UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

CAMPUS LUIZ MENEGHEL

EDNARDO PADUAN

ADMINISTRAÇÃO DE UMA REDE CORPORATIVA UTILIZANDO O WINDOWS SERVER E LINUX

Bandeirantes

2012

EDNARDO PADUAN

ADMINISTRAÇÃO DE UMA REDE CORPORATIVA UTILIZANDO O WINDOWS SERVER E LINUX

Monografia apresentada ao Curso de Sistemas de Informação da Universidade Estadual do Norte do Paraná – *campus* Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistema de Informação.

Orientador: Prof. Me. Luiz Fernando Legore do Nascimento

Bandeirantes

2012

EDNARDO PADUAN

ADMINISTRAÇÃO DE UMA REDE CORPORATIVA UTILIZANDO O WINDOWS SERVER E LINUX

Monografia apresentada ao Curso de Sistemas de Informação da Universidade Estadual do Norte do Paraná – *campus* Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistema de Informação.

COMISSÃO EXAMINADORA

_____

Prof. Prof. Me. Luiz Fernando Legore do Nascimento
UENP – *Campus* Luiz Meneghel

_____

Prof. Neimar Neltzel
UENP – *Campus* Luiz Meneghel

_____

Prof. Estevan Costa
UENP – *Campus* Luiz Meneghel

Bandeirantes, 29 de Novembro de 2012

AGRADECIMENTOS

Agradeço à minha esposa Lucimara dos Santos Paduan, que soube entender as minhas ausências durante as noites nas quais fiquei estudando e que sempre esteve ao meu lado nas horas difíceis; ao meu Orientador Prof. Fernando por sua dedicação e cooperação para que eu pudesse realizar esse projeto.

RESUMO

Em empresas onde há um grande número de computadores, há a necessidade de se controlar os acessos aos serviços providos pela mesma. Seja referente ao uso de arquivos compartilhados, *backups* e acesso à rede Internet, a qual muitas vezes é feita de forma indisciplinada e abusiva. Um PDC (controlador de domínio primário), presente em uma empresa, permite uma maior organização do parque tecnológico e da segurança da informação. Através das políticas de trabalho definidas nesse controlador, é possível atribuir diretivas de trabalhos aos usuários nele cadastrados. Além das diretivas locais essas podem ser concedidas à outras ferramentas de controle. A exemplo disso, é possível que o acesso ao conteúdo web possa ser administrado por contas existente nesse PDC, como é o caso de um servidor proxy/cache. Administrar uma rede corporativa de forma correta e responsável é reduzir prejuízos relacionados com o mal uso da rede, a qual degrada os recursos computacionais da empresa, reduz a produtividade e ainda impede drasticamente os prejuízos causados pela instalação de *software* não autorizados. Esse trabalho apresenta um estudo de caso em uma empresa local, a qual necessita organizar seu parque tecnológico, criando hierarquias de pastas compartilhadas e definindo políticas de acesso à rede Internet. Para isso objetiva-se apresentar um conjunto de ferramentas computacionais as quais possam melhor atender as necessidades da mesma oferecendo a ela, melhor custo benefício.

Palavras-chave: Active Directory, PDC, Proxy/Cache, Administração de rede.

ABSTRACT

In companies where there are a large number of computers, there is a need to control access to services provided by it. Be concerning the use of shared files, backups and access to the Internet, which is often done so undisciplined and abusive. A PDC (Primary Domain Controller), present in a company, allows for greater organization of the technological and information security. Through workplace policies defined in this controller, you can assign policies to users it works registered. Apart from these local policies may be granted for other control tools. As an example, it is possible that access to web content may be managed by existing accounts in PDC, such as a proxy / cache. Managing a corporate network correctly and responsibly is to reduce losses associated with the misuse of the network, which degrades the computational resources of the company, reduces productivity and drastically even prevents the damage caused by the installation of unauthorized software. This paper presents a case study in a local company, which needs to organize its technology, creating hierarchies of shared folders and defining policies for access to the Internet. For this objective to present a set of computational tools which can better meet the needs of the same offering her money better.

Keywords: Active Directory, PDC, Proxy / Cache, Network Administration.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

LISTA DE SIGLAS

ACL - Access Control List

AD - Active Directory

FTP - File Transfer Protocol

GPL - General Public License

HTTP - Hypertext Transfer Protocol

HTTPS - HyperText Transfer Protocol Secure

IP - *Internet Protocol*

IPX/SPX- Interwork Packet Exchange / Sequenced Packet Exchange

ISA - Industry Standard Architecture

LAN - Local Area Network

LDAP - Lightweight Directory Access Protocol

MAN - Metropolitan Area Network

MSP - Microsoft Proxy Server

NAT - Network Address Translation

NCSA - *National Center for Supercomputing Applications*

OSI - O*pen System Interconnection*

P2P - Peer to Peer (Arquitetura de Sistemas Distrituídos)

PAN - Personal Area Network

PDC - Primary Domain Controller

SARG - Squid Analisys Report Generation

SCOM - System Center Operations Manager

SCVMM *Systen Center Virtual Machine Manager*

SMTP - Simple Mail Transfer Protocol

TCP - Transmission Control Protocol

TCP/IP - *Transmission Control Protocol/Internet Protocol*

TI - Tecnologia da Informação

UDP - User Datagran Protocol

VM - Virtual Machine

VMM - Virtual Machine Monitor

WAN - Wide Area Network

WLAN - Wireless Local Area Network

XML - Extensible Markup Language

1 INTRODUÇÃO

Em um ambiente corporativo, praticamente todas as empresas possuem equipamentos computacionais, *desktops, laptops*, celulares, *tables* entre outros, conectados a uma rede. Tais equipamentos podem ser tanto de propriedade da empresa quanto de uso pessoal. Executivos, visitantes e até mesmo os próprios funcionários de uma empresa, em algum momento necessitar em fazer o uso da rede. Conceder o acesso aos recursos tecnológicos dessa empresa sem que haja nenhum cuidado, pode ser perigoso. Qualquer pessoa sem nenhuma identificação poderá usar tais recursos, tanto para fins lícitos como ilícitos. A responsabilidade nesse caso é do departamento de TI (Tecnologia da Informação), o qual é o departamento responsável pela administração, gerenciamento, suporte à todo o parque tecnológico. Segundo Percília (2012).

> [..]a empresa pode monitorar os passos do funcionário, desde que o mesmo esteja ciente disso. A ocorrência mais comum é o monitoramento do histórico de navegação, tendo unicamente o objetivo de garantir a produtividade e impedir a contaminação por vírus ou o extravio de documentação e informações confidenciais. Com a crescente utilização da internet em práticas ilícitas, as empresas estão dispensando um cuidado maior para que esse tipo de prática não ocorra em suas dependências[..] (Percília (2012).

Manter os índices de produtividade de forma a minimizar a dispersão por parte de seus funcionários em navegação por sítios não condizentes as práticas empresariais é sempre uma tarefa difícil e polêmica. Para isso torna-se necessário, aplicar regras as quais impeçam o uso abusivo de determinados conteúdos da rede Internet. Manter uma rede constantemente monitorada, tanto para o compartilhamento de arquivos quanto de conteúdo *web*, é uma prática cada vez mais frequente também em pequenas empresas. A fim de obter uma base legal, as corporações têm adotado a estratégia de embasarem-se em uma política de segurança, notificando o usuário através de um termo de compromisso. Além disso, cada empresa adota sua política de segurança e a forma de acesso à rede

empresarial, utilizando para tanto, uma série de ferramentas computacionais capazes de bloquear e relatar a ocorrência de eventos que venham a ferir as políticas adotadas.

Neste trabalho, é apresentado um modelo para o controle de acesso, tanto de conteúdo *web* como os serviços de diretórios em uma empresa local. Para tanto foram feitas análises preliminares, buscando investigar as necessidades da empresa de forma que se pudesse elaborar um conjunto de ferramentas e soluções capazes de atender a realidade do parque tecnológico investigado. Nesse caso, foram analisados a jornada de trabalho dos funcionários, o consumo da banda de rede Internet, o número de programas instalados nas máquinas locais, os quais não tiveram autorização concedida pelo administrador. Além disso, foram ainda quantificados as máquinas que entraram em manutenção em função da contaminação por vírus.

Ao fim da investigação um modelo utilizando algumas das principais ferramentas que permitisse melhor administrar foi apresentado aos administradores do parque tecnológico da empresa estudada. A implementação foi feita em apenas parte da empresa, a qual serviu como ambiente de teste. A partir disso, espera-se novas discussões por parte dos dirigentes da empresa para que novas regras possam ser implementadas bem como a efetiva implantação do modelo em todas as dependências da empresa.

1.1 Justificativa

Administrar uma rede ainda que pequena, permite-se aumentar a produtividade da mesma, reduzir gastos com a manutenção de equipamentos e principalmente dar segurança as informações. O uso de ferramentas computacionais destinadas a gerenciar um parque tecnológico permite relatar o real uso da rede. Dessa forma, os investimentos nesse setor passam a ser coerentes com a realidade da empresa, ou seja, a redução do mau uso da rede

implica diretamente em melhorias na produtividade e aumenta a vida útil dos equipamentos.

1.2 Objetivo Geral

Reduzir perdas, tanto de produtividade como na manutenção de equipamentos, em uma rede corporativa, utilizando um servidor o qual possa controlar parte dos processos referentes ao controle de acesso ao conteúdo web e aos diretórios. Além de propor um modelo que juntamente com algumas ferramentas computacionais possa auxiliar no processo de organização e políticas de uso da rede.

1.2.2 Objetivos específicos

- Analisar e planejar uma estrutura de gerência dos serviços de diretório e do conteúdo *web* em um ambiente corporativo;
- Integrar as ferramentas de controle utilizadas de forma a construir um sistema que possibilite uma boa administração;
- Apresentar um modelo para a administração do parque tecnológico de uma empresa local.
- Avaliar os resultados obtidos após a implantação das ferramentas.

1.3 Metodologia

Para o encaminhamento metodológico elegeu-se a modalidade Estudo de Caso, por configurar-se como um método específico de pesquisa de campo, Gil (1991). Nesta perspectiva, a presente pesquisa tomou como caso, uma empresa local atuante na área de *designer* gráfico, fotografias e cobertura de eventos, o qual utiliza recursos tecnológicos computacionais como ferramenta de trabalho diário. Autorizado por um dos diretores da empresa investigada, foram realizadas entrevistas com diversos funcionários, dentre eles o responsável pelo setor de TI. Nessas entrevistas foram levantados subsídios suficientes para que o cenário a ser implementado pudesse ser delineado. A partir dai, tornou-se possível definir quais seriam as ferramentas tecnológicas a serem utilizadas.

Para a implementação desses recursos tecnológicos, foram levados em consideração as atuais máquinas em uso, além da preocupação em se aproveitar aquilo que o parque tecnológico já dispunha, dado a solicitação de se fazer mais com aquilo que ela já possui. Essa implementação consiste na montagem de um servidor de teste, trabalhando em paralelo com a atual estrutura existente, de forma a oferecer esses novos recursos a somente parte da rede. Objetiva-se nessa abordagem, obter uma avaliação dos recursos atuais utilizados.

