UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

GUSTAVO DOS SANTOS DE LUCCA

DIAGNÓSTICO DO TRÁFEGO DE REDE WEB E ANÁLISE DA BASE DE DADOS GERADA PELO *MICROSOFT INTERNET SECURITY AND ACCELERATION* 2006: ESTUDO DE CASO NA SATC

CRICIÚMA, JULHO DE 2009.

UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

GUSTAVO DOS SANTOS DE LUCCA

DIAGNÓSTICO DO TRÁFEGO DE REDE WEB E ANÁLISE DA BASE DE DADOS GERADA PELO *MICROSOFT INTERNET SECURITY AND ACCELERATION* 2006: ESTUDO DE CASO NA SATC

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. Esp. Arildo Sônego

Co-orientador: Prof. Esp. Kristian Madeira

CRICIÚMA, JULHO DE 2009.

GUSTAVO DOS SANTOS DE LUCCA

Diagnóstico do tráfego de rede web e Análise da base de dados gerada pelo Microsoft Internet Security and Acceleration 2006: Estudo de caso na SATC

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Prof. MSc. Rogério Antônio Casagrande
Coordenador Adjunto do Curso de Ciência da Computação

Banca Examinadora:

Prof. Esp. Arildo Souego(UNESC)
Orientador

Prof. Esp. Kristian Madeira(UNESC)
Co-Orientador

Adjano Scarmagnani

Prof. Esp. Adjano Scarmagnani (Depto de TI – UNESC)

Prof. MSc. Rogério Antônio Casagrande

A minha namorada, aos meus pais, Sidnei José De Lucca e Maria Lucia dos Santos, meu irmão Guilherme e minha irmã Gabriela e aos meus amigos devido à força.

AGRADECIMENTOS

Agradeço a minha família pelo incentivo dado para conclusão e obtenção do grau de Bacharel em Ciência da Computação.

Agradeço também:

Aos meus colegas de trabalho Daniel, Fabiano, Giana e Tiago pelo apoio e respostas perante questionamentos durante o processo de desenvolvimento do trabalho.

Agradeço ao coordenador de informática da SATC onde foi feito o estudo de caso, Valter Blauth Junior, devido aos esclarecimentos e ênfase na idéia do trabalho.

A instituição SATC por permitir que fosse realizado o trabalho dentro da instituição, por muitas vezes deixando o serviço indisponível, e de certa forma prejudicando os serviços prestados.

Agradeço encarecidamente ao orientador Arildo Sonego e co-orientador Kristian Madeira pelo incentivo dado a pesquisa e pelo conhecimento agregado pela conclusão da mesma.

A minha amiga e namorada Luana, pelo incentivo dado para atingir o objetivo do término da graduação.

A professora Merisandra, devido as suas contribuições junto ao entendimento e andamento do desenvolvimento do trabalho, bem como, as suas contribuições quanto as normas e estruturação da pesquisa.

Enfim, a todos que contribuíram para a execução desse trabalho, seja pela ajuda

constante ou por uma simples palavra.

"*O único lugar em que o sucesso vem antes do trabalho é no dicionário.*"

(Autor Desconhecido)

RESUMO

O crescente aumento do volume de computadores nas corporações fez com que surgisse a necessidade de se gerenciar os computadores da mesma. O avanço do uso da internet para os mais variados serviços fez com que os problemas se tornassem mais comuns e com eles aparecem soluções para gerenciamento e monitoramento de dispositivos pela rede. Dentre os recursos disponíveis, têm-se as ferramentas de *Firewall* e *Proxy*, que são usadas para manter um controle do uso do serviço de Internet, bem como atuam como forma de segurança de ataques externos. Sendo assim servem como remediadores no problema do acesso a internet em corporações, sendo estas no campo do comércio, indústria e instituições de ensino. Tendo em vista a necessidade de monitoramento do uso de serviços de Internet, desenvolve-se uma pesquisa com o intuito de auxiliar no gerenciamento da rede onde foi efetuado o estudo de caso. Esta pesquisa baseia-se em métodos estatísticos efetuados com o intuito de comprovação da hipótese antes apresentada informalmente pelos usuários do serviço de Internet na SATC. Comprovado o problema de desempenho em determinados horários do dia foi efetuada a implementação de um sistema que auxiliasse na detecção do tráfego da rede local para a Internet nos horários especificados. Por meio da análise da base de dados gerada pelo Microsoft ISA Server 2006, este sendo o servidor de Firewall e *Proxy* da SATC, foram desenvolvidos relatórios que servem de auxilio na detecção de problemas ou mau uso do serviço. Esta interpretação de mau se dá por meio da análise feita pelos administradores da rede da SATC em conjunto com a avaliação das políticas de acesso a Internet que a empresa adota em relação aos colaboradores.

Palavras-chave: monitoramento de rede, métodos estatísticos, diagnóstico de rede, análise de tráfego e monitoramento de registros.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

DoD	*Department of Defense*
IP	*Internet Protocol*
ISA	*Internet Security and Acceleration*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
Mbps	*Mega bits por segundo*
RM-OSI	*Reference Model - Open System Interconnection*
TCP	*Transfer Control Protocol*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
WAN	*Wide Area Network*
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Nas empresas públicas ou privadas e em instituições de ensino, o uso de redes de computadores é importante, uma vez que objetivam a troca de informações e compartilhamento de recursos. O crescimento dos ambientes de trabalho cooperativo é uma realidade, formando-se intranets, onde mesmo geograficamente separadas, matrizes e filiais trocam informações de forma segura e estável, sendo essa troca feita por Virtual Private Network (VPN), conexões por protocolos seguros ou acesso a *sites* na World Wide Web (WWW).

Desta forma, essas intranets devem ser administradas e gerenciadas, para que as empresas e instituições usufruam dos recursos das redes computacionais em sua totalidade. Nessas redes de computadores corporativas existem diversos tipos de recursos compartilhados, sendo eles por meio de servidores ou de recursos locais nas estações dos usuários. Além das intranets os ambientes de trabalho cooperativo possuem normalmente acesso à extranet, que é na verdade o acesso à Internet, redes WAN, por meio de um provedor, ou de grandes redes de Pesquisa Educacionais. Sendo assim, o papel dos administradores é manter todos os serviços e recursos disponíveis para os usuários executarem suas tarefas de maneira eficiente.

Dentro dos ambientes corporativos existem políticas de acesso à rede, tanto interna quanto externa. Políticas essas, definidas por decisões dos administradores de redes, por meio de análises de uso de serviços e recursos. Porém, a tarefa de definição dessas políticas nem sempre é simples, muitas vezes por falta de ferramentas específicas para cada ambiente.

Este trabalho visa desenvolver o protótipo de uma ferramenta de tratamento das informações da base de dados de um servidor de *Firewall* e *Proxy* com o intuito de auxiliar na administração de redes. O protótipo pretende analisar os *logs* do servidor, gerando relatórios de uso. Pretende-se assim gerar informação relevante aos administradores de rede, auxiliando-os na tomada de decisão, para eventuais criações das novas políticas para acesso aos serviços voltados à rede WAN da instituição. Por meio dos relatórios apresentados será possível aos administradores de rede atuar de acordo com as políticas de acesso aos serviços de Internet.

1.1. OBJETIVO GERAL

Desenvolver o protótipo de uma ferramenta para tratar as informações geradas pelo Microsoft Internet Security and Acceleration (ISA) 2006 no ambiente de rede da SATC com o objetivo de auxiliar no monitoramento do serviço de Internet e administração da rede da instituição.

1.2. OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa são:

a) verificar por meio de métodos estatísticos a hipótese de lentidão no uso da Internet apresentada pelos usuários da SATC;

b) monitorar o acesso à Internet da SATC, objetivando a detecção e averiguação da hipótese apresentada;

c) compreender o armazenamento de dados realizado pela ferramenta Microsoft ISA Server 2006;

d) identificar quais dados são relevantes e devem ser tratados pelo protótipo de monitoramento dentro do ambiente de rede da SATC;

e) realizar testes com a ferramenta de monitoramento, verificando a viabilidade de sua adoção como instrumento de auxílio e suporte ao gerenciamento da utilização dos serviços voltados para a web na instituição;

f) verificar se as informações apresentadas pelos relatórios da ferramenta de monitoramento estão de acordo com a necessidade para monitoramento do acesso à Internet na SATC.

1.3. JUSTIFICATIVA

Instituições de ensino e pesquisa usufruem do acesso à rede mundial de computadores como um meio de suporte à obtenção de informações. Visando que este suporte não venha apresentar falhas, os administradores de rede dessas instituições devem permitir que os acadêmicos, docentes e funcionários acessem à Internet de maneira eficaz. Porém estas redes estão se tornando mais complexas, principalmente quando se trata de serviços voltados

para a web, onde se tem um número cada vez maior de novas funcionalidades com o uso diversificado de aplicações.

Administradores de rede conseguem monitorar e gerenciar estas redes de computadores de maneira mais segura e eficaz com o auxílio de ferramentas, visando confiabilidade e disponibilidade.

Dentro da Instituição SATC, por ser uma rede corporativa com acesso à Internet, a tarefa de gerenciamento da rede se torna complexa. E conforme relatado por usuários dos serviços, o acesso à Internet em determinados horários tem se tornado moroso.

O princípio do protótipo da ferramenta é gerar relatórios de uso dos serviços da web a partir da base de dados gerada pelo Microsoft Internet Security and Acceleration 2006, visando detectar a queda de desempenho no serviço de Internet.

Desta forma, objetiva-se com a implantação desta ferramenta auxiliar os administradores da rede, na tomada de decisões para seu ambiente de aplicação. Espera-se que, com o auxílio dos relatórios, os supervisores possam visualizar com maior facilidade como estão sendo utilizados os serviços voltados para a web, permitindo assim reavaliar políticas de uso, alterando-as se necessário.

1.4. ESTRUTURA DO TRABALHO

Esta pesquisa está dividida em seis capítulos, sendo o primeiro deles retratando o tema proposto, objetivos e justificativa para a realização da pesquisa.

No capítulo 2 estão destacados os conceitos fundamentais de redes de computadores, necessárias para a compreensão do estudo efetuado.

No capítulo 3 tem-se ao entendimento sobre gerência de redes, dando destaque para os conceitos de *Firewall* e *Proxy*, em que este trabalho está fundamentado.

O presente trabalho procurou destacar o levantamento de uma hipótese, usando-se de métodos estatísticos para efetuar a comprovação desta. Estes procedimentos estão destacados no capítulo 4, onde são apresentados os conceitos dos métodos estatísticos necessários para elaboração do estudo.

Alguns exemplos de estudos que estão sendo efetuados na área de diagnóstico de rede por meio de estatística estratificada são levantados no capítulo 5. E no capítulo 6 está apresentado todo o estudo efetuado bem como o desenvolvimento do HEFESTO, um protótipo de ferramenta de análise de base de dados de *Firewall/Proxy*.

E por último, tem-se a conclusão deste trabalho apresentando algumas sugestões para trabalhos futuros.

2 REDES DE COMPUTADORES

Há aproximadamente 30 anos a tecnologia de informação vem evoluindo rapidamente, tanto no campo doméstico como no campo das corporações. Novas tecnologias vêm surgindo com o objetivo de automatizar sistemas. As formas como tudo é organizado no mundo computacional foram se alterando de acordo com a passagem dos anos. O conceito de uma Unidade Central de Processamento dentro da empresa onde os usuários levam os programas a serem processados está ultrapassado. Com o objetivo de fazer com que a empresa não necessite desta sala central única surge o conceito de redes de computadores, que é a capacidade de realizar os trabalhos da empresa por interconexões entre os computadores (TANEMBAUM, 1997).

Sendo assim, uma rede de computadores se define por um conjunto de dispositivos capazes de efetuar qualquer tipo de troca de mensagens através de um meio de transmissão, sendo este por meio de fios de cobre, fibras ópticas, ar, entre outros (SOARES; LEMOS; COLCHER, 1995).

Sucintamente quando se existem dois, ou mais, módulos processadores interligados por um meio de transmissão, fisicamente ou logicamente, havendo ou não a troca de informações, existirá uma rede de computadores.

As redes de computadores são a principal maneira de troca de informações entre as instituições educacionais, governamentais e empresas em geral. E dessa troca de informações surgiram formas de organizar a maneira como os computadores estão interligados e como é feita a troca de informações entre eles (MURHAMMER et al, 2000).

2.1. TOPOLOGIAS DA REDE

Sistemas de comunicação possuem um tipo de topologia interligando os dispositivos para a troca de mensagens. O conceito de topologia de rede é a forma como os dispositivos de troca de mensagens estão interligados ao meio físico. A topologia em que este sistema de comunicação está fisicamente interligado faz com que dois parâmetros de monitoramento de rede possam ser influenciados, que são velocidade e desempenho (SOUSA, 2001).

A topologia em anel, representada pela Figura 1, requer que cada nó seja capaz de verificar as mensagens que chegam. Caso estas mensagens não sejam destinadas a ele, deverão ser passadas adiante. Na topologia em anel existe um circuito fechado entre as estações, sendo cada uma delas um repetidor, para passar adiante a mensagem. Porém se um nó destes pára de transmitir informação, todo o circuito de comunicação fica comprometido (SOARES; LEMOS; COLCHER, 1995).

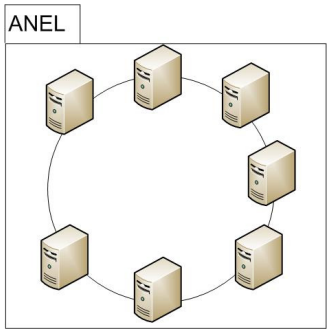

Figura 1. Topologia em Anel.

Quando os computadores estão interligados em estrela, esta rede possui um nó central, chamado de mestre, onde todas as mensagens que trafegam na rede devem passar por ele. Este nó central pode executar diversas funções como chaveamento e processamento,

podendo efetuar a compatibilidade de comunicação entre o nó de origem e o nó de destino. A Figura 2 está representando uma topologia em estrela (SOARES; LEMOS; COLCHER, 1995).

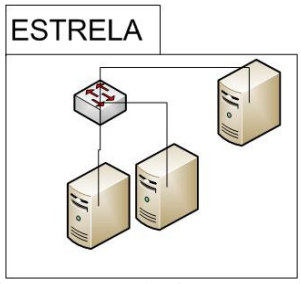

Figura 2. Topologia em Estrela.

Em uma rede onde se emprega uma topologia em barramento, tem-se um meio de transmissão onde todos os nós se conectam, podendo cada nó capturar as mensagens que estão trafegando na rede. Com uma topologia muita parecida com o anel, se diferencia desta no fato de se um nó parar de funcionar o circuito poderá continuar funcionando. Na Figura 3 pode-se visualizar a topologia em forma de barra (SOARES; LEMOS; COLCHER, 1995).

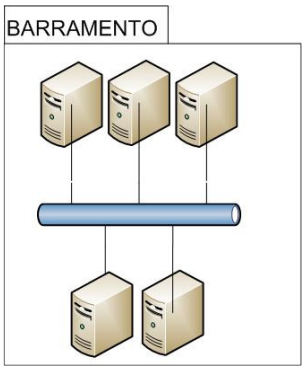

Figura 3. Topologia em Barramento.

Em uma instituição de ensino e pesquisa, ou indústria podem ser encontradas redes em anel, barramento e estrela, devido à grande necessidade da troca de informações entre os setores. Desta maneira existem formas de abrangência das redes de computadores, que especificam o quão grande e que tipo de recursos que essas redes apresentam.

2.2. ABRANGÊNCIA DAS REDES

Redes de computadores podem ser classificadas quanto a sua abrangência, sendo estas divididas em *Local Area Network* (LAN), *Metropolitan Area Network* (MAN) e *Wide Area Network* (WAN), onde são representadas pelo número de dispositivos processadores, organizadas em um tamanho físico (TANENBAUM, 2003).

Dentre os tipos de abrangência de redes de computadores, a LAN, trata de redes locais, sendo sempre redes privadas, onde a abrangência delas equivale, por exemplo, a um laboratório ou um escritório, como mostra a Figura 4. São empregadas em pequenas distâncias, para que computadores pessoais e estações de trabalho possam trocar informações e disponibilizar serviços, como por exemplo, o compartilhamento na utilização de um recurso de impressão. As LAN`s têm um tamanho restrito, podendo utilizar taxas de transferência de 10, 100 ou 1000Mbps. Como são redes que ocupam uma pequena área geográfica, é possível se prever como esta rede funcionará, havendo a possibilidade de determinar o tempo de transferência dos dados entre as estações de trabalho, obtendo-se uma maior facilidade em seu gerenciamento (NASCIMENTO; TAVARES, 2006; TANENBAUM, 1997).

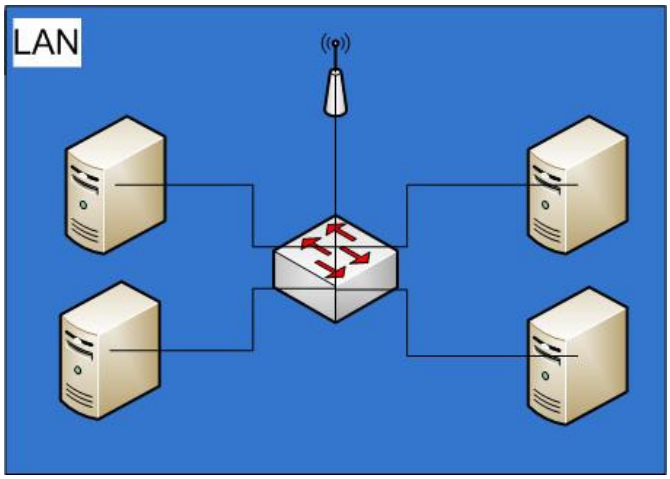

Figura 4. LAN.

