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

JORGE JOSÉ KLEINUBING

# ESTUDO DE CASO: IMPLANTAÇÃO DE SERVIDORES LINUX NA REDE DE UMA PEQUENA EMPRESA

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO
2018

JORGE JOSÉ KLEINUBING

# ESTUDO DE CASO: IMPLANTAÇÃO DE SERVIDORES LINUX NA REDE DE UMA PEQUENA EMPRESA

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

Orientador: Dr. Eden Ricardo Dosciatti

PATO BRANCO
2018

**Ministério da Educação**
**Universidade Tecnológica Federal do Paraná**
Câmpus Pato Branco
Departamento Acadêmico de Informática
*III Curso de Especialização em Redes de Computadores*

## TERMO DE APROVAÇÃO

# ESTUDO DE CASO: IMPLANTAÇÃO DE SERVIDORES LINUX NA REDE DE UMA PEQUENA EMPRESA

por

**Jorge José Kleinubing**

Esta monografia foi apresentada às 17h30min do dia 21 de novembro de 2018, como requisito parcial para obtenção do título de ESPECIALISTA, no III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Prof. Dr. Eden Ricardo Dosciatti
Orientador / UTFPR-PB

Prof. Dr. Fábio Favarim
UTFPR-PB

Prof. Dr. Dalcimar Casanova
UTFPR-PB

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

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

# RESUMO

KLEINUBING, Jorge José. Implantação de servidores Linux em redes corporativas para melhorar o desempenho e segurança da rede. 2018. 64 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2018.

O presente trabalho aborda a importância dos servidores Linux nas redes corporativas para melhorar o desempenho e a segurança da rede. Analisando o cenário de uma empresa de pequeno a médio porte, nota-se que a estrutura da rede local não possui nenhuma preocupação quanto a segurança dos dados da empresa, e a otimização do tráfego de dados na rede. Desta forma, foi realizada uma análise de quais os serviços necessários para contribuir de forma significativa com o desempenho da rede, para a melhoria do tráfego, e o que seria ideal para o cenário da empresa, em relação a segurança da rede. O possível crescimento da rede também foi analisado, assim como a necessidade de instalação de novos serviços para a rede.

**Palavras-chave**: Linux. Servidores Linux. Redes de Computadores. Kernel.

## ABSTRACT

KLEINUBING, Jorge José. Deployment of Linux servers in corporate networks to improve network performance and security. 2018. 64 f. Monograph (Specialization in Computer Networks) – Academic Department of Informatics, Federal Technological University of Paraná, Campus Pato Branco. Pato Branco, 2018.

This paper discusses the importance of Linux servers in corporate networks to improve network performance and security. Analyzing the scenario of a small to medium-sized company,it is noticed that the structure of the local network has no concern about the security of the company's data, and the optimization of data traffic in the network. In this way, an analysis was made of which services needed to contribute significantly to network performance, traffic improvement, and what would be ideal for the company scenario in relation to network security. The possible growth of the network was also analyzed, as well as the need to install new services for the network.



**Keywords**: Linux. Linux Servers. Computer network. Kernel.

## LISTA DE FIGURAS

## LISTA DE QUADROS

## LISTA DE TABELAS

## LISTAGENS DE CÓDIGOS

## LISTA DE SIGLAS

| | |
|---|---|
| ADSL | *Assymetrical Digital SubscriberLine* |
| APT | *AdvancedPackage Tool* |
| BD | Banco de Dados |
| CIFS | *Common Internet File System* |
| DHCP | *Dynamic Host ConfigurationProtocol* |
| DMZ | *DeMilitarized Zone* |
| DNS | *DomianName System* |
| ERP | *Enterprise Resource Planning* |
| FSF | *Free Software Foundation* |
| FTP | *File TransferProtocol* |
| FV | Força de Vendas |
| GRUB | *GRandUnifieldBootloader* |
| IP | *Internet Protocol* |
| LAN | *Local Area Networks* |
| LTS | *LongTermSupport* |
| LVM | *LogicalVolume Manager* |
| MAC | *Media Access Control* |
| NAT | *Network AddressTranslation* |
| QOS | *Qualityof Service* |
| RDP | *Remote Desktop Protocol* |
| RHEL | *Red Hat Enterprise Linux* |
| RPM | *Red Hat Package Manager* |
| SMB | *Server MessageBlock* |
| SO | Sistema Operacional |
| SSH | *Secure Shell* |
| TI | Tecnologia da Informação |
| VM | *Virtual Machine* |
| VPN | *Virtual Private Network* |
| WAN | *WideArea Network* |
| WIFI | *Wireless Didelity* |

**SUMÁRIO**

# 1 INTRODUÇÃO

O Sistema Operacional (SO) tem como finalidade facilitar o uso do computador através de uma interface amigável. Ele é responsável por intermediar e controlar todos os recursos físicos e lógicos que a máquina utiliza em uma determinada atividade. O SO está entre os softwares de aplicação que recebe comandos do usuário e o hardware que executa esses comandos e/ou armazena os dados. Inicialmente o Linux, foi criado para exercer funções intermediárias entre o *hardware* e o *software*, sendo denominado como o núcleo (*Kernel*) do SO. A partir disso, surgiram as distribuições Linux, que são os SOs que tem seu *kernel* baseado ou estruturado no Linux. Uma distribuição Linux possui, um programa de instalação, aplicativos e softwares que possibilitam que o computador se torne uma ferramenta de trabalho, ou seja, utilizado para entretenimento ou para outras finalidades desejadas pelo usuário.

A forma como o Linux foi projetado fez com que seu uso em servidores se tornasse uma prática comum entre os administradores de Tecnologia da Informação (TI). Essa preferência deve-se ao fato de que as distribuições baseadas em Linux, disponíveis para servidores, possuam inicialmente somente os serviços básicos e essenciais para o funcionamento do computador, com o mínimo de ferramentas instaladas. Isso faz com que os recursos de hardware da máquina sejam pouco exigidos, concentrando todos os seus recursos disponíveis para tarefas realmente necessárias e essenciais para aquele tipo de serviço que será executado no servidor. Isso ocorreu por vários fatores, como: melhoria de desempenho, segurança, estabilidade e confiança apresentado no seu uso (BRITO, 2017).

Atualmente, existem distribuições Linux que são instaladas com mais frequência nos servidores e merecem destaque, como, por exemplo, Debian GNU/Linux, FedoraCentOS, Ubuntu Server, Oracle Linux, RedHat Enterprise Linux (RHEL), Slackware e SUSE Linux Enterprise Server (SLES). Algumas destas distribuições possuem suporte comercial e foram desenvolvidas exclusivamente para uso em servidores, possuindo aplicações instaladas com serviços específicos para determinadas finalidades, tornando-se um diferencial oferecido pela distribuição (BRITO, 2017).

A distribuição Debian GNU/Linux, uma das mais tradicionais, possui seu foco na estabilidade das versões que são lançadas para seus usuários. Como seu desenvolvimento é totalmente voluntário, seu ciclo de atualizações é mais demorado quando comparado com distribuições que possuem financiamento de empresas. Um exemplo de distribuição com aporte financeiro privado é o Ubuntu Server, que é baseada no Debian e foi lançada em 2004

pela empresa Canonical LTD e possui uma política de manutenção que lança uma nova versão a cada seis meses devido ao incentivo financeiro que recebe de uma empresa com fins lucrativos (BRITO, 2017).

O uso das distribuições Linux nos servidores de empresas, independentemente de seu porte, é algo muito comum hoje em dia, por fornecer serviços a custo zero, com recursos avançados e praticidade no seu uso. A instalação de uma distribuição Linux pode ocorrer em máquinas com poucos recursos de *hardware*, facilitando a vida financeira de uma empresa. Levando em consideração o exposto, o presente estudo consiste em apresentar a implementação de serviços Linux com o intuito de melhorar o desempenho da rede e aumentar a segurança dos dados das empresas. Também, apresentar a configuração e estruturação dos servidores com serviços que contribuam na segurança da rede, na facilidade do compartilhamento e armazenamento de arquivos e no desempenho de navegação da rede em empresas de médio porte.

## 1.1 OBJETIVOS

### 1.1.1 Objetivo Geral

Apresentar a implantação de servidores Linux com serviços que contribuem para a segurança da rede local, gerenciamento, armazenamento e compartilhamento de dados em uma empresa de pequeno porte.

### 1.1.2 Objetivos Específicos

- Identificar os serviços que a rede necessita para funcionar com segurança e eficiência;
- Analisar a probabilidade de crescimento da rede e programar uma estrutura escalável com planejamento para a instalação de novos serviços e equipamentos;
- Instalar o sistema operacional Linux sem interface gráfica e configurar os serviços destinados para a tarefa que o servidor irá desempenhar na rede.

## 1.2 JUSTIFICATIVA

Já faz algum tempo que as empresas, sejam do setor público ou privado, dependem da TI para realizar vários processos que competem ao seu negócio. Nos dias atuais, são poucas as empresas que realizam suas operações sem depender diretamente de um computador ou um software. Essa dependência, em alguns casos, pode resultar em investimentos tecnológicos desnecessários e/ou mal investido. Esses erros podem ocorrer tanto nas empresas públicas, quanto nas empresas privadas. Nas empresas privadas de pequeno a médio porte esse fator geralmente ocorre devido à falta de uma área de TI na empresa para gerenciar as questões pertinentes a investimentos na área, resultando em empresas estruturadas operacionalmente, mas sem nenhum planejamento, organização e visão na sua área de TI.

Atualmente um número considerável de empresas já percebeu a importância de se ter uma boa estrutura de TI para atender suas necessidades e expectativas, mas sua implantação, gerenciamento e manutenção resulta em adição de valores no orçamento da empresa que, em alguns casos, não possuem previsão desses valores ou pretendem investir o mínimo possível para que sua empresa funcione. Existe um termo chamado governança de TI, que engloba um conjunto de tópicos relacionados à gestão da área de informática de uma empresa com a intenção de investir o dinheiro de forma eficiente, neste setor, evitando desperdícios ou gastos desnecessários (LUNARDI, BECKER, MAÇADA, 2010).

É importante que o setor de TI de uma empresa possua gerenciamento, organização e planejamento para ter o alinhamento com as necessidades da empresa, garantindo o máximo de segurança dos dados gerados por ela, reduzir o mais próximo possível de zero, os problemas de hardware ou software que interrompam os processos da empresa e gerem tempo ocioso dos usuários, e controle dos custos. Dessa forma é possível demonstrar para os gestores que uma empresa com uma boa estrutura de TI é uma empresa com investimento em recurso tecnológico que permite realizar os seus processos com mais agilidade e rapidez, obtendo resultados satisfatórios.

Sabendo dessa dependência e da busca por investimentos cada vez menores e certeiros que o uso do sistema operacional Linux nos servidores da empresa em estudo é uma boa alternativa para estruturar e configurar com custo o mais próximo do zero, isso porque, os serviços e ferramentas disponibilizados pela distribuição é livre, sem custos financeiros. Ainda, haverá uma melhoria na parte de segurança dos dados que trafegam pela rede interna da empresa proporcionando mais estabilidade e um maior gerenciamento da rede, através da

implementação de servidores Linux. Também se destaca a possibilidade de configurar novos serviços para melhorar a estrutura da rede para atender novas necessidades e obter resultados satisfatórios.

A empresa em questão é de pequeno porte e atua na distribuição de medicamentos, possui a necessidade de ter conexão com a internet assim como qualquer outra empresa de qualquer ramo na atualidade. Possuir uma rede local com alguns computadores que acessam a Internet e servidores para atender as necessidades da empresa, é um cenário comum entre as empresas hoje em dia, não importando seu tamanho. Após uma reunião com o diretor da empresa e algumas invasões que ocorreram em outras empresas pequenas da região, houve o entendimento da necessidade de investimento para melhorar a estrutura atual.

Após realizar um levantamento analisando o cenário da empresa e o atual e único servidor da rede, foi decidido que possuir um servidor com somente o serviço de firewall para realizar a segurança da empresa, separar os serviços de compartilhamento e armazenamento de dados dos demais serviços de gestão, seria importante para a estrutura da empresa e ficou decido que dois novos servidores fariam parte da estrutura da empresa.

# 2 REFERENCIAL TEÓRICO

## 2.1 HISTÓRIA DO LINUX

No ano de 1991, o estudante de ciência da computação da Universidade de Helsinque, na Finlândia, Linus Benedict Torvalds, na época com 21 anos, falou sobre um suposto sistema operacional que ele desenvolveria. O "sistema operacional" que Linus se referia era o que mais tarde se chamaria Linux. Baseado no Minix, sistema criado por Andrew Tanenbaum. O Linux era um kernel e não um sistema operacional completo com aplicativos e instaladores (MOTA FILHO, 2012).

Em suma, o Linux foi desenvolvido para fazer o interfaceamento entre o hardware e o software, o que muitos chamam somente de Linux, na verdade são distribuições baseadas no kernel do Linux, que possuem programas que são compatíveis com o kernel Linux formando um sistema operacional. O kernel sozinho não possui muita utilidade sem os aplicativos, o que Linus criou foi um sistema que faz a ligação entre o *hardware* e os *softwares* criados pelas distribuições para realizar alguma tarefa (MOTA FILHO, 2012).

O nome original escolhido por Linus para o seu sistema foi Freix (Free Unix), mas, na época, o administrador do servidor FTP (*File TransferProtocol*) nic.funet.fi, solicitou que Linus mudasse o nome caso contrário ele não disponibilizaria o código. Diante dessa recusa, surgiu então o nome Linux, uma junção entre seu nome Linus e o sistema Unix.

É de conhecimento de todos que um computador sem sistema operacional (SO) não possui muita utilidade, o início da história do Linux surge dessa necessidade. Através da união da AT&T, General Electric, Laboratório Bell e o projeto MAC, do MIT (*MassachusettesInstituteof Technology*) surge um sistema operacional chamado MULTICS. Essa união não apresentou resultados satisfatórios e os Laboratórios Bell deixou o projeto. Um novo projeto com base no MULTICS foi iniciado resultando no sistema chamado UNIX (TEIXEIRA, 2007).

No início, o UNIX teve um grande crescimento na AT&T, mas, mesmo assim, era distribuído gratuitamente junto com o código fonte para as universidades. Após um período e, pela grande procura pelo sistema operacional, a empresa começou a comercializar. O UNIX se tornou um sistema multitarefa, multiusuário, compatível com várias plataformas, muito confiável e robusto, porém, era muito caro. Em 1983 Richard Stallman fundou a FreeSoftware

Foundation (FSF), criando então o projeto GNU, que tinha como finalidade criar um clone do UNIX que fosse gratuito e não tivesse o código fonte do UNIX (TEIXEIRA, 2007).

Ao final da década de 80, o projeto ainda não tinha atingido seu objetivo, mas o projeto não era um fracasso, foi utilizando ferramentas do projeto GNU que Linus Torvalds desenvolveu o Linux. Desenvolvido com base no UNIX, o kernel Linux, na sua origem, é ideal para ser utilizado em servidores intermediando a comunicação entre o hardware e softwares desenvolvidos pelas distribuições Linux (TEIXEIRA, 2007).

### 2.1.1 SERVIDORES LINUX

Servidor pode ser considerado como um dispositivo que oferece recursos para a rede, ou um dispositivo compartilhado por muitos usuários. Os serviços oferecidos por um servidor são vários, como serviço de impressão, servidor web, servidor de arquivos, etc.. Um único servidor pode executar vários serviços ao mesmo tempo, porém, para que isso seja possível, deve ser levado em consideração a quantidade de trabalho e a disponibilidade de *hardware* (MORIMOTO, 2008).

Os servidores Linux podem ser classificados: (i) conforme os serviços que possui configurado; (ii) de acordo com os serviços que rodam compartilhamento de conexão, impressoras, autenticação de usuários, compartilhamento de arquivos e; (iii) os que servem como servidor de *firewall*. Os servidores que hospedam aplicações para a grande rede e sites são classificados como servidores de Internet (MORIMOTO, 2008).

