CENTRO UNIVERSITÁRIO DO SUL DE MINAS - UNIS-MG
BACHARELADO EM SISTEMAS DE INFORMAÇÃO
ADEMILSON ALVES BIE

ESTUDO DE VIABILIDADE DE IMPLANTAÇÃO DE SERVIDOR PROXY ATRAVES DE SOFTWARE LIVRE

Varginha/MG
2014

ADEMILSON ALVES BIE

ESTUDO DE VIABILIDADE DE IMPLANTAÇÃO DE SERVIDOR PROXY ATRAVES DE SOFTWARE LIVRE

Trabalho apresentado ao curso de Bacharelado em Sistemas de Informação do Centro Universitário do Sul de Minas – UNIS/MG como pré-requisito para obtenção do grau de bacharel, sob orientação do Prof. Rodrigo Franklin Frogeri.

Varginha/MG
2014

ADEMILSON ALVES BIE

ESTUDO DE VIABILIDADE DE IMPLANTAÇÃO DE SERVIDOR PROXY ATRAVES DE SOFTWARE LIVRE

Monografia apresentada ao curso de Bacharelado em Sistemas de Informação do Centro Universitário do Sul de Minas – UNIS/MG, como pré-requisito para obtenção do grau de bacharel pela Banca Examinadora composta pelos membros:

Aprovado em / /

Prof. Esp.Rodrigo Franklin Frogeri

Profa. Dra. Letícia Rodrigues da Fonseca

DEDICATÓRIA

Dedico este trabalho a minha esposa que sempre me incentivou nos momentos difíceis.

AGRADECIMENTOS

Agradeço primeiro a Deus, aos meus colegas, professores e a minha esposa por terem ajudado na construção deste trabalho.

RESUMO

Esse trabalho visa apresentar um estudo de viabilidade de uma forma simples e eficiente de controle e limitação na navegação web, através da implementação, configuração e uso de um servidor Proxy utilizando o Pfsense e o Squid, ambos softwares livre , na escola estadual Professor Carlos Dalmo Moreira, localizada na cidade de Itamarandiba Minas Gerais bem como elencar os ganhos que esta implementação trará para a instituição, com um comparativo entre o antes e o depois da aplicação usando a metodologia do pdca e as ferramentas a esta associadas.

Palavras-chave: Redes. Servidores. Proxy.

ABSTRACT

This paper presents a feasibility study of a simple and efficient way to control and limit web browsing through the implementation, configuration and use of a proxy server using pfSense and Squid, both free software in public school Teacher Carlos Dalmo Moreira, located in Minas Gerais Itamarandiba and list the gains that this implementation will bring to the institution, with a comparison between before and after the application using the methodology of pdca and tools associated to this.

Keywords: Network. Servers. Proxy

Lista de Figuras

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

A popularização da internet e a evolução constante dos recursos computacionais podem ser consideradas como as grandes responsáveis pelo crescente volume de informação, tanto na Web quanto nas organizações. A informação ficou acessível a todas as classes, mas grande parte desta informação está relacionada a assuntos irrelevantes para o ambiente corporativo ou acadêmico. As pessoas perdem tempo acessando assuntos, que em sua grande maioria, não sabem quais são as possíveis conseqüências que isso pode acarretar ao seu trabalho e conseqüentemente colocando em risco os dados das empresas ou instituição. O mau uso da internet nas empresas e instituições fizeram com que estas tomassem providências em relação a essa questão, limitando o acesso e desenvolvendo políticas e ações de controle do uso da internet pelos seus funcionários ou alunos.

Esse trabalho visa apresentar um estudo de viabilidade de uma forma simples e eficiente de controle e limitação na navegação web, através da implementação, configuração e uso de um servidor Proxy utilizando o Pfsense e o Squid, ambos softwares Livres, na Escola Estadual Professor Carlos Dalmo Moreira em Itamarandiba/MG bem como elencar os ganhos que esta implementação trará para a instituição, com um comparativo entre o antes e o depois da aplicação usando a metodologia do pdca e as ferramentas a esta associadas.

1.1 Tema específico

Implantação de um servidor Proxy com pfsense e squid na escola estadual professor Carlos Dalmo Moreira.

1.2 Problema de pesquisa

Como permitir o acesso a internet e garantir que a informação acessada é adequada para uma instituição de ensino?

1.3 Problematização

A necessidade do controle e gerenciamento da rede em empresas e instituições torna-se fundamental a cada dia, visto o crescente índice de ameaças as empresas nos últimos anos e o crescente acesso dos funcionários e alunos a sites de relacionamentos e salas de bate papo que comprometem tanto o desempenho profissional quanto o aprendizado dos alunos.

1.4 Hipóteses

Bloquear sites usando programas de execução local.
Monitorar o acesso individualizado.
Implantar servidor Proxy.

1.5 Objetivo geral

Avaliar a viabilidade de Implantação de um servidor Proxy que possibilite o gerenciamento e controle da informação da rede, e elencar os ganhos pos instalação do servidor através de um comparativo entre a rede com o servidor proxy e sem o servidor.

1.6 Objetivos Específicos

Apresentar um estudo de viabilidade de uma forma simples e eficiente de controle e limitação na navegação web, através da implementação, configuração e uso de um servidor Proxy utilizando o Pfsense e o Squid, ambos softwares Livres, na Escola Estadual Professor Carlos Dalmo Moreira em Itamarandiba/MG bem como elencar os ganhos que esta implementação trará para a instituição., com um comparativo entre o antes e o depois da aplicação .

1.7 Justificativa

Em visita a escola, desenvolvendo um trabalho voluntário de manutenção dos computadores da instituição, notei como era recorrente a infecção das maquinas da escola devido a falta de controle a conteúdos que os alunos acessavam.

Atualmente, a escola estadual professor Carlos Dalmo Moreira conta com 04 computadores em toda a escola e o link de internet via satélite recebido por um modem skyedge é dividido através de um switch de 24 portas cisco, o acesso dos usuários é livre a toda a rede o que demanda sempre um funcionário na biblioteca para inibir o acesso a conteúdo inapropriado, principalmente pelas classes iniciais da escola que ainda não possuem um total domínio do uso de computadores e internet. Mas esta forma de controle não se mostra totalmente eficaz, pois depende da supervisão constante o que nem sempre é possível.

Desta forma nasceu a idéia de fazer um estudo de viabilidade da implantação do servidor na escola estadual professor Carlos Dalmo Moreira, que propiciará um ambiente mais seguro para a escola trazendo ganhos para professores e alunos que estarão usando a internet como ferramenta para aumentar a produtividade e o conhecimento. Como beneficio de imediato temos:

- Navegação mais segura.
- Controle por parte da escola do conteúdo mais acessado pelos alunos.
- Elaboração de projetos baseados nas informações mais buscadas pelos alunos
- Restrição sem necessidade de supervisão.
- Melhor utilização da banda disponível.

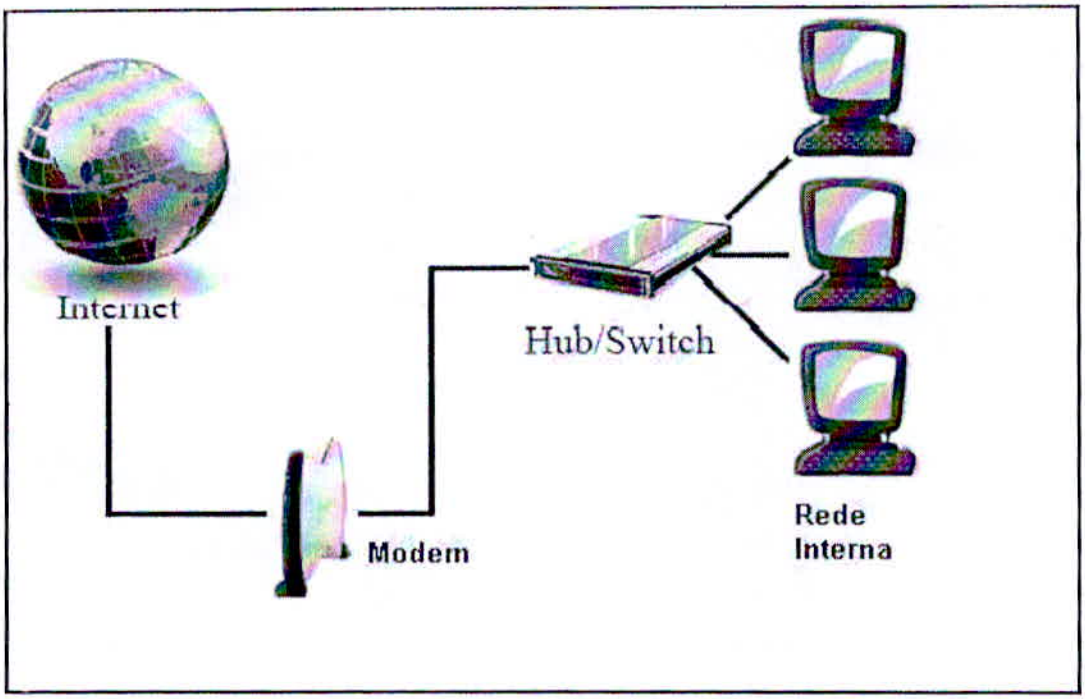
Os pontos negativos:

- Possível aumento no consumo de energia.
- Necessidade de treinamento para no mínimo 02 funcionários.

2. PROXY

Na maioria dos computadores dos usuários de internet o browser faz a conexão direta com a rede WAN (internet) como figura abaixo.

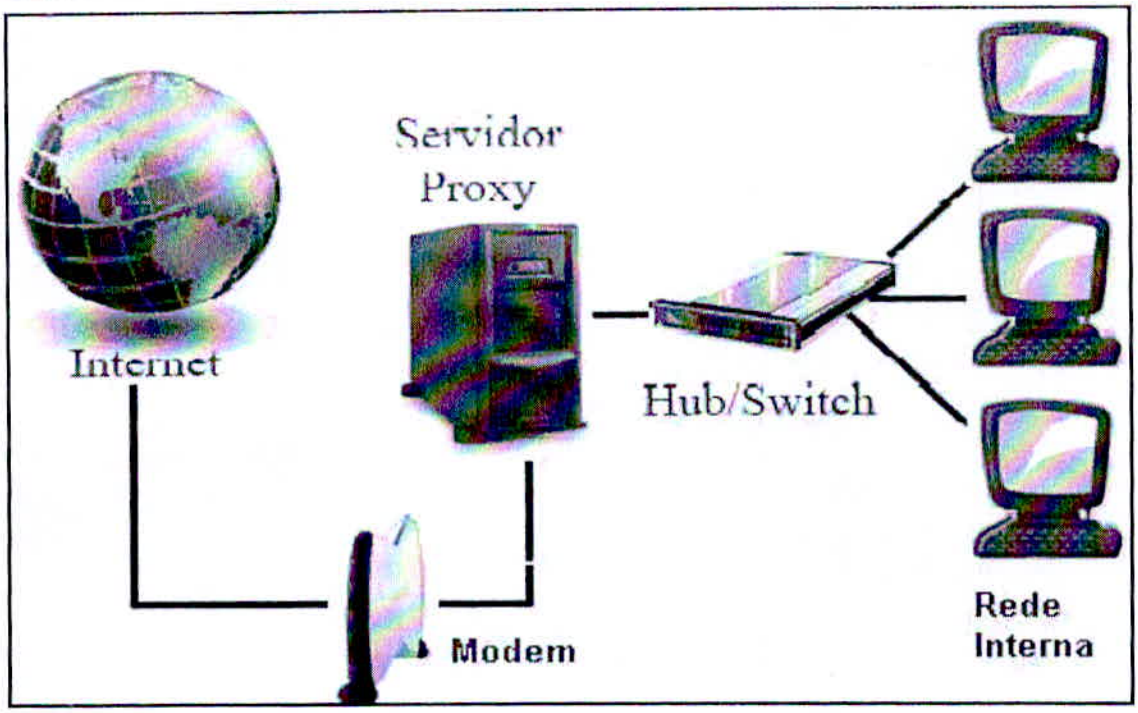
Figura 1 - Rede sem Proxy



Fonte: Acesso em: 01 Nov. 2014. Disponível em: http://www.portalgsti.com.br/

Conforme Palma e Prates (2000 p.1) "cada vez mais os administradores têm que controlar e monitorar o acesso a recursos das redes de computadores". Mas em empresas ou locais onde se queira restringir e monitorar o acesso a rede o ideal é ter um servidor Proxy. Segundo Ricci e Mendonça (2006 P.1) "O conceito de Proxy refere-se a um software que atua como gateway de aplicação entre o cliente e o serviço a ser acessado, interpretando as requisições e repassando-as ao servidor de destino"; Ou seja, funciona como um intermediário entre o cliente e o servidor de destino, uma ligação entre uma rede externa (WAN) e uma rede interna (LAN).

Figura 2- Rede com Proxy



Fonte: Acesso em: 01 Nov. 2014. Disponivel em: <http://www.portalgsti.com.br/>/

Ainda segundo Ricci e Mendonça (2006 P.1) "o servidor Proxy é capaz de analisar os pacotes de rede na camada de aplicação, ou camada sete, do modelo OSI (Open Systems nterconnection)". Isto permite que o tráfego dentro de um serviço, como o tráfego da porta 80 (http) possa ser filtrado, os servidores Proxy analisam o tráfego http ou ftp, e determinam se deve ou não passar. Se houver uma regra (ACL) que impeça a passagem de qualquer endereço web que contiver a palavra "sexo", então qualquer pedido de url http que contiver "sexo" será negado. O Proxy tem a função de concentrar todas as requisições das mais diversas origens, canalizando-as por uma mesma saída, ele é que, efetivamente, faz a requisição ao destino.

O servidor efetua tais requisições seguindo regras, ou filtros, implementados pela ferramenta de Proxy. Tais filtros têm a função de proibir ou liberar acessos a sites, endereços, identificadores de máquinas e redes, strings e até mesmo limitar velocidade de determinado acesso. Além disso, são capazes de coibir o acesso através de regras que atuam sobre os clientes da rede interna, como nomes de usuários, grupos de usuários, endereços identificadores de máquinas etc.

- O browser solicita a conexão ao web Server pela porta 80,
- O Proxy responde para o browser estabelecendo a conexão;
- O Proxy estabelece uma conexão com o web Server;

- O browser solicita o conteúdo do site (GET/http1.1) para o Proxy;
- O Proxy solicita ao web Server quais objetos formam a página;
- O Proxy verifica se os objetos existentes no cache ainda são válidos.
- O Proxy entrega imediatamente o conteúdo válido e busca no web Server apenas os objetos não válidos;
- A página está carregada.

Segundo Jamil (2010) "Do ponto de vista de segurança, um servidor proxy é uma opção muito eficaz para se evitar problemas relacionados a acesso a páginas não permitidas. Como todo o acesso pode ser monitorado fica mais fácil visualizar uma possível ação maliciosa ou fraudulenta".

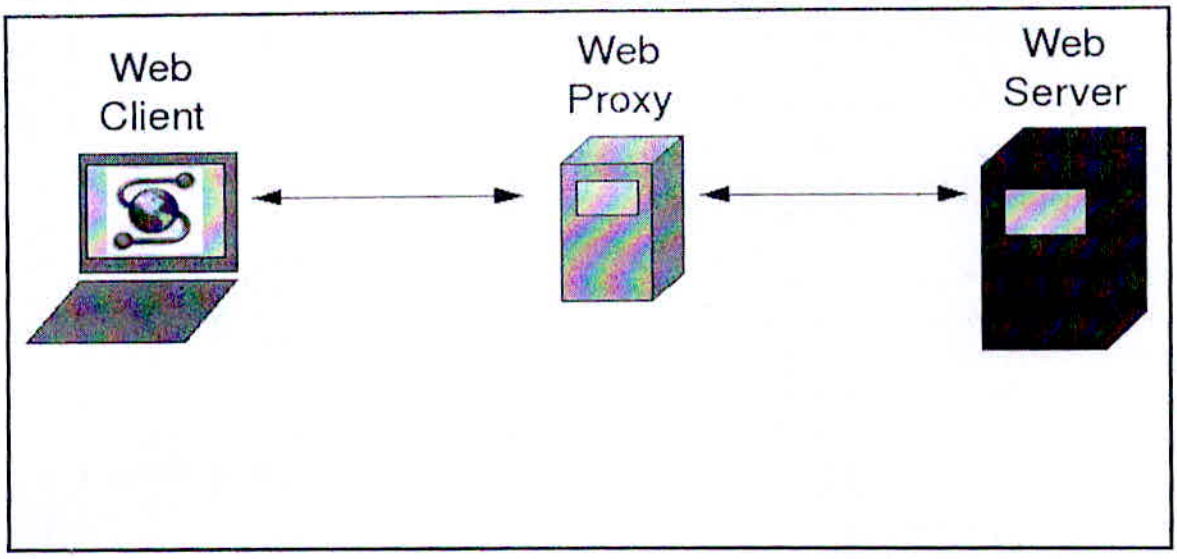
2.1.1 Tipos de Proxy

Os quatro principais tipos de Proxy são: Web, caching, reverter e transparente. Alguns servidores têm proxies que incluem várias funções, tais como Web e cachê ou reverter e cachê.