As redes metropolitanas, que possuem uma abrangência um pouco maior que as LANs, podem ser empregadas em redes privadas ou públicas. Geograficamente uma MAN, pode ter uma abrangência atingindo escritórios vizinhos de uma empresa, ou vários laboratórios de uma instituição de ensino e pesquisa. Quando há uma interconexão de duas ou mais LANs, tem-se uma MAN. Normalmente atuam com taxas de transferência de 10 ou 100Mbps utilizando-se de meios físicos como fibras ópticas. A Figura 5 mostra a representação de uma MAN (NASCIMENTO; TAVARES, 2006; TANENBAUM, 1997).

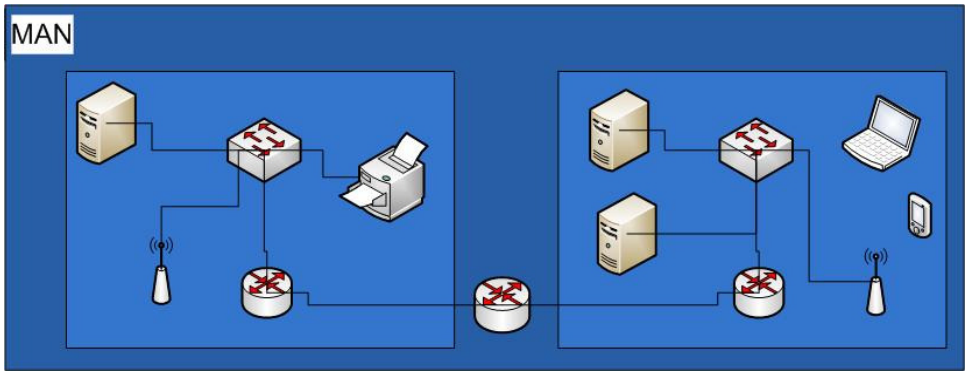

Figura 5. MAN.

Já as redes geograficamente distribuídas, representadas pela Figura 6, ou WAN, por sua vez possuem grandes áreas geográficas de abrangência, normalmente conectadas por meio de *links* com baixa taxa de transmissão e de domínio público. Comunicam-se por meios físicos como fibras ópticas, satélite e cabos submarinos (NASCIMENTO; TAVARES, 2006; TANENBAUM, 1997).

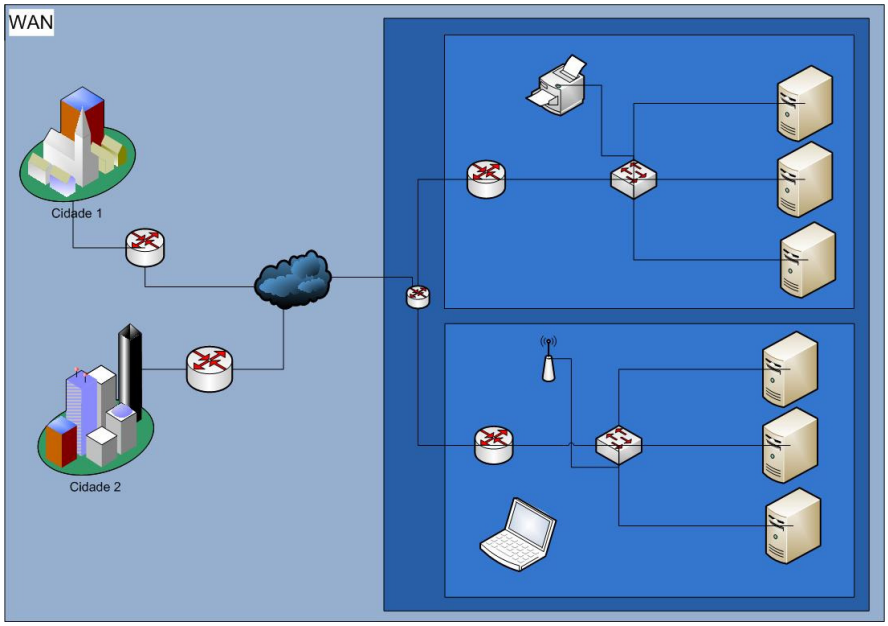

Figura 6. WAN.

Dentro de uma LAN, MAN ou WAN, pode-se apresentar topologias em anel estrela ou barramento, isso depende da necessidade e do ambiente de rede apresentado. Mesmo assim isso não deve influenciar na comunicação destas redes. Para isto existem regras e discrepâncias a serem seguidas.

2.3. PROTOCOLO

Redes de computadores são divididas em modelos arquitetônicos, sendo eles modelos de referência para implementação. Estes modelos de referência são divididos em camadas, que servem para facilitar a troca de mensagens entre dois dispositivos. Essas trabalham de forma independente, o protocolo se torna um “tradutor” da camada inferior para a superior, ou seja, é um conjunto de normas e regras que fazem com que dois níveis, de uma

arquitetura de redes de computadores, se comuniquem sem ocorrer falhas (TANENBAUM, 1997; NASCIMENTO; TAVARES, 2006;).

Por isso, o conceito de protocolos para cada camada é a maneira mais eficiente de se formar uma arquitetura de redes. Essas arquiteturas de redes no início eram elaboradas de maneiras diferentes, onde cada fabricante desenvolvia seu padrão de utilização. Esses padrões são chamados de arquiteturas de redes proprietárias (SOARES; LEMOS; COLCHER, 1995).

Pode-se fazer uma analogia ao entendimento da função de um protocolo como sendo um tradutor. Para que uma rede de computadores possa trocar informações com uma rede que utiliza outro padrão, será necessário este tradutor no meio, fazendo com que as duas redes, mesmo tratando os pacotes de maneira diferente, possam trocar mensagens de forma eficiente. Por isso existem modelos de referência para constituição de Arquitetura de Redes.

Com base nestas informações pode-se concluir que toda rede de computadores necessita de um protocolo para funcionar de maneira correta. Sendo necessário um protocolo, as empresas desenvolveram seus protocolos de comunicação internos, porém com o crescimento das redes locais houve a necessidade de se criar padrões para que houvesse troca de informações entre as empresas de maneira eficiente.

2.4. MODELO RM-OSI

Devido ao surgimento de diversas arquiteturas de redes de computadores juntamente com diversos protocolos, desenvolvidos pelos fabricantes, a *International Organization* for *Standardization* (ISO), elaborou um projeto de padronização que possuía o

objetivo de que, de forma abstrata, os modelos de comunicação de dados entre dispositivos fossem efetuados da mesma maneira por todos os dispositivos de troca de mensagens (CARVALHO, 1997).

O modelo ISO 7498, assim designado pela organização de padronização mundial, descreve um modelo de sete camadas, denominadas por 1 - Física, 2 - Enlace de Dados, 3 - Rede, 4 - Transporte, 5 - Sessão, 6 – Apresentação e 7 - Aplicação, onde cada camada fornece serviços para a camada superior, e é auxiliada pela camada inferior para dispor de seus serviços. Sendo estas divididas em dois grandes grupos, onde as camadas 1, 2, 3 e 4, são chamadas de camadas de fluxo de dados, e as camadas 5, 6 e 7 são chamadas de camadas de aplicação (MURHAMMER et al, 2000).

Este modelo de referência, que está representado na Figura 7, possui a vantagem de tornar o ambiente de comunicação de redes menos complexo, dividindo a comunicação em partes menores, possibilitando a comunicação entre diferentes hardwares e softwares de rede. E ainda, a modularização em camadas faz com que as mudanças em uma camada de atuação, não influenciem nas outras camadas (NASCIMENTO; TAVARES, 2006).

A camada física do Modelo OSI tem como principal característica os dispositivos físicos de comunicação como conectores, fios, cabos e linhas de comunicação. Neste nível trata-se a transmissão propriamente dita. É nesta camada que trafegam os bits. Na camada física não é aplicado nenhum tipo de protocolo, porém existem alguns padrões como X.21[1], V.24[2] e RS-232[3] (SOUSA, 2001).

[1] Padrão International Telecommunication Union (ITU) que rege a interface entre o DCE e DTE para operação síncrona em redes públicas de dados (BLACK BOX, 1997).

[2] Padrão International Telecommunication Union (1964) que define as funções de todos os circuitos para a interface RS-232. Os conectores e atribuições dos pinos são definidos na norma ISO 2110 (BLACK BOX, 1997).

A segunda camada denominada de enlace de dados ou link de dados busca fornecer uma comunicação confiável dos dados através dos meios físicos. Sendo ela responsável pelo endereçamento físico, topologia de rede, notificação em caso de erros e entrega sincronizada dos quadros. Equipamentos como *bridges*, *switches* e a interface de rede de uma estação se situam nesta camada, sendo nesta aplicados protocolos como *Ethernet*[4], *FastEthernet*[5] e *Token Ring*[6] (NASCIMENTO; TAVARES, 2006).

Na camada três ou camada de rede atuam equipamentos como os roteadores, que têm como principal função efetuar a comunicação entre redes distintas, fazendo com que por meio deste processo o pacote de origem chegue até seu destino. Nesta camada é efetuado o controle de congestionamento, a qualidade de serviço (retardo, tempo em tráfego, instabilidade, etc). A camada de rede tem como função resolver problemas como o tráfego de pacotes em redes distintas, se a rede do destino possui um endereçamento diferente da rede de origem, cabe a esta camada efetuar a comunicação correta entre as duas redes. Nela se tem o emprego de protocolos como IP[7], o X.25[8] e o CLNP [9] (TANENBAUM, 2003).

A camada de transporte tem como função principal gerenciar a comunicação entre os pacotes que estão trafegando entre o host de destino e o host de origem, promovendo a confiabilidade de troca de mensagens. Ela possui funções de controlar erros, prioridade de

---

[3] Padrão recomendado pela Eletronic Industries Association (EIA) para interfaces mecânicas e elétricas, que especifica um conector DB-25. Idêntica a norma ITU v.24/v.28 (BLACK BOX, 1997).

[4] Rede local (LAN) desenvolvida pela XEROX, Digital Equipment Corporation e Intel (IEEE 802.3). Ethernet conecta nós com velocidade de até 10Mbps por cabo par-trançado, coaxial ou fibra óptica (BLACK BOX, 1997).

[5] Geralmente refere-se à alta velocidade da Ethernet, velocidade como 100Mbps (BLACK BOX, 1997).

[6] Mecanismo de acesso a rede com topologia em anel onde um token de supervisão é passado de estação em estação como uma sondagem na rede (padrão IEEE 802.5) (BLACK BOX, 1997).

[7] Além de ser um protocolo de comunicação da camada 3 do modelo OSI, é usado para roteamento de mensagens entre redes (BLACK BOX, 1997).

[8] Interface padrão de comutação de pacotes de dados em comunicações eletrônicas, designado pela ITU (BLACK BOX, 1997).

[9] Protocolo de rede que fornece fundamentalmente o mesmo serviço subjacente a uma cada de transporte, como o IP (THE INTERNET ENGINEERING TASK FORCE, 1993);

comunicação, tempo máximo de tráfego de pacotes e segurança. Coordena o envio e recebimento de pacotes, para evitar que sejam enviados mais de uma vez (STALLINGS, 1999).

Na camada de sessão fica o controle de comunicação entre dois hosts, onde se abre uma sessão entre o nó de origem e o nó de destino, trafega-se os dados, e depois se fecha a conexão entre os dois hosts. Nesta camada são implementadas técnicas de comunicação como *full duplex, half duplex* e *simplex*. Nesta que ocorre o sincronismo entre a comunicação dos hosts. Como exemplos de protocolos para esta camada têm-se NFS[10], SQL[11], RPC[12], entre outros (SOUSA, 2001).

Na sexta camada que é chamada de apresentação se tem a garantia de que toda a informação vinda da camada de aplicação de um sistema que seja legível para a camada de aplicação do outro sistema. Ela deve ser capaz de converter dados de forma que ambos os nós de comunicação entendam as informações trafegadas. Nesta camada estão recursos como ASCII[13], multimídia e formato de figuras (NASCIMENTO; TAVARES, 2006).

E, por fim a sétima camada, chamada de aplicação. Essa sim é a camada que o usuário final tem acesso com navegadores de Internet, programas que recebem e enviam e-mails, downloads na Internet, etc. É a única que não provê serviços à outra camada, porém provê serviços à camada de aplicação, possui a funcionalidade de recuperação de erros e de controle de integridade de dados (NASCIMENTO; TAVARES, 2006).

---

[10] Sistema de arquivos distribuídos pela SunSoft que permite que os dados sejam compartilhados através de uma rede independente da máquina, sistema operacional, arquitetura de rede, ou protocolo (BLACK BOX, 1997).

[11] Linguagem utilizada para processar dados em um banco de dados relacional (BLACK BOX, 1997).

[12] Define como um protocolo para execução de proceditmentos remotos em computadores ligados em rede (GARCIA, 2008).

[13] Código binário para textos, comunicações e controle de impressora. ASCII é um código 7-bit fornecendo 128 combinações de caracteres (BLACK BOX, 1997).

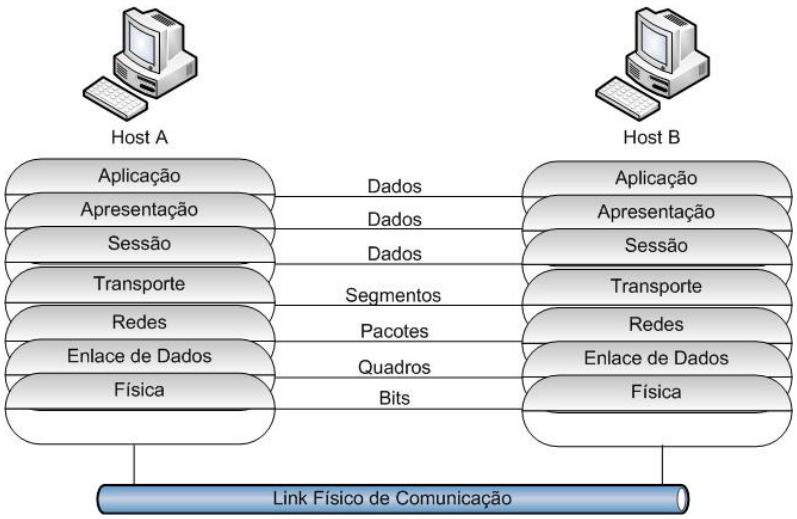

Figura 7. Representação Gráfica do RM-OSI.

O modelo de referência apesar do conceito de diminuir a complexidade de comunicação entre sistemas processadores se torna de tal forma complexo, pelo fato de possuir sete camadas de comunicação. Por isso, o surgimento de outra arquitetura, chamada de TCP/IP conseguiu sobressair-se em relação ao modelo OSI da ISO.

2.5. ARQUITETURA TCP-IP

A Arquitetura TCP/IP é um modelo aberto de interconexão de redes, e isso faz dele o padrão mundial de comunicação entre computadores na Internet. Além da Internet muitas empresas adotam o modelo TCP/IP de comunicação como forma de comunicação interna na empresa, redes também conhecidas como intranets (COMER; STEVENS, 1999).

Ela surgiu a partir de uma necessidade do *Department of Defense* (DoD), que queria um modelo de arquitetura que continuasse sua comunicação nas condições mais

adversas. O DoD precisava de um sistema que continuasse trafegando informações não importando qual meio físico estivesse sido empregado (NASCIMENTO; TAVARES, 2006).

Como o modelo OSI da ISO, a arquitetura TCP/IP se divide em camadas, como mostra a Figura 8, cada uma com suas funções e protocolos, onde cada camada fornece serviços à camada superior. A diferença para o modelo OSI é que ele se divide em quatro camadas, sendo elas, 1 – Camada de Interface com a Rede, 2 – Camada de internet, 3 – Camada de Transporte e por fim a 4 – Camada de Aplicação (TORRES, 2001).

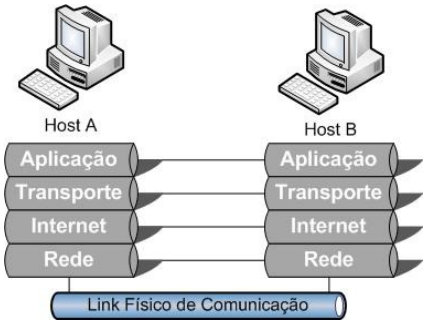

Figura 8. Representação Gráfica do Modelo TCP-IP.

A arquitetura TCP/IP não especifica nenhum protocolo de utilização na primeira camada do modelo, ou seja, a camada de Interface com a Rede. Simplesmente diz que se pode usar qualquer interface de rede disponível, o que demonstra o quão aberto é o modelo de Arquitetura TCP/IP. Nesta camada há o contato direto com o meio físico da comunicação por meio de fios, do ar, ou interconexão entre os dispositivos processadores que efetuarão a troca de mensagens (MURHAMMER et al, 2000).

Na camada de internet, que é a segunda de baixo para cima na arquitetura, tem-se a funcionalidade de que os *hosts* trafeguem os pacotes na rede sem se preocupar com ordem. O objetivo é confirmar o recebimento do pacote no *host* de destino, sem se preocupar que tipo

de rede em que este pacote será inserido. Em uma comparação ao modelo OSI, esta camada é muito semelhante à camada de redes deste modelo (TANENBAUM, 2003).

A terceira camada da Arquitetura TCP/IP, chamada de transporte, é equivalente a mesma camada do Modelo OSI, sendo que sua principal função é organizar os dados repassados pela camada de aplicação, colocar esses dados em pacotes, e repassá-los para a camada de internet, para que esta os trafegue na rede. Existem dois protocolos operantes nesta camada, o TCP, que possui confirmação de entrega de pacotes, e o UDP, que não é orientado à conexão, ou seja, não possui confirmação na entrega de pacotes. Ao se fazer a recepção dos dados, esta camada organiza os pacotes recebidos da camada de internet e repassa as informações à camada de aplicação (TORRES, 2001).

