Edilberto Rodrigues da Cruz

Lidio Felipe de Jesus Gomes

ESTUDO DA VIABILIDADE DE IMPLANTAÇÃO E GERENCIAMENTO DE SERVIDORES LINUX COM ÊNFASE EM VPN E VIRTUALIZAÇÃO

FACULDADES UNIFICADAS DE TEÓFILO OTONI

TEÓFILO OTONI – MG

2017

Edilberto Rodrigues da Cruz

Lidio Felipe de Jesus Gomes

ESTUDO DA VIABILIDADE DE IMPLANTAÇÃO E GERENCIAMENTO DE SERVIDORES LINUX COM ÊNFASE EM VPN E VIRTUALIZAÇÃO

Monografia apresentada ao Curso de Sistemas de Informação das Faculdades Unificadas de Teófilo Otoni, como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação.

Área de concentração: Redes de Computadores

Orientador: Professor Wilbert Viana Barbosa

FACULDADES UNIFICADAS DE TEÓFILO OTONI

TEÓFILO OTONI – MG

2017

rede de ensino
DOCTUM

FACULDADES UNIFICADAS DE TEÓFILO OTONI
NÚCLEO DE TCC / SISTEMAS DE INFORMAÇÃO
Autorizado pela Portaria 4.012 de 06/123/2004 – MEC

FOLHA DE APROVAÇÃO

A monografia intitulada: *Estudo da viabilidade de implantação e gerenciamento de Servidores Linux com ênfase em VPN e virtualização,*

elaborada pelos alunos Edilberto Rodrigues da Cruz
Lídio Felipe de Jesus Gomes,

foi aprovada por todos os membros da Banca Examinadora e aceita pelo curso de Sistemas de Informação das Faculdades Unificadas de Teófilo Otoni, como requisito parcial da obtenção do título de

BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Teófilo Otoni, 21 de novembro de 2017

Professor Orientador: Wilbert Viana Barbosa

Professor Examinador: Luiz Fernando Alves Souza

Professor Examinador: Salim Ziad Pereira Aouar

LISTA DE ABREVIATURAS E SIGLAS

CIFS - Common Internet File System (sistema de arquivos da internet comum)
DNS - Domain Name System (sistema de nomes e domínios)
FTP - File Transfer Protocol (protocolo de transferência de arquivos)
IP - Internet Protocol (protocolo de internet)
KVM - Kernel-based Virtual Machine (máquina virtual baseada em núcleo)
LAN - Local Area Networks (rede de área local)
OSI - Open System Interconnection (sistema aberto de interconexão)
PMK - Pairwise Master Key (Chave Mestra Dupla)
PTK - Pairwise Transient Key (Chave Transiente de Dupla)
RSAT - Remote Server Administration Tools Windows (administrando servidores remotamente)
SMB - Server Message Block (bloco de mensagem de servidor)
SMTP - Simple Mail Transfer Protocol (protocolo de transferência de correio simples)
TCP - Transmission Control Protocol (protocolo de controle de transmissão)
UDP - User Datagram Protocol (protocolo de datagramas de utilizador)
VM - Virtual Machines
VPN - Virtual Private Network (rede particular virtual)
WAN - Wide Area Network (rede de longa distância)
WEP - Wired Equivalent Privacy (privacidade equivalente à de redes com fios)
WPA - Wi-Fi Protected Access (acesso sem fio protegido)

LISTA DE GRÁFICOS

RESUMO

A presente monografia concentra-se na área de Redes de computadores e visa enfatizar como uma estrutura computacional de uma empresa pode ser melhorada com a utilização de ferramentas *Open Source* tendo como objetivo ressaltar a importância da aplicação da tecnologia de informação em empresas de pequeno e médio porte. Esta pesquisa tem um foco direcionado preponderantemente à criação de ambientes virtualizados em KVM (Qemu) e comunicação por VPN. A *Internet* tem evoluído de maneira gradativa e a enorme quantidade de informações que trafega nas redes de comunicações diariamente exige cada vez mais uma estrutura que suporte altas taxas de transferência de dados. Isso faz com que pequenos e médios empresários comecem a notar os benefícios que a tecnologia de informação pode trazer para o seu negócio. Tais benefícios operam de forma que possibilitam um melhor aproveitamento do *hardware* com o uso de multiplataformas na mesma estrutura física, redução de custos em aquisição de equipamentos de informática, suprir necessidades no envio e recebimento de informações entre matriz e filial utilizando ferramentas gerenciáveis e de baixo custo, melhorias na qualidade dos serviços prestados pela empresa e possibilitar que a estrutura de servidores da empresa seja capaz de acompanhar seu crescimento.

Palavras Chave: KVM, Multiplataformas, *Open Source*, Virtualização, VPN.

SUMÁRIO

INTRODUÇÃO

A presente monografia visa utilizar *softwares* livres para aplicar melhorias a estrutura tecnológica de empresas de pequeno e médio porte, visando maior produtividade e qualidade nos serviços prestados. Para a realização dos procedimentos de viabilidade foi testado em uma empresa de tratamento de água e esgoto da cidade de Itambacuri. Através da estrutura da empresa pode-se fazer o levantamento das hipóteses e requisitos necessários.

A empresa de saneamento básico possui uma matriz que se localiza no centro da cidade de Itambacuri onde funciona o escritório, uma extensão que funciona a alguns quilômetros de distância da matriz que não possui ligação entre as redes de computadores do escritório. Na filial funciona uma estação de tratamento de água onde são gerados relatórios. Por não possuir ligação entre as redes da matriz e filial o atraso no envio de informações prejudica significativamente a produtividade da empresa devido a filial se localizar em uma área de difícil acesso.

Neste trabalho serão exploradas ferramentas que podem ser viáveis para solucionar os problemas enfrentados pela empresa e que poderiam ser aplicadas em empresas de qualquer segmento. Ferramentas de virtualização como o KVM e Servidores VPN, DHCP, DNS, arquivos, Controlador de domínio e procedimentos que irão elevar os níveis de segurança da empresa serão abordados e explicados posteriormente.

A grande quantidade de informações que trafega nas redes de comunicações diariamente exige cada vez mais uma estrutura que suporte altas taxas de transferência de dados, isso faz com que pequenos e médios empresários comecem a notar os benefícios que a tecnologia de informação pode trazer para o seu negócio.

Com a evolução da tecnologia, diferentes desafios são enfrentados pelos empreendedores, “Como manter meu negócio atualizado e competitivo? ”. Para suprir

as necessidades que surgem com a evolução da tecnologia de informação, ferramentas e recursos de comunicação são criados praticamente na mesma proporção em que há evolução da tecnologia de informação, com características diferentes para demandas diferentes.

Buscam-se objetivos específicos como: (1) identificar a influência que o sistema de informação possui na qualidade do atendimento da empresa; (2) implantar ferramentas de software que influenciam de forma positiva na velocidade de transmissão de dados, a fim de aumentar a produtividade da empresa; (3) corrigir problemas relacionados a segurança de informação.

Destaca-se a proposta geral do trabalho solucionar problemas relacionados a segurança de informação e produtividade, visando melhor atendimento ao cliente e condições de trabalho favoráveis aos colaboradores.

Este trabalho foi desenvolvido em capítulos de acordo com o sumário. O capítulo 1 explica sobre redes de computadores e a relação cliente/servidor e os seus protocolos. O capítulo 2 aborda as funcionalidades do Samba4, controlador de Domínio *Open Source*, comparação com outros serviços similares e integração com o AD da *Microsoft*. O capítulo 3 mostra as conexões VPN entre Matriz e filial de maneira segura com o *OpenVPN*. O capítulo 4 aborda virtualização explicando como funciona e suas vantagens na utilização. O capítulo 5, *Software* Livre e as licenças de *Software* e seus termos. O capítulo 6 trata da Segurança de informação e o porquê de sua vital importância. O capítulo 7 será explica sobre as ferramentas utilizadas.

1 EMPRESA DE SANEAMENTO BÁSICO

Os dados utilizados para o desenvolvimento da pesquisa foram extraídos de uma empresa de saneamento básico do município de Itambacuri, onde a mesma apresentou grande necessidade de melhorias em sua estrutura de redes de computadores e automação comercial. O atendimento ao público depende de *softwares* de gestão que dependem de servidores para o devido funcionamento, a desorganização estrutural da parte de tecnologia da empresa tem acarretado lentidão no atendimento aos clientes, como na resolução de tarefas relativamente simples que dependem do processamento de dados.

As lentidões no processamento de dados podem ser causadas por diversos fatores entre eles, a comunicação ineficiente entre os setores da organização, uso desregrado da *Internet* que podem causar oscilações na transferência de dados e falta de um servidor que suporte cargas diárias de trabalho.

A estação de tratamento de água se localiza a alguns quilômetros da matriz e o envio de relatórios, requisições de materiais e processos de produção que necessitam de computadores são extremamente prejudicados por não possuir comunicação entre as redes da empresa.

O grande volume de dados gerados diariamente pela a autarquia, exige uma estrutura flexível e robusta para a implantação de novos recursos. Um recurso indispensável, se tratando de banco de dados empresarial, seria o *backup* diário. Os *backups* são cópias de segurança de todo o trabalho realizado em um intervalo de tempo. As cópias de segurança devem ser mantidas em locais seguros, elas servirão como plano de contingência caso haja perda da base de dados principal. Por não possuir equipamentos de armazenamento com capacidade suficiente para a

realização de *backups*, a empresa não faz uso deste recurso deixando assim todo o seu arsenal de dados em um só local, correndo o risco de perder todos os registros.

Tendo em vista os déficits presentes na empresa no ramo do saneamento básico em Itambacuri, foi sugerido a implantação de servidores Linux para melhorar o tráfego de dados e segurança na rede, promovendo a redução de custos de aquisição/manutenção e melhorando a prestação de serviço aos clientes da empresa. As ferramentas foram configuradas, testadas em ambientes virtuais e apresentadas aos tomadores de decisões da empresa. Tendo em vista que o projeto apresentado resolveria 90% dos problemas estruturais da rede atual da empresa, ficou decido que a presente pesquisa é uma solução viável para a empresa e será aplicada a partir de janeiro de 2018.

2 REDES DE COMPUTADORES

Segundo Filho (2012, p.770), em um sistema de redes pode-se possuir servidores e clientes onde o servidor seria uma máquina que oferece um ou mais serviços dentro da rede e o cliente seria uma máquina da rede que utiliza os serviços oferecidos pelos servidores. Pode-se classificar uma rede de computadores de acordo com a sua arquitetura e extensão geográfica. Quando há comunicação entre computadores interligados por cabos ou via rádio, pode-se classificar como uma LAN (*Local Area Networks*). Já a interligação de várias redes podendo ser próximas ou em continentes diferentes é denominada como WAN (*Wide Area Network*). A interconexão de WANs dá origem a rede mundial de computadores, conhecida popularmente como Internet.