### 2.1.2 SERVIDORES DE REDE LOCAL

Para que se tenha uma rede local, o primeiro passo é realizar o cabeamento que distribuirá os pontos de acesso pelo ambiente, pontos esses que podem ser através de cabos ou via *wireless*. Nos pontos onde a rede é cabeada, a conexão é mais estável, com uma velocidade maior e mais segurança. Por outro lado, onde o acesso é via *wireless*,a vantagem é a praticidade no acesso, em contrapartida, existe a perda em velocidade, estabilidade e segurança. Embora o ponto de acesso sem fio possua mais desvantagens na questão de

desempenho e segurança quando comparada com o ponto de acesso cabeado, a combinação entre as duas é ideal (MORIMOTO, 2008).

Após a estruturação da rede e o início do seu funcionamento, o próximo passo é o compartilhamento da conexão. É neste momento que entra em cena o servidor de rede local com os serviços para contribuir com esse compartilhamento, melhorando o desempenho da rede e facilitando processos dos usuários da rede. Os serviços instalados, nesse tipo de servidor, dependem muito do tamanho e da necessidade da empresa e, são instalados serviços que atendam a necessidade e a demanda da mesma (MORIMOTO, 2008).

Um serviço fundamental para o bom funcionamento da rede local é o serviço de DHCP (*Dynamic Host ConfigurationProtocol*), que contribui com a distribuição e gerenciamento de endereços IPs (*Internet Protocol*) para os dispositivos da rede. Outra área importante de uma empresa que o servidor de rede local pode contribuir é no compartilhamento de arquivos e impressoras. Em uma empresa onde vários usuários compartilham de um mesmo arquivo é muito mais prático possuir esse arquivo salvo e centralizado em um único lugar em vez de possuir vários arquivos espalhados pela rede com versões diferentes, obtendo, também, economia de espaço no HD das máquinas dos usuários. É importante ressaltar que, ao centralizar os arquivos em uma única máquina, o *backup* dos arquivos se torna mais simples de ser feito e também necessário (MORIMOTO, 2008).

### 2.1.3 SERVIDORES DE INTERNET

Para que se possa entender melhor o que são servidores de Internet e como funcionam, é necessário abordar o que é a Internet e como ela funciona. A Internet tem como peça principal os roteadores, distribuídos estrategicamente pelo mundo e interligados através de uma malha de cabos submarinos de fibra óptica, interligando praticamente todos os continentes.

São os roteadores que fazem a ligação entre os diferentes segmentos de rede tornando a Internet uma só rede. Conhecendo seus vizinhos e as redes conectadas aos mesmos, o roteador escolhe o caminho mais perto para um pacote chegar ao seu destino (MORIMOTO, 2008).

Para que os pacotes trafeguem pela rede, precisam sair de algum lugar e ir para outro, é nesta ação que os data centers, que hospedam a maioria dos servidores com conteúdo da

Internet, fazem seu papel e são conhecidos como servidores de Internet. Data center é um ambiente controlado com salas refrigeradas, *links* de acesso à Internet redundantes, geradores de energia, instalações elétricas especiais e manutenção 24 horas por dia, para permitir que os servidores de Internet funcionem de forma confiável (MORIMOTO, 2008).

## 2.2 SEGURANÇA EM REDES CORPORATIVAS

As organizações, de todos os tipos e segmentos, fazem parte do mundo virtual, a Internet. As empresas não podem se dar ao luxo de não fazer parte deste meio virtual, existem diversos processos do dia a dia de uma empresa que necessitam da Internet para que eles ocorram. O mundo virtual possui problemas, soluções e paradigmas que se assemelham com mundo real, onde temos empresas privadas que são acessadas (visitadas), no virtual temos servidores, máquinas de usuários que respectivamente também são acessadas.

Como ocorre no mundo real, o virtual também necessita de proteção contra os acessos indesejados, as lojas no mundo real permitem que seus clientes acessem as dependências da loja até uma determinada área destinada a ele, nas áreas restritas da empresa a entrada dos clientes é vedada. Esse tipo de medida de restrição de acesso também deve ser aplicado no mundo virtual, para que somente pessoas autorizadas possuam acesso aos dados e informações restritas da empresa (NAKAMURA, 2007).

Atualmente, existem várias empresas especializadas no monitoramento de vírus e ataques na Internet que ocorrem no mundo todo, apresentando dados que contribuem para realização de medidas de segurança. Como mostra a Figura 1, a lista dos 10 ataques mais utilizados e seus respectivos percentuais e um gráfico com a quantidade de ataques diários variam entre 20 milhões e 32.5 milhões no período entre setembro e outubro de 2018 (NAKAMURA, 2007).

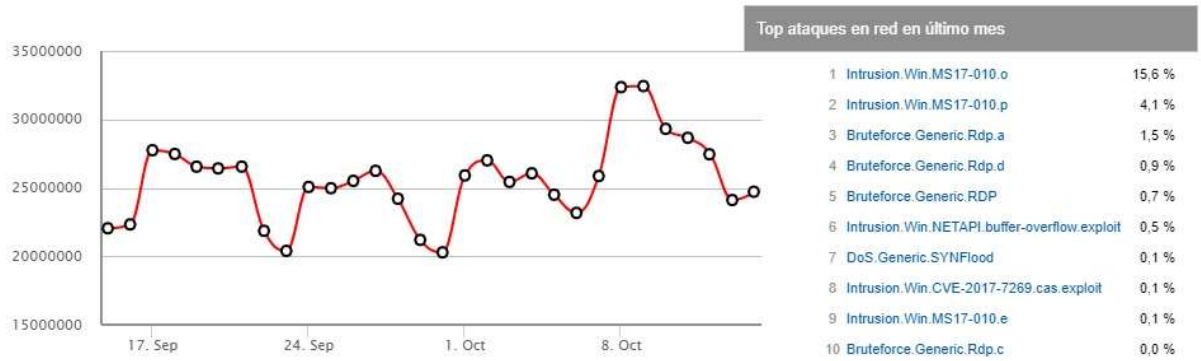



**Figura 1 – Estatística de ataques**
Fonte: SECURELIST (2018).

As duas primeiras posições, sexta e nona posições da lista de ataques estão as vulnerabilidades do SO Windows, mais especificamente o SMB (Server MessageBlock), um protocolo de rede da camada de aplicativo que utiliza as portas TCP 139 e 445, utilizadas no compartilhamento de acessos a serviços remotos, arquivos e impressoras. Da terceira a quinta posição da lista e s, em décimo lugar, está o ataque de força bruta, que consiste em descobrir o usuário e senha utilizados para o acesso remoto do Windows através do protocolo RDP (*Remote Desktop Protocol*), protocolo da Microsoft que apresenta uma interface gráfica para o usuário realizar uma conexão remota por meio de uma rede. Na sétima colocação está um *malware*, programa projetado para gerar ataques através de várias solicitações para outro computador. Na oitava colocação estão os ataques de intrusão, que exploram serviços dos SOs que possuem alguma vulnerabilidade ou foram configurados de forma errada, deixando assim, uma vulnerabilidade e permitindo o ataque.

Para que se tenha segurança nas informações e dados da empresa no mundo virtual é necessário tomar algumas medidas de segurança, as quais devem estar em constante evolução para evitar possíveis novos métodos de ataques. As medidas de segurança no meio virtual ocorrem através de *firewalls*, que é como se fossem os porteiros, vigias, portões, cercas da vida real. É no *firewall* que a política de segurança para acessar os dados é configurada, quais os critérios para se ter acesso a determinados dados e informações (NAKAMURA, 2007).

### 2.2.1 FIREWALL

É de suma importância manter os dados gerados pela empresa e os arquivos utilizados protegidos de possíveis ataques vindos da Internet. Para suprir esta necessidade, um

servidor Linux pode ser configurado como *firewall* desempenhando o papel de *border firewall*, que fica situado entre a Internet e a rede local protegendo os dados de acessos externos indesejados (MORIMOTO, 2008). A implantação de um *firewall* é um dos métodos que pode ser utilizado nas redes privadas como um intermediador que monitora a comunicação entre a rede local LAN (*Local Area Network*) e a Internet, por onde passará todo o tráfego de dados que entra e sai da LAN, como apresenta a Figura 2.

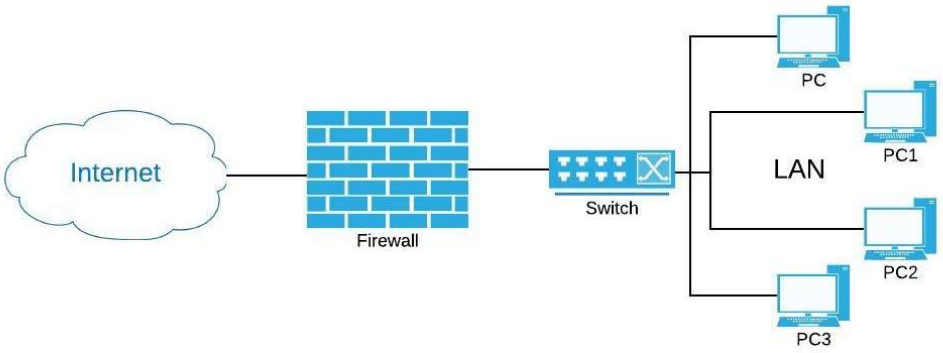



**Figura 2 – Estrutura da rede com firewall**
Fonte: AUTORIA PRÓPRIA (2018).

A utilização do *firewall* geralmente é para proteger uma rede segura de outra rede pública, não tão confiável assim, é um dos mais antigos e está entre os principais e mais conhecidos métodos de segurança utilizados. Em várias empresas o acesso à Internet necessita de controle para que os usuários não acessem sites de redes sociais ou qualquer outro inapropriado para o ambiente de trabalho, como consequência dessas necessidades ocorreu a evolução do *firewall* para atender essas necessidades.

Composto por vários componentes, com funcionalidades diferentes, mas cada um com sua importância dentro da política de segurança da rede, o *firewall* conta com as funcionalidades de filtros, *proxies*, *bastion hosts*, Zonas desmilitarizadas, Nat (*Network AddressTranslation*), VPN (*Virtual Private Network*) e autenticação/certificação, que foram inseridos no contexto devido à necessidade de monitorar, limitar, otimizar e controlar o acesso à Internet e as redes privadas (NAKAMURA, 2007).

Os filtros analisam os pacotes de dados através das informações que estão contidas nos seus cabeçalhos, dessa forma, o pacote é aceito ou descartado. A configuração do *proxy* cria uma máscara para o endereço da máquina local através de conexões TCP (*TransmissionControlProtocol*) no *firewall*, dessa forma ocorre um reendereçamento do tráfego de dados evitando a conexão direta entre o servidor externo e a máquina interna. Bastion hosts são equipamentos que possuem serviços instalados que estão em contato direto

com a Internet, fornecendo algum conteúdo. Esses equipamentos devem estar sempre atualizados fornecendo somente as aplicações essenciais e com o máximo de segurança possível, para minimizar as possíveis chances de ataque, pois esses serviços se encontram em uma DMZ (*DeMilitarized Zone*). Uma zona desmilitarizada DMZ é criada justamente para conter os Bastions Hosts, isso porque ela é uma rede que fica entre a Internet, rede não segura, e a rede interna que está protegida pelo *firewall*. Dessa forma, se o equipamento que está nela sofrer algum ataque e ficar comprometido, os demais equipamentos contidos na rede interna não serão afetados e continuarão seguros.

A configuração do NAT (*Network AddressTranslation*) se dá através da necessidade de endereços de IP (*Internet Protocol*) válidos para navegar na Internet. Dessa forma, os endereços IP internos inválidos são convertidos em endereços válidos e roteáveis, para navegar. Atuando dessa forma o NAT contribui também para a segurança, escondendo os endereços de rede da rede interna, o que dificulta possíveis ataques. Devido à necessidade de manter a integridade dos dados e o sigilo de informações geralmente de empresas a VPN (*Virtual Private Network*), foi criada justamente para houvesse uma comunicação segura entre redes diferentes baseadas em determinados protocolos passando pela Internet. O protocolo-padrão da VPN mais conhecido como IPSec (IP Security) garante o tráfego seguro dos dados através de criptografia.

Outra forma de contribuir com o *firewall* é a autenticação e certificação, que podem ser alternativas de segurança que são baseadas em endereços IP, *tokens*, *smartcards*, certificado digital, senhas ou biometria. Como o *firewall* será a única entrada para a rede protegida, pode ser configurado nele um balanceamento de carga, onde pode ser priorizado o tráfego que possui uma importância maior. Considerada uma das tecnologias mais “antigas” na área de segurança, o *firewall* está em constante evolução, devido as novas necessidades de segurança que vão surgindo com o passar do tempo, e não pode ser considerada uma tecnologia estável.

### 2.2.2 DHCP

O bom funcionamento de uma rede TCP/IP depende da sua configuração. Todo dispositivo que estiver conectado em uma rede com configuração não compatível com a mesma terá problemas tanto para navegar na Internet, quanto na rede interna. O serviço DHCP fornece, automaticamente, para os dispositivos da rede, dados para que ocorra a

conexão entre eles e com a Internet. Os dispositivos recebem informações como endereço de IP, máscara de sub-rede, domínios, *gateways* de rede, endereços dos servidores DNS, entre outras informações.

Através do DHCP, o administrador de rede consegue estruturar e centralizar as informações utilizadas por cada um dos dispositivos da rede. O serviço possui uma tabela com informações de cada cliente da rede, informações como MAC (*Media Access Control*) da placa de rede, endereço de IP, tempo que a máquina está com esse endereço, entre outras informações importantes para o gerenciamento e funcionamento da rede. Sempre que um dispositivo se conectar na rede e não possuir um endereço de IP, seu sistema operacional envia uma mensagem *broadcast* procurando por um servidor DHCP, que fornecerá todos os dados necessários para navegar pela rede interna ou externa (MOTA FILHO, 2012).

### 2.2.3 SAMBA

A integração em ambientes heterogêneos que possuem dispositivos com o Linux e também com o Windows é fundamental para o compartilhamento de arquivos, impressoras, configurar o controle de acessos dos usuários ou até mesmo para alguns recursos mais avançados como serviço de diretório quando um servidor Linux fará o controle de domínio dos dispositivos Windows. É através do serviço Samba que máquinas com sistemas operacionais diferentes conseguem compartilhar arquivos e impressoras.

Utilizando o protocolo SMB/CIFS (*Server MessageBlock/Common Internet File System*), protocolo responsável pela permissão da comunicação entre as máquinas Windows e Linux. É este protocolo que intermedia e permite que os arquivos e impressoras contidos na máquina com o SO Windows, compartilhem com as máquinas com o SO Linux, dessa forma o compartilhamento entre os dispositivos da rede se torna mais simples e rápido (BRITO, 2017).

## 2.3 DISTRIBUIÇÕES LINUX

Atualmente existem muitas distribuições Linux disponíveis para uso e, basicamente, todas podem ser utilizadas como servidores. A escolha de qual distribuição Linux utilizar é pessoal e vai depender de como será a configuração do servidor, e qual o tipo de serviço que

será instalado. No geral, os serviços utilizados pelas diferentes distribuições são os mesmos, o que muda, de uma distribuição para outra, é como a ferramenta é instalada. Cada distribuição possui suas particularidades e suas ferramentas de configuração (MORIMOTO, 2008).

### 2.3.1 HISTÓRIA DO DEBIAN

Criado em 1993 por Ian Murdock, o Debian é um sistema operacional completo, composto por softwares, sistema de gestão e instalação baseados no Linux. Ao desenvolver o sistema, Murdock, priorizou que duas características eram fundamentais em seu sistema: qualidade e liberdade. O desenvolvimento seria com todo cuidado possível para que o sistema correspondesse a altura o kernel Linux, e, ao finalizar, a distribuição não seria comercial e seria competitiva para concorrer em condições de igualdade com as principais distribuições que eram comerciais à época (HERTZOG e MAS, 2015).