Na camada de aplicação da Arquitetura TCP/IP, têm-se o software que está sendo utilizado para comunicação entre os dois hosts. Como o TCP/IP permite conexões simultâneas, para se determinar qual aplicação está sendo utilizada naquele momento, se utiliza portas de comunicação. Essas portas são exemplificadas por números, de acordo com o serviço que está sendo disponibilizado. Serviços como WWW[14], TelNet, FTP[15] e HTTP (TANENBAUM, 2003).

A porta de comunicação da camada de Aplicação do Modelo TCP/IP tem como fundamental objetivo o de identificar qual processo no *host* local está se comunicando com qual processo no *host* remoto. Por meio deste código identifica-se que tipo de aplicação está sendo executada por determinado *host*, e assim consegue-se disponibilizar o serviço desejado (MURHAMMER et al, 2000).

[14] Serviço de Internet que provê ligações entre os hipertextos de servidor para servidor (BLACK BOX, 1997).
[15] Em uma rede TCP/IP, é um conjunto de comandos utilizados para se autenticar na rede, listar diretórios e copiar arquivos (BLACK BOX, 1997).

Sendo assim, fazendo-se uma comparação do Modelo OSI com a arquitetura TCP/IP consegue-se determinar que o Modelo OSI se torne mais complexo, por ter um número maior de camadas. Por isso, a arquitetura TCP/IP tem uma aceitação da maioria das arquiteturas de computadores e sistemas operacionais que atuam no mercado de hoje. A Figura 9 representa a comparação entre os dois modelos, sendo possível verificar a maior complexidade do modelo OSI.

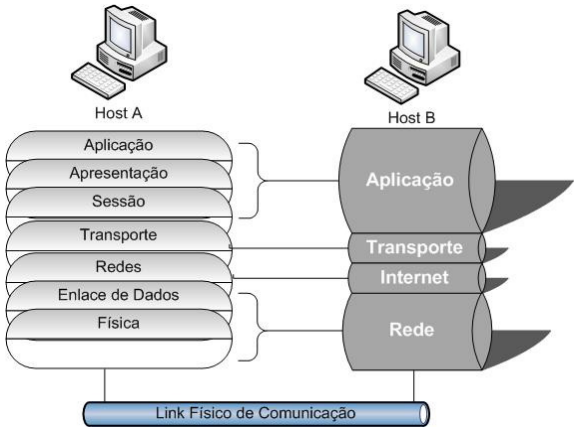

Figura 9. Comparação do Modelo OSI com Modelo TCP-IP.

Mesmo que apresentando um número menor de camadas, o modelo TCP-IP também possui características de complexidade. Existem vários fatores que influenciam no tráfego de redes de dados. Por isso a capacidade de gerenciamento de redes de dados é fundamental quando o objetivo é manter os links e hosts *on-line* para acesso aos serviços disponíveis.

3 GERÊNCIA DE REDES

O surgimento de novas aplicações e serviços utilizados por meio das redes de computadores, e também com a expansão contínua das redes locais, metropolitanas e de longa distância, a tarefa de monitoramento e gerenciamento das redes se tornou mais complexa. Com isso a tarefa de engenharia de tráfego se tornou mais importante, fazendo com que ferramentas de monitoramento de tráfego de rede façam parte de um conjunto de aplicações que auxiliam os administradores de rede (MORAES; VILELA, 2008).

Assim, o tráfego de redes possui uma quantidade enorme de informação útil aos administradores. Com a observação de registros do tráfego da rede os administradores são capaz de avaliar métricas como desempenho, segurança e análise de carga. Estudos de desempenho em tráfego de redes podem ser adquiridos por meio de análises estatísticas de monitoramento. Além disso, o monitoramento de rede visa detectar erros de comunicação e também efetuar monitoramento de segurança em redes de computadores (ZAKI; DARWISH; OSMAN, 2003).

A gerência de redes, segundo a OSI se divide em algumas áreas, que tratam as maneiras de monitoramento da rede. Este monitoramento serve para se ter um maior controle sobre os equipamentos que estão atuando na rede. Cada área de gerenciamento trata o monitoramento diferente, onde cada uma delas possui uma função específica. A seguir estão descritas as áreas com suas respectivas funções: (ZACKER; DOYLE, 2000).

a) **monitoramento de falhas:** deve-se monitorar os equipamentos da infra-estrutura de rede com o intuito de detectar falhas de comunicação, e ainda, se possível, ter formas de respostas às falhas;

b) **monitoramento de configuração:** suprir a capacidade de se gerenciar remotamente a configuração de um dispositivo lógico ou físico;

c) **monitoramento e análise do desempenho:** capacidade de análise de estatísticas da rede, com o objetivo de planejamento de capacidades;

d) **monitoramento e controle de segurança:** controlar acesso a dispositivos da rede por meio de uma interface única de configuração. Controle de equipamentos como, por exemplo, roteadores, switches e servidores de impressão, com o uso de senhas e outras formas de controle;

e) **monitoramento de registros:** capacidade de capturar dados de quem, quando e talvez porque está usando determinado serviço da infra-estrutura de rede.

Sendo definidas as áreas de gerenciamento, existem métricas parametrizadas a serem monitoradas por ferramentas que visam gerenciar redes de computadores. Algumas das métricas são definidas:

a) **disponibilidade:** antes de se efetuar o gerenciamento de uma rede de computadores, deve-se primeiro verificar o funcionamento dela. Por meio de ferramentas e serviços consegue-se verificar esse funcionamento e disponibilidade (ABREU; PIRES, 2008);

b) **tempo de resposta:** é determinado pelo tempo entre uma requisição que um usuário faz a um serviço da Internet, e em quanto tempo o usuário terá disponível para ele na sua tela (STALLINGS, 1999);

c) **utilização da rede:** é um valor percentual que determina o tempo de uma informação que foi transmitida de um *host* para outro (ABREU; PIRES, 2008);

d) **vazão (*throughput*):** é definido por taxa de requisições por unidade de tempo que o sistema é capaz de executar. É chamada de taxa nominal de transferência do sistema quando a carga de trabalho aumenta até um limite (MARTINS, 2002);

e) **capacidade de transmissão:** deve-se efetuar o monitoramento dos *links* entre hosts para que seja verificada a possibilidade de que algum esteja defeituoso e também se existe algum dispositivo causando interferência nas transmissões (STALLINGS, 1999).

Um projeto de redes de computadores necessita não só de sua configuração de interfaces e equipamentos, deve-se determinar também métodos de monitoramento constante dos enlaces, com o objetivo de detectar falhas, e assim obter um melhor desempenho da rede (FARREL, 2005).

Existe também uma preocupação dos dirigentes das corporações quanto ao uso da Internet por seus funcionários. Na maioria das empresas deseja-se um controle do acesso ao serviço da WEB, sendo ele para bloqueio de alguns *sites*, ou simplesmente para um monitoramento do que está sendo acessado. Então, para se fazer estas formas de monitoramento existem dois tipos de ferramentas, os *Proxies* e *Firewalls*, onde os *Firewalls*

servem para restringir alguns tipos de conteúdos ou URL, e os *Proxies* podem ser usados para restringir o acesso a um usuário individual (ou grupo de usuários) com base em políticas de acesso aos serviços (DIMARZIO, 2001).

O gerenciamento de rede não está somente ligado ao motivo pelo qual o serviço ficou indisponível. Não importa o que aconteceu, o importante é somente quanto tempo o serviço ficou indisponível e qual o custo daquele problema para uma organização. Por isso, existem meios de se gerenciar e monitorar redes de computadores de organizações. O termo de gerência de redes, não se resume somente a aspectos de configuração e controle, mas também de relatórios capazes de auxiliar o gerenciamento da rede (FARREL, 2005; STALLINGS, 1999; TORRES, 2001).

Os administradores da rede devem ser auxiliados por dados estatísticos como uma forma de planejamento de crescimento da rede da corporação. Devem se preocupar que sua rede irá crescer em número de equipamentos e também de usuários, tendo assim um volume maior de dados e havendo a possibilidade de um planejamento da área de tecnologia da informação. Uma rede não gerenciada pode acarretar diversos problemas se crescer de forma desordenada, problemas como congestionamento, má utilização de recursos disponíveis, problemas de segurança etc (OLIVEIRA et al, 1998).

Sendo assim, a construção de ferramentas que auxiliem os administradores de rede em sua tarefa é desejável. Os administradores de rede devem se preocupar com todas as áreas de gerenciamento, porém dando enfoque a área que mais estiver ligada ao seu ambiente de aplicação. Este enfoque deve ser na área de monitoramento de registros e *logs*, ou na área de controle de equipamentos.

3.1. MONITORAMENTO E ANÁLISE DE DESEMPENHO

O monitoramento de desempenho atua no sentido de verificar dispositivos na rede, permitindo determinar o nível de operacionalidade dos mesmos. Por meio de análises estatísticas os administradores de redes devem conseguir identificar degradações que estão ocorrendo nos dispositivos de rede, e ainda a possibilidade de identificação de possíveis gargalos na rede. A partir do momento que os administradores de rede conseguem identificar problemas na rede, a aplicação de ações necessárias para coibir que os problemas ocorram deve ser tomada. Além disso, há a possibilidade de se fazer planejamentos de longo prazo, como ampliação da capacidade de acordo com o volume de usuários, e implantação de novos serviços de acordo com a necessidade (TEIXEIRA JUNIOR, 1999).

Sendo assim, para efetuar o monitoramento de desempenho de infra-estrutura de rede necessita-se de quantificar, medir, informar, analisar e controlar o desempenho de diversos componentes da rede. Dentre eles, equipamentos individuais, links de comunicação ou taxa de transferência (KUROSE; ROSS, 2006).

Para fazer com que os administradores de rede consigam gerenciar de forma competente a rede, deve-se utilizar ferramentas que o auxiliem nesta tarefa, permitindo planejar o aumento de infra-estrutura e também a capacidade de detecção de gargalos na rede, evitando problemas que provocariam a possível paralisação do sistema e o conseqüente prejuízo para a corporação.

3.2. MONITORAMENTO DE REGISTROS

Os administradores de rede devem ter um controle de acesso aos serviços da rede tanto em termos de usuários individuais quanto de grupo de usuários. A razão deste tipo de controle se dá muitas vezes ao fato de estar acontecendo um abuso por parte dos usuários, ocorrendo uma sobrecarga de dispositivos. Os administradores de rede devem ter capacidade de alterar políticas de acesso a serviços com o intuito de aumentar o desempenho da rede. Com o monitoramento de acesso em nível de usuário ou grupo deles, o administrador terá uma visão do que ocorre na sua infra-estrutura, podendo assim fazer um melhor planejamento de crescimento da rede (STALLINGS, 2005).

O gerente de rede deve ser capaz de contabilizar o uso de serviços da rede pelo usuário, bem como poder acompanhar o uso, dos recursos disponibilizados, por parte dos usuários (TEIXEIRA JUNIOR, 1999).

O registro dos acessos por parte dos usuários só é possível com o uso de ferramentas de autenticação desses usuários. Existem algumas maneiras de se identificar um colaborador, seja por meio do número de matrícula na empresa ou instituição de ensino, seu CPF, ou alguma outra forma de identificação. Quanto à autenticação, ela pode ser feita com o uso de uma senha, cartão, e ainda características físicas ou biométricas[16]. As formas de autenticação se diferem pelo custo, a senha é a forma mais barata, e ela possui um nível de proteção alto quando se elaboram políticas de manipulação de senhas, como tempo de expiração, número mínimo de caracteres e ainda quantas senhas deverão ser armazenadas até

[16] Ramo da ciência que estuda a mensuração dos seres vivos (FERREIRA, 1999).

que o usuário possa utilizar a mesma novamente. Por meio de cartão o custo é mais elevado, porém apenas o colaborador que possuí-lo pode acessar determinado serviço. Já por meio de características físicas ou biométricas seria por meio de leitura de retina ou impressão digital, ficando um custo elevado. Desta forma, as empresas devem usar-se daquilo que for necessário para o seu ambiente. (FONTES, 2006).

As ferramentas de segurança possuem recursos de emissão de relatórios sobre a estrutura de segurança e também das atividades dos usuários. Porém muitas delas não permitem a formatação dos dados de forma específica para uma organização. Por isso, muitas destas ferramentas possuem o recurso de armazenamento de registros em um arquivo intermediário, que poderá ser utilizado como entrada para uma ferramenta específica de acordo com o ambiente de aplicação. E ainda possuem maneiras de armazenar em bancos de dados diferentes, sendo possível o acesso a esses dados em tempo real. Estes dados armazenados se distinguem em dois grupos de controle que se diferem em estrutura de segurança e atividades dos usuários. Onde, o primeiro destaca a interação entre os usuários e os recursos, já o segundo retrata a forma como os usuários estão acessando os recursos disponíveis (CARUSO; STEFFEN, 1999).

Existem duas formas de restringir o acesso aos serviços da Internet dos usuários, que são os *Firewalls*[17] *e Proxies*[18]. É possível se juntar as duas formas, pois uma não interfere no funcionamento da outra. O uso das duas ferramentas em conjunto possibilita aos administradores dizer quem tem acesso a Internet e após ser permitido o acesso, qual o conteúdo este determinado cliente poderá acessar. Portanto o P*roxy* impede usuários não

[17] Um nó de rede configurado como fronteira para impedir o tráfego de um segmento que cruza sobre outro. Os *Firewalls* são usados para melhorar o tráfego da rede, bem como para fins de segurança (BLACK BOX, 1997).
[18] É um nó pelo qual todos os usuários de uma rede acessam a Internet (DIMARZIO, 2001).

autorizados de acessar o serviço de Internet, enquanto o *Firewall* tem a função de restringir os usuários de acessar conteúdo não aprovado na Internet (DIMARZIO, 2001).

Com isso, devem-se implantar ferramentas como *Firewall* e *Proxy* para que se consiga ter um monitoramento do acesso dos usuários a serviços disponibilizados pela Internet. Desta forma, os gestores das organizações terão uma melhor representação de como estão sendo utilizados os serviços.

3.3. *FIREWALL*

O acesso a Internet por usuários domésticos é também uma forma de entretenimento, porém dentro das corporações necessita-se de uma atenção maior, pois muitas empresas possuem suas informações confidenciais sendo acessadas por meio da Web. Além do perigo dessas informações virem a público, existe também a possibilidade de vírus e softwares mal intencionados estarem atuando na rede interna tentando desestabilizar os sistemas de rede para enviarem informações para fora da intranet. Ao encontro a essa constante busca em torno da informação, surge o conceito de *Firewall*, que são ferramentas que forçam todos os pacotes, que saem e entram na rede da empresa, e que tem como destino a Internet, trafegarem por ele para que seja efetuada uma filtragem (STALLINGS, 2005).

Desta forma, os *Firewalls* são ferramentas que tem o objetivo de verificar o que está trafegando entre duas redes distintas. E, com o uso de políticas pré-determinadas, é possível efetuar a filtrarem do que trafegará de informação entre as duas redes. Então com o uso de *Firewall* os administradores de rede conseguem um controle maior do fluxo de entrada

e saída de pacotes da rede. E, assim com a aplicação de políticas, determina quais serviços estarão disponíveis aos usuários (TEIXEIRA JUNIOR, 1999).

O *Firewall* trabalha entre o domínio privado e público da corporação. Normalmente o acesso é feito por um *gateway*, porém quando se tem um *Firewall*, tudo que passa da rede interna com direção a WAN, e vice-versa, estará sendo tratado. Uma de suas características é a capacidade de filtragem de pacotes com base em algumas propriedades, como por exemplo, endereço IP de origem e destino, número de porta de destino e origem, ou outro critério elaborado pela política de uso da Internet da corporação. A filtragem de pacotes pode ser feita de maneira inclusiva ou exclusiva, de forma que na inclusiva, o pacote está dentro das especificações corretas e terá passagem permitida, já na exclusiva o pacote será destruído no momento que estiver saindo ou entrando na rede corporativa da instituição (FARREL, 2005).

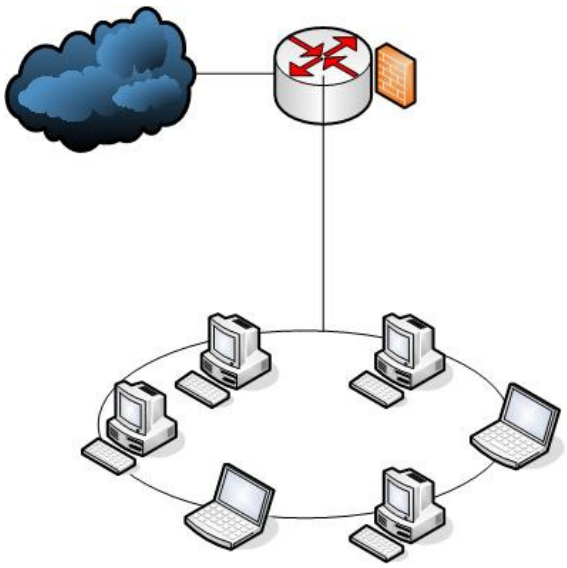

Figura 10. Representação gráfica de *Firewall* (roteador).
Fonte: Adaptado de KUROSE, J; ROSS, K. (2006).

3.4. *PROXY*

O *Proxy* é uma ferramenta que funciona como um *gateway*, a qual todos os usuários passarão para acessar a Internet. Por isso é possível que nele se façam configurações, de quais usuários ou grupos de usuários, possuem acesso à Internet. Para muitos administradores isto pode ser uma solução mais viável, ao invés de usar um *Firewall* com a função de restrição do que será permitido no acesso à Internet, usa-se um *Proxy* com o intuito de especificar quais usuários terão acesso à Internet e quais as permissões específicas de cada usuário. Com a utilização de um servidor *Proxy* os administradores tem registrado o que o usuário acessou em determinado horário e por quanto tempo, por exemplo. Sendo possível a verificação se o usuário acessou *sites* que não são permitidos perante a política da instituição (DIMARZIO, 2001).

