VLADIMIR BRAUER BATISTA

IMPLANTAÇÃO DE UM SERVIDOR LINUX PROXY, DHCP ARQUIVOS E FIREWALL NA EMPRESA ASPROVEL NA CIDADE DE TEÓFILO OTONI – MG

TEÓFILO OTONI - MG

FACULDADES UNIFICADAS DOCTUM DE TEÓFILO OTONI

2015

VLADIMIR BRAUER BATISTA

IMPLANTAÇÃO DE UM SERVIDOR LINUX PROXY, DHCP ARQUIVOS E FIREWALL NA EMPRESA ASPROVEL NA CIDADE DE TEÓFILO OTONI – MG

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: Administração de Redes.
Orientador: Prof. Salim Ziad Pereira Aouar.

TEÓFILO OTONI - MG

FACULDADES UNIFICADAS DOCTUM DE TEÓFILO OTONI

2015

FACULDADES UNIFICADAS DE TEÓFILO OTONI -MG

FOLHA DE APROVAÇÃO

A Monografia intitulada: IMPLANTAÇÃO DE UM SERVIDOR LINUX PROXY, DHCP ARQUIVOS E FIREWALL NA EMPRESA ASPROVEL NA CIDADE DE TEÓFILO OTONI – MG

elaborada pelo aluno VLADIMIR BRAUER BATISTA

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

BACHAREL EM SISTEMAS DE INFORMAÇÃO

Teófilo Otoni, 30 de novembro de 2015

_____
Prof. Orientador Salim Ziad Pereira Aouar

_____
Prof. Examinador 1

_____
Prof. Examinador 2

Dedico esta monografia a Deus, a minha filha (Júlia), minha esposa (Débora), meus pais (Natalino e Marly) e a minha vó (Té).

AGRADECIMENTOS

Agradeço primeiramente à Deus por conceder-me a realização desse sonho. Aos meus pais, Marly e Natalino, pelo apoio, à minha esposa Débora pelo incentivo, apoio e compreensão, à minha filha Júlia por trazer alegria nos momentos difíceis e ao meu irmão Plinio pelo apoio. Aos meus tios Waldemar e Cristalino, pela ajuda e apoio, as minhas tias Eliane e Fatima que sempre acreditaram na realização dessa conquista e a minha avó (Té) por todo o apoio dado. Ao orientador, Prof. Salim Ziad Pereira Aouar, pela orientação, dedicação, comprometimento e seu incentivo para que eu pudesse realizar esta monografia, aos demais mestres do curso de sistemas de informação que ajudaram a alcançar o meu objetivo. Agradeço também aos meus colegas de classe em especial Jefferson Machado, Vinicius Knack e Gabriel Somerlate por me ajudarem sempre que precisei de apoio nas horas mais difíceis nesta trajetória. Também agradeço a Rafael Pungirum pela oportunidade de desenvolver esta pesquisa na Asprovel. Um muito obrigado a todos que participaram desta caminhada!

RESUMO

Esta monografia intitulada “Implementação de um Servidor Linux, Proxy, DHCP, Arquivos e Firewall na empresa Asprovel na cidade de Teófilo Otoni/MG”, concentrada na área de administração de redes, apresenta um estudo sobre a viabilidade de gerenciamento de redes em uma empresa, com ênfase em servidor de rede usando software livre. Com o objetivo de trazer melhorias de controle, segurança e gerenciamento da estrutura de redes da empresa, usando sistema operacional e ferramentas confiáveis com baixo custo financeiro. Para proporcionar esta melhoria foram implementadas ferramentas Iptables para regras de firewall, o isc-dhcp-server como servidor de IP da rede, Samba para controlar acessos a arquivos e pastas e servidor de domínio juntamente com o servidor Proxy Squid que tem também a função de controlar acessos à internet e fazendo armazenamento em cache.

Palavras-Chave: Servidor; GNU/Linux; Firewall; Proxy; DHCP; Samba.

SUMÁRIO

INTRODUÇÃO

A presente monografia foi elaborada e apresentada no 8º período da graduação em Sistemas de Informação, como requisito final para a conclusão do curso. Trata-se de um estudo sobre o tema “Servidores GNU/LINUX”, com o título “Implementação de um Servidor Linux, Proxy, DHCP, Arquivos e Firewall na empresa Asprovel na cidade de Teófilo Otoni/MG”.

Por abordar sobre gerenciamento de rede através de um servidor a área de concentração desta pesquisa é Administração de Redes.

Empresas que possuem objetivos concretos e que visam o crescimento dentro do seu respectivo mercado, o atual cenário exige a necessidade de entender o quanto é importante a segurança das informações e torna também urgente a necessidade de implantar um servidor LINUX num ambiente corporativo.

Em se tratando de rede de computadores, servidor é um computador que tem como objetivo processar e entregar pedidos para os demais computadores na rede local ou externa (Intranet e Internet). Suas configurações são, na maioria das vezes, mais elevadas que as dos demais computadores, dependendo de como será utilizado, já que existem diversos tipos de servidores como: servidor web, servidor de arquivo, servidor de e-mail e tantos mais que trazem diversas opções de funcionalidade e configuração.

No mercado mundial os servidores LINUX vêm crescendo de forma rápida. Por se tratar de um sistema mais eficaz, robusto, confiável e também pelo fato de ser um software livre, onde não gera custos para quem adquire suas distribuições, faz com que ele venha a ganhar mais mercado.

Esta pesquisa teve como foco a implementação de servidores Proxy (Squid), que tem a função de controlar o que seus usuários podem acessar na rede de internet; o DHCP (isc-dhcp-server) para distribuir IP´s e restringir acessos à rede por

computadores não autorizados; o servidor de Arquivos (samba4) para que os usuários possam criar pastas com seus determinados perfis necessários para o armazenamento de arquivos; e o Firewall (iptables), que serve para aumentar a segurança em relação aos acessos externos, bem como controlar o grau de sigilo de suas informações.

A questão levantada, a qual originou a realização desta pesquisa, consiste em responder à seguinte indagação: Qual a viabilidade de implantação do servidor Linux Proxy (Squid), DHCP (isc-dhcp-server), Arquivos (samba4) e Firewall (iptables) na empresa Asprovel na cidade de Teófilo Otoni/MG?

Buscando responder a tal questão foram levantadas e analisadas diversas situações para que se chegasse a uma solução válida ao final do presente trabalho, o que originou as seguintes hipóteses:

H0 - Não seria viável a implantação do sistema servidor Linux Proxy, DHCP, Arquivos e Firewall, pois a empresa não tem interesse em alterar sua rotina e seus processos atualmente existentes;

H1 – Não seria recomendável a implantação do servidor Linux Proxy, DHCP, Arquivos e Firewall, já que a empresa não iria arcar com o custo de um servidor;

H2 - Seria viável a implantação do servidor Linux Proxy, DHCP, Arquivos e Firewall, pois a empresa iria trabalhar com software livre, sem gastos com suas respectivas licenças;

H3 - Seria viável a implementação do servidor, já que com ele aumentaria a segurança, o controle e confiabilidade sobre dados e informações existentes na empresa.

A presente pesquisa foi dividida em 4 capítulos descritos da seguinte forma: o primeiro capitulo, intitulado “Revisão Literária”, aborda as informações sobre redes de computadores, softwares livres, sistemas operacionais, servidores de rede e as demais ferramentas utilizadas para a elaboração da pesquisa; o segundo capítulo trata sobre o desenvolvimento do trabalho, abordando as pesquisas, os materiais e métodos utilizados, a instalação e configuração do servidor e seus serviços, bem como a instalação, configuração dos clientes e testes realizados; já no terceiro capítulo é relatado os resultados e discursões sobre a pesquisa; e por último, no quarto capítulo, faz-se a conclusão da presente pesquisa.

1 REVISÃO LITERÁRIA

1.1 REDES DE COMPUTADORES

Redes de computadores são um conjunto de computadores autônomos, interconectados, capazes de compartilhar recursos. A estrutura básica de uma rede é formada por linhas de comunicação e nós, que tem a função de interconectar as estações à rede e roteadores quadros (conjunto de bits). Em uma rede local como a Ethernet, um dos nós é a placa de rede, responsável pela conexão da estação de trabalho (workstation) ao cabo de rede pelo envio dos quadros da estação de trabalho pelo cabo. As duas topologias principais de redes são redes canais ponto a ponto e redes canais multiponto (FERREIRA, 2003, p.350).

> LAN (Local Área Network) - Conjunto de computadores dentro de uma determinada área, dentro de uma sala, edifício ou edifícios vizinhos.
>
> MAN (Metropolitan Area Natwoark) – Conjunto de computadores interligados dentro da uma cidade.
>
> WAN (Wide Area Network) – Conjunto de computadores interligados dentro de uma região geográfica.[1]

[1] FERREIRA, RUBENS, 2003, p.350

Serviços e protocolos são conceitos diferentes, embora sejam confundidos com frequência. O serviço é um conjunto de primitivas (operações) que uma camada oferece a uma camada acima dela. O serviço define as operações que a camada está preparada para executar em nome de seus usuários, mas não informa absolutamente nada sobre como essas operações são implementadas. Um serviço se relaciona a uma interface entre duas camadas, sendo a camada inferior o fornecedor do serviço e a camada superior o usuário do serviço.

Já o protocolo é um conjunto de regras que controla o formato e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares contidas em uma camada. As entidades utilizam protocolos com a finalidade de implementar definições de serviço. Elas têm liberdade de trocar seus protocolos, desde que não alterem o serviço visível para os seus usuários. Portanto, o serviço e o protocolo são independentes um do outro. (TANENBAUM, WOODHULL, 2003, p.39).

Segundo Ferreira (2003, p.358), com o objetivo de padronizar a conectividade para interligação de sistemas de computadores locais ou remotos, a ISO (International Standardizion Organization) em 1977 criou o modelo OSI (Open System Interconnection). Para melhor compreensão de questões fundamentais sobre a rede, conforme mostra a Figura 1, o Modelo OSI é composto por sete camadas, com regras que orientam a conversação entre as camadas, essas regras são chamadas de protocolo da camada. Assim a arquitetura de rede é formada por camadas, interfaces e protocolos. Cada camada oferece um conjunto de serviços à camada superior, usando funções realizadas na própria camada e serviços disponíveis nas camadas inferiores.

Figura 1: CAMDAS DE REDE

Fonte: http://ftp.feb.unesp.br/autodesk/pos/Disciplina-1-redes.pdf

A camada física é a responsável pela transmissão de bits bruto, através de um canal de comunicação. Esta camada trabalha na maior parte com interfaces mecânicas, elétricas e de sincronização, e com o meio físico de transmissão que está abaixo da camada física.

A camada de enlace tem como função transformar um canal de transmissão bruto em uma linha livre de erros de transmissão não detectável para a camada de rede, para isso esta camada faz com que o transmissor faça a divisão dos dados de entrada em quadros de dados e os envie em quadros sequenciados, que ao chegar até o receptor retorna um quadro de dados confirmando a recepção correta. Outra questão que a camada de enlace também trabalha, é a correção de como impedir que um transmissor rápido envie quantidade excessiva de dados a um receptor lento (TANENBAUM, 2003, p.42).

A camada de rede faz o controle de movimentação de uma máquina para outra; esta camada provê o serviço de entrega do segmento à camada de transporte na máquina de destino (KUROSE, ROSS, 2006, p.37).

A camada de transporte é a camada que liga a origem ao destino e sua função básica é aceitar dados da camada acima dela, dividi-los em unidades menores se for necessário, repassar essas unidades à camada de rede e assegurar que todos os fragmentos cheguem corretamente ao seu destino (TANENBAUM, 2003, p.43).

A camada de sessão permite que usuários de sistemas consigam estabelecer sessões entre si; também é responsável pelo controle de diálogo, controlando quem deve transmitir a cada momento, controle de token, que impede que duas partes executem a mesma operação crítica ao mesmo tempo, e a sincronização que realiza verificações periódicas de transmissões longas para permitir que continuem do ponto onde estavam quando ocorreu uma falha.