A distribuição Debian segue à risca todos os princípios do software livre, principalmente para atender o desejo de seu criador com relação a qualidade. As novas versões do Debian só são liberadas após vários meses de testes para encontrar possíveis *bugs* no sistema. Não importa se a data inicial prevista para o lançamento de uma versão não será cumprida e necessite ser adiada, a prioridade é lançar uma versão onde todos os *bugs* críticos do sistema sejam resolvidos antes de lançar a nova versão (HERTZOG e MAS, 2015).

O projeto Debian é gerenciado por uma associação americana voluntária e sem fins lucrativos, contando com aproximadamente mil programadores trabalhando no seu desenvolvimento. Por trás dessa equipe gigantesca de programadores está uma comunidade de voluntários que são desenvolvedores esporádicos, pessoas que relatam *bugs*, patrocinadores etc.. Existe uma grande estrutura oferecida por patrocinadores onde vários servidores estão conectados através da Internet para contribuir com o projeto. Os desenvolvedores Debian são livres e podem se envolver em várias equipes aumentando, assim, sua responsabilidade no projeto, mas, cada desenvolvedor é responsável por, pelo menos, um pacote do sistema (HERTZOG e MAS, 2015).

Por mais que a equipe responsável pelo sistema seja gigantesca, a política para tratar da manutenção dos pacotes que compõe o sistema segue regras que garantem a qualidade dos mesmos, regras essas que estão contidas no manual de políticas Debian e podem ser vistas através do endereço https://www.debian.org/doc/debian-policy/. Este manual de políticas

contribui para o lançamento de versões confiáveis e estáveis, contendo regras que onde uma versão só pode ser lançada após vários testes que confirmem sua estabilidade. Nunca pode ser lançada uma versão se ela não estiver estável (HERTZOG e MAS, 2015).

### 2.3.2 HISTÓRIA DO UBUNTU

A história do Ubuntu teve início em abril de 2004, através da ideia de Mark Shuttleworth em realizar uma reunião com vários desenvolvedores que faziam parte dos projetos Debian, GNU Arch e GNOME,para debater e trocar ideias. Nesta reunião, Mark perguntou para os desenvolvedores se existia a possibilidade de criar um SO melhor do que os existentes, e a resposta foi “sim”. Com base nessa afirmativa, Mark então, questionou os desenvolvedores perguntando como deveria ser esse sistema, e quais as soluções para esses novos apontamentos feitos por eles. Após chegarem as soluções para os apontamentos feitos decidiram tornar esse sistema real.

O grupo de desenvolvedores do projeto Ubuntu se autodenominou “Warthogs”, e deram também um codinome para a primeira versão WartyWarthorg. Decidiram então que teriam um prazo de 6 meses para que um protótipo desse SO fosse “apresentado”, em pouco tempo após esse lançamento o Ubuntu já estava em primeiro lugar em vários rankings sobre popularidade de distribuições GNU/Linux. O projeto Ubuntu teve o maior crescimento e a trajetória mais impressionante da história dentre todos os projetos de software livre (HILL *etal*, 2018).

Conforme ocorreu com a primeira versão as versões posteriores também foram e são lançadas rigorosamente a cada seis meses, é o primeiro SO a seguir um calendário de lançamentos. No ano de 2006 notou-se a necessidade de lançar uma versão com suporte a longo prazo, desde então a cada quatro versões lançadas, ou seja, de dois em dois anos é lançada uma versão LTS (LongTermSupport), que é mais estável. O Ubuntu possui uma única equipe que é dividida em comercial e comunitária, trabalhando junto para produzir uma única versão para os usuários. Usuários que desejam um suporte mais avançado, consultoria, ferramentas diferenciadas de gerenciamento, entre outras vantagens, são atendidos pela Canonical, empresa criada por Mark com fins lucrativos para pagar a equipe comercial de desenvolvedores (UBUNTU, 2018).

Atualmente, o Ubuntu possui várias ferramentas e versões diferentes disponíveis para várias funções e públicos dos mais variados. Está incluso, nesse leque de opções, a versão Ubuntu Server, exclusiva para servidores. Através dos lançamentos semestrais o Ubuntu defende a ideia de que seus sistemas operacionais são os mais atualizados possíveis e compatíveis com as novas arquiteturas do mercado.

### 2.3.3 HISTÓRIA DO RED HAT

No ano de 1993 a Red Hat (chapéu vermelho) é fundada, Marc Ewing, um dos co-fundadores da empresa, escolheu este nome porque quando trabalhava no laboratório de informática da Carnegie Mellon, ele usava um chapéu vermelho que ganhou do seu avô. Desta forma, quando iniciou a distribuição da sua versão Linux, Marc escolheu o nome Red Hat. Outro co-fundador, Bob Young, defensor do código aberto e da Red Hat, apresentava a empresa utilizando analogias com carros e convencia os clientes a utilizar seu sistema (RED HAT, 2018).

A Red Hat se tornou a primeira empresa de software com código-fonte aberto a desenvolver um SO focado em servidores chamado RHEL (Red Hat Enterprise Linux), para atender as necessidades corporativas mais exigentes e críticas para o governo e empresas privadas. Com o desenvolvimento do RHEL, em março de 2012, versão para servidores comerciais, estável e, suportada pela empresa, que se tornou o principal produto, surge o Fedora, distribuição patrocinada pela Red Hat e que é gratuita para uso pessoal (NEGUS, 2014).

Agregado a venda do RHEL, a Red Hat oferece, para os seus clientes, vários benefícios e diferentes ferramentas. Benefícios como uma assinatura que permite implantar qualquer versão do SO. Caso o cliente não utilize mais o RHEL, essa licença pode ser utilizada para outras ferramentas da empresa. Outro diferencial que a empresa possui é o empacotamento RPM (*Red Hat Package Manager*), um formato específico da distribuição, sendo que este pacote não possui somente os arquivos referentes a atualização e configuração, mas também informações sobre a versão do pacote que está sendo instalado, informações como data de criação, quem criou, facilitando assim encontrar o pacote instalado para removê-lo ou atualizá-lo.

Outras inovações, criadas pela Red Hat, como o instalador Anaconda, facilitaram a instalação do Linux através de perguntas básicas conduzindo o usuário para uma instalação padrão do SO. O painel com administração gráfica para tarefas administrativas básicas de configuração e instalação de dispositivos, permitindo mais facilidade, permitindo que os usuários possam administrar o sistema sem ter que executar linhas de comandos. (NEGUS, 2014).

## 2.4 COMPARAÇÃO ENTRE DISTRIBUIÇÕES LINUX

Esta comparação apresenta as características de cada um dos SO, baseados no Linux.Com base nesta comparação, será definido qual SO será instalado e configurado nos dois servidores que serão implementados na estrutura da empresa.

Serão apresentadas características das três distribuições Linux naQuadro1.

**Quadro 1 - Comparação distribuições Linux**

| Distribuição Linux | Custo | Características |
|---|---|---|
| Debian | Grátis | Lançamento de versão não obedece calendário, só é lançada quando está estável e segura, Manutenção feita pelo projeto da comunidade Debian, grande compatibilidade com softwares e hardwares. |
| Red Hat | Pago | Versão exclusiva para servidores, empacotamento personalizado, integração com softwares de terceiros, instalador intuitivo, painel com administração gráfica. |
| Ubuntu | Grátis/Pago | Versão exclusiva para servidores; versões lançadas a cada 6 meses; manutenção feita pela equipe da Canonical; grande compatibilidade com softwares e hardwares; versões instáveis devido ao seu lançamento a cada 6 meses. |

Fonte: AUTORIA PRÓPRIA (2018).

### 2.4.1 PORQUE A DISTRIBUIÇÃO DEBIAN

No momento de escolher um sistema operacional para instalar em um computador *desktop,* alguns usuários se preocupam com determinados critérios que, para eles, são importantes. Em se tratando de servidores, alguns fatores como estabilidade da versão (sem falhas ou *bugs*), segurança, ferramentas disponíveis para os serviços que são necessários para

a empresa, desempenho, período de atualizações e suporte, devem ser analisados e levados em consideração.

A escolha pela distribuição Debian é devida sua estabilidade nas versões lançadas, segurança, variedade de ferramentas administrativas para as redes de computadores, por ser uma das distribuições mais antigas no mercado e seus pacotes de atualização serem sem custo. Todos os fatores citados colaboram para redução do tempo de interrupções dos serviços fornecidos pelo servidor (HERTZOG e MAS, 2015).

# 3 MATERIAIS E MÉTODO

Este capítulo enfatiza os materiais e método utilizados para o desenvolvimento do projeto, ocorrendo uma divisão dos materiais entre físicos e virtuais, sendo físico os componentes que compõem um computador e virtual os sistemas operacionais que interagem com o meio físico através de aplicações específicas para cada serviço.

O método que foi utilizado para o desenvolvimento do trabalho, leva em consideração o uso de softwares livre baseados em Linux e a montagem de servidores através de hardwares que não foram desenvolvidos para tal finalidade, com a intenção de reduzir custos e apresentar uma solução para a empresa.

## 3.1 MATERIAIS

Para o desenvolvimento deste trabalho foi incluído, no cenário atual da empresa, apresentado na Figura 3, dois novos servidores para disponibilizar os serviços responsáveis pela segurança e melhoria do desempenho da rede, servidor *firewall* e servidor DHCP e dados.

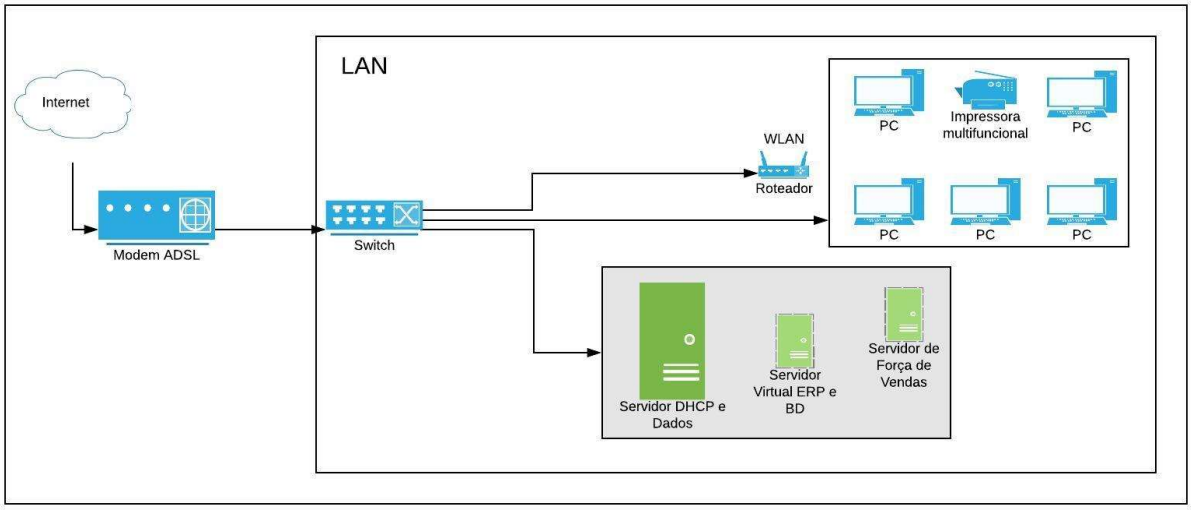



**Figura 3 – Estrutura de rede atual da empresa**
Fonte: AUTORIA PRÓPRIA (2018).

A inclusão do servidor *firewall,* responsável pela segurança da rede local, ocorreu entre o modem ADSL (*Asymmetric Digital SubscriberLine*) e o *switch*, este computador possui dois adaptadores de rede responsáveis pelo tráfego entre a Internet e a rede local. O

acesso à Internet chega no *firewall* através da interface de rede enp0s3. A interface enp0s8 está conectada no *switch* que é responsável pela distribuição da rede local. O servidor com os serviços de DHCP que desempenhará a função de atribuir endereços aos dispositivos conectados na rede e armazenar informações sobre os mesmos, e o serviço do Samba, que compartilhará e armazenará os dados, e compartilhará dispositivos na rede local, foi incluso na rede após o *switch* como o outro servidor existente na rede.

### 3.1.1 IPTABLES

No Linux, o *firewall*, está agregado diretamente na arquitetura do kernel. Desta forma, todo tráfego de dados que sai (*output*), entra (*input*) ou atravessa (*forward*) é analisado diretamente no núcleo do SO. As regras que determinam se um pacote possui permissão ou não para seguir, são baseadas no endereço/porta de origem e endereço/porta de destino e qual o protocolo de transporte. Essas informações estão contidas no cabeçalho do pacote (BRITO, 2017).

O nome do *firewall* é *NetFilter*, mas popularmente é conhecido por *iptables*, que é a interface que o usuário utiliza para escrever as regras e administrar o *firewall*. Um servidor *firewall* pode ser considerado de natureza *stateful*, que permite criar regras mais flexíveis e armazenar registros das conexões realizadas, consumindo mais recursos de *hardware*, ou pode ser considerado de natureza *stateless*, que é menos flexível, não armazena registros das conexões e utiliza as regras mais explícitas criadas pelo administrador.

Todas as regras criadas pelo administrador encontram-se armazenadas em tabelas que o *iptables* cria automaticamente para que as regras sejam salvas conforme são criadas. Cada tabela criada possui uma função específica e diferente da outra, as regras criadas com a função de filtragem de pacotes que permitem ou não que o pacote siga caminho se encontram na tabela *filter*, o *firewall* possui dois complementos: (i) a tradução de endereços, onde suas regras ficam armazenadas na tabela *nat*; e (ii) a outra função, que é complementar, está ligada a implementação de serviços de QOS (*Qualityof Service*), e são armazenadas na tabela *mangle*, utilizadas para realizar a manipulação avançada dos cabeçalhos dos pacotes.

Cada uma das regras criadas pelo administrador deve estar ligada a uma das três tabelas, logicamente a qual corresponda com o objetivo pretendido pela mesma. Se o responsável pela criação da regra não informar a tabela que corresponde com a regra, no

momento de sua criação, com a utilização do parâmetro -t, a regra será alocada na tabela *filter*, que é a padrão e que corresponde a função básica do *firewall*. As três tabelas são capazes de trabalhar com fluxos e tráfegos de dados de diferentes sentidos, mais conhecidos como *chains*. Qualquer regra criada, que esteja em ambas as tabelas, pode tomar uma decisão com relação ao fluxo de *INPUT* (Entrada), *OUTPUT* (Saída) ou *FORWARD* (atravessando) pelo servidor.

Para criar regras no *iptables*é necessário utilizar alguns parâmetros que correspondem a informações referentes a qual tabela a regra corresponde. A *chain*que ela tratará, qual a camada de transporte do pacote que corresponde a regra, qual a porta ou IP que se refere o tráfego e, por último, qual a ação que a regra exercerá sobre o pacote. A Quadro 2 apresenta os parâmetros mais comuns utilizados no *iptables.*

**Quadro 2 – Parâmetros comuns do *iptables***

| Parâmetro | Descrição | Opções |
|---|---|---|
| -i | Interface de entrada | Nome da interface |
| -o | Interface de saída | Nome da interface |
| -s | Endereço IP de origem | Host ou rede |
| -d | Endereço IP de destino | Host ou rede |
| -p | Protocolo | Icmp ou TCP ou UDP |

Fonte: BRITO (2012).

