FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Leonardo Maiochi Fontanetti

Segurança da Informação em Redes Empresariais com *Firewall Netfilter*

Americana, SP

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Leonardo Maiochi Fontanetti

Segurança da Informação em Redes Empresariais com *Firewall Netfilter*

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do (a) Prof.(o) Dr. Renato Kraide Soffner

Área de concentração: Segurança da Informação

Americana, SP.

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

F759s FONTANETTI, Leonardo Maiochi

Segurança da informação em redes empresariais com firewall Netfilter. / Leonardo Maiochi Fontanetti. – Americana, 2018.

36f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Renato Kraide Soffner

1 Segurança em sistemas de informação I. SOFFNER, Renato Kraide II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Leonardo Maiochi Fontanetti

Segurança da Informação em Redes Empresariais com *Firewall Netfilter*

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 05 de Dezembro de 2018.

Banca Examinadora:

Renato Kraide Soffner (Presidente)
Doutor
Fatec Americana

Márcio Roberto Baldo Taglietta (Membro)
Especialista
Fatec Americana

Murilo Fujita (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, os quais contribuíram para a formação do meu caráter profissional e pessoal. A minha filha Júlia por ser minha motivação diária. E aos meus colegas de classe pela companhia nesses anos.

DEDICATÓRIA

Aos meus pais que me ensinaram o significado de ser um homem.

RESUMO

O presente texto conceitua a segurança da informação, seus pilares e principais ameaças enfrentadas pelas empresas nas redes de computadores atualmente. Demonstrando como desenvolver e aplicar uma política de segurança de informação para proteger os ativos computacionais da organização. Apresenta o uso da rede de computadores no ambiente empresarial, conceituando seus componentes, metodologia de funcionamento e principais configurações de uso. Conceitua o *Firewall* como dispositivo de promoção a segurança da informação, apresentando e diferenciando os principais tipos de *firewalls* disponíveis atualmente. Comenta o uso do f*irewall Netfilter,* presente nas distribuições Linux, suas aplicações, configurações e implementação. Finalizando a revisão bibliográfica com um estudo de caso, relacionando o apresentado sobre o f*irewall Netfilter* com sua aplicabilidade em uma empresa de pequeno porte. Realizando um estudo das informações apresentadas e trazendo o caso no qual será apresentado o problema e uma solução plausível. Considerando ao final, os resultados obtidos, discutindo a viabilidade de implementação da sugestão de solução.

Palavras Chave: Segurança da Informação, Redes Empresariais, *Firewalls*.

ABSTRACT

The present text conceptualizes the information security, its pillars and main threats faced by the companies in the computer networks today. Demonstrating how to develop and enforce an information security policy to protect the organization's computing assets. Presents the use of the computer network in the business environment, conceptualizing its components, operating methodology and main usage configurations. Conceptualizes Firewall as a device to promote information security, presenting and differentiating the main types of firewalls currently available. Discuss the use of Netfilter Firewall, present in Linux distributions, its applications, configurations and implementation. Finishing the bibliographic review with a case study, relationship the presented on the Netfilter Firewall with its applicability in a small business. Carrying out a study of the presented information and bringing the case in which the problem will be presented and a plausible solution. Considering at the end, the results obtained arguing the feasibility of implementing the solution suggestion.

Keywords*: Information Security, Enterprise Networks, Firewalls.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

TCP – Transmission Control Protocol
IP – Internet Protocol
DoS – Denial of Service
DDoS – Distributed Denial of Service
DNS – Domain Name Server
ISP – Internet Service Provider
ICMP – Internet Group Message Protocol
ARP – Address Resolution Protocol
RARP – Reverse Address Resolution Protocol
UDP – User Datagram Protocol
SCTP – Stream Control Transmission Protocol
HTTP – Hypertext Transfer Protocol
FTP – File Transfer Protocol
IMAP – Internet Message Access Protocol
ISO – International Organization for Standardization
OSI – Open System Interconnection
LAN – Local Area Network
MAN – Metropolitan Area Network
WAN – Wide Area Network
NAT – Network Address Translation
DHCP – Dynamic Host Configuration Protocol
VDI – Virtualbox Disk Image

1 INTRODUÇÃO

O presente trabalho teve como objetivo geral analisar o uso do *firewall Netfilter* em uma rede empresarial de computadores, com foco em promover a segurança da informação.

Como objetivos específicos pode-se encontrar a conceituação da segurança da informação, bem como as principais ameaças e vulnerabilidades presentes em uma rede de computadores atualmente. A apresentação do desenvolvimento e implantação de uma política de segurança da informação. A contextualização da segurança da informação aplicada à rede de computadores no ambiente empresarial, bem como seu método de funcionamento e configurações de uso. Além disso, conceituar e diferenciar os principais tipos de *firewall*, suas aplicações e configurações, com foco no uso do *firewall Netfilter* para então aplicar os conceitos estudados em um estudo de caso, identificando o problema e apresentando uma sugestão plausível de solução.

O método científico utilizado foi a pesquisa descritiva, com fins práticos. Realizando uma abordagem de natureza qualitativa, baseada na análise da literatura conceitual do tema. Aplicando o método hipotético dedutivo, utilizando procedimentos de revisão bibliográfica, análise de documentos e demonstrando um estudo de caso.

Apesar da crescente relevância do tema segurança da informação e dos elevados custos relacionados a resposta a um incidente. Por vezes, este assunto tem sido negligenciado pelas empresas, principalmente as de pequeno porte. Não sendo incomum, a existência de empreendedores que há pouco tempo iniciaram pequenos negócios e não tem nenhum método de defesa a ataques cibernéticos ou política de segurança da informação. Para desta forma prevenir e combater, possíveis invasões, roubo e extravio de dados. Sendo as consequências destes atos negativas, com impactos financeiros e à imagem da organização. Com grande parte dos empreendedores ainda considerando os gastos com tecnologia e segurança da informação, um custo adicional sem justificativa. Além disso, recentemente a Kaspersky Lab publicou um estudo que aponta o Brasil como nono pais que mais sofre ataques de *hackers* em todo o mundo. Um estudo da Fiesp de 2015, indicou que 65,2% dos ataques cibernéticos envolviam pequenas e médias empresas (ESTADÃO SEGURANÇA DIGITAL, 2017). Em vista desses fatos, o presente

trabalho analisou uma alternativa de baixo custo, que pode proporcionar resultados expressivos, no que diz respeito a proteger uma rede empresarial contra tentativas de ataques maliciosos. Com o uso de uma ferramenta de *software* livre, que possui documentação e passo a passo de implementação, facilmente encontrada na rede mundial de computadores. Visando assim, demonstrar a facilidade de implantação e os inúmeros benefícios oferecidos pela aplicação de um *firewall* de *software* livre em uma rede empresarial. Diminuindo as vulnerabilidades desta e assim, não expondo a riscos um dos mais valiosos ativos de qualquer organização, a informação.

No capítulo dois, o tema segurança da informação foi abordado, conceituando-o, bem como seus principais pilares. As principais questões relacionadas às ameaças e vulnerabilidades são expostas e em seguida os passos para elaboração e implantação de uma política de segurança da informação foram explicados. No capítulo três, as redes de computadores, bem como seus principais componentes e meios de funcionamento são desenvolvidos. As camadas de protocolos de rede são relacionadas a suas principais funções e um breve resumo de cada uma delas foi realizado. Em seguida as redes empresariais são categorizadas de acordo com sua abrangência e topologia, os principais pontos positivos e negativos de cada uma das topologias são explanados. Ainda neste capítulo o *firewall*, como dispositivo de promoção a segurança da informação é conceituado, e a diferenciação entre os principais tipos é realizada. O uso do *firewall Netfilter* presente nos *kernels* das distribuições Linux é aclarado, bem como os principais comandos utilizados para realizar sua configuração. Em seguida, no capítulo quatro, um estudo de caso foi realizado para aplicar o uso do *firewall,* afim de solucionar um problema de vulnerabilidade na rede de uma empresa de consultoria contábil. O trabalho é finalizado, com uma conclusão que analisou os resultados obtidos, bem como sua viabilidade de aplicação.

2 A SEGURANÇA DA INFORMAÇÃO

Desde a revolução industrial até aos efeitos recentes causados pela tecnologia da informação aplicada aos negócios, é possível identificar a informação desempenhando um papel de suma importância na gestão de negócios. A mesma tem sido utilizada para obtenção de vantagem estratégica independente do ramo de atuação da empresa, desde a otimização de processos, aumento da produtividade, ganho de mercado, até ao apoio a tomada de decisão. Em todos os segmentos de mercado ela, já demonstrou vital importância na obtenção de diferencial competitivo (SÊMOLA, 2003).

Após a globalização as organizações têm enfrentado o maior nível de competitividade da história. Concorrentes podem existir em qualquer parte do mundo e a busca pela produção de produtos de qualidade, prestação de serviços com excelência, bem como velocidade, qualidade e eficiência nas comunicações, sejam de vital importância para o triunfo da organização em meio ao mercado competitivo. O uso de tecnologias inovadoras deixou de ser um diferencial e se tornou questão de sobrevivência para qualquer nicho de mercado, sejam elas utilizadas para desenvolvimento de novos produtos ou para estabelecimento de canais de relacionamento com os clientes (NAKAMURA; GEUS, 2007).

Rezende e Abreu (2013) conceituam a informação e a diferencia do dado, sendo que a:

> "[...] informação é todo o dado trabalhado, útil, tratado, como valor significativo atribuído ou agregado a ele e com sentido natural e lógico para quem usa a informação. O dado é entendido como um elemento da informação, um conjunto de letras, números ou dígitos, que, tomando isoladamente, não transmite nenhum conhecimento, ou seja, não contém um significado claro."

Fontes (2010) também afirma que a informação é mais que um conjunto de dados, são recursos de valor, diz ser o recurso que move o mundo e que os indivíduos são o que são porque transformam informação em vida. Defende que as organizações precisam valorizar e proteger a informação da mesma forma com que o fazem com recursos financeiros e materiais. Por se tratar de um recurso crítico para a realização do negócio, o acesso à informação deve possuir regras e procedimentos. Desta forma define a segurança da informação como um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por

objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão alcançada. Para que este objetivo seja alcançado, faz-se necessário o uso dos pilares da segurança da informação, sendo eles:

- Disponibilidade: a informação precisa ser acessível, estar disponível sempre que necessário.
- Integridade: a informação precisa ser integra, correta, verdadeira, não faltando nem sendo acrescentado nenhum dado a mesma.
- Confidencialidade: a informação deve ser acessível única e exclusivamente àqueles a quem ela diz respeito, e para aqueles que receberam autorização prévia para o acesso.
- Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentada e licenciada. Além de ser conforme aos princípios éticos da organização e sociedade.
- Auditabilidade: todo acesso a informação precisa ser registrado, possibilitando identificar a quem o realizou.
- Não repúdio: aquele que criou ou alterou a informação não deve ser capaz de negar o fato.