2.1.2 Web Proxy

Conforme Ricci e Mendonça(2006 p.3) "Em uma configuração de Proxy Web, o computador se conecta ao Proxy e faz o pedido para ser conectado a um servidor específico O servidor Proxy se conectar ao servidor desejado e atua como um intermediário entre você e servidor." Desta forma o servidor ao qual você deseja se conectar só vê o servidor Proxy e não o seu computador. Seu endereço IP (endereço único que o identifica na rede) permanece desconhecido para o servidor web de destino e garante o anonimato do uso.

Figura 3 - Web Proxy



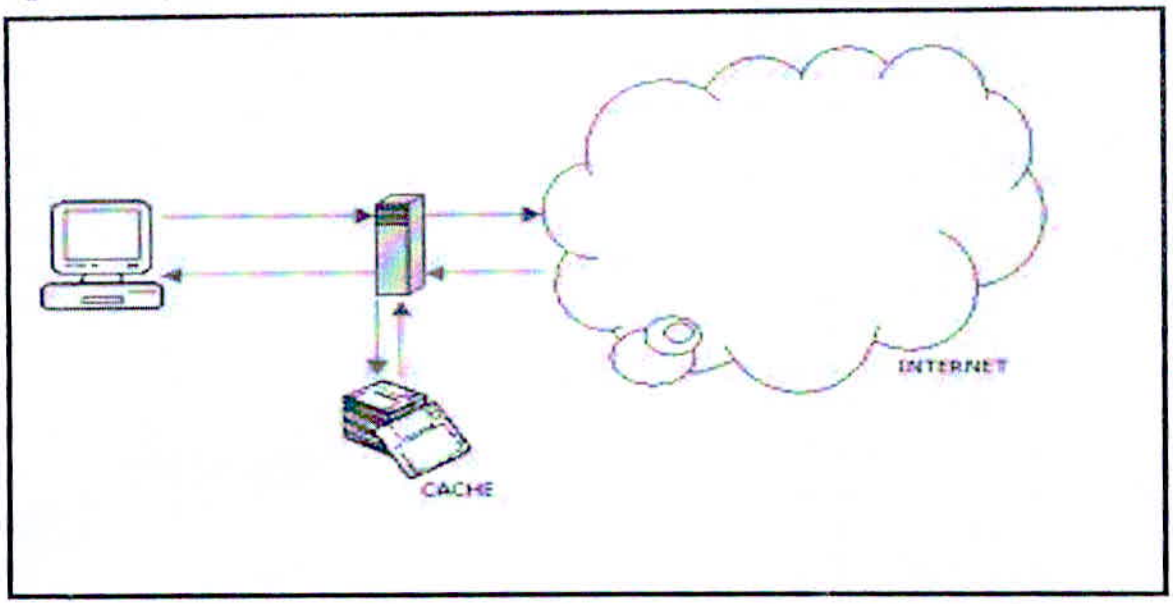
Fonte: Acesso em: 01 Nov. 2014. Disponível em: <http://www.linuxjournal.com/>

2.1.3 Proxy Cache

Conforme Watanabe (2000), "o cache é onde os arquivos requisitados pelo servidor Proxy são armazenados e repassados posteriormente para os clientes, que são as estações de trabalho da rede interna". Normalmente, o mesmo Proxy é usado por todos os clientes em uma sub-rede. Isto torna possível para ele fazer caching eficiente de todos os documentos requisitados. Um Proxy cache age como um intermediário entre você e o servidor que deseja se conectar. Um Proxy de armazenamento em cache armazena todos os dados não criptografados em um meio de armazenamento. Se você ou outra pessoa faz um pedido para ser conectado ao mesmo servidor, o Proxy cachê enviará os dados que tem no armazenamento em vez de conectar-se ao servidor solicitado. Esse sistema permite uma redução significativa em termos de tempo de acesso e largura de banda para a empresa que implementa um Proxy cache.

O uso de cache também torna possível acessar algumas páginas mesmo que servidores estejam fora do ar.

Figura 4- Proxy cache

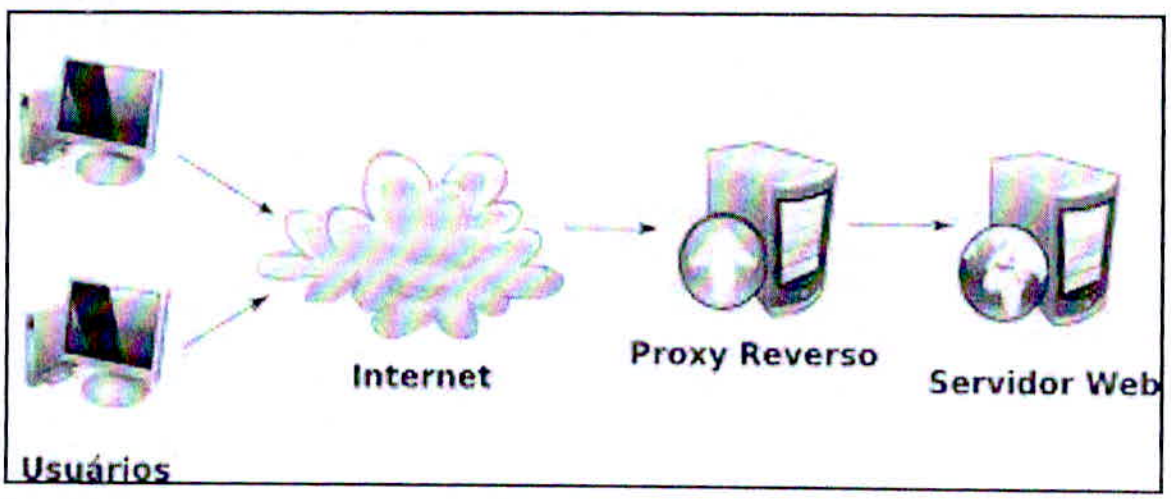


Fonte:Elaborada pelo autor

2.1.4 Proxy reverso

Enquanto Web e o Proxy cache residem no lado do cliente da rede, um Proxy reverso reside no lado do servidor. Ao solicitar uma conexão a um servidor, o computador realmente faz a conexão com o Proxy reverso. O Proxy reverso, em seguida, obtém os dados solicitados por você a partir de um ou vários servidores que só ele tem acesso. O Proxy reverso é usado para aumentar o tempo de entrega e reduzir a carga nos servidores Web por trás dele.