Utilizando a palavra *iptables*, é iniciada a interface em nível de usuário que possibilita escrever as regras que serão utilizadas pelo *kernel*, como podemos observar no exemplo a seguir:

```
iptables –t filter –A INPUT –p tcp --dport 80 –j ACCEPT
```

Descrevendo a regra acima, na tabela *filter* (-t *filter*) será inserida, na*chain INPUT* (-A INPUT), uma regra que terá ação sobre os pacotes que entram com o protocolo TCP (-p tcp), endereçados para a porta 80 (--dport 80). A ação é de aceitar todos os pacotes que se enquadram nesta regra (–j ACCEPT). Todas as regras criadas serão perdidas caso ocorra um *reboot* na máquina. Portanto, é essencial que elas sejam armazenadas em um *script* que será executado no processo de inicialização da máquina, retornando assim todas as regras. A política padrão do *iptables* é de *ACCEPT*, conhecido também como caixa branca, aceitando todo o tráfego. É recomendado, do ponto de vista de segurança, que as regras sejam todas

*DROP*, conhecida como caixa preta, recusando todo tráfego, exceto as permissões, se assim existirem (BRITO, 2017).

## 3.2 MÉTODO

Este trabalho apresenta uma solução utilizando o sistema operacional Linux e suas ferramentas específicas para o gerenciamento de redes locais, propondo a implantação em empresas de pequeno e médio porte, de um servidor *firewall* para deixar a rede local segura e um servidor com serviços de DHCP e SAMBA que contribuirão para a otimização da navegação da rede, permitindo o armazenamento e compartilhamento de dados.

A distribuição Linux instalada tanto no servidor de *firewall* quanto no servidor de DHCP e SAMBA foi a Debian na versão 9. A instalação em ambos os servidores foi realizada sem instalar a interface gráfica, contribuindo para o desempenho do servidor. No servidor que irá fazer a linha de defesa da rede interna não necessitou realizar a instalação de serviços, pois o Netfilter/iptables são ferramentas nativas do Linux, só necessitaram de configurações e ativação.

Foi configurado um script com regras para o firewall as quais iniciam junto com o SO toda vez que o servidor for iniciado, o bloqueio total com liberação de acessos que são somente necessários para a empresa ocorrerá em um segundo momento. De qualquer forma já foram criadas duas regras que liberar as portas que o sistema de força de vendas utiliza para se comunicar com o servidor interno.

No servidor de DHCP e compartilhamento através do SAMBA foram realizadas instalações e configurações para ajustar conforme a necessidade. Primeiramente foi instalado o serviço de DHCP e em seguida configurado o range de IP´s que devem ser atribuídos para novos dispositivos na rede. A instalação e configuração do samba foi um pouco mais complexa, porque além da instalação do serviço foram feitas várias configurações para criar pastas, alterar permissões das mesma, criar usuários e grupos, atribuir os usuários para os grupos, alterar os grupos das pastas e criar os usuários dentro do SAMBA, para que pudessem ter acesso as pastas criadas.

# 4 RESULTADOS

Este trabalho consiste em apresentar o processo de implantação de servidores Linux em redes corporativas de pequeno a médio porte, instalando um servidor *firewall* e um servidor com serviços de DHCP e Samba. A inclusão desses dois servidores na rede local contribuirá para que a rede esteja segura e com um melhor desempenho.

O cabeamento é o início de toda rede de computadores, através dele que surgem os pontos de acesso via cabo ou sem fio, mais conhecido por WIFI (*Wireless Fidelity*) que os dispositivos se conectam e fazem parte de uma rede, podendo ser ela simples contendo somente dois dispositivos ou até mesmo ser bem complexa com vários dispositivos e/ou uma ou várias redes dentro de uma rede.

É muito comum, em empresas de pequeno porte, as redes possuírem um único servidor na rede que, ao mesmo tempo, compartilha um sistema de gerenciamento financeiro, serve como um servidor de banco de dados, como um servidor de arquivos e como servidor de serviços de rede, como, por exemplo, o DHCP. Esta estrutura de rede pode até atender as necessidades da empresa por um período, porém ela não atende uma necessidade básica que toda empresa deveria se preocupar, que é a segurança dos seus dados.

Com o passar do tempo e o crescimento da empresa, a quantidade de informações geradas cresceu, os serviços agregados a rede e ao servidor também aumentam, tonando a rede mais lenta devido ao tráfego de pacotes e, principalmente, pelo único servidor desempenhando várias funções.

Pensando em segurança dos dados e a melhoria de desempenho da rede que, através do método experimental, ocorrerá a implantação de servidores Linux buscando observar os resultados que os mesmos podem oferecer em um ambiente controlado, recebendo influência de diversas variáveis a todo momento (GIL, 2008).

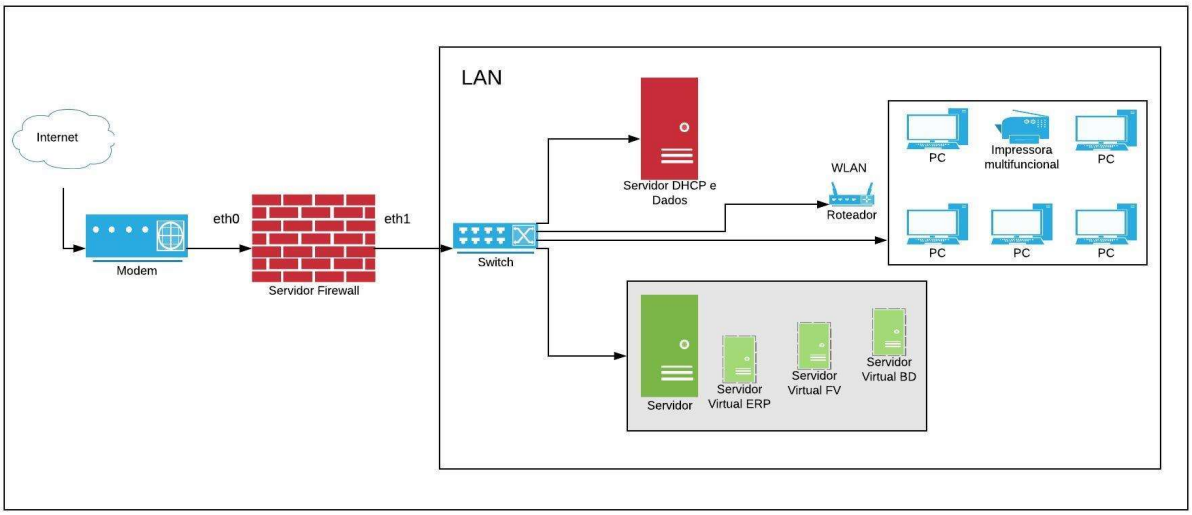



**Figura 4 – Estrutura de rede com a inclusão dos novos servidores**
Fonte: AUTORIA PRÓPRIA (2018).

Conforme exposto na Figura 4, o servidor *firewall* é responsável por proteger a rede local segura, da Internet não segura. Todo o tráfego que entrar ou sair da rede local obrigatoriamente passa pelo *firewall* que realiza o controle dos pacotes conforme as regras configuradas. O servidor de DHCP e dados ficaram na rede local protegido pelo *firewall*, gerenciando os endereços IP dos dispositivos da rede, armazenando e compartilhando dados e compartilhando a impressora.

Em ambos os servidores foi instalado o SO Debian 9, sendo a última versão estável da distribuição. No servidor *firewall*, além do SO, foi configurado o *iptables*, ferramenta que realiza todo controle de pacotes da rede local. Por ser um servidor de borda não possui nenhuma outra ferramenta instalada. Neste servidor foram configuradas todas as regras que trata da segurança da rede local e do acesso dos usuário, atendendo as necessidades comerciais da empresa.

No outro servidor que foi alocado dentro da rede local, foi instalado e configurado o serviço de DHCP, para fornecer endereços IPs para os dispositivos que se conectarem na rede e não possuem um endereço válido. Toda a configuração de range de IP's alocados para essa distribuição e também o *script* para executar na inicialização deste servidor foram realizadas, para que não ocorra problemas na configuração, caso o servidor seja desligado ou reiniciado. Por fim, foi instalado o Samba, onde foram criadas pastas públicas e privadas para o compartilhamento de arquivos e informações entre os usuários da rede local.

O sistema operacional instalado no servidor, os serviços que fornecerão a segurança, armazenamento e compartilhamento de dados são softwares livres, estando isentos de

pagamento de qualquer taxa ou mensalidade, contribuindo, assim, para o financeiro da empresa. Os custos para a empresa foi na aquisição de duas máquinas *desktop* normal que foram utilizadas como servidores para implementar melhorias na rede.

## 4.1 ESTRUTURA ANTERIOR A IMPLANTAÇÃO

O cenário da empresa de médio porte, antes da implantação dos servidores Linux, pode ser definida como crítica, isso porque tem a dependência de somente uma máquina física para fornecer quatro serviços diferentes em três servidores configurados através de máquinas virtuais. Em uma máquina virtual VM (*Virtual Machine*) está instalado o sistema operacional Windows Server 2008 R2 que fornece o serviço de ERP (*Enterprise Resource Planning*) para gerenciamento da empresa, e nesta mesma VM está instalado o banco de dados do ERP.

A segunda VM possui instalado o sistema operacional Windows Server 2008 R2 fornecendo o sistema de força de vendas para os vendedores externos da empresa, e, a terceira VM está configurada com o sistema operacional Linux Debian 8 Jessie, fornecendo os serviços de servidor de arquivos e servidor DHCP.

O *hardware* que executa as três VMs é uma máquina *desktop* normal montada com um processador Core I3, 12GB de memória, dois HD's de 1TB, 7200 Rpm cada, uma placa-mãe com *socket* LGA 1151, 4 slot's para memória DIMM DDR4, 2 slot's PCI *express* e 2 slot's PCI, duas placas de rede /10/100/1000 Intelbrás, e uma fonte real de 500 W. É de conhecimento dos profissionais de TI que máquinas *desktop,* fabricadas para uso de atividades do dia a dia em empresas, não são projetadas para serem utilizadas como servidores, mas é comum encontrar este cenário em pequenas, médias e até grandes empresas, por questões de economia (POPOVICI, 2015).

Esta estrutura apresentada, pode até atender a necessidade da empresa por um período, sem que ocorram problemas no *hardware* ou no(s) *software*(s) que estão instalados, pois, se um problema de *hardware* impedir a máquina de funcionar a empresa toda pode parar. Mas o maior problema que pode ser destacado nesta estrutura de rede é a falta de segurança dos dados que são gerados pela empresa e armazenados no banco de dados, bem como, os que estão armazenados no servidor de arquivos como foi mostrado anteriormente, na Figura 3.

A estrutura da empresa possui uma rede lógica projetada para distribuir os pontos de rede pelos setores da empresa, como pode ser visto na Tabela 1. Todos os cabos da rede estão centralizados em um painel lógico, que se liga a um mini *rack* de parede. No setor da

recepção existe um ponto de rede; na sala da diretoria temdois pontos de rede; na sala do setor administrativo tem 11 pontos de rede; na expedição, responsável pela conferência dos produtos, existem 5 pontos de rede; no depósito tem 10 pontos de rede; na sala do telemarketing são 5 pontos de rede; e, na sala do TI, onde encontra-se o servidor, possui quatro pontos de rede. No total são 38 pontos de rede, sendo 12 pontos de acesso ativos.

Entre os pontos de rede ativos, 11 pontos são de máquinas dos usuários, dois pontos de rede que estão conectados nas duas placas de rede da máquina servidor, um ponto de acesso que possui uma impressora conectada e um ponto de acesso com um roteador WIFI, formando uma nova rede WLAN, separada da rede da empresa que é para acesso de dispositivos móveis dos funcionários. Esta estrutura foi apresentada anteriormente na Figura 4.

**Tabela 1 – Pontos de rede da empresa.**

| Setor | Qtd. Pontos Ativos | Qtd. Pontos Inativos | Total |
|---|---|---|---|
| Recepção | 0 | 1 | 1 |
| Diretoria | 1 | 1 | 2 |
| Administrativo | 7 | 4 | 11 |
| Expedição | 2 | 3 | 5 |
| Depósito | 0 | 10 | 10 |
| Telemarketing | 3 | 2 | 5 |
| TI | 2 | 2 | 4 |
| **Total:** | **15** | **23** | **38** |

Fonte: AUTORIA PRÓPRIA (2018).

Para distribuir todos os pontos de redes da empresa, em um mini rack de parede, está alocado um *switch* modelo *Power Connect* 2824 que está conectado diretamente no modem ADSL (*Assymetrical Digital SubscriberLine*) que se encontra dentro do *rack*. Neste cenário, a rede da empresa não é complexa, nem possui muitos dispositivos conectados que dificultem o seu gerenciamento, porém, a rede não possui proteção alguma de ataques externos, o que pode ser considerada uma grava falha de segurança.

## 4.2 SERVIÇOS NECESSÁRIOS PARA MELHORIA DA REDE

Para se definir a quantidade de servidores que deveriam ser acrescentados na rede e quais serviços deveriam ser instalados em cada servidor para contribuir de forma significativa com a velocidade da rede, compartilhamento e segurança dos dados, foi necessário uma

análise de todo cenário da empresa, pontuando os serviços que atenderiam a necessidade e poderiam trazer melhorias para a rede, se instalados nos servidores.

Primeiramente, para que fosse iniciada a escolha dos serviços que a rede necessitaria, foi analisado o servidor atual que a empresa possuía. A Figura 5 mostra como o servidor estava configurado, tendo duas VM (*Virtual Machine*), a primeira VM possui instalado os serviços de ERP (*Enterprise Resource Planning*) e BD (Banco de Dados) e a segunda VM contêm o serviço de FV (Força de Vendas). O Linux que hospedava essas duas VM's executa também o serviço de DHCP e o SAMBA para compartilhamento e armazenamento de arquivos.

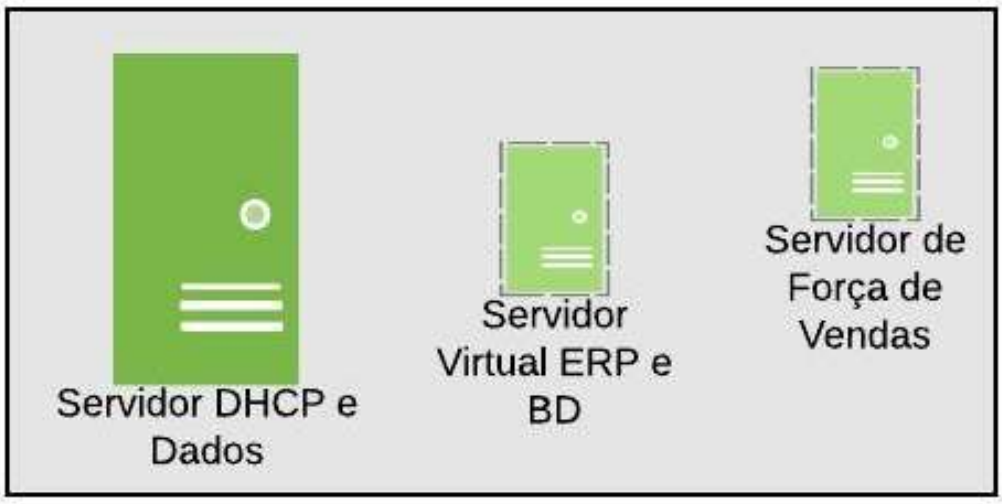



**Figura 5 – Configuração do servidor atual da empresa**
Fonte: AUTORIA PRÓPRIA (2018).

Ao analisar o servidor atual, percebeu-se que já existiam dois serviços instalados, que era o DHCP, para melhor gerenciando da rede e o SAMBA, para compartilhamento de arquivos, serviços esses que poderiam ser otimizados para melhorar o desempenho da rede. A configuração atual do SAMBA não possuía uma lixeira para os arquivos que fossem excluídos, melhoria necessária para a nova instalação. As pastas não possuíam restrições, dessa forma os arquivos poderiam ser acessados por qualquer usuário que estivesse conectado na rede, e se algum arquivo fosse excluído seria perdido, configurar restrições para as pastas e um serviço de *firewall* para aumentar a segurança da rede.