1.5 Organização do Trabalho

Definido os objetivos e, comprovada a relevância temática, pela justificativa apresentada, o presente estudo está organizado da seguinte forma: no Capítulo 2, é apresentada a fundamentação teórica. O Capítulo 3 descreve as ferramentas utilizadas na investigação. O Capítulo 4 apresenta as análises do parque tecnológico da empresa estudada e o modelo escolhido para a implementação do trabalho proposto. O Capítulo 5 apresenta a conclusão sobre resultados apresentados. Capítulo 6 a proposta de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Aspecto de segurança

Cada vez mais as empresas possuem informações sigilosas disponíveis em seus computadores, fazendo com que certos cuidados sejam necessários, a fim de protegê-las, como limitar o acesso físico e lógico aos computadores, através de mecanismos de segurança. Essa preocupação torna-se ainda maior com a popularização da Internet nas empresas. Informações não devidamente protegidas podem ser acessadas ou alteradas utilizando os recursos da rede.

Para tornar uma rede mais segura e confiável, deve-se estar atento às principais ameaças que podem comprometer a integridade das informações de uma empresa. Ao contrário do que se pensa, nem sempre o principal inimigo está fora da rede, mas sim dentro dela.

Segundo Monteiro (2002), as principais funções de segurança são:

- **Autenticidade –** Verifica se a pessoa com quem está se trocando informações sigilosas é realmente quem deveria ser;
- **Confidencialidade –** Limita o acesso a informações, geralmente através do uso de criptografia;
- **Integridade –** Assegura que os dados não serão alterados durante uma transmissão;
- **Controle de acesso –** Limita o acesso e a utilização de recursos apenas a pessoas autorizadas;
- **Disponibilidade –** Mantém os recursos disponíveis, mesmo em caso de ataques;
- **Não-repúdio –** Impede que uma entidade (computador, pessoa, etc.) envolvida em uma transação negue a sua participação no evento.

2.2 Redes de computadores

A necessidade de interconexão dos equipamentos computacionais permitiu que fossem feitos compartilhamentos de recursos de *hardware* e *software.* Tais compartilhamentos permitiu-se as trocas de informações entre usuários, criando assim, um ambiente propício para o desenvolvimento das redes de computadores (SOARES, 1995).

Segundo Tanenbaum (1997) uma rede de computador é definida como sendo um conjunto de dispositivos computacionais autônomos interconectados, trocando informações entre si, através de diversos meios de acesso. A exemplo disso, fios de cobre, fibras ópticas, sinais de rádio frequência, etc. Esse autor salienta ainda que,

> [...] uma empresa pode ter computadores separados para monitorar a produção, controlar os estoques e elaborar a folha de pagamento. Inicialmente, cada um desses computadores funciona isolado dos outros, mas, em um determinado momento, a gerência deve ter decidido conectá-los para poder extrair e correlacionar informações sobre a empresa inteira [...] a questão aqui é o compartilhamento de recursos, e o objetivo é tornar todos os programas, equipamentos e especialmente dados ao alcance de todas as pessoas na rede [...]. Um exemplo óbvio e bastante disseminado é um grupo de funcionários de um escritório que compartilham uma impressora comum [...]. (TANENBAUM, 1997, p. 3).

Pinheiro (2005), considera também que em redes de computadores é necessário garantir que todos os recursos de informação sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, a rede deve possuir meios de transmissão eficientes, regras básicas (protocolos) e mecanismos capazes de garantir o transporte das informações entre os seus elementos constituintes.

Atualmente, com a importância cada vez maior de se dispor de acesso a informações e facilidades de comunicação, as redes de computadores estão projetadas para crescer indefinidamente, sendo a Internet o melhor exemplo disso.

Tipos de redes:

- **Rede local** (LAN - *Local Area Network*) - tem o objetivo de interligar computadores localizados na mesma sala, edifício ou campus, possuindo uma distância máxima de alguns quilômetros entre as estações mais distantes. Normalmente as redes locais possuem uma taxa de transferência de dados maior do que 1 Mbps e são propriedade de uma única organização;

- **Rede metropolitana** (MAN - *Metropolitan Area Network*) - tem o objetivo de interligar computadores dentro da mesma cidade e arredores, possuindo distâncias até aproximadamente 100 Km;

- **Rede de longa distância** (WAN - *Wide Area Network*) - tem o objetivo de interligar computadores distantes um do outro, ou seja, computadores localizados em cidades, estados ou mesmo países diferentes. Normalmente as redes de longa distância são oferecidas por empresas de telefonia, não possuindo uma faixa de velocidades específica.

- **Rede local sem fios** (WLAN - *Wireless Local Area Network*) é uma rede que permite cobrir o equivalente de uma rede local de empresa, ou seja, um alcance de uma centena de metros. Permite ligar os terminais presentes na zona de cobertura.

- **Rede de área pessoal** (PAN- *Personal Area Network**)*** **–** Também é designada como redes de área pessoal, é o tipo de rede onde é utilizada tecnologias de rede sem fios para interligar os mais variados dispositivos (ex. computadores, smartphones, tablets etc) em uma área muito reduzida.

Na Internet todas as atividades de comunicação são governadas por protocolos de comunicação. Por exemplo, (i) protocolos fim-a-fim, os quais

garantem a integridade dos dados transmitidos através de mecanismos de reconhecimento e retransmissão; (ii) protocolos de roteamento os quais determinam o caminho de um pacote de dados da fonte até o destino; (iii) protocolo de *hardware,* o qual através de um adaptador de rede controla o fluxo de *bits* sobre os fios que interligam dois dispositivos computacionais.

Os exemplos citados utilizam o protocolo TCP (*Transmission Control Protocol*) que integra um serviço de controle de fluxo. Nesse serviço, é assegurado que nenhum dos lados da comunicação envia pacotes rápido demais, pois uma aplicação em um lado pode não conseguir processar a informação na velocidade que está recebendo. Além disso, um serviço ajuda a prevenir ocorrência de congestionamentos na rede (TORRES, 2001). Denominado como serviço orientado a conexão, o cliente e o servidor trocam pacotes de controle entre si antes mesmo deles enviarem os pacotes de dados. O procedimento onde se estabelece os parâmetros de conexão é denominado de *handshaking.* Nesse caso, o serviço de transferência é considerado garantido, ou seja, é assegurado que os dados trocados são livres de erros, ou seja, caso algum erro de transmissão ocorra é solicitado a retransmissão dos pacotes que não foram recebidos ou apresentaram erros. (SANTOS, 2005).

Outro serviço é dito não orientado a conexão quando não há *handshaking*; ou seja, quando um lado de uma aplicação quer enviar pacotes ao outro lado sem a necessidade de garantia de entrega dos pacotes. Como o serviço não garantido, também não há reconhecimento, de forma que a fonte nunca tem certeza que o pacote foi recebido pelo destinatário. Como o serviço é mais simples, os dados podem ser enviados mais rapidamente. O protocolo responsável por esse tipo de conexão tem o nome de UDP (*User Datagram Protocol*).

As informações trafegadas na rede são feitas na forma de pacotes de dados, chamados de datagramas (TORRES, 2001). O protocolo denominado IP *(Internet Protocol)* é o responsável por estabelecer o caminho por onde seguirá cada datagrama dentro da rede. Para isso cada computador necessita de um

endereço conhecido como endereço IP. Assim, para que uma mensagem seja enviada de uma máquina para outra, ambas devem possuir um endereço IP.

2.3 Camadas de protocolos

Para que os dispositivos de redes possam se comunicar é necessário que eles falem a mesma “língua”, ou seja, utilizem um mesmo protocolo para sua comunicação. Vários protocolos foram criados para transmissão de dados em uma rede. Dentre os mais comuns, pode-se citar: TCP/IP, o *NetBIOS Extended User Interface* (NetBEUI) e o (IPX/SPX) *Interwork Packet Exchange / Sequenced Packet Exchange.*

Como inicialmente para as redes de computadores diversos fabricantes trabalharam de forma separada no desenvolvimento de suas tecnologias, muitas delas incompatíveis entre si. Nesse caso, tornou-se necessário de fosse estabelecido algum tipo de padronização permitindo assim que houvesse uma integração entre as diversas tecnologias. A arquitetura escolhida para essa finalidade foi a TCP/IP.

Arquitetura TCP/IP

O TCP/IP é um conjunto de protocolos de interconexão de sistemas, executado em ambiente aberto, utilizando uma arquitetura de quatro camadas, definidas a seguir como:

- **Camada de Aplicação:** fornece a interface do usuário de rede na forma de aplicativos e serviços de rede;
- **Camada de Transporte:** responsável por organizar as mensagens recebidas de camadas mais altas nos segmentos, por controlar os erros e por controlar o fluxo de fim-a-fim;

- **Camada de Rede:** responsável pelo endereçamento dos equipamentos e pela transmissão (ou roteamento) dos dados em redes diferentes;
- **Camada de Interface de rede:** responsável por controlar o fluxo de dados e organizar os bits da camada física.

O protocolo IP

Este protocolo é um dos mais importantes da arquitetura TCP/IP e é utilizado para rotear os pacotes, para que estes possam chegar com rapidez ao seu destino e endereçar cada equipamento de rede, de modo que eles possuam um único número capaz de identificá-los. Este número é composto por 32 bits, representado por quatro campos de números decimais inteiros, que variam de 0 a 255, conforme a Figura 2.1.3.

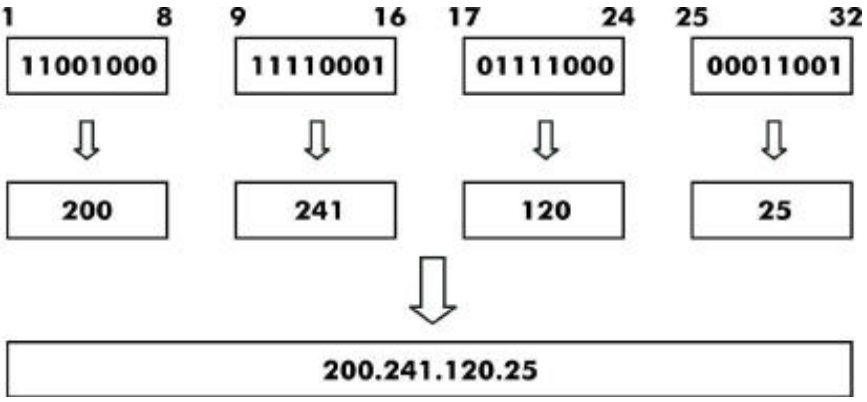


Figura 2.1: Endereçamento IP
Fonte: CYCLADES, 2000, p. 68.

Conjunto de Protocolos TCP/IP

O conjunto de protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*) é um padrão industrial de protocolos destinados a redes geograficamente distribuídas, ou WANs, sendo as principais peças da arquitetura Internet. Essa arquitetura tem por objetivo a interligação de computadores, não

importando em qual tipo de rede os mesmos estejam conectados, a qualquer outro computador da rede mundial de computadores. Para interligar redes distintas a arquitetura Internet usa uma máquina como ponto de ligação entre as redes, sendo está conhecida como roteador (ou *gateway*). Esse equipamento é o responsável pelo roteamento das mensagens na malha que forma a rede Internet.

2.4. Serviço de Diretório

Serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na rede, isso significa que é uma maneira de organizar e simplificar o acesso aos recursos de sua rede centralizando-os; Bem como, reforçar a segurança e dar proteção aos objetos da base de dados contra intrusos, ou controlar acessos dos usuários internos da rede. Permite aos administradores de rede gerenciar o acesso dos usuários e sistemas a esse recurso, servindo de abstração entre os usuários e esses recursos.

