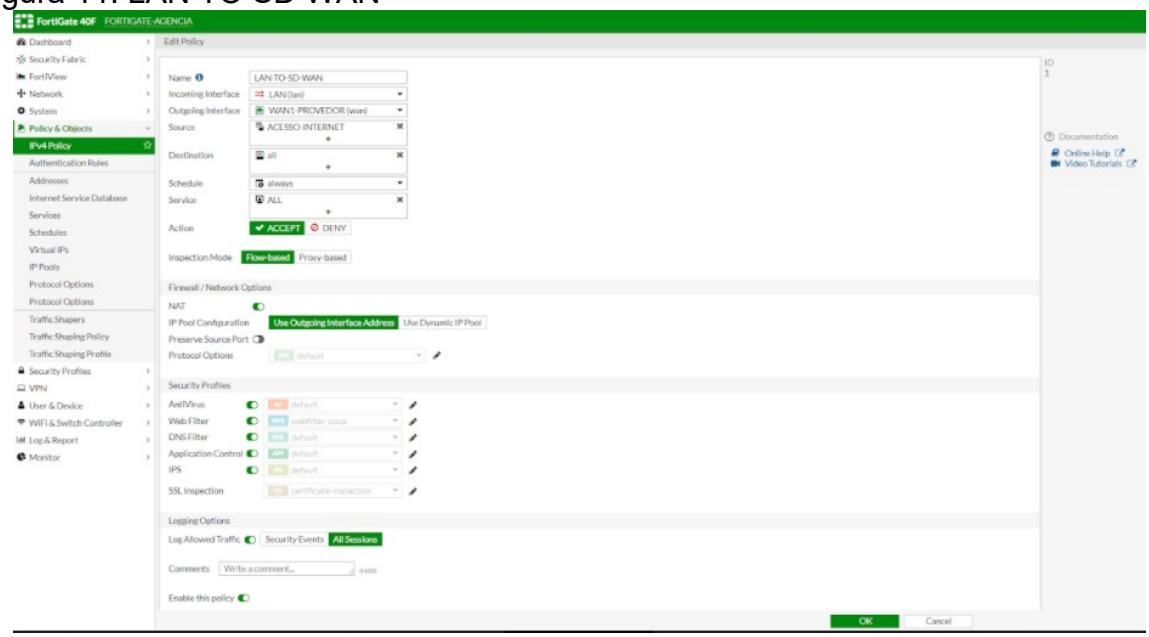
(Fonte: Do autor)

Figura 10: LAN TO DMZ



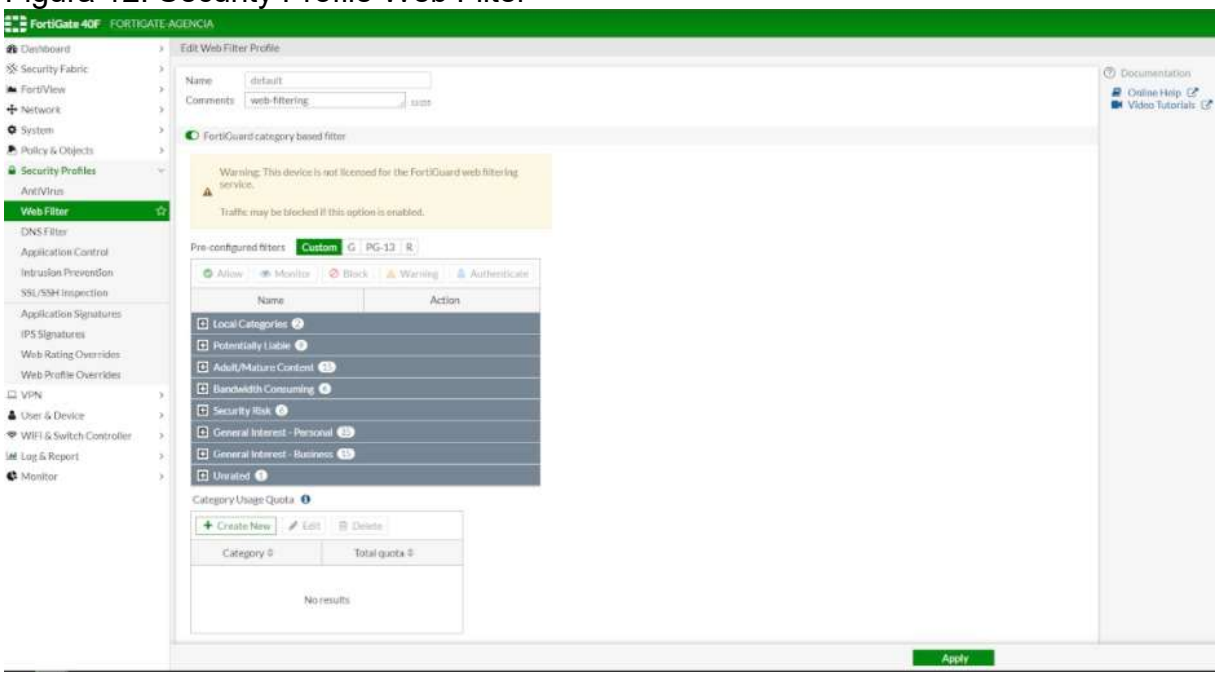
(Fonte: Do autor)