A camada de apresentação está relacionada à sintaxe e à semântica das informações transmitidas, esta camada também gerência as estruturas de dados abstratas e permite a definição e o intercâmbio de estrutura de dados de nível mais alto (TANENBAUM, 2003, p.44).

A camada de aplicação é onde residem aplicações de rede e seus protocolos. Esta camada inclui vários protocolos como o HTTP, que faz requisição e transferência

de documentos pela Web, o SMTP para correio eletrônico e o FTP, que faz transferências entre dois sistemas finais. (KUROSE, ROSS, 2006, p.37).

1.2 SOFTWARES LIVRES

Usar o *software* livre é fazer uma escolha política e ética, onde se afirma o direito de aprender e compartilhar o que se aprende com os outros. *Software* livre tornou-se a base de uma sociedade de aprendizagem, compartilhando o conhecimento para que outros possam desfrutar e aprimorar.

Nos dias atuais muitas pessoas usam *software* proprietário, que negam aos seus usuários a liberdade e os benefícios que se pode desfrutar de um *software* livre. As empresas por trás de *software* proprietário, muitas vezes, espionam suas atividades e os restringem de compartilhar com outros. O Movimento do *software* livre trouxe a ideia de reunir um grupo mundial de programadores éticos, talentosos e comprometidos com o pensamento de escrever e compartilhar *software* uns com os outros; e qualquer um pode fazer parte e beneficiar desta comunidade mesmo sem ser um especialista em computadores ou ter conhecimento sobre programação. O movimento do software livre iniciou em 1983 pelo cientista da computação Richard M. Stallman, quando ele lançou um projeto chamado GNU, substituindo o sistema operacional *UNIX*.[2]

Executar o programa como você desejar para qualquer propósito, poder estudar seu funcionamento, adaptá-lo de acordo com suas necessidades, poder redistribuir cópias e redistribuir cópias modificadas ajudando ao próximo são requisitos essenciais para um programa ser um *software* livre.[3]

[2] <https://www.fsf.org/about/what-is-free-software>
[3] <http://www.gnu.org/philosophy/free-sw.pt-br.html>

1.3 SISTEMAS OPERACIONAIS

Um sistema operacional é um programa que gerência o hardware do computador. Ele também oferece uma base para aplicativos e atua como um intermediário entre o usuário e o hardware do computador. Para a realização de diferentes aspectos, os sistemas variam de acordo com sua necessidade. Como por exemplo, para computadores de grande porte ele busca melhorar e otimizar a utilização de hardware, já para computadores pessoais ele aceita jogos complexos, aplicações comerciais e tudo que se encontra entre eles e para computadores portáteis são projetados para facilitar a comunicação entre o usuário e seus aplicativos.[4]

Segundo Norton (1996, p. 238), um sistema operacional é um programa muito complexo e importante para o computador, por fazer o equipamento reconhecer a CPU, memória, teclado, vídeo, unidades de disco e os demais periféricos, além de ser uma plataforma para a execução de aplicativos.

O sistema operacional funciona da mesma maneira que um software comum de computador, porém sua diferença está na intenção do programa: o sistema operacional direciona o processador para o uso dos recursos do sistema e na sincronização e execução dos outros programas (STALLINGS, 2010, p.212).

> Hardware – É o computador em si, onde o kernel é executado.
>
> Kernel - É o núcleo do sistema operacional, a parte mais próxima do hardware. Composta de chamadas ao sistema, de acesso aos Dispositivos de entrada e saída e de gerenciamento dos recursos da máquina.
>
> Shell - é o nome genérico de uma classe de programas que funciona como interpretador de comandos de linguagem de programação script no Unix.[5]

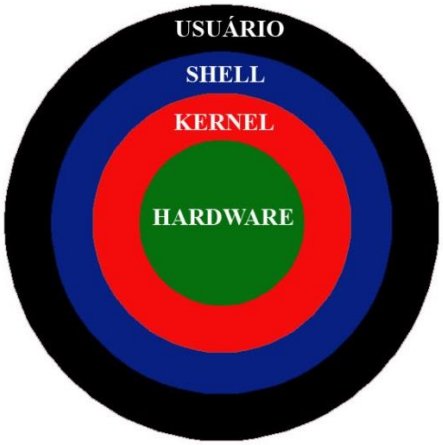
As camadas de um Sistema Operacional são distribuídas conforme mostra a Figura 2.

---

[4] SILBERSCHATZ, GAGNE, GALVIN, 2004, p.3

[5] FERREIRA, RUBENS, 2003, p.29

Figura 2: Camadas do Sistema Operacional



Fonte: http://www.hardware.com.br/comunidade/artigo-shell/929574/

1.4 GNU/LINUX

Como uma alternativa barata para aqueles que não estão dispostos a pagar um preço elevado por uma licença UNIX, o LINUX foi criado para suprir tais necessidades por um clone do UNIX (FERREIRA, 2003, p.24).

O desenvolvimento do GNU/LINUX teve início em 1984, pela *Free Software Foundation* quando começou a desenvolver um sistema operacional livre com base no UNIX que foi chamado de GNU. O projeto GNU passou a desenvolver então um conjunto de ferramentas e sistemas operacionais, como por exemplo o Linux. A referida Fundação continua sendo a maior contribuinte do projeto e que ainda conta com grupos ao redor do mundo.[6]

Geralmente os usuários do GNU/Linux não sabem que o Linux é o núcleo (kernel) do sistema operacional e não entendem que o sistema é basicamente o GNU com o Linux funcionando como Núcleo.[7]

---

[6] <https://www.debian.org/releases/wheezy/mips/ch01s02.html.pt>
[7] <http://www.gnu.org/gnu/linux-and-gnu.html>

Em 5 de outubro de 1991 era lançada a primeira versão oficial do Linux por um ex-aluno da Universidade de Helsinque, localizada na Finlândia, chamado Linus Benedict Torvalds. Tal lançamento somente foi possível depois de muito trabalho e da contribuição de terceiros que se interessaram pelo projeto após uma mensagem de desafio enviada por ele a uma lista de discussão onde Linus reconhecia não ser capaz de conseguir desenvolver sozinho o Linux (FERREIRA, 2003, p.25).

1.5 SERVIDORES DE REDE GNU/LINUX

Segundo Morimoto (2008, p.3) ao estudar a história do Linux e do Unix, se percebe que os dois foram originalmente desenvolvidos para uso em servidores e só mais tarde passou a ser usado em desktops.

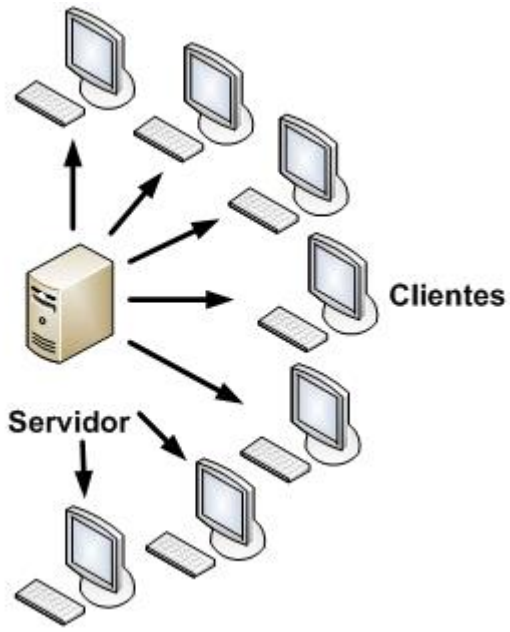
Os servidores têm funções diversas e estas máquinas servidores estão sempre ligadas exercendo suas tarefas, que podem ser de acordo com as necessidades de quem utilizam suas funcionalidades. Encontramos diversos tipos de servidores, como servidores de web, servidores de arquivos, servidores de serviços, servidores de impressão dentre vários outros tipos, e uma só máquina pode rodar vários serviços de servidores simultaneamente, como demostra a Figura 3 abaixo uma rede Cliente/Servidor.

A maior parte das distribuições Linux podem ser usadas como servidor, que se dividem em dois grupos, que são os de rede local, utilizadas para compartilhar arquivos, conexões, autenticação de usuários e também serem usados como firewall; já o outro grupo são os servidores de internet, que são hospedeiros de aplicações e web na grande rede.

As distribuições Linux mais usadas como servidor são o Debian, CentOS, Fedora, Ubuntu, SuSE e Mandriva, sendo que a maior parte dos seus serviços que são utilizados como Apache, Bind, MySQL e outros são os mesmos, diferenciando na

maior parte somente pela sua instalação, mas também cada um vem com uma série de ferramentas de configurações diferentes.

Figura 3: Cliente/Servidor



Fonte: http://www.gta.ufrj.br/ensino/eel879/trabalhos_v1_2009_2/kikuchi/introducao.html

1.5.1 FIREWALL (IPTABLES)

Segundo Hunt (2004, p.385) para ter uma boa administração de sistema é essencial ter uma boa segurança, e esta é fundamental para se reduzir e se recuperar de ataques que são comuns, por isso é importante trabalhar nas vulnerabilidades de ameaças de segurança de um servidor.

O firewall é o responsável por trazer a segurança à rede local, protegendo da rede global, onde passa todo o tráfego de entrada e saída de rede, filtrando e protegendo do tráfego não desejado. O Linux tem essas ferramentas de filtragem, que controla todos os acessos dentro do próprio servidor.

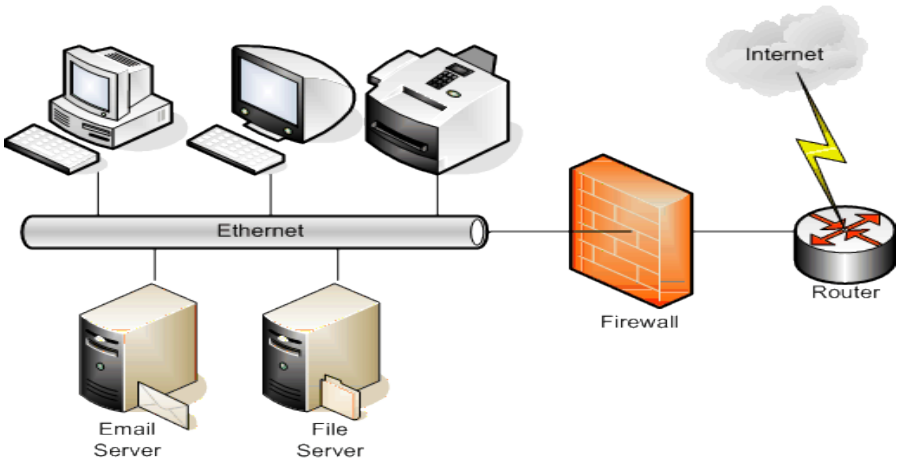
O IPTABLES é um programa de linha de comando que é utilizado para fazer filtragem de pacotes trafegados na rede através de um conjunto de regras.[8]

> A *Iptables* é uma aplicação que permite ao administrador do sistema configurar tabelas *Netfilter*, cadeias e regras. O *Netfilter* é um modulo que fornece ao sistema operativo Linux as funções de firewall, NAT e registo de utilização da rede. A *Iptables* funciona com base nas regras estabelecidas pelo administrador. Todos os pacotes que chegam ao sistema entram no *kernel* para serem analisados.[9]

Suas principais características incluem a filtragem de pacotes *Stateless* e *Stateful* IPv4 e IPv6, infraestrutura flexível e extensível e múltiplas camadas API. Com o *Iptables* podemos fazer a filtragem de pacotes na internet, implementar clusters de *firewall stateful e stateless*, fazer manipulação de pacotes, usar NAT para implementar proxies transparentes.[10]

A Figura 4, demostra que tudo é filtrado antes da entrada e saída pacotes na rede.