2.5. Protocolo LDAP

O LDAP(Lightweight Directory Access Protocol),é um protocolo para atualizar e pesquisar diretórios rodando sobre o protocolo TCP/IP e segue o modelo de árvore de nós, onde cada nó representa um conjunto de atributo com seus valores. Disponibiliza um servidor e várias ferramentas para auxiliar nas consultas, inclusão, remoção e sincronização de informações de um é um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP.

O LDAP, é um protocolo suportado em várias distribuições Linux que visa autenticar, localizar e gerir utilizadores e recursos numa rede TCP/IP de Internet. A informação recolhida por este servidor é depois armazenada de forma

hierárquica. Por sua vez, o AD é um software concebido com a mesma finalidade do LDAP mas direcionado para o ambiente Windows.

A integração de LDAP com AD permite a uma organização usufruir de um sistema de autenticação centralizado que se adapta aos diferentes ambientes e sistemas operativos em funcionamento.

3. FERRAMENTAS UTILIZADAS

Nesse Capítulo são abordadas as ferramentas computacionais, que foram utilizadas para a construção de uma solução a qual permitirá oferecer uma melhor gerência da rede, para a empresa utilizada nesse objeto de estudo.

3.1 *Active Directory*

O AD (*Active Directory)* nasceu da necessidade de se criar uma estância ativa, a fim de administrar e gerenciar redes híbridas e sistemas distribuídos. Esta ferramenta disponibiliza ao usuário uma conta, na qual, pode-se utilizar de todos os recursos acessíveis pelo sistema de controle do domínio, como contas de acesso a redes, acesso aos sistemas de gestão, conta de e-mail, entre outros serviços. O sistema foi baseado na versão Windows 2000 Server, e oferece as seguintes funcionalidades: contas de acesso à rede corporativa, conta de e-mail, inclusão de usuários em grupos de trabalho, definir perfis de acesso para os usuários que fazem parte de um determinado grupo na rede, autenticação de usuários. Todos esses dados são armazenados em um banco de dados a fim de gerenciar todas as atividades realizadas por usuários em uma rede de computadores, independente do seu porte. Os principais componentes de um servidor AD são segundo (SANCHES, 2008):

- Domínio;
- *Workgroups* (Grupo de Trabalho);
- *Tree* (Árvore); *e*
- *Forest* (Floresta).

A ferramenta AD não só tem um papel fundamental na infra-estrutura de redes, como também faz o levantamento e a criação de toda a estrutura

lógica/física e design da organização, bem como no auxilio à tomada de decisões por parte dos gerentes de TI e administradores na implementação de planos/projetos de redes (SANCHES, 2008). Esse serviço de diretório é pertencente as redes Microsoft Windows.

O AD mantém dados como contas de usuários, impressoras, grupos, computadores, servidores, recursos de rede, etc. Ele pode ser totalmente escalonável, aumentando conforme a nossa necessidade. Esse serviço de diretório, é composto por objetos, ou seja, todo recurso da nossa rede é representado como um objeto no AD. Esses objetos possuem propriedades o que são chamados de atributos dos objetos. A base de dados do AD é um arquivo chamado NTDS.dit, onde todos os recursos são armazenados no mesmo.

Os objetos do AD são divididos em três categorias: recursos físicos, serviços disponíveis e contas. Na categoria dos recursos físicos estão todos os equipamentos disponíveis na rede tais como o servidor, as estações de trabalho e também as impressoras de rede. A segunda categoria envolve os serviços disponíveis na rede como o correio eletrônico e o servidor de impressão. O terceiro grupo é o que está relacionado aos usuários ou contas. É aqui que o administrador da rede define quem pode utilizar a rede e quais recursos (físicos e serviços) estarão disponíveis para cada usuário. Além disso, o administrador pode definir quais serão os grupos de usuários (por exemplo, Diretoria, Departamento Financeiro, Almoxarifado), cada um características e capacidades diferentes e que podem ser atribuídas muito facilmente a qualquer usuário já existente. De forma similar, a segurança também é um atributo inerente ao AD. Do ponto de vista do gerenciamento, administrador da rede tem acesso a todos os objetos do diretório por meio de uma única conta. O acesso à infra-estrutura e aos serviços disponíveis por parte dos demais usuários somente será possível após a sua autenticação no AD.

3.2 Servidor Proxy/Cache

É uma aplicação instalada em um servidor o qual funciona como intermediário entre um navegador Web e a Internet. Um servidor proxy ajuda a melhorar o desempenho na Web, armazenando uma cópia das páginas utilizadas com maior frequência. Quando um navegador solicita a requisição de uma página que está armazenada na coleção do servidor proxy (o cache), ela é disponibilizada pelo servidor proxy, o que é mais rápido do que acessar a Web. Os servidores proxy também ajudam a melhorar a segurança porque podem filtrar alguns tipos de conteúdo da Web, como por exemplo softwares mal-intencionados. Alguns dos servidores proxys conhecidos são: (MSP) Wingate, Microsoft Proxy Server, Polipo e Squid. Nesse trabalho foi optado pelo uso do Squid como servidor proxy por ser este uma ferramenta livre e robusta, e podendo esta ser instalada na plataforma Linux, o qual é nosso ambiente virtualizado.

Segundo (WESSELS, 2004), o squid trata-se de uma ferramenta capaz de aceitar requisições *HTTP* (Hypertext Transfer Protocol) e *HTTPS* (HyperText Transfer Protocol Secure) de clientes e capaz de efetuar requisições *HTTP*, *FTP* e *Gopher* para servidores, além de implementar várias características comumente úteis em ambientes corporativos:

- Controle de banda no acesso a Internet;
- Redução do tempo de carga de páginas na Internet;
- Coleta de estatísticas do tráfego de acesso a Internet proveniente da rede privativa;
- Bloqueio de sítios considerados de conteúdo inapropriado;
- Garantia de que somente os usuários autorizados terão acesso a Internet;
- Conversão de requisições *HTTPS* de um lado em *HTTP* do outro lado;

- Proteção de máquinas internas de acessos externos uma vez que as requisições a sítios externos são efetuadas pelo *Proxy*.

O *Squid* foi escrito com a preocupação de ser portável, assim ele funciona na maioria dos sistemas operacionais *Unix*, como: *Linux, BSD/OS, FreeBSD, NetBSD, OpenBSD, Solaris, HP-UX, OSF/DUNIX/TRU-64, Mac OS/X, IRIX e AIX, além de funcionar em ambientes Microsoft Windows(WESSELS, 2004).*

Os requisitos de *hardware* necessários para sua implantação são, em geral, modestos. Mesmo assim, memória é o recurso mais importante, uma vez que pouca quantidade de memória degrada consideravelmente a performance. Espaço em disco é outro fator importante, pois mais espaço em disco significa mais objetos em *cache* e, portanto, menores tempos de resposta. O fato de ser *Proxy* permite ao *Squid* intermediar as transações entre clientes e servidores. Ele aceita requisições dos clientes, processa e as encaminha ao servidor desejado. Tais requisições podem ser registradas, rejeitadas e modificadas antes do encaminhamento. Além disso, por funcionar como *Cache*, a ferramenta armazena localmente conteúdo de páginas acessadas recentemente com o objetivo de reutilizá-las, aumentando assim a performance pela diminuição do tempo de resposta. A característica de *Cache* é passível de desativação, o que não ocorre com a função de *Proxy*, por ser a essência do *Squid*. Na Figura 3.2 é mostrado como são feitos os acessos através da Proxy.

A aplicação permite ainda a implementação de várias funcionalidades através do uso de *ACLs (Access Control List)*. Esta implementação permite a criação de listas capazes de filtrar desde simples domínios até tipos de conteúdo especificados. Outro ponto forte é: a capacidade de trabalhar com diferentes módulos de autenticação, como *NCSA (National Center for Supercomputing Applications),* autenticação baseada em *LDAP* e autenticação utilizando *Kerberos*. Além disso, oferece avançadas opções de armazenamento de cache em disco além da interceptação de pacotes *HTTP*.

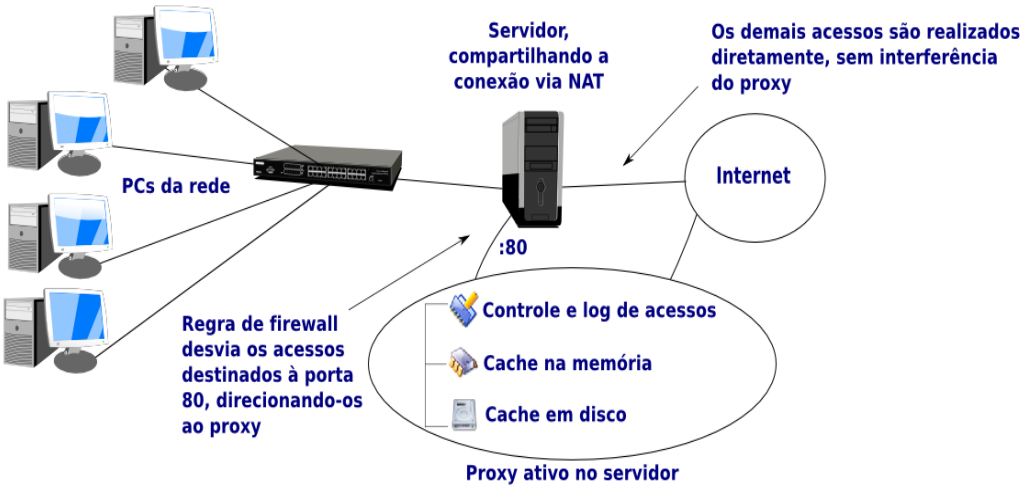


Figura 3.2 – Funcionamento de um Servidor Proxy

3.3 Relatórios de Acessos

O *SARG* (*Squid Analisys Report Generator*) é um analisador de logs do *Squid* capaz de informar ao administrador em um formato bastante agradável por onde os usuários estão navegando na Internet. A ferramenta lê os logs do *Squid* por meio de um agendamento que deve ser configurado pelo administrador. Normalmente executado diariamente no mesmo horário. É gerado um arquivo em formato texto contendo informações úteis sobre a navegação na Internet durante aquele período. Um *script* é executado com o objetivo de mostrar as informações do arquivo *txt* em formato *Web* conforme pode ser visto na Figura 3.3.

- Está disponível em mais de vinte línguas, dentre as quais: português, inglês e espanhol;

- É capaz de ler logs do *ISA Server (* gateway integrado de segurança de borda que ajuda a proteger seu ambiente de TI das ameaças baseadas em Interne), servidor proxy da *Microsoft*;

- É possível customizar os relatórios com informações consideradas relevantes como por exemplo: sítios mais visitados, usuários que visitaram determinados sítios, sítios visitados por determinado usuário, etc.

Embora não haja uma obrigatoriedade do SARG como analisador de logs de acesso, pois além dele outros podem ser utilizados, como é o caso do FreeSA, e o WebAlizer, o Sarg foi escolhido por se tratar de uma ferramenta a qual mostrou-se com mais recursos, embora esta seja mais lenta quanto os relatórios tornam muito grandes.