Figura 11: LAN TO SD WAN



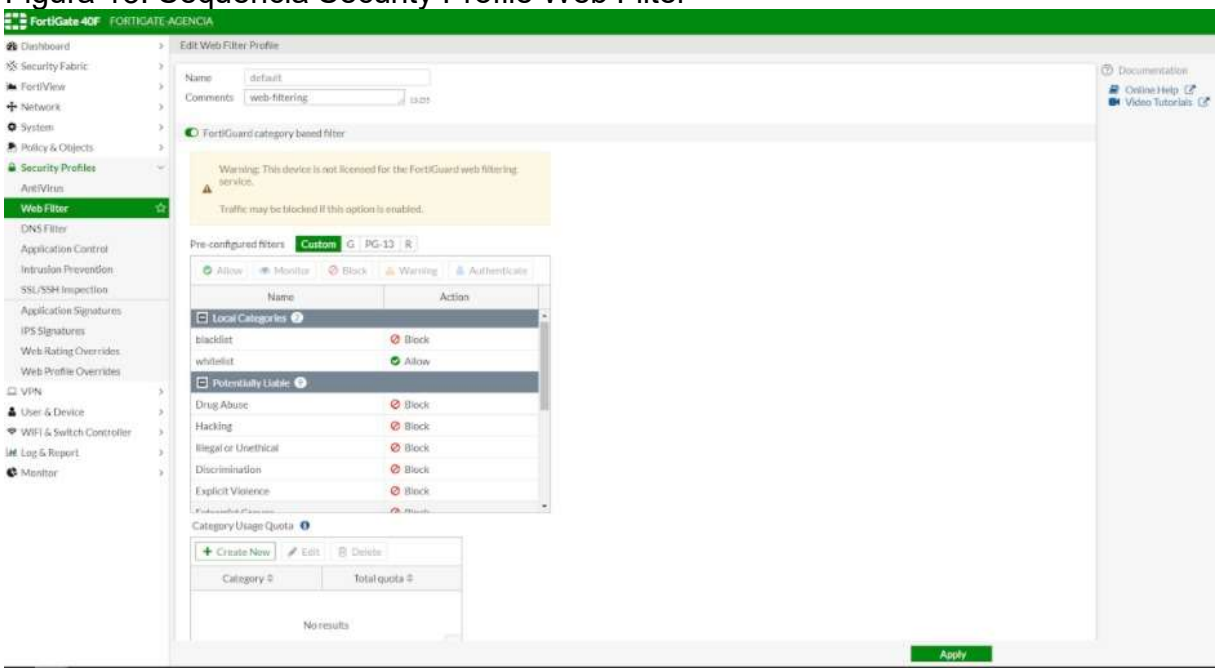
(Fonte: Do autor)