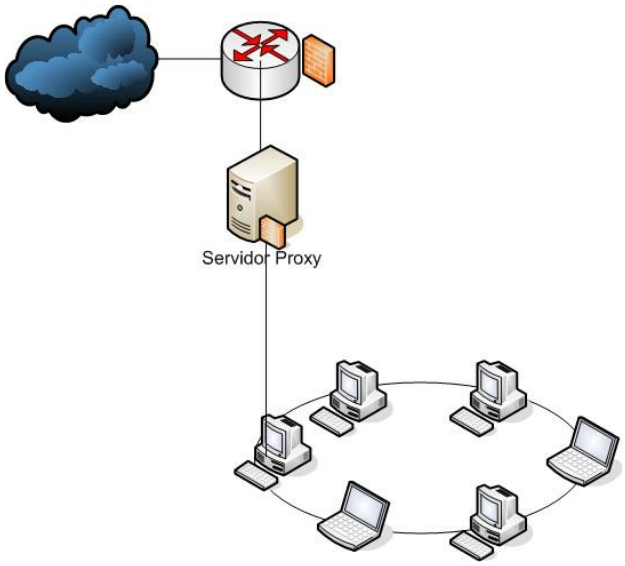

Figura 11. Representação gráfica de *Proxy*.
Fonte: Adaptado de KUROSE, J; ROSS, K. (2006).

3.5. UTILIZAÇÃO INTEGRADA DE *FIREWALL* E *PROXY*

A melhor solução para se garantir um controle maior dos acessos dos usuários a serviços da Internet é a utilização de um *Firewall* e um *Proxy* integrados, determinando assim quais usuários, ou grupo deles irão acessar os serviços disponíveis da Internet, e ainda de que forma será feito este acesso, ou seja, quais *sites* ou serviços estarão especificamente disponíveis para os usuários. Além disso, deve-se manter um registro desses dados para que seja possível utilizar ferramentas estatísticas para elaborar planos de ação perante situações que ocorram na rede (DIMARZIO, 2001).

O uso de *Firewall* com *Proxy* deve auxiliar os administradores de rede na sua tarefa de manter a segurança da informação da instituição, bem como a capacidade de gerar informação e/ou conhecimento a partir de dados armazenados. Com isso é possível a elaboração de estratégias de configuração e assim planejar a aquisição de novos equipamentos, objetivando sempre a manutenção dos serviços disponíveis aos usuários. Estas ferramentas de controle possuem funcionalidades que geram bases de *logs* com dados relacionados ao tráfego da rede. Sendo assim, ferramentas que consigam analisar estes dados, com o intuito de disponibilizar aos administradores informações, são de grande valia.

4 AS CONTRIBUIÇÕES DA ESTATÍSTICA PARA A GESTÃO DE REDES

O volume de dados armazenados não somente por ferramentas de *Firewall* e *Proxy*, como também por outras ferramentas como *Data Webhouses*, pode ser considerável. Segundo Kimball e Merz (2000) tem-se cada vez um volume maior de espaço de armazenamento, e esta quantidade tende a aumentar. Porém busca-se melhorar as técnicas de análise dos dados, como estatística procurando assim o aperfeiçoamento da busca de conhecimento nesses grandes volumes de dados. Sendo assim, ainda segundo Kimball e Merz (2000), uma forma de melhoramento seria o gerente de determinado setor, seja ele no campo de negócios ou em outras áreas, possuir a autonomia de gerar relatórios a partir de sua base de dados com as informações realmente necessárias para visualização.

Desta forma, a estatística retrata modelos que são utilizados de forma a planejar experimentos. Os resultados estatísticos são conseguidos após a obtenção, organização e a simplificação de dados colhidos de alguma forma, seja esta coleta através de entrevistas, questionários, ou por meio da medição de alguma variável que seja quantitativa. Porém, a estatística não é apenas um conjunto de gráficos e cálculo de médias, e sim uma ferramenta importante para gestores tomarem as melhores decisões em seus ambientes de gestão (TRIOLA, 1999).

Mesmo assim, não basta somente dominar as técnicas estatísticas e denominar corretamente os dados da amostra. Deve-se fazer com que essa amostra seja obtida representando uma população. A representatividade da amostra não pode perder as características da população. De certa forma deve-se garantir que a amostra de um determinado dado estatístico tenha uma representação confiável (COSTA NETO, 1981).

Desta maneira, existem técnicas de amostragens que são utilizadas como forma de garantir a representatividade de uma amostra. A técnica de amostragem aleatória simples consiste em selecionar uma amostra por meio de um sorteio, sem restrições, ou seja, todos os elementos da população fazem parte do sorteio. Sendo assim, qualquer estrato retirado do conjunto total de elementos, população, sendo que com o mesmo número de elementos, possui a mesma chance de fazer parte da amostra (BARBETTA, 2004).

Partindo da técnica de amostragem aleatória simples, tem-se a amostragem sistemática que determina que se deva sortear o primeiro elemento, e a partir deste pegar os próximos elementos do conjunto, tornando-se uma amostragem sistemática, porém aleatória. A técnica de amostragem estratificada consiste em adquirir estratos da população, sendo estes estratos semelhantes à população de acordo com os parâmetros utilizados no estudo. Esta técnica se divide em amostragem estratificada proporcional, que é definida onde o tamanho de cada estrato é proporcional a população, e a amostragem estratificada uniforme, onde é selecionado o mesmo número de elementos em cada estrato (BARBETTA, 2004).

Após a verificação das técnicas de amostragem deve-se verificar o tamanho da amostra. Pode-se representá-lo de forma genérica, onde é especificado pelo tamanho de uma *amostra aleatória simples*[19]. A determinação da amostra só é válida cientificamente quando se tem um *erro amostral*[20] que dirá quanto o estatístico pode errar na avaliação de interesse. O enfoque do erro amostral deve ser probabilístico, pois, por maior que seja o tamanho da amostra, sempre existirá o risco de se gerar uma amostra com características distintas da

[19] Aquela em que a probabilidade de escolha de um membro da população para participar da amostra é igual para todos os membros em todas as escolhas (FERREIRA, 1999).

[20] Erro amostral é a diferença entre uma estatística e o parâmetro que se quer estimar (BARBETTA, 2007).

população. A seguir será representada uma fórmula para o tamanho mínimo da amostra perante uma população (BARBETTA, 2007):

$$n_0 = \frac{1}{E_0^2}$$

a) n_0 uma primeira aproximação para o tamanho da amostra;

b) E_0 erro amostral tolerável.

Um primeiro cálculo do tamanho da amostra pode ser feito, mesmo desconhecendo o tamanho da população. Se a população for muito grande (mais que vinte vezes o valor calculado n_0), então n_0, pode ser adotado como tamanho da amostra. Caso contrário, é sugerido o seguinte cálculo para correção:

$$n = \frac{N * n_0}{N + n_0}$$

a) N tamanho (número de elementos) da população;

b) n_0 uma primeira aproximação para o tamanho da amostra, conseguido através do primeiro cálculo;

c) n tamanho mínimo da amostra que deverá ser extraída a partir da população.

Ressalta-se que a relação entre a população e o tamanho da amostra é não linear como pode ser verificado na Figura 12.

Figura 12. Não linearidade do cálculo do tamanho da amostra aleatória simples.
Fonte: BARBETTA, P.; REIS, M.; BORNIA, A. (2008).

Além disso, o método estatístico, que trata da aplicação das teorias estatísticas tornando-se um auxilio para uma investigação, se difere do *método experimental*[21] no sentido de que existem campos de estudo em que os dados não se mantêm constantes, como por exemplo, na coleta de tráfego de uma rede de computadores. Por isso, com a aplicação de modelos estatísticos consegue-se gerir todas as causas possíveis de um fato, mesmo ele sendo inconstante. Com o uso de análise e interpretação estatística é possível obter informações sobre um determinado problema, para assim elaborar procedimentos que possam vir a acarretar em ações e como conseqüência a possível solução do problema (CRESPO, 2002).

Em trabalhos científicos pesquisadores buscam sempre confirmar hipóteses, que são afirmações apresentadas pelo pesquisador. Para confirmação da hipótese deve-se sempre efetuar o levantamento dos dados e analisar os mesmos estatisticamente. O levantamento dos dados sempre vem de dados de amostras, desta forma a decisão final a respeito de uma hipótese está associada à probabilidade de erro. Portanto, estatística inferencial é o método que permite ao pesquisador comprovar suas hipóteses de acordo com um erro mensurado, e por meio de testes estatísticos. Estes testes estatísticos podem atuar sobre dados quantitativos, que se fundamenta em dados como média, bem como dados qualitativos que se baseiam em dados como proporções e probabilidades (CALLEGARI-JACQUES, 2004).

[21] Método científico que consiste em observar um fenômeno natural sob condições determinadas que permitem aumentar o conhecimento que se tenha das manifestações ou leis que regem este fenômeno (FERREIRA, 1999).

Um dos testes de hipóteses é o teste *t de student* que atua sobre o cálculo de probabilidades a partir do erro amostral e não no erro populacional, portanto o cálculo efetuado ocorre a partir da amostra e não da população. O teste *t de student* é utilizado quando se deseja comparar dois conjuntos de dados quantitativos em relação as suas médias apresentadas a partir de amostras e não de populações. O teste é semelhante ao teste da curva normal, porém os dois se diferem em função do primeiro utilizar-se de graus de liberdade, que é um parâmetro determinado por qualquer número real maior ou igual a zero. E ainda, deve-se levar em consideração se o teste da hipótese está realmente apresentando uma diferença significativa estatisticamente (BARBETTA, 2004).

Conforme Callegari-Jaques (2004) uma das possibilidades de uso do teste *t de student* seria na comparação de duas médias onde se busca o cálculo do t que irá representar se a hipótese é rejeitada ou comprovada. Por meio da fórmula a seguir consegue-se chegar no valor de t.

$$t_{calc} = \frac{\bar{x}_A - \bar{x}_B}{\sqrt{s_0^2 (\frac{1}{n_A} + \frac{1}{n_B})}}$$

a) t_{calc} Valor de t perante nível de significância;

b) $\bar{x}_A ; \bar{x}_B$ Valor da média do conjunto A e do conjunto B;

c) s_0^2 Estimativa de variância das duas amostras;

d) $\frac{1}{n_A} ; \frac{1}{n_B}$ O inverso do número de elementos da amostra de A e B.

E ainda conforme Callegari-Jaques (2004), o denominador dessa expressão é o erro padrão das diferenças entre as médias amostrais. Para se efetuar o cálculo desse valor

estima-se a variância da amostra perante a população. Tomando por base que a variância é a mesma para as duas populações A e B, obtém-se s_0^2, que é a variância estimada para duas amostras pela média ponderada das variâncias amostrais, como pode ser verificado na fórmula a seguir:

$$s_0^2 = \frac{(n_A - 1)s_A^2 + (n_B - 1)s_B^2}{n_A + n_B - 2}$$

Onde a obtenção da variância calcula-se a partir da fórmula a seguir. Fórmula essa que diz que a variância de um elemento consegue-se a partir da soma de todos os elementos multiplicado pelo valor d_i elevado a segunda potência, e dividindo-se pelo valor *n -1*.

$$s^2 = \frac{\sum_{i=1}^{n} d_i^{\,2}}{n-1}$$

O valor de d_i pode ser obtido pela subtração do valor de x da média de todos os valores. Como pode ser verificado na expressão a seguir.

$$d_i = x_i - \bar{x}$$

Sendo assim por meio do cálculo do valor de *t de student* pode-se verificar se há evidências a um nível de significância α estipulado pelo pesquisador que o a amostra A, ou B, é estatisticamente mais significante perante uma população (BARBETTA, 2004).

Desta forma, a análise estatística auxilia na interpretação de dados por meio de relatórios, gráficos e outras formas de representação. Sendo possível por meio destes a obtenção de dados e informações sobre a análise efetuada.

É importante ressaltar que análises estatísticas são métodos que auxiliam a tomada de decisões por parte dos gestores. Isso pode ser aplicado em diversas áreas, e uma delas é a informática. Com o uso de análises estatísticas aplicadas, é possível se buscar soluções para problemas. Como por exemplo, avaliar o desempenho de um serviço disponibilizado para usuários, desde que exista alguma forma de se medir e analisar um registro com esses dados.

4.1. ANÁLISE ESTATÍSTICA APLICADA A INFORMÁTICA

Anteriormente ao uso de computadores como ferramentas estatísticas, a maior parte do trabalho executado para se fazer uma análise estatística era o cálculo manuscrito muitas vezes com o uso da calculadora. Com a utilização do computador como ferramenta estatística, o cálculo deixou de ser a mais importante, podendo-se dar ênfase a parte de análise dos dados estatísticos (BISQUERRA; SARRIERA; MARÍNEZ, 2004).

Por isso, a questão não é a quantidade de informação disponível para análise, mas sim como essa informação poderá ser tratada pelos gestores, a fim de achar as melhores soluções para os problemas (LEVINE; BERENSON; STEPHAN, 2000).

Com isso, sistemas computacionais são utilizados como ferramentas de auxílio na gestão dessas grandes quantidades de dados disponíveis para análise, para que seja possível extrair a informação de um volume de dados. Estes sistemas computacionais possuem uma variabilidade constante de premissas. Pode-se então usar modelos estatísticos para avaliar características computacionais como processamento, percentual de utilização de memória,

taxa de transferência de dados, e ainda de forma mais perceptível ao usuário, pode-se avaliar tempo de resposta de um aplicativo, taxa de transferência de mensagens entre computadores com a utilização de um serviço de correio eletrônico, entre outros. Estes modelos podem ser considerados como uma forma de representação da realidade, dando ênfase aos aspectos que realmente têm importância e excluindo dados que não acarretarão na avaliação dos resultados obtidos (BARBETTA; REIS; BORNIA, 2008).

Pode-se dizer que segundo Milone (2004), modelo estatístico entende-se como uma representação de forma reduzida de um fenômeno, objeto ou evento. Serve como um instrumento que permite uma simulação experimental, com o intuito de descrever, verificar, explicar, controlar ou produzir eventos similares. Cada área possui seus modelos estatísticos específicos, porém estes são divididos em cinco grupos, como apresentados a seguir:

a) **determinísticos:** são os que estabelecem claramente suas variáveis, podendo ser tratados de forma experimental;
b) **estatísticos:** que fixam relações entre dados variáveis ou constantes e que ocorrem de forma casual;
c) **estocásticos:** são aqueles em que seus componentes se desenvolvem de acordo com o processo;
d) **caóticos:** onde o erro possível na variável analisada pode decorrer de fatos casuais e naturais;
e) **descritivo:** que aponta características de um evento, através de tabelas, entre outros.

Levando-se em consideração os modelos estatísticos na área de Tecnologia da Informação, pode-se usufruir do modelo determinístico, sendo possível gerar gráficos e

relatórios a partir de bases de dados armazenadas por ferramentas e podendo efetuar o planejamento na disponibilização de novos serviços.

Dentro deste âmbito de aplicabilidade de modelos estatísticos, pode-se elaborar ferramentas de suporte aos administradores de rede, onde estas ferramentas, utilizando-se de métodos estatísticos como formas de visualização dos dados gerados pelo monitoramento da rede, tenham a capacidade de transformar estes dados em informação. Essas análises estatísticas dão suporte aos gestores de diversas áreas, então a aplicabilidade de análises estatísticas na área de monitoramento do uso dos serviços de rede dentro de uma corporação se torna viável.

5 ALGUNS EXEMPLOS DE MONITORAMENTO DE REDES POR MEIO DE MÉTODOS ESTATÍSTICOS

O serviço de auxílio à administração de redes de computadores por meio de análise dos serviços vem sendo estudado em diversas oportunidades pela comunidade científica, sendo alguns deles descritos a seguir:

a) A Universidade do Extremo Sul Catarinense – UNESC, Trombim (2006), desenvolveu um trabalho abordando uma técnica de amostragem estatística, onde foi analisado o tráfego no servidor *Proxy* da rede acadêmica da universidade. Este *Proxy* possuía sistema operacional LINUX, e foi utilizado o software *ethereal* para efetuar o monitoramento e assim aplicar os conceitos de amostragem estatística.
b) Ainda na Universidade do Extremo Sul Catarinense – UNESC, Jesus (2008), aplicou o método de estatística estratificada para efetuar o monitoramento do tráfego na empresa TSA Química do Brasil. Por meio do monitoramento foi possível analisar o que estava trafegando na rede da empresa e pode-se então repassar aos administradores de rede possíveis otimizações para o uso dos serviços de rede da empresa. Pode-se ainda verificar o quanto de banda estava sendo utilizado por todos os serviços disponíveis, podendo-se averiguar o tráfego gerado para o servidor de e-mail, servidor de banco de dados, servidor de arquivos, etc.
c) Na Universidade Federal do Rio Grande do SUL – UFRGS, Alex Fabio Pellin desenvolveu um trabalho chamado de Um Monitor de Transações de Serviços de Internet. O mesmo focou o trabalho no intuito de as empresas possuírem cada vez mais a necessidade de se desenvolver ferramentas de auxilio aos administradores

de rede. Por meio da avaliação de ferramentas de monitoramento Alex desenvolveu um protótipo de monitoramento de interfaces que se utilizam do protocolo TCP/IP para o tráfego dos dados. O trabalho foi desenvolvido para a obtenção do título de mestre em Ciência da Computação, sendo que o mesmo efetuou uma comparação das ferramentas do mercado com o protótipo desenvolvido (PELLIN, 2004).

6 MONITORAMENTO DE REDE: ESTUDO DE CASO NA SATC

Nesta parte do trabalho será apresentado como foram efetuados os procedimentos de coleta e monitoramento de interface de saída para a Internet da SATC, os cálculos de estatística estratificada realizados para efetuar o monitoramento da interface, a forma como foi desenvolvido o protótipo ferramenta análise de *logs* do *Firewall/Proxy*, e ainda os resultados obtidos com o desenvolvimento do protótipo do HEFESTO e de que forma ele auxilia na gerência de redes da SATC.