Para se ter um cenário onde as interrupções por falha de *hardware* sejam o menor possível, foi necessário configurar dois novos servidores Linux, além do atual servidor da empresa, deixando o servidor atual responsável somente pelo fornecimento dos serviços referentes ao sistema de ERP, BD e FV. Esta ação deixou os serviços essenciais da empresa

com um hardware exclusivo para processar as atividades de suma importância para o dia a dia da empresa, diminuindo assim o esforço realizado pela parte física do servidor, resultando em um desgaste menor dos *hardwares* e uma vida útil maior.

A instalação dos outros serviços, citados anteriormente nos dois novos servidores, foi feita pensando no melhor desempenho dos *hardwares*, relação entre os serviços e principalmente na segurança da rede. Um dos servidores foi configurado somente com o serviço de *firewall* utilizando o *iptables* para proteger a rede da empresa de acessos indesejados. O outro servidor recebeu os serviços de DHCP e SAMBA. Ficou definido, dessa forma, pois os serviço de DHCP contribui para o funcionamento da rede, já o SAMBA está neste servidor por questão de segurança pois, se estivesse no mesmo servidor de *firewall* seus arquivos poderiam ficar acessíveis sem nenhum esforço caso algum ataque conseguisse entrar no servidor.

## 4.3 CRESCIMENTO DA REDE E POSSÍVEIS SERVIÇOS FUTUROS

A sede atual da empresa tem uma estrutura física com 8 anos, foi projetada para atender à necessidade da época, com uma pequena margem para crescimento em se tratando no número de colaboradores. Atualmente, existem 9 portas livres no *switch* que podem receber novos pontos de acessos, mas sem uso. Dessas portas, duas serão utilizadas pelo servidor de *firewall*e uma pelo outro servidor Linux com os serviços de redes e compartilhamento de arquivos.

Conforme informações coletadas em conversas informais com a diretoria da empresa, a previsão de crescimento da equipe interna é de somente mais 3 colaboradores, sendo que somente 2 (duas) das 3 necessitarão de um computador conectado na rede. Desta forma, sobrará apenas 4 portas livres no *switch* para receber novos dispositivos na rede, possibilitando que seja conectado ao menos mais um servidor *web* para o site da empresa, que hoje tem hospedagem terceirizada e um outro servidor de *e-mail* que também está terceirizado.

Levantou-se a hipótese de futuramente incluir, na estrutura, mais um servidor de *proxy/cache* para gerenciar melhor o controle de banda da Internet da empresa e diminuir o tráfego do link WAN (*WideArea Network*), e, utilizar também, para controle de acesso de sites indesejados. Neste momento foi descartada essa possibilidade pois a empresa não possui problemas quanto a largura e consumo de banda e também os acessos que são feitos pelos

usuários não estão necessitando desse controle. Esta opção de não criar nenhum bloqueio de acesso foi uma opção da diretoria da empresa.

## 4.4 INSTALAÇÃO DO LINUX

O sistema operacional utilizando em ambos os servidores que foram adicionados na estrutura da empresa foi o Debian 9, uma das distribuições Linux mais tradicionais e antigas existentes no mercado. O Debian é conhecido pela sua estabilidade e segurança das versões disponibilizadas para seus usuários, o que cumpre com a filosofia e ideologia de criação do mesmo. A seguir veremos um passo a passo de como baixar e instalar o Linux sem a interface gráfica contendo somente o sistema básico. Para adquirir a versão do Debian 9 foi necessário acessar o site através do link https://www.debian.org e clicar na aba Obtendo o Debian, conforme apresenta a Figura 6.


**Figura 6 – Obtendo o Debian**
Fonte: DEBIAN (2018).

Ao clicar na aba Obtendo o Débian, foi apresentado algumas opções de versões para serem baixadas, a versão escolhida foi uma pequena imagem de instalação de 64 bits conforme podemos observar na Figura 7. Foi escolhida esta versão porque ela possui somente o sistema básico do Linux contribuindo para o desempenho do servidor.

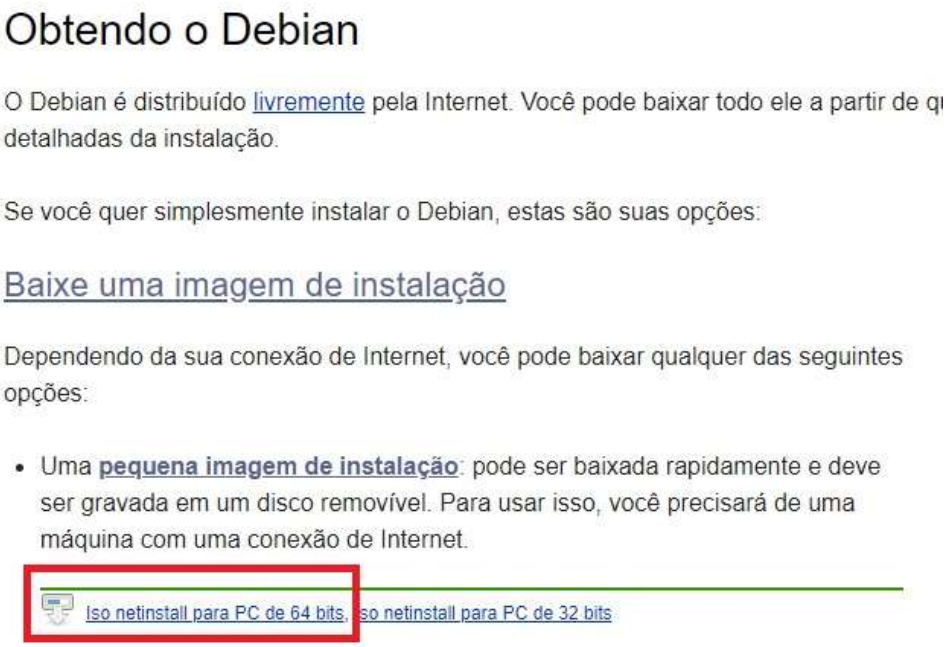



**Figura 7 – Baixando pequena imagem do Linux 64bits**
Fonte: DEBIAN (2018).

Após baixar a imagem foi realizada a instalação do Debian, a primeira janela que apareceu ao executar a imagem solicitava qual o tipo de instalação que era a desejada, foi utilizado o modo de instalação gráfico como demonstra a Figura 8.

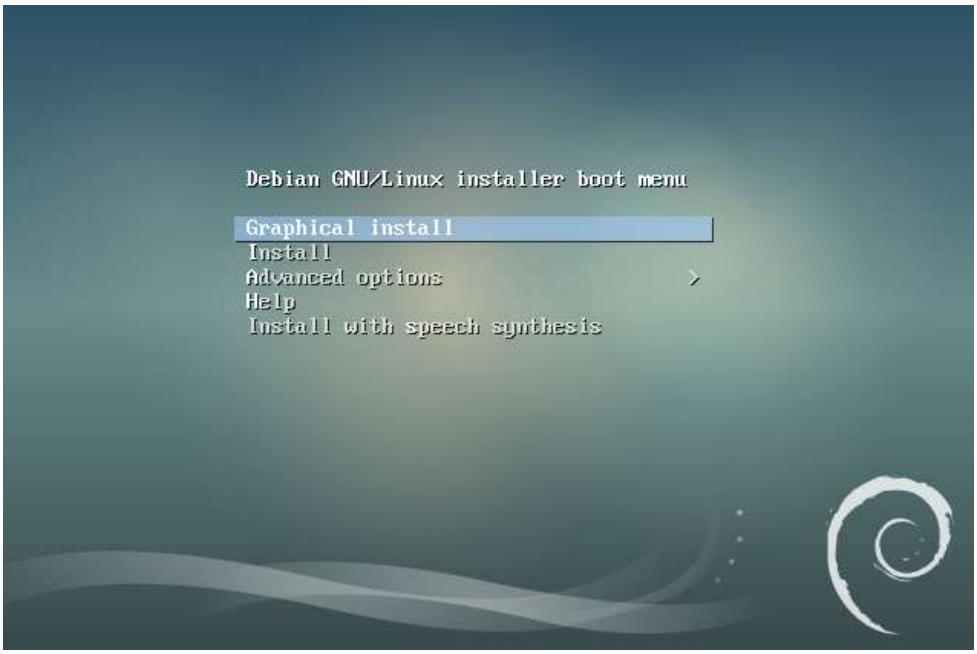



**Figura 8 – Modo de instalação do Debian**
Fonte: DEBIAN (2018).

Confirmado o modo de instalação foi solicitado a linguagem que era a desejada, foi escolhida português do Brasil que é a nossa linguagem (Figura 9).

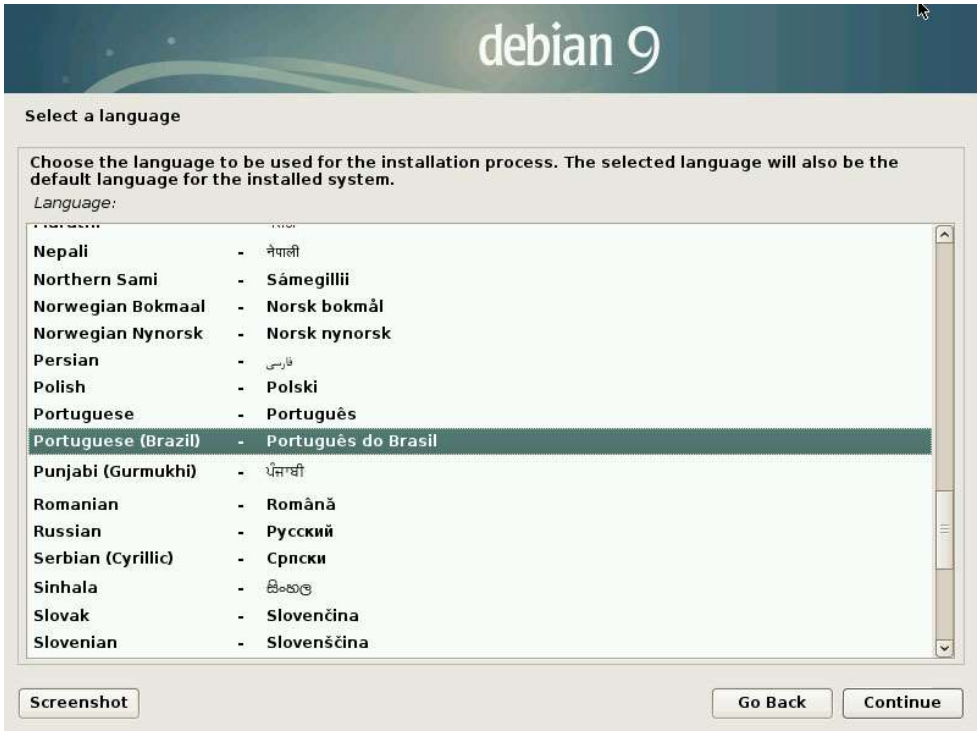



**Figura 9 – Escolha da linguagem**
Fonte: DEBIAN (2018).

Em seguida foi solicitado qual a localidade que se encontrava a máquina que estava sendo instalado o Debian (Figura 10).


**Figura 10 – Localidade**
Fonte: DEBIAN (2018).

A próxima etapa solicitada foi a configuração do idioma do teclado, logicamente foi escolhido o padrão brasileiro como podemos ver na Figura 11.

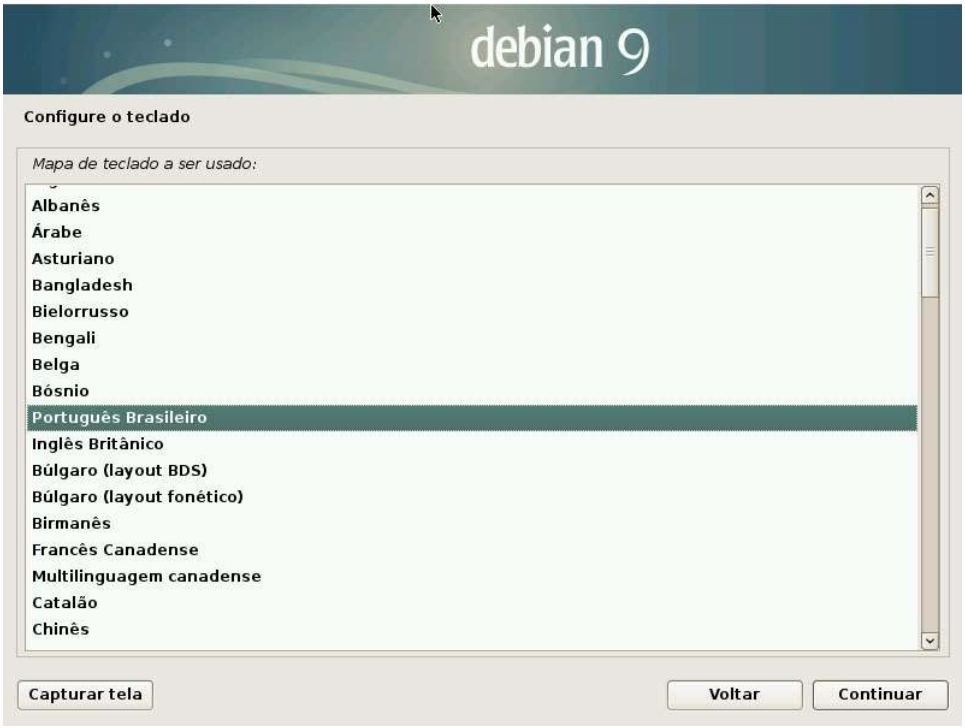



**Figura 11 – Idioma do teclado**
Fonte: DEBIAN (2018).

O passo seguinte foi a configuração das placas de rede existentes no servidor, como podemos observar na Figura 12 eram duas placas de redes ativas e o Debian solicitou saber qual seria a placa que seria a da entrada da internet, foi selecionada a enp0s3.


**Figura 12 – Escolha da placa de rede com acesso a Internet**
Fonte: DEBIAN (2018).

Placas de rede configuradas então foi solicitado que fosse atribuído um nome para a máquina, a Figura 13 apresenta o nome firewall porque foi feito o print do servidor de firewall, o outro servidor recebeu o nome de service.


**Figura 13 – Nome do servidor firewall**
Fonte: DEBIAN (2018).

Neste passo seguinte, o qual é muito importante, foi solicitado a configuração de uma senha para o root, usuário o qual é o administrador do Linux. A configuração desta senha deve ser feita utilizando um certo grau de complexidade utilizando letras, números e quem sabe até caracteres especiais para dificultar que qualquer pessoa possa descobrir a senha e realizar um login como root e causar algum problema (Figura 14).


**Figura 14 – Configuração da senha para o root**
Fonte: DEBIAN (2018).

Um procedimento padrão do Debian é a criação de um usuário o qual ele solicitou o nome completo e criou o mesmo (Figura 15).


**Figura 15 – Usuário padrão do Debian**
Fonte: DEBIAN (2018).

Nome completo de usuário informado, o próximo passo solicitado foi informar um nome de acesso para este usuário, como podemos ver na Figura 16 o nome dado foi firewall.


**Figura 16 – Nome de acesso para o usuário**
Fonte: DEBIAN (2018).

Logicamente o próximo passo solicitado foi a configuração de uma senha para o usuário recém informado (Figura 17).