Figura 12: Security Profile Web Filter



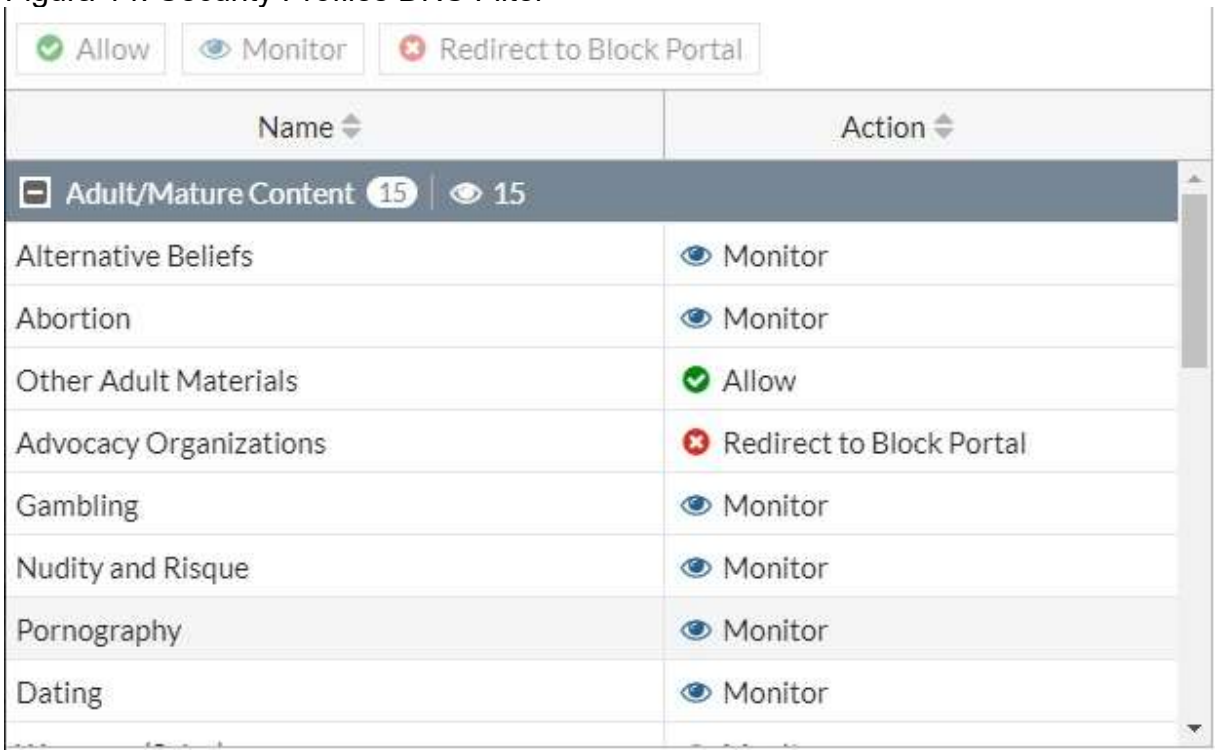
(Fonte: Do autor)