Empresas de diversos segmentos podem usufruir dos recursos oferecidos pela rede mundial de computadores, para o envio e recebimento de informações, a *Internet* passa constantemente por processos de evolução, aperfeiçoando os modelos de transmissão de dados. Através da *Internet* deu-se origem as redes sociais que vêm se destacando na atualidade. Foi um grande passo para o mundo da tecnologia e para a sociedade colaboraram para a evolução de vários modelos de negócios como exemplo o *Marketing* digital, *e-commerce* e diversos outros.

A comunicação na *Internet* é feita através da arquitetura cliente/servidor, este método refere-se à distribuição de dados entre plataformas distintas, onde dois ou mais computadores se comunicam independente do seu sistema operacional. Neste modelo um computador é responsável por centralizar as informações e disponibilizá-las aos demais usuários da rede. Abaixo pode-se analisar algumas características presentes na arquitetura cliente e no servidor:

Cliente

- Cliente, também denominado de “*front-end*” e “*WorkStation*”, é um processo que interage com o usuário através de uma interface gráfica ou não, permitindo consultas ou comandos para recuperação de dados e análise e representando o meio pela qual os resultados são apresentados;
- É o processo ativo na relação Cliente/Servidor;
- Inicia e termina as conversações com os Servidores, solicitando serviços distribuídos;
- Não se comunica com outros Clientes;
- Torna a rede transparente ao usuário.

Servidor

- Também denominado Servidor ou “*back-end*”, fornece um determinado serviço que fica disponível para todo Cliente que o necessita. A natureza e escopo do serviço são definidos pelo objetivo da aplicação Cliente/Servidor;
- É o processo reativo na relação Cliente/Servidor;
- Possui uma execução contínua;
- Recebe e responde às solicitações dos Clientes;
- Não se comunica com outros Servidores enquanto estiver fazendo o papel de Servidor;
- Presta serviços distribuídos;
- Atende a diversos Clientes simultaneamente.

2.1 VLAN

As redes locais crescem gradativamente e cada vez mais o nível de complexidade tende a aumentar, equipadas por diversos roteadores e *switchs*, torna-se a gerência ainda mais complexa, sendo necessário trabalhar diversas tecnologias e procedimentos para trazer velocidade e estabilidade às redes de computadores. Uma ferramenta que poderia aumentar o desempenho e segurança da rede são as VLANS, redes virtuais que trataria o envio de pacotes entre as redes de segmentação

IP diferentes. As VLANs permitiriam a segmentação das redes físicas, sendo que a comunicação entre máquinas de VLANs diferentes teriam que passar por um roteador ou outro equipamento capaz de realizar encaminhamento, que será responsável por encaminhar o tráfego entre redes (VLANs) distintas.

2.2 Serviços e Protocolos

De acordo com Rios (2012, p.15), “os protocolos são desenvolvidos por algoritmos, instruções bem definidas para executar uma tarefa. Os protocolos são utilizados em duas ou mais máquinas em rede, para se comunicarem. ” Há inúmeros protocolos no mundo inteiro os quais oferecem diversos serviços de comunicação entre computadores.

Os serviços são processos trabalhando em conjunto em segundo plano para oferecer aos usuários ferramentas que darão funcionalidades às redes internas e/ou externas. Se tratando de redes de computadores há serviços como: *Firewall,* DNS (*Domain Name System*)*,* entre outros*.* Cada um deles tem a tarefa de estabelecer a comunicação eficiente entre dois ou mais computadores.

Com o avanço da *Internet,* as possibilidades de compartilhamentos nas redes de computadores crescem, tornando possível e prático a troca de informações entre computadores conectados pelo mundo.

Para que os pacotes de dados possam trafegar de uma origem até um destino, através de uma rede, seria importante que todos os dispositivos da rede usassem a mesma linguagem ou protocolo. Um conjunto de regras que tornam mais eficiente a comunicação em uma rede poderia ser denominada como protocolo. A camada de aplicação provê protocolos para garantir a comunicação de aplicativos de acordo com sua finalidade, bate-papo, videoconferência, *e-mail*, entre outros. Exemplo de alguns protocolos da camada de aplicação:

- HTTP: *Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto, trata de pedidos e respostas entre o cliente e o servidor na internet;
- SMTP: Simple Mail Transfer Protocol ou Protocolo de Transferência de e-mail. Protocolo responsável pelo envio do e-mail;
- IMAP: *Internet Message Access Protocol* ou Protocolo de acesso a mensagem da internet. Recebe e-mail;

- Telnet: Permite a comunicação remota entre computadores conectados em rede;
- SSH: *Secure Shell* ou Terminal Seguro Permite a comunicação remota entre computadores conectados em rede utilizando criptografia;
- DHCP: *Dynamic Host Configuration Protocol* ou Protocolo de configuração dinâmica de estação. Concede endereços IP's e outros parâmetros dinamicamente para estações de trabalho;
- DNS: *Domain Name System* ou Sistema de Nome de Domínio, é um sistema de gerenciamento de nomes hierárquico e distribuído; ele permite acessar outro computador na rede sem ter conhecimento do endereço IP.

Segundo Tanenbaum (2003, p.44), serviços e protocolos têm seus conceitos diferentes apesar serem confundidos com muita frequência. O serviço determina operações nas quais a camada está preparada para executar em nome dos usuários e que não informam nada sobre como são implementadas. Um serviço relaciona-se com a interface entre duas camadas: (1) a camada inferior e (2) a camada superior que é o usuário do serviço.

2.3 Modelos de referência

2.3.1 Protocolo TCP/IP

O TCP/IP (*Transmission Control Protocol*/Internet Protocol) é um protocolo de controle de transmissão de dados, responsável por identificar cada equipamento conectado à rede atribuindo um endereço numérico, sendo que, cada equipamento deve receber um endereço diferente. Em uma rede com muitos *hosts* pode-se dividir em várias sub-redes, cada uma em classes *IP* diferentes, podendo assim, melhorar o gerenciamento da rede como um todo.

O modelo *TCP/IP* foi subdivido em 4(quatro) camadas: (1) Camada inter-redes, (2) Camada de transporte, (3) Camada de aplicação e (4) Camada *host*/rede;

Tanenbaum (2003, p.48-49) define cada camada do modelo TCP/IP:

- Camada inter-redes: “Integra toda a arquitetura. Sua tarefa é permitir que os hosts injetem pacotes em qualquer rede e garantir que eles trafeguem independentemente até o destino. ” Esta determina um formato de pacote oficial e um protocolo IP o qual entrega pacotes IP onde são necessários. Devido a estas funções, pode-se dizer que a camada de rede é muito parecida com a camada OSI.
- Camada de transporte: “A camada localizada acima da camada inter-redes é chamada camada de transporte. A finalidade dessa camada é permitir que as entidades pares dos hosts de origem e de destino mantenham uma conversação. ” Nesta camada, são definidos dois protocolos: (1) TCP e (2) um protocolo orientado à conexão confiável, no qual possibilita a entrega sem erros de um fluxo de *bytes* de uma máquina para qualquer outro computador da inter-rede.
- Camada de aplicação: “Acima da camada de transporte, encontramos a camada de aplicação. Ela contém todos os protocolos de nível mais alto. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). ”
- Camada host/rede: “Abaixo da camada inter-redes, encontra-se um grande vácuo. O modelo de referência TCP/IP não especifica muito bem o que acontece ali, exceto o fato de que o host tem de se conectar à rede utilizando algum protocolo para que seja possível enviar pacotes IP. Esse protocolo não é definido e varia de host para host e de rede para rede. ”

2.4 Modelo de Referência OSI

Estabelece regras para que a comunicação entre dois ou mais dispositivos de rede possa acontecer, originou-se da organização ISO em 1971 e foi formalizado em 1983.

Para que ocorra esta intercomunicação o modelo de referência subdivide em sete camadas, cada uma delas responsável por encapsular e desencapsular as informações.

Tanenbaum (2003, p.45-47) define as sete Camadas do modelo OSI:

- **Camada física:** A camada física trata da transmissão de bits brutos por um canal de comunicação. O projeto da rede deve garantir que, quando um lado enviar um bit 1, o outro lado o receberá como um bit 1, não como um bit 0;
- **Camada de enlace de dados:** A principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruta em uma linha que pareça livre de erros de transmissão não detectados para a camada de rede;
- **Camada de rede:** A camada de rede controla a operação da sub-rede. Uma questão fundamental de projeto é determinar a maneira como os pacotes são roteados da origem até o destino;
- **Camada de transporte:** A função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores caso necessário, repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade;
- **A camada de sessão:** A camada de sessão permite que os usuários de diferentes máquinas estabeleçam sessões entre eles. Uma sessão oferece diversos serviços, inclusive o controle de diálogo (mantendo o controle de quem deve transmitir em cada momento), o gerenciamento de símbolos (impedindo que duas partes tentem executar a mesma operação crítica ao mesmo tempo) e a sincronização (realizando a verificação periódica de transmissões longas para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha);
- **Camada de apresentação:** Diferente das camadas mais baixas, que se preocupam principalmente com a movimentação de bits, a camada de apresentação está relacionada à sintaxe e à semântica das informações transmitidas;
- **Camada de aplicação:** A camada de aplicação contém uma série de protocolos comumente necessários para os usuários. Um protocolo de aplicação amplamente utilizado é o HTTP (*Hyper Text Transfer Protocol*), que constitui a base para a *World Wide Web*.

2.5 Topologia da rede

2.5.1 Rede Hierárquica

A distribuição de dados entre computadores que compartilhar o espaço físico pode gerar aspectos positivos ou negativos, mesmo sem possuir uma estrutura bem planejada. As redes podem trazer benefícios diversos para uma empresa, o problema é que de acordo com o crescimento se não houver um preparo podem virar uma tremenda dor de cabeça tanto para o analista de redes, quanto para a empresa em geral. É muito comum encontrarmos redes desorganizadas com problemas que nem os administradores sabem direito a origem do problema. A organização da rede é fundamental para um bom funcionamento e uma boa administração. O modelo hierárquico de rede poderia evitar diversos problemas futuros, com ela seria possível adaptar a metodologia que melhor se encaixar ao seu espaço físico, facilitar o gerenciamento, se preparar para um possível crescimento, e também, poderia ganhar mais agilidade nas resoluções dos problemas. As três camadas do modelo hierárquico são:

- Camada de Acesso: Camada que serve como um meio de conexão a dispositivos à rede, controla quais possuem permissão de comunicação, estabelece a conexão de equipamentos como: roteadores, switches, bridges, hubs e pontos de acesso wireless;
- Camada de Distribuição: Camada responsável por controlar o fluxo de transferência de dados das redes e determinar os domínios de broadcast, realizando funções de distribuição entre as VLANs;
- Camada de Núcleo: Camada responsável por disponibilizar os grandes volumes de dados entre as redes e transferência de dados em alto desempenho.