6.1. CENÁRIO ONDE FOI APLICADO O ESTUDO

O ambiente onde foi feito o estudo de caso divide-se em duas estruturas básicas, sendo elas definidas neste trabalho como *rede acadêmica*, que define a forma de acesso dos discentes, docentes e pesquisadores da SATC, e, a r*ede corporativa* que é acessada pelos colaboradores da mesma.

Estas duas estruturas estão separadas fisicamente e logicamente por meio de equipamentos e meios físicos. O controle do acesso a WAN é feito pelas duas redes por meio de dois servidores de *Firewall/Proxy* diferentes, sendo aplicadas políticas de forma distintas para as duas redes, ou seja, as políticas aplicadas aos discentes, docentes e pesquisadores, são diferentes das políticas aplicadas aos colaboradores da instituição. Sendo que muitos dos docentes e pesquisadores, em certos horários usufruem do acesso corporativo, em função de suas atividades extra classes.

O link de acesso a Internet é provido pela Rede Catarinense de Telecomunicações (RCT), integrante da Fundação de Apoio à Pesquisa Científica e Tecnológica de Santa Catarina (Fapesc), que é um órgão do governo de Santa Catarina. Este link é disponibilizado pela RCT à Universidade do Extremo Sul Catarinense (Unesc), que então disponibiliza à SATC. O link provido possui capacidade de 20Mbps, compartilhado entre algumas instituições de ensino.

Figura 13. Equipamentos CPD onde se encontram os Servidores de *Firewall/Proxy*.

6.1.1. Rede Acadêmica

No campus principal da instituição circulam em média 5100 pessoas, levando-se em consideração discentes, docentes e pesquisadores. A SATC possui cerca de 23 laboratórios de informática, porém aproximadamente 13 deles possuem acesso a Internet, com média de 20 computadores em cada laboratório. Estes laboratórios possuem links de fibra óptica com a Central de Processamento de Dados (CPD).

No CPD existe um switch CISCO Catalyst 3560 onde todos os *links* dos laboratórios se interconectam fisicamente, porém não logicamente, pois as redes dos laboratórios, com exceção de algumas, são separadas logicamente por meio deste *switch* que trabalha na camada de internet do modelo TCP/IP. Este *switch* possui um link com o ISA Server acadêmico, onde é feito o registro em bases de dados de tudo o que trafega de dentro para fora, e vice-versa, da rede acadêmica. A Figura 14 está representando graficamente a estrutura acadêmica dos laboratórios e na Figura 17 pode-se observar o CISCO Catalyst 3560.

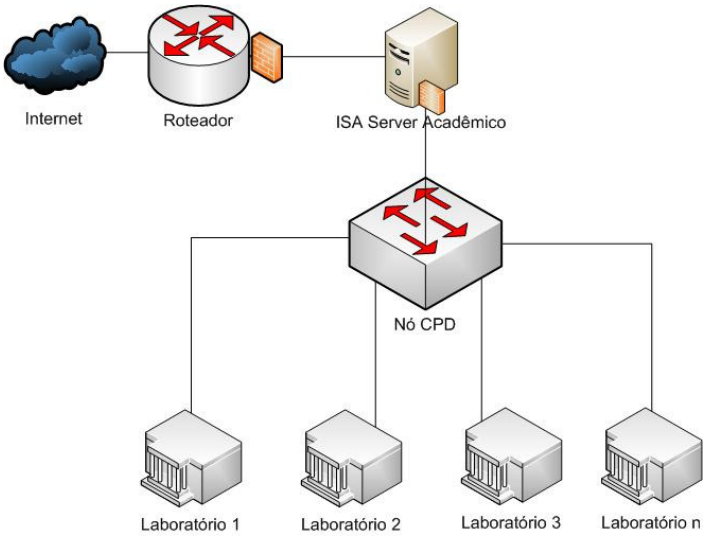

Figura 14. Estrutura da rede acadêmica.

Além da rede acadêmica a rede corporativa possui acesso ao link de Internet por meio de um switch CISCO Catalyst 2960. Portanto foi por meio do monitoramento de uma interface deste switch se tornou possível o monitoramento para posterior análise dos dados coletados.

6.1.2. Rede Corporativa

A rede corporativa se designa da mesma forma que a rede acadêmica possuindo *links* de fibra óptica com os prédios da SATC, chegando eles até o CPD onde os colaboradores têm o acesso aos serviços disponibilizados, inclusive a Internet. No CPD são distribuídos entre *switches*, que atuam na camada rede do modelo TCP/IP, interligados em cascata com os servidores de um modo geral, como pode ser visualizado na Figura 15. Neste mesmo cascateamento está o servidor de *Firewall/Proxy* corporativo onde estão armazenados os dados referentes aos registros de acesso a Internet. O servidor de *Firewall/Proxy* corporativo possui uma característica que se difere da rede acadêmica. Característica esta que está no fato de existir uma política de autenticação do usuário, onde cada colaborador possui um usuário e senha para ter o acesso ao serviço de Internet.

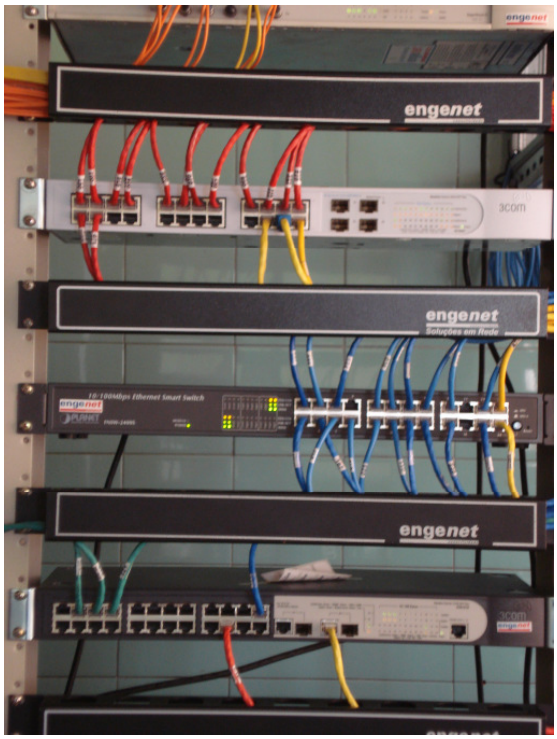

Figura 15. Cascateamento rede corporativa.

O número de colaboradores da SATC hoje está em torno de 600, porém cerca de 300 deles tem acesso direto aos serviços disponibilizados. Na Figura 16 pode-se visualizar graficamente como está representada a rede corporativa da instituição.

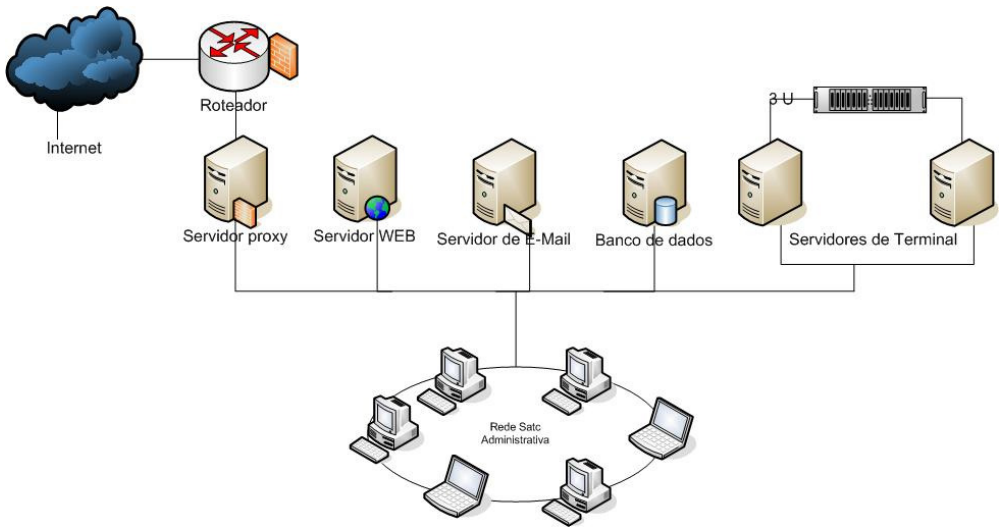

Figura 16. Estrutura da rede corporativa.

O acesso a WAN é feito pelo mesmo link, por isso as duas redes estão interligadas fisicamente por meio de um *switch* CISCO 2960, que atua na camada de internet do modelo TCP/IP, neste equipamento que está interligado o link WAN da instituição. A Figura 17 está mostrando os nós que fazem a ligação da rede acadêmica e corporativa com a interface de saída para Internet.

Figura 17. Equipamentos de interligação do ISA Server com a saída para a Internet.

A ferramenta utilizada para monitoramento bem como os métodos de monitoramento efetuados no ambiente apresentado até esta seção estão descritos no desenvolvimento deste trabalho.

6.2. METODOLOGIA

Os dados apresentados a seguir são pertinentes aos estudos efetuados bem como visualizados durante o processo de desenvolvimento do trabalho. Algumas informações serão omitidas em função da privacidade dos dados da empresa onde foi aplicado o estudo de caso.

Em um primeiro momento será descrito o motivo pelo qual se optou desenvolver este trabalho, mostrando uma hipótese problemática bem como suas possíveis comprovações. Serão apresentados os métodos utilizados para comprovação da hipótese tornando-a um problema.

A seguir conforme já citado na justificativa descreve-se o problema que ocorria e que deu origem ao comprometimento e elaboração deste trabalho.

6.2.1. Hipótese levantada perante diagnóstico informal

O desenvolvimento do protótipo surgiu da necessidade de que os usuários da rede onde foi efetuado o estudo de caso reclamavam que em determinados horários o acesso ficava mais lento que o normal, prejudicando o desempenho da rede local. Sendo assim como forma de diagnóstico do problema foram adotados dois métodos, o primeiro seria por meio de questionário aplicado aos usuários do serviço. O segundo seria utilizar o método de estatística estratificada, já utilizado em outros trabalhos, Trombim (2006) e Jesus (2008), para se comprovar os horários que a rede se apresentava com volume de acessos elevado.

6.2.2. Métodos utilizados para comprovação da hipótese

O primeiro método levantado para se efetuar a possível comprovação do que acontecia por informação dos usuários do sistema, seria a aplicação de um questionário dentro do universo de usuários comprovando o possível problema, e efetuar o possível diagnóstico dos horários em que o problema ocorria. Porém fazendo-se uso do que foi apresentado no Capítulo 4, mais precisamente no item que relata o método de estatística, onde a partir de uma população extraem-se parcelas que sejam realmente representativas da população, o processo

de questionário se tornou inviável devido ao fato de ter que efetuar aproximadamente 670 entrevistas com os usuários e após efetuar as entrevistas tabular os resultados. A seguir está descrito o cálculo efetuado para se chegar ao extrato realmente representativo da população de usuários.

N ≅ 5100 (população de usuários)

E_0 = 3,6% (erro amostral)

n ≅ 670 (tamanho do extrato)

$$n_0 = \frac{1}{E_0^2} \qquad n = \frac{n_0.N}{n_0 + N}$$

$$n_0 = \frac{1}{(0{,}036)^2} \qquad n = \frac{771.5100}{771+5100}$$

$$n_0 = \frac{1}{0{,}001296} \qquad n = \frac{3.932.100}{5871}$$

$$n_0 \cong 771 \qquad n \cong 670$$

O extrato varia de acordo com o tamanho da população e com o erro amostral utilizado. Porém quanto menor a população maior será o tamanho do extrato perante àquela população, para fazer com que este extrato seja representativo em relação à amostra. A seguir está um exemplo de uso do método de estatística onde foi realizado o mesmo cálculo para descobrir as intenções de voto para prefeito da cidade de Criciúma do ano de 2008, o cálculo foi retirado a partir dos dados fornecidos pelo documento que se encontra no Anexo A.

N ≅ 132.007 (população de eleitores)

E_0 = 3,6% (erro amostral)

n ≅ 765 (tamanho do extrato)

$$n_0 = \frac{1}{E_0^2} \qquad n = \frac{n_0.N}{n_0 + N}$$

$$n_0 = \frac{1}{(0{,}036)^2} \qquad n = \frac{771.132.007}{771 + 132.007}$$

$$n_0 = \frac{1}{0{,}001296} \qquad n = \frac{101777397}{132778}$$

$$n_0 \cong 771 \qquad n \cong 765$$

Comparando-se as duas formas de cálculo apresentadas, o tamanho da população do segundo cálculo é muito maior que o primeiro. Usando-se do mesmo erro amostral os extratos calculados se tornam muito diferente relacionados à proporção.

Descartando-se a possibilidade de aplicar um questionário dentro da instituição em função de tempo hábil para se tabular os resultados, aplicou-se um método de estatística estratificada na interface de saída para Internet da instituição. Método este utilizado de forma semelhante por, Trombim (2006) e Jesus (2008), sendo que os mesmos apresentaram resultados satisfatórios.

O monitoramento da interface de saída foi efetuado com o auxílio da ferramenta *PRTG Traffic Grapher V6.0.6.675*. É possível se utilizar a ferramenta por 30 dias de forma *Shareware*[22] após cadastro junto ao site do desenvolvedor (http://www.paessler.com). O fabricante ressalta ainda que para utilização em estudos e testes o produto pode ser utilizado de forma *Trial* sendo ainda de grande auxílio para verificações.

[22] Software distribuído numa base experimental, por meio de serviços online, e-mail e grupos de usuários (BLACK BOX, 1997).

6.2.3. Coleta base efetuada e Definição do tempo de cada coleta

Por meio da ferramenta *PRTG Traffic Grapher* foi efetuada uma coleta base no dia 08/04/2009, e assim a partir desta coleta base verificou-se quais horários o problema realmente ocorria. Como se pode verificar pelo gráfico, existe um horário de pico entre 09:00 e 10:00 da manhã e a partir das 14:00 até as 17:00, horários estes de maior reclamação por parte dos usuários.

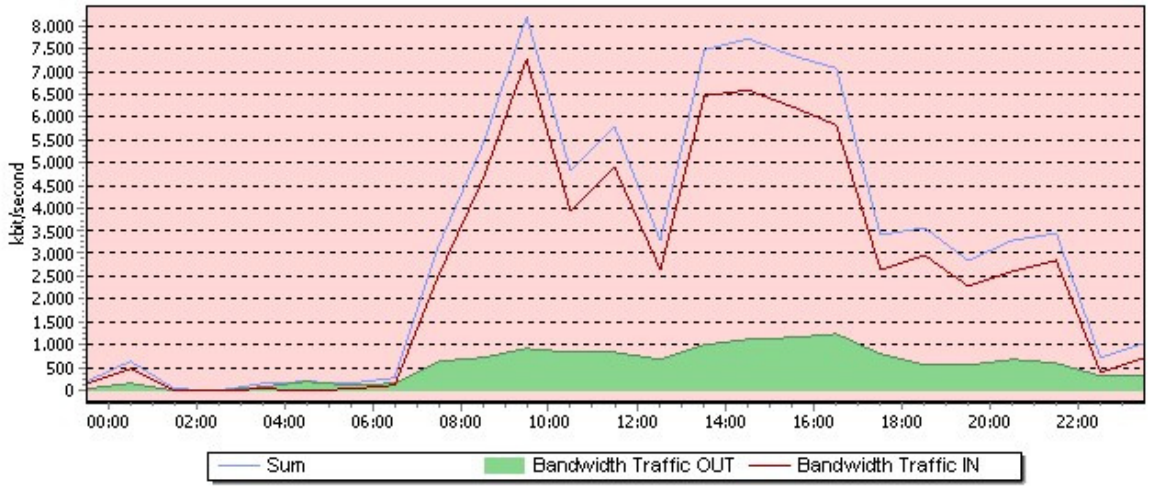

Figura 18. Coleta base efetuada no dia 08/04/2009.

Pode-se verificar os dados utilizados para se gerar o gráfico no Apêndice A. A partir da coleta efetuada no dia 08/04/2009, foram efetuados os cálculos de estatística estratificada apresentado no Capítulo 4 deste trabalho, conforme estão especificados no Apêndice B. Por meio dos cálculos efetuados foi possível gerar a

Tabela 1, onde estão apresentados os tempos de monitoramento para cada dia da semana informado de maneira aleatória conforme, Barbetta (2008). O horário utilizado para monitoramento da interface foi das 07:00 às 22:00, horário de expediente e de aula da

instituição onde foi feito o estudo de caso, e horário que contém uma representação significativa diante da população.

Tabela 1. Horários e tempo de duração de cada coleta.

Dia da Semana	Coleta	Horário de Coleta	Tempo de Coleta
Sexta-feira	1	07:00 às 08:00	00:02:48
Quarta-feira	2	08:00 às 09:00	00:04:02
Quinta-feira	3	09:00 às 10:00	00:06:14
Terça-feira	4	10:00 às 11:00	00:04:00
Sexta-feira	5	11:00 às 12:00	00:02:57
Segunda-feira	6	12:00 às 13:00	00:02:38
Segunda-feira	7	13:00 às 14:00	00:06:01
Quinta-feira	8	14:00 às 15:00	00:06:17
Quarta-feira	9	15:00 às 16:00	00:05:51
Quarta-feira	10	16:00 às 17:00	00:05:29
Segunda-feira	11	17:00 às 18:00	00:06:01
Quinta-feira	12	18:00 às 19:00	00:03:07
Sexta-feira	13	19:00 às 20:00	00:02:14
Terça-feira	14	20:00 às 21:00	00:02:48
Terça-feira	15	21:00 às 22:00	00:02:58

A partir do tempo de monitoramento definido foi utilizada a ferramenta *PRTG Traffic Grapher V6.0.6.675* para gerar os gráficos de utilização nos horários especificados. A ferramenta utilizada possui relatórios a partir da escala de minutos. Portanto para se manter uma representatividade dos dados, Barbetta (2008) retrata que se deve arredondar o tempo de monitoramento para cima. No apêndice B é possível verificar o tempo de monitoramento com o volume de tráfego apresentado na interface.