Figura 13: Sequencia Security Profile Web Filter



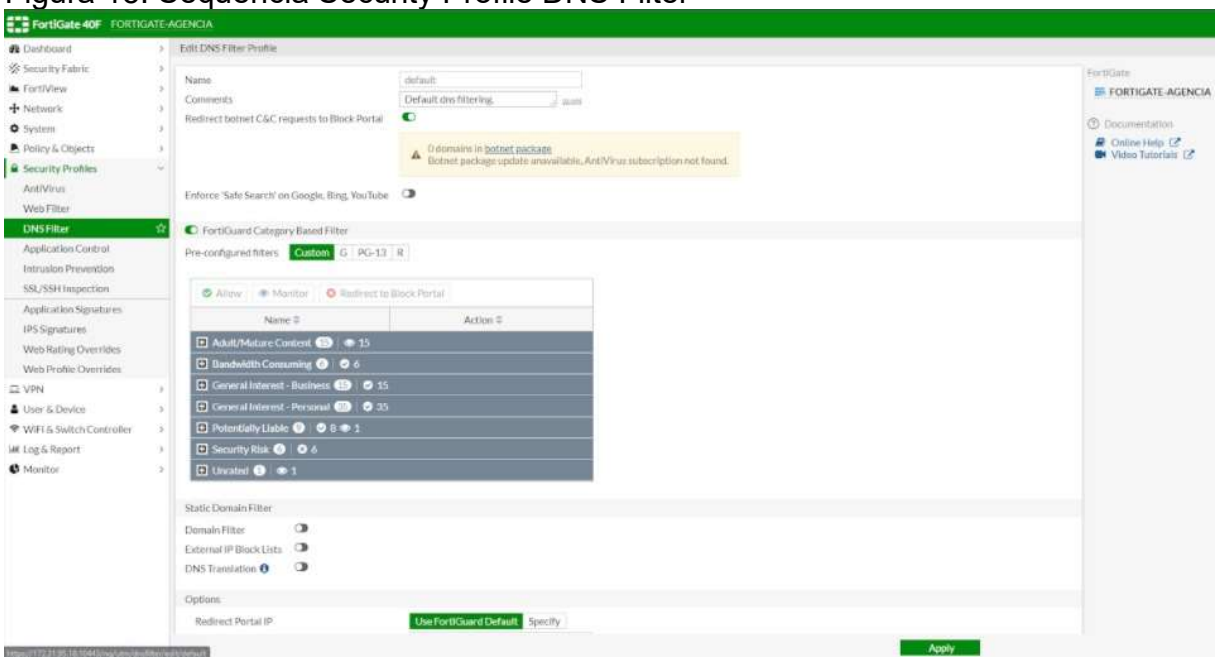
(Fonte: Do autor)

Figura 14: Security Profiles DNS Filter



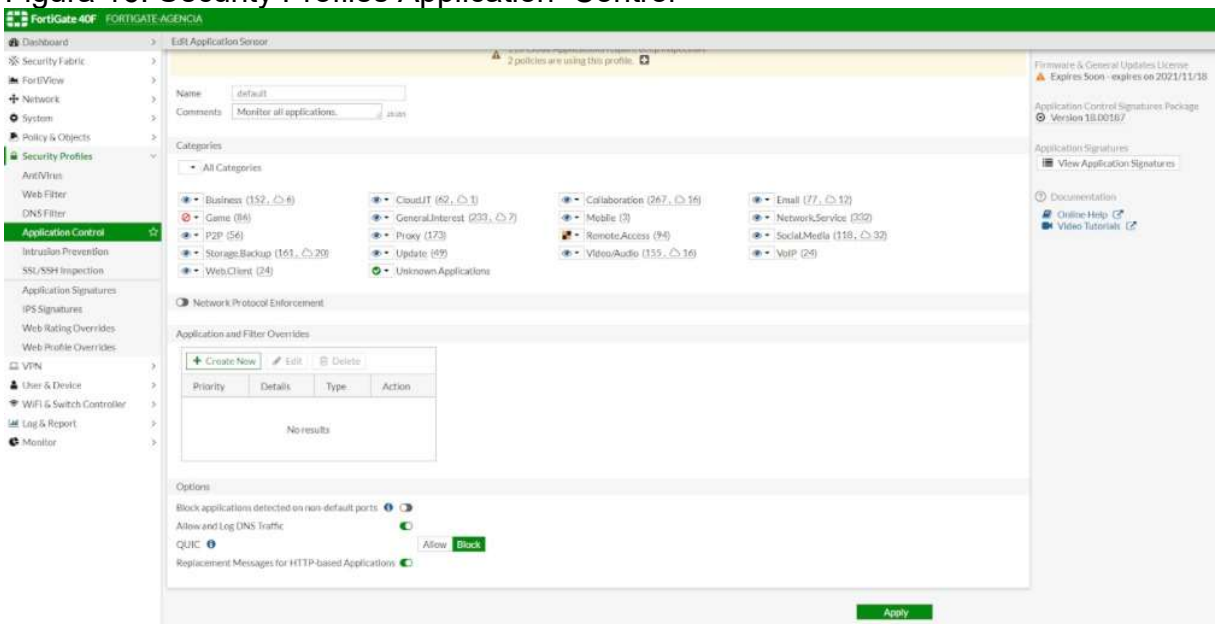
(Fonte: Do autor)