2.5.2 Ponto a ponto

Em uma rede ponto a ponto os computadores trabalham ao mesmo nível, dessa forma poderia interligar os computadores interconectados através de um *Switch*, assim eles poderiam trocar informações entre si e compartilhar o acesso à *Internet*, sem necessitar de um servidor na rede onde ficariam todas as máquinas interconectadas e fazendo o compartilhamento de dados.

2.5.3 Barramento

A aplicabilidade desse modelo não seria o mais viável para uma empresa. A rede em barramento todos os computadores ficariam interligados a mesma linha de transmissão através de cabos.

2.5.4 Anel

Ao enviar uma mensagem ela entraria no anel e circularia até ser retirada pelo host destino, ou então voltaria ao emissor, dependendo do protocolo empregado. A baixa tolerância a falhas desse modelo poderia fazer com a uma mensagem entre em loop infinito caso ocorra algum tipo de falha em sua transmissão.

2.5.5 Estrela

Uma topologia que possibilitaria a conexão de todos os cabos ao ponto central de conexão, dessa maneira, facilitaria a manutenção caso um dos *hosts* saíssem da rede por mal funcionamento ou algum problema no cabo que o liga no ponto *hub* ou *switch*, que neste caso seriam os responsáveis pela distribuição de pacotes. Esse modelo seria melhor aplicável para pequenas e médias empresas, devido ao fato da maioria dos *hubs* e *switchs* não possuírem muitas portas.

3 SAMBA

De acordo com Filho (2012, p.823) o SAMBA é um serviço famoso por implementar o protocolo SMB/CIFS no GNU/Linux. Esse protocolo é responsável por permitir que máquinas MS *Windows* compartilhem arquivos e impressoras, além de outras tarefas inerentes às redes *Microsoft*.

O SAMBA é compatível com a maioria dos sistemas operacionais da Microsoft e em alguns casos como o do SAMBA 4 é possível gerenciar sua interface através de uma ferramenta da *Microsoft*, RSAT (*Remote Server Administration Tools Windows*). Com esta ferramenta é possível utilizar todas as facilidades do *Active Directory* que é uma ferramenta paga desenvolvida pela *Microsoft*.

O SAMBA sobressai em relação aos serviços concorrentes por ser uma ferramenta *Open Source* e não possuir custo de adesão. Em um ambiente corporativo o compartilhamento e gerenciamento de arquivos, impressoras e nível de acesso dos usuários podem influenciar diretamente na segurança de informação da corporação. Através do Samba seria possível criar grupos de trabalho similares aos setores da organização e disponibilizar pastas com níveis de acesso para as diferentes plataformas distribuídas pela rede. Assim torna-se possível o compartilhamento de dados entre máquinas *Windows* e Linux. Por exemplo, pastas criadas pelo setor contábil que possua instalado distribuições Linux, poderiam ser visualizadas pelo setor de vendas que possua máquinas *Windows*, mas o setor de vendas se limita apenas na visualização sendo impossibilitado de remover, adicionar ou editar arquivos da pasta compartilhada. Com o servidor Samba seria possível controlar o acesso a determinados recursos de rede com igual ou maior eficiência que servidores baseados em sistemas operacionais da *Microsoft*.

4 VPN

De acordo com Silva (2002 p.21) dois ou mais computadores interligados formam uma rede de computadores (*network*). Esses equipamentos juntos compartilhando informações, formam uma rede privada LAN, onde apenas os equipamentos pertencentes a este grupo podem ter dados compartilhados. Existem equipamentos de rádio que proporcionam o longo alcance na comunicação entre dispositivos e transferência de dados, podendo assim, interligar componentes a quilômetros de distância. Caso haja algum tipo de obstáculo, a conexão por rádio pode perder boa parte do seu desempenho. Outro fator que pesa na hora criar uma estrutura a rádio é o alto custo dos equipamentos.

Estes equipamentos como *hubs* ou *switches* são interligados às placas de rede existentes em cada equipamento, realizando as ligações entre máquinas e possibilitando o compartilhamento de informações.

A conexão VPN (*Virtual Private Network*) seria uma opção para corrigir algumas falhas apresentadas em um sistema a rádio. A criação de túneis virtuais criptografados permitiria que a comunicação entre dois ou mais computadores fosse feita sem precisar investir um alto valor em dinheiro para estabelecer a troca de informações entre eles. Para que aconteça o uso dos recursos do túnel criptografado gerado, é criado um certificado digital que irá garantir que o cliente que requisita o acesso está de fato liberado para estabelecer a comunicação. Ao estabelecer a conexão com a outra máquina que se encontra do outro lado do túnel pode-se configurar o cliente para que usufrua dos recursos da rede disponíveis através de configurações que irão direcionar a conexão cliente para o servidor. Para aumentar a eficiência no quesito segurança, seria viável a criação de um servidor VPN dentro de uma rede que já possua o *FIREWALL* configurado de acordo com as regras de negócios da empresa.

Conciliar uma rede VPN que interligaria as filiais de uma organização com uma aplicação *web*, poderia satisfazer as necessidades de uma empresa quanto a velocidade na troca de informações. Um dos pontos fortes em utilizar uma estrutura de tunelamento, seria o fato de que os tomadores de decisões, mesmo que estejam em uma viagem de negócios, possam consultar o sistema da empresa de onde quer que estejam, facilitando significativamente nas tomadas de decisões. Em outros cenários, um vendedor poderia consultar o estoque da empresa antes de efetuar uma venda através de um *smartphone* ou *tablet* com acesso à *Internet*.

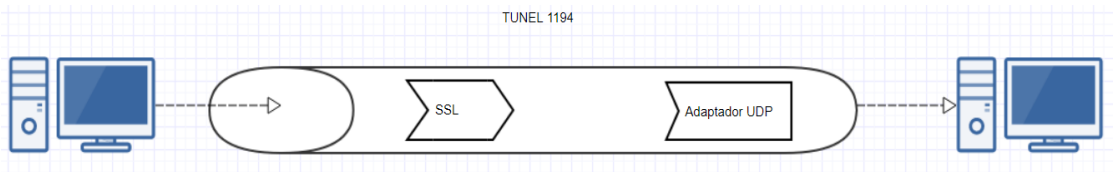
4.1 OpenVPN

OpenVPN é uma ferramenta de código aberto desenvolvida pelo Projeto OpenVPN/OpenVPN *Technologies*. Seu lançamento inicial foi em 13 de Maio de 2001. Esta ferramenta contém recursos de chaves pré-compartilhadas e autenticação por certificado digital.

O custo de um *link* de *Internet* dedicado é alto e talvez não seja viável para pequenas empresas. O *OpenVPN* possibilitaria o compartilhamento de impressoras, *softwares*, pastas, rede interna de telefone IP utilizando *Voip*. Tudo isso de forma segura desde que em cada loja haja conexão com *Internet* e configurações necessárias, dispensando assim a necessidade de um alto investimento em um link dedicado de internet. A utilização de um *firewall* aumentaria a segurança da rede VPN, apesar do *OpenVPN* possuir seu próprio firewall e gerar um *script* de autenticação totalmente fechado. Seria aconselhável implementar o *firewall* específico de acordo com as necessidades.

Conforme mostra a figura 1, o tráfego do OpenVPN usa a criptografia SSL que o ajudaria a manter a segurança dos dados criando também um adaptador virtual para uma conexão UDP que encapsula os pacotes e os transporta para o destino, pelo túnel 1194 que é sua porta padrão.

Figura 01: OpenVpm



Fonte: dos próprios autores

5 VIRTUALIZAÇÃO

De acordo com Veras (2016, p.2), “a virtualização de servidores em arquiteturas abertas e de baixo custo, como a arquitetura x86, vem resolver um problema-chave relacionado à construção dessa infraestrutura. ” A virtualização adequa o *hardware* à carga de trabalho que foi criada pela aplicação. Sendo assim, se a aplicação necessita de muito recurso computacional, pode-se alterar a configuração do *data center* de maneira dinâmica e este recurso é fornecido subtraindo o recurso de aplicação que até aquele momento precisava de demanda. Em outro momento, pode-se novamente restabelecer a configuração original e até expandir o uso do recurso.

O aumento do poder computacional tem proporcionado experiências relevantes relacionadas a virtualização, elevando o nível de segurança e flexibilidade de informação. Através desta tecnologia pode-se aprimorar o aproveitamento do hardware de um computador. Ao contrário do que a maioria dos usuários finais estão acostumados, em ter apenas um sistema operacional funcionando por vez no microcomputador, em um ambiente virtualizado seria possível a criação de vários serviços em diferentes sistemas operacionais, por exemplo, um serviço de firewall sendo executado por um servidor Linux, um serviço web sendo executados por um sistema *Windows*, todos sendo executados ao mesmo tempo em cima da mesma estrutura de hardware, essa portabilidade é uma das grandes vantagens de uma estrutura virtualizada.

A construção de um ambiente virtualizado depende de um hardware que suporte às tecnologias de virtualização, um sistema operacional com a função de fatiar as partes do hardware dividindo-as entre as máquinas virtuais.

A virtualização de servidores traz inúmeras vantagens, como:

- **Custo-benefício:** Ao contrário de possuir um computador para cada serviço a ser executado, com a utilização de ambientes virtualizados, pode-se executar todos na mesma estrutura física, com isso, economiza espaço e dinheiro.
- **Flexibilidade**: De acordo a rede for expandindo a sua estrutura física e as máquinas virtualizadas começar a exigir mais capacidade de hardware, pode-se incluir mais capacidade ao servidor que solicita, fatiando a estrutura física fazendo o uso de ferramentas que podem realocar recursos de uma máquina virtual para a outra, além disso, pode-se trocar a máquina virtual de plataforma, a fim de aumentar o seu desempenho.
- **Recuperação de Desastres**: Os clones das máquinas virtuais podem ser feitos com finalidade de salvar o estado atual, para que de forma redundante ela possa executar o mesmo serviço, trabalhar com os mesmos dados caso haja falhas na máquina principal.