Por meio dos dados apresentados nos Apêndice B, Apêndice C, Apêndice D, Apêndice E, Apêndice F e Apêndice G, foi possível gerar o gráfico a seguir, comprovando os horários de maior tráfego na rede e assim verificando-se os horários de maior volume de requisições ao serviço de Internet.

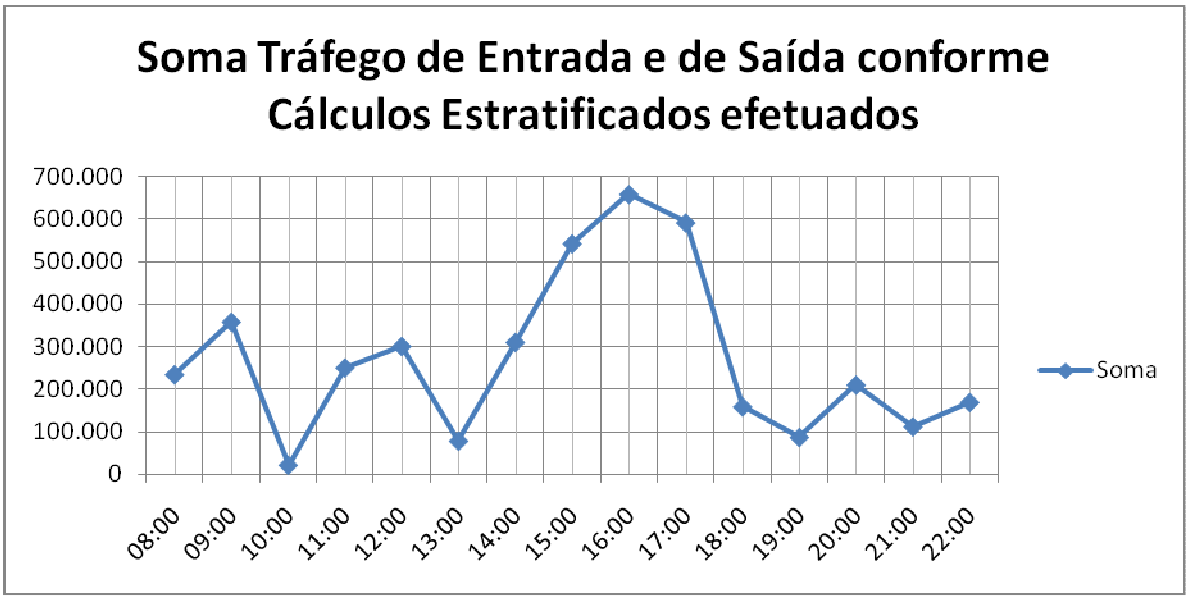

Figura 19. Gráfico de Monitoramento após coleta efetuada.

Comparando-se a Figura 18 e Figura 19 é possível verificar o andamento do fluxo de dados de um dia como também de uma semana. Desta forma, os cálculos apresentados constatam que no período vespertino ocorre um maior volume de tráfego de dados na interface, comprovando assim o problema relatado pelos usuários do serviço.

Sendo assim deverá ser verificado o que está trafegando nos horários em que o volume de tráfego é superior ao restante do dia. Isto se dá através de análise dos *logs* gerados pelos ISA Servers instalados na instituição.

6.2.4. Microsoft Internet Security and Acceleration 2006 – ISA Server

O Microsoft ISA Server é uma ferramenta que possui a funcionalidade de *Firewall/Proxy* trabalhando na camada de aplicação do modelo TCP/IP. Por meio desta é feito

o encaminhamento de requisições e respostas entre a Internet e os clientes internos. Possui a aplicabilidade de filtros e bloqueio a sites específicos de acordo com políticas adicionadas.

O ISA Server 2006 gera um arquivo de *logs* por dia. Este, tem como funcionalidade o possível acompanhamento e análise do Serviço de *Firewall* e *Web Proxy*. Pode-se gerar por meio do ISA *logs* nos seguintes formatos: W3C (World Wide Web Consortium), formato de arquivo nativo do ISA Server, Open Database Connectivity (ODBC), MSDE 2000 e Microsoft OLE Provider. O ISA Server divide a geração dos *logs* em dois arquivos diferentes especificados por *Firewall Logging* e *Web Proxy Logging*. No primeiro os dados armazenados são referentes à conexão entre os clientes internos e externos sendo armazenados dados referentes a ataques externos e internos da rede. Já no *Web Proxy Log* ficam os dados referentes à camada de aplicação, atuando em protocolos como HTTP, HTTPS, SSL-Tunnel, FTP, SMTP, etc.

Outra possibilidade de configuração da ferramenta no âmbito de geração dos arquivos de *logs* é o fato de poder selecionar quais os campos que realmente são necessários armazenar em arquivos para posterior análise. O Anexo B está mostrando todos os campos possíveis de configuração no ISA Server.

6.2.5. Modelagem da aplicação HEFESTO

A modelagem da aplicação HEFESTO foi feita sobre os padrões *Unified Modeling Language* (UML), com o intuito de se desenvolver os diagramas de caso de uso e de atividade.

O diagrama de caso de uso mostra as funções desempenhadas pelo usuário e pelo sistema, como pode ser verificado pela Figura 20:

a) O usuário especifica os parâmetros de entrada, como data de utilização e tipo de base de dados a ser utilizada;
b) O sistema se encarrega de processar os relatórios e trazer para o usuário os resultados.

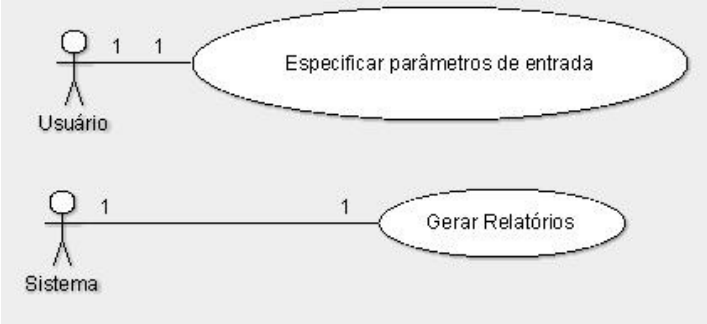

Figura 20. Diagrama de caso de uso do HEFESTO.

O diagrama de atividades, que está demonstrado através da Figura 21, mostra as atividades desempenhadas dentro do sistema, onde é informada a data e o tipo de base de dados. Caso a base de dados não exista o usuário será informado por Base não encontrada, caso exista o usuário conseguirá visualizar os relatórios.

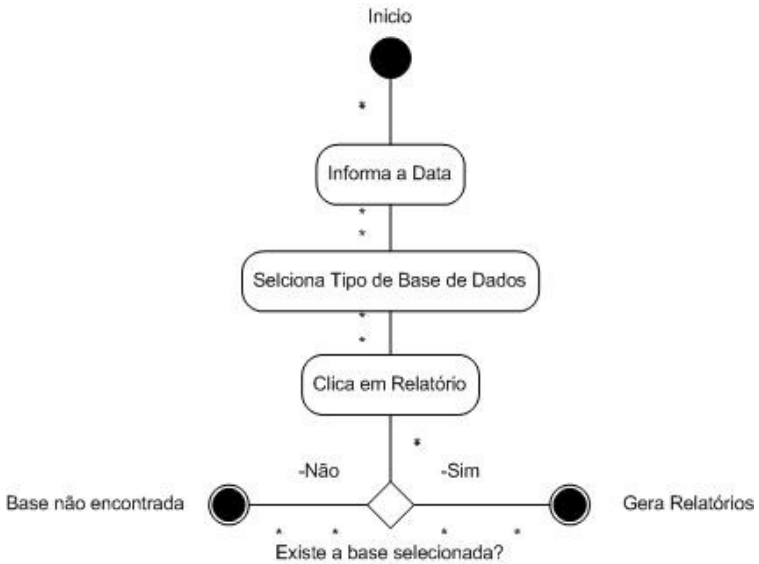

Figura 21. Diagrama de atividades.

6.2.6. Método utilizado para determinação do parâmetro de maior significância

Perante a coleta base efetuada no dia 08/04/2009 foi efetuado o teste *t de* student com o intuito de determinar o parâmetro de maior significância se comparando o Tráfego de Entrada e o Tráfego de Saída da interface de comunicação com a internet da SATC. Como o monitoramento foi efetuado a partir da variável de soma do Tráfego de Entrada e de Saída da interface, deve-se verificar qual valor tem maior significância, se é o Tráfego de Entrada ou o Tráfego de Saída da mesma.

Para efetuação dos cálculos foram utilizados os métodos do cálculo do teste *t de student* apresentados no capítulo 4 deste estudo. Desta maneira, a seguir está apresentada a seqüência de cálculos efetuados a partir de um nível de significância (α) de 5%, onde os dados utilizados para efetuação dos cálculos podem ser verificados no Apêndice A.

Serão apresentados os cálculos com a primeira amostra da variável *Bandwidth Traffic IN*, sendo desnecessária a apresentação dos cálculos com a segunda variável *Bandwidth Traffic OUT* como também o cálculo com todas as amostras da primeira variável, devido aos dois parâmetros possuírem o mesmo raciocínio.

- Descoberta do valor de significância da variável *Bandwidth Traffic IN*

$$\bar{x}_{IN} = \frac{\sum_{i=1}^{n} xi}{n} = 1212615{,}69$$

$$d_{IN_1} = 318464{,}38 - \chi_{IN} = 318464{,}38 - 1212615{,}69 = -894151{,}32$$

$$d_{IN_1}^2 = (-894151{,}32)^2 = 799506575308{,}43$$

O cálculo de todos os valores de *d* para as amostras bem como para as amostras da variável *Traffic Bandwidth OUT* são os apresentados nos Apêndice HApêndice I.

$$s_{IN}^2 = \frac{\sum_{n=1}^{n} di^2}{n-1} = \frac{26865327810625{,}50}{23} = 1168057730896{,}76 = 1{,}1681\text{E}+12$$

- Descoberta do valor de significância das duas médias

A partir do valor de s_{IN}^2 e s_{OUT}^2, calcula-se o valor se significância s_O^2

$$s_0^2 = \frac{(n_A - 1)s_A^2 + (n_B - 1)s_B^2}{n_A + n_B - 2} = \frac{((24-1) * (1{,}16806\text{E}+12)^2) + ((24-1) * (27816599279)^2)}{(24+24)-1} \Rightarrow$$

$$s_0^2 = 597937165087{,}67 = 5{,}97937\text{E}+11$$

- Cálculo *t de student*

Após detecção do valor de s_O^2 calcula-se o valor de *t*.

$$t_{calc} = \frac{\chi_A - \chi_B}{\sqrt{s_0^2(\frac{1}{n_A} + \frac{1}{n_B})}} = \frac{1.212.615{,}69 - 252.602{,}54}{\sqrt{5{,}97937\text{E}+11(\frac{1}{24} + \frac{1}{24})}} = 4{,}300708755$$

- Definição da significância da variável *Bandwidth Traffic In* sobre a variável *Bandwidth Traffic OUT*

Após determinação do t_{calc} verifica-se o valor de *t tabulado*, este valor pode ser conseguido a partir do nível de significância juntado ao grau de liberdade apresentado no cálculo. Os valores de *t tabulado* podem ser encontrados no Anexo D. Como pode ser verificado na Figura 22, o valor de t_{calc} é maior que o valor de $t_{0,05;46}$.

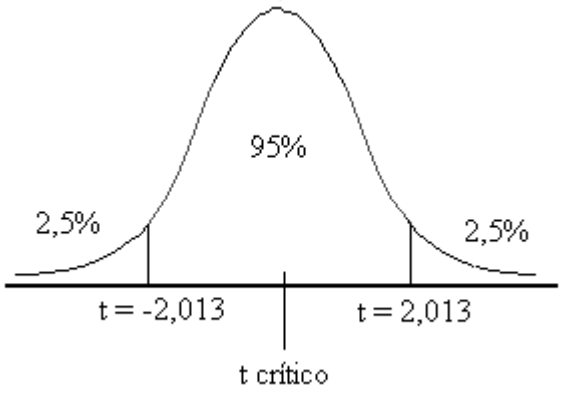

Figura 22. Representação da Curva do teste *t de student*.

Os dados calculados pelo teste *t de student* estão apresentados na Tabela 2.

Tabela 2. Valores encontrados nos cálculos do Teste *t de student.*

Média IN	1.212.615,59
Média OUT	252.602,54
n IN	24
n OUT	24
Alfa(nível de significância)	5% (0,05)
Grau de Liberdade	46
s_{IN}^2	1,1681E+12
s_{OUT}^2	27.816.599.279
s_0^2	5,97937E+11
$t_{0,05;46}$	2,013
t_{calc}	4,300708755

Portanto, como se tem 4,3 > 2,013, há evidências a um nível de significância α = 0,05 de que o tráfego de entrada representado pela variável *Bandwidth Traffic IN*, é maior que o tráfego de saída representado pela variável *Bandwidth Traffic OUT*. Desta forma os relatórios apresentados pelo HEFESTO estão organizados pelo tráfego de entrada de dados, que é a variável que possui maior significância estatística perante os tráfego de dados monitorado.

6.3. HEFESTO

O protótipo da ferramenta de análise de *logs* dos ISA Server – Hefesto - foi desenvolvido sob a ótica de auxiliar os administradores de rede na SATC onde foi feito o estudo, objetivando a interpretação dos dados gerados pela ferramenta de *Firewall/Proxy* utilizada chamada de Microsoft Internet Security and Acceleration 2006. Por meio de relatórios apresentados sob a linguagem ASP, tentou-se desenvolver relatórios capazes de chegar a informações necessárias aos administradores de rede.

A opção de armazenamento escolhida para utilização no trabalho foi MSDE 2000, onde se pode gerar a base de dados em um SQL Server que estava na mesma rede. Para o desenvolvimento do protótipo da ferramenta foram utilizados os dados gerados na base de dados de *Web Proxy Log* pois o intuito da mesma é auxiliar o gerenciamento de uso do recurso interno dos usuários, verificando-se o que está sendo acessado e em qual momento.

Todos os campos foram utilizados na geração dos *logs* durante o processo de desenvolvimento do protótipo. Porém após verificação das informações solicitadas pela

administração de rede da SATC, foram selecionados somente os atributos necessários para geração dos relatórios. Com isso, obteve-se uma diminuição no tamanho das bases de dados, bem como, se conseguiu um melhor desempenho na geração dos relatórios. Os campos utilizados para geração dos relatórios estão apresentados na Tabela 2.

Tabela 3. Campos utilizados para geração dos relatórios HEFESTO.

Campo	Descrição
ClientIP	Endereço IP do Cliente
ClientUserName	Conta de usuário que fez a solicitação. Um ponto de interrogação (?), ao lado do nome do usuário indica que o nome do usuário foi enviado, porém o mesmo não foi autenticado pelo ISA Server. Se o ISA Server não está configurado para controle de acesso por usuários, o mesmo é listado como Anonymous.
logTime	A hora local quando ocorreu o evento de autenticação.
DestHost	O nome do computador de destino que forneceu o serviço para a conexão atual. Um hífen (-) neste campo pode indicar que o objeto solicitado foi concedido pelo cache local.
Processingtime	Total de tempo, em milisegundos, que foi necessário para o ISA Server processar a conexão atual. Sendo contado a partir do momento que se inicia a conexão até quando o cliente recebe todos os dados e fecha a conexão.
Bytesrecvd	Total de bytes recebidos pelo computador remoto, vindo do cliente.
Bytessent	Total de bytes enviados do computador remoto para o cliente.
Protocol	Protocolo utilizado pela conexão, no nível de aplicação.
Uri	URL solicitada pelo cliente.

Após verificação dos campos necessários para geração dos relatórios, foi efetuado o desenvolvimento do protótipo utilizando-se a linguagem de programação ASP. Foi escolhida essa linguagem devido ao fato de que a instituição já possui um portal corporativo todo nesta linguagem e ainda, com o intuito de que no futuro a ferramenta se torne disponível em tempo de execução junto ao portal do colaborador da empresa.

Para efetuação dos testes com o Hefesto foram utilizadas catorze bases de dados disponibilizadas pela instituição. Sendo sete delas geradas pelo ISA Server Acadêmico e sete delas pelo ISA Server Corporativo. Os dados armazenados pelo ISA Server são sempre relativos a ele, portanto quando apresentado nos relatórios descrição de Bytes Recebidos,

seriam os bytes recebidos do cliente interno para com o ISA Server, e quando for apresentado a descrição Bytes Enviados, serão os dados enviados por ele ao cliente interno.

6.3.1. Relatórios gerados e apresentados como forma de monitoramento

Os relatórios apresentados para as bases de dados se diferem devido ao fato que os mesmo estão ligados aos dados armazenados. Desta maneira conforme a data e o tipo de base de dados selecionados na interface principal (Figura 23), os relatórios serão apresentados.