Figura 15: Sequencia Security Profile DNS Filter



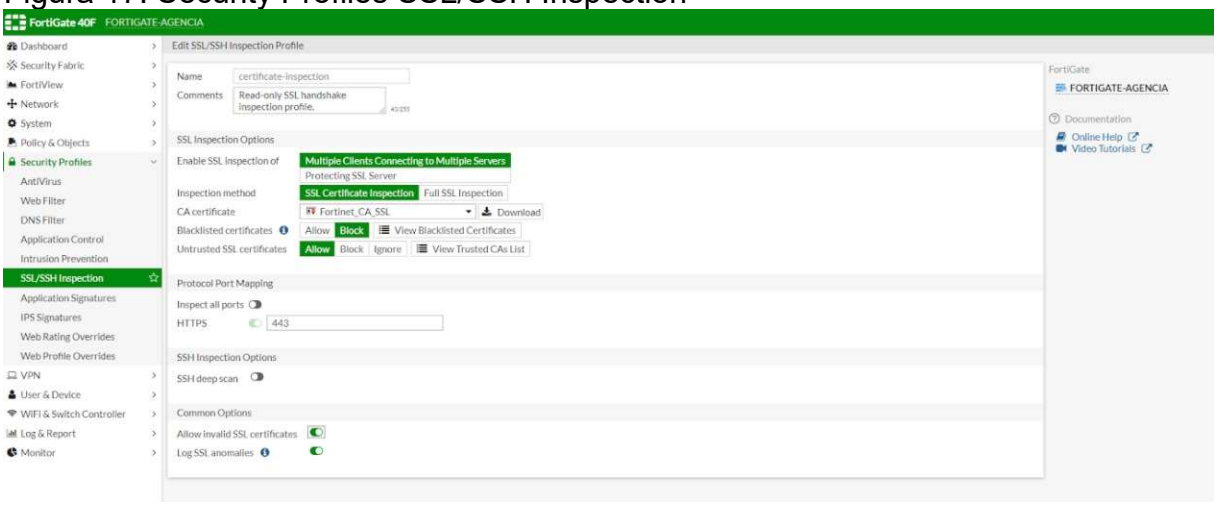
(Fonte: Do autor)

Figura 16: Security Profiles Application Control



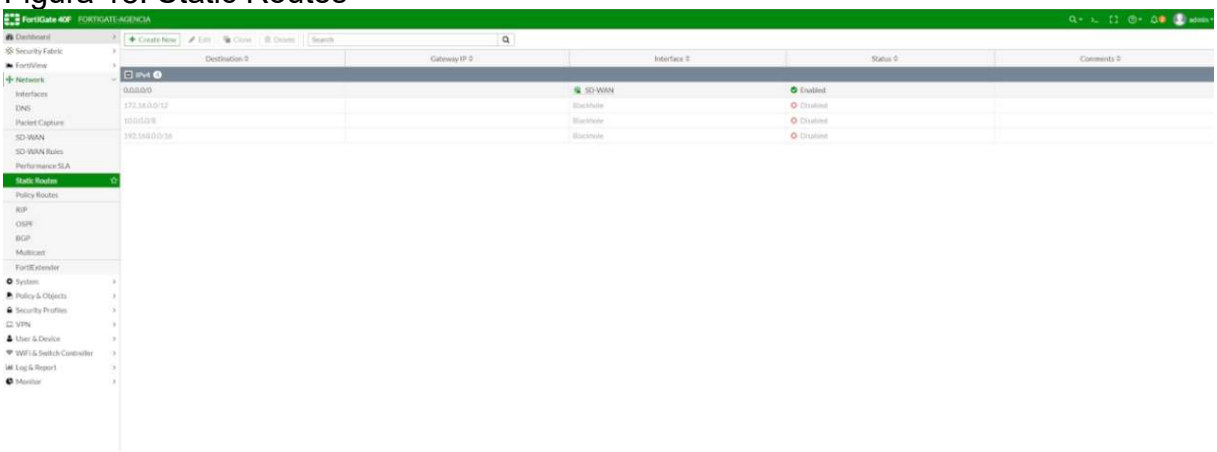
(Fonte: Do autor)