Figura 4: Firewall



Fonte: http://firewall.web.tr/

[8] <http://repositorio-aberto.up.pt/bitstream/10216/59107/2/Texto%20integral.pdf
[9] <http://www.netfilter.org/projects/iptables/>
[10] <http://www.netfilter.org/>

1.5.2 DHCP (isc-dhcp-server)

Para que cada sistema ligado em rede seja corretamente identificado, é necessário que o mesmo tenha um endereço IP único. Esse endereço pode ser atribuído manualmente a cada posto ou de uma forma automática e dinâmica, graças ao protocolo *DHCP* (*Dynamic Host Configuration Protocol* ou Protocolo dinâmico de configuração de postos).[11]

O IP é o protocolo de internet que transmite dados em forma de datagramas entre os computadores, e para que esses dados sejam enviados via rede o IP divide os dados em pacotes; já o TCP/IP são um conjunto de protocolos de comunicação que fazem diferentes tipos de computadores “conversarem” uns com os outros. O TCP, que vem do inglês Protocolo de Controle de Transmissão (*Transmission Control Protocol*), assegura que os datagramas de uma mensagem seja remontados ou reenviados aos que estão faltando de forma correta em seu destino final.[12]

O endereço IP é um número binário de 32 bits no caso do IPV4, que atribuído a interfaces de rede em computadores, diferencia um computador dos demais na rede. (FERREIRA, 2003, p.364)

Todos os dispositivos IP precisam de endereço, e o ISC-DHCP é o meio mais eficiente e rápido de fornecê-los. O ISC DHCP é um software *open source* que implementa o DHCP (*Dynamic Host Configuration Protocol*), para conectar a uma rede IP. É um software que oferece uma solução completa para implementação de um servidor DHCP para clientes de redes pequenas e redes para grandes empresas, O ISC DHCP suporta tanto IPv4 quanto IPv6, sendo adequado para aplicações grandes e de alta confiabilidade.[13]

[11] <http://servidordebian.org/pt/jessie/intranet/dhcp/start>
[12] FERREIRA, RUBENS, 2003, P.361
[13] <https://www.isc.org/downloads/dhcp/>

1.5.3 DNS (BIND)

Segundo Tanenbaum (1997, p. 617), Domain Name System (Sistema de Nomes e Domínios), tem a função de mapear um nome em um endereço IP, funcionando como um tradutor de endereços IP para nomes de domínios. Como a rede reconhece entre si só endereços numéricos, foi desenvolvido este mecanismo para converter os strings ASCII em endereços de rede. Sua essência é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuídos para implementar o esquema de nomenclaturas.

Os Sistemas Linux usam duas técnicas para converter nomes de hosts em endereços: a tabela de hosts e o Domain Name System (DNS). Na tabela hosts é um arquivo de texto simples que é pesquisado sequencialmente para combinar nomes de hosts para endereços IP; já o DNS, é um sistema de banco de dados hierárquico e distribuído com milhares de servidores através da Internet, que controlam consultas de nome e de endereço. Cada um desempenha seu papel, porém o DNS é o mais importante. (HUNT, 2004, p.91).

O DNS no Linux é implementado com o software Berkeley Internet Name Domain (BIND). No BIND o DNS é um sistema cliente/servidor. O Cliente é chamado de resolvedor, e que forma as consultas e as envia ao servidor de nome. (HUNT, 2004, p.94).

O BIND é um software de código aberto mais utilizado na Internet, proporcionando uma plataforma robusta e estável com sistemas totalmente compatíveis com os padrões DNS. O BIND teve originou na Universidade da Califórnia em Berkeley.[14]

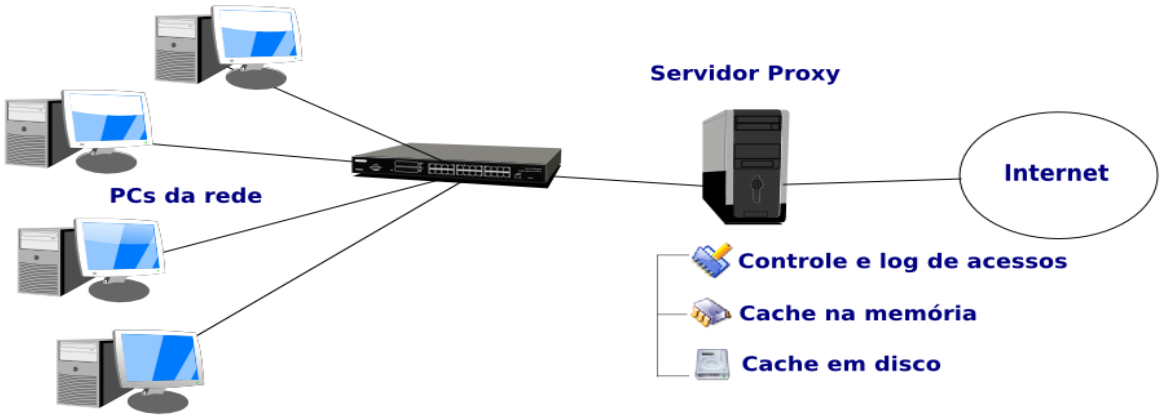
[14] <https://www.isc.org/downloads/bind/> pesquisado 21-09-15

1.5.4 Proxy (Squid)

O Squid é um servidor proxy-cache com opções de otimização de tráfego com armazenamento em cache, oferecendo também um ambiente poderoso de controle de acesso, gerenciamento e modelagem de tráfego, que foi desenvolvido no início de 1990. Seu projeto foi feito pela NSF que fazia uma pesquisa sobre tecnologia de armazenamento em cache. Cada vez mais, as empresas buscam o uso do Squid para melhorar seu desempenho visando uma navegação mais rápida.

Um servidor Squid guarda com armazenamento em cache de conteúdo, ajuda a melhorar a largura de banda salvando o conteúdo localmente, assim economizando o tráfego na banda e fazendo downloads mais velozes. Mesmo sem armazenamento em cache, o Squid melhora a velocidade otimizando o fluxo TCP, facilita a distribuição de conteúdo como streaming de mídia para os servidores economizando grandes gastos com modernização de equipamentos e com ampliação de largura da banda conforme mostra a figura 5.[15]

Figura 5: SERVIDOR PROXY



Fonte: http//:www.hardware.com.br/livrosservidores-linuxconfigurando-servidor-proxy-com-squid.html

[15] <http://www.squid-cache.org/Intro/why.html>

1.5.5 Arquivos (Samba)

Segundo Ferreira (2003, p.596) o Samba é um programa que tem como função principal o compartilhamento de arquivos e impressoras para o Windows. A equipe que desenvolveu o Samba tinha o objetivo de apresentar todas as funcionalidades de um servidor *Windows* ou uma estação de trabalho *Microsoft*.

Desde seu lançamento em 1992 o Samba vem se popularizando mais, por conta da flexibilidade em configurações facilitando a administração de redes, e liberdade por trabalhar em diversas plataformas diferentes como, *Windows*, *Linux, Unix, OpenVMS* e outros sistemas operacionais. Ele é um *Open Sourse*, que tem no seu projeto o objetivo de eliminar os obstáculos entre diferentes plataformas.[16]

Tudo começou quando *Andrew Tridgell* precisou montar um espaço em disco no seu PC que rodava o sistema operacional DOS para um servidor *UNIX*, que resolveria com a utilização de um sistema de arquivos NFS, mas ele também precisava de suporte ao protocolo *NetBios* que não é suportado pelo NFS; para solucionar o problema *Andrew* desenvolveu um programa para captura de tráfego de dados na rede. Para analisar o tráfego de dados gerado pelo protocolo *NetBios* ele usou a engenharia reversa no protocolo SMB e implementou no *UNIX*, permitindo assim montar sistemas de arquivos compartilhados do servidor *UNIX*.[17]

1.6 SISTEMA OPERACIONAL DEBIAN 7

O sistema operacional Debian é distribuição de software livre que utiliza o Kernel Linux, lançada em 4 de maio de 2013 a sua versão 7 com o Kernel 3.2, de codinome Wheezy baseado no projeto GNU.

---

[16] <https://www.samba.org/samba/what_is_samba.html>
[17] <https://www.samba.org/samba/docs/SambaIntro.html>

O desenvolvimento do Debian é proveniente de uma base de milhares de voluntários em todo o mundo, que colaboram com dedicação e compromisso para fornecer um melhor sistema operacional. Esta versão inclui recursos de suporte à multiarquitetura e várias ferramentas[18].

[18] https://www.debian.org/News/2013/20130504

2 PESQUISA

2.1 MATERIAIS E MÉTODOS UTILIZADOS

Para a implementação do servidor, o sistema operacional foi utilizado a distribuição Debian com a versão 7 e com o Kernel 3.2.

O Hardware utilizado para implementação do sistema operacional foi um micro computador desktop com um processado Core 2 Duo, 4GB de memória, um hd de 2 Terabytes com uma placa de rede 10/100/1000 onboard e uma placa de rede 10/100/1000 offboard.

2.2 INSTALAÇÃO E CONFIGURAÇÃO DO SERVIDOR E SERVIÇOS.

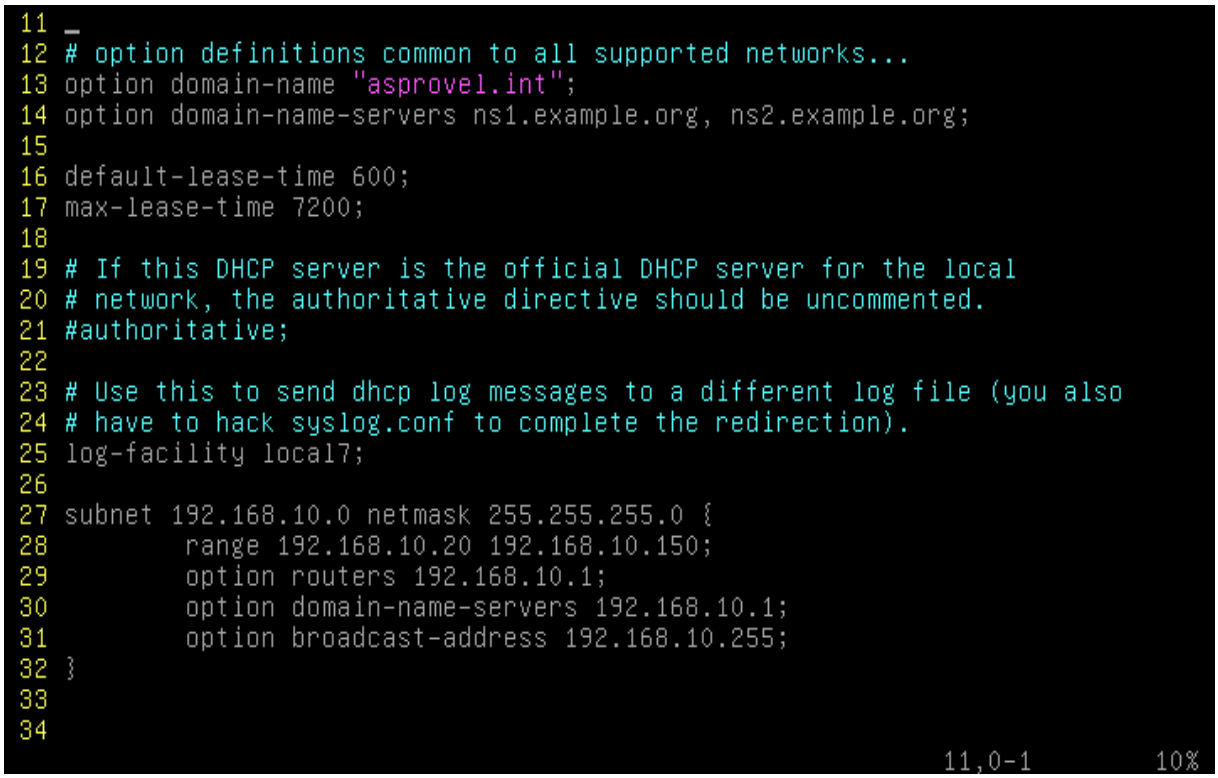
2.2.1 Servidor DHCP

A ferramenta utilizada para implementar o servidor DHCP foi ISC-DHCP-SERVER 4.2.2, e para a instalação e configuração foram feitos os seguintes comandos:

#apt-get update – Para realizar atualização dos repositórios. #apt-get install isc-dhcp-server – Para a instalação da ferramenta.