NUM		USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
1		192.168.0.31	2.40K	165.01M	83.69%	0.79%	99.21%	03:09:38	11.37M	66.13%
2		192.168.0.41	1.60K	12.75M	6.47%	14.12%	85.88%	00:10:45	645.53K	3.75%
3		192.168.0.36	609	3.35M	1.70%	15.49%	84.51%	00:02:27	147.36K	0.86%
4		192.168.0.38	209	3.32M	1.69%	5.93%	94.07%	00:17:26	1.04M	6.08%
5		192.168.0.34	365	2.19M	1.11%	61.48%	38.52%	00:05:44	344.48K	2.00%
6		192.168.0.44	276	2.05M	1.04%	6.46%	93.54%	00:02:51	171.04K	0.99%
7		192.168.0.33	119	1.62M	0.82%	48.50%	51.50%	00:06:32	392.54K	2.28%
8		adriana	116	1.56M	0.79%	0.12%	99.88%	00:03:01	181.22K	1.05%
9		helder	197	1.54M	0.78%	2.27%	97.73%	00:15:43	943.36K	5.48%
10		192.168.0.32	154	1.21M	0.61%	83.64%	16.36%	00:01:21	81.48K	0.47%
11		192.168.0.4	496	821.81K	0.42%	0.29%	99.71%	00:07:43	463.59K	2.69%
12		cristiano	15	480.90K	0.24%	1.39%	98.61%	00:01:38	98.83K	0.57%
13		rodrigo	24	305.00K	0.15%	0.53%	99.47%	00:16:59	1.01M	5.92%
14		192.168.0.45	73	238.62K	0.12%	9.68%	90.32%	00:00:32	32.37K	0.19%
15		administrador	2	230.53K	0.12%	0.00%	100.00%	00:00:04	4.01K	0.02%
16		192.168.0.12	1	228.27K	0.12%	0.00%	100.00%	00:00:00	0	0.00%
17		edson	239	149.76K	0.08%	10.33%	89.67%	00:00:33	33.96K	0.20%
18		renato	7	46.88K	0.02%	0.00%	100.00%	00:00:04	4.88K	0.03%
19		192.168.0.35	3	13.69K	0.01%	10.99%	89.01%	00:03:31	211.05K	1.23%
20		vanessa	7	4.76K	0.00%	0.00%	100.00%	00:00:04	4.21K	0.02%
21		192.168.0.43	2	2.13K	0.00%	0.00%	100.00%	00:00:01	1.21K	0.01%
22		silvestre	2	1.75K	0.00%	0.00%	100.00%	00:00:01	1.68K	0.01%
23		sandra	2	1.00K	0.00%	0.00%	100.00%	00:00:00	726	0.00%
		TOTAL	6.92K	197.17M		3.65%	96.35%	04:46:47	17.20M	
		MÉDIA	301	8.57M				00:12:28	748.17K	

Figura 3.3 Estatísticas de acesso no *SARG*.

O *SARG* é uma ferramenta simples e de fácil implementação e manutenção, que se integra muito bem ao *Squid* (CISNEIRO 2005). Os relatórios gerados por esta aplicação são importantes para o corpo gerencial da corporação uma vez que os dados estatísticos produzidos podem servir como embasamento para tomada de decisão.

3.4 Virtualização

As máquinas virtuais (virtual machines – VM) foram idealizadas e introduzidas nas décadas de 50 e 60, com a finalidade de permitir o *time-sharing* (compartilhamento de tempo) de equipamentos que eram muito caros e ficavam, por vezes, ociosos por muito tempo. A principal proposta do compartilhamento de hardware era prover a máxima utilização dos equipamentos Mainframe da IBM de forma segura, conseguindo assim aperfeiçoar o uso do hardware entre vários usuários (FEDOROVA, 2003).

Virtualização é uma tecnologia que faz um computador físico funcionar como se fosse mais computadores onde cada computador “virtualizado” possui a mesma arquitetura básica como se fosse um computador físico. Existem várias maneiras de se fazer isso, e cada um tem os seus prós e contras (MARSHALL, 2006).

De acordo com Moreira (2006) o problema de se utilizar um servidor para disponibilizar cada serviço, é que ele aproveita mal os recursos das máquinas. Em média, os servidores utilizam somente de 5% a 10% da sua capacidade. Com o objetivo de reduzir os custos de administração e manutenção e centralizar o trabalho dos gerentes de tecnologia, as empresas apostaram em um novo conceito: utilizar equipamentos mais robustos, com mais recursos de processamento e espaço em disco, para hospedar as diversas aplicações da empresa, prática batizada de consolidação de servidores.

Para Marshall (2006), virtualização é um conceito que permite dividir ou partilhar os recursos de um computador por vários ambientes simultaneamente. Esses ambientes podem interoperar mesmo sem conhecer uns aos outros. Um único ambiente pode, ou não, saber o que está sendo executado em um ambiente virtual. Esses ambientes são mais comumente conhecidos como máquinas virtuais (VMs). VM será quase sempre um local onde está instalado um sistema operacional (por exemplo, Linux, Windows) e são conhecidos como sistemas operacionais do cliente. Instruções para uma VM é geralmente transmitida

diretamente para o hardware físico permitindo que o ambiente funcione mais rápido e eficiente do que uma emulação.

Os principais aplicativos de virtualização que são instalados sobre um SO são o VMWare Server, O Microsoft Virtual Server e o Citrix XenServer Express. Todos são free. Como sistemas de virtualização bare-metal existem o VMWare ESX Server (VMWare Infrastructure), Citrix XenServer Enteprise Edition e o Oracle VM. Desde então, as tecnologias de virtualização vêm sendo aprimoradas cada vez mais, tendo em vista a grande aceitação por parte das empresas e dos usuários. Em pesquisa realizada pelo IDC Brasil, em Setembro de 2006, 80% das grandes e médias empresas brasileiras investiram em virtualização (INFO CORPORATE, 2008).

Como a virtualização desassocia o sistema operacional do hardware, traz ferramentas novas e úteis . A virtualização permite que um operador controle o uso da CPU, memória, armazenamento e de outros recursos do sistema operacional do convidado, de forma que cada convidado receba apenas os recursos que precise. Este controle elimina o risco de um processo que consuma toda a memória disponível ou a CPU. Permite também que a equipe de TI atenda os requisitos de nível de serviço de aplicações específicas ajustando as alocações de recursos.

Como o convidado não está atrelado ao hardware, é possível transferir dinamicamente um sistema operacional de uma máquina física para outra. E quando o sistema operacional de um determinado convidado começar a consumir mais recursos durante um período de pico, o operador pode transferir esse convidado para um outro servidor com menos demanda. Esse tipo de flexibilidade muda o conceito tradicional de aprovisionamento do servidor e de planejamento de capacidade. Nos ambientes virtualizados é possível tratar os recursos computacionais como CPU, memória e armazenamento como um cache de recursos e aplicações que podem ser facilmente realocados para receber os recursos necessários, quando necessário.

3.4.1 Hyper-v

De acordo com a própria Microsoft®, o Hyper-V do Windows Server é o recurso de virtualização permite que as organizações de TI reduzam custos, melhorem a utilização do servidor e crie uma infraestrutura de TI mais dinâmica. Além disso, o Hyper-V fornece maior flexibilidade devido às capacidades dinâmicas, confiáveis e escalonáveis de plataforma combinadas com um único conjunto de ferramentas integradas de gerenciamento para gerenciar recursos físicos e virtuais, permitindo, assim, a criação de um *datacenter* ágil e dinâmico e a obtenção de progressos por meio de sistemas dinâmicos de auto-gerenciamento.

Por ser baseado em hipervisor, o Hyper-V é apenas uma pequena camada de programa entre o hardware e as máquinas virtuais que gerencia todo o acesso aos recursos físicos, sem perdas significativas de desempenho. O Hyper-V é baseado em partições lógicas que são isoladas umas das outras. É necessário ter pelo menos uma partição pai que possui acesso privilegiado e direto aos recursos físicos, capaz de criar partições filhas. Estas por sua vez, não possuem acesso direto aos recursos físicos e não controlam interrupções reais, possuindo apenas uma visão virtual dos recursos.

Alguns motivos para o uso desta tecnologia, conforme segue abaixo:

- **Alta disponibilidade com um custo menor;** Se valendo dos recursos de *cluster* das edições Windows Server 2008 Enterprise e Datacenter, o Hyper-V suporta alta disponibilidade para as máquinas virtuais, os recursos de balanceamento de carga de rede e *clustering* suportam o aumento da disponibilidade, reduzindo a indisponibilidade planejada e não planejada e ajudando a melhorar a continuidade dos negócios, o que é muito importante, uma vez que uma tecnologia sempre é implementada visando a melhoria dos negócios.

- **Reduz custos de Infraestrutura;** Ao consolidar múltiplas cargas de trabalho em uma única plataforma de *hardware*, a empresa reduzirá custos com equipamentos, consumo elétrico e espaço físico. As políticas de licenciamento flexíveis de virtualização permitem que as organizações implantem uma solução de consolidação que atenda melhor as necessidades.
- **Minimiza o tempo de indisponibilidade com uma migração rápida e eficaz;** Indisponibilidade é uma palavra que não é bem vista no mundo dos negócios. O Hyper-V permite que migrar rapidamente uma máquina virtual em execução de um sistema de hospedagem física para outro, com o tempo de indisponibilidade mínimo. O que pode ser um ponto a favor desta tecnologia.
- **Segurança e a confiabilidade;** Segurança faz parte do dia-a-dia do mundo corporativo, ter uma ferramenta que proporcione segurança e confiabilidade é um fator muito importante para os negócios. A arquitetura de hypervisor micro-kernelizado do Hyper-V foi projetada para minimizar a superfície de ataque e aumentar a segurança, particularmente no Hyper-V com uma função de núcleo do servidor. O Hypervisor não contém drivers de dispositivos ou código de terceiros, promovendo uma base mais estável, leve e segura para execução das máquinas virtuais, especialmente quando comparada às plataformas de virtualização baseadas em um hypervisor monolítico.
- **Reduz o tempo de suporte com um gerenciamento integrado;** Com o Hyper-V, não se precisa criar uma infraestrutura de gerenciamento separada para o seu ambiente virtual. O Hyper-V foi projetado para ter uma ótima integração com as ferramentas de gerenciamento da Microsoft, como o SCVMM (System Center Virtual Machine Manager) e o SCOM (System Center Operations Manager), e ainda ferramentas de gerenciamento de terceiros. Isso permite que você gerencie todos os recursos físicos e virtuais através de um único console.

3.4.2 Oracle Virtual Box

VirtualBox é um software de virtualização desenvolvido pela Oracle que, visa criar ambientes para instalação de sistemas distintos. Criado pela empresa Innotek, inicialmente oferecia uma licença proprietária, existia uma versão do produto para uso pessoal ou de avaliação sem custo. Em Janeiro de 2007 foi lançado a versão VirtualBox OSE (Open Source Edition) com a licença GPL (General Public License), versão 2. Em Fevereiro de 2008 a empresa Innoteck foi adquirida pela Sun Microsystems. No dia 20 de Abril de 2009 a Oracle compra a Sun Microsystems e todos o seu produtos, incluindo o VirtualBox.