Sêmola (2003) ainda defende que a informação precisa ser protegida de maneira adequada em todo o seu ciclo de vida, e que se em algum momento deste ciclo, ela estiver vulnerável a uma ameaça potencial, um indecente poderá ocorrer. Para ele existem quatro momentos que merecem atenção especial no ciclo de vida da informação, sendo:

1. Manuseio: momento em que a informação é criada e manipulada, pode ser ao folhear um maço de papel, digitar um texto, inserir uma senha de acesso a um sistema computacional.
2. Armazenamento: momento em que a informação é armazenada, seja em um banco de dados, ou em pedaço de papel guardado em um arquivo de metal.
3. Transporte: momento em que a informação é transportada, ao enviar um e-mail, um fax, uma carta pelo correio, ou ao falar no telefone sobre um assunto confidencial.
4. Descarte: momento em que a informação é descartada, ao jogar um pedaço de papel na lixeira, ou se desfazer de um CD-ROM, mesmo quando este apresenta falha na leitura.

2.1 AMEAÇAS E VULNERABILIDADES

Laureano (2005), conceitua a ameaça como uma potencial violação de segurança, que apenas poderá existir se houver uma vulnerabilidade a ser explorada, e suas consequências incluem divulgação, usurpação, decepção e rompimento. E as classifica como:

- Naturais: decorrentes de fenômenos da natureza, como enchentes, terremotos, tempestades, etc.
- Involuntárias: inconscientes, causadas pelo não conhecimento, de maneira não proposital. Podem ser causadas por erros, falhas, acidentes, etc.
- Voluntárias: propositais causadas por agentes humanos como *hackers*, espiões, ladrões, etc.

Ele também diferencia a ameaça inteligente, onde um adversário possui o conhecimento e as ferramentas técnicas adequadas para detectar e explorar uma vulnerabilidade de um sistema, da ameaça de análise. Sendo esta última, como o nome sugere, uma análise das ocorrências e consequências de ações prejudiciais a um sistema.

Oliveira (2003), classifica os principais atacantes a sistemas de informação como *hackers* e *crackers*. Identificando o *hacker* como aquela pessoa que tem muito conhecimento sobre sistemas de informação, redes, sistemas operacionais. Sendo extremamente especializado nesta área, o que faz com que tenha facilidade para identificar vulnerabilidades e utiliza as mais variadas técnicas para explorá-las. O *cracker,* entretanto, possui o mesmo conhecimento que o *hacker*, contudo após conseguir um acesso não autorizado, este geralmente deixa alguma marca ou recado, danifica ou destrói informações ou partes de sistemas. Aos *crackers* também é atribuída a retirada de sistemas de controle, contra cópias não autorizadas de sistemas, por isso estão diretamente ligados a “pirataria”.

Desta forma classifica as ameaças pelos principais tipos de intrusos, sendo:

- Curioso: aquele que se interessa pelo tipo de dado presente no sistema.
- Malicioso: aquele que desejar destruir dados, documentos, e evitar que serviços continuem a ser ofertados, como por exemplo em um ataque a um *webserver*.

- Intruso de alto nível: intruso que deseja apenas obter popularidade demonstrando suas habilidades.
- Concorrente: aquele que quer conhecer os dados para obter alguma vantagem estratégica ou lucro.

Oliveira (2003), classifica e explica os principais tipos de ataques, sendo:

- *Spoofing:* o invasor convence alguém da organização que ele é algo ou alguém que não é, desta forma consegue autenticação para acesso a algum sistema ou rede, falsificando seu endereço de origem.
- *Sniffers:* um programa de computador que monitora o tráfego de dados na rede. Este tipo de programa pode ser utilizado legitimamente por um administrador da rede. Nestes casos o intruso se aproveita do fato de os pacotes TCP/IP não serem criptografados e assim consegue nome de usuários e senhas, para acessos não autorizados.
- Ataques de negação de serviço (DoS – *denial of service*): tem por objetivo, como o nome sugere, impedir que um serviço seja ofertado durante um período de tempo. Nestes casos, atacantes forçam o sistema ao limite com um grande número de requisições ou o induzindo a falha. Por exemplo um *site* de uma empresa que recebe um número de acessos maior que o seu servidor pode suportar.
- Ataques de DDoS *(destributed denial of service)*: semelhante ao ataque de negação de serviço, porém neste caso a origem está espalhada por milhares de pontos disparando ataques DoS.
- DNS *Spoofing*: tem por finalidade destruir o servidor de nomes e assim permitir que máquinas não confiáveis se passem por confiáveis. Para tanto o invasor precisa de acesso ao servidor de DNS (*Domain Name Server*) desta forma ele obterá os nomes e endereços IP das máquinas da rede. Assim ele pode alterar o nome e IP da máquina do invasor para um nome e IP de uma máquina confiável.
- Quebra de senhas: o invasor tenta descobrir a senha utilizada para acesso ao sistema. Nesta técnica são utilizadas senhas padrão de dispositivos, nomes de pessoas, datas entre outros. Existem programas especializados neste tipo de ataque com dicionários de senhas. Que testam inúmeras combinações de nome de usuário e senha até obterem o acesso.

- Vírus: são programas de computador que se reproduzem e tem por objetivo danificar os arquivos da rede, um exemplo desse tipo de programa são os chamados *worms*. Além desse, outro tipo de vírus muito conhecido é o *trojan*, ou cavalo de Tróia, este insere um pedaço de código num programa inofensivo colocando um hospedeiro no sistema alvo, permitindo que o invasor controle a máquina da vítima.

Sobre as vulnerabilidades, Laureano (2005) explica que é o ponto onde os sistemas são suscetíveis aos ataques, sejam eles recursos, processos, configurações. Diz também que todos os ambientes são vulneráveis, e que este fator está presente no dia a dia das organizações, não existindo apenas uma única causa para o surgimento das mesmas. Sendo as vulnerabilidades a principal causa de ocorrências de incidentes de segurança nas empresas. Quando uma vulnerabilidade é explorada causando um incidente de segurança, o negócio da empresa pode ser afetado, impactando negativamente clientes, produto e a imagem da empresa.

Segundo Laudon e Laudon (2004), *apud* Laureano (2005), os sistemas de armazenamento de informação eletrônicos são mais vulneráveis que os de formato manual, devido ao fato de sistemas de informação estarem interconectados por meio de redes e desta forma a ameaça poderá estar localizada em qualquer ponto da rede. Estando susceptível a falhas de *software* e *hardware*, uso indevido por programadores, pessoal de manutenção e usuários finais.

Defende que a Internet é especialmente vulnerável pois foi projetada para ser de fácil acesso, por qualquer pessoa utilizando diferentes tipos de sistemas em qualquer lugar do mundo.

2.2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Ferreira e Araújo (2006) defendem que para garantir que as informações e serviços oferecidos por uma empresa, sejam corretamente protegidos das ameaças e vulnerabilidades existentes na rede, faz-se necessário implementar uma política de segurança da informação. Sendo esta um conjunto de normas, métodos, procedimentos, que são utilizados na manutenção da segurança da informação. Para atingir este objetivo, contudo é preciso que em sua elaboração, se utilize de uma visão criteriosa, metódica e técnica. Garantindo que a política tenha o perfil da organização e expresse os anseios dos proprietários ou acionistas, responsáveis por

decidir os destinos de todos os recursos da organização, dentre eles o uso da informação por todos os que têm acesso a ela. Sendo imprescindível que na elaboração da política de segurança da informação da empresa haja, o estabelecimento do conceito da informação como um ativo importante para organização, exista o envolvimento da alta administração da empresa. E defina de forma clara e formal, qual o papel dos colaboradores da empresa na salvaguarda da informação. Estabelecendo padrões para manutenção da segurança da informação.

Também é importante para o sucesso da implantação da política, que a mesma seja formalizada preferencialmente antes que um incidente de segurança ocorra, tendo um escopo bem definido, pois o que precisa ser protegido está além de *softwares* e *hardwares*, abrangendo pessoas e processos de negócios. Para isto recomenda a formação de um comitê de segurança da informação, composto de vários profissionais de diversos departamentos da empresa. Este comitê tem por função, catalogar e agrupar todas as informações da empresa por categorias e atribuir a cada uma dessas categorias um proprietário, responsável pelo controle de acesso, manuseio e segurança em geral.

Para garantir o sucesso e aderência, as políticas precisam ser simples e compreensíveis, homologadas pela alta administração da empresa, estruturada de forma a permitir sua implantação em fases, alinhadas com a estratégia da empresa, orientadas aos riscos, flexíveis e moldáveis aos requerimentos de tecnologia e negócios, protetoras de ativos de informação, priorizando o de maior valor, positivas e não concentradas em ações proibitivas e punitivas.