Após a instalação, foram feitas alterações no arquivo dhcpd.conf que é o arquivo de configuração do servidor dhcp, que se encontra no diretório /etc/dhcp/, como está demonstrado na Figura 6.

FIGURA 6: dhcpd.conf



Fonte: Do próprio pesquisador.

- Linha 13: Nome do domínio.
- Linha 27: Define a faixa de endereço ip e a máscara de rede.
- Linha 28: Define o range de ip´s a serem distribuídos na rede.
- Linha 29: Indica gateway da rede.
- Linha 30: O servidor DNS.
- Linha 31: O endereço de broadcast da rede.

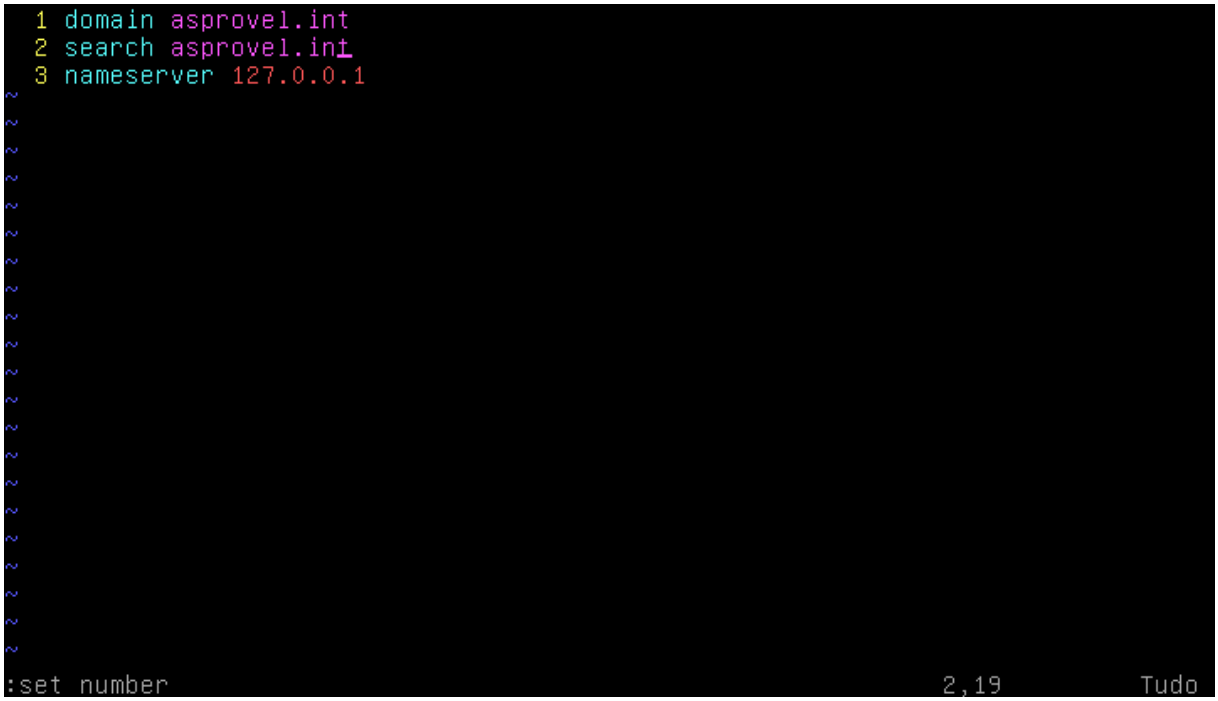
2.2.2 Servidor DNS

Para o servidor DNS foi instalada a ferramenta BIND na versão 9, os seguintes comandos foram utilizados para que fosse feita a instalação e configuração da mesma:

```
#apt-get update – Atualizar a lista de repositórios.
#apt-get install bind9 – Para instalar o pacote BIND.
```

Também foram feitas alterações no arquivo /etc/resolv.conf que é o arquivo responsável por informar qual é o servidor de nomes que irá responder na rede, como está na figura abaixo.

Figura 7: resolv.conf



- Fonte: Do próprio pesquisador.

- Linha 1: O servidor irá responder o domínio asprovel.int.
- Linha 2: A pesquisa será também respondida pelo servidor interno.
- Linha 3: Indica que o servidor DNS é a máquina local.

Outras configurações também foram efetuadas no arquivo de opções globais de configuração do BIND que é o arquivo /etc/bind/named.conf.options, para aumentar a segurança do servidor, demonstrado na figura 8.

Figura 8: named.conf.optins

```
13          // forwarders {
14          //      0.0.0.0;
15          // };
16
17          //========================================================================
    ======
18          // If BIND logs error messages about the root key being expired,
19          // you will need to update your keys.  See https://www.isc.org/bind-
    keys
20          //========================================================================
    ======
21          dnssec-validation auto;
22
23          auth-nxdomain no;    # conform to RFC1035
24          listen-on-v6 { none; };
25          listen-on { localhost; 192.168.10.1; };
26          allow-transfer { none; };
27          allow-query { localhost; 192.168.10.0/24; };
28          allow-recursion { localhost; 192.168.10.0/24; };
29          version none;
30
31
32 };
33 _
                                                              33,0-1        Fim
```

Fonte: Do próprio pesquisador.

- Linha 24: Alterado para não responder o protocolo IPV6.
- Linha 25: Possibilita a qual rede IPV4 responderá.
- Linha 26: Não aceita transferência de resposta que não seja da rede local.
- Linha 27: Permite a consulta da rede local.
- Linha 28: Permite consulta recursiva na rede local.
- Linha 29: Não permite consultar a versão do BIND.

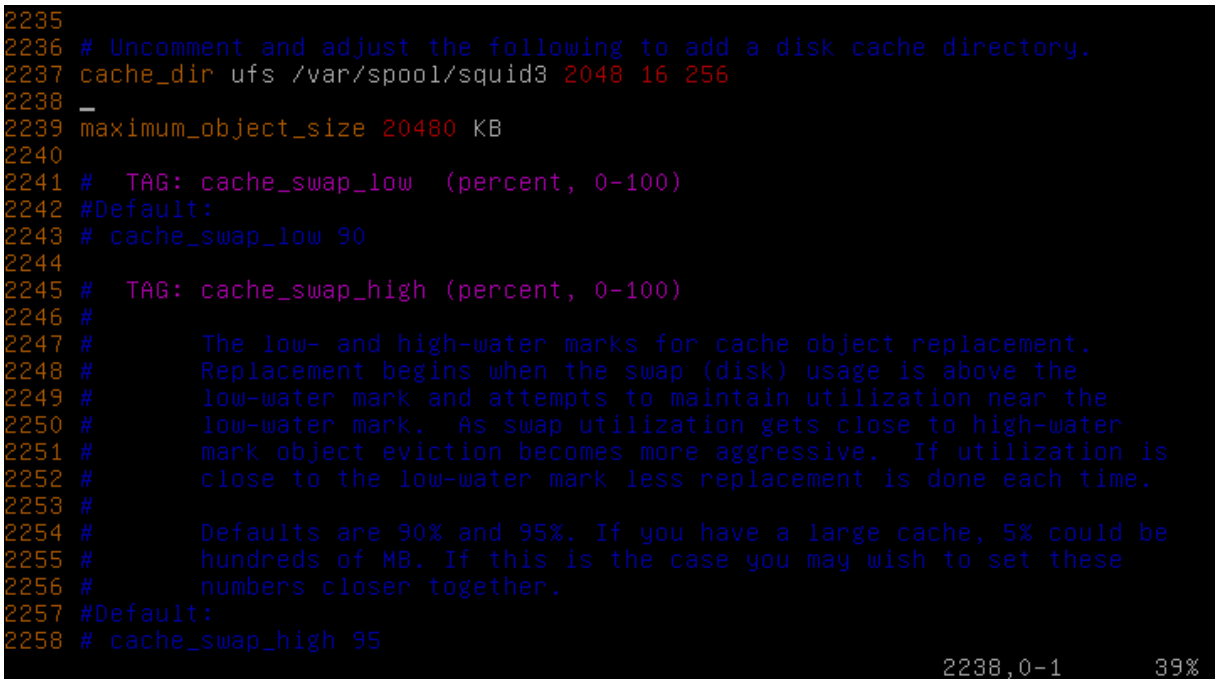
2.2.3 Squid

A ferramenta Squid foi utilizada a versão 3.0, para ser o servidor proxy da rede, fazendo armazenamento de cache, e controle de acesso à internet. Para a instalação foram efetuados os seguintes comandos:

#apt-get update – para que fosse atualizados os repositórios.
#apt-get install squid3 – para a instalação do Squid.

Após a instalação da ferramenta, mudanças no arquivo de configuração do Squid foram feitas para adequar seu funcionamento de acordo com as necessidades de armazenamento em cache, este arquivo se encontra no diretório /etc/squid/squid.conf, conforme a próxima figura.

Figura 9: squid.conf

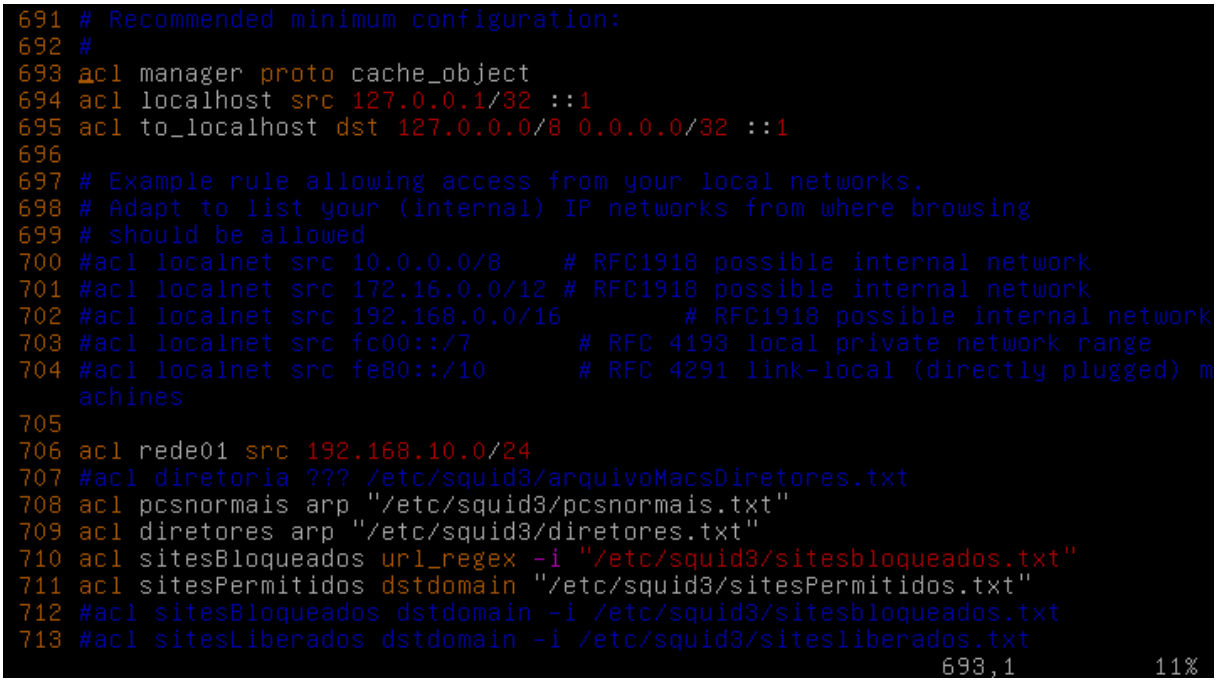


- Fonte: Do próprio pesquisador.

- Linha 2237: Define o diretório de cache com o sistema de arquivos ufs padrão, o tamanho do cache, o número de diretórios e também o número de subdiretórios.
- Linha 2239: Define o tamanho máximo do arquivo que será armazenado no cache.