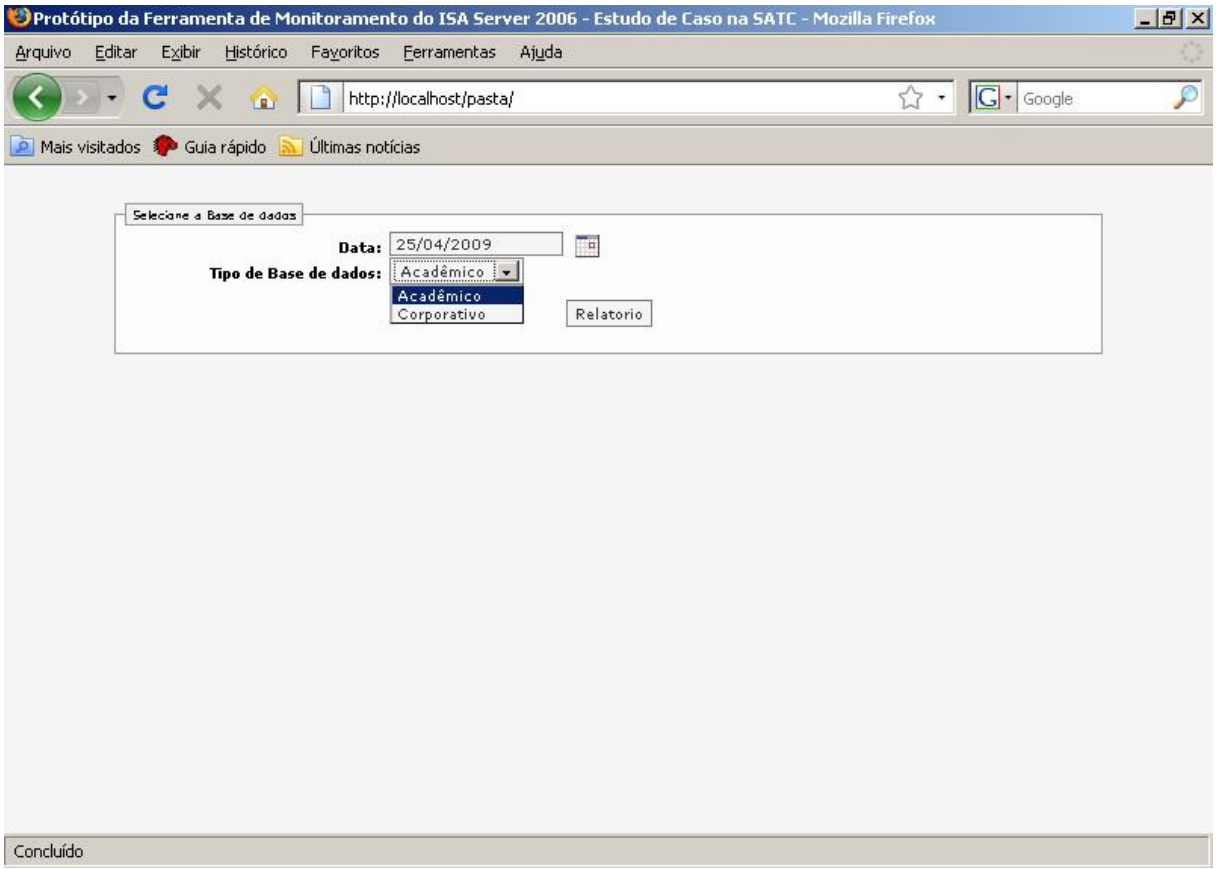

Figura 23. Interface principal HEFESTO.

O usuário deverá especificar qual base de dados estará sendo verificada e de qual dia. Após essa especificação o HEFESTO gera os possíveis relatórios de acordo com as informações selecionadas. Os possíveis relatórios gerados podem ser verificados na Tabela 3.

Tabela 4. Relatórios gerados pelo HEFESTO.

Descrição Relatório	**Acadêmico**	**Corporativo**
Top Site	X	X
Top Cliente IP	X	X
Top Usuário	-	X
Top Laboratório	X	-
Top Protocolo	X	X
Gráfico de Fluxo de Dados	X	X
Gráfico por hora	X	X
Relatório de Uso por Hora	X	X

Como base de informações para escrita do trabalho foi utilizada a base de dados do dia 24/04/2009, pois se trata de uma sexta-feira e onde foi constatado um volume maior de dados. Bem como por meio deste dia é possível se verificar uma quantidade maior de informações. A seguir estão descritos os relatórios gerados pelo HEFESTO. Lembrando que informações como nome de usuário estão sendo restringidas em função das políticas de acesso da SATC.

- Top Site (Figura 24)

Apresenta os sites mais acessados durante o dia conforme volume de dados trafegados, sendo possível por meio deste verificar o tempo gasto naquele site, o número de bytes recebidos, e bytes enviados, e o total de requisições efetuadas. Este relatório é apresentado para os dois tipos de base de dados. Por meio do acesso ao link total de requisições é possível se verificar o IP de acesso, o usuário, data e hora, url, tempo de processamento, bytes recebidos e bytes enviados de acordo com cada requisição efetuada para aquele site.

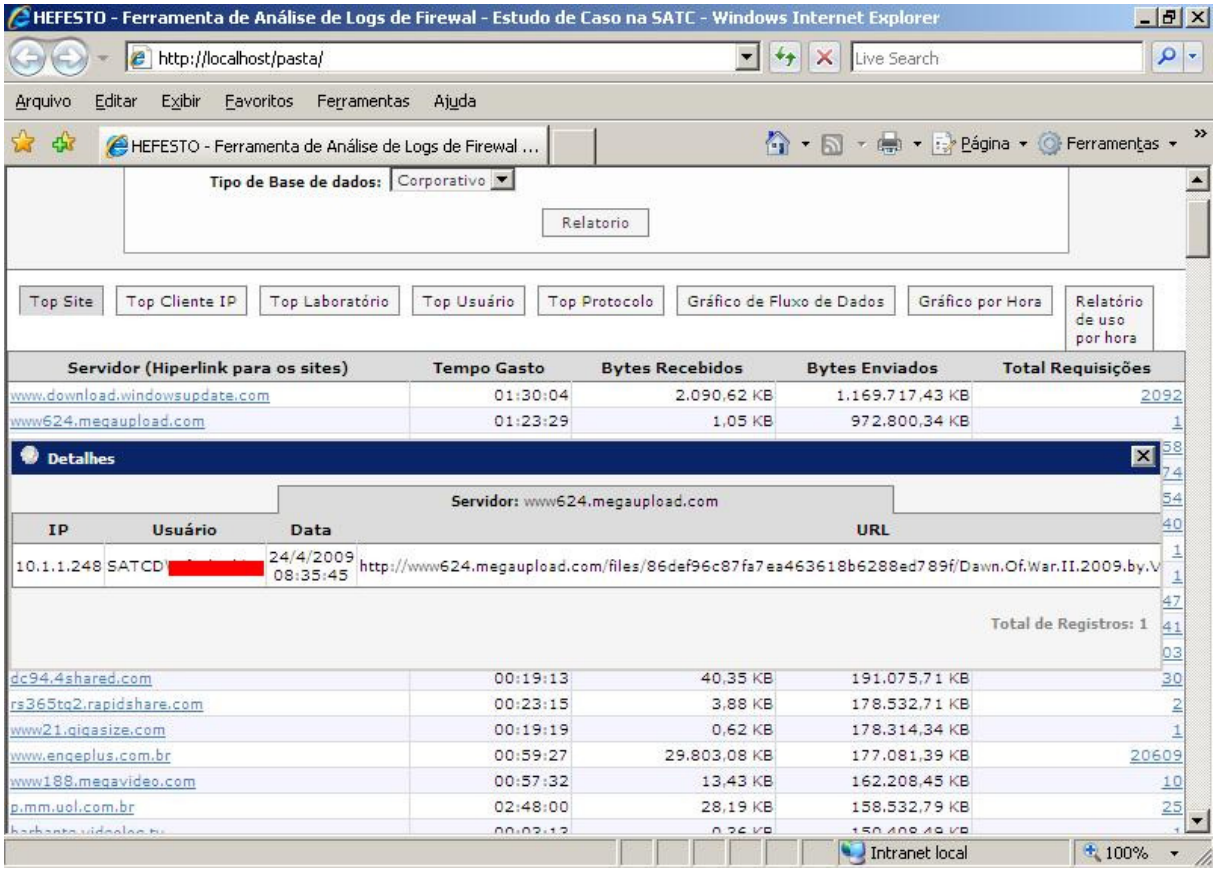

Figura 24. Relatório Top Site.

- Top Cliente IP (Figura 25)

Mostra os clientes IP internos que apresentaram um maior volume de troca de informações com o ISA Server, sendo possível por meio deste verificar o tempo gasto, o número de bytes recebidos e enviados, os *sites* acessados por meio deste IP, bem como todas as requisições efetuadas por este IP. É possível ainda verificar quais hosts este IP acessou e quais URL`s foram acessadas por ele. Este relatório está disponível tanto para as bases acadêmicas como para as corporativas.

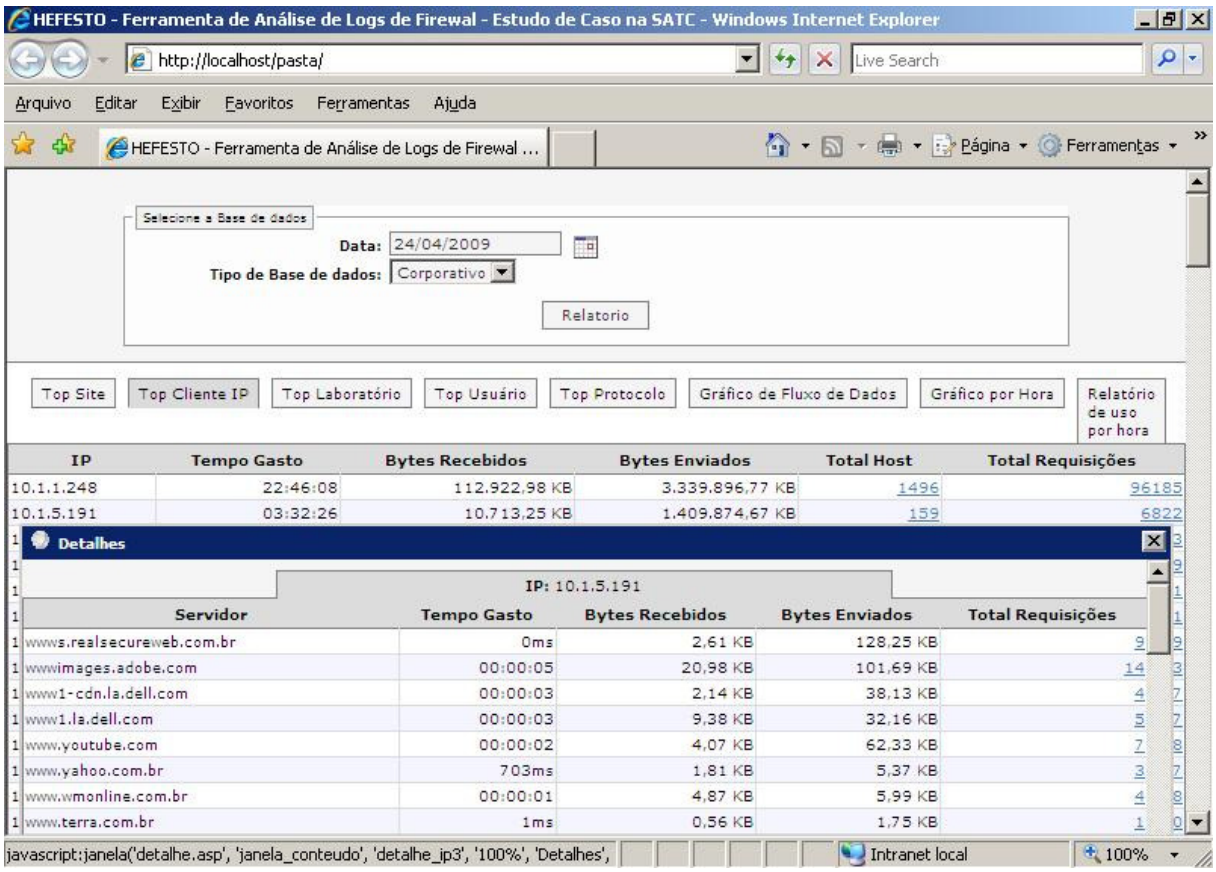

Figura 25. Relatório Top Cliente IP.

- Top Laboratório (Figura 26)

Possui informações relativas aos Laboratórios ou Rede que mais acessou o recurso de Internet. Por meio deste verifica-se a rede, a descrição do mesmo de acordo com as especificações da SATC, tempo gasto, bytes recebidos, bytes enviados, total de hosts acessados e ainda o total de requisições efetuadas por aquele laboratório ou rede. É possível também verificar quais hosts foram acessados neste laboratório, bem como as URL`s acessadas no mesmo. Este relatório está disponível apenas quando bases de dados acadêmicas forem selecionadas.

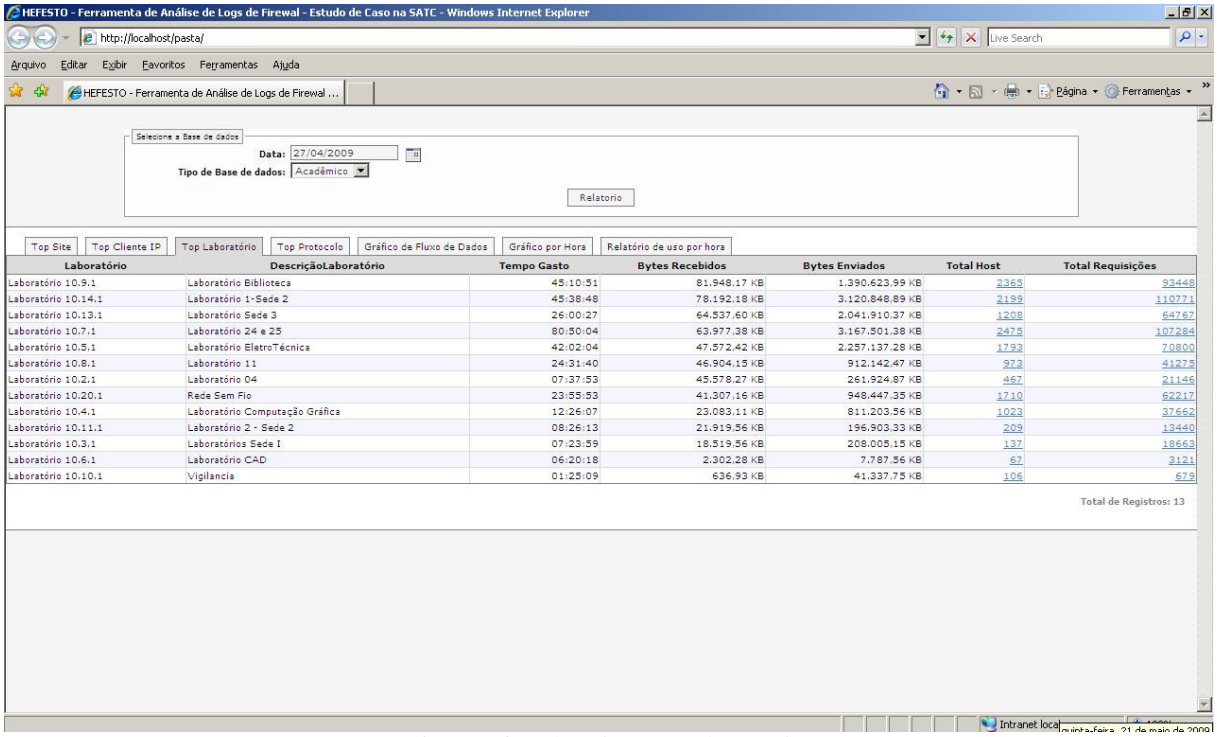

Figura 26. Relatório Top Laboratório.

- Top Usuário (Figura 27)

Possui informações relativas aos usuários que usufruíram do serviço de Internet. Este relatório só pode ser visualizado caso a base de dados escolhida seja corporativa, devido ao fato de a rede corporativa possuir autenticação, conforme mencionado anteriormente. Este relatório foi apontado pela administração de rede como sendo um dos que tem maior valia, devido ao fato de poder atuar diretamente no usuário do serviço, visando a possível otimização dos recursos. Pelo relatório é possível verificar o usuário, tempo gasto, bytes recebidos, bytes enviados, total host e total de requisições, conforme relatórios anteriores. Sendo possível ainda ser verificado por qual IP o usuário acessou, data e hora de acesso, volume de tráfego das informações, e URL`s acessadas.

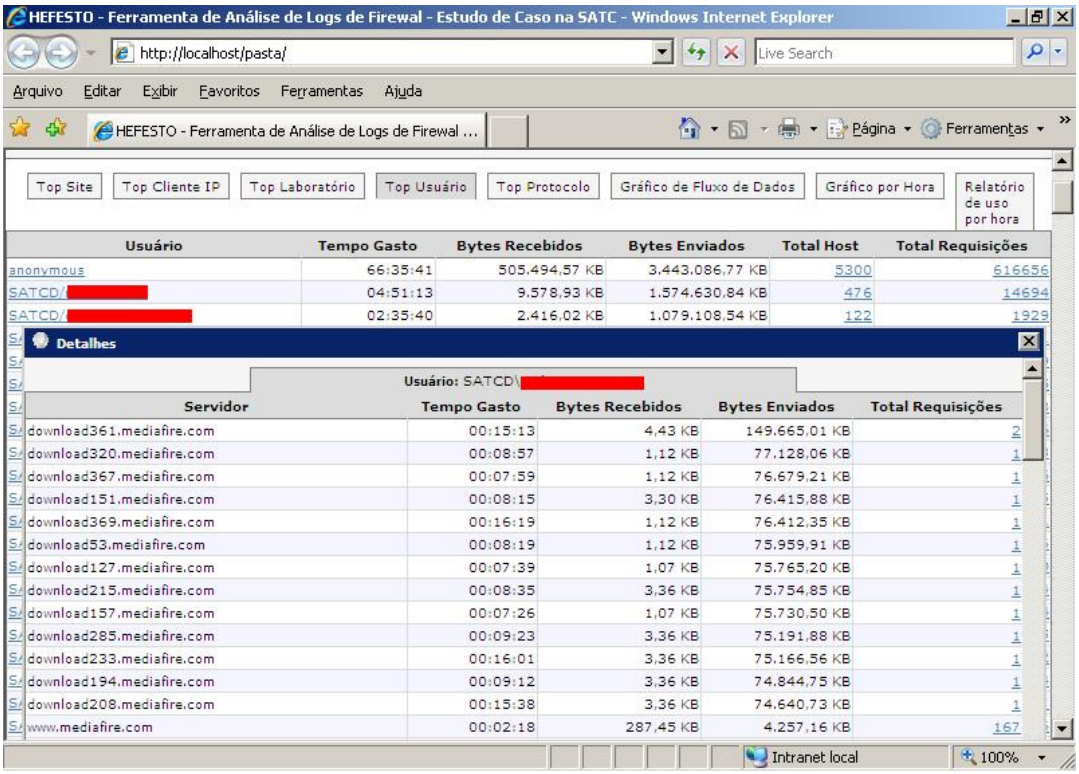

Figura 27. Relatório Top Usuário.