A virtualização de servidores traz alguns pontos negativos como:

- **Segurança:** Se a máquina hospedeira possuir alguma falha de segurança todas as outras correm o risco de serem afetadas;
- **Desempenho:** A inserção de mais uma camada entre o sistema operacional e hardware, gera um consumo bem maior de recursos, podendo afetar o desempenho da estrutura;

A seguir alguns exemplos de gerenciadores de máquinas virtuais:

- **Virtualbox:** Foi criado pela empresa Innotek depois comprada pela Oracle. Ele está disponível de forma gratuita através do site da Oracle. É usado para virtualização de vários sistemas operacionais e disponíveis em vários sistemas como Windows, Linux e Mac.

5.1 KVM

Kernel Virtual Machine (KVM) é um *software* de virtualização similar ao *Virtualbox*, facilmente gerenciável pelo *Virt-manager* que também é gratuito. Disponível para plataformas Linux, ele é capaz de emular a maioria dos sistemas operacionais e suporta as tecnologias de virtualização da *Intel* e AMD. Por possuir integração a tecnologia *Quemu* que o permite acesso direto ao *hardware* e *drivers* inclusos na árvore de *kernel* do Linux, faz dele mais rápido se comparado com alguns

softwares do mesmo segmento. O gerenciamento do sistema de virtualização do KVM é feito através do v*irt-manager*, uma interface gráfica no qual tem a função de auxiliar os usuários a fatiar *hardware* com as máquinas virtuais podendo configurar e alterar os parâmetros das mesmas. Alguns processadores não possuem suporte para virtualização que é um dos requisitos mínimos para a execução do KVM, podendo ser emulado em uma ou mais máquinas virtuais no computador, sendo necessários uma quantidade de memória *ram* que dê conta de executar o sistema a raiz e as VMs.

6 SOFTWARE LIVRE

O *software* Livre possui diversas opções que podem beneficiar uma empresa, funciona como uma forma de distribuir conteúdo a uma comunidade para que ela possa estudar copiar, modificar, executar, distribuir e melhorar os *softwares*.

A liberdade das ferramentas livres permite que o *software* evolua conforme a necessidade dos seus usuários, sendo que os códigos podem ser facilmente acessíveis, fazendo com que os desenvolvedores interessados molde o pacote de *software* de acordo com a sua necessidade.

Os pacotes desenvolvidos voltados para o mundo *open Source* atendem qualquer tipo de organização, sendo possível modificar o programa para adaptá-lo ao modelo de negócio desejado, fazendo dessas ferramentas algo diferenciado no mercado da tecnologia e proporcionando a produção de mais *softwares* que atendam certos tipos de demandas com possibilidades de mudanças em relação a proposta original.

Existe uma certa diferença entre *software* livre e *software* grátis, sendo que os *softwares* grátis geralmente são protegidos por leis de propriedade intelectual, como o *copyright*, onde o dono do programa define como será usado o seu produto de *software*.

O *software* livre também deve seguir regras ou liberdades conforme cita o Gnu:

- A liberdade de executar o programa como você desejar para qualquer propósito;
- A liberdade de estudar como o programa funciona, e adaptá-lo às suas necessidades. Para tanto o acesso ao código-fonte é um pré-requisito.
- A liberdade de redistribuir cópias de modo que você possa ajudar ao próximo.

- A liberdade de distribuir cópias de suas versões modificadas a outros. Desta forma, você pode dar a toda comunidade a chance de se beneficiar de suas mudanças. Para tanto, acesso ao código-fonte é um pré-requisito.

O GNU também usa algo parecido com o *copyright* ou *copyleft*, que contém certas regras de distribuir o *software* e proteger legalmente as quatro liberdades.

O GNU utiliza o *Kernel* do Linux, desta forma, devido a esta combinação é que o sistema operacional GNU/Linux recebe este nome. De acordo com a comunidade existem vários tipos de licenciamento no *Software* Livre:

Conforme Reis (2003, p.14) apresenta algumas das licenças mais usadas:

- **GNU GPL:** A licença de *software* livre mais importante atualmente segundo o freshmeat.net. Ela permite redistribuição apenas se for mantida a garantia de liberdade aos receptores da cópia redistribuída e das modificações se acompanhadas de código-fonte.
- **BSD, X, MIT, Apache:** Permite redistribuir, no entanto as licenças BSD originais inclui uma cláusula que obriga cópias redistribuídas a manter um aviso de *copyright*. As X e MIT permitem versões não livres.
- **MPL, GNL LGPL:** Não são muito permissivas, só permitindo a redistribuição do código quando garantida a liberdade inalterada do código. Permitindo que o código seja usado em um “produto maior” sem que este tenha que ser licenciado livremente. Se modificações forem feitas o código, devem ser fornecidas junto com código fonte.

7 SEGURANÇA DE INFORMAÇÃO

A Tecnologia da Informação tem exercido um papel cada vez mais relevante para instituições de administração Públicas e Privadas. Grandes empresas têm centralizado seus dados em sistemas computadorizados, como por exemplo, empresas do ramo bancário, onde seus clientes fazem diversas transações por aparelhos celulares ou computadores. O crescimento consequentemente trouxe maiores riscos, no mundo virtual a segurança de informação torna-se um ponto crucial para o avanço das instituições.

O investimento em segurança de informação é elevado e necessário. Antes da popularização dos computadores a segurança dos dados se limitava a uma porta de armário trancado ou até mesmo de um cofre contendo documentos confidenciais. Nos dias atuais a segurança de informação tomou rumos diferentes, exigindo um pouco mais de complexidade para se ter acesso aos dados. Atualmente os dados são armazenados em um computador servidor, configurado com regras de segurança cada vez mais sofisticadas.

De acordo com a NBR ISO/IEC 17799 (2005) define a Segurança da Informação como:

> Política de proteção existente sobre as informações de uma determinada organização de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades do negócio. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.[1]

Os riscos que poderiam acarretar ao conectar um computador que possua uma base de dados à rede mundial de computadores, pode ser de roubo de informações à

[1] Disponível em: <http://www.cienciananasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf>

falência de uma empresa. Técnicas e estratégias poderiam elevar a confidencialidade dos dados, levando em consideração as dificuldades de implementação das regras de negócios de cada organização em seu sistema de informação, sendo que cada empresa tem sua cultura, processos administrativos específicos, funcionários de diferentes perfis. Cada detalhe poderia ser analisado e estudado ao elaborar implantação de medidas de segurança de informação, a fim de precaver desastres digitais, além da implementação em nível de *software* seria necessário o controle de acesso ao hardware servidor e conscientização dos administradores.

7.1 C I D

Confidencialidade, Integridade e disponibilidade são os pilares principais para garantir a segurança de informação na rede de computadores. Goodrich (2012, p. 3-4) descreve CID como:

- **Confidencialidade:**

"Confidencialidade é evitar a revelação não autorizada de informação. Isto é, confidencialidade envolve a proteção de dado, propiciando acesso àqueles que são autorizados a vê-los e não permitindo que outros saibam algo a respeito de seu conteúdo".

A informação manter-se secreta é incessantemente a essência da segurança de informação e é este conceito que antecede os computadores. Nos primeiros registros de criptografia Júlio César comunicava-se com os seus superiores utilizando uma codificação muito simples: cada letra da mensagem era substituída, sendo D por A, E por B e sucessivamente. Na época, esta codificação era provavelmente segura, uma vez que a maioria dos inimigos de César não liam em latim.

Nos dias atuais, conseguir confidencialidade é mais desafiador. Ela é a que mais sofre com ameaças de segurança e para que isso não ocorra projetistas de sistema tem desenvolvido ferramentas para diminuir sua vulnerabilidade.

- Encriptação: a alteração da informação utilizando um segredo, chamado de chave de encriptação, de tal forma que essa informação só possa ser lida com a chave de decriptação. Para ser realmente seguro o esquema deve ser extremamente difícil para que alguém possa descobrir a informação original sem a utilização da chave de decriptação;

- Controle de acesso: regras e políticas que limitam o acesso à informação a pessoas autorizadas;
- Autenticação: determinação da identidade da pessoa que vai usar o sistema. A autenticação pode ser feita com uma senha, cartão, dispositivo armazenador de senhas, impressão digital, scanner de rosto entre outros recursos que podem ser adotados;
- Autorização: permissão que a pessoa ou um sistema deve ter para acessar recursos baseado na política de controle de acesso, evitando acessos a áreas ou arquivo protegidos;
- Segurança física: estabelece barreiras físicas para limitar o acesso a dados protegidos. O que pode ser cadeados em gabinetes, câmeras de segurança, alarmes, etc. Tudo que por meio físico impeça o acesso aos dados.

➢ **Integridade:**

A integridade é a forma que a informação circula sem alteração por não autorizados. Goodrich (2012, p.7) também detalha meios que podem ajudar a manter a integridade dos dados:

- Cópias de segurança: arquivamentos dos dados para que possam ser restaurados caso tenha sido alterado;
- Somas de verificação (*checksums*): “a computação de uma função que mapeie o conteúdo de um arquivo para um valor numérico. ” Esse valor é usado para verificar brechas na integridade dos dados;
- Códigos de correção de dados: são métodos para armazenamento de dados de maneira que alterações sejam detectadas e automaticamente corrigidas;

➢ **Disponibilidade:**

A disponibilidade apoia-se no princípio de que a informação deve ser acessível, disponível e modificável para uso oportuno a qualquer momento para usuários autorizados quando mais se necessita. Na disponibilidade, Goodrich (2012, p. 8) descreve ferramentas que ajudam a manter a informação acessível:

- Proteções físicas: infraestrutura capaz de armazenar de forma segura que resista ou tenha perversão a todos os problemas que uma estrutura física possa ter;

- Redundâncias computacionais: “computadores e dispositivos de armazenamento que servem como reserva no caso de falhas”.

7.2 Firewalls

Os pacotes enviados de uma rede para outra poderiam passar pelo *firewall* que teria o papel de analisá-los e determinaria se eles representam algum risco para a integridade do sistema. Caso seja detectado algum risco, os pacotes seriam descartados. Configurado para prover filtragem controlada na rede, permitiria o acesso restrito a algumas portas de comunicações na Internet, e bloquearia o acesso a quase todo o resto das outras conexões. Uma das principais funções do firewall seria garantir a segurança de sua rede contra acessos maliciosos.

A velocidade na troca de informações é um ganho para a humanidade, mas quando o assunto é segurança surge enormes preocupações, pois além de não possuir leis específicas para qualificar alguns crimes cibernéticos, existem diversas pessoas mal-intencionadas que estão na rede à procura de uma falha de segurança e prontas para se beneficiar delas, seja de forma positiva ou não. Uma medida para precaver possíveis ataques são os *Firewalls.* Para melhor exemplificar, imagine-se uma rede física cercada por paredes cujo único acesso é através de uma porta. É basicamente assim que funciona o *firewall*, é criado um cerco virtual em volta da rede de computadores controlando todos os pacotes que entram e saem da rede e restringindo acesso com intuito de evitar que invasores tenham acesso a informações privilegiadas.