Outras configurações também foram feitas para configurar o Squid por meio também do arquivo /etc/squid/squid.conf, demonstrado nas figuras 10 e 11.

Figura 10: squid.conf



Fonte: Do próprio pesquisador.

- Linha 706: Indica que aquela determinada faixa de ip pertence a “rede01”.
- Linha 708: ACL criada onde o caminho determinado indica o arquivo que contém os endereços MAC´s dos computadores que pertencem aos colaboradores da empresa.
- Linha 709: ACL criada onde o caminho determinado indica o arquivo que contém os endereços MAC´s dos computadores que pertencem aos diretores da empresa.

- Linha 710 e 711: ACL´s criadas para determinar o caminho onde estão os arquivos que contenham os endereços dos sites bloqueados e os liberados.

Figura 11: squid.conf

```
843 #
844 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
845 #
846
847 # Example rule allowing access from your local networks.
848 # Adapt localnet in the ACL section to list your (internal) IP networks
849 # from where browsing should be allowed
850 #http_access allow localnet
851 http_access allow localhost
852 #http_access allow rede01 !sitesBloqueados
853 http_access allow sitesPermitidos
854 http_access allow diretores
855 http_access deny pcsnormais
856
857 #Autenticacao integrada com a base do SaMBa
858 #auth_param basic program /usr/lib/squid3/smb_auth -W asprovel.int -U 192.1
    68.10.1
859 #auth_param basic children 5
860 #auth_param basic realm asprovel.int
861 #auth_param basic credentialsttl 2 hour
862
863
864 #acl autenticacao proxy_auth REQUIRED
865 #http_access allow autenticacao
                                                    859,1         14%
```

Fonte: Do próprio pesquisador.

- Linha 851: Permite a navegação do computador local.
- Linhas 853, 854 e 855: Define as perdições determinadas nas ACL´s criadas.

Após a configuração do squid.conf, foram criados os arquivos contendo as informações de cada regra necessária para o gerenciamento da navegação da internet, dentro da pasta /etc/squid3/, para isso foram usados os seguinte comandos:

```
#vim /etc/squid3/arquivoMacsdiretores.txt
#vim /etc/squid3/pcsnormais.txt
#vim /etc/squid3/sitesbloqueados.txt
#vim /etc/squid3/sitespermitidos.txt
```

Onde no arquivo Macsdiretores.txt foram inseridos os endereços MAC´s dos computadores dos diretores, no pcsnormais.txt o MAC dos computadores dos demais

colaboradores, no stesbloqueados.txt todos os sites bloqueados cadastrados, no sitespermitidos.txt o cadastro do sites permitidos ao uso pelos colaboradores. Desta maneira o servidor ficou configurado para dar acesso total aos diretores e acesso restrito aos demais usuários da rede.

2.2.4 Samba

A ferramenta Samba foi instalada na versão 4, para fazer o compartilhamento de arquivo na rede e também trabalhando como controlador de domínio de rede, para sua instalação foram usados os comandos abaixo:

```
#apt-get update – para atualização dos repositórios.
#apt-get install samba4-common-bin.
```

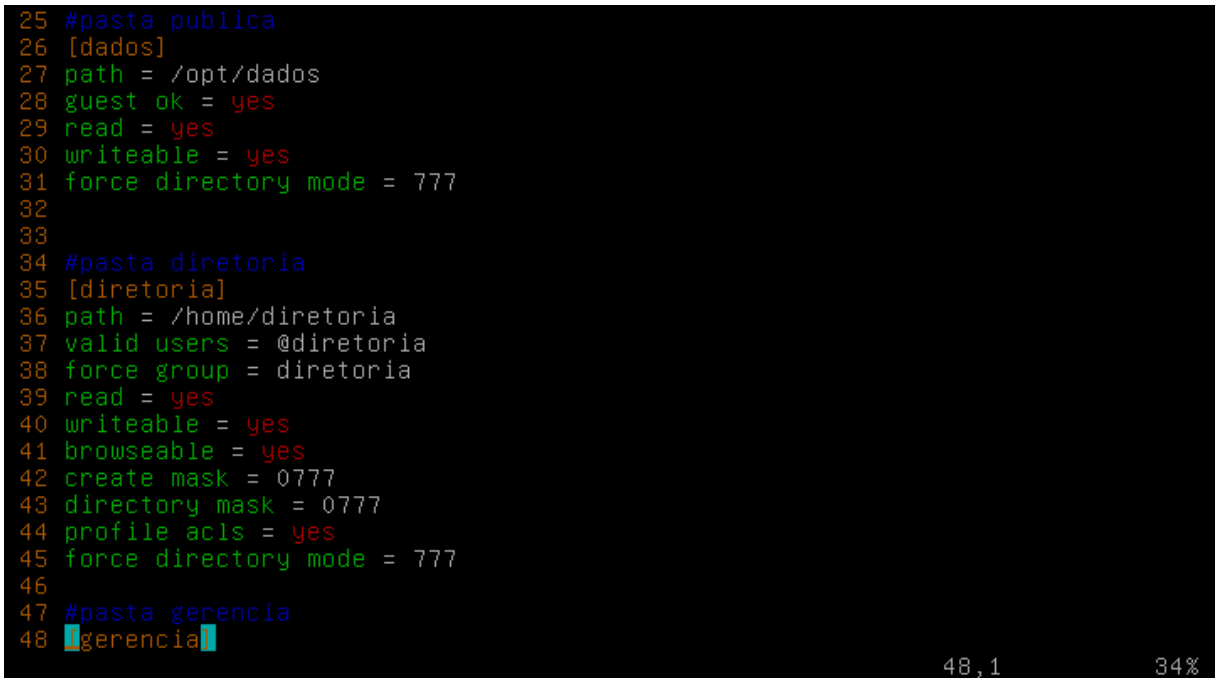
Assim que instalada esta ferramenta foram feitas alterações em seu arquivo de configuração que está localizado na pasta /etc/samba/samba.conf, como demonstra a figuras 12, 13 e 14:

Figura 12: smb.conf

Fonte: Do próprio pesquisador.

- Linha 2: Indica o nome do domínio.
- Linha 3: Nome do servidor.
- Linha 4: Descrição do nome do servidor.
- Linha 6: Adiciona as estações de trabalho automático, no ingresso do domínio da rede.
- Linha 11: Arquivo de script.
- Linhas 12 e 13: Onde são criados os arquivos de perfil.
- Linhas 19 a 23: Configurações do netlogon.

Figura 13: smb.conf



- Fonte: Do próprio pesquisador.

- Linhas 26 até 31: Definições da pasta pública dados.
- Linhas 35 à 45: Definições da pasta da diretoria.

Figura 14: smb.conf

Fonte: Do próprio pesquisador.

- Linhas 49 à 58: Configurações da pasta gerência.
- Linhas 61 até 67: Definições da pasta home dos usuários.

Após feitas as configurações no arquivo de configuração do samba, foram criados os grupos, os usuários, configuradas as permissões de usuários da rede e os usuários foram adicionados nos respectivos grupos. Também foram criadas as pastas compartilhadas na rede e inseridas as permissões de acesso em cada uma deles, para isso os seguintes comandos foram utilizados:

#groupadd nome do grupo – Cria o grupo com o nome desejado.
#adduser nome do usuário – Cria o usuário.
#smbpasswd -a nome do usuário – Para criar senha para o usuário.
#useradd -g nome do grupo -s /bin/bash -d /home/nome do usuário -c “Descrição do usuário” -m nome do usuário. – Esta opção insere o usuário no seu determinado grupo já criado e também insere uma descrição sobre o usuário.
#mkdir /home/nome da pasta – Para criar pasta.

Foram configuradas também as quotas de disco por usuário, definindo assim o espaço utilizado por cada um dos usuários de maneira que não poderão ultrapassar o tamanho máximo de espaço configurado, facilitando o gerenciamento de espaço em disco.

Para dar mais segurança, foram criadas pastas compartilhadas na rede com permissões por grupo de usuários, onde uma pasta com o nome “dados” foi criada para uso de todos os usuários da rede, independente do grupo à qual é pertencente, uma pasta “gerencia” com permissão restrita aos grupos gerentes e diretores e uma pasta “diretores” que somente os usuários vinculados ao grupo diretores tem acesso. Para estas configurações foram usados os seguintes comandos:

```
#mkdir gerencia
#chown root:”nome do grupo” “nome da pasta”
#chmod 0777 “nome da pasta”
#gpasswd –a “nome do diretor” “nome da pasta”
```

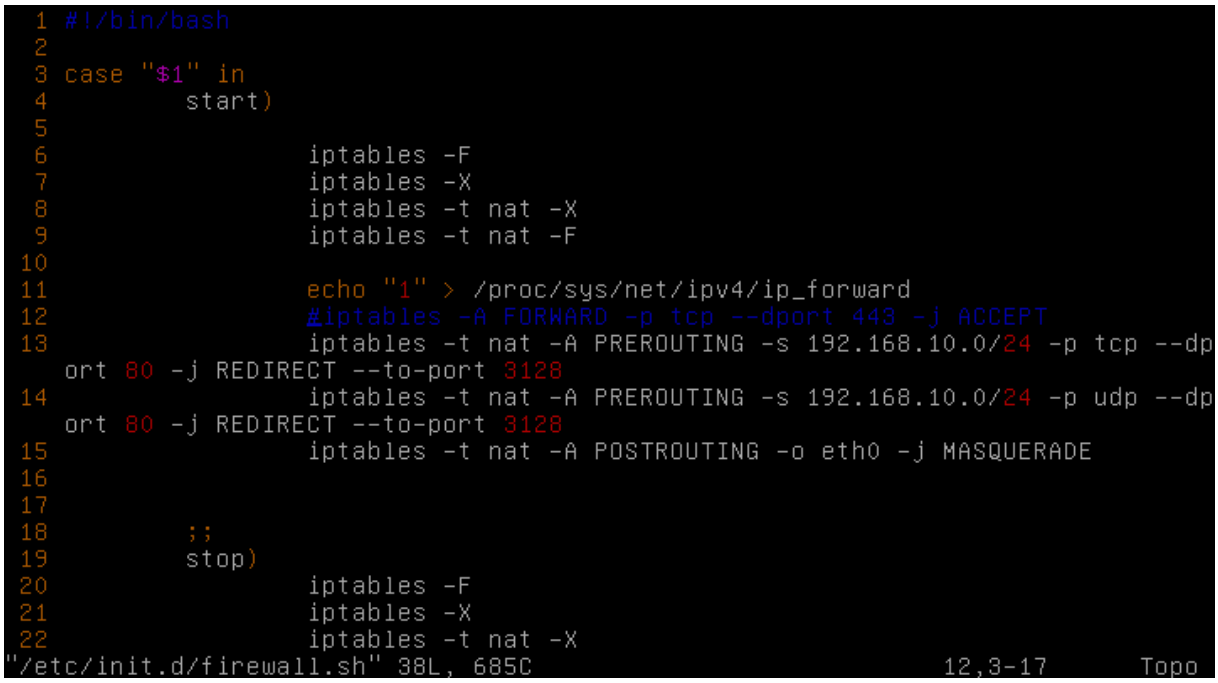
Na pasta /etc/netlogon/ os arquivos diretoria.bat, gerencia.bat que definem as pastas montadas na rede para estes grupos, que são acionadas no arquivo netlogon.bat que também define a pasta de uso geral montada na rede assim que seja feito o logon na rede.

2.2.5 Firewall

Como dito no capítulo anterior 2.1, este servidor contem 2 placas de rede para que possa realizar as funções destinadas. A eth0, que é a placa onboard é a responsável por receber a internet, já a eth1 placa offboard é a placa que tem como função responder a rede local. O Iptables é um módulo que já é instalado no momento da instalação do sistema operacional Debian, portanto para seu funcionamento é necessário a criação de um script onde estará todas a regras de firewall necessárias. O arquivo criado para esta tarefa é o arquivo “firewall.sh” que foi criado pelo comando “#vim /etc/init.d/firewall.sh” e para rodar automaticamente sempre que o servidor seja iniciado foi utilizado o comando “update-rc.d firewall.sh defaults”.