Figura 5- Proxy reverso

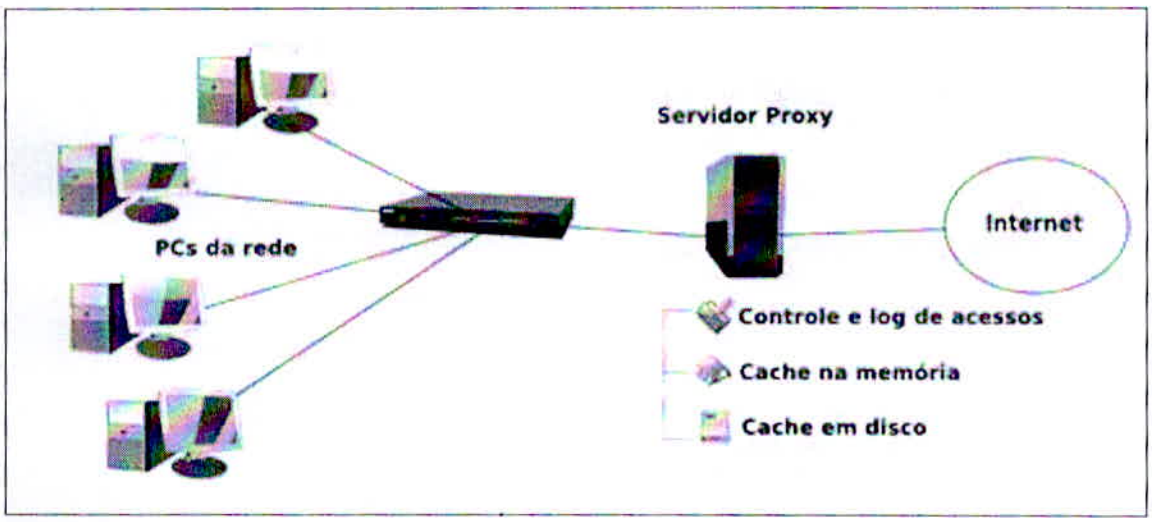


Fonte: Acesso em: 01 Nov. 2014. Disponível em: <http://www.vivaolinux.com.br/artigo/>

2.1.5 Proxy Transparente

Um Proxy transparente é um Proxy que intercepta todas as informações que estão passando em sua rede e realiza um reendereçamento para uma porta especifica. Web proxies e cache , quando configurado como proxies não transparentes , serão necessários configurar seu aplicativo (geralmente seu navegador de internet) especificamente para usar o Proxy. Se o navegador da Web não está configurado, o Proxy não é usado. Proxies transparentes são invisíveis para os usuários finais, proporcionando as mesmas vantagens que as procurações regulares.

Figura 6 - Proxy Transparente



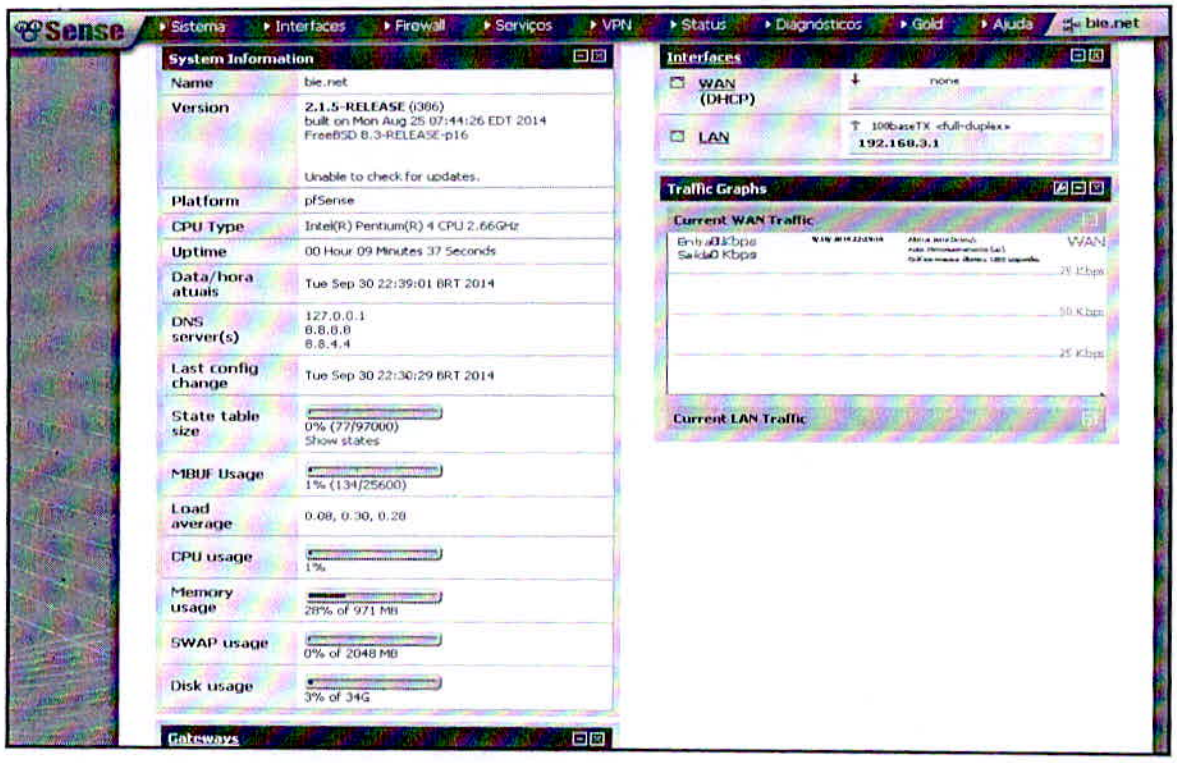
Fonte : Acesso em: 01 Nov. 2014. Disponível em: <http://www.hardware.com.br/>

Conforme Ricci e Mendonça(2006 p.4)"A utilização da técnica de web Proxy transparente consiste no administrador criar um redirecionando de porta utilizando regras de firewall" Com o Proxy transparente o usuário é obrigado a passar por ele para obter a conexão desejada, como não há configuração na maquina do cliente o processo de configuração se torna mais simples e mais seguro.

3. PFSENSE

Conforme Willianson, (2012 p.1) "Pfsense é um sistema operacional open source, ou seja, código fonte aberto, e foi usado pela primeira vez em 1998 por programadores para identificar seus programas como software livre". O pfsense transforma qualquer computador em um firewall, roteador; é uma distribuição FreeBSD feita com base no projeto m0n0wall, uma distribuição de firewall poderosa e leve, o m0n0wall foi aperfeiçoado e adicionado uma variedade de serviços de rede mais usados. O PfSense é uma ferramenta que faz a integração de várias ferramentas que fazem parte da área de rede e segurança.Depois de instalado sua manipulação é feita através do browser acessando o endereço ip recebido da rede.