Ferreira e Araújo (2006), dividem as etapas de desenvolvimento e implantação de uma política de segurança da informação em fases, conforme sugere a Tabela 1:

Tabela 1 – Fases de desenvolvimento e implantação de uma política de segurança da informação

FASES	DESCRIÇÃO
FASE I	**Levantamento de informações**
1.1	Obtenção dos padrões, normas e procedimentos de segurança já existentes para análise.
1.2	Entendimento das necessidades e uso dos recursos da tecnologia da informação (sistemas, equipamentos e dados) nos processos de negócios.
1.3	Obtenção de informação sobre os ambientes de negócios: • Processos de negócios; • Tendências de mercado; • Controles e área de riscos.
1.4	Obtenção de informações sobre o ambiente tecnológico: • Workflow em ambientes;

	• Redes de aplicações; • Plataformas computacionais.
FASE II	**Desenvolvimento do conteúdo das políticas e normas de segurança**
2.1	Gerenciamento da política de segurança: • Definição da segurança da informação; • Objetivo do gerenciamento; • Fatores críticos de sucesso; • Gerenciamento da versão e manutenção da política; • Referência para outras políticas, padrões e procedimentos.
2.2	Atribuição de regras e responsabilidades: • Comitê de segurança da informação; • Proprietário das informações; • Área de segurança da informação; • Usuários de informações; • Recursos humanos; • Auditoria interna.
2.3	Critérios para classificação das informações: • Introdução; • Classificando a informação; • Níveis de classificação; • Reclassificação; • Armazenamento e descarte; • Armazenamento e saídas.
2.4	Procedimentos de segurança de informações: • Classificação e tratamento das informações; • Notificação e gerenciamento de incidentes de segurança da informação; • Processo disciplinar; • Aquisição e uso de *hardware* e *software*; • Proteção contra *software* malicioso; • Segurança e tratamento de mídias; • Uso da Internet; • Uso de correio eletrônico; • Utilização dos recursos de TI; • Backup; • Coleta e registro de falhas; • Gerenciamento e controle da rede; • Monitoração do uso e acesso aos sistemas; • Uso de controles de criptografia e gerenciamento de chaves; • Controle de mudanças operacionais; • Inventário dos ativos de informação; • Controle de acesso físico às áreas sensíveis • Segurança física; • Supervisão de visitantes e prestadores de serviço.
FASE III	**Elaboração dos Procedimentos de Segurança da Informação**
3.1	Pesquisa sobre as melhores práticas em segurança da informação
3.2	Desenvolvimento de procedimentos e padrões, para discussão com a Alta Administração, de acordo com as melhores práticas de mercado e com as necessidades e metas da organização.
3.3	Formalização dos procedimentos para integrá-los às políticas corporativas
FASE IV	**Revisão, Aprovação e Implantação das Políticas, Normas e procedimentos de segurança da informação**
4.1	Revisão e aprovação das políticas, normas e procedimentos de segurança da informação.
4.2	Efetiva implantação das políticas, normas e procedimentos de segurança da informação por meio das seguintes iniciativas: • Atuação junta à área responsável pela comunicação, ou área correspondente, na

	orientação para a preparação do material promocional, de divulgação e de consulta; • Divulgação das responsabilidades dos colaboradores às políticas, normas e procedimentos de segurança da informação desenvolvidas, tendo por público-alvo a Presidência, Diretorias e Gerências; • Realização de palestras referentes às políticas, normas e procedimentos de segurança, tendo por público-alvo outros colaboradores da organização.

Adaptado de Ferreira e Araújo (2006)

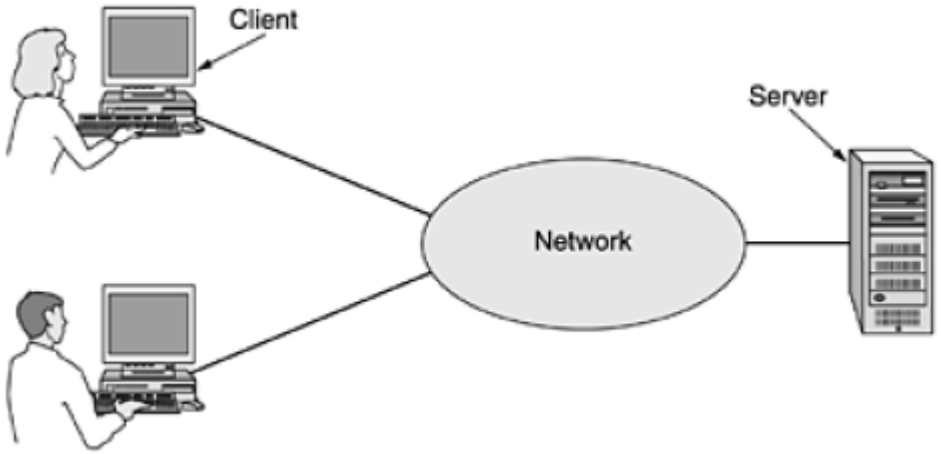
Fontes (2008), explica que o objetivo da implementação de uma política de segurança da informação deve ser o de definir o tratamento que será dado às informações armazenadas, processadas ou transmitidas no ambiente organizacional. Sendo que a mesma deverá se aplicar a todos os que utilizam a informação, desde funcionários e estagiários a prestadores de serviços. Defende também a criação de uma área de gerenciamento da segurança da informação, que deverá coordenar as demais áreas e em conjunto com elas desenvolver e implementar projetos e processos para operacionalização desta política. Cada informação deverá possuir o seu gestor, indicado formalmente pela diretoria da empresa, sendo o gestor da informação a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação. A autorização de acesso a informação deverá ser realizada levando-se em consideração a confidencialidade da mesma e a necessidade de acesso do usuário.

Conclui que a segurança e proteção da informação é de responsabilidade contínua de cada usuário. Deste modo a utilização da informação no ambiente empresarial, precisa estar conforme a política de segurança implementada na empresa. Todos os usuários devem conhecer e entender este documento e o não cumprimento desta política deve constituir falta grave sujeitando o usuário a penalidades administrativas e contratuais. Ele também atribui a gerencia de segurança da informação a responsabilidade pela existência efetiva de um processo de proteção a informação da organização.

3 AS REDES DE COMPUTADORES

O compartilhamento de recursos especificamente dados e informações, em uma rede corporativa é explicado por Tanembaum (2003). Segundo ele, atualmente, a maioria das empresas possuem diversos computadores, sendo que em alguns deles encontramos informações sobre clientes, em outros, informações financeiras e em outros, ainda, sobre folhas de pagamentos. A rede permite principalmente que as informações sejam compartilhadas, facilitando a extração e a sua correlação, tornando possível que todos os programas e recursos da organização estejam disponíveis para todos os usuários independente de sua localização física. Assim, empresas com atuação global podem ter fácil acesso às informações em qualquer lugar do mundo. Entretanto, para que isso seja possível, é necessário que essas informações sejam armazenadas em bancos de dados, presentes em computadores potentes, chamados de servidores. Essas máquinas, estão frequentemente localizadas em centros estratégicos e são mantidas por administradores especializados. Assim, os usuários finais podem dispor apenas de um dispositivo mais simples, chamado de cliente, com o qual acessam e compartilham informações disponibilizadas no servidor. As máquinas clientes são conectadas ao servidor através de uma rede, conforme a Figura 1. A este modelo de trabalho, é dado o nome de cliente/servidor.

Figura 1 - Uma rede com dois clientes e um servidor



Fonte: Tanenbaum (2003)

Este modelo é utilizado tanto em redes locais, onde tanto os clientes quanto o servidor estão fisicamente no mesmo prédio, quanto em clientes e servidores que estão a uma grande distância. Neste último caso, a conexão cliente/servidor poderá ser estabelecida através da Internet como acontece, por exemplo, nos casos em que um usuário acessa uma página na World Wide Web*,* em um servidor *web.*

De maneira simplificada, a comunicação entre as duas máquinas se dá através de processos. Um processo na máquina cliente envia uma solicitação ao servidor e aguarda por uma resposta, o servidor por sua vez recebe a solicitação e pode tanto processá-la quanto realizar uma busca pelos dados solicitados e então encaminhar a resposta para a máquina cliente.

Além do compartilhamento de informações, a comunicação via rede, com uso de *e-mail*, vídeo conferência e aplicativos de mensagens instantâneas, a realização de negócios com outras empresas, especialmente nos casos entre cliente e fornecedores e o comércio pela Internet, são os principais objetivos da configuração e utilização de uma rede de computadores.

3.1 COMPONENTES DE REDE

Segundo Kurose e Ross (2010), a Internet é uma rede de computadores que incialmente era composta por “computadores de mesa, estações de trabalho Linux e os assim chamados servidores que armazenam e transmitem informações[...]” Atualmente, porém, a rede mundial de computadores é composta pelos mais diversos dispositivos finais, de computadores domésticos, passando por televisões e consoles de jogos, até dispositivos móveis como celulares e *notebooks*.

Estes dispositivos são interligados por enlaces, que podem ser cabos coaxiais, cabos de cobre, fibra ótica e ondas de rádio. O material de fabricação destes componentes influencia na velocidade e qualidade de conexão.

Quando uma informação precisa ser enviada de um dispositivo final a outro, ela é segmentada em pequenos pedaços de dados aos quais são adicionados *bytes* de cabeçalho. Estes segmentos recebem o nome de pacotes e são enviados através do enlace ao dispositivo final onde são reagrupados e ordenados na informação original.

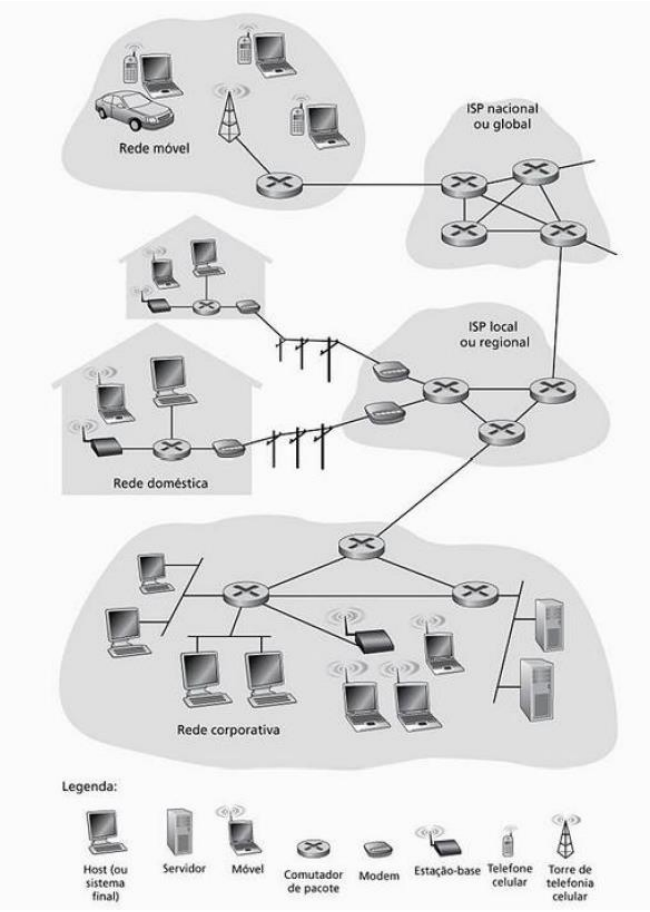
Para encaminhar os pacotes aos dispositivos finais adequados, entre os dispositivos de origem e destino, existem componentes de redes denominados

comutadores de pacotes. Estes têm por função receber os pacotes através de seu enlace de entrada, e encaminhar o pacote ao seu destino através de seu enlace de saída. Atualmente são utilizados dois tipos principais de comutadores de pacotes: os roteadores, utilizados principalmente no núcleo da rede, e os comutadores de camada de enlace (*switchs*), utilizado principalmente em redes de acesso. O caminho que um pacote percorre entre o dispositivo de origem, passando por todos os comutadores até chegar ao destino, é denominado rota.