As configurações do arquivo “firewall.sh” foram definidos conforme mostra a Figura 15:

Figura 15: firewall.sh



Fonte: Do próprio pesquisador.

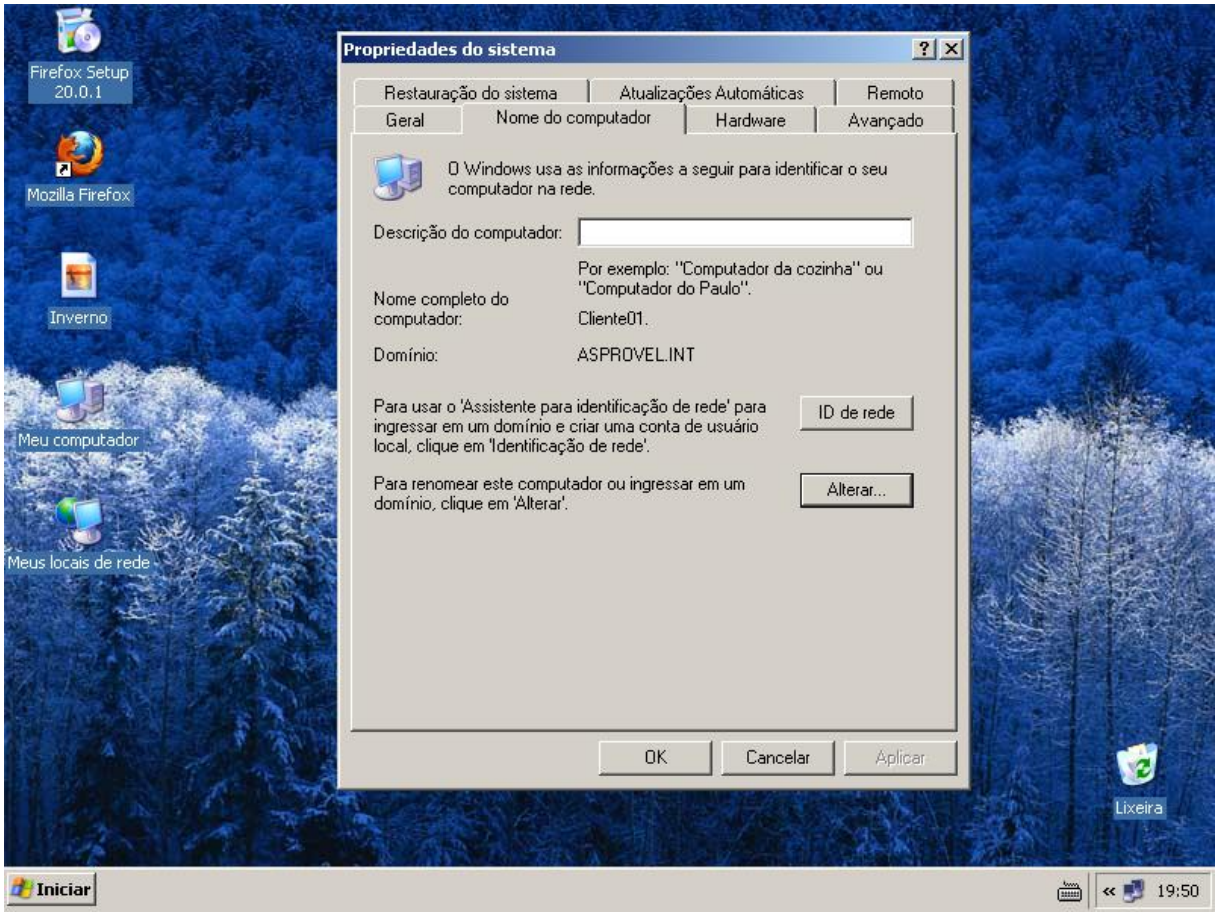
- Linhas de 6 a 9: Limpa qualquer regra aplicada anteriormente.
- Linha 11: Ativa o encaminhamento de pacotes.
- Linhas 13 e 14: Redireciona a porta TCP 80 para o Squid.
- Linha 15: Mascara tudo que sair da eth0.
- Linhas 19 a 22: Para o serviço do firewall e limpa todas as regras.

2.3 - INSTALAÇÃO E CONFIGURAÇÃO DOS CLIENTES

Na empresa os computadores clientes da rede, utilizam sistemas operacionais Microsoft Windows. Para a configuração destes computadores foram inseridos no domínio “asprovel.int”.

Para fazer esta configuração, foi acessado “Propriedades do Sistema”, “Nome do Computador” e “Alterar”. Como na Figura 16:

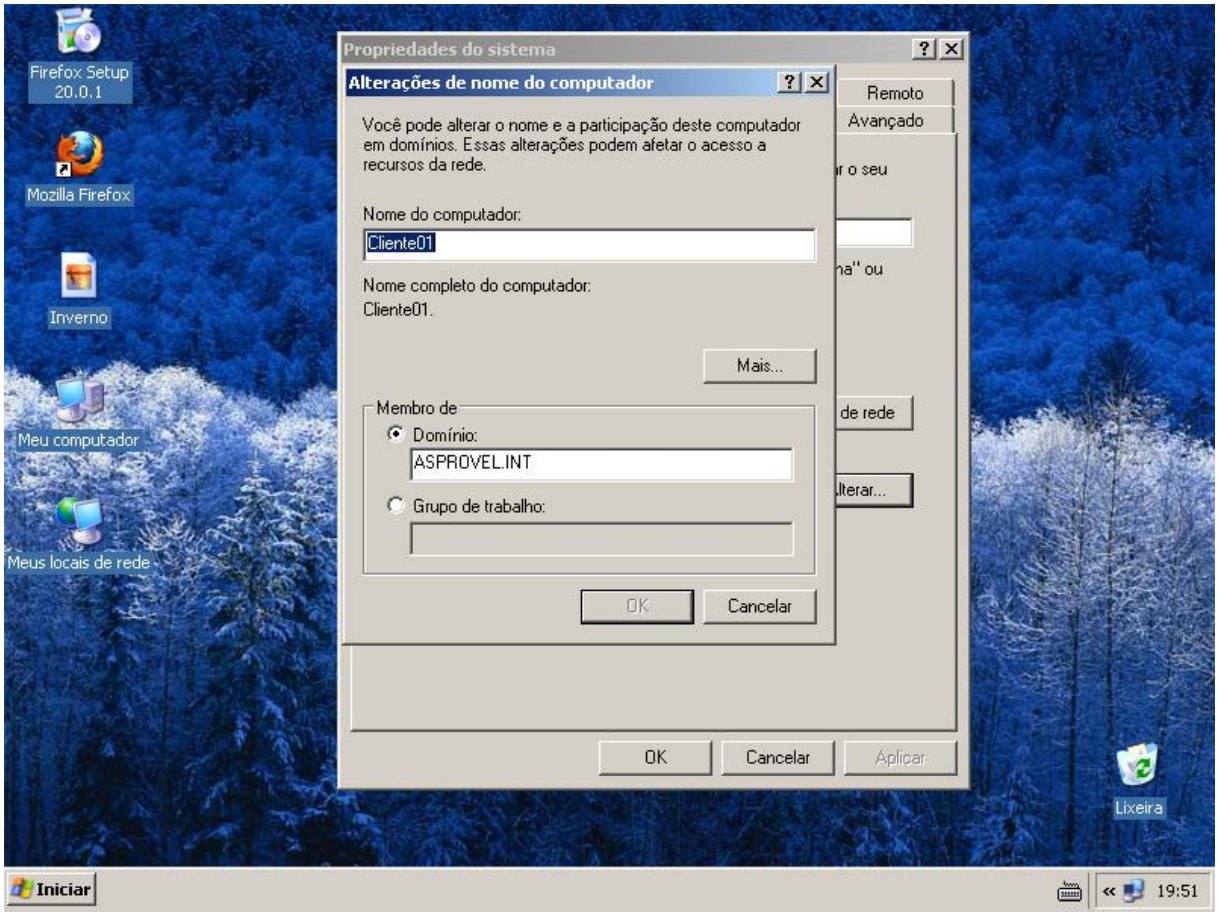
Figura 16: Configuração Cliente 1



Fonte: Do próprio pesquisador.

No próximo passo foi definido o nome do computador e o seu novo domínio de rede, também demonstrado na Figura 17.

Figura 17: Configuração Cliente 1.



Fonte: Do próprio pesquisador.

Desta maneira simples e rápida os computadores cliente foram instalados e configurados, exigindo somente a reinicialização do sistema após a fazer parte do domínio configurado.

2.4 TESTES REALIZADOS

Foram efetuados testes num ambiente montado dentro da empresa, para que não houvesse nenhum transtorno para o funcionamento nem problemas durante o decorrer do período de trabalho dos colaboradores da empresa.

Na primeira etapa, os testes foram das funcionalidades do servidor DHCP, onde todas a maquinas receberam ip´s de forma automática, o que teve resultado satisfatório. Também foram realizados os testes de autenticação de usuários na rede pelo servidor Samba, o que obteve sucesso em todos os usuários cadastrados.

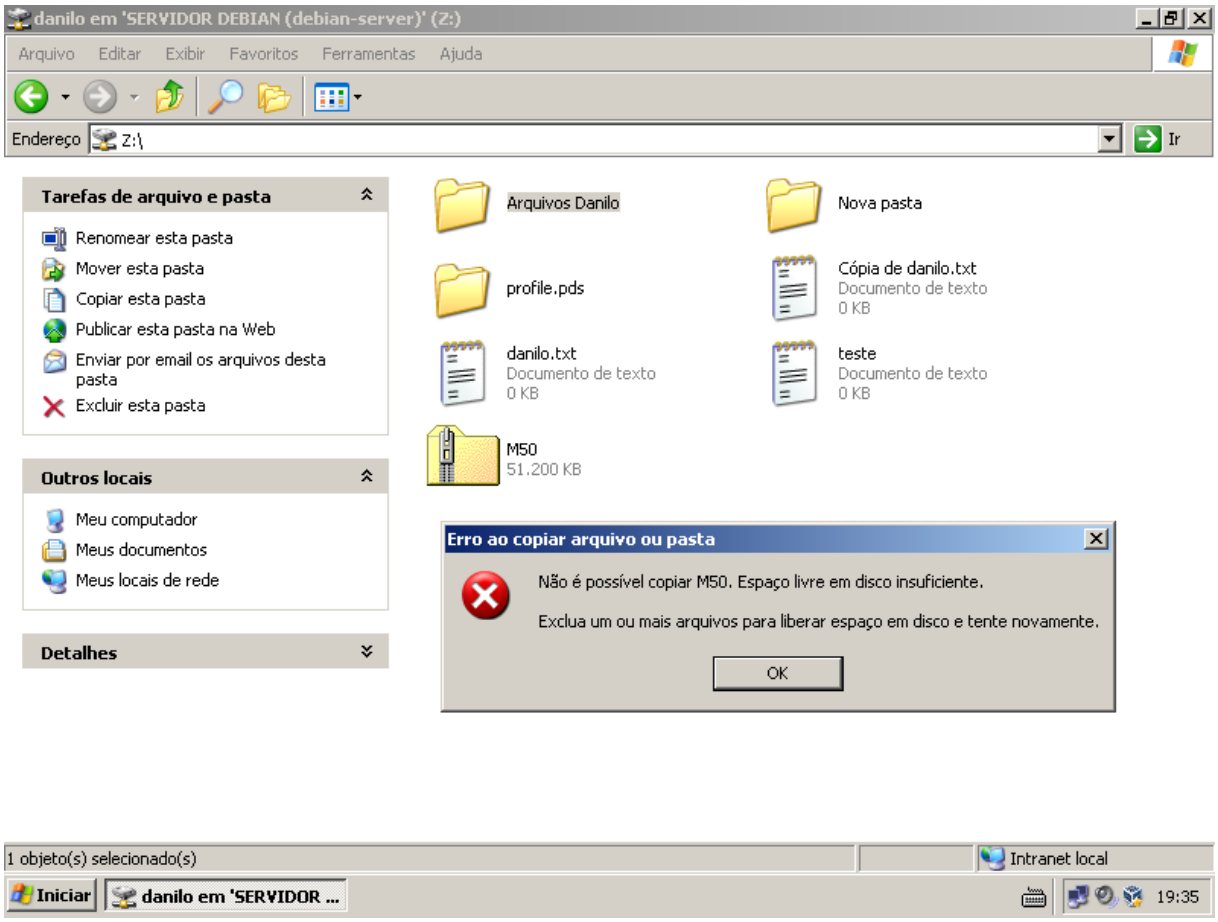
Para uma segunda etapa foram realizados os testes de compartilhamento de arquivos com suas respectivas políticas de restrição, também realizou-se teste para cada usuário, para acesso a arquivos compartilhados no servidor e acessos à internet por meio de seus navegadores a sites, de acordo com o privilégio de cada grupo de usuários cadastrados nos servidores Samba e Squid, também com resultado bem sucedido.