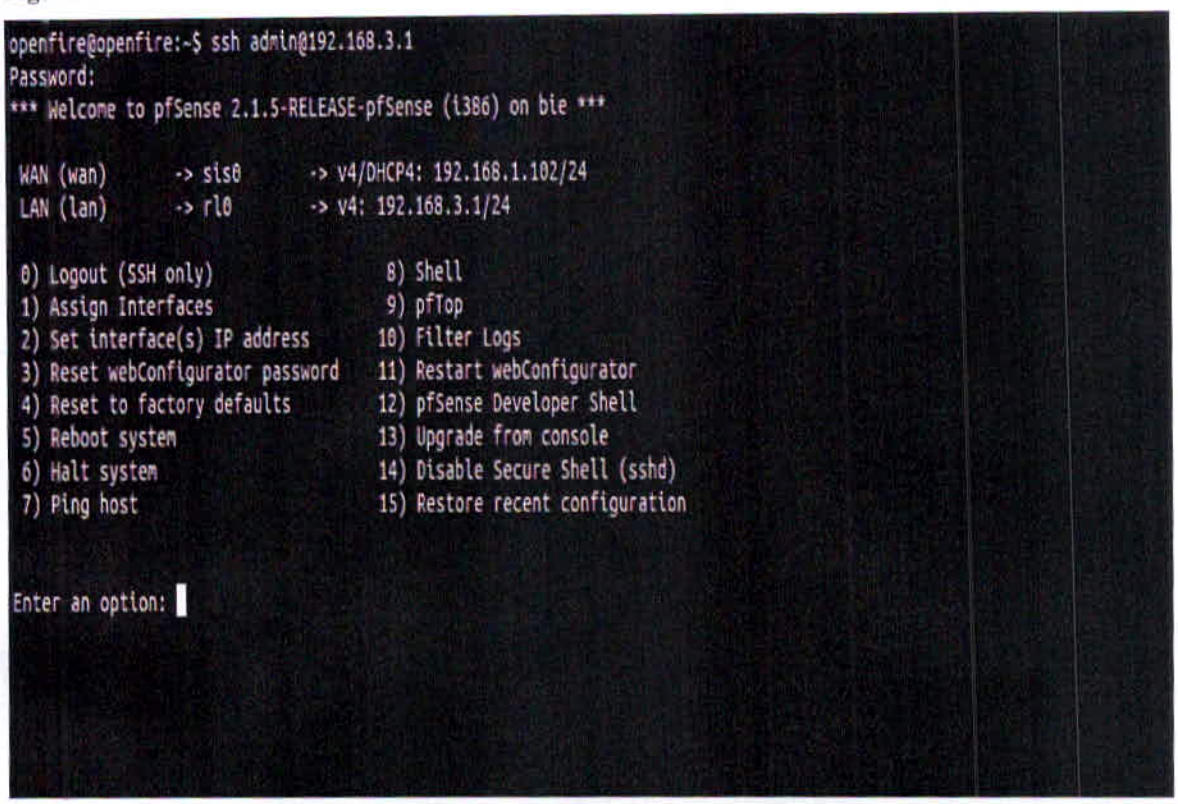
Figura 7 - Tela Inicial Pfsense



Fonte: Elaborada pelo autor

Ou através do console ssh.

Figura 8 - Acesso via ssh



Fonte: Elaborada pelo autor

Conforme Williamson,(2012, p.1), "o PfSense é um software com a licença na base do bsd license. Com base no sistema operacional freebsb, adaptou-se para que trabalhasse como uma ferramenta de firewall e/ou roteador para redes." Hoje ele já vem com diversas tecnologias embutidas, assim se tornando uma ferramenta extremamente eficiente.

3.1 História do PfSense

O projeto teve inicio por volta de 2004, por Chris Buechler e Ullrich Scott. juntando códigos por bastante tempo, do projeto m0n0wall, que é um projeto semelhante ao PfSense, mas com um foco em dispositivos que pudessem rodar diretamente em memória principal, com isso muitas funções ficaram a desejar, Chris juntou forças com Ullrich e começaram então o projeto.

3.2 Porque Usar o Pfsense?

Embora seja uma versão customizada do Free BSD, não é necessário qualquer conhecimento sobre este sistema para operar o pfsense, visto que ele é atualizado e completamente configurado através de uma interface web. Na maioria dos casos o pfsense tem sido aplicado como um firewall de perímetro, roteador, Access point wireless, servidor dhcp, servidor dns e vpn. O mesmo apresenta diversos recursos gráficos para análise de tráfego, pacotes, desempenho, etc. Além de configurações avançadas para regras de firewall para lan, wan e utilização de Aliases de forma simples e intuitiva. Com essa poderosa ferramenta é possível administrar:

- Proxy (squid)
- Proxy Filter (squid Guard),
- Sniffer (tcpdump),
- Traffic Shaping,
- Firewall (packet filter),
- Wireless,
- VPN,
- Autenticação, entre outras.

Mesmo o computador mais modesto nos dias atuais roda com folga o Pfsense que tem os seguintes requisitos Mínimos de Hardware:

- Um CPU - Pentium 100 MHz;
- Uma memória RAM de 128 MB;
- Um disco rígido de 1Gb.

pode ser usado de várias formas como:

- Live CD com Instalador;
- Instalação no Disco Rígido;
- Incorporado o Compact Flash (CF); este tipo de mídia é pouco utilizado nos dias atuais, Perdeu mercado com a popularização do Secure Digital (SD) que continham espaço igual a um preço reduzido. Visto que nem todos precisam de velocidade.

3.3 Vantagens do Pfsense:

- Código aberto (open source), não há necessidade de aquisição de licenças;
- Construído em cima de uma base sólida (freebsd);
- Gerenciamento fácil via interface Web;
- Projetado para rodar em cima de hardware Intel x86/x86_64 bits (servidores comuns);
- Infra-estrutura estável construída para atender as mais diversas demandas;
- Controle de MSN (permite gravar as mensagens trocadas pelos funcionários);
- Bloqueio por tipo de arquivos (ex: Excel, programas, zip, áudio);
- Controle de banda (permite priorizar o tráfego para algumas máquinas ou pessoas);
- Relatórios detalhados de navegação;
- Redundância automática de links de internet;
- Gateway VPN;
- Integração com serviço de diretório.
- Infra-estrutura estável construída para atender as mais diversas demandas;

4. SQUID

Squid é fornecido como, software livre de código aberto e pode ser usado sob a GNU General Public License (GPL) da Free Software Foundation.O Squid foi originalmente concebido para ser executado em sistemas baseados em Unix, mas também pode ser executado em máquinas Windows.O Squid é um servidor Proxy e cache que permite tanto compartilhar o acesso à Web com outros PCs da rede, quanto melhorar a velocidade de acesso através do cache. O Squid possui tudo o que você precisa para dar acesso à Internet para os funcionários de uma grande empresa, por exemplo, sem perder o controle.O squid permite compartilhar a conexão com vários computadores, ele vai ser o intermediário ente a internet e o usuário. Segundo Morimoto (2006 p.7) "O servidor de Proxy Squid não limita as requisições dos usuários ele analisa todo o conteúdo dos dados e separa o que não pode e o que pode ser acessado pelo usuário"

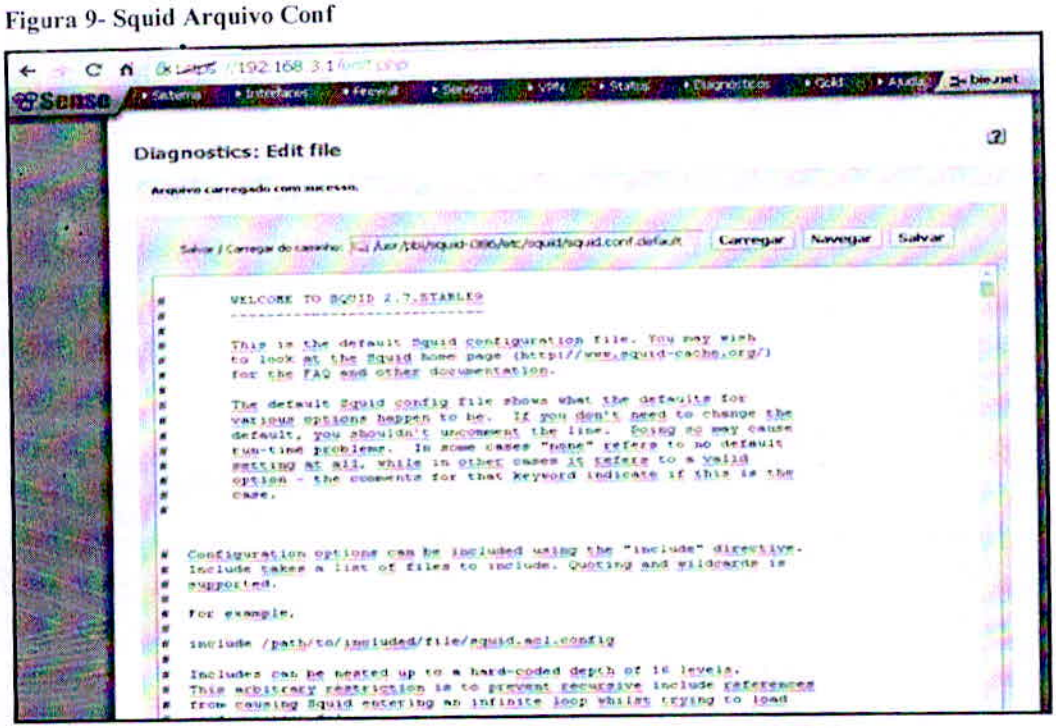
o Squid é o Proxy mais popular para o Linux, pode ser utilizado como firewall, baseados em protocolos que irão filtrar acessos vindos da rede interna, ou seja, a internet no qual faz parte como canal de saída.

Segundo Wessels (2004 p.3) alguns dos principais usos e vantagens do Squid são:

- Economizar banda do provedor de Internet enquanto se navega na web;
- Diminuir o tempo que uma página leva para carregar;
- Coletar estatísticas sobre o tráfego web da rede;
- Bloquear o acesso às páginas inapropriadas conforme a política de uso da empresa;
- Garantir que apenas usuários autorizados possam navegar na Internet.