O software tem um desenho extremamente modular com interfaces de programação internas bem definidas e um desenho cliente/servidor. Isso torna fácil o controle de várias interfaces de uma só vez. Por exemplo: pode iniciar uma máquina virtual em uma máquina típica virtual de interface gráfica e, em seguida, controlar essa máquina a partir da uma linha de comando, ou possivelmente remotamente. As definições de configuração de máquinas virtuais são armazenados em XML e são totalmente independentes das máquinas locais. Por isso, as definições podem ser facilmente transferidas para outros computadores.

4. DESENVOLVIMENTO

Para o desenvolvimento desse trabalho, foi inicialmente feito uma análise daquilo que a empresa já possuía. Analisou-se o consumo de banda em determinado período, bem como a quantidade de máquinas que foram para manutenção e o uso das portas, onde se buscou detectar tráfego de rede P2P (formato de rede de computadores em que a principal característica é descentralização das funções convencionais de rede, onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo).

4.1 Análise do Parque Tecnológico da Empresa

A empresa na qual foi feita a análise das necessidades de administração de redes, opera no ramo de confecção e vendas de álbuns de eventos para formaturas. A empresa é dividida em vários setores como: administração, financeiro, produção, suporte ao cliente, compras e vendas, almoxarifado, laboratório de seleção de fotos, contratos, recursos humanos, controle de frota, recepção e sala de vídeo conferência. Essa empresa dispõe atualmente de 42 computadores interligados por cabos e rede sem fio os quais utilizam um determinado *software* para a gestão dos contratos e serviços a serem realizados dentro da linha de produção. O *software* usado para esse serviço é uma aplicação desktop o qual utiliza como banco de dados, o Microsoft SQL Server.

Algumas das seções possuem uma jornada de trabalho contínua, ou seja, são 3 turnos diários onde nem sempre os responsáveis pelo setor estão presentes. A empresa busca adotar uma política para acesso aos recursos da rede de forma consciente.

Na Figura 4.1, esta apresentada a arquitetura que esta sendo usada na empresa atualmente, onde não há controle alguns ao acesso a internet e às pastar onde estão armazenados arquivos de uso da empresa.

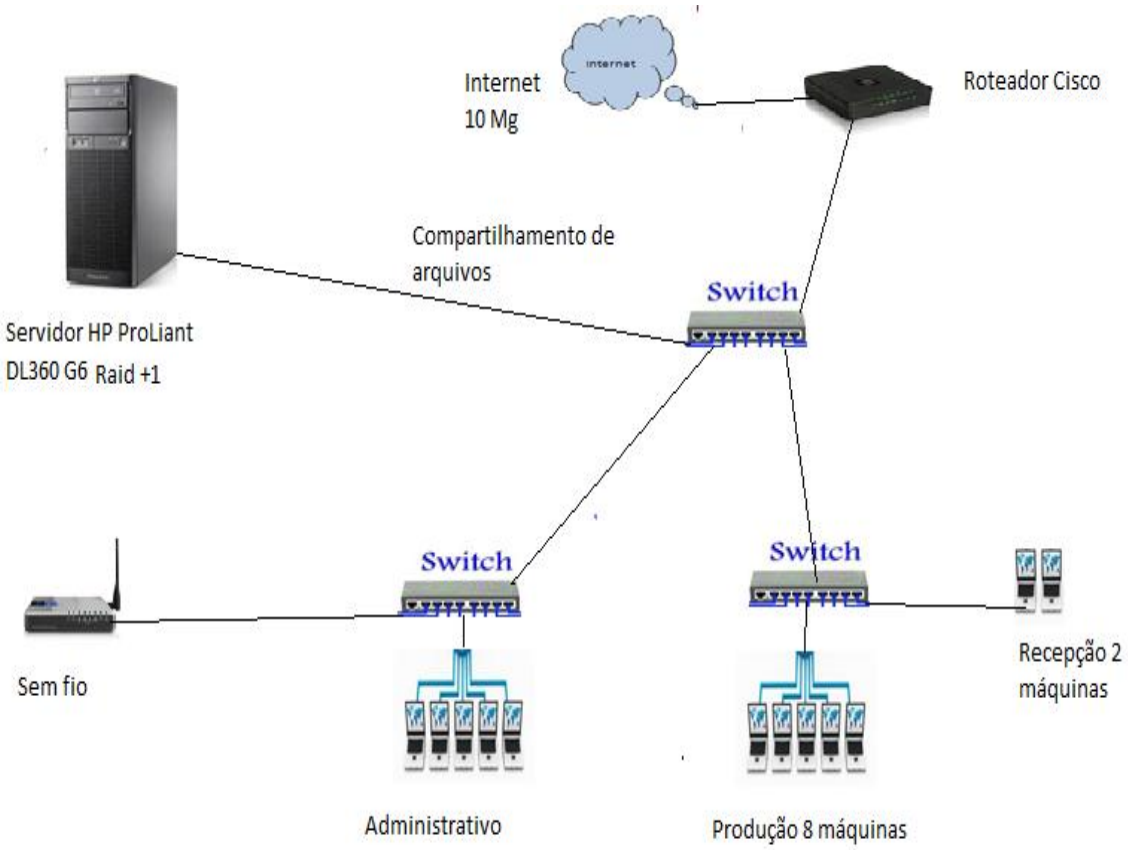


Figura 4.1 Arquitetura de rede atual.

No quadro 4.1 é apresentada a quantidade de máquinas dispostas por setor.

Quadro 4.1 Distribuição dos computadores dentro da empresa

Local	Quant.	Equipamento	Observação
CPD	1	HP ProLiant DL360 G6	Trabalhando em RAID 0+1 (Backup)
CPD	1	Desktop	Suporte Técnico
Financeiro	5	Desktop	
Almoxarifado	2	Desktop	
Direção	3	Notebooks	
Produção	8	Desktop	Trabalho em 3 Turnos
Tratamento de fotos	12	Desktop	
Recursos humanos	4	Desktop	
Controle de frotas	2	Desktop	
compras e vendas	9	Desktop	
Recepção	3	Desktop	
Portaria	2	Desktop	
Total	42		

O Quadro 4.2 apresenta a quantidade de manutenção ocorridas durante o mês de julho de 2012.

Quadro 4.2 Quantidade de computadores que apresentaram problemas

Quantidade	Infectadas	Softwares desnecessários	Falha de Hardware	Falha comunicação na rede
3	x	X		
2			X	
5		X		
2				X

Antes da implementação de um modelo proposto foi implantado um servidor de teste para coleta das informações no qual todo o acesso da rede à Internet passará por ele, conforme arquitetura apresentada na Figura 4.2

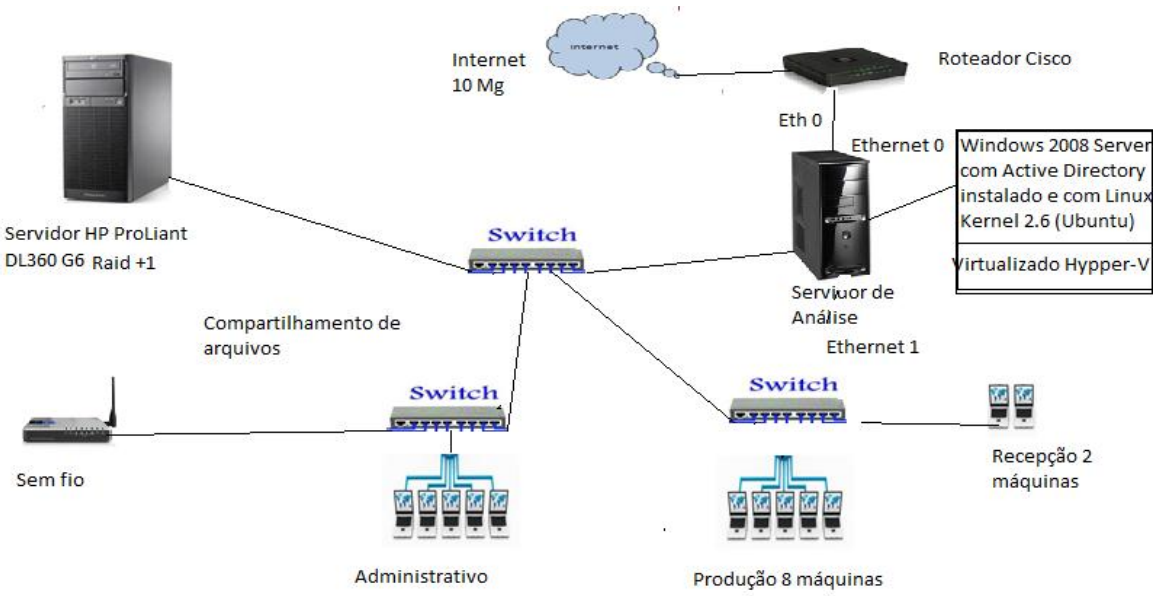
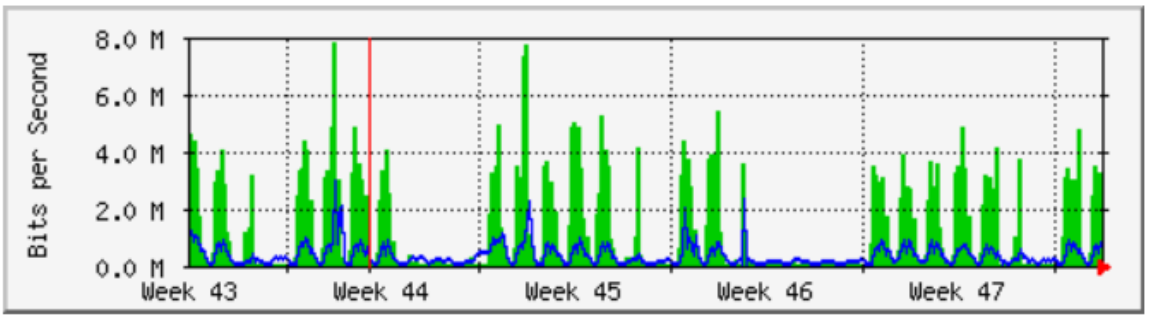


Figura 4.2 Arquitetura de rede para teste.

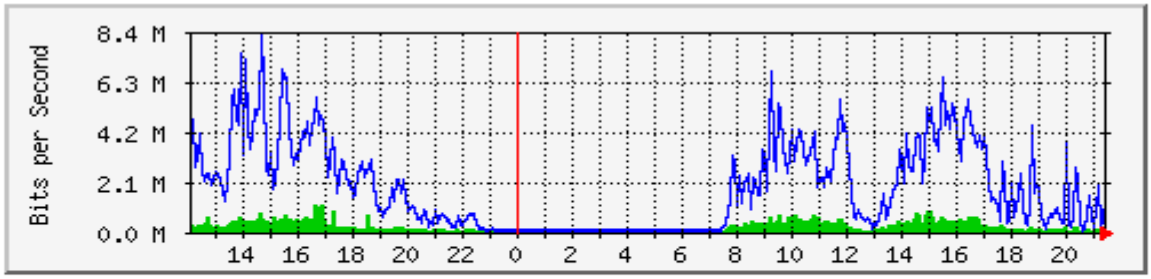
Na Figura 4.3 é apresentada os resultados obtidos pela *interface* de rede externa correspondente ao uso da rede no dia 15/09/2012. A largura de banda contratada pela empresa é de 10 Mbps sendo esta um link do tipo *full duplex*, ou seja, a taxa de *upload* e *download* são simétricas.