Tanenbaum (2003, p.582) explica que:

> A capacidade de conectar qualquer computador em qualquer lugar a qualquer outro computador em qualquer lugar é uma faca de dois gumes. É muito divertido para as pessoas navegarem pela Internet quando estão em casa. Para os gerentes de segurança das empresas, trata-se de um pesadelo. Muitas empresas têm grandes quantidades de informações confidenciais on-line — segredos comerciais, planos de desenvolvimento de produtos, estratégias de marketing, análises financeiras etc. A revelação dessas informações para um concorrente poderia ter terríveis consequências.

Há um perigo caso as informações confidenciais de uma empresa venham a público e caso ocorra o vazamento de tais informações poderia levar uma empresa a falência, dependendo da informação, pode destruir uma empresa. Por isso, a segurança de informação de uma organização é indispensável. Vírus, Malweres, ou

outras “pestes” digitais podem burlar a segurança de uma empresa e destruir dados que sejam valiosos e consumir tempo e recursos de administradores que tentam eliminá-los e consertar a bagunça e prejuízo causados por eles. Frequentemente podem ser inseridos nos computadores da empresa por funcionários descuidados que acessam sites duvidosos ou utilizam programas que comprometem a segurança da organização.

Para alcançar os objetivos de impedir que pestes digitais e intrusos invadam a rede da empresa o uso dos *firewalls* seria indispensável.

7.3 Segurança Sem Fios

As redes de computadores sem fios se tornaram realidade e uma opção viável para instituições públicas, privadas ou até mesmo para uso doméstico. Mas, as redes sem fio apresentam uma série de vulnerabilidades que tem sua origem na concepção dos padrões adotados. Ao contrário das redes cabeadas, as redes sem fios são de transmissão não guiada num meio comum e acessível a todos, dentro do raio de ação das antenas. Neste cenário, caso a rede não tenha configurado mecanismos mínimos de segurança, o acesso a essa rede fica imediatamente disponível a quem esteja dentro do raio de alcance.

A tentativa de tornar as *interfaces* dos gerenciadores de redes sem fios em uma ferramenta intuitiva para os usuários, faz com que o essencial não tenha tanta atenção, neste caso a segurança. Em geral, quando o usuário adquire um dispositivo *wireless,* ao conectá-lo na eletricidade, instantaneamente um sinal *wi-fi* fica disponível em seu raio de alcance quase sempre sem qualquer segurança. Se ele for conectado a uma rede local, todo tráfego desta rede estará disponível para qualquer usuário que esteja com acesso.

7.3.1 Mecanismos de Criptografia

7.3.1.1 WEP

Paim (2012, p.2) define o funcionamento do WEP dividida em duas partes: (1) autenticação e encriptação e (2) decriptação de mensagens. Baseado na troca de quadros encriptados pelo algoritmo RC4. A ordem apresentada será inversa dos textos da área: primeiro o processo de troca de mensagens e então, o de autenticação. Esta ordem é mais interessante pelo fato da autenticação utilizar mecanismos que estão presentes na troca de mensagens. A compreensão do funcionamento do mecanismo de encriptação/decriptação baseia-se no entendimento do algoritmo RC4. Como detalhe adicional, para garantir maior segurança ao processo, a permutação oriunda do KSA deve ser diferente a cada mensagem enviada.

7.3.1.2 WPA

Segundo Paim (2012, p.2), WPA é o protocolo usado para encriptação da mensagem transmitida. Ele faz uso do algoritmo RC4, da mesma forma que o WEP, mas toma algumas precauções para evitar ataques, como: (1) não enviar a chave secreta em claro e (2) trabalhar com uma política de vetores de inicialização mais inteligente. O WPA funciona a partir de uma chave secreta contendo entre 32 e 512 bits conhecida como PMK, que gera uma PTK, a partir de alguns parâmetros obtidos durante a conexão, sendo compartilhada entre o computador e o ponto de acesso.

7.3.1.3 WPA2

A definição dada por Horovits (2013, p7), é que o WPA2 utiliza um protocolo denominado "*Advanced Encryption Standard*" (AES), que é muito eficiente, mas possui a desvantagem de exigir bastante processamento. O seu uso é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de

equipamentos de redes pouco sofisticadas. O principal objetivo do WPA2 é suportar as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e codificação, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio.

8 PROCEDIMENTOS METODOLÓGICOS

O desenvolvimento deste trabalho baseia-se em livros de redes de computadores, segurança de informação, artigos, cursos online e nas disciplinas de Redes de Computadores estudadas na graduação. Realizado por meio de análise corporativa, tendo como alvo principal os desenvolvimentos de melhoria na estrutura de rede de uma autarquia do município de Itambacuri-MG.

8.1 Ferramentas

8.1.1 Firewall

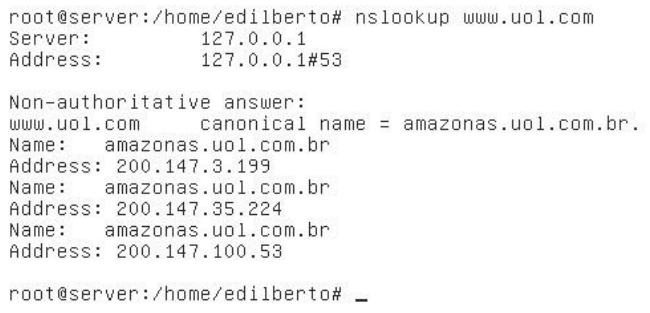
Com intuito de aplicar melhorias na segurança, foram elaboradas regras aplicadas ao *firewall* para gerenciar a entrada e a saída de pacotes e acesso às portas do servidor principal. A ferramenta de *firewall* utilizada foi o *Netfilter* que trabalha diretamente vinculado ao *Kernel* do Linux e é gerenciada pela ferramenta *iptables*. O vínculo com o *Kernel* faz com que os níveis de segurança sejam mais confiáveis do que em *firewalls* que trabalham na camada de aplicação. O *firewall* desenvolvido neste trabalho tem como objetivo permitir acesso à *Internet* para as máquinas das redes locais, gerenciar a comunicação das máquinas locais e interligadas via VPN e fiscalizar tudo que entra e sai dos clientes.

8.1.2 DNS

O servidor DNS funciona como um sistema de tradução de endereços IPs para nomes de domínios e vice-versa, quando estes endereços são resolvidos em um

servidor local temos um ganho de velocidade e segurança. O servidor DNS também tem seu papel nas redes locais onde a configuração de uma zona DNS permite resolver nomes de máquinas ligadas ao servidor local facilitando a gerência das redes. Existem duas formas de acessar páginas *webs* na *Internet*: pelo nome do domínio ou através do endereço IP do servidor onde a página está configurada. A mesma página pode ser acessada por vários endereços IPs, mas possui nomenclatura de domínio única. Por exemplo, ao executar o comando 'nslookup' vinculado a página da UOL do nosso servidor local, que está configurado como servidor DNS, retorna o resultado como mostra a figura abaixo:

Figura 02: IPs



Fonte: Dos próprios autores

Como mostra a figura 02, são três endereços IPs diferentes vinculados ao domínio amazonas.uol.com.br

8.1.3 DHCP

Em uma rede de computadores doméstica a atribuição de endereços IPs pode ser feita de forma manual ou através do gerenciamento de um roteador, já nas redes corporativas há a exigência de um sistema gerenciável flexível. O servidor DHCP aqui

utilizado foi o ISC-DHCP-SERVER, que possibilita a criação de diretórios para a gerência das redes.

A distribuição de endereços está sendo feito de forma automática para as seguintes faixas:

192.168.10.0/24

192.168.20.0/24

192.168.30.0/24

Sendo assim, em qualquer uma das interfaces que o Host seja conectado, ele obteria um endereço IP automaticamente, dessa forma, poderia ser definido um range de endereços para as redes onde eles seriam distribuídos dentro de um intervalo configurado de acordo com as necessidades da empresa.

8.1.4 Samba

O *software* Livre Samba4 não precisa de licença e vem carregado de inúmeras facilidades para as empresas estabelecerem a comunicação, gerência e transferência de dados entre os seus computadores. Nele será simulado os setores da empresa. Através da ferramenta Rsat, será feito o gerenciamento do Samba usando uma máquina *Windows* e facilitando a manutenção e gerência.

As permissões dos diretórios gerenciados pelo servidor Samba serão definidas de acordo com a definição física da organização. Os diretórios compartilhados serão montados automaticamente através de um *script* que vai ser executado nas máquinas clientes.

Com o Samba4 é possível:

- Criar um AD (*ACTIVE DIRECTOY*) completo;
- Criar um controlador de domínio Principal;
- Pode ser administrado usando interface Gráfica do próprio Windows;
- Migrar de forma fácil de AD *Windows* para um AD Linux e vice-versa;
- É possível trabalhar com perfil móvel;
- Trabalhar com permissões como a do Windows;
- Trabalhar com GPO;

- Por ser *software* Livre, não precisa de licença;
- Pode-se fazer com que o SAMBA 4 trabalhe como controlador de domínio adicional do Windows server;
- Já vem com DNS, kerberos, LDAP integrado;
- Posso fazer a integração do SAMBA 4 com o proxy *Squid*, PfSens.

8.1.5 Proxy/Cache

O *proxy* pode fazer o controle de acessos às páginas *webs* acessadas pelos *hosts* da rede, sendo possível, além de bloquear o acesso à páginas indesejadas que não estejam de acordo com as políticas internas da empresa, permitir que as requisições sejam armazenadas e distribuídas através dos dados armazenados de uma requisição anterior. O *cache* funciona da seguinte forma: Quando for feito o acesso em uma determinada página *web*, o servidor *proxy* faz o armazenamento temporário dos registros daquela página, sendo assim quando um outro usuário requisitar a mesma página ela será carregada através dos dados temporários armazenados ao invés de fazer nova requisição do servidor na *Internet*. O *Proxy* tem como função principal intermediar as requisições de clientes para outros servidores.