Numa outra parte foi feito testes com relação ao servidor BIND, verificando a melhoria com relação a velocidade no serviço de domínio de nomes, e com relação ao servidor Squid no armazenamento em cache. Nestes testes foi possível verificar a melhoria do serviço de internet, onde obteve uma performance satisfatória.

Por último e também muito importante, realizou-se testes no Firewall, com softwares que utilizam portas diferentes das cadastras.

A Figura 18 demonstra um teste para cópia de arquivo que ultrapassa o tamanho máximo da quota que foi configurada para um determinado usuário.

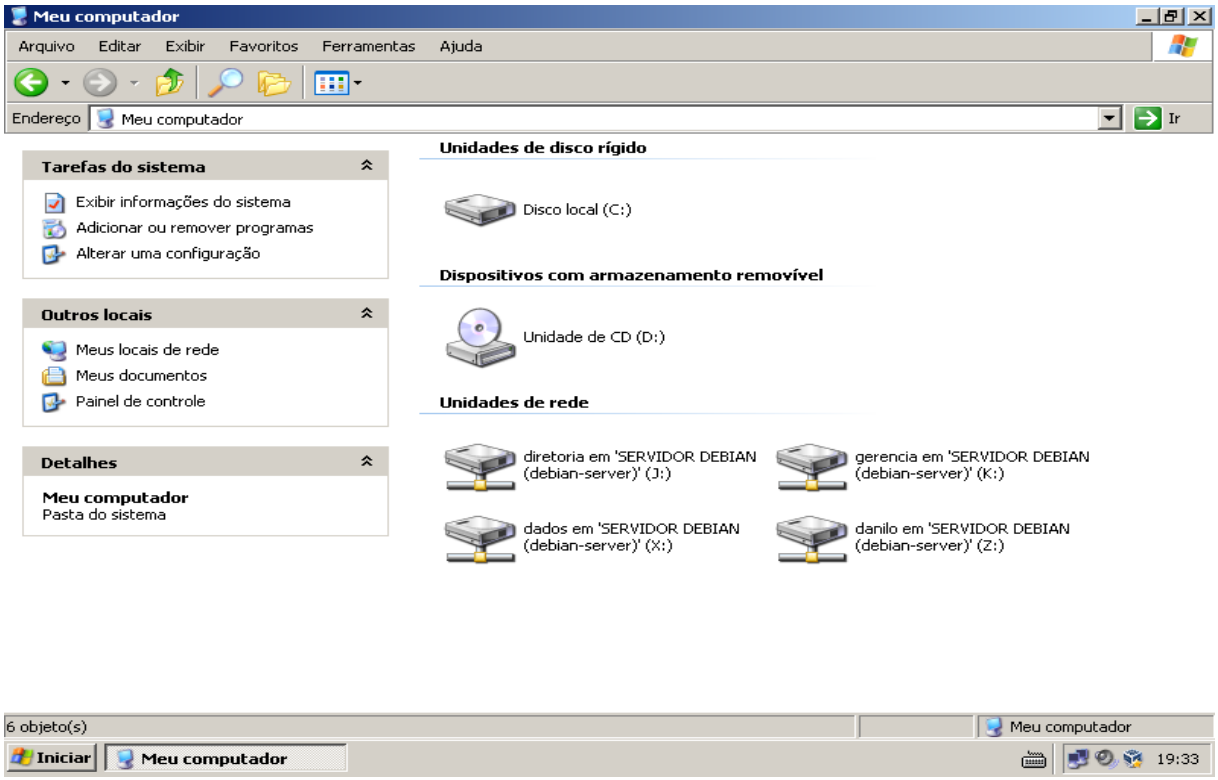
Figura 18: Quotas



Fonte: Do próprio pesquisador.

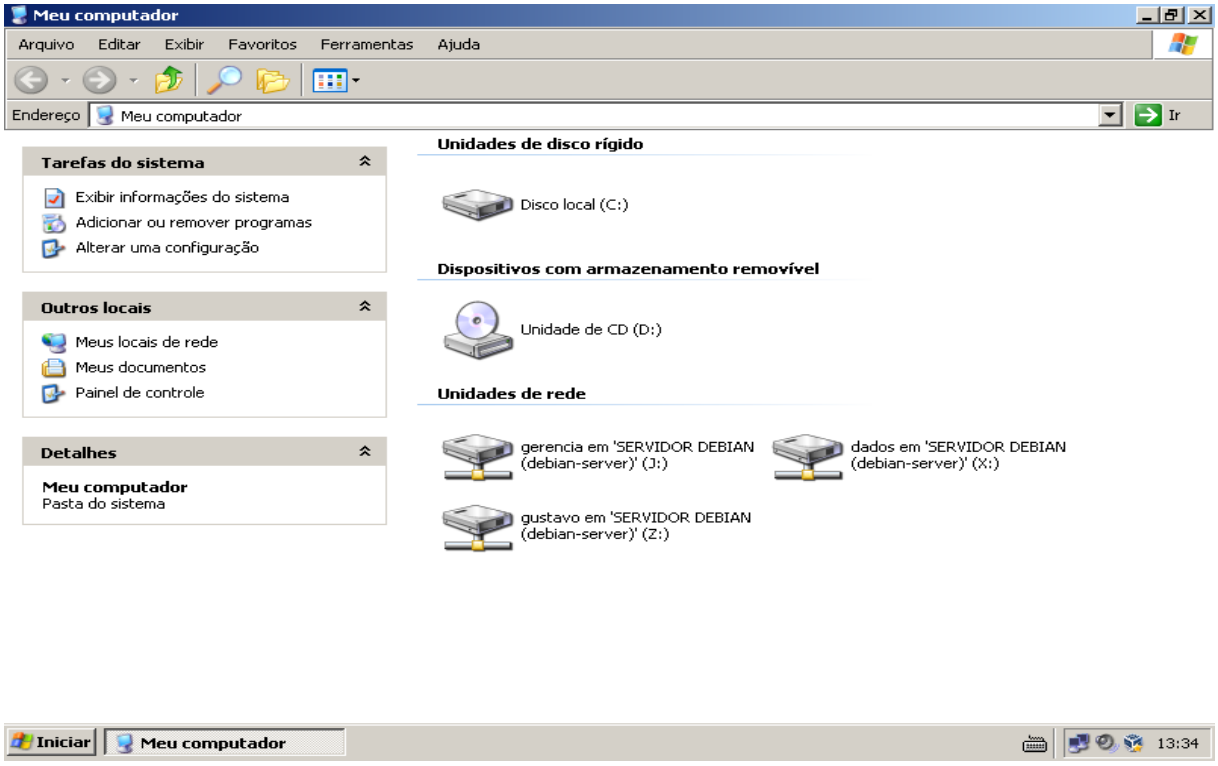
Para os testes realizados à respeito das pastas de usuários que são mapeadas na rede sempre que executam o logon, temos as Figuras 19, 20 e 21 mostrando na Figura 19 as pastas montadas do usuário do grupo diretor, que por sua vez tem acesso as pastas da gerência da diretoria e também a pasta de uso geral, já na Figura 20 temos as 3 pastas que podem ser acessadas pela gerência e na Figura 21 temos o exemplo de um usuário que faz parte de um grupo comum, que só tem acesso a sua pasta pessoal e a pasta de uso geral da rede.

Figura 19: Usuário do grupo diretor.



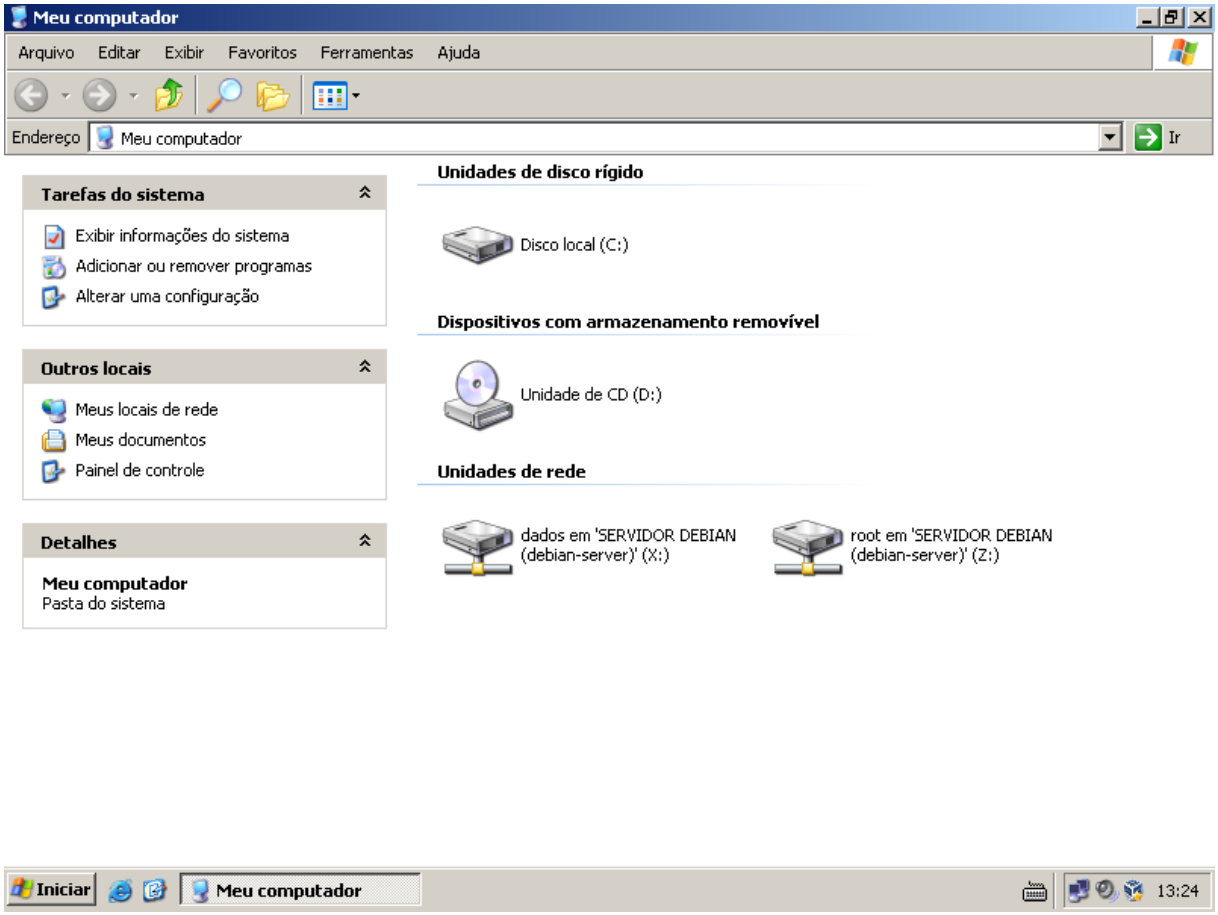
Fonte: Do próprio pesquisador.