As configurações do Squid estão concentradas no arquivo /usr/pbi/squid-i386/etc/squid/squid.conf.default. Para editá-lo no pfsense basta navegar até o arquivo fazer a alteração e salvar.

Figura 9- Squid Arquivo Conf



Fonte: Elaborada pelo autor

Nos clientes você precisará apenas configurar o navegador para acessar através do Proxy ou configurar o Proxy transparente no servidor . No caso de configuração dos navegadores você deve acessar a configuração da conexão, marcar a opção de acessar através de um servidor Proxy e dar o endereço IP do servidor Proxy ou nome no caso de domínio e a porta que configurou na primeira opção; geralmente pela porta 80. O servidor pode ser usado por clientes rodando qualquer navegador e qualquer sistema operacional.

5. POLITICA DE SEGURANÇA DA REDE

A política de segurança serve para que todas as possíveis ameaças sejam minimizadas e combatidas eficientemente. Juntamente com a diretoria foi elaborada a política de segurança da escola que define regras sobre senhas e condutas a ser seguida pelos professores que possuem acesso ao servidor ou acesso a serviços da escola que possua acesso restrito. Existem várias razões para nos preocuparmos com segurança em nossa rede, e ter uma política de segurança bem estabelecida por mais simples que seja pode nos poupar grandes transtornos, basicamente a segurança esta relacionada a três fatores:

5.1 Segurança Física

Refere-se a tudo que envolve hardware e o ambiente que o servidor se encontra. Não adianta nos cercamos dos melhores softwares e hardware se nosso servidor fica numa sala onde todos têm acesso.

5.2 Software

Se refere aos softwares utilizados para a implementação do servidor desde aplicativos básicos até ao sistema operacional. Em se tratando de um servidor Proxy cuja principal função é restringir o acesso, devemos analisar as principais ameaças existentes que tem função de tentar burlar o bloqueio do servidor Proxy dentre os quais destacamos:
O UltraSurf é um software desenvolvido pela empresa UltraRech, que permite aos usuários em redes com controle de acesso burlar a política de segurança de acesso à Internet ou pelo menos tentar. A ferramenta utiliza um túnel criptografado, via porta TCP 443. A interface do software é bem simples, é portátil e não requer instalação o que facilita para o usuário e dificulta o bloqueio. A forma mais simples de bloqueio para este programa seria bloqueando a porta 443, usando um Proxy não transparente e liberando o acesso manualmente a medida que forem surgindo as solicitações , dependendo do tamanho da rede esta solução se torna trabalhosa , visto que teremos que configurar o endereço do proxy nos navegadores dos clientes mas se mostrou eficaz durante a implementação do servidor , como adicional de segurança instalamos o snort. Segundo Caswell et al. (2003) o Snort é uma ferramenta NIDS (Sistema de Detecção de Intrusão de Redes) desenvolvido por Martin Roesch, bastante popular por sua flexibilidade nas configurações de regras e constante atualização frente às

novas ferramentas de invasão. O Snort monitora o tráfego de pacotes em redes IP, realizando análises em tempo real sobre diversos protocolos (nível de rede e aplicação) e seu conteúdo (hexa e ASCII). Outro ponto positivo desse software é o grande número de possibilidades de tratamento dos alertas gerados

5.3 Pessoas

Este é o componente mais importante da segurança, quando se tem uma política de segurança bem estabelecida e as pessoas envolvidas recebem o devido treinamento e conscientização sobre como a segurança é importante e como esta pessoa está inserida neste contexto já minimizamos a possibilidade de erros e conseqüentemente temos uma segurança mais efetiva. Devemos dar atenção especial nos treinamentos para evitar a engenharia social.

Figura 10- Engenharia social

Fonte: Acesso em: 01 Nov. 2014. Disponível em: < http://sergiodiabreu.blogspot.com.br/>/

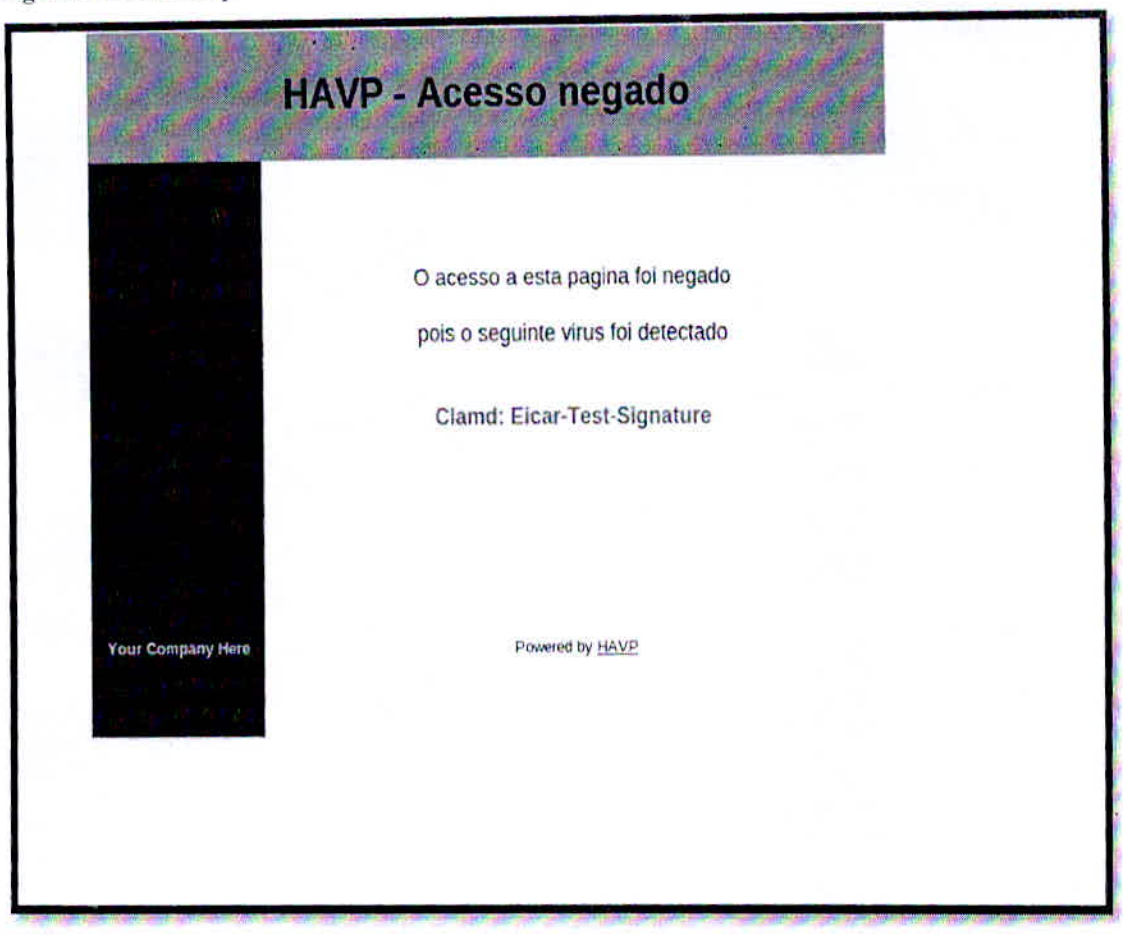
Engenharia social é um ataque onde a principal arma utilizada é a habilidade de lidar com pessoas induzindo-as a fornecer informações, executar programas e muitas vezes fornecer senhas de acesso seja pessoalmente via email,telefone etc.

A segurança não pode ser complicada, quanto mais você complica maior a chance de algo sair errado, além de dificultar a posterior manutenção.

5.4 Integração com Antivírus

Mesmo com a instalação do squid a rede ainda não está totalmente livre da ameaça de vírus e conteúdos maliciosos , desta forma é necessário a utilização de um antivírus , o pfsense tem o pacote do Havp que é uma solução confiável para proteção da rede .