Já o Servidor de Cache faz o armazenamento de dados de navegações localmente, possibilitando uma economia de banda de *Internet* e uma melhoria no tempo de resposta para os usuários, pois os dados estarão disponíveis *off-line.*

8.1.6 KVM e QEMU

Estas ferramentas ao contrário de opções similares como o *virtual box,* que trabalha a nível de aplicação, trabalham a nível de *Kernel* o que faz delas uma opção mais viável para redes corporativas, pois podem garantir uma melhoria de desempenho para as máquinas virtualizadas permitindo a criação e gerência dos servidores virtuais, possibilitando de formas simples os *backups* das configurações dos servidores e se houver troca da estrutura física não haverá grandes transtornos, pois podemos restaurar o backup na nova estrutura. A possibilidade de fatiar o hardware entre as máquinas virtuais, faz com que o aproveitamento dos recursos

disponíveis seja feito de forma eficiente. Em *hardware* real, o Sistema Operacional traduz os programas em instruções que são executadas pela CPU física. Em uma máquina virtual, a principal diferença é que a CPU virtual é realmente emulada (ou virtualizada) pelo *hypervisor.* Portanto, o *software* do *hypervisor* tem a função de traduzir as instruções destinadas à CPU virtual.

8.1.7 OpenVPN

Quando se tem matriz e filial a comunicação entre os estabelecimentos devem ocorrer de forma segura, quando as estruturas físicas estão geograficamente próximas esta comunicação pode ser feita através de rádios. Mas, se estão em outras cidades, esta comunicação passa a ser o um obstáculo para os rádios, sendo necessário a utilização de túneis criptografados. Neste trabalho utilizaremos o OpenVPN.

8.2 Metodologia

8.2.1 Firewall

Para configuração do firewall foi criado um arquivo em *Shell Script* no diretório “/etc/firewall.txt” após sua criação foi adicionado as seguintes regras, como mostra o arquivo 01.

Arquivo 01: Comandos que se aplicam ao interromper o firewall para todas as interfaces

```
###Regras para o case de STOP
parar(){
iptables -F
iptables -t nat -F
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
}
```

Fonte: Dos próprios autores

Arquivo 02: Comandos padrões para aplicar o *firewall*

```
###Regras Gerais
geral(){
iptables -F
iptables -t nat -F
iptables -P INPUT DROP
iptables -P FORWARD DROP
modprobe ip_conntrack_ftp
}
```

Fonte: Dos próprios autores

Arquivo 03: Gerencia das portas de entrada dos servidores

```
###Regras para o INPUT do próprio servidor

entrada(){

#Gerais

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j
ACCEPT

iptables -A INPUT -p icmp -j ACCEPT

iptables -A INPUT -p tcp --dport 67 -j ACCEPT #DHCP

iptables -A INPUT -p udp --dport 67 -j ACCEPT #DHCP

iptables -A INPUT -p tcp --dport 68 -j ACCEPT #DHCP

iptables -A INPUT -p udp --dport 68 -j ACCEPT #DHCP
```

Fonte: Dos próprios autores

Arquivo 04: Permissões para o DNS

```
###DNS

iptables -A INPUT -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --sport 53 -j ACCEPT
```

Fonte: Dos próprios autores

Arquivo 05: Permissões para NTP

```
###NTP

iptables -A INPUT -p udp --dport 123 -j ACCEPT

iptables -A INPUT -p udp --sport 123 -j ACCEPT
```

Fonte: Dos próprios autores

Arquivo 06: Permissões para a rede1 se comunicar com SSH e SQUID

```
#Rede1

iptables -A INPUT -s 192.168.10.0/24 -p tcp --dport 2222 -j
ACCEPT #SSH

iptables -A INPUT -s 192.168.10.0/24 -p tcp --dport 3128 -j
ACCEPT #SQUID

iptables -A INPUT -s 192.168.10.0/24 -p udp --dport 3128 -j ACCEPT
#SQUID
```

Fonte: Dos próprios autores

Arquivo 07: Permissões para o *squid* na rede2

```
#Rede2
iptables -A INPUT -s 192.168.20.0/24 -p tcp --dport 3128 -j ACCEPT
#SQUID

iptables -A INPUT -s 192.168.20.0/24 -p udp --dport 3128 -j ACCEPT
#SQUID
```

Fonte: Dos próprios autores

Arquivo 08: Permissões para SSH na DMZ

```
#DMZ

iptables -A INPUT -s 192.168.30.0/24 -p tcp --dport 2222 -j ACCEPT
#SSH
```

Fonte: Dos próprios autores

Arquivo 09: Permitir comunicação entre as redes

```
###Regras para o FORWARD

encaminhamento(){

#Gerais

Iptables -A FORWARD -p icmp -j ACCEPT

Iptables -A FORWARD -p tcp -m state --state ESTABLISHED,RELATED -
j ACCEPT

Iptables -A FORWARD -p tcp -s 192.168.20.0/24 -d 192.168.30.12 -j
ACCEPT

Iptables -A FORWARD -p udp -s 192.168.20.0/24 -d 192.168.30.12 -j
ACCEPT

Iptables -A FORWARD -p tcp -d 192.168.20.0/24 -s 192.168.30.12 -j
ACCEPT

Iptables -A FORWARD -p udp -d 192.168.20.0/24 -s 192.168.30.12 -j
ACCEPT
```

Fonte: Dos próprios autores

Arquivo 10: Regras aplicas à rede1 para os protocolos htttp/https

```
#Rede1

#iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport 80 -j
ACCEPT #HTTP

#iptables -A FORWARD -s 192.168.10.0/24 -p udp --dport 80 -j
ACCEPT #HTTP

#iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport 443 -j
ACCEPT #HTTPS

iptables -A FORWARD -s 192.168.10.0/24 -p tcp --dport 8080 -j
ACCEPT #HTTP
```

Fonte: Dos próprios autores

Arquivo 11: Regras aplicadas à rede2 para os protocolos http/https

```
#Rede2

#iptables -A FORWARD -s 192.168.20.0/24 -p tcp --dport 80 -j
ACCEPT #HTTP

#iptables -A FORWARD -s 192.168.20.0/24 -p udp --dport 80 -j
ACCEPT #HTTP

#iptables -A FORWARD -s 192.168.20.0/24 -p tcp --dport 443 -j
ACCEPT #HTTPS

#iptables -A FORWARD -s 192.168.20.0/24 -p tcp --dport 8080 -j
ACCEPT #HTTP
```

Fonte: Dos próprios autores

Arquivo 12: Permitir acesso FTP entre as rede2 e DMZ

```
iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.30.11 -p tcp --
dport 21 -j ACCEPT #FTP

iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.30.11 -p tcp --
dport 20 -j ACCEPT #FTP

iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.30.11 -p tcp --
dport 989 -j ACCEPT

iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.30.11 -p tcp --
dport 990 -j ACCEPT

iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.30.11 -m tcp -p
tcp  --dport 1024:65534 -j ACCEPT #ftpssl
```

Fonte: Dos próprios autores

Arquivo 13: Permitir comunicação via SSH entre a rede2 e a DMZ

```
iptables -A FORWARD -s 192.168.20.0/24 -d 192.168.30.0/24 -p tcp
--dport 2222 -j ACCEPT #ssh

iptables -A FORWARD -d 192.168.20.0/24 -s 192.168.30.0/24 -p tcp -
-dport 2222 -j ACCEPT #ssh
```

Fonte: Dos próprios autores

Arquivo 14: Permissões para a rede DMZ

```
#DMZ

iptables -A FORWARD -s 192.168.30.0/24 -p tcp --dport 80 -j ACCEPT
#HTTP

iptables -A FORWARD -s 192.168.30.0/24 -p udp --dport 80 -j ACCEPT
#HTTP

iptables -A FORWARD -s 192.168.30.0/24 -p tcp --dport 443 -j
ACCEPT #HTTPS

iptables -A FORWARD -s 192.168.30.0/24 -p tcp --dport 8080 -j
ACCEPT #HTTP

iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.30.11 -p tcp --
dport 21 -j ACCEPT #FTP

iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.30.11 -p tcp --
dport 20 -j ACCEPT #FTP

iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.30.11 -p tcp --
dport 989 -j ACCEPT

iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.30.11 -p tcp --
dport 990 -j ACCEPT

iptables -A FORWARD -s 192.168.30.0/24 -d 192.168.30.11 -m tcp -p
tcp --dport 1024:65534 -j ACCEPT #ftpss
```

Fonte: Dos próprios autores

Arquivo 15: Regras de saída

```
###Regras para o OUTPUT

saida(){
iptables -A OUTPUT -o lo -j ACCEPT
}
```

Fonte: Dos próprios autores

Arquivo 16: Compartilhar internet da eth0 para as demais interfaces

```
###Regras para NAT na chain POSTROUTING

nat_pos() {
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
}
```

Fonte: Dos próprios autores

Arquivo 17: Configuração do PREROUTING

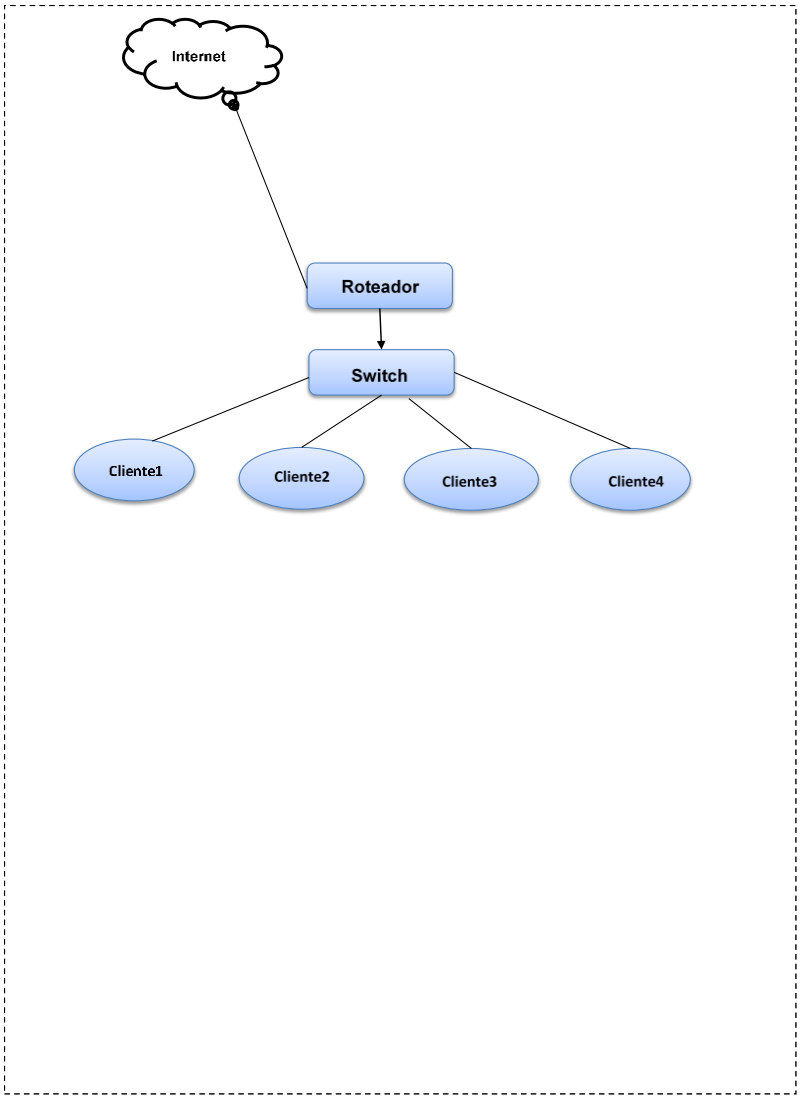
```
#nat_pre() {

#}

case $1 in

start)

geral

entrada

encaminhamento
saida

nat_pos

#nat_pre

echo "Firewall iniciado com sucesso!"
;;
stop)

parar
echo "Firewall parado com sucesso!"
;;
```