Figura 17: Security Profiles SSL/SSH Inspection



(Fonte: Do autor)

Figura 18: Static Routes



(Fonte: Do autor)

Figura 19: VPN

(Fonte: Do autor)

9 RECURSOS

Tabela 1 - Recursos	
Materiais	Recursos
Firewall	R$ 0 a R$ 5.000,00 ou mais
Internet	R$ 100,00
Total	Aproximadamente R$ 5.100,00

10 CRONOGRAMA

Tabela 2 - Cronograma

Mês	Atividade
Agosto	Apresentação da proposta para uma empresa ou pessoa em home office
Setembro	Teste com aplicabilidade do firewall adequado de acordo com a necessidade
Outubro	Pesquisa bibliográfica sobre potenciais falhas nas redes empresariais
Novembro	Verificação da funcionalidade do firewall de acordo com a pesquisa realizada
Dezembro	Conclusão e apresentação do trabalho

11 RESULTADOS ESPERADOS

Indiscutivelmente, a empresa só fica protegida quando consegue unir a segurança patrimonial física a todos os aspectos que também englobam as questões digitais. Contar com um firewall de qualidade deixou de ser um luxo para se tornar uma necessidade cada vez mais nítida no cotidiano das empresas. Com isso, como descrito neste trabalho, foi implantado um firewall em uma cooperativa de crédito e com isso obteve-se o aumento da segurança da rede na agência.

Os benefícios ao investir nessa área de proteção são inúmeros, entre eles o aumento da produtividade de profissionais internos e externos; melhora da qualidade de serviços e produtos; realização de objetivos e metas empresariais com mais facilidade; diminuição do tempo necessário para a execução de rotinas operacionais; eliminação de tarefas repetitivas por meio do aumento da automação interna; a redução de custos operacionais; o aumento da transparência; a eliminação de processos burocráticos; a maior flexibilização operacional; o aumento da capacidade de resposta a mudanças no mercado; ganho de market share por meio da melhora da competitividade; redução dos custos ambientais de toda a cadeia operacional e o aumento da segurança e diminuição do número de acidentes. (CESAR, Leonardo. Mundo Coop. 2021).

De acordo com as pesquisas realizadas durante a elaboração deste trabalho, talvez não haja a possibilidade de ficar completamente protegido, visto que até empresas de grande porte como a NASA, CIA e FBI já sofreram com a invasão de hackers. Entretanto, a segurança da informação é um sistema complexo com bases simples, sendo de suma importância estar em constante aprimoramento, erguendo barreiras e preenchendo possíveis brechas que surjam.

Para isso, o mercado de tecnologias de segurança em redes está em constante crescimento, havendo muitas ferramentas que podem ser utilizadas para combater problemas de segurança de qualquer espécie, apesar disso, muitas empresas de pequeno e médio porte possuem pouca ou nenhuma tecnologia de proteção. Espera-se que, com a pesquisa realizada, as empresas percebam a importância em proteger os dados das redes, que a vulnerabilidade pode ser substituída pela proteção, e a partir dessa conscientização, utilizem os métodos para a segurança das informações.