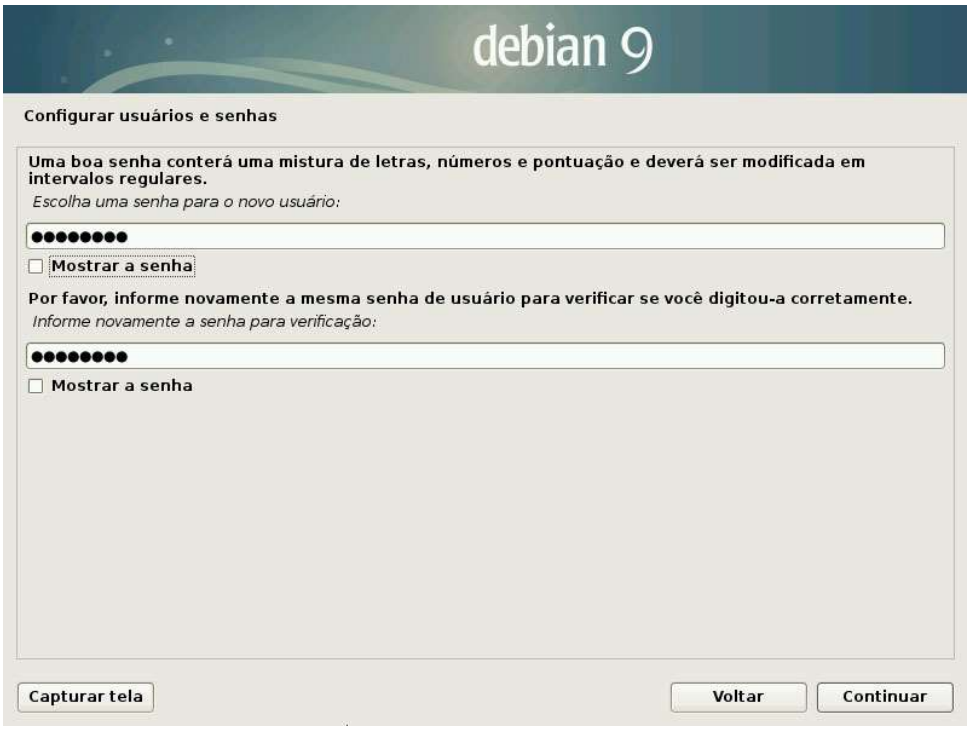



**Figura 17 – Senha para o usuário padrão**
Fonte: DEBIAN (2018).

Continuando com a instalação chegou em uma etapa onde foi solicitado o fuso horário que a máquina pertence, ao informar a cidade essa questão é configurada automaticamente (Figura 18).

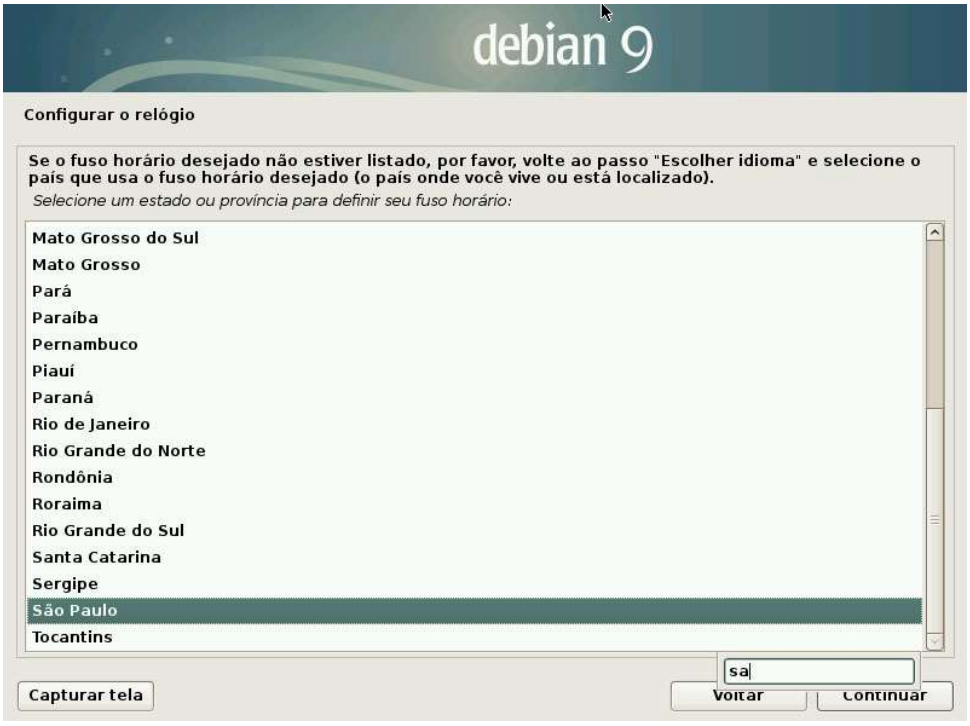



**Figura 18 – Configuração do fuso horário**
Fonte: DEBIAN (2018).

Outro assunto importante na instalação do Debian foi o particionamento dos discos, os servidores de modo geral vão armazenando informações competentes aos serviços que estão sendo fornecidos por ele. A limitação das partições é importante para contribuir com o desempenho e evitar possíveis problemas com indisponibilidade do servidor por falta de espaço em disco. O particionamento contribui também na recuperação de desastres e também na manutenção do servidor, sabendo dessas informações foi escolhido então a segunda opção, que possui uma opção de gerenciamento de volumes e permite a inclusão de novos HD´s no servidor e a configuração das partições quando necessário (Figura 19).

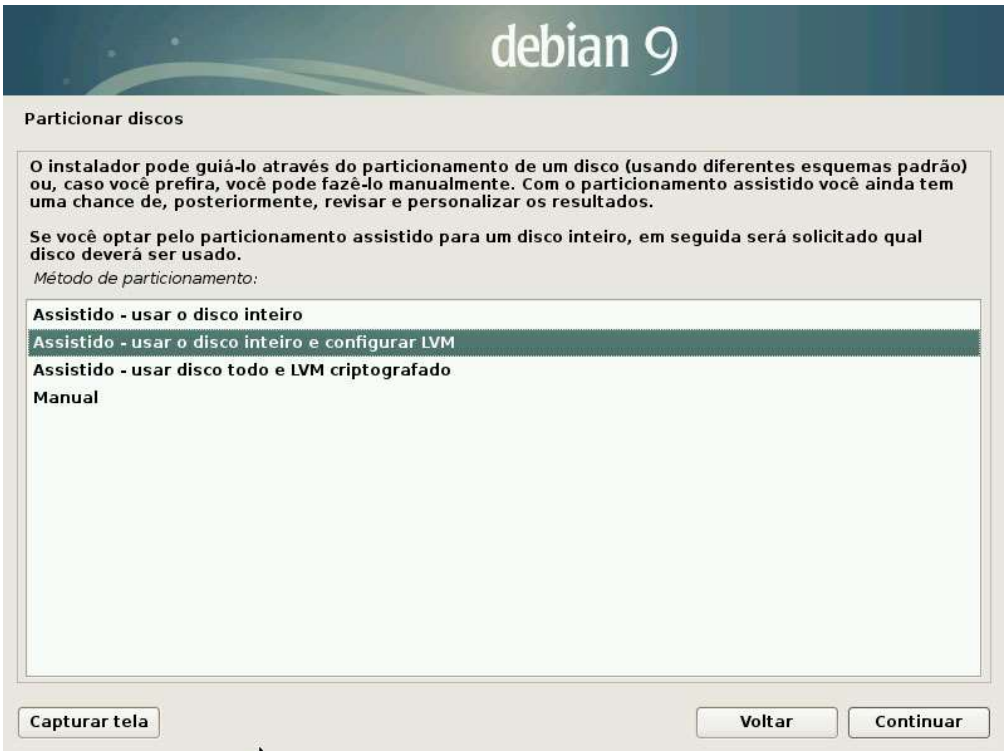



**Figura 19 – Configuração do particionamento**
Fonte: DEBIAN (2018).

Na sequência da configuração das partições e escolha do disco foi perguntado qual o tipo de particionamento que deveria ser feito no disco, conforme apresentado na Figura 20, o tipo escolhido foi o que separa a pasta home (pastas de usuários), var (partição com logs e alguns serviços do Linux) e tmp (arquivos temporários). Quando selecionada esta opção o Debian configurou automaticamente essas pastas.

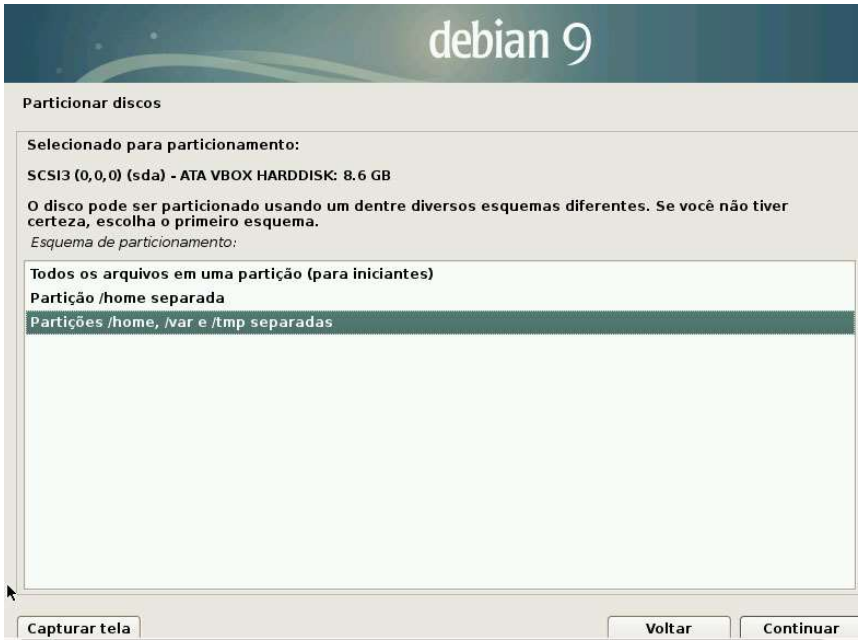



**Figura 20 – Tipo de particionamento**
Fonte: DEBIAN (2018).

Escolhido os tipos de configurações relacionadas a partição foi perguntado que desejava grava as mudanças escolhidas nos discos e configurar a ferramenta de LVM (*Logical Volume Manager)*, foi escolhida a opção sim (Figura 21).

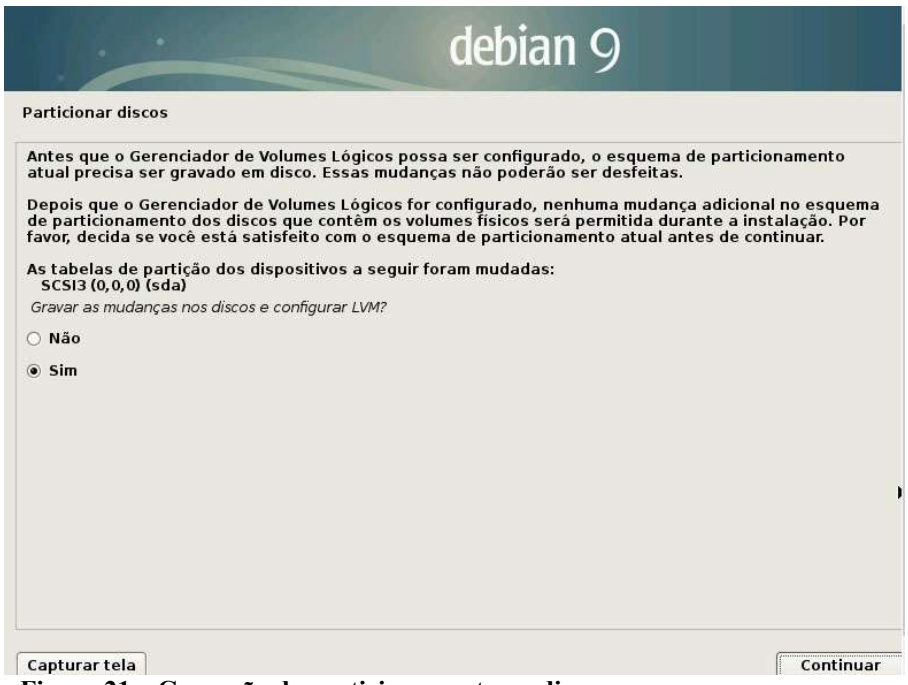



**Figura 21 – Gravação do particionamento no disco**
Fonte: DEBIAN (2018).

Finalizada a questão de particionamento dos discos o Debian solicitou que fosse configurado o gerenciados de pacotes, existem vários servidores espalhados pelo mundo que disponibilizam os pacotes para atualização do SO, como podemos ver na Figura 22 foi escolhido um servidor do Brasil.

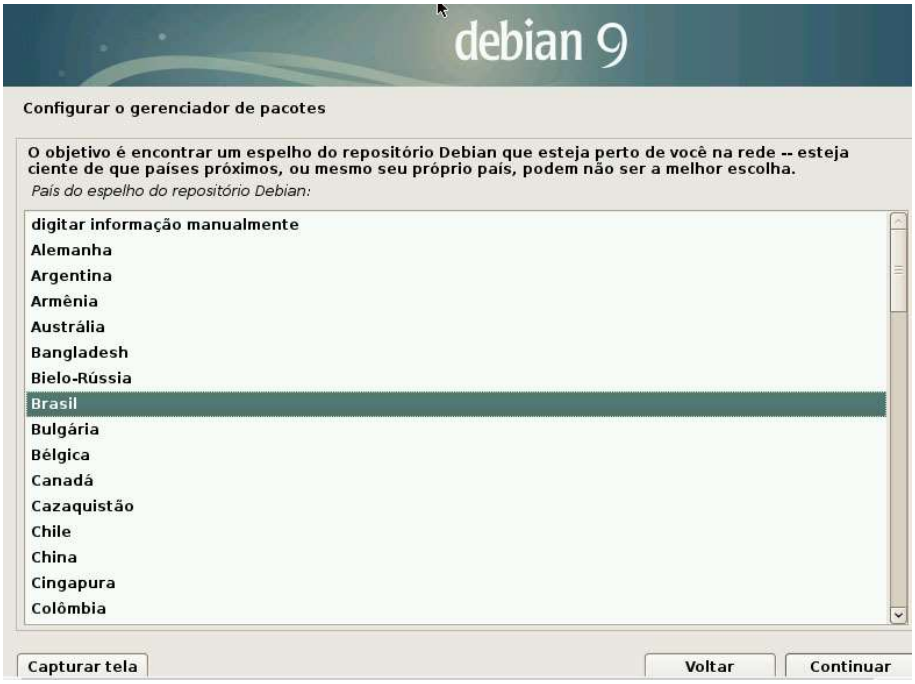



**Figura 22 – Configuração do pais/servidor**
Fonte:DEBIAN (2018).

Na Figura 23 podemos observar que foi solicitado também um repositório padrão para que seja utilizado para baixar os pacotes quando necessário.


**Figura 23 - Repositório padrão do Debian**
Fonte: DEBIAN (2018).

Chegando próximo da finalização da instalação foi solicitado se existia a necessidade de instalar interface gráfica e foram fornecida algumas opções de interface, foi dada a opção de instalar serviços web, impressão e SSH para acesso remoto. Foi instalado somente o SSH caso houvesse alguma necessidade de acesso remoto e os utilitários de sistema padrão (Figura 24).


**Figura 24 - Instalação do software**
Fonte: DEBIAN (2018).

Antes de finalizar a instalação foi solicitado se desejava instalar o GRUB (*GRandUnifieldBootloader)* que é um gerenciador de inicialização, conforme apresenta a Figura 25 podemos ver que foi marcada a opção sim. Em seguida foi escolhido o disco principal e a instalação foi finalizada.


**Figura 25 - Instalação do GRUB**
Fonte: DEBIAN (2018).

Antes de finalizar a instalação foi solicitado se desejava instalar o GRUB (*GRandUnifieldBootloader)* que é um gerenciador de inicialização, conforme apresenta a

Figura 25 podemos ver que foi marcada a opção sim. Em seguida foi escolhido o disco principal e a instalação foi finalizada.