Fonte: Dos próprios autores

8.3 Resultados

A estrutura da empresa sem a aplicação das ferramentas apresentadas se encontrava da seguinte forma:

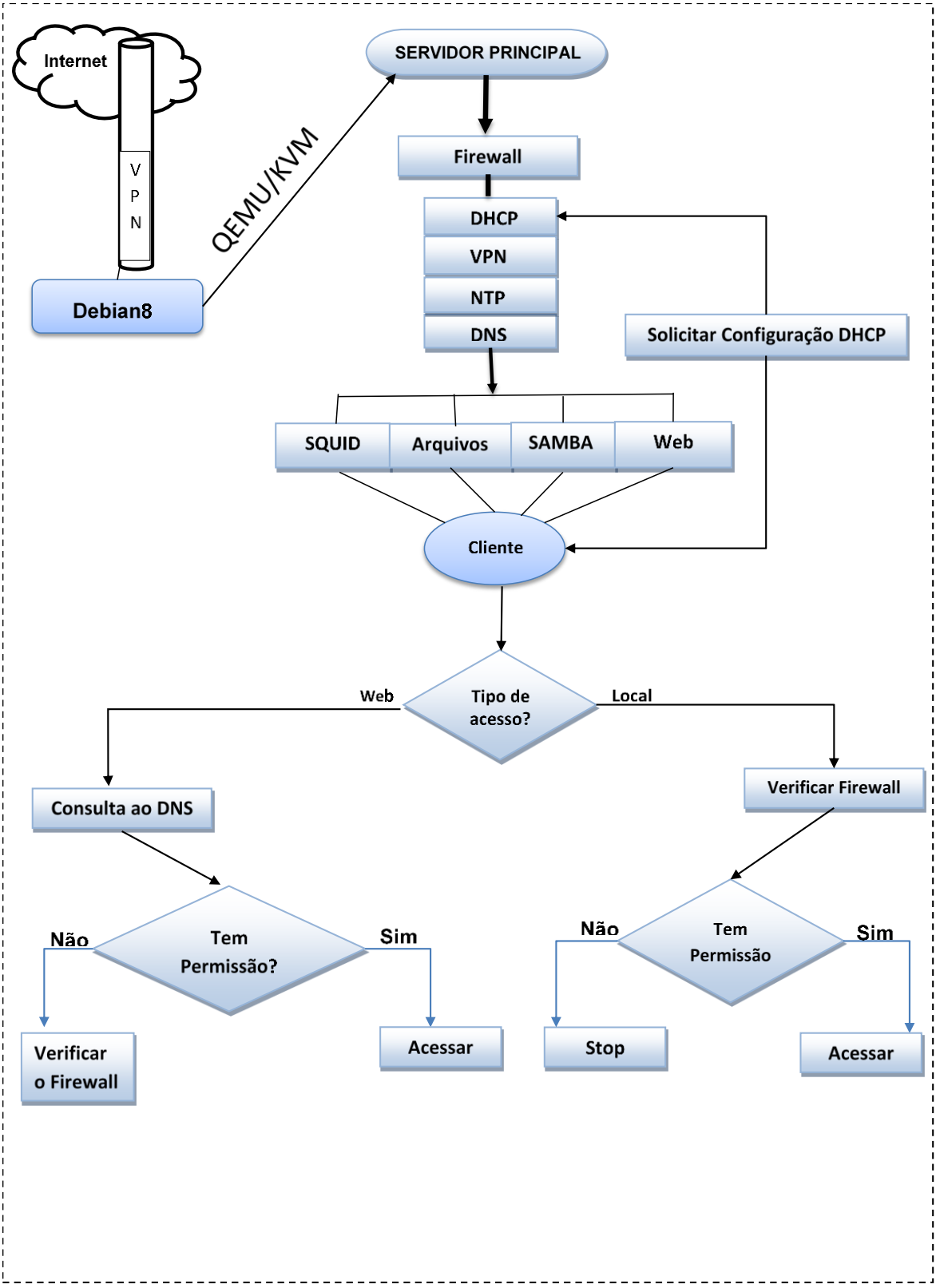
Figura 03: Estrutura inicial



Fonte: Dos próprios autores

Após os estudos e soluções encontradas por este trabalho foi montada a seguinte estrutura:

Figura 04: Estrutura final



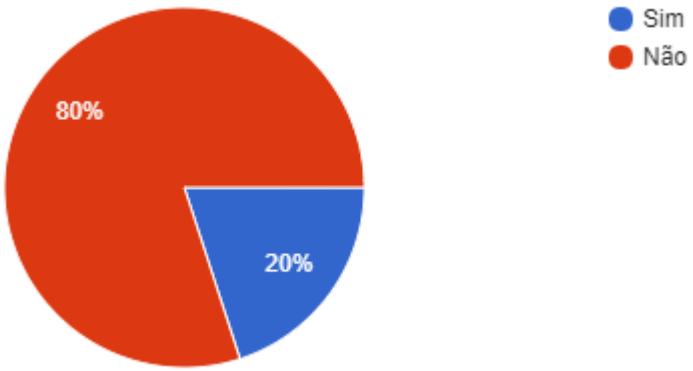
Fonte: Dos próprios autores

Os testes realizados foram feitos online e por análise da estrutura física da empresa antes da implantação e através dos questionários obtivemos os seguintes resultados:

Quando questionados a respeito da segurança da rede, 77,8% dos entrevistados não acham que seus dados estão seguros e 22% tem opinião contrária, segundo mostra o gráfico 01.

Você acha a rede de computadores da empresa segura?

Gráfico 01: Segurança

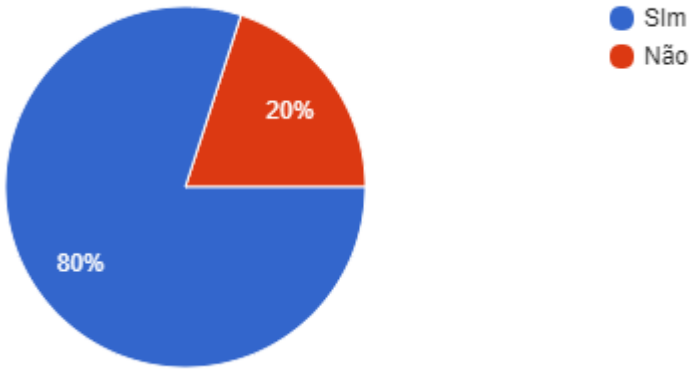


Fonte: Dos próprios autores

No gráfico 02, 80% confirmam que o mal funcionamento do sistema tem atrapalhado o atendimento ao cliente.

O mal funcionamento do sistema tem interferido no atendimento ao cliente?

Gráfico 02: Atendimento

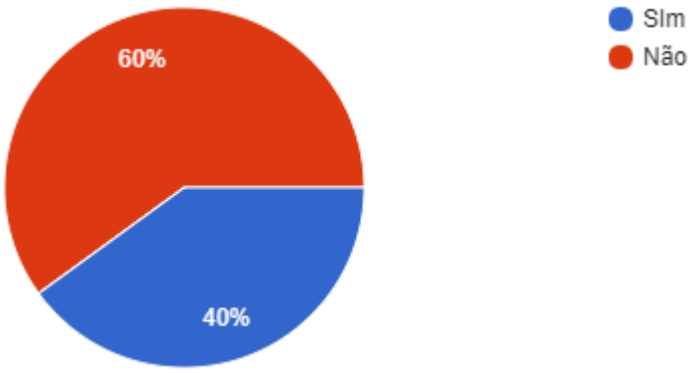


Fonte: Dos próprios autores

No gráfico 03, 40% dos computadores da empresa estão afetados com *malware*. Além das respostas dos funcionários através do formulário, essa informação pode ser validada através de análise técnica.

O seu computador tem alertado suspeitas de vírus?

Gráfico 03: Vírus

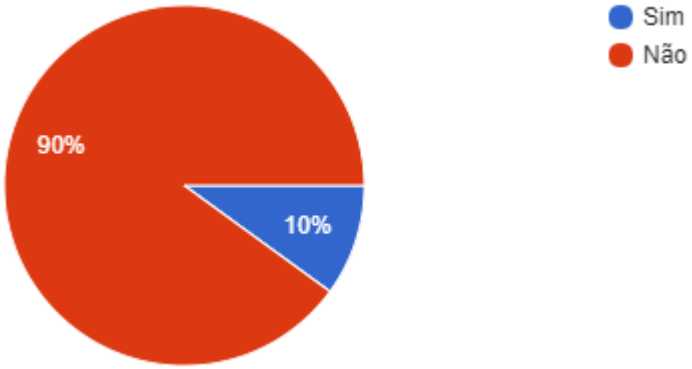


Fonte: Dos próprios autores

No gráfico 04, 90% dos entrevistados não utilizam programas que podem comprometer a segurança da empresa.

Você utiliza programas para fazer download (Torrent) em seu computador?

Gráfico 04: Programas



Fonte: Dos próprios autores

CONSIDERAÇÕES FINAIS

O interesse por esse estudo surgiu mediante a curiosidade de identificar o impacto que um bom gerenciamento de redes computacionais dentro de uma empresa pode acarretar para a melhoraria da segurança de informação, aumento de produtividade e atendimento aos clientes da empresa. As soluções comercias em servidores estão a cada dia mais robustas para atenderem as necessidades das empresas, cada uma com sua peculiaridade, fica explícito como os desenvolvedores têm se empenhado em desenvolver e aprimorar as tecnologias relacionadas a redes computacionais.