	Max	Average	Current
In	7821.0 kb/s (7.8%)	1045.8 kb/s (1.0%)	2977.6 kb/s (3.0%)
Out	2899.6 kb/s (2.9%)	315.9 kb/s (0.3%)	589.3 kb/s (0.6%)

Figura 4.3 – Rede Externa – 15/09/2012 (MRTG)

Na Figura 4.4 é mostrado um gráfico mensal ao tráfego de rede observado, sendo essa vista através da interface de rede interna. Além do tráfego de rede Internet o qual é feito através de NAT(Network Address Translation que é um protocolo que faz a tradução dos endereços Ip e portas TCP da rede local para a Internet), os usuário também acessam conteúdo de pastas e sistemas de gestão da própria empresa.



	Max	Average	Current
In	1149.1 kb/s (1.1%)	222.6 kb/s (0.2%)	81.1 kb/s (0.1%)
Out	8229.5 kb/s (8.2%)	1786.0 kb/s (1.8%)	1461.8 kb/s (1.5%)

Figura 4.4 – Rede Interna – 15/09/2012 (MRTG)

A Figura 4.5 é ilustrado o funcionamento da rede. Observa-se que as requisições feitas pela rede interna passa pelo servidor que cria um novo endereço de IP. Como é feito um NAT e sem nenhuma regra de controle deste, todo o tráfego ocorre livremente.

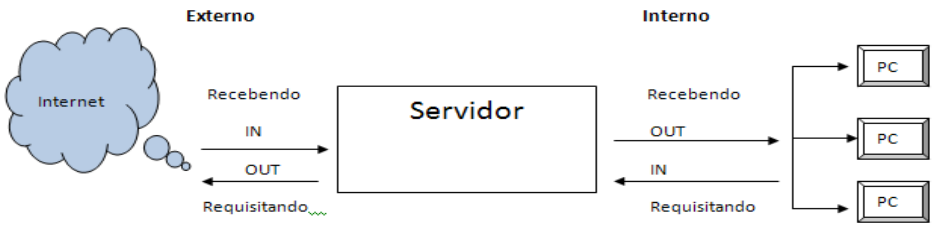


Figura 4.5: Servidor de Acesso.

.

Com o auxílio da ferramenta SARG, foram coletados os acessos feitos pelos usuários da rede da empresa.

Squid Analysis Report Generator

Squid User Access Report

Periodo: 2012Sep16-2012Sep21
Ordem: BYTES, reverse
Topuser Relatorio

NUM	LOCAL ACESSADO	CONEXÃO	BYTES	TEMPO
1	profile.ak.fbcdn.net	8.63K	29.73M	2.17M
2	www.facebook.com	2.15K	28.53M	2.64M
3	ads.imguol.com	1.03K	444.91K	277.81K
4	i.ytimg.com	1.01K	13.37M	1.76M
5	img100.xvideos.com	888	6.19M	352.19K
6	static.ak.fbcdn.net	817	6.05M	198.58K
7	notify4.dropbox.com	545	166.31K	29.91M
8	200.171.88.69	493	135.77K	19.70M
9	h.imguol.com	485	7.36M	222.93K
10	alphaeditora.mysuite.com.br	480	287.04K	274.84K
11	www.youtube.com	474	2.19M	257.70K
12	bn.uol.com.br	473	1.10M	204.59K
13	s.youtube.com	401	216.64K	175.42K
14	s.glbimg.com	380	3.64M	197.46K
15	notify18.dropbox.com	378	116.11K	21.04M
16	notify15.dropbox.com	376	115.50K	20.89M
17	notify17.dropbox.com	375	115.19K	20.88M
18	notify10.dropbox.com	373	114.57K	20.73M
19	i4.ytimg.com	356	5.32M	256.79K
20	0-jg-w.channel.facebook.com	328	1.04M	3.24M
21	photos-e.ak.fbcdn.net	316	2.71M	197.50K
22	i.cdn.turner.com	315	15.21M	423.85K
23	photos-f.ak.fbcdn.net	313	2.70M	206.73K
24	photos-c.ak.fbcdn.net	310	2.86M	196.34K
25	s2.glbimg.com	304	1.80M	124.78K

Figura 4.6: Relatório Sarg.

Na Figura 4.6 é apresentado a coleta de dados do período de 16 de setembro de 2012 à 21 de setembro de 2012, pode se observar que o acesso às páginas de relacionamento ocuparam o primeiro e o segundo lugar dentro do quadro de acessos da empresa, acompanhado da página de vídeos aparecendo em quinto lugar dentro da tabela, mostrando assim que há um grande dispersão por parte dos usuários dentro do ambiente de trabalho, como mostrado.

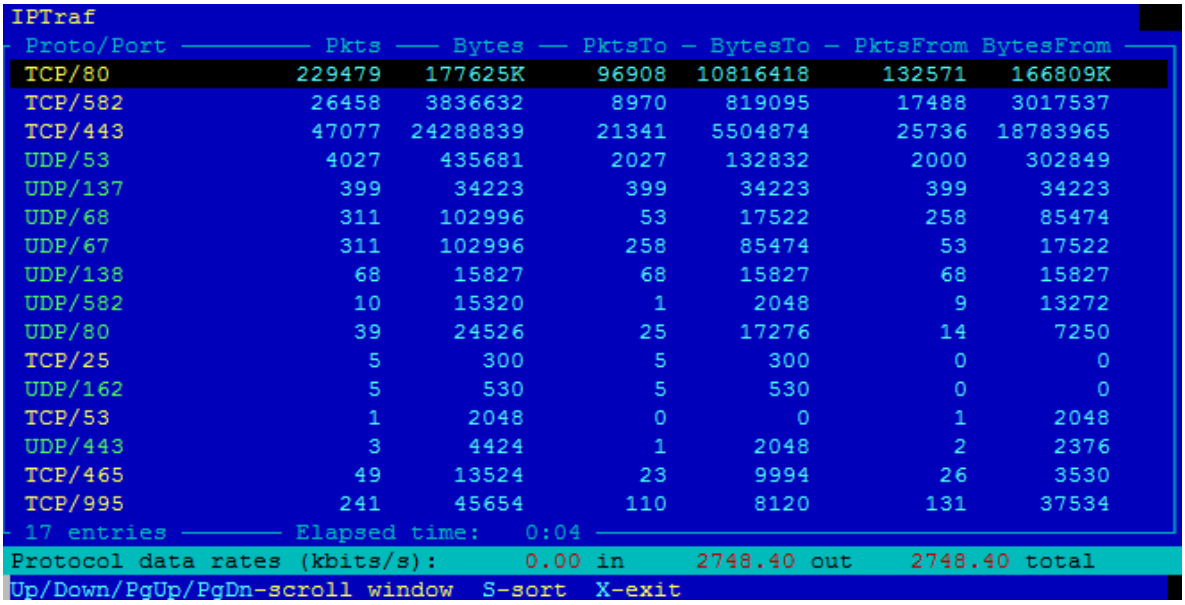


Figura 4.7: Relatório IPTraf

Fonte: Coletado Autor

Na Figura 4.7 são apresentadas as informações coletadas com o uso da ferramenta IPTraf. Nesta, é possível observar o acesso às portas feitas no servidor da rede.

Porta	Descrição
80 , 443	Website da empresa e acesso ao um dos sistemas web da empresa (http e https)
582	Porta criada para o gerenciamento e acesso remoto (SSH)
53	DNS (Resolvedor de nomes da rede interna e web)
137	Netbios-ns (a porta 137 UDP é usada para a navegação, incluindo a visualização dos compartilhamentos disponíveis).
67, 68	bootps, bootpd/dhcp Estes dois protocolos podem ser usados em sistemas de boot remoto
25	e-mail (serviço de mensagens entre servidores da própria rede e do sistema)
162	SNMPTRAP Simple Network Management Protocol (SNMP)
465, 965	E-mail (google Apps)

Quadro 4.3 – Portas utilizada durante análise

A porta TCP 80 e 443 é a que o servidor faz acesso a internet, a porta 582 é utilizada para se fazer os acessos remotos.

5 Modelo Proposto

Convencionou-se que a rede Internet fosse filtrada em alguns determinados setores, como por exemplo, a linha de produção a qual trabalha em 3 turnos. Uma listagem com diversos endereços de sites e palavras chaves de bloqueio foi implantado no servidor de proxy, o qual foi bloqueado durante praticamente todas as redes sociais e sites não condizentes a política idealizada pela empresa. No entanto foram permitidos que houvesse pelo menos 3 diferentes aberturas para acesso a sites de relacionamento, bate-papo, etc, durante o período do café.

Nos setores de compra e venda, administrativo e suporte à cliente os serviços de mensagem instantânea foram liberados. Para os visitantes, fornecedores e clientes, toda a navegação foi registrada. A cada acesso foi gerado *logs* de acesso os quais foram armazenados para análises caso fosse constatado algum tipo de irregularidade.

O Quadro 5.1 são ilustradas as regras de bloqueio implementadas no servidor proxy Squid. No arquivo de configuração da ferramenta (squid.confg) pode ser observado as acls as quais atribuem as permissões de acesso.

A sub rede, produção, é declarada na seguinte acl:

(acl bloq src 192.168.10.0/255.255.255.0) a qual utiliza a regra

(http_access deny bloq) negando a navegação dos usuários desse setor.

Em seguida é possível observar um caminho para o arquivo Ip_nlivre.txt o qual é um arquivo texto contendo todos os IPs das máquinas que podem ter acesso irrestrito a rede Internet.

Para que a ferramenta squid funcione adequadamente, primeiro é necessário liberar algum regras e depois restringi-las. Utilizando como exemplo, a palavra “sexologia” é necessária ser liberada, uma vez que esta é de natureza

comum. Em seguida é necessário bloquear a palavra “sexo” evitando assim a acesso a endereços dessa natureza. Essa ferramenta no entanto deve ser constantemente ajustada tendo em vista o grande número de palavras novas acessadas e a personalização segundo as necessidades de cada empresa.

Quadro 5.1 – Regras de Bloqueios no Servidor

```
##bloq total - producao-#################################
acl bloq src 192.168.10.0/255.255.255.0
http_access deny bloq

#-Range de IPs - Navegação Livre-############################
acl ip_nlivre src "/usr/local/firewall/ip_nlivre.txt"
http_access allow ip_nlivre all

### Palavras Chaves Liberadas-#################################
acl txtlivres url_regex "/usr/local/firewall/txtlivres.txt"
http_access allow txtlivres all

### Sites Liberados-###########################################
acl siteslivres url_regex "/usr/local/firewall/siteslivres.txt"
http_access allow siteslivres all

### Palavras Chaves Bloqueadas -###############################
acl txtbloq url_regex "/usr/local/firewall/txtbloq.txt"
http_access deny txtbloq all

### Bloqueio por Sites (URLs) -################################
acl sitesbloq url_regex "/usr/local/firewall/urlsbloq.tmp"
http_access deny sitesbloq all

### Bloqueio por downloads -###################################
acl downloadsbloq url_regex "/usr/local/firewall/downloadsbloq.txt"
http_access deny downloadsbloq all

##-Range de IPs - Navegacao Filtrada-##########################
acl ip_nfiltrada src "/usr/local/firewall/ip_nfiltrada.txt"
#error_directory /usr/local/squid/share/errors/pt-br
http_access allow ip_nfiltrada all
```

Da mesma forma determinados sites são primeiramente liberados através da regra http_access allow siteslivres all e depois resgringidos através da regra, acl sitesbloq url_regex "/usr/local/firewall/urlsbloq.tmp".