12 CONSIDERAÇÕES FINAIS

Com base no conhecimento adquirido durante esse processo de pesquisa e desenvolvimento, é certo que as empresas e as pessoas comuns hoje estão mais preocupadas com a segurança das informações que armazenam, fornecem e obtêm. Embora a maioria das pequenas e médias empresas tenha considerado os riscos e danos que podem ser causados por invasões, muitas delas ainda não investiram em segurança da informação.

Neste trabalho a respeito do conceito de segurança de rede de computadores, os três questionamentos feitos inicialmente agora podem ser respondidos, pois a segurança da informação é indispensável, com o intuito de prevenção, evitando possíveis danos, como os financeiros, integridade das informações em si e até mesmo de credibilidade.

Através da fundamentação, foi possível entender como reconhecer o melhor sistema de segurança a ser implantado, de acordo com a opção que mais se adeque ao perfil dos acessos da rede. Observa-se com o desenvolvimento desse projeto, que em um futuro próximo o investimento na segurança de informações e a capacitação de pessoas na área será muito maior por conta dos fatores apresentados.

Por fim, a implantação de firewall demonstrada tem como objetivo elucidar o funcionamento do firewall de última geração, e também demonstrar e fornecer uma base para trabalhos futuros, demonstrando outros software e hardware visando a segurança e controle de acesso, pois tende a um crescimento exponencial, com atualizações. Portanto, é cabível também para trabalhos futuros: A implementação de diferentes fornecedores de sistemas firewall; comparativos entre ramos de atuação diferente.

13 REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. Info Wester, 2013 **O que é firewall?**. Disponível em <http://www.infowester.com/firewall.php>.

GALLO, Michael A.; HANCOCK, W. M. **Comunicação entre Computadores e Tecnologias de Rede**. São Paulo, 2003

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. 2oedição. São Paulo: Futura, 2003.

PEREIRA, Jonathas Bitencourt; SOUZA, Marta Alves de; COSTA, Helder Rodrigues Da. **Segurança da informação em ambientes corporativos**. Disponível em <http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a29.pdf>.

ZANCANELLA, Luiz Carlos. **Segurança Computacional**. Graduação em Sistemas de Informação – INE – Universidade Federal de Santa Catarina (UFSC), 2006. Disponível em <http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-seg-redes/Cap6-Sniffers.pdf>.

ZOTTO, Fernando Derenievicz. **Segurança da informação: uma proposta para segurança de redes em pequenas e médias empresas**. Universidade Tecnológica Federal do Paraná – UTFPR. Curitiba, 2012. Disponível em <https://docs.google.com/file/d/0Bx7iZfTfN4y0MVpUQWQ2VlR0aGs/edit>.

CHESWICK, William R; BELLOVIN, Steven M.; RUBIN, Aviel D. **Firewalls e Segurança na Internet: repelindo o hacker ardiloso**. Tradução de Edson Furmankiewicz. 2.ed. Porto Alegre: Bookman, 2005.

FERREIRA, Rubem E. **Linux – Guia do Administrador do Sistema**. São Paulo: Novatec Editora Ltda, 2003.

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. **Segurança de Redes em ambientes cooperativos**. 2.ed. São Paulo: Futura, 2003.

PEREIRA, Marcio Machado. **Análise e estudo de segurança de corporações utilizando firewalls**. Espírito Santo: UFES, 2002. Monografia (Bacharelado em Ciência da Computação), Centro Tecnológico, UFES, 2002.

TELECO. **Rede de Computadores**. Disponível em <http://www.teleco.com.br/Curso/Cbrede/pagina_3.asp >. Acesso em: 03/06/2021

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. 2oedição. São Paulo: Futura, 2003.

PEREIRA, Jonathas Bitencourt; SOUZA, Marta Alves de; COSTA, Helder Rodrigues Da. **Segurança da informação em ambientes corporativos**. Disponível em <http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a29.pdf>.

MORIMOTO, Carlos E. **Redes, Guia prático**. Porto Alegre, 2010.