Embora existam muitos *softwares* gratuitos desenvolvidos com a finalidade de prover serviços em rede, muitas organizações optam em utilizar *softwares* pagos, isso ocorre devido a facilidade do manuseio e suporte técnico da empresa que fornece o *software*. Os *softwares* Livres apesar de não possuir custo na adesão, exige mão de obra preparada, podendo sair mais caro do que algumas ferramentas pagas, mesmo assim, são soluções que valem o investimento, mesmo exigindo mão de obra especializada. Podendo sair cara para a organização, as ferramentas *Open Source* se mostram em sua maioria superior nos quesitos segurança e flexibilidade, quando comparadas com ferramentas pagas.

O estudo pertinente em *software* livre traz grandes ganhos acadêmico, para os desenvolvedores da pesquisa, quanto para o leitor, uma vez que as ferramentas modernas em redes de computadores, como o *Cloud Computing* (Computação em Nuvem), vêm sendo desenvolvidas principalmente por ferramentas *Open Source*.

Estudar o que as ferramentas livres oferecem abre um leque de possibilidades despertando o interesse do acadêmico em ir a fundo nos seus estudos e consequentemente, ele poderá ser levado rumo a uma carreira de sucesso.

A tecnologia tem sido responsável por movimentar boa parte da economia mundial, talvez, sem os recursos que ela oferece a economia não teria alcançado um desenvolvimento tão rápido como tem acontecido nos últimos anos. As ferramentas de software livre têm colaborado diretamente no desenvolvimento do setor público e privado, por não possuir custos de licença e possuir ferramentas para atender vários tipos de demandas. O aprimoramento dessas ferramentas poderia contribuir diretamente na melhoria da qualidade de vida das pessoas.

A aplicabilidade desses conhecimentos no mercado de trabalho é de muita valia, pelo o fator Custo e Benefício, pequenos e médios empresários em sua maioria têm uma estreita visão relacionado a tecnologia de informação, muitos limitam suas empresas em alguns computadores conectados à *Internet*, protegidos por um antivírus. E desconhecem ou ignoram termos como *Firewall, Squid*, DNS, entre outros. Levar estas ferramentas até o cliente e convencê-lo de forma sucinta de que é viável utilizá-las em sua organização, pode render bons frutos para o cliente e para profissionais da área.

O presente estudo foi desenvolvido a partir da estrutura de redes de uma empresa do ramo hídrico que não possui estrutura de servidores adequada para o tamanho da sua estrutura física. A geografia atual da rede de computadores da empresa é composta por vários computadores e dispositivos sem fios e não possui um computador servidor, fazendo com que a produção da empresa seja prejudicada e poderia acarretar em uma sobrecarga nas transferências de informações e ocasionar travamentos. Através das análises feitas da organização, foi desenvolvido em ambiente virtualizado, soluções que resolveria os problemas da empresa, simulações de uma nova estrutura computacional com servidores executando serviços de rede para a empresa.

Foram diversas as dificuldades encontradas no desenvolvimento, desde o levantamento de requisitos até a configuração dos servidores e encontrar soluções viáveis que resolveriam os problemas da organização foi uma das maiores dificuldades, pois, existem diversas ferramentas que executam o mesmo trabalho.

As hipóteses levantadas foram analisadas através dos testes em ambientes virtualizados e para a validação das hipóteses foram feitos além de testes de aplicabilidade das ferramentas, também foi aplicado questionários para os funcionários da empresa de tratamento de água e esgoto de Itambacuri, com perguntas relacionadas ao desempenho das tecnologias atuais da empresa.

H0 - **A segurança e velocidade de navegação poderiam ser melhoradas fazendo o uso da internet através do Squid;** A segurança pode ser melhorada, pois o *Squid* faz comunicação direta com o *firewall,* inclusive já vem pré-definido com suas próprias diretrizes de segurança e a velocidade de navegação também obteve melhoras significativas após a implementação do servidor *proxy*, pois o mesmo reduz a utilização da conexão e melhora os tempos de resposta fazendo *cache* de requisições frequentes de páginas *web*. Mostrou-se viável nos ambientes virtualizados, pois consome pouco recurso de *hardware*, sendo ideal, uma vez que a empresa não possui *hardware* de alto nível de processamento.

H1 - **A comunicação entre matriz e filial poderia ser feita através de ferramentas VPN;** O OpenVPN permite a criação de túneis virtuais criptografados que permitem a comunicação de matriz e filial de forma segura. OpenVPN foi utilizado com intuito de estabelecer a comunicação entre as filiais e matriz, compartilhando o software e arquivos utilizados pela empresa.

H2 - **A Virtualização de servidores é um recurso que aproveitaria ao máximo os recursos de hardware disponíveis;** Através da virtualização poderia aplicar em um mesmo computador físico, várias máquinas virtualizadas, cada um executando um serviço diferente. A virtualização utilizando o Qemu/KVM permitiu maior aproveitamento do *hardware* podendo facilmente implementar novas funcionalidades. Foi amplamente utilizado não só para realização dos testes, como para validação do trabalho por completo. Nele foram feitos os estudos das ferramentas para este trabalho.

H3 - **Utilizar o módulo Netfilter para aplicar regras de firewall tornando a navegação entre as redes mais segura;** A implantação do *firewall* permite a comunicação entre várias redes locais ou externas de forma segura, passando todas as informações pelo o servidor principal onde será permitido ou negado pacotes enviado e recebidos, essa análise será feita de acordo com as regras aplicadas. O *Netfilter* foi validado junto com *Squid* nos testes realizados. A estrutura atual da empresa se encontra totalmente defasada e apresenta vários problemas de segurança, entre eles a facilidade de acesso aos dados empresa através da rede sem fio. Aplicação do *firewall* foi feita visando corrigir problemas básicos e avançados na segurança da organização e trouxe resultados satisfatórios.

As ferramentas aplicadas e testadas em ambientes virtualizadas podem trazer melhorias significativas para a organização e também seria a porta de entrada para

novas tecnologias, um dos maiores ganhos para a empresa seria o fato de poder estabelecer a comunicação entre a matriz e a filial que situa a alguns quilômetros da matriz, com isso poderia ser feito o compartilhamento de dados, telefone e diversos outros recursos através da comunicação por VPN. A utilização de recursos virtualizados aproveitaria melhor o hardware disponível na empresa, além disso, possui grande parte dos dados pessoais como cpf, rg, endereço de grande parte da população de um município e faz necessário a implementação de medidas de segurança. O *firewall* implementado nesta pesquisa atendeu parte das necessidades da organização fazendo viável sua implantação.

Este trabalho se mostrou altamente funcional e adaptativo, ele atendeu perfeitamente a todos os principais problemas enfrentados pela empresa fazendo o uso de softwares livres estudados nos capítulos anteriores.

Segue abaixo uma lista de possíveis estudos e melhorias para desenvolvimento de trabalhos futuros:

- Plano de contingência para possíveis erros como um erro no servidor, que concentra grande parte dos dados da empresa. O uso de armazenamento em nuvem poderia ajudar como também uma rotina de backup diária internamente na empresa.
- O uso de ferramentas de monitoramento e controle de usuários poderia complementar o que foi feito no trabalho, poderia ajudar a empresa a ter um controle maior dos seus equipamentos e relatórios sobre sua produtividade com os seus funcionários e clientes.
- Uma tentativa social na empresa de estímulo a tecnologia poderia evitar que fique desatualizada com as novas demandas do mercado. Uma equipe de Tecnologia da Informação junto com uma cultura de buscar soluções tecnológicas inovadoras.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799:2005: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. Disponível em: < http://www.ciencianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf>. Acesso em 14 jul 2017.

FILHO. João Eriberto. *Descobrindo o Linux,* 3ed. São Paulo: Novatec Editora, 2012. 928p.

GOODRICH, Michael. *Introdução à Segurança de Computadores,* 1ed. Porto Alegre: Bookman Editora, 2012. 568p.

HOROVITS, Henrique Daniel; SILVA, Edilberto Magalhães. *Explorando vulnerabilidades em Redes sem Fio: Usando as principais ferramentas de ataque e configurações de defesa*. Brasília. 2013.

JUNIOR, Vanderlei Freitas et al. *Tecnologia e Redes de Computadores*. Instituto Federal Catarinense – Campus Avançado Sombrio. Sombrio. 2015. 229p. Disponível em: <http://redes.sombrio.ifc.edu.br/wp-content/uploads/sites/7/2015/12/Livro-Tecnologia-e-Redes-de-Computadores-2015.pdf>. Acesso em: 1 maio. 2017.

MASSALINO, Fábio. *Virtualização De Servidores E Suas Principais Ferramentas*. Escola Superior Aberta Do Brasil – Esab Curso De Pós-Graduação Lato Sensu Em Sistemas De Telecomunicações. Vila Velha. 2012. Disponível em: <https://www.esab.edu.br/wp-content/uploads/monografias/fabio-massalino.pdf>. Acesso em: 3 mai 2017.

MATTOS, Diogo Menezes. *Virtualização: VMWare e Xen*. S/E. Grupo de Teleinformática e Automação. S/E. Rio de janeiro. S/D. 13p. Disponível em: <http://files.carvconsultoriainformatica.webnode.com.br/200000034d05b2d1552/artigo.pdf>. Acesso em 19 jul 2017.

MORIMOTO, Carlos Eduardo. *Redes e Servidores Linux*, 2ed. s/l: GDH Press e Sul Editores. 2006. 448p.

PAIM, Rodrigo Rodrigues. *WEP, WPA e EAP*. S/E. S/L. 11p. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/index.html >. Acesso em 12 jul 2017.

REIS, Christian. *Caracterização de um Processo de Software para Projetos de Software Livre*. USP, São Carlos, 2003. Disponivel em:< http://www.teses.usp.br/teses/disponiveis/55/55134/tde-12112014-100100/pt-br.php>. Acesso em 12 jun 2017

RIOS, Renan Osório. *Protocolos e Serviços de Redes*. S/E. Colatina: Instituto Federal Espirito Santo. 2012. 80p. Disponível em: <http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_comun/tec_inf/081112_protserv_redes.pdf>. Acesso em 14 jul 2017.

SILVA, Fábio Rodrigo. *Vantagens e desvantagens na utilização de software de virtualização em servidores de empresas de pequeno e médio porte: estudo de casos em faculdades particulares no Recife*. 2007. 52 f -Recife, 2007. pdf. Disponível em: < https://www.coursehero.com/file/21321930/vantagens-desvantagens-virtualizacao/>. Acesso em 14 jul 2017.

SILVA, Lino Sarlo. *Virtual Private Network*. São Paulo: Novatec. 2002. 240p.

TANENBAUM, Andrew Stuart. *Redes de computadores*, 4ed. Rio de Janeiro: Campus. 2003. 968p.

VERAS, Manoel. *Virtualização: Tecnologia Central do Datacenter.* 2ed. Rio de Janeiro: Brasport. 2016. 224p.