Observe que também foram criados bloqueios aquivos com determinadas extensões, evitando assim downloads de músicas, vídeos, .com, etc.

Para que a proposta tivesse uma eficiência maior, adotou-se que todo o tráfego de informações da rede fosse controlado pelo servidor Proxy, o qual foi feito de forma manual, isto é, a configuração do servidor proxy foi feita em cada navegador de Internet. Além disso, foi eliminado o tráfego de rede via servidor de NAT, o que poderia permitir maior índice de acessos desnecessários as rotinas da empresa, ou seja, os usuários poderiam burlar as regras estabelecidas. Figura 5.1. Optou-se então por fazer o controle de tráfego de rede somente pelo Servidor Proxy como ilustra a Figura 5.1.

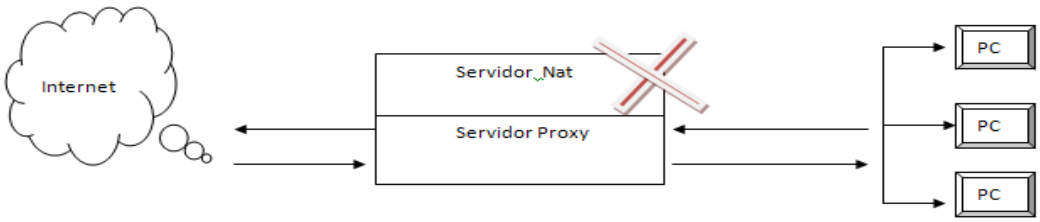


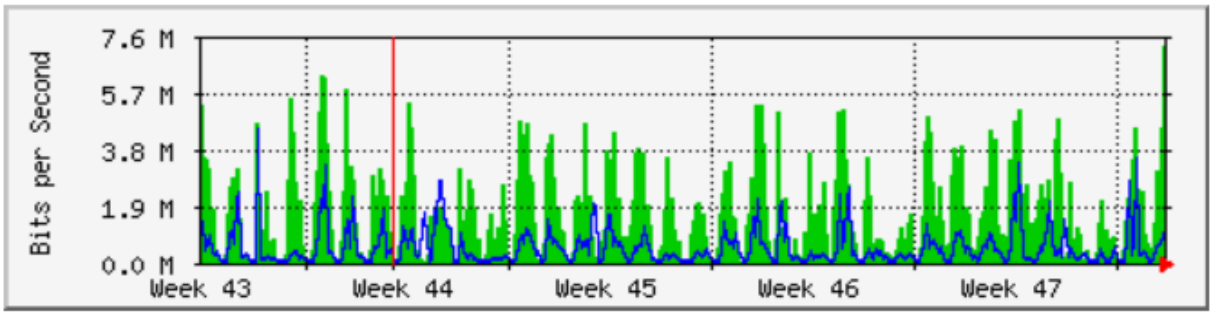
Figura 5.1: Servidor Proxy de Acesso.

Para que internamente houvesse um controle maior das informações que ficam armazenadas dentro do parque tecnológico, foi instalado o AD e através dele fosse criado *login* e senha para cada usuário afim de evitar acessos desnecessários a essas informações por departamentos que dele não fazem uso, ficando assim disponíveis somente aos departamentos autorizados para estarem fazendo uso destas informações. Com a criação de pastas para usuários, fez com que os mesmos trabalhassem dentro do perfil estipulado a eles, mantendo assim uma organização sobre os acessos a arquivos da empresa.

Após a criação dos usuários nos departamento de produção e recepcionista, foram definidos os perfis de cada usuário e a que eles podem acessar dentro do que foi acordado, ficando somente ao departamento de gerência o acesso liberado a todas as pastas. Nesse período de teste foram criados somente para os departamentos de produção e recepcionista devido ao grande número de informação que se trabalha nesse período em que os eventos mais acontecem e não é possível estar fazendo alterações em alguns departamentos.

5.1 Resultados Obtidos

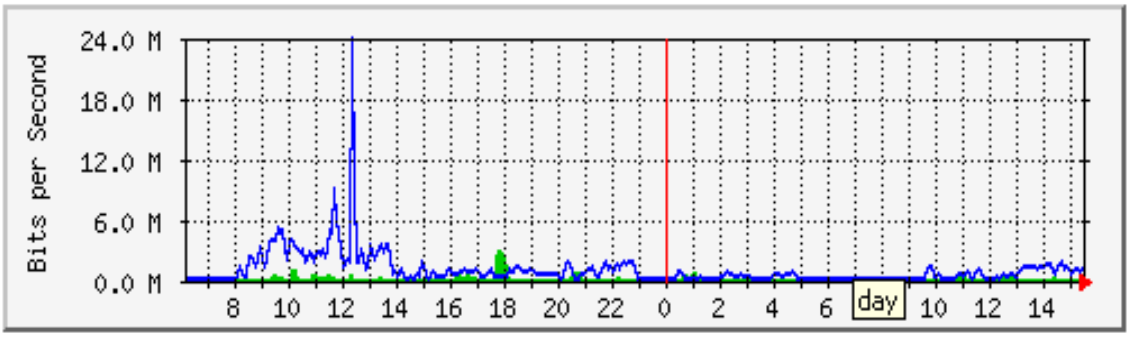
A Figura 5.2 apresenta os resultados obtidos pela *interface* de rede externa correspondente ao uso da rede no dia 30/10/2012. Apresentando uma queda de consumo de banda de 2431,1 Kb em relação ao gráfico coletado no dia 15/09/12.



	Max	Average	Current
In	7249.1 kb/s (0.7%)	1590.6 kb/s (0.2%)	7249.1 kb/s (0.7%)
Out	4458.9 kb/s (0.4%)	475.8 kb/s (0.0%)	1091.9 kb/s (0.1%)

Figura 5.2 – Rede Externa – 30/10/2012 (MRTG)

A Figura 5.3 apresenta os resultados obtidos pela *interface* de rede externa correspondente ao uso da rede no mês outubro colhido no dia 30/10/2012. Apresentando um aumento no consumo de banda interno, que demonstra um maior numero de acesso as pastas internas.



	Max	Average	Current
In	2968.9 kb/s (0.3%)	137.4 kb/s (0.0%)	59.1 kb/s (0.0%)
Out	23.9 Mb/s (2.4%)	946.8 kb/s (0.1%)	1196.7 kb/s (0.1%)

Figura 5.3 – Rede Interna – 30/10/2012 (MRTG)

Dados coletados no período de 07 de outubro a 14 de outubro de 2012, período em que já estava implantado as ferramentas nos mostra que acessos como o Facebook que na amostragem do dia 16 a 21 do mês anterior ocupavam o primeiro e o segundo lugar na tabela dos *sites* acessados no período da ultima coleta esta ocupando o sexto lugar como mostra a Figura 5.4, dando lugar aos acessos que são de prioridade da empresa e diminuindo assim a dispersão por parte dos funcionários em relação a *sites* de relacionamentos e diminuído assim também o consumo de banda.

Squid Analysis Report Generator

Squid User Access Report

Periodo: 2012Oct07-2012Oct14

Top 100 sites

NUM	LOCAL ACESSADO	CONEXÃO	BYTES	TEMPO
1	www.alphaeditora.com.br	26.72K	2.49G	2.44M
2	urs.microsoft.com:443	5.45K	27.37M	5.54M
3	alphaeditora.mysuite.com.br	3.95K	4.47M	2.29M
4	www.alphaeditora.net	1.15K	94.94M	826.74K
5	s.glbimg.com	1.00K	17.71M	32.63K
6	profile.ak.fbcdn.net	928	3.17M	267.14K
7	consultanumero.abr.net.br	594	4.14M	235.73K
8	s2.glbimg.com	508	4.43M	12.28K
9	www.google-analytics.com	490	572.80K	9.45M
10	rad.msn.com	483	745.22K	156.49K
11	by153w.bay153.mail.live.com	447	7.12M	288.46K
12	www.facebook.com	447	3.38M	697.47K
13	static.dafity.com.br	393	1.80M	19.23K
14	www.administradores.com.br	341	3.32M	41.95K
15	static.ak.fbcdn.net	332	5.05M	80.05K
16	www.dafiti.com.br	306	1.07M	176.06K
17	h.live.com	302	169.08K	72.93K
18	alphaeditora.com.br	269	981.52K	102
19	col.stb01.s-msn.com	268	2.69M	72.05K
20	col.stb00.s-msn.com	258	3.06M	84.74K
21	images.minhavida.com.br	245	1.39M	60.65K
22	a.rad.msn.com	241	283.99K	87.77K
23	www.google.com.br	234	3.75M	75.93K

Figura 5.4: Relatório Sarg.

Através da ferramenta IPTraf, pouco se observou de alteração nas portas utilizadas, Figura 5.5. Embora o tráfego de rede P2P e Torrent possa utilizar portas conhecidas para a transferência de informações. Não foi possível observar grandes mudanças, nem mesmo a detecção do mesmo. Relatos dos administradores dizem que esse tipo de problema não é ainda um fator preocupante para eles, uma vez que é raro encontrar softwares dessa natureza nas máquinas da empresa.

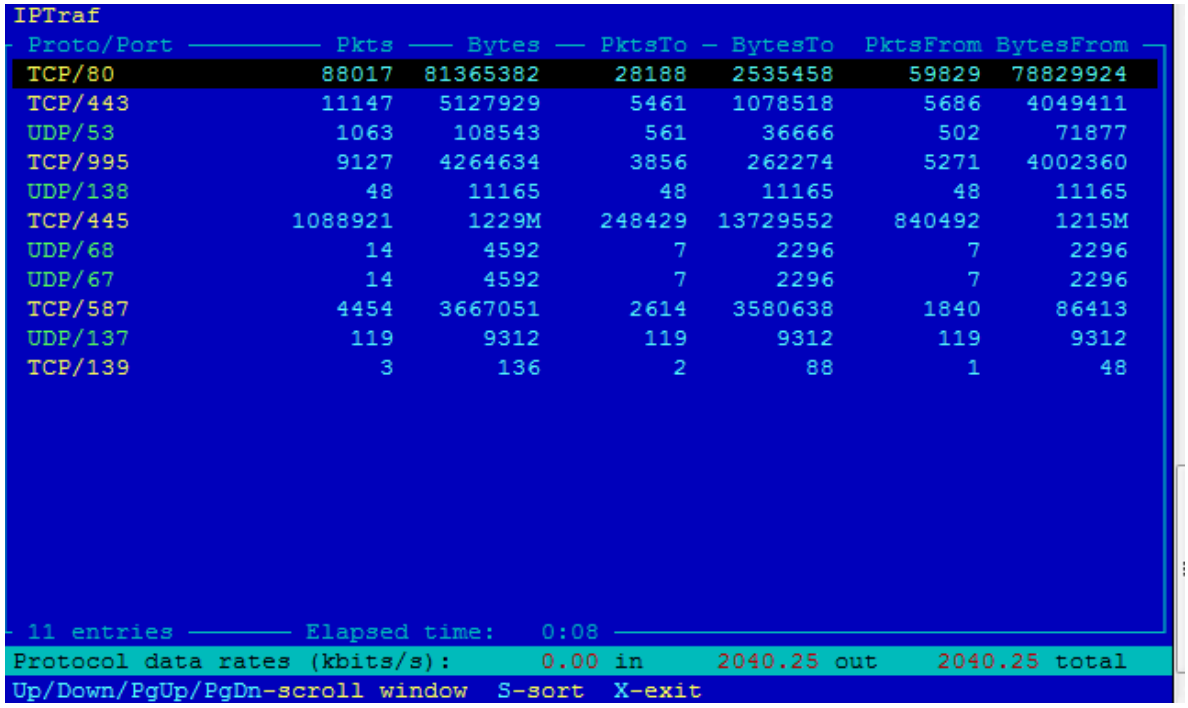


Figura 5.5- Portas utilizadas pelas máquinas da empresa no servidor.