Os dispositivos finais se conectam à rede por meio de ISP's *(Internet service provider)*, de baixo nível, como por exemplo empresas provedoras de TV a cabo e telefonia, estas se conectam a ISP's de alto nível, nacionais e internacionais afim de garantir que o pacote seja entregue ao seu dispositivo de destino.

A Figura 2, ilustra alguns componentes da rede mundial de computadores.

Figura 2 - Alguns componentes da Internet



Fonte: Kurose e Ross (2010)

Todos os componentes da rede executam protocolos que controlam o envio e recebimento de informações, como exemplo o TCP (*Transmission Control Protocol* –

Protocolo de controle de transmissão) e o IP (*Internet Protocol* – Protocolo da Internet). Estes dois protocolos figuram entre os mais importantes e utilizados entre os protocolos de comunicação de rede e por isso nomeiam o conjunto de camadas de protocolos mais utilizados nos dias de hoje, as camadas de protocolos TCP/IP. Este conjunto de camada de protocolos será melhor explicado na próxima sessão deste trabalho.

3.2 CAMADAS DE PROTOCOLOS DE REDES

Kurose e Ross (2010) explicam o que é um protocolo, fazendo uma analogia com a comunicação humana. Quando é necessário perguntar as horas a uma pessoa, primeiro dizemos “oi”, se a pessoa responde cordialmente com um “oi”, então segue-se o protocolo humano e pode-se perguntar as horas. Se após o “oi” inicial é emitido uma resposta grosseira, verifica-se que a pessoa não fala a mesma língua que a que perguntou ou nenhuma resposta é recebida, entende-se que de acordo com o protocolo humano, que não será possível perguntar as horas. Algo muito semelhante acontece com os protocolos de rede. Por exemplo, se é necessário visualizar uma página da Internet. Digita-se um endereço em um navegador de Internet, e um computador pessoal envia uma mensagem ao servidor que hospeda a página que desejasse visualizar, solicitando uma conexão. O servidor *Web* devolve uma mensagem informando que a conexão poderá ser estabelecida, o computador pessoal então entende que está tudo certo para realizar a conexão. Neste momento, uma solicitação pela página da Internet que deseja-se visualizar é enviada a partir do computador pessoal. O servidor *Web* recebe a solicitação e envia a página para o computador pessoal que a exibe na tela.

Embora o exemplo acima seja bastante simples, existem dezenas de protocolos de rede. Com o intuito de organizá-los, otimizar sua compreensão e utilização, o modelo de protocolos por camadas foi criado. Kurose e Ross (2010) demonstram que os protocolos são agrupados em camadas e cada camada tem foco no serviço que é disponibilizado a camada superior. Estes protocolos podem ser implementados tanto em *hardware* quanto em *software* e algumas vezes em uma combinação dos dois. O conjunto de protocolos agrupados em pilhas de protocolos é formado por cinco camadas: física, de enlace, de rede, de transporte e de aplicação. Kurose e Ross (2010) afirmam que:

> "[...] a divisão em camadas proporciona um modo estruturado de discutir componentes de sistemas. A modularidade facilita a atualização desses componentes. Devemos mencionar, no entanto, que alguns pesquisadores e engenheiros de sistema se opõem veementemente ao sistema de camadas. Uma desvantagem potencial desse sistema é que uma camada pode duplicar a funcionalidade de uma camada inferior."

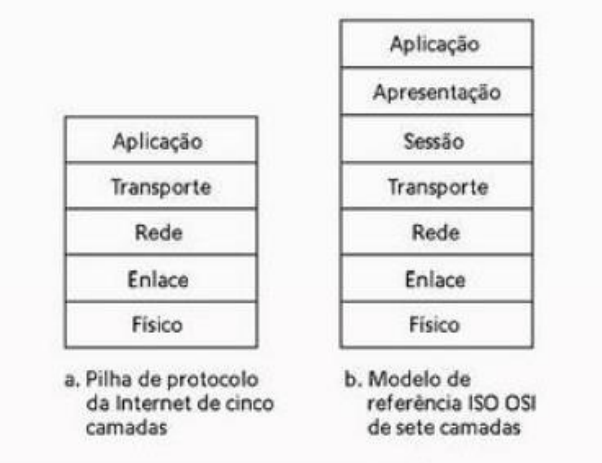
Forouzan (2010) relaciona cada camada a seus principais protocolos da seguinte forma:

- Camadas física e de enlace: nestas camadas não são definidos nenhum protocolo específico, elas apenas suportam os protocolos padrão.
- Camada de rede: esta camada suporta o protocolo IP (*Internet Protocol*), mecanismo de transmissão com menor esforço que não verifica ou controla erros, tem por foco que a transmissão chegue ao destino, mas sem garantias. O IP transporta dados em pacotes chamados de datagramas, não monitorando as rotas e sem recursos para reordená-los. O ICMP (*Internet Group Message Protocol*) protocolo utilizado para enviar notificação de problemas de datagramas aos remetentes. Envia mensagens de consultas e relatórios de erros. Além desses dois importantes protocolos, o ARP utilizado para associar um IP ao um endereço físico, RARP que permite que o host descubra seu endereço na transmissão de mensagens simultâneas a um grupo de destinatários, também estão presentes na camada de rede.
- Camada de transporte: é tradicionalmente representada pelos protocolos TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*). Sendo que o TCP é o protocolo mais confiável pois possui mecanismos de garantia de entrega de pacotes, e é orientado a conexão, o que significa que uma conexão precisa ser estabelecida antes do início da transmissão. Os pacotes neste protocolo são chamados de segmentos que recebem uma sequência numérica para ordenação no destino. O UDP é um protocolo mais simples, não orientado a conexão, que adiciona apenas um endereço e porta, controle de erro e soma de verificação e informação de comprimento de dados para a camada superior. Além desses o SCTP é um protocolo relativamente novo, para suporte a novas aplicações que combinam bons recursos do TCP e do UDP.
- Camada de aplicação: Muitos protocolos são definidos nesta camada, como por exemplo o HTTP (*Hypertext Transfer Protocol*) protocolo base para comunicação de dados na *World Wide Web*, o FTP (*File Transfer Protocol*) utilizado

na transferência de arquivos via rede, IMAP (*Internet Message Access Protocol*), um protocolo de gerenciamento de correio eletrônico, entre outros.

O modelo de camadas TCP/IP no entanto não é o único existente, no final dos anos 70, a Organização Internacional para Padronização (ISO), propôs um modelo de 7 camadas de protocolos, denominada Interconexão de Sistemas Abertos (OSI). O modelo OSI, como é conhecido, surgiu quando os protocolos para Internet ainda estavam em amadurecimento e seus criadores provavelmente não tinham em mente que esses protocolos seriam mais tarde utilizados na rede mundial de computadores. As instituições de ensino na época perceberam que o modelo proposto provavelmente ganharia notoriedade, devido a exigência da ISO e incluíram cursos a respeito do mesmo em suas grades curriculares, razão pela qual até hoje este modelo é abordado na literatura e em cursos sobre redes (KUROSE; ROSS, 2010). A Figura 3 demonstra as 7 camadas do modelo OSI em relação as do TCP/IP:

Figura 3 - A pilha de protocolo da Internet e o modelo de referência OSI



Fonte: Kurose e Ross (2010)

3.3 REDES EMPRESARIAIS

Forouzan (2008) categoriza as redes de acordo com sua abrangência. Uma rede local (LAN – *local área network*), normalmente cobre uma área pequena, de até 3 quilômetros. Este tipo de rede é privada e interliga dispositivos em uma organização, sua complexidade depende do tipo de tecnologia utilizada e da necessidade da organização a que pertence. Pode ser muito simples e interligar apenas dois computadores e uma impressora, ou se estender por toda uma

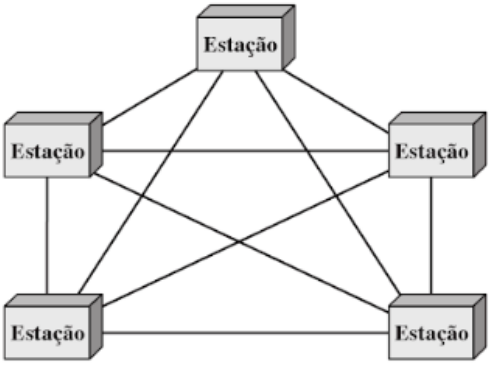
empresa, conectando diversos dispositivos dos mais variados tipos, como periféricos de áudio e vídeo. Elas são projetadas para que recursos computacionais possam ser compartilhados entre estações de trabalho, recursos estes que podem ser *hardware*, *software* ou dados. Uma função comum encontrada em redes empresariais é a de interligar grupos de trabalhos de departamentos como engenharia e contabilidade. Nestes casos, um dos computadores pode receber um *hardware* de maior capacidade e abrigar um *software*, que será utilizado por todo o departamento através da rede. As primeiras LANs tinhas taxa de transmissão de 4 a 16 megabits por segundo. Hoje, porém as velocidades chegam a 1000 megabits por segundo. As redes de tamanho intermediários, conhecidas como redes de abrangência metropolitana (MAN – *metropolitan área network*) tem cobertura de dezenas de quilômetros. Já as WANs (*wide área network*) podem ter cobertura mundial.

A tecnologia de rede local (LAN) foi desenvolvida a partir da rede *ethernet* da Xerox Corporation. Esta foi criada pela empresa com o objetivo de compartilhar recursos disponíveis em vários prédios e estações de trabalho e foi desenvolvida em conjunto com a DEC e a INTEL. Ela se tornou a primeira rede comercial e uma das mais importantes redes locais do mundo, servindo como base para definição de um dos padrões ISO, o ISSO 8802.3. (ROSS 2008).