Figura 11- Tela Havp



Fonte: Elaborada pelo autor

6. MATERIAL E MÉTODOS

Inicialmente foi realizada uma pesquisa bibliográfica sobre os requisitos necessários para a implantação propriamente dita do Servidor Proxy. A metodologia que foi empregada neste trabalho é baseada na aplicação de observação sistemática. Para Marconi e Lakatos(2003, p. 193) e Thums (2003, p. 155), neste tipo de observação há um planejamento de ações, sendo uma observação direcionada.Foi adotado o modelo do ciclo PDCA e algumas ferramentas a ele associadas para diagnosticar a situação atual e posteriormente apresentar os ganhos decorrentes com o uso do servidor Proxy para a escola. Num primeiro momento será feito o monitoramento da rede para identificar de forma quantitativa os sites e serviços mais requisitados, bem como a duração de execução. Num segundo momento será feita amostragem qualitativa por grupos de serviços e sites; através dos resultados obtidos aplicaremos o PDCA até atingir o resultado esperado pela escola. O ambiente pesquisado será composto por 05 computadores com acesso a internet sendo um o servidor Proxy. O hardware disponível para a pesquisa contará com 01 servidor, com hardware bastante modesto e que até então não tinha nenhuma utilidade para a escola, pois era considerado obsoleto e com recursos limitados para uso dos aplicativos atuais tendo assim a seguinte configuração:

Tabela 1 - hardware utilizado

Modelo	*Processador*	*Memória*	*Hard Disk*
Transglobe Itautec	Pentium 4	512mb	40GB

Fonte: Elaborado pelo autor

Tabela 2 - Sistema operacional e serviços do Servidor

Modelo	*Sistema*	*Serviços*
Transglobe Itautec	Pfsense	Proxy Squid ,

Fonte: Elaborado pelo autor

7. RESULTADOS

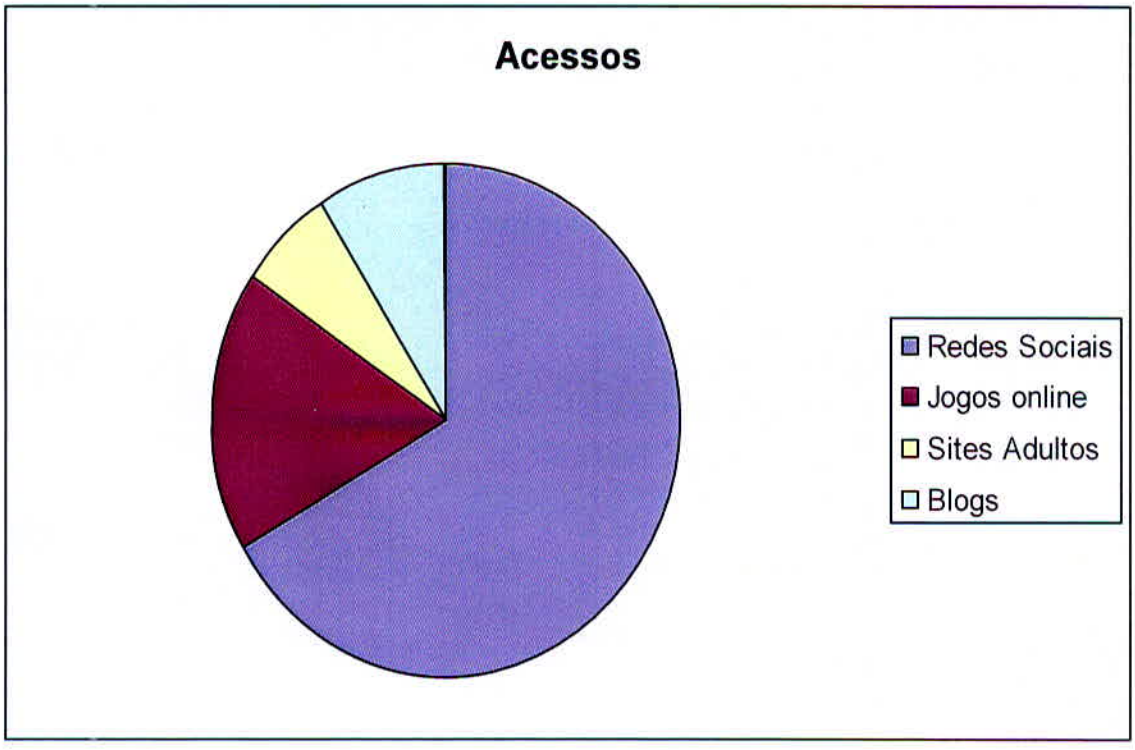
Na primeira semana após a instalação do servidor Proxy squid, deixamos tudo liberado para monitorar os acessos e identificar qual forma mais eficiente de realizar os bloqueios, usando o diagrama de pareto obtivemos os seguintes resultados aos conteúdos considerados inapropriados:

Tabela 3 - Diagrama de pareto

Conteúdo	*%*	*Ocorrências*	
Redes Sociais	66,67	30
Jogos on-line	17,78	8
Sites Adultos	6,67	3
Blogs	8,89	4
Total	100,00	45,00

Fonte: Elaborado pelo autor

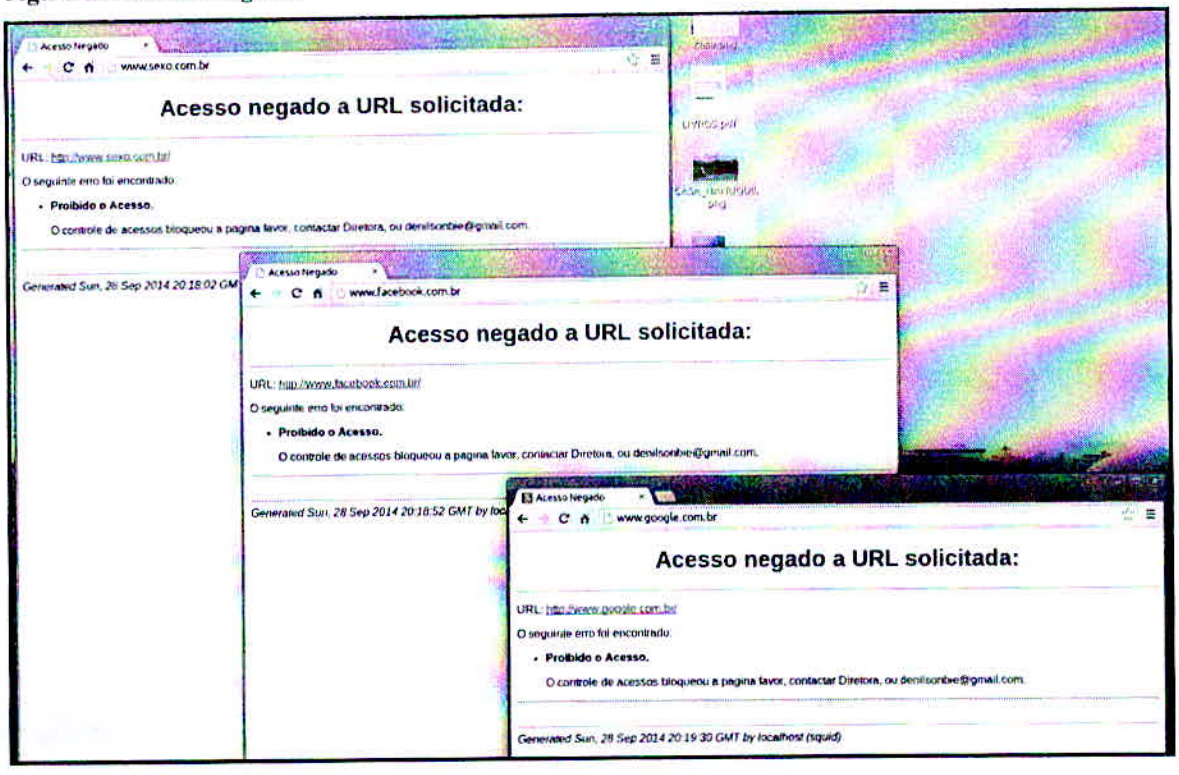
Gráfico 1 – Acessos sem o Proxy ativo



Fonte: Elaborado pelo autor

Após a analise dos acessos implantamos o servidor com bloqueio total , colocando na blacklist do squid um ponto (.) e liberamos na whitelist as extensões .gov.br , .edu.br e incluímos uma regra acl para o https do facebook por bloqueio por ip de destino.