## 4.5 INSTALAÇÃO DO SERVIDOR FIREWALL

Após a instalação do Linux o próximo passo foi instalar o serviço de *firewall* na máquina que será exclusiva para este serviço. Uma das vantagens de se ter um servidor *firewall* instalado no Linux é que suas funções são adicionadas na arquitetura do kernel, com isso todo tráfego que entra (*input*), atravessa (forward) ou sai (*output*) tem seu processamento realizado no núcleo do Linux. Este é um servidor de borda que separou a WAN da LAN evitando possíveis acessos indesejados em dispositivos da LAN.

Inicialmente foi configurado as duas placas de redes do servidor, a interface enp0s3 de entrada da internet ficou com atribuição de IP automático, e a interface enp0s8 teve atribuído um ip fixo. Essa configuração foi realizada através da alteração do arquivo interfaces utilizando o editor de textos VI (Visual), através do comando apresentado na Listagem 1.

```
root@firewall:~# vi /etc/network/interfaces
```

**Listagem 1 - Configurando as interfaces do servidor firewall**

Como podemos ver anteriormente a *Listagem 1* apresentou o comando para abrir o arquivo de configuração das interfaces, nele foi configurada a interface enp0s3 como DHCP e a interface enp0s8 com ip fixo (Figura 26).

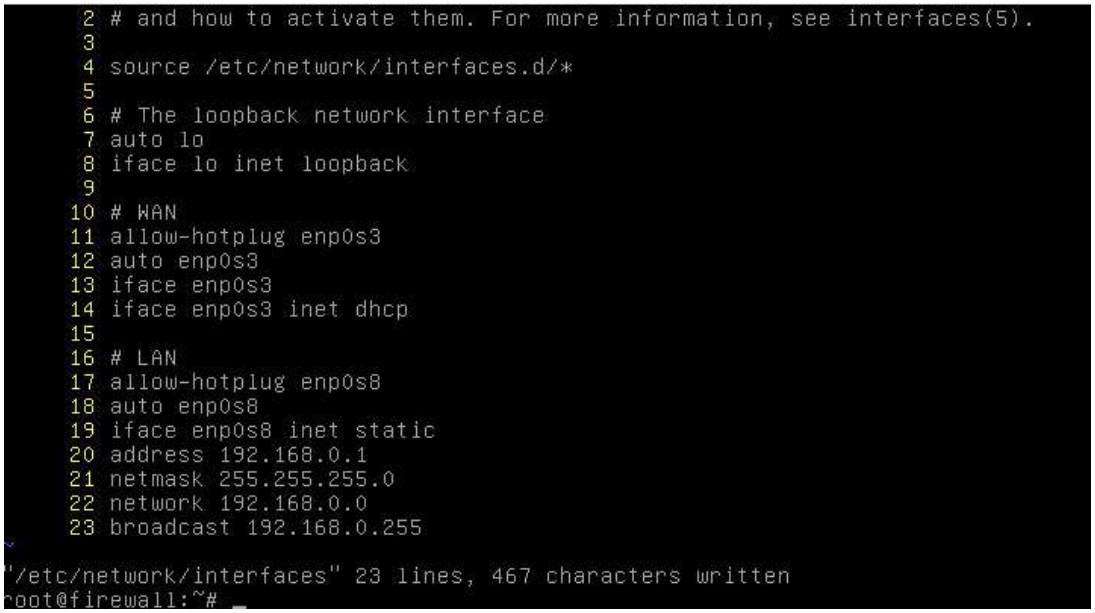



**Figura 26 – Configuração das placas de rede enp0s3 e enp0s8**
FONTE: AUTORIA PRÓPRIA (2018).

As configurações realizadas em ambas as placas de rede só serão válidas após reiniciar o serviço de rede, na Listagem 2 é apresentado o comando para realizar a operação.

```
root@firewall:~# systemctl restart networking
```

**Listagem 2 – Reiniciando serviço de rede**

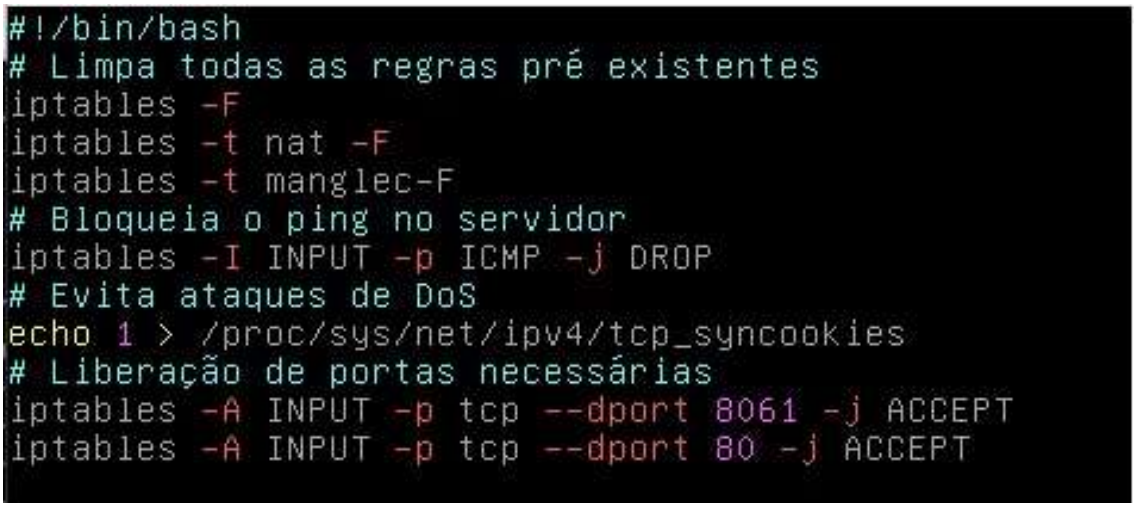
Especialistas em segurança de redes recomendam que por padrão a configuração do *firewall* dever bloquear tudo e libera somente o necessário, como ainda não existe uma política de acessos e segurança na empresa inicialmente não será feito nenhum bloqueio a pedido da diretoria. Para facilitar a configuração futura no momento em que ocorra o bloqueio total e seja liberado somente o necessário, foi realizada a inclusão de algumas regras que serão necessárias após o bloqueio.

Essas regras serão criadas em um script que inicializará junto com o SO, dessa forma toda vez que o servidor for reiniciado as regras não serão perdidas. O script de inicialização deve ser criado no diretório cd /usr/local/bin, diretório padrão do sistema. A Listagem 3 apresenta o comando para criar o arquivo de script no diretório citado.

```
root@firewall:/usr/local/bin# vi firewall.sh
```

**Listagem 3 – Reiniciando serviço de rede**

Arquivo de texto para criar o script foi configurado com poucas regras inicialmente, isso devido ao pedido da diretoria de não criar bloqueios de acesso em um primeiro momento, esse bloqueio ocorrerá futuramente com um planejamento melhor. A primeira linha do scritp é obrigatória, conhecida como shebang, ela que “apresenta” que o arquivo é um executável. As linhas de número 3,4,5 é para apagar regras pré-existentes ao reiniciar, na linha 7 é o comando que está bloqueando o ping no servidor, a linha de número 9 evita ataques de Dos como cita o comentário acima na linha 8, as linhas 11 e 12 estão liberando o acesso através das portas especificadas para atender à necessidade futura das conexões dos tablets (Figura 27).



```
#!/bin/bash
# Limpa todas as regras pré existentes
iptables -F
iptables -t nat -F
iptables -t manglec-F
# Bloqueia o ping no servidor
iptables -I INPUT -p ICMP -j DROP
# Evita ataques de DoS
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
# Liberação de portas necessárias
iptables -A INPUT -p tcp --dport 8061 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

**Figura 27 – Script de regras do firewall**
Fonte: AUTORIA PRÓPRIA (2018).

Com o script criado para iniciar as regras do firewall junto com o SO, foi necessário alterar a permissão para que este arquivo pudesse ser executado e as regras iniciassem junto com o sistema (Listagem 4).

```
root@firewall:/usr/local/bin# chmod +x firewall.sh
```

**Listagem 4 – Incluindo permissão de execução no script do firewall**

A criação do script só terá efeito para iniciar junto com o Linux após a criação do arquivo que corresponde ao script no systemd, este arquivo foi criado no diretório /etc/systemd/system. Estando no diretório correspondente a arquivos de scripts que inicializam junto com o Linux, foi criado então o arquivo que permitiu essa inicialização junto com o SO (Listagem 5).

```
root@firewall: /etc/systemd/system # vi firewall.service
```

**Listagem 5 – Criando o arquivo para inicialização das regras junto com o linux**

Dentro do arquivo criado, foram inclusas as linhas para que o sistema interprete e saiba que aquele script deve ser inicializado com o SO. Como podemos observar na Figura 28.


**Figura 28 - Script de inicialização do firewall junto com o SO**
Fonte: AUTORIA PRÓPRIA (2018).

Arquivo de configuração criado, dessa forma o script das regras do firewall serão iniciadas junto com o Linux. Para que o systemd reconheça este novo arquivo foi necessário reiniciá-lo (Listagem 6).

```
root@firewall: /etc/systemd/system # systemctl daemon-reload
```

**Listagem 6 – Atualizando o systemd**

Mesmo após todas essas configurações é necessário habilitar e ativar o serviço do firewall, como podemos ver na Listagem 7, o primeiro comando habilita o firewall para iniciar junto com o SO e o segundo comando ativa o serviço.

```
root@firewall: /etc/systemd/system # systemctl enable firewall
root@firewall: /etc/systemd/system # systemctl start firewall
```

**Listagem 7 – Atualizando o systemd**

Esses foram os passos realizados para configurar o servidor *firewall*, por se tratar de um servidor que pode impactar diretamente na rotina dos usuário o diretor da empresa resolveu iniciar sem bloqueio algum, realizar levantamento do que é necessário ser liberado para cada setor e após possuir um levantamento documentado realizar o bloqueio total liberando somente o que consta no documento com as exceções solicitadas para cada setor.

A parti do momento que o bloqueio total for realizado será liberado somente o necessário para o funcionamento da empresa, não será liberado nenhuma outra porta ou acesso, porque a empresa não tem necessidade de compartilhar arquivos via FTP (*File TransferProtocol*), conexões via SSH (*Secure Shell*) ou qualquer outro tipo de serviço remoto, o email da empresa está na nuvem e a hospedagem do site também, por isso não tem necessidade de outras liberações.

## 4.6 INSTALAÇÃO DO SERVIDOR DHCP E SAMBA

O segundo servidor foi instalado o Linux e posteriormente instalado os serviços de DHCP e SAMBA para melhorar o desempenho da rede e compartilhar arquivos entre os usuários. Serviços que melhorarão o desempenho da rede, o DHCP evitará que haja conflito de IP entre os dispositivos novos que sejam adicionadosna rede e o SAMBA possibilitará que máquinas Linux e Windows realizem troca de arquivos e compartilhamento de impressoras.

Para que um dispositivo se conecte em uma rede TCP/IP é necessário que ele possua um endereço IP que seja compatível com a rede que ele está se conectando, assim poderá usufruir e acessar tudo que a rede possui em modo compartilhado. Instalar um serviço de DHCP na rede permitiu reservar faixas de IP para novos usuários da rede, evitando conflitos com os já conectados, informação de *gateway*, entre outras informações complementares. O comando utilizado para instalar o serviço está apresentado conforme a Listagem 8.

```
root@service:~# apt-get installisc-dhcp-server
```

**Listagem 8 - Comando de instalação do serviço de DHCP**

Instalação do DHCP terminada,foi necessário configurar a entrega de Ip´s para os dispositivos que se conectarem na rede, o arquivo responsável por essa configuração se encontra no caminho /etc/dhcp/.Dentro do diretório citado anteriormente está o arquivo denominado *dhcpd.conf*. que possui as configurações referentes ao serviço de "empréstimo" de endereços para os dispositivos. Para que esse arquivo fosse alterado foi necessário utilizar o comando VI (visual) que é um editor de texto do Linux, permitindo então realizar as alterações necessárias no arquivo de texto. A Listagem 9 apresenta o comando utilizado para acessar este arquivo.

```
root@service:~# vi /etc/dhcp/dhcpd.conf
```

**Listagem 9 - Comando de acesso ao *dhcp.conf***

Após executar o comando o arquivo de texto que contém as informações do serviço de DHCP abre o arquivo para que sejam feitas as edições necessárias conforme a rede. Foi incluso no final do arquivo as informações correspondentes com a rede da empresa, DNS, máscara, e o intervalo de Ip´s que será destinado para atribuição quando um dispositivo conectar na rede (Listagem 10).

```
subnet 192.168.0.1 netmask 255.255.255.0 {
     # default gateway
option routers 192.168.0.1;
     # Mascara de rede
```

```
option subnet-mask 255.255.255.0;
     # Faixa de entrega
range dynamic-bootp 192.168.0.125 192.168.0.200;
}
```

**Listagem 10 - Configuração do*dhcp.conf***

O próximo passo após a realização da alteração do arquivo é reiniciar o serviço para que ele inicie com as novas configurações que foram incluídas no arquivo, a Listagem 11 apresenta o comando que realiza esta operação.

```
root@service:~# systemctl restart isc-dhcp-server
```

**Listagem 11 - Reiniciando o serviço DHCP**

Este servidor DHCP possui uma tabela com informações dos dispositivos conectados na rede para manter o controle dos endereços IP da rede. Nesta tabela é armazenado o tempo de empréstimo do IP de determinada máquina, qual o MAC (*Media Access Control*) da placa de rede que possui o IP emprestado. O trabalho deste servidor será retornar as mensagens de *broadcast* enviadas por dispositivos que solicitam informações para se configurar e acessar a rede, respostas que devem ser *unicast* somente para a máquina que solicitou e não para toda a rede evitando assim um aumento de tráfego na rede.

O último serviço configurado neste servidor, foi o SAMBA. Um conjunto de ferramentas que possibilitou o compartilhamento de impressoras e arquivos de sistemas diferentes como por exemplo o Linux e o Windows. A configuração do SAMBA foi para compartilhar uma impressora que está conectada na rede e também possibilitar que os usuários possam compartilhar pastas entre eles. Também foram criadas pastas particulares para armazenar arquivos “particulares”.

Foi criada uma pasta raiz pública onde todos os dispositivos da rede podem ver, acessar, alterar e armazenar arquivos, porém não conseguirão excluir esta pasta em momento algum. Uma nova pasta chamada diretoria foi criada para que somente a diretoria tivesse acesso a ela. Isso foi possível através da solicitação de uma senha ao tentar acessar os arquivos que a pasta possui. Uma pasta de acesso restrito para o setor de informática da empresa foi criada, uma pasta de acesso restrito para o setor financeiro e outra pasta de acesso restrito para o setor de contabilidade.

Primeiramente antes de instalar o SAMBA é necessário criar as pastas que serão compartilhadas na rede, como foi citado anteriormente será uma pasta pública e as demais para cada setor serão privadas. A criação dessas pastas foi feita através do comando apresentado na Listagem 12.

```
root@service:~# mkdir /publica
```

```
root@service:~# mkdir/diretoria
root@service:~# mkdir/informatica
root@service:~# mkdir/contabilidade
root@service:~# mkdir/financeiro
```

**Listagem 12 - Criação das pastas**

Pastas criadas então foi configurado a permissão para cada uma delas referente as ações que os usuários que acessarem essas pastas possam realizar dentro das mesmas. Na pasta pública foi aplicada a permissão total para todos os usuários (Listagem 13).

```
root@service:~# chmod 777 /publica
```

**Listagem 13 - Alterando permissão da pasta publica**

As demais pastas que não possuem compartilhamento público também devem sofrer alterações nas permissões das ações que podem ser feitas dentro delas, sendo que o proprietário e o grupo possuem permissão total e os demais usuários nenhuma permissão. (Listagem 14).