Figura 20: Usuário do grupo gerência.



Fonte: Do próprio pesquisador.

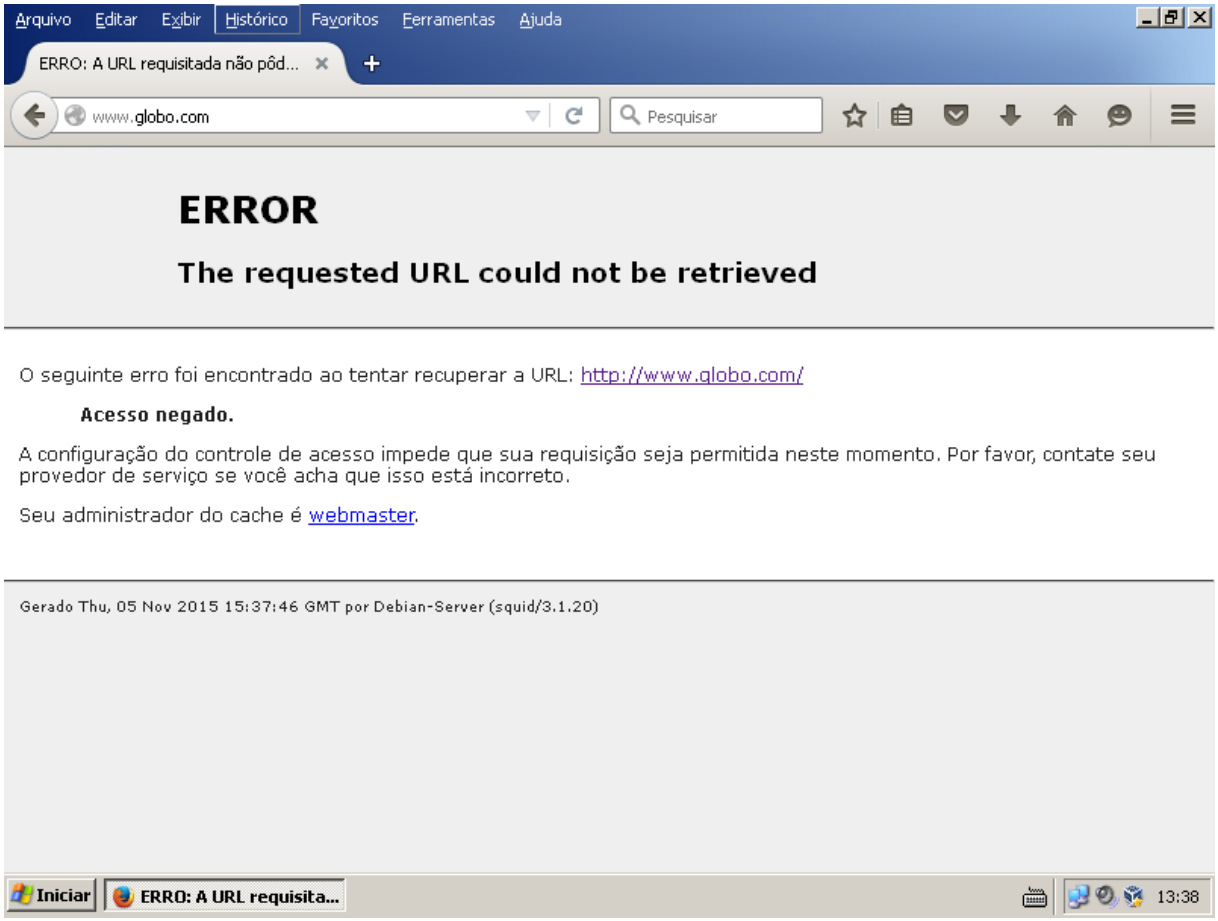
Figura 21: Usuário do grupo comum.



Fonte: Do próprio pesquisador.

Testes com relação ao acesso de sites bloqueados também foram feitos e demonstrado como na Figuras 22, onde teve a tentativo de acessar o site globo.com que estava na lista de sites bloqueados:

Figura 22: Site bloqueado.



Fonte: Do próprio pesquisador.

3 RESULTADOS E DISCUSSÕES

Por meio dos testes realizados no ambiente laboratorial, pode ser concluído que os resultados pretendidos para a melhoria do funcionamento no controle, segurança e confiabilidade em relação ao encontrado antes da implementação do servidor e suas ferramentas, foram alcançados.

Com a utilização destas novas ferramentas, foi possível fazer restrições em pastas e arquivos, de maneira que apenas usuários cadastros e autorizados pudessem acessar os dados respectivos a sua política de restrição. Também para o acesso a site da internet foram adotadas medidas de restrição melhorando a qualidade na utilização da internet.

Outro ponto importante, é a melhoria na segurança com as regras de firewall, que passou a filtrar todos os pacotes enviados na rede local e externa.

A qualidade da internet passou a ser notada, com a implementação do Squid fazendo armazenamento em cache e também do BIND que de maneira eficiente diminuiu o gargalo na rede e o tempo de resposta em momentos de pico.

O Quadro 1 mostra como estava o funcionamento da empresa antes de ser feita a implementação do servidor e seus serviços, e mostra também como ficaram os serviços utilizados após a implementação do servidor. Onde desta maneira se nota as vantagens obtidas através de um pacote de serviços eficientes que trouxeram benefícios com qualidade para uma empresa trabalhar de forma responsável, aumentando o desempenho do trabalho dos seus colaboradores.

Quadro 1: Antes e Depois

Serviços	Antes	Depois
Compartilhamento de arquivo em rede	Era feito sem restrições, onde qualquer usuário da rede tinha acesso a todos os arquivos e pastas.	Compartilhamento de arquivos e pastas controlados por restrições de usuários e grupos.
Acesso à internet	Sem controle de acesso, onde todos os usuários tinham acesso sem restrições a qualquer sites. Sem armazenamento em cache.	Controle de acesso feitos pelo Squid, com restrições a usuários comuns e sem restrições ao grupo de usuários da diretoria. O Squid passou a fazer armazenamento em cache, diminuindo o gargalo na rede
Firewall	Era usado o firewall do próprio sistema operacional.	Filtragem de todos os pacotes na rede, abrindo somente as portas necessárias para trabalho.
DNS	Usava-se o servidor DNS do Google.	Com o BIND o servidor local passou a fornecer o serviço de DNS, aumentando a velocidade de tradução de nomes, assim melhorando também a velocidade de acesso à sites.

Fonte: Do próprio pesquisador.

CONCLUSÃO

Através dos conhecimentos acadêmicos obtidos para a realização deste trabalho, foi possível fazer a implementação de um servidor na empresa Asprovel, solucionando diversos problemas que foram encontrados durante esta pesquisa.

De maneira satisfatória foi adquirido experiência teórica e técnica para enfrentar com mais eficiência o mercado de trabalho, que com o tempo está se tornando mais exigente principalmente para profissionais que possam satisfazer as necessidades desse setor de Tecnologia da Informação, setor este que evolui de forma rápida mudando sempre as diretivas de segurança de informação. Sendo a internet uma evolução sem fim, faz com que as empresas busquem um melhor meio de comunicação e agilidade através de recursos tecnológicos para prestarem um serviços cada vez mais eficiente. Desta forma, neste trabalho foi mostrado ferramentas eficientes para trazer mais segurança e confiabilidade no ambiente desta empresa.

Adotou-se neste trabalho uma solução flexível e viável, onde trará benefícios incalculáveis em se tratando de segurança de informações para esta empresa que necessita de proteção e sigilo de seus dados. As ferramentas implementadas puderam ajudar a alcançar vários objetivos, de forma eficaz e com baixo custo, já que tratamos de usar Software Livre.

Sobre à validação das hipóteses chegou-se a seguinte conclusão:

H0 - Não seria viável a implantação do sistema servidor Linux Proxy, DHCP, Arquivos e Firewall, pois a empresa não tem interesse em alterar sua rotina e seus processos atualmente existentes; se tornou inválida, pois com a alteração da rotina e processos da empresa, ela se tornou mais eficiente.

H1 – Não seria recomendável a implantação do servidor Linux Proxy, DHCP, Arquivos e Firewall, já que a empresa não iria arcar com o custo de um servidor; invalidada, pois o computador utilizado para a implementação do servidor, foi um micro já em uso na empresa para uma função já não mais necessária.

H2 - Seria viável a implantação do servidor Linux Proxy, DHCP, Arquivos e Firewall, pois a empresa iria trabalhar com software livre, sem gastos com suas respectivas licenças; válida, pois como dito a empresa não teve nenhum custo com relação a aquisição do sistema operacional e suas ferramentas.

H3 - Seria viável a implementação do servidor, já que com ele aumentaria a segurança, o controle e confiabilidade sobre dados e informações existentes na empresa. Viável, como demonstrado nos testes realizados foi possível concluir que foi possível obter os objetivos propostos neste trabalho.

Portanto, este trabalho realizado propõe uma melhoria para soluções em políticas de segurança de redes, e considera-se que possibilitará ser base de estudos para implementação de servidores baseados em software livre em diversos ambientes empresariais.

REFERÊNCIAS

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

HUNT, Craing. **Linux Servidores de rede.** 4º Edição. Rio de Janeiro: Ciência Moderna, 2004.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet.** 3º Edição. São Paulo: Pearson Education do Brasil, 2006.

MORIMOTO, Carlos E. **Servidores Linux, Guia Prático**. São Paulo: GDH Press e Sul Editores, 2008.

NORTON, Peter, **Introdução à Informática.** São Paulo: Pearson Makron Books, 1996.

SILBERSCHATZ, Abraham; GAGNE; Greg, GALVIN, Peter B. **Sistemas Operacionais com Java.** São Paulo: Elsevier Editora, 2004.

SILVA, Vitor. **Análise e Concepção de Servidores Linux Seguros.** Disponível em: <http://repositorio-aberto.up.pt/bitstream/10216/59107/2/Texto%20integral.pdf> Acessada em 26 de setembro de 2015.

STALLINGS, William, **Arquitetura e Organização de Computadores.** 8º Edição. São Paulo: Pearson Praticce Hall, 2010.

TANENBAUM, Andrew S., **Redes de Computadores.** 4° Edição. Rio de Janeiro: Elsevier Editora, 2003.

Sobre o Debian. Disponível em: <https://www.debian.org/News/2013/20130504> acessado em 16 de outubro de 2015.

O que é Software Livre. Disponível em: <https://www.fsf.org/about/what-is-free-software> acessado em 23de maio de 2015.

O que é Software Livre. Disponível em: <http://www.gnu.org/philosophy/free-sw.pt-br.html> acessado em 10 de setembro de 2015.

O que é GNU/Linux? Disponível em: <https://www.debian.org/releases/wheezy/mips/ch01s02.html.pt> acessada em 10 de setembro de 2015.

Linux e o Sistema GNU. Disponível em: <http://www.gnu.org/gnu/linux-and-gnu.html> acessada em 14 de setembro de 2015.

Por que eu deveria implantar o Squid. Disponível em: <http://www.squid-cache.org/Intro/why.html> acessado em 15 de setembro de 2015.

Servidor Debian. Disponível em: <http://servidordebian.org/pt/jessie/intranet/dhcp/start> acessado em 16 de setembro de 2015.

ISC DHCP. Disponível em: <https://www.isc.org/downloads/dhcp/> Acessado em 16 de setembro de 2015.

O que é iptables? Disponível em: <http://www.netfilter.org/projects/iptables/> acessada em 26 de setembro de 2015.

O que é netfilter.org? Disponível em: <http://www.netfilter.org/> acessado em 27 de setembro de 2015.

O que é Samba? Disponível em: <https://www.samba.org/samba/what_is_samba.html> Acessado em 26 de setembro de 2015.

Samba: Introdução. Disponível em: <https://www.samba.org/samba/docs/SambaIntro.html> Acessado em 26 de setembro de 2015.