Além de classificar as redes por sua abrangência, Forouzan (2008) também as classifica as LANs de acordo com sua topologia, sendo:

- Topologia de malha: cada dispositivo possui uma conexão ponto a ponto dedicada a cada um dos demais dispositivos. Para acomodar todas conexões cada dispositivo precisa ter *n*-1, portas de entradas e de saídas, sendo *n* o número de nós na rede. O uso de conexões dedicadas, garantindo a capacidade de suporte ao próprio volume de dados, eliminando problemas com tráfego, é uma das vantagens deste tipo de topologia. A principal desvantagem é o número de dispositivos e cabos para realizar as conexões necessárias

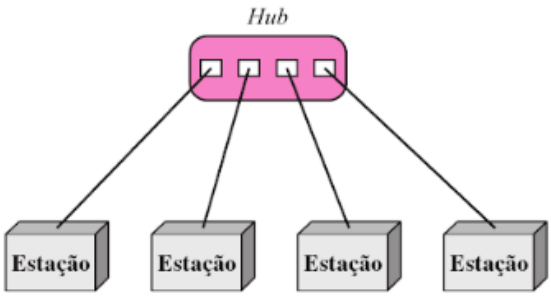
Figura 4 - Topologia de malha



Fonte: Forouzan (2008)

- Topologia estrela: nesta topologia, cada dispositivo possui apenas uma conexão ligada a um controlador central que pode ser um *hub* ou *switch*, não sendo ligados entre si. Um número menor de dispositivos de conexão e cabos, bem como a facilidade de instalação e configuração é uma vantagem deste tipo de topologia. Além disso, há maior facilidade na identificação e isolamento de falhas, uma vez que se um dispositivo falhar, apenas ele será afetado. A dependência de toda a topologia a um único ponto de interconexão é uma desvantagem neste tipo de topologia.

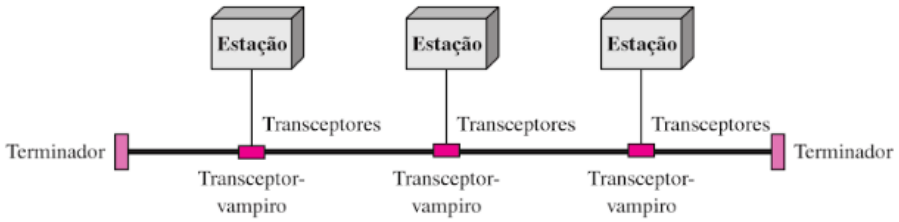
Figura 5 - Topologia estrela



Fonte: Forouzan (2008)

- Topologia de Barramento: é uma topologia multiponto, onde um longo cabo atua como barramento interligando todos os dispositivos da rede. Os nós são conectados ao cabo principal por meio de cabos transceptores e transceptores-vampiros, que são cabos que se unem ao cabo principal perfurando sua blindagem e criando contato com o núcleo de metal. A facilidade de instalação é uma vantagem desta topologia, e a dificuldade de reconfiguração e isolamento de falhas uma desvantagem. Além disso a intensidade do sinal é inversamente proporcional ao comprimento do cabo e por isso apenas um número limitado de dispositivos pode ser interligado desta forma.

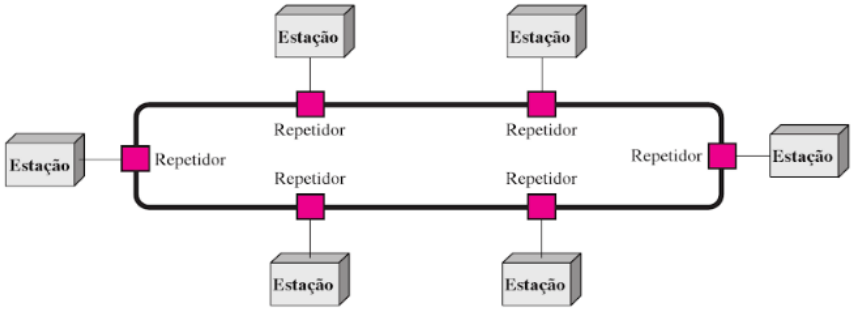
Figura 6 - Topologia de barramento



Fonte: Forouzan (2008)

- Topologia de anel: neste cada dispositivo possui uma conexão ponto a ponto com outros dois dispositivos conectados aos seus lados. O sinal percorre todo o anel até alcançar o dispositivo de destino. Cada dispositivo possui um repetidor, quando um dispositivo recebe um sinal destinado a outro dispositivo, o repetidor instalado nele regera os dados e reenvia. Uma das vantagens dessa tipologia é fácil instalação e reconfiguração, além disso o isolamento de falhas é simplificado. O tráfego unidirecional é uma desvantagem, uma interrupção no anel pode impedir a comunicação de toda a rede.

Figura 7 - Topologia anel



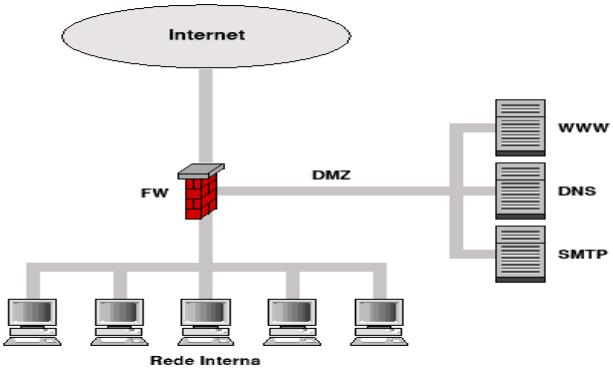
Fonte: Forouzan (2008)

- Topologia de hibrida: neste caso duas ou mais das citadas acima podem ser mescladas para atender as necessidades da organização.

Dentre todas as tecnologias que podem ser empregadas para promover a segurança da informação em uma rede empresarial, Fazzanaro (2009) destaca o uso de uma zona desmilitarizada, como uma das mais importantes. Defende que a utilização da mesma é interessante pois separa serviços que são acessados pela rede externa, da rede interna. Tanembaum (2003) explica que a zona desmilitarizada é uma área franca, uma camada que define o limite entre duas redes com políticas de segurança diferentes. O *firewall* que veremos na próxima sessão deste trabalho é

que defini o limite entre essas duas redes e não permite o tráfego livre de informação entre elas.

Figura 8 - Exemplo de rede com zona desmilitarizada



Fonte: Cert.br (2018)

3.4 *FIREWALL*

Um *firewall* é um equipamento ou dispositivo de rede que tem por função manter a segurança aplicando políticas a determinados pontos de uma rede. Controlam e regulam o tráfego de dados dentro de uma rede ou entre redes distintas, impedindo a comunicação e acessos não permitidos de uma rede para outra (NAHES; PEREIRA, 2007).

De acordo com a CERT.BR (2018), um *firewall* bem configurado é um instrumento de extrema importância na implantação de políticas de segurança de redes. Por outro lado, não são infalíveis e não devem ser a única ferramenta de defesa presente em uma rede, uma vez que os mesmos são capazes de proteger a rede apenas de ataques externos. É importante que o ambiente no qual o *firewall* será implantado seja de domínio do administrador da rede a que pertence. É aconselhável que o *firewall* siga a mesma filosofia da plataforma onde são executados.

A Redhat Customer Portal (2018), explica que diversos fabricantes têm criado soluções de firewall com foco em todos os níveis de mercado, desde usuários domésticos até banco de dados de empresas, protegendo informações vitais. Classifica estes dispositivos, primeiro de acordo com suas características físicas, sendo os *firewalls* de *hardware*, aqueles equipamentos baseados somente em *hardware*, como os fabricados pela Cisco, Nokia entre outras. E os *firewalls* de *software*, soluções desenvolvidas por empresas como a McAfee e Symantec. Além

dessa classificação, também difere os *firewalls* de acordo com a forma de funcionamento, conforme demonstrado na Tabela 2:

Tabela 2 - Tipos de firewall

MÉTODO	DESCRIÇÃO
NAT	*Network Address Translation* (NAT) coloca sub-redes IP privadas atrás de um ou pequeno grupo de endereços IP, mascarando todas as requisições em uma fonte ao invés de diversas. O *kernel* do Linux possui a funcionalidade NAT embutida através do subsistema do *kernel Netfilter*.
FILTRO DE PACOTES	Um *firewall* de filtro de pacote lê cada pacote de dados que passa por uma LAN. Ele pode ler e processar os pacotes por informações de cabeçalho e filtra o pacote baseado em conjuntos de regras programáveis implementada por um administrador de *firewall*. O *kernel* do Linux possui uma funcionalidade de filtro de pacotes embutida através do subsistema do *kernel*, o *Netfilter*.
PROXY	Os *firewalls* de *proxy* filtram todas as requisições de um certo protocolo ou tipo de clientes LAN para uma máquina de *proxy*, que então faz essas requisições para a Internet em nome do cliente local. Uma máquina *proxy* age como um buffer entre os usuários remotos mal-intencionados e as máquinas clientes de rede internas.

Adaptado de Redhat Customer Portal (2018)

A Cert.br (2018) destaca a utilização do *firewall* de filtro de pacotes, por serem amplamente utilizados devido ao seu baixo custo de implantação, uma vez que estão integrados a dispositivos de rede como roteadores, *switches* e *kernel de* diversos sistemas operacionais. Este tipo de *firewall* normalmente analisa as informações contidas nos cabeçalhos dos pacotes que trafegam na rede, nestes conseguem identificar, endereço de IP de origem e destino, protocolo utilizado e portas de comunicação. Existem duas categorias de filtragem de pacotes a estática (*stateless*), onde o *firewall* é projetado para tomar decisões do tipo bloquear e permitir, não considerando o contexto em que o pacote está inserido, sendo necessário estabelecer regras de forma explicita, tanto para os pacotes que trafegam para dentro, quanto para os que saem da rede. Já a categoria de *firewalls* de filtros dinâmicos (*statefull*), rastreiam e mantém o estado das conexões, desta forma o pacote é a analisado dentro do contexto da conexão que o contém. Assim o desempenho apresentado por um *firewall* de filtro dinâmico é superior ao de filtro estático, pois o tráfego de resposta é gerenciado automaticamente.

O *kernel* do Linux, oferece um sistema de filtragem de pacotes chamado *Netfilter*, ele possui a habilidade de ler informações do cabeçalho de pacotes IP e desta forma permite o roteamento avançado e gerenciamento de estado de conexão. Ele é implementado utilizando a ferramenta de administração *iptables*, que substituiu a *ipchains* a partir do *kernel* 2.4 no Linux, mantendo, contudo, uma sintaxe

semelhante ao de seu antecessor. O *iptables* utiliza o *Netfilter* para aprimorar a conexão de rede, inspeção e processamento. Além disso, apresenta autenticação avançada, ações pré e pós roteamento, tradução de endereços de rede e encaminhamento de portas. (REDHAT CUSTOMER PORTAL, 2018).

Neto (2004), explica que o *Netfilter* presente nas distribuições Linux, possui 3 tabelas principais sendo elas *filter*, NAT e *mangle*, com funções específicas. E que através da combinação das formas de controle de cada uma delas, podemos implementar inúmeras regras de filtragem visando garantir a segurança da rede.