```
root@service:~# chmod770 /diretoria
root@service:~# chmod 770 /informatica
root@service:~# chmod 770 /contabilidade
root@service:~# chmod 770 /financeiro
```

**Listagem 14 - Alterando permissão das pastas privadas**

Para que as permissões feitas nas pastas com acesso restrito possuíssem efeito foi criado os usuários correspondente a cada pasta que terão permissão de acesso a elas, como esses usuários serão somente para ter acesso ao compartilhamento e não terão acesso ao servidor, não necessitará criar a pasta *home* para este usuário, não terá senha e terá o *login* desabilitado (Listagem 15).

```
root@service:~# adduser –no-create-home –disabled-password –disabled-login
diretoria
root@service:~# adduser –no-create-home –disabled-password –disabled-login
informatica
root@service:~# adduser –no-create-home –disabled-password –disabled-login
contabilidade
root@service:~# adduser –no-create-home –disabled-password –disabled-login
financeiro
```

**Listagem 15 - Criando usuários**

Usuários criados então foram criados os grupos para cada setor da empresa, isso permitirá que um usuário tenha acesso a outras pastas que estão liberadas para os grupos que ele pertence (Listagem 16). Para que ficasse mais fácil a distinção entre usuários e grupos os usuário foram criados com letras minúsculas e os grupos com letras maiúsculas.

```
root@service:~# groupadd DIRETORIA
root@service:~# groupadd INFORMATICA
root@service:~# groupadd CONTABILIDADE
```

```
root@service:~# groupadd FINANCEIRO
```
**Listagem 16 - Criando grupos**

Em seguida foi feito o vínculo entre o usuário e o grupo, o usuário diretoria que tem acesso a todas as pastas faz parte de todos os grupos, os demais usuários só fazem parte dos grupos dos seus setores (Listagem 17).

```
root@service:~# usermod –a –G DIRETORIA diretoria
root@service:~# usermod –a –G INFORMATICA diretoria
root@service:~# usermod –a –G CONTABILIDADE diretoria
root@service:~# usermod –a –G FINANCEIRO diretoria

root@service:~# usermod –a –G INFORMATICA informatica
root@service:~# usermod –a –G CONTABILIDADE contabilidade
root@service:~# usermod –a –G FINANCEIRO financeiro
```
**Listagem 17 - Vinculando usuário ao grupo**

Quando as pastas são criadas tanto o dono quanto o grupo padrão é o *root*, como as pastas são de acesso restrito ao grupo que corresponde a ela foi necessário trocar o grupo das pastas (Listagem 18).

```
root@service:~# chgrp DIRETORIA /diretoria/
root@service:~# chgrp INFORMATICA /informatica/
root@service:~# chgrp CONTABILIDADE /contabilidade/
root@service:~# chgrp FINANCEIRO /financeiro/
```
**Listagem 18 - Trocando o grupo da pasta**

Configurações de pastas, permissões, usuários e grupos realizados então foi realizada a instalação do SAMBA utilizando o comando apresentado pela Listagem 19.

```
root@service:~# apt-get install samba
```
**Listagem 19 - Instalação do SAMBA**

Com o SAMBA instalado foi necessário realizar algumas configurações para que o compartilhamento funcionasse corretamente. O arquivo de texto que possui as configurações referentes ao compartilhamento se encontram no caminho /etc/samba/smb.conf, para realizar as alterações será utilizado o editor de texto VI assim como foi utilizado para alterar o arquivo de configuração do DHCP. Na Listagem 20 é apresentado o comando para abrir o arquivo de texto para realizar as configurações.

```
root@service:~# vim /etc/samba/smb.conf
```
**Listagem 20 - Alteração arquivo smb.conf**

Comando executado o arquivo de texto smb.conf abriu, se a rede utilizasse algum domínio diferente do padrão do Windows necessitaria configurar esse domínio, como não é o caso iniciou-se a configuração informando qual a rede que teria acesso a este

compartilhamento. Como podemos observar na Listagem 21 já vem como padrão a rede de loop-back configurada, então foi acrescentado a rede que terá acesso ao compartilhamento.

```
interfaces = 127.0.0.0/8 enp0s3 192.168.1.0/24 enp0s8
```

**Listagem 21 - Inclusão da permissão de compartilhamento para a rede**

Para que a configuração da rede que tem acesso ao compartilhamento funcione é necessário configurar o comando que permite o acesso somente as redes informadas, como podemos ver na Listagem 22 o comando que se refere a esta configuração.

```
bind interfaces only = yes
```

**Listagem 22 - Permissão para somente a rede configurada ter acesso**

É importante também criar um bloqueio para algum usuário que não está cadastrado mas tente acessar o compartilhamento que não seja público, para que esse bloqueio ocorra é adicionado ao arquivo de configuração uma linha de comando, como podemos ver na Listagem 23.

```
map to guest = Bad User
```

**Listagem 23 - Bloqueio de usuário não cadastrado**

Realizada as configurações referente a rede que tem acesso ao compartilhamento e o bloqueio de usuários não cadastrados, foi incluso no final do arquivo seções referentes as pastas que serão compartilhadas. Para cada uma das pastas criadas foi adicionado as configurações competentes a elas, a pasta pública não possui restrições, já as pastas privadas possuem bloqueio para os usuários que não fazem parte do grupo que possui permissão para acessar Listagem 24.

```
[publica]
path = /publica/
writable = yes
guest ok = yes
guest only = yes
create mode = 0777
directory mode = 0777

[diretoria]
comment = Pasta privada
path = /diretoria/
writable = yes
create mode = 0770
directory mode = 0770
guest ok = no
valid users = @DIRETORIA

[informatica]
comment = Pasta privada
path = /informatica/
writable = yes
```

```
create mode = 0770
directory mode = 0770
guest ok = no
valid users = @INFORMATICA

[contabilidade]
comment = Pasta privada
path = /contabilidade/
writable = yes
create mode = 0770
directory mode = 0770
guest ok = no
valid users = @CONTABILIDADE

[financeiro]
comment = Pasta privada
path = /financeiro/
writable = yes
create mode = 0770
directory mode = 0770
guest ok = no
valid users = @FINANCEIRO
```

**Listagem 24 - Configuração de compartilhamento das pastas**

Com o SAMBA instalado e suas configurações de compartilhamento realizadas foi adicionado os usuários que foram criados no SAMBA, dessa vez os usuários criados possuem uma senha que será utilizada para acessar as pastas restritas (Listagem 25).

```
root@service:~# smbpasswd –a diretoria
root@service:~# smbpasswd –a informatica
root@service:~# smbpasswd –a contabilidade
root@service:~# smbpasswd –a financeiro
```

**Listagem 25 - Permissão para somente a rede configurada ter acesso**

Configuração de compartilhamento do samba realizada, para que ela funcionasse corretamente foi realizado o reinício do SAMBA para que ele iniciasse novamente com as configurações que foram inclusas (Listagem 26).

```
root@service:~# systemctl restart smbd
```

**Listagem 26 - Reiniciando o samba**

Outra configuração importante que foi realizada com relação ao SAMBA foi criar uma lixeira para receber os arquivos que fossem excluídos, dessa forma se por algum motivo fosse excluído um arquivo e fosse necessário recuperá-lo seria possível através da lixeira. Essa foi uma das melhorias realizadas na nova estrutura de rede da empresa, no servidor que antes estava instalado o samba não existia uma lixeira. Essa configuração é feita acessando o arquivo de configuração do SAMBA através do editor de texto VI, após ter acessado o arquivo de texto foi incluso as configurações de qual pasta será a lixeira, quais tipos de

arquivos que não devem ir para a lixeira, manter salvo o local de origem do arquivo e também ter versões do arquivo com o mesmo nome (Listagem 27).

```
root@service:~# vim /etc/samba/smb.conf
# Configurações da lixeira
recycle:keeptree = yes
recycle:versions = yes
recycle:repository = /lixeira/
recycle:exclude = *.tmp; *.bkp
```

**Listagem 27 – Configurando a lixeira**

Lixeira criada foi adicionada nas seções de compartilhamento criadas no SAMBA a permissão de lixeira para todas as pastas compartilhadas (Listagem 28).

```
vfs objects = recycle
```

**Listagem 28 – Adicionando a lixeira nos compartilhamentos**

Ainda no arquivo de configuração do SAMBA para que a lixeira funcione é necessário criar uma seção de compartilhamento para a Lixeira (Listagem 29).

```
[lixeira]
comment = Diretório da lixeira do SAMBA
path = /lixeira/
writable= yes
read only = no
guest ok = yes
browseable = yes
```

**Listagem 29 – Adicionando compartilhamento para a lixeira**

Com todas as configurações referentes a lixeira criadas no SAMBA, foi necessário criar a pasta lixeira para receber os arquivos excluídos (Listagem 30).

```
root@service:~# mkdir /lixeira
```

**Listagem 30 – Criando a pasta lixeira**

Assim como foi feito com as outras pastas é necessário aplicar permissão total para a pasta lixeira, permitindo que qualquer usuário possa acessar a pasta (Listagem 31).

```
root@service:~# chmod 777 /lixeira
```

**Listagem 31 – Permissão para a pasta lixeira**

A lixeira só ficou disponível após reiniciar o serviço do samba (Listagem 32).

```
root@service:~# systemctl restart smbd
```

**Listagem 32 - Reiniciando o samba**

Inicialmente essas foram as configurações realizadas nos dois novos servidores para contribuir com o tráfego da rede da empresa e aumentar o nível de segurança dos dados e da rede. Possíveis ajustes serão feitos conforme novas necessidades e situações forem surgindo,

cada caso será analisado e tratado de forma que atenda a necessidade da empresa e mantenha a qualidade de navegação e segurança.

# 5 CONCLUSÃO

A globalização leva as organizações a investir constantemente em tecnologia, o grau de competitividade imposto por ela não permite que uma empresa fique estagnada e não acompanhe a evolução tecnológica e dos mercados. Qualquer empresa atualmente pode estar presente em qualquer lugar do mundo, e isso é possível através de investimentos no desenvolvimento de produtos de qualidade, relacionamento com os clientes, inovação em prestação de serviços, velocidade e eficiência na produção e comunicação com os clientes. Para que uma empresa possa usufruir de todas as ferramentas e oportunidades que as tecnologias oferecem, tanto para produção, comunicação, exposição de produtos, vendas entre outras comodidades é fundamental ter, mesmo que pequena, uma infraestrutura de tecnologia da informação.

Para estar conectado com as oportunidades que surgem, a todo momento, no mundo dos negócios, é necessário possuir uma rede de computadores na estrutura da empresa, conectada na Internet, para que a empresa usufrua de tudo que lhe convém para seu negócio. O bom funcionamento de uma rede cooperativa, depende de como ela foi estruturada e como os dispositivos e serviços que compõe este cenário, contribuem, de forma positiva e eficiente, para os negócios da empresa. A configuração da rede com os equipamentos e serviços básicos e específicos para que a rede funcione sem falhas ou interrupções, é tão importante quanto possuir uma rede de computadores na empresa. De nada adianta ter uma rede se ela não funciona corretamente.

Basicamente para que haja um bom funcionamento de uma rede cooperativa existe a necessidade de um mínimo de dispositivos, com os serviços básicos instalados para que não ocorram falhas nem interrupções nas atividades. Como pode ser observado no trabalho a rede da empresa antes da implementação dos novos dispositivos e serviços não possuía um serviço básico de segurança e otimização na navegação e, todas as operações administrativas da estrutura de rede e de operações da empresa dependiam exclusivamente de uma única máquina. Se ela falhasse a empresa parava. Identificou-se que seria necessário a instalação de um serviço para tornar a rede segura, outro serviço para otimizar a navegação da rede e, com isso, dois novos dispositivos foram adquiridos para suprir as necessidades básicas da empresa.

Como toda empresa, sempre são aspiradas expectativas de crescimento em vários âmbitos, este fator possui uma grande relevância para a estruturação e configuração de uma rede de computadores. Este assunto foi abordado pelo trabalho para permitir que a empresa pudesse crescer por um período sem se preocupar com limitaçõesfísicas e lógicas, levando-se

em consideração, a pretensão e intenção da diretoria em agregar à estrutura da empresa, novos serviços, funcionários e equipamentos.

Tão importante quando a identificação, a inclusão de novos dispositivos na rede e o planejamento de crescimento, é a instalação e configuração dos serviços básicos para que a rede esteja segura e funcionando da melhor forma possível. Foram apresentadas no trabalho, as configurações realizadas para tornar a rede segura e com agilidade na navegação, demonstrando onde cada serviço deveria ser instalado e a localização dos novos dispositivos na rede, formando assim uma nova estrutura, segura, eficiente e confiável.

Com base nas informações apresentadas e na necessidade tecnológica existente para todas as empresas, ficou claro que uma rede cooperativa, por mais pequena e simples que ela seja, é de fundamental importância possuir o mínimo de dispositivos para que não ocorra interrupção nas atividades do dia a dia, atrelado aos serviços básicos que oferecer segurança e agilidade na navegação da rede. Foram apresentadas ações básicas e fundamentais para que uma empresa possua uma rede confiável que permita encarar os desafios impostos pelo mercado e as mudanças repentinas no mundo dos negócios.

## REFERÊNCIAS


BRITO, S. H. B. **“Serviços de Redes em Servidores Linux”.**Novatec Editora Ltda. São Paulo, 2017.

GERALDI, L, M, A. **“Linux Configurações de Serviços de Rede”.** 1ª ed. – Taquaritinga: AgBook. 2013.

GIL, A. C. **“Métodos e Técnicas de Pesquisa Social”.** 6ª ed. – São Paulo: Atlas. 2008.

HERTZOG, R, **O Manual do Administrador Debina: Debian Jessie, da Descoberta à Maestria**, 2015. Disponível em: <https://debian-handbook.info/browse/pt-BR/stable/index.html>. Acesso em: 28 ago. 2018.

HILL, M, B.; BACON, J. **“O Livro Oficial Ubuntu”.** 2ª ed. – Porto Alegre: Bookman. 2008.

LUNARDI, Guilherme L.; BECKER, João L.; MAÇADA, Antonio C. G. Impacto da Adoção de Mecanismos de Governança de Tecnologia de Informação (TI) no desempenho da Gestão da TI: uma análise baseada na percepção dos executivos. **Reviste de Ciências da Administração**, set/dez, 2010, p. 11-39.

MORIMOTO, C. E. **“Redes e Servidores Linux: guia prática”.** 2ª ed. – Porto Alegre: Sul Editores. 2006.

MOTA FILHO, J.E. **“Descobrindo o Linux: Entenda o Sistema Operacional GNU/Linux”.** 3ª ed. – São Paulo: Novatec Editora. 2012.

NAKAMURA, T, E. GEUS, L, P. **“Segurança de Redes: Em Ambientes Cooperativos”.** 1ª ed. – São Paulo: Novatec Editora. 2007.

NEGUS, C. BRESNAHAN, C. **“Linux: A Bíblia”.** 8ª ed. – Rio de Janeiro: Alta Books. 2014.

PINTO, N. BATISTA, J. **“Sistemas Operacionais”.** 1ª ed. – Cuiabá: IFRO. 2014.

POPOVICI, **Falandosobre hardware**, 2015. Disponível em: < https://books.google.com.br/books?id=4ilECgAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 15 set. 2018.

RED HAT. **“História do Red Hat”** Disponível em: < http://redhat.slides.com/brand-team/redhat-book/fullscreen?token=owT11wUz#/>. Acesso em: 25 out. 2018.

SECURELIST. **“Estatísticas”** Disponível em: < https://securelist.lat/estadisticas/>. Acesso em: 08 out. 2018.

TEIXEIRA, J. **“Linux Sem Segredos”.** 1ª ed. – São Paulo: Digerati Books. 2008.

TERPSTRA, J. et al. **“Segurança Para Linux”.** 1ª ed. – Rio de Janeiro: Elsevier. 2005.

UBUNTU. **“História do Ubuntu”** Disponível em: <https://www.ubuntu.com/about>. Acesso em: 20 out. 2018.