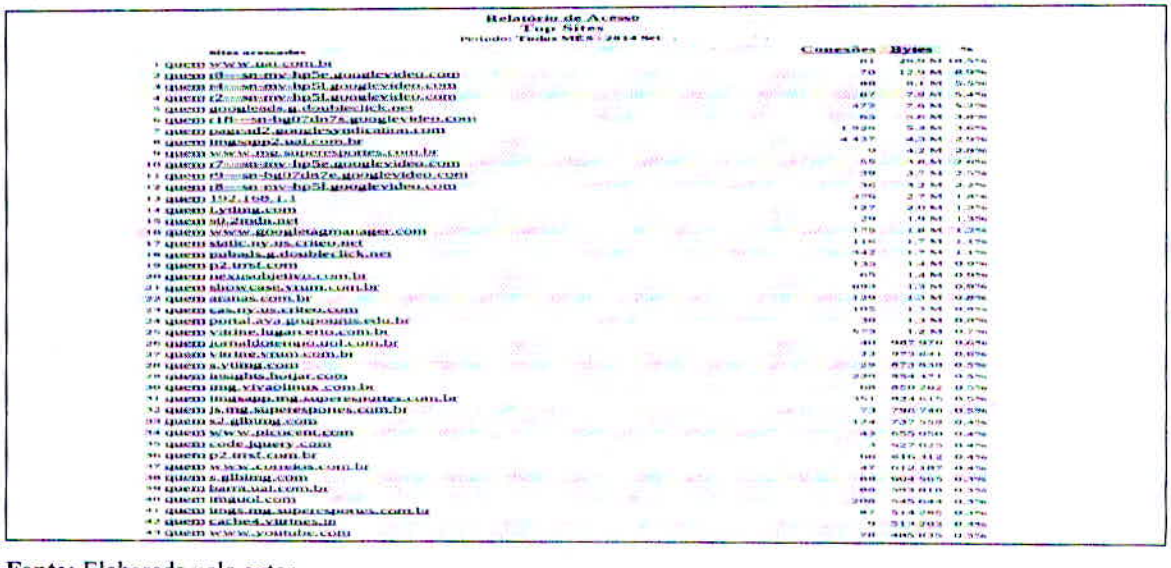
Figura 12- Acessos negados



Fonte: Elaborada pelo autor

Ainda usando a metodologia do pdca, monitoramos novamente os acessos para identificar possíveis falhas do Proxy.

Figura 13 – Relatórios de acessos



Fonte: Elaborada pelo autor

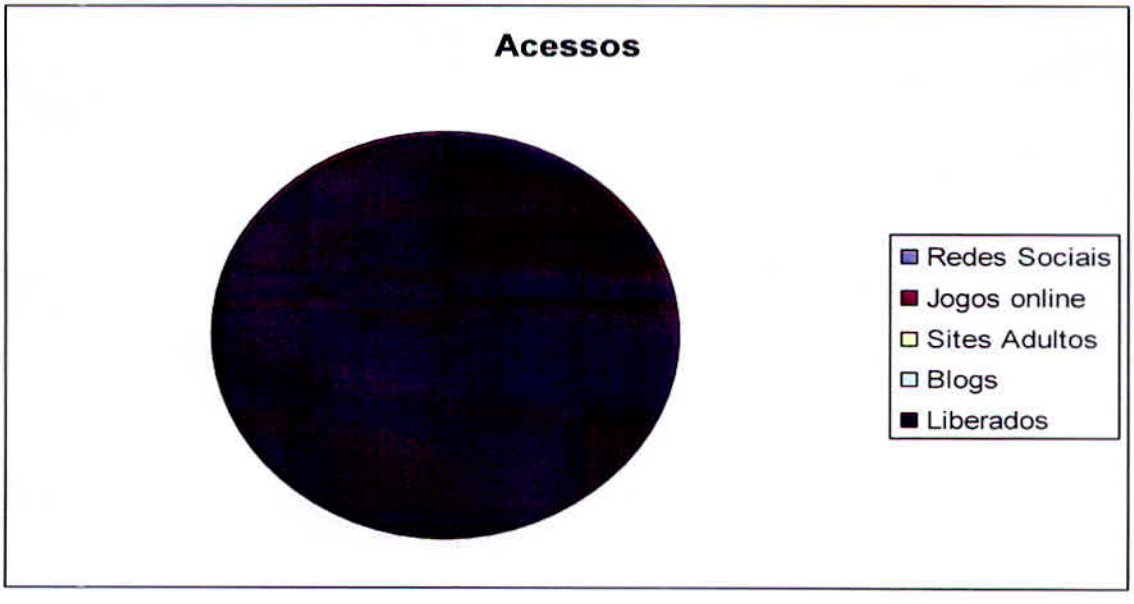
Após esta nova analise chegou-se ao objetivo esperado, pois não foi identificado nenhum acesso a conteúdo proibido pela instituição.

Tabela 4 – Diagrama de Pareto

Conteúdo	*%*	*Ocorrências*
Redes Sociais	0,00	0
Jogos on-line	0,00	0
Sites Adultos	0,00	0
Blogs	0,00	0
Liberados	100,00	45
Total	100,00	45,00

Fonte: Elaborada pelo autor

Gráfico 2 - Acessos com o Proxy ativo



Fonte: Elaborado pelo autor

8. CONCLUSÃO

A construção do protótipo de implantação do servidor pfsense como solução para resolver os problemas da Escola Estadual professor Carlos Dalmo Moreira em Itamarandiba foi a concretização de mais uma etapa de aprendizagem no curso de Bacharelado em Sistemas de informação, além de um embasamento teórico e técnico construído durante a pesquisa na área de redes e, profundas noções sobre a utilização de sistemas operacionais (GNU/Linux), o pfsense e seus pacotes e o Proxy (SQUID).

Na implantação do Servidor, é possível observar a integração do pfsense e squid que possibilitam a integração dos serviços e centralização de informações de acessos. A implantação do servidor trará vários benefícios para a instituição, conforme foi apresentado no capítulo um , podendo se destacar a agilidade para o administrador de rede em gerenciar o sistema e a proteção ao usuário, que estará num ambiente mais seguro. Ressaltando que a construção do projeto se deu pensando em projetos futuros. Foram utilizadas ferramentas altamente compatíveis, deixando-o de fácil escalabilidade com a possibilidade de ser implantado em outras instituições. Com os resultados do capítulo 5, que trata da implantação dos serviços, pode-se afirmar que a solução adotada para o projeto é uma alternativa viável para a instituição, que busca a segurança dos dados, controle de banda e, principalmente a restrição a conteúdos proibidos pela escola.Sendo assim, a implantação do projeto, que se deu através da busca de seus objetivos, contemplou a hipótese levantada na fase de projeto (vide introdução), uma vez que a implantação do servidor Proxy utilizando o pfsense e o squid na Escola Estadual professor Carlos Dalmo Moreira integrará a rede, acabando com acessos a conteúdo proibido pelos usuários e aumentará a segurança das informações.

REFERÊNCIAS

JAMIL,Vitor. Servidor Proxy.Em:<www.scriptcase.com.br/blog/servidor-proxy/>. (Acesso em: 10 setembro 2014.)

LAKATOS, E. M.; MARCONI, M. A. Fundamentos de metodologia científica. São Paulo: Atlas, 2003.

MATT, WILLIAMSON Livro pfsense 2.0 2012.

MORIMOTO, Carlos. E., Entendendo e Dominando o Linux 5 ed. - 2006 .

PALMA, L.; PRATES, R. TCP/IP: guia de consulta rápida. São Paulo: Novatec, 2000

RICCI, B. MENDONÇA, N. Squid: A Solução definitiva. Rio de Janeiro: Ed. Ciência moderna Ltda.2006.

WATANABE, C. S. Introdução ao cache de web. [Rio de Janeiro], [2000]. Disponível em: <http://memoria.rnp.br/newsgen/0003/cache.html >. Acesso em: 18 set. 2014.

WESSELS, Duane. Squid: The Definitive Guide. Sebastopol: O'Reilly, 2004.