A tabela *filter* é explicada por Hunt (2004), ele categoriza o tráfego de dados em uma rede em três grupos, para dessa maneira aplicar diferentes regras de filtragem para cada categoria, sendo:

- *INPUT* (entrada): onde o tráfego entrante é testado contra as regras do *firewall* antes de ser aceito.
- *OUTPUT* (saída): onde o tráfego de saída é testado contra as regras do *firewall* antes de ser enviado.
- *FORWARD* (encaminhamento): onde o tráfego que está sendo encaminhado é testado contra as regras do *firewall* antes de ser encaminhado.

Os conjuntos de regras de entrada (*INPUT*) e saída (*OUTPUT*), são aplicadas quando o sistema atua como um hospedeiro, as regras de encaminhamento são aplicadas quando o sistema atua como um roteador.

Um *firewall* funciona comparando os pacotes que recebe, com as regras inseridas pelo administrador. Uma vez que um pacote combina com uma regra, uma ação definida pelo administrador é tomada. A opção –j *target* define a ação a ser tomada, sendo que esta, pode ser uma predefinição, ou um salto para uma cadeia de regras definida pelo administrador. As palavras-chave *target* que identificam a ação a ser realizada com o pacote, podem as seguintes:

- *ACCEPT* (aceitar): deixa o pacote passar;
- *DROP* (derrubar): descarta o pacote, e não devolve nenhuma resposta informando o descarte;
- *REJECT* (rejeitar): descarta o pacote, mas envia uma mensagem informando que o pacote foi barrado;
- *LOG*: Apenas cria um registro sobre um pacote, não dando termino ao processo de avalição.

A tabela NAT, tem a função de redirecionamento e alteração de pacotes, e implementa as seguintes situações:

- *PREROUNTING*: utilizado quando existe a necessidade de se fazer alterações no pacote, antes que o mesmo seja roteado;
- *OUTPUT*: utilizado quando pacotes são originalmente emitidos pelo *firewall;*
- *POSTROUTING*: é utilizado quando existe a necessidade de se fazer alterações no pacote, após o tratamento de roteamento.

Assim como na tabela *filter*, existem 4 ações na tabela NAT, sendo:

- *SNAT*: realiza a troca de endereços IP de origem;
- *DNAT*: altera os endereços de IP de destino;
- *MASQUARADE*: faz o mascaramento de IP;
- *REDIRECT*: redireciona o pacote para uma porta local.

A tabela *Mangle* faz implementações de alterações especiais, podendo alterar a prioridade de um pacote de dados baseado no tipo de serviço. As cadeias da tabela *mangle* são cinco: *PREROUTING, POSTROUTING, INPUT, OUTPUT e FORWARD*, todas correspondem às cadeias de outras tabelas do *iptables* (DELFINO, 2018).

Hunt (2004) demonstra que além desses comandos presentes nas tabelas, outros parâmetros podem ser utilizados para construir um filtro de pacotes, que pode comparar o protocolo usado, a fonte ou endereço de destino, e a interface de rede pela qual o pacote é recebido ou enviado. Estes parâmetros e suas funções, são:

-p *protocol*: define o protocolo ao qual a regra se aplica, este valor pode ser um número, previamente definido na tabelas de protocolos no sistema operacional, ou palavras-chave como TCP, UDP, ICMP;

-s *address[/mask]*: define a fonte a qual a regra se aplica, podem ser o nome ou endereço IP de um hospedeiro ou rede, seguido de uma máscara opcional;

--sport[port[:port]]: define a porta de origem para qual a regra se aplica, sendo que *port* pode ser um número ou nome do arquivo de definição de serviços do

sistema operacional. Se nenhum valor for especificado, o comando se aplicará a todas as portas de comunicação;

-d address[/mask]: Define o destino do pacote para o qual a regra se aplica. As mesmas regras utilizadas para definição de regras de endereços de origem se aplicam a este parâmetro;

--dport[port[:port]]: semelhante ao comando –sport, mas define a porta de destino para a qual a regra se aplica;

--icmp-type type: define o tipo de ICMP para o qual a regra se aplica, sendo *type,* qualquer número ou nome do tipo de mensagem ICMP válido;

-j target: define uma política padrão para controlar o pacote;

-i name: define o nome da interface de rede de entrada a qual a regra se aplica;

-o name: define o nome da interface de rede de saída a qual a regra se aplica;

-f: indica que a regra se aplica apenas a fragmentos secundários de pacotes fragmentados.

4 ESTUDO DE CASO

Afim de apresentar um resultado, será realizado um estudo de caso em uma empresa de consultoria contábil da cidade de Americana. Como serão estudadas as principais vulnerabilidades de segurança da rede da empresa, o nome da mesma será preservado. Desta maneira, a empresa não será exposta a riscos, caso opte por não aplicar as sugestões de melhorias propostas neste trabalho.

4.1 AMBIENTE

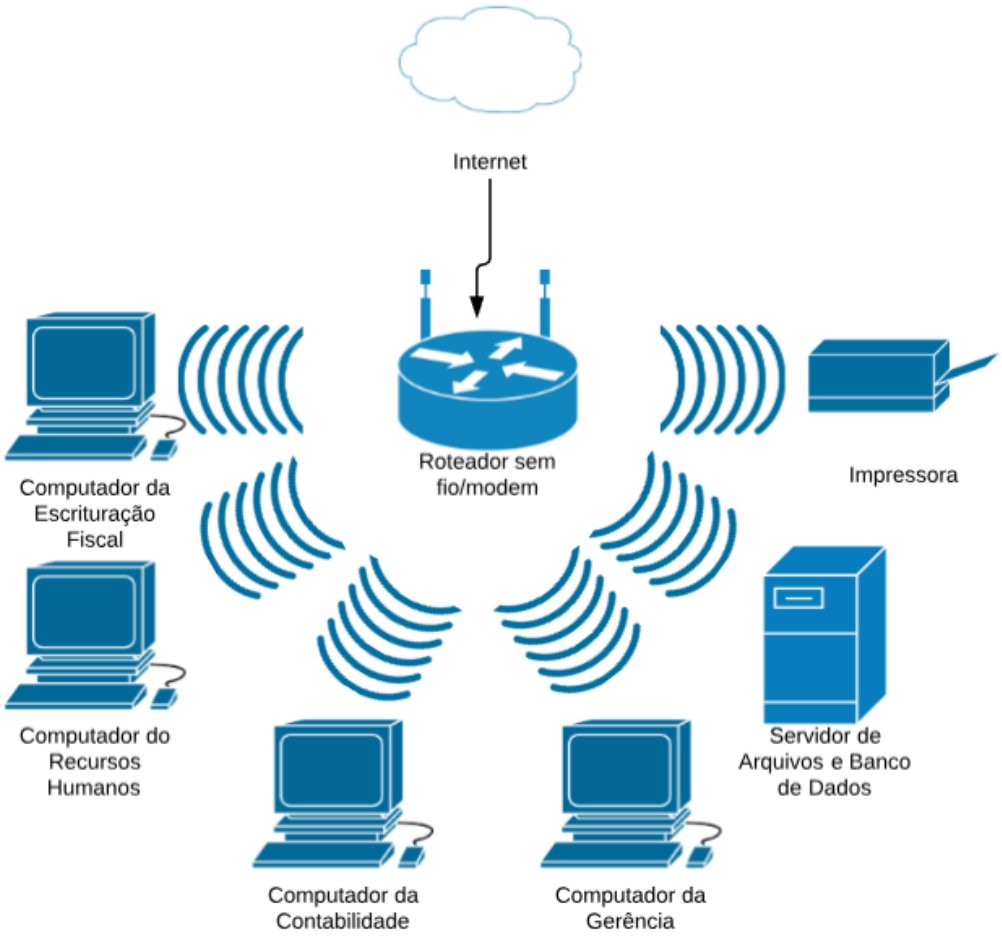
Sendo uma empresa de consultoria contábil, a mesma precisa manter contato com seus clientes em tempo real. Para isso, utiliza-se de ferramentas de comunicação como e-mail e mensageiros instantâneos. O foco da empresa tem sido auxiliar os clientes nos procedimentos de escrituração fiscal, sendo assim o envio e armazenamento de documentos relacionados a notas fiscais de entrada e saída de produtos e serviços é de suma importância para continuidade e sucesso do negócio. Para manipulação e controle desses arquivos, geralmente recebidos no formato .xml, a empresa conta com um *software* de gerenciamento contábil e um servidor de banco de dados, que também é utilizado como servidor de arquivos.

Além da escrituração fiscal, a empresa também oferece consultoria para as áreas de recursos humanos e contabilidade. O mesmo *software* utilizado para o gerenciamento das notas fiscais, oferece módulos de controle para os outros dois segmentos.

A topologia de rede da empresa é do tipo estrela e sua configuração é muito simples, sendo que a comunicação entre as máquinas clientes e o servidor é feito através de um roteador de rede sem fio. O acesso à Internet é feito através deste dispositivo, que foi fornecido pela empresa provedora de acesso à Internet, que fornece um *link* de 15 MB e mantém suas configurações padrão. Não existe nenhuma configuração de controle de acesso ao servidor de banco de dados. A mesma rede utilizada pelos donos e funcionários da empresa pode ser acessada pelos clientes em eventuais visitas através da rede sem fio. A distribuição de endereços de IPs é feita via DHCP, serviço oferecido de maneira nativa pelo roteador da rede. A empresa conta com 5 computadores, sendo quatro *laptops*,

utilizados como clientes e um *desktop* utilizado como servidor de banco de dados e arquivos, além de uma impressora, como pode-se visualizar na Figura 9:

Figura 9 - Configuração atual da rede da empresa



Fonte: elaborado pelo autor

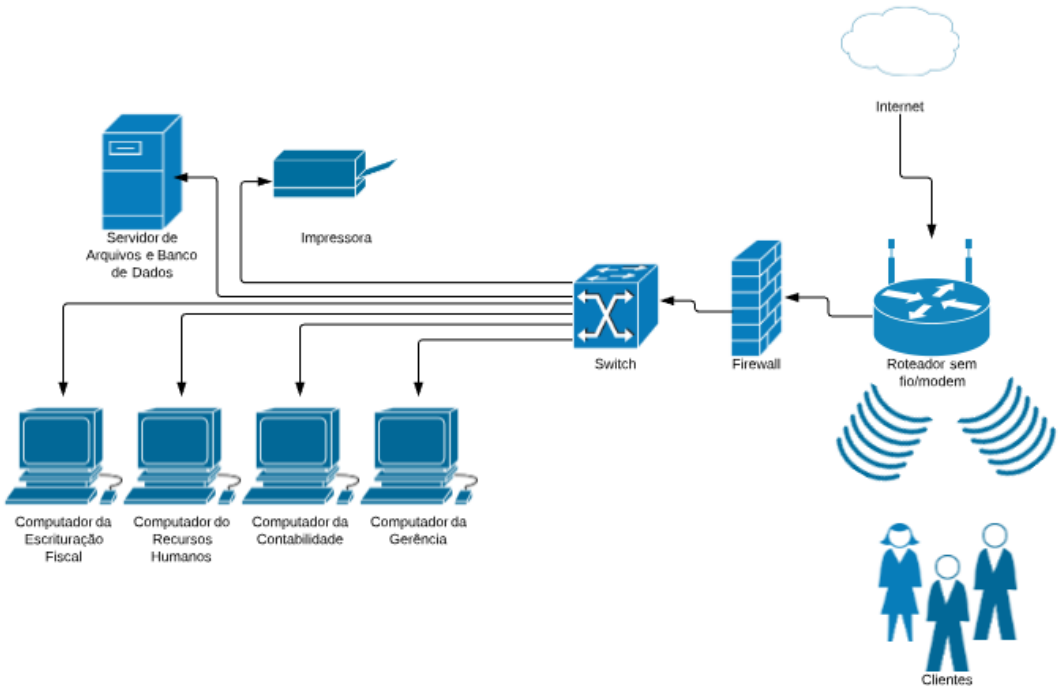
4.2 PROBLEMA

Não existe nenhuma barreira entre a rede mundial de computadores e a rede interna da empresa. Isso torna as informações da empresa e de seus clientes, armazenadas no servidor de banco de dados, bem como todos os documentos armazenados nesta mesma máquina, vulneráveis a ataques de terceiros. Também não existe uma divisão entre a rede utilizada pelos colaboradores da empresa e a utilizada pelos visitantes, o que permite o fácil acesso a quaisquer informações confidenciais da empresa, por qualquer visitante que tenha recebido acesso a rede sem fio.

4.3 POSSÍVEIS SOLUÇÕES

Afim de proteger a rede da empresa das ameaças oferecias pela conexão com a internet, um *firewall* será adicionado a rede, criando uma barreira de proteção entre a rede da empresa e a rede mundial de computadores. Também com auxilio deste dispositivo, a rede da empresa será separada da rede de clientes, que poderá ser acessada pelo roteador de rede sem fio. Os demais dispositivos da rede receberão um IP fixo e a conexão das máquinas será realizada via cabo *ethernet*. Com as alterações sugeridas a rede da empresa terá a seguinte configuração, demonstrada na Figura 10:

Figura 10 - Proposta de configuração de rede



Fonte: elaborado pelo autor

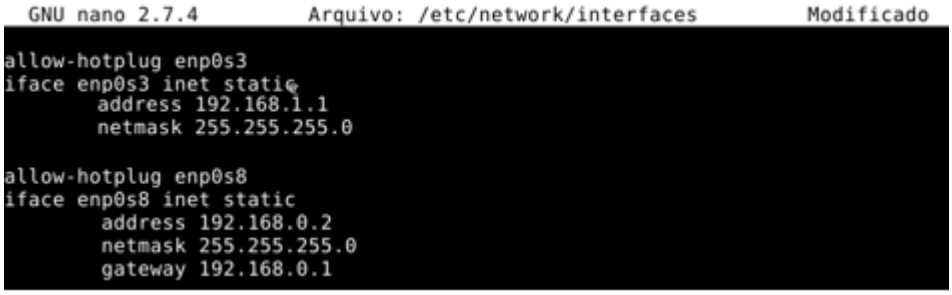
Afim de viabilizar a proposta de configuração de rede, um novo computador com duas interfaces de rede precisará ser adquirido pela empresa, nele seria instalado uma distribuição Linux. Outra opção seria utilizar uma máquina virtual instalada no próprio servidor de arquivos e banco de dados da empresa. Para este trabalho utilizaremos o *software* de virtualização da Oracle, o Oracle VM VirtualBox em sua versão gratuita de número 5.2.2. A distribuição Linux escolhida foi a Debian 9.5.0 amd64, 512 MB de memória RAM foi alocado para a máquina virtual e 8 GB de disco rígido. O tipo de disco rígido criado foi do tipo VDI (*VirtualBox Disk Image*) que

foi dinamicamente alocado. Foram configuradas duas interfaces de rede na máquina virtual em modo *NAT* com as placas de rede do servidor. Uma instalação padrão do Debian 9.5.0, foi realizada na máquina virtual recém-criada.

Após a conclusão da instalação do Debian, o *login* foi feito com o usuário *root*, e no terminal foram realizados os seguintes procedimentos:

As duas interfaces de rede da máquina virtual tiveram seus IP definidos, sendo que a interface enp0s3 fará conexão direta com a rede interna da empresa e a interface enp0s8 com a rede externa. O arquivo /etc/network/interfaces foi editado da seguinte forma:

Figura 11 - Configuração de interfaces de rede do *firewall*



Fonte: elaborado pelo autor

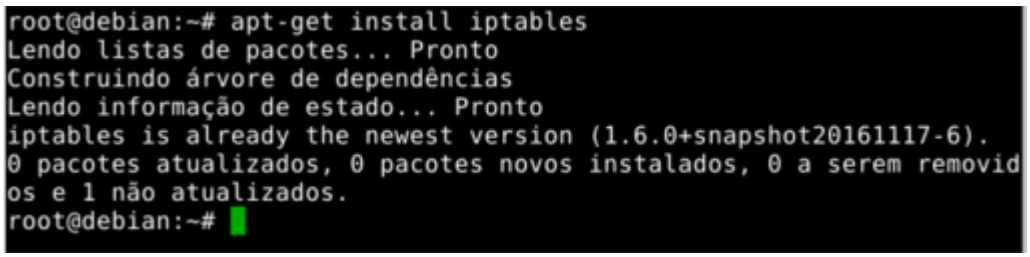
As interfaces de rede foram reiniciadas com os comandos *ifdown* e *ifup*, para que as configurações tivessem efeito.

Figura 12 - Atualizando o repositório de instalação do Debian

Fonte: elaborado pelo autor

Após a atualização do repositório de instalação, o comando para autalizar o *iptables* foi inserido.

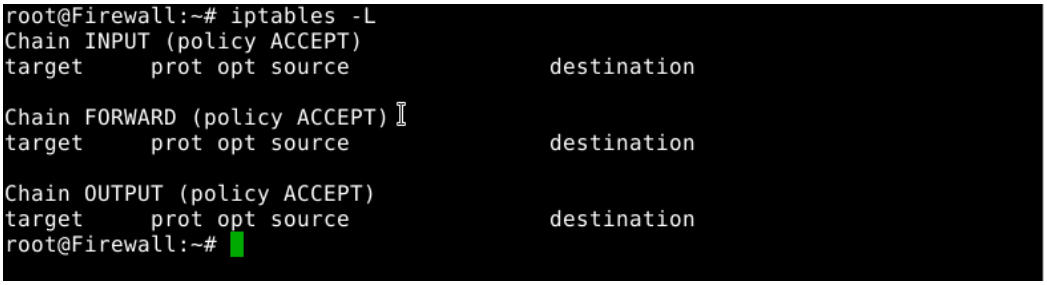
Figura 13 - Instalação e atualização do iptables



Fonte: elaborado pelo autor

Finalizadas as configurações e atualizações da máquina virtual, o comando “iptables -L” foi inserido afim de verificarmos a regras ativas na tabela *filter*. Conforme demonstra a Figura 14:

Figura 14 - Configuração de regras padrão da tabela filter



Fonte: elaborado pelo autor

Desta forma, foi possível verificar que as 3 *chains* da tabela *filter,* estão configuradas para permitir todo trafego na rede.

O arquivo /proc/sys/net/ipv4/ip_forward foi alterado, substituindo o valor 0 pelo 1, para permitir a encaminhamento de pacotes através da máquina virtual.

Após instalação do *iptables*, a primeira configuração definida foi a de mascaramento de pacotes, ela permite que a rede interna receba pacotes da rede externa através da tradução de IP.

Figura 15 - Configuração de mascaramento de pacotes

Fonte: Elaborado pelo autor

Porém, após a máquina ser reiniciada os comandos inseridos acima foram perdidos, afim de evitar que os mesmos sejam inseridos todas as vezes em que a máquina for reiniciada, um *script* contendo as regras de encaminhamento, mascaramento e *firewall* foi criado. Para isto, primeiro um arquivo de nome firewall.sh foi criado com as seguintes características:

Tabela 3 - *Script* de regras de *firewall*

```
#!/bin/sh
####################DECLARANDO VARIÁVEIS#######################
internet="enp0s8"
redelocal="enp0s3"
```

```
####################ATIVANDO IPTABLES#######################
# Limpando as regras #
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -F POSTROUTING -t nat
iptables -F PREROUTING -t nat
iptables -F -t nat

# Definindo a Politica Default das Cadeias
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Desabilitar o trafego IP entre as placas de rede #
echo "0" > /proc/sys/net/ipv4/ip_forward
echo "Desabilitar o trafego IP entre as placas .............[ OK ]"
# Impedimos que um atacante possa maliciosamente alterar alguma rota
echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects

# Proteção contra port scanners
iptables -N SCANNER
iptables -A SCANNER -m limit --limit 15/m -j LOG --log-prefix "FIREWALL: port scan
ner: "
iptables -A SCANNER -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL FIN,URG,PSH -i  $internet -j SCANNER
iptables -A INPUT -p tcp --tcp-flags ALL NONE -i  $internet -j SCANNER
iptables -A INPUT -p tcp --tcp-flags ALL ALL -i  $internet -j SCANNER
iptables -A INPUT -p tcp --tcp-flags ALL FIN,SYN -i  $internet -j SCANNER
iptables -A INPUT -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -i  $internet -j SCAN
NER
iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -i  $internet -j SCANNER
iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -i  $internet -j SCANNER
# Libera acesso externo a determinadas portas
##Algumas portas devem ser negadas.
iptables -A INPUT -p tcp --dport 1433 -j DROP
```

```
iptables -A INPUT -p tcp --dport 6670 -j DROP
iptables -A INPUT -p tcp --dport 6711 -j DROP
iptables -A INPUT -p tcp --dport 6712 -j DROP
iptables -A INPUT -p tcp --dport 6713 -j DROP
iptables -A INPUT -p tcp --dport 12345 -j DROP
iptables -A INPUT -p tcp --dport 12346 -j DROP
iptables -A INPUT -p tcp --dport 20034 -j DROP
iptables -A INPUT -p tcp --dport 31337 -j DROP
iptables -A INPUT -p tcp --dport 6000  -j DROP
# Impedindo Traceroutes
iptables -A INPUT -p udp --dport 33434:33523 -j DROP
iptables -A INPUT -p tcp --dport 113 -j REJECT
iptables -A INPUT -p igmp -j REJECT
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j REJECT
# porta para contabilidade
  #DCTF
  iptables -A FORWARD -p tcp --dport 3456 -j ACCEPT
  #DPI
  iptables -A FORWARD -p tcp --dport 24001 -j ACCEPT
  #ted
  iptables -A FORWARD -p tcp --dport 8017 -j ACCEPT
#Portas para departamento pessoal
 #sefip
 iptables -A FORWARD -p tcp  --dport 2004 -j ACCEPT
 iptables -A FORWARD -p tcp  --dport 2631 -j ACCEPT
 iptables -A FORWARD -p tcp  --dport 1494 -j ACCEPT
 iptables -A FORWARD -p tcp  --dport 5017 -j ACCEPT
 iptables -A FORWARD -p tcp -s 10.0.0.7 --dport 9090 -j ACCEPT
#cadastro
 iptables -A FORWARD -p tcp --dport 25777 -j ACCEPT
 iptables -A FORWARD -p tcp --dport 5432 -j ACCEPT
#datasiga
  iptables -A FORWARD -p tcp --dport 20650 -j ACCEPT
  iptables -A FORWARD -p tcp --dport 10650 -j ACCEPT
#vnc
```

```
  iptables -A FORWARD -p tcp --dport 5700 -j ACCEPT
  iptables -A INPUT -p tcp --dport 5700 -j ACCEPT

# PORTA 53 - ACEITA PARA A REDE LOCAL
iptables -A FORWARD -i  $redelocal -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i  $redelocal -p udp --dport 53 -j ACCEPT

# PORTA 110 - ACEITA PARA A REDE LOCAL
iptables -A FORWARD -i  $redelocal -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -i  $redelocal -p udp --dport 110 -j ACCEPT

# PORTA 25 - ACEITA PARA A REDE LOCAL
iptables -A FORWARD -i  $redelocal -p tcp --dport 25 -j ACCEPT

# https
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i  $redelocal -p tcp --dport 443 -j ACCEPT

# PORTA 20 - ACEITA PARA A REDE LOCAL
iptables -A FORWARD -p tcp --dport 20 -j ACCEPT
iptables -A INPUT -p tcp --syn --dport 22 -m recent --name sshattack -set
iptables -A INPUT -p tcp --dport 22 --syn -m recent --name sshattack --rcheck --se
conds 60 --hitcount 3 -j LOG --log-prefix 'SSH REJECT: '
iptables -A INPUT -p tcp --dport 22 --syn -m recent --name sshattack --rcheck --se
conds 60 --hitcount 3 -j REJECT --reject-with tcp-reset
iptables -A FORWARD -p tcp --syn --dport 22 -m recent --name sshattack -set
iptables -A FORWARD -p tcp --dport 22 --syn -m recent --name sshattack --rcheck --
seconds 60 --hitcount 3 -j LOG --log-prefix 'SSH REJECT: '
iptables -A FORWARD -p tcp --dport 22 --syn -m recent --name sshattack --rcheck --
seconds 60 --hitcount 3 -j REJECT --reject-with tcp-reset
# PORTA 21 - ACEITA PARA A REDE LOCAL
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT
# PORTA 22 - ACEITA PARA A REDE INTERNET
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
```

```
# Cadeia de Reenvio (FORWARD).
# Primeiro, ativar o mascaramento (nat).
iptables -t nat -F POSTROUTING
iptables -t nat -A POSTROUTING -o  $internet -j MASQUERADE# Agora dizemos quem e o que podem acessar externamente
# O controle do acesso a rede externa e feito na cadeia "FORWARD"
iptables -A FORWARD -i  $internet -j ACCEPT
iptables -A FORWARD -o  $internet -m state --state ESTABLISHED,RELATED -j ACCEPT

###BLOQUEANDO TODAS AS SAIDAS E PORTAS
iptables -A INPUT -p all -j DROP
iptables -A FORWARD -p all -j DROP

################################################
# Tabela FILTER
# Proteção contra telnet
iptables -A INPUT -p TCP -i  $internet --dport telnet -j DROP

# Descarta pacotes TCP indesejaveis
iptables -A FORWARD -p tcp ! --syn -m state --state NEW -j DROP

# Proteção contra ping da morte
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
#Allow ALL other forwarding going out
iptables -A FORWARD -o  $internet -i  $redelocal -j ACCEPT

# Habilitando o trafego IP, entre as Interfaces de rede
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Adaptado de Cabral (2008)

Após a criação do arquivo de *script,* é necessário habilitar a execução do mesmo. Para isto o comando “chmod +X firewall.sh” foi inserido. Para que o *script* possa ser executado na inicialização do sistema operacional, o mesmo foi movido para o diretório /etc/init.d e o comando “update-rc.d firewall.sh defaults” foi aplicado.

Outras regras podem ser adicionadas, ou estas editadas conforme a necessidade da empresa.

A rede sem fio destinada a clientes, continuará a receber IPs via DHCP. Os equipamentos da rede interna, no entanto, terão seus IPs fixados seguindo o seguinte padrão:

Tabela 4: Distribuição de IP na rede da empresa

Equipamento	IP
Firewall	192.168.1.1/24
Switch	192.168.1.2/24
Servidor de arquivos e banco de dados	192.168.1.3/24
Impressora	192.168.1.4/24
Computador da Gerência	192.168.1.5/24
Computador da Escrituração Fiscal	192.168.1.6/24
Computador do Recursos Humanos	192.168.1.7/24
Computador da Contabilidade	192.168.1.8/24

Fonte: Elaborado pelo autor

5 CONCLUSÃO

Com o referencial bibliográfico e a análise dos resultados obtidos durante o estudo de caso, pode-se concluir que a segurança da informação é assunto dos mais importantes para a continuidade de negócio de qualquer empresa em qualquer nicho de mercado. Não somente na obtenção de vantagem estratégica mas para preservação de sua imagem e ativos organizacionais. Também é possível concluir que por vezes a mesma tem sido negligenciada apesar dos riscos inerentes a esta displicência.

Ficou claro que uma rede de computadores pode ser utilizada para facilitar o compartilhamento de informações e recursos, para que assim a empresa tenha maior agilidade na realização de processos, na análise de dados e tomada de decisão. O que pode se tornar grande diferencial, de extrema importância no atual mundo globalizado.

Também é possível afirmar que com pouco investimento e algum estudo, qualquer empresa pode aumentar significativamente o nível de segurança da informação encontrada em sua rede. Com a implantação de um *firewall* presente no *kernel* de um *software* livre, a rede da empresa pode ser protegida de ataques de terceiros, e as informações da empresa e de seus clientes podem ser resguardadas de exposição, alteração e acesso ilícito.

REFERÊNCIAS BIBLIOGRÁFICAS

ESTADÃO SEGURANÇA DIGITAL: **65% dos ataques de hackers miram pequenas empresas, diz estudo.** São Paulo, 24 abr. 2017. Disponível em: <https://pme.estadao.com.br/noticias/pme,65-dos-ataques-de-hackers-miram-pequenas-empresas-diz-estudo,70001746157,0.htm>. Acesso em: 08 nov. 2018.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. 11. ed. Rio de Janeiro: Campus, 2003. 154 p.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007. 285 p.

REZENDE, Denis Aleides; ABREU, Aline França de. **Tecnologia da informação:** aplicada a sistemas de informação empresariais. 9. ed. São Paulo: Atlas, 2013. 376 p.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. 4. ed. São Paulo: Saraiva, 2010.

LAUREANO, M. A. P. **Gestão de segurança da informação**. 2005. 130 p. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20 .pdf>. Acesso em: 02 out. 2018.

OLIVEIRA, Wilson. **Técnicas para hackers:** soluções para segurança. 2. ed. Lisboa: Centro Atlântico, 2003. 603 p.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política da segurança da informação:** guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006. 177 p.

FONTES, Edison. **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008. 283 p.

TANENBAUM, Andrew S.. **Redes de computadores.** 4. ed. São Paulo: Campus, 2003. 945 p.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores e a Internet:** uma abordagem top-down. 5. ed. São Paulo: Pearson, 2010. 614 p.

FOROUZAN, Behrouz A..**Protocolo TCP/IP.** 3. ed. São Paulo: Amgh, 2010. 839 p.

FOROUZAN, Behrouz A.. **Comunicação de dados e redes de computadores.** 4. ed. Porto Alegre: Amgh Editora, 2008. 1134 p.

ROSS, Julio. **Redes de computadores.** Rio de Janeiro: Antenna Edições Técnicas, 2008. 148 p

FAZZANARO, Pablo Luis. **Segurança em redes de computadores.** Joinville: Clube de Autores, 2009. 70 p.

CERT.BR (Org.). **Práticas de Segurança para Administradores de Redes Internet.** 2018. Disponível em: <https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec4.12>. Acesso em: 19 out. 2018.

NAHES, Paulo Henrique Mariotto; PEREIRA, Marco Antonio Alves. Segurança em redes de computadores com uso de firewalls. **Interface Tecnológica**, Taquaritinga, v. 1, n. 4, p.107-115, 01 jul. 2007. Disponível em: <https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/15/13>. Acesso em: 19 out. 2018.

REDHAT CUSTOMER PORTAL. **Firewalls.** Disponível em: <https://access.redhat.com/documentation/pt-br/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-firewalls#>. Acesso em: 19 out. 2018.

NETO, Urubatan. **Dominando Linux firewall iptables.** Rio de Janeiro: Ciência Moderna, 2004. 112 p.

DELFINO, Pedro. **Tabelas do iptables**: entenda a lógica do firewall Linux. Disponível em: https://e-tinet.com/linux/tabelas-do-iptables-firewall-linux/. Acesso em: 01 nov. 2018.

HUNT, Craig. **Linux:** servidores de redes. 8. ed. Rio de Janeiro: Ciência Moderna, 2004. 567 p.

CABRAL, Paulo. **Firewall:** Iptables no Debian. 2008. Disponível em: <https://www.vivaolinux.com.br/script/Firewall-+-iptables-no-Debian>. Acesso em: 13 nov. 2018