6. CONCLUSÃO

Após a avaliação dos resultados, chegou-se a conclusão de que o nível de acessos a conteúdos desnecessários, muitas vezes são prejudiciais, tanto no que diz respeito ao carregamento da rede da empresa, como também os prejuízos causados nas máquinas podem ser reduzidos com a aplicação de normas e limites impostos nos departamentos que tem o livre acesso. Pôde-se observar também que o nível de dispersão por parte dos funcionários acaba diminuindo, uma vez que os mesmos não ficam navegando em *sites* que trazem informação de pessoas conhecidas que lhes causam interesses, e com isso aumenta-se a dedicação a função exercida.

Quadro 6.1 – Quadro comparativo de resultados obtidos

	Antes	**Depois**
Número de máquinas em manutenção	12	10
Quantidade de banda consumida (interna)	1149,1 Kb	2968,9 Kb
Quantidade de banca consumida (externa)	8229,5 Kb	5798,4 Kb
Sites mais acessados 3 primeiros	profile.ak.fdc.net www.facebook.com ads.imguol.com	www.alphaeditora.com.br urs.microsoft.com:443 alphaeditora.mysuite.com.br
Scan de Porta Utilizadas	80, 443, 582, 53, 137,67, 68, 25, 162, 465, 965 (portas conhecidas)	80, 443, 53, 995, 67, 68, 587, 137, 139 (portas conhecidas)
Detecção de tráfego Torrent	Não detectado	Não detectado
Hierarquia de Pastas (Serviço de diretório)	Não existia	Diretoria / TI / Suporte / Recepcao01 / Recepcao02 Temporario

Com a coleta das informações dos gráficos colhidos na data 30/10/2012 pôde-se avaliar que houve uma grande queda nos acessos a internet em relação

a data de 15/09/12, aumentando assim o trafego de informações que realmente pertencem a empresa e que estão armazenadas internamente, evitando assim o alto número de acessos a *sites* não condizentes com a realidade da empresa.

As máquinas que precisaram de manutenção, apesar de um curto tempo de avaliação foram 10, e comparando com a coleta relacionada ao mês de agosto de 2012 teve uma redução de 16,7% no mês de outubro, passando de 12 máquinas em agosto para 10 máquinas em outubro, não servindo como parâmetros exatos devido ao curto período, mas que as máquinas que apresentavam maior índice de problemas estão localizadas no departamento de produção onde foi implantado o sistema de controle.

Considerando a existência de uma máquina servidora Windows, com com seu sistema já instalado, o modelo indicado é a arquitetura conforme vista na Figura 6.1, com as ferramentas de proxy para controle de conteúdo a fim de filtrar os acessos à Internet.

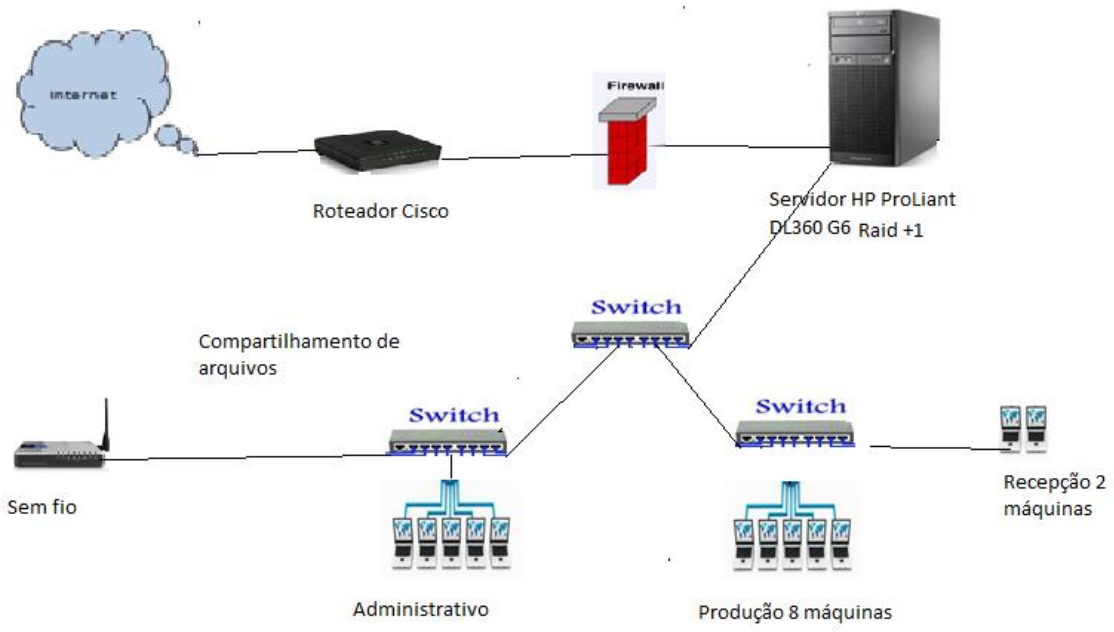


Figura 6.1- Modelo proposto.

6.1 Trabalhos Futuros

Neste trabalho não foi contemplado o bloqueio de redes P2P e torrente, pode-se analisar e encontrar meios para o bloqueio ou redução do tráfego de torrente.

7 REFERÊNCIAS

3COM CORPORATION. 3Com OfficeConnect: Network Assistant. Santa Clara, EUA: 3Com, versão 2.02, 2000. 1 CD-ROM.

BATISTA, Thaís Vasconcelos. Segurança em Redes de Computadores. Natal, 2002. Aula 1. Disponível em: http://www.dimap.ufrn.br/~thais/Seguranca/home.html>.
Acesso em: 17 nov 2002.

BATTISTI, JULIO - Certificação Microsoft - Guia de Estudos Para o MCSE - Exame 70-216 - Curso Completo – ISBN: 8573231963, Ano: 2003 - Editora: Axcel Books.

BATTISTI, JULIO - Windows Server 2003 - Curso Completo – ISBN: 8573231963, Ano: 2003 - Editora: Axcel Books

CISNEIROS, H. Gerando relatórios do Squid com o SARG. 2003.

Http://www.devin.com.br/eitch/sarg/. Visitado em março de 2005.

COMER, D. E., Redes de Computadores e Internet - Abrange Transmissão de Dados, Ligação Inter-redes, Web e Aplicações, 4a Edição, Rio de Janeiro: Bookman, 2007.

CYCLADES. Guia Internet de Conectividade. 6ª Edição. São Paulo: SENAC, 2000. 167 p.

DOUGLAS E. COMER- Redes de Computadores e Internet - BOOKMAN COMPANHIA EDITORA LTDA - 2007

FEDOROVA, Alexandra. **Making the most of OS Virtual Machine Technology.** Disponível em: <http://www.eecs.harvard.edu/~fedorova/papers/253final-fedorova.pdf>. Acesso em: 9 dez. 2008, 14:38:20.

GIL, A.C. Métodos e técnicas de pesquisa social. São Paulo: Atlas, 1991.

INFO CORPORATE. **Máquinas virtuais chegarão a 4 milhões em 2009, diz Gartner**. Disponível em: <http://info.abril.com.br/corporate/noticias/noticia_231932.shtml>. Acesso em: 9 dez. 2008.

KUROSE, J. F. e ROSS, K, W – Redes de computadores e a Internet: Uma nova abordagem, Addison Wesley, São Paulo, 2003. (Biblioteca CEFET- SJ – reserva).

MARSHALL, D. et al. **Advanced Server Virtualization**. EUA: Auerbach Publications, 2006.

MONTEIRO, Edmundo. Segurança em Redes. Coimbra, Portugal, 1999. Capítulo 1. Disponível em: <http://eden.dei.uc.pt/~sr/Teoricas/>. Acesso em: 15 nov 2002.

MOREIRA, Daniela. **Virtualização: rode vários sistemas operacionais na mesma máquina.** Disponível em: <http://idgnow.uol.com.br/computacao_corporativa/ 2006/08/01/idgnoticia.2006-07-31.7918579158/>. Acesso em: 6 set. 2008, 16:51:59.

NETTO e VITTAL, 2004 **Viabilizando o Acesso a Internet para Pequenas Empresas** Disponível em: < http://www.convibra.com.br >. Acesso em: 25 jun.2012.

Percilia, Eliene. O uso dos equipamentos e recursos da empresa. Disponível em **http://www.brasilescola.com/informatica/o-uso-dos-equipamentos-recursos-empresa.htm**. Acesso em 20 jul. 2012.

PEREIRA, OTAÁVIO e MOSTARDINHA, RICARDO - OPTIMIZAÇÃO DO DESEMPENHO DE UMA REDE LOCAL – UM CASO PRATICO BASEADO EM VLANS E ACTIVE DIRECTORY - Conferência IADIS Ibero-Americana WWW/Internet 2006.

PONTE, João Pedro (2006). **Estudos de caso em educação matemática.** Bolema**, 25**, 105-132. Versão revista e atualizada de artigo anterior: Ponte, J. P. (1994). O estudo de caso na investigação em educação matemática. Quadrante, 3 (1).pp 3-18.

SANCHES, L. **As dez tecnologias dos próximos anos, segundo o Gartner**. Disponível em:http://www.itweb.com.br/noticias/index.asp?cod=51443&utm_source= newsletter_20080918&utm_medium=email&utm_content=As%20dez%20tecnologias%20dos%20pr%C3%B3ximos%20anos,%20segundo%20o%20Gartner&utm_campaign=ITWebDirect>. Acesso em: 18 set. 2008, 13:31.

SANTOS, Pinheiro**. Sistemas estruturados em redes de computadores**. Disponível em: <http://www.projetoderedes.com.br>. Acesso em: 25 jun.2012.

SCHÄFFER, Guilherme**. Entendendo a virtualização de servidores – parte II.** Disponível em: <http://www.baguete.com.br/blogs/post.php?id=4,119>. Acesso em: 7 set. 2008, 13:04:28.

SOARES, Luiz Fernando Gomes. Redes de computadores. 2. ed.rev. e ampl. Rio de Janeiro: Campus, 1995.José Mauricio dos Santos Pinheiro .

TANNENBAUM, Andrew S. **REDES de Computadores**. 4ª ed. Rio de Janeiro: Editora Campus, 2003.

TORRES, Gabriel. **Redes de computadores Curso completo**. Rio de Janeiro: Axcel Books, 2001.

YIN, R.K. Estudo de caso. Planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.