- Top Protocolo (Figura 28)

Este relatório foi especificado como sendo para efeito de curiosidade para administração de rede da SATC. Conforme especificado por eles, será apenas para verificação do tipo de protocolo que está sendo utilizado no tráfego da instituição. Este relatório está disponível para os dois tipos de bases de dados.

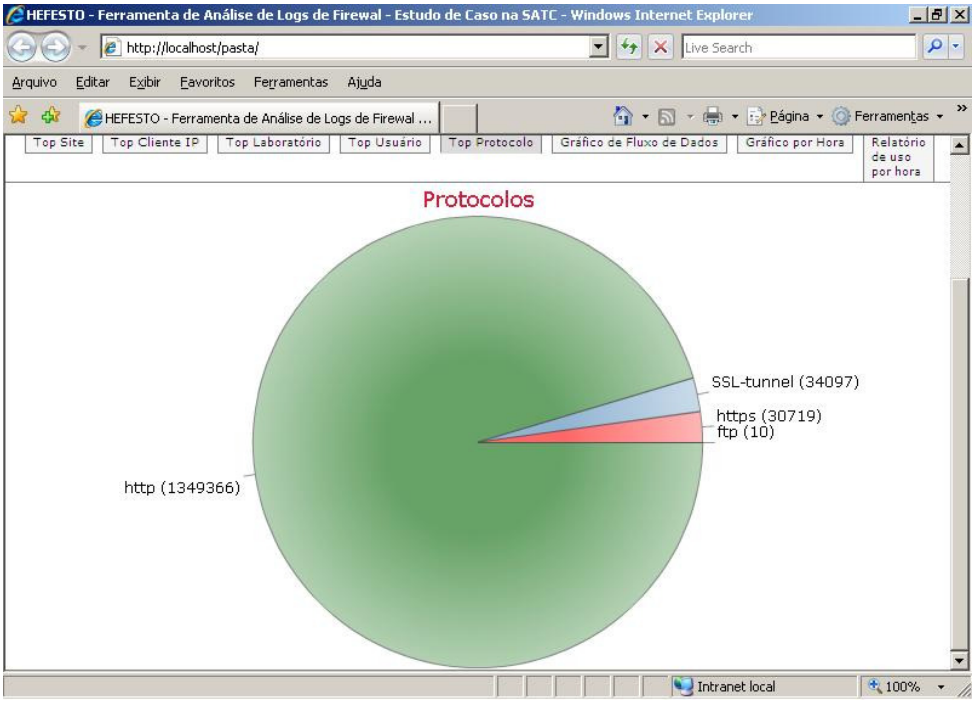

Figura 28. Relatório Top Protocolo.

Como se pode verificar na Figura 28, o ISA Server trata o protocolo HTTPS e SSL-Tunnel de maneira distinta. Isso ocorre porque quando o protocolo HTTPS ou SSL-Tunnel é utilizado, existe um túnel de comunicação entre o cliente interno e o cliente externo. Desta forma, o ISA Server detecta como sendo HTTPS quando é possível abrir este canal e verificar o que está sendo trafegado. Porém quando essa abertura não é permitida pelo servidor de destino, então o ISA Server detecta como sendo SSL-Tunnel.

- Gráfico de Fluxo de Dados e Gráfico por Hora (Figura 29 e Figura 30)

Os dois gráficos foram gerados para exemplificar como está o uso dos recursos por hora. Por meio destes é possível averiguarem quais horários existe um maior fluxo de dados trafegando na rede.

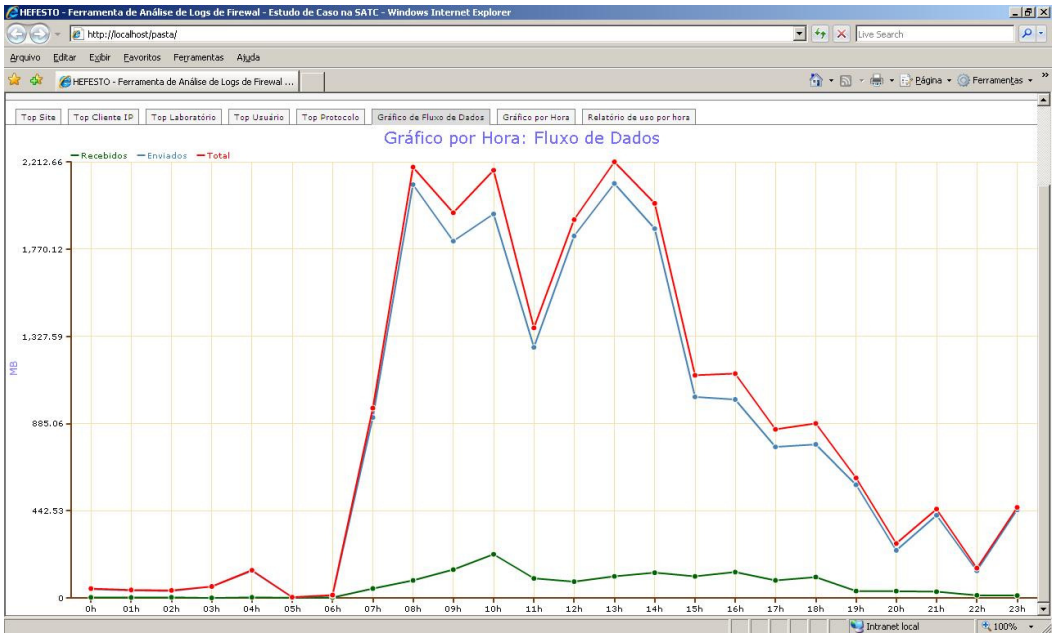

Figura 29. Gráfico de Fluxo de Dados.

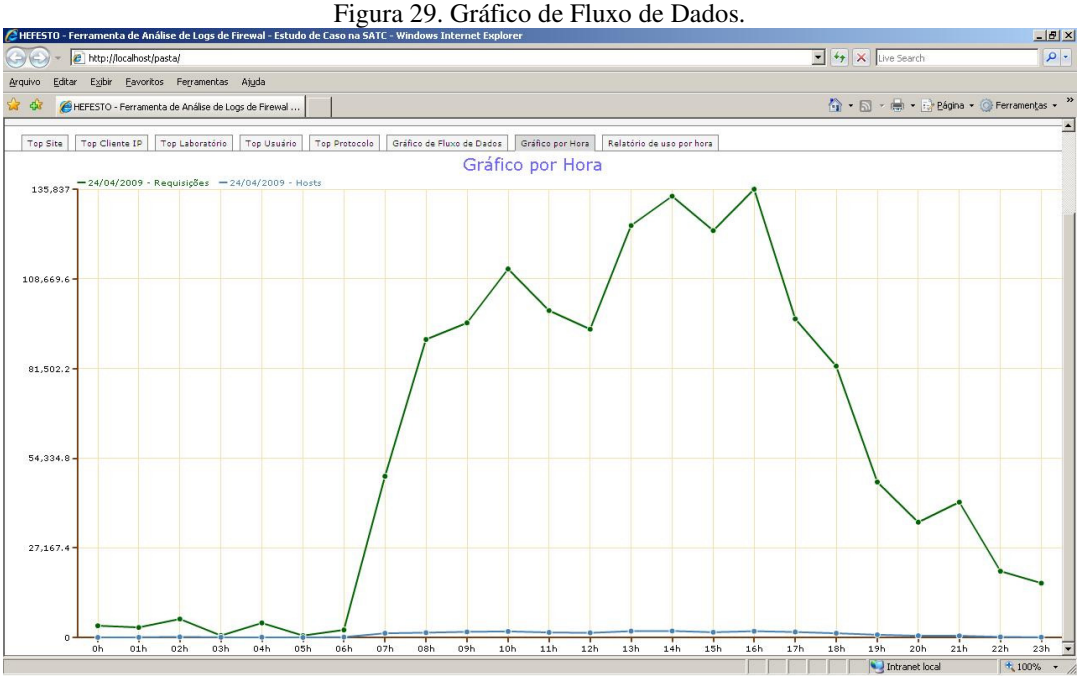

Figura 30. Gráfico por hora.

- Relatório por hora de uso (Figura 31)

Por meio deste relatório é possível verificar o que estava sendo acessado em determinado horário e por quem. Desta maneira é possível se verificar de acordo com o que foi proposto no monitoramento efetuado, e assim tomar as devidas providências, criando regras de acesso no *Firewall/Proxy*.

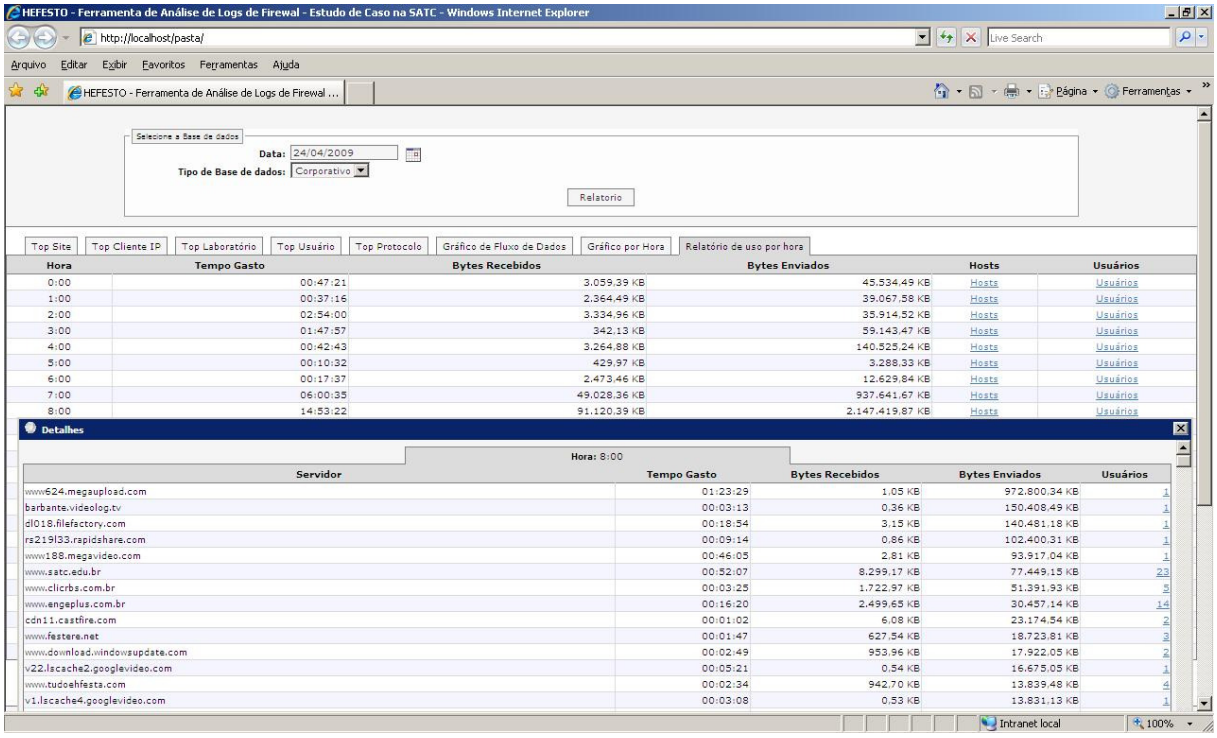

Figura 31. Relatório de Uso por Hora.

Finalizada a implementação dos relatórios de uso do serviço de Internet bem como disponibilizadas as informações aos administradores de rede, foram verificadas junto a administração de redes algumas regras que poderiam ser criadas para que se objetivasse um ganho de desempenho do recurso disponível.

6.4. RESULTADOS OBTIDOS

Os resultados foram obtidos por meio da observação e análise dos relatórios apresentados para a administração de redes da SATC. Para que se chegasse aos relatórios conforme fora solicitado pela administração de rede utilizou-se de um notebook com sistema operacional Windows Server 2003 R2 Enterprise Edition Service Pack 2, processador Intel Core 2 Duo 1.60 GHz e 3GB de Memória RAM.

Inicialmente foram verificadas as regras já existentes na instituição, com o objetivo de reaproveitá-las, ou reestruturá-las de acordo com a necessidade. Estas regras não poderão ser divulgadas devido a tratarem dados sigilosos da SATC.

Como exemplo foi retirado dos testes efetuados o seguinte relatório, onde foi verificado um maior volume de acessos ao site www294.megaupload.com, durante 01:10 de tempo das 08:00 às 09:00 horas do dia às 23/04/2009 pelo usuário especificado. Propõe-se a instituição a criação de uma regra que restrinja o acesso ao mesmo nos horários especificados. O relatório pode ser verificado pela Figura 32.

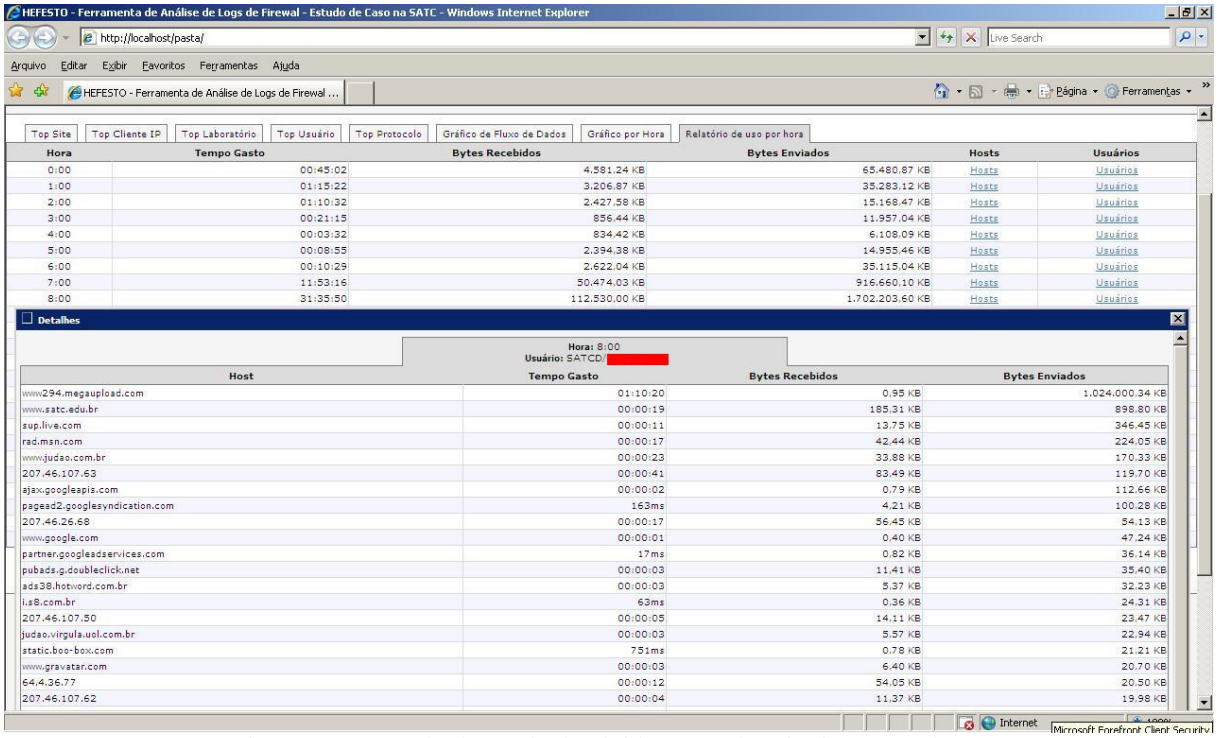

Figura 32. Exemplo de resultado obtido com relatório de uso por hora.

Diante deste exemplo citado constata-se que os relatórios apresentados servem de grande valia para que se consiga efetuar uma administração de rede na SATC com maior eficiência conforme declarado pela própria administração de rede da Instituição no Anexo C.

CONCLUSÃO

A tarefa de administração de redes corporativas pode ser simplificada com o uso de ferramentas auxiliares que forneçam suporte ao volume de informações a serem gerenciadas. Considerando os ambientes corporativos com diversos usuários e acessos diferenciados à Internet essas ferramentas fazem com que os administradores de rede tenham vantagens no diagnóstico de problemas.

Entre os tipos de ferramentas existentes, este trabalho fundamentou-se no entendimento do monitoramento de registros e desempenho, por meio de métricas como capacidade de vazão de um link de Internet.

Usando-se de métodos estatísticos como estatística estratificada, estatística sistemática e pelo teste *t de student* foi possível a verificação da hipótese de queda de desempenho em determinados horários na instituição.

Portando o desenvolvimento do protótipo de ferramenta de monitoramento dos dados gerados pelo ISA Server serve como uma forma de verificação do que está trafegando nos horários em que ocorre queda no desempenho do serviço. E desta forma os administradores podem tomar precauções objetivando o ganho de desempenho no uso do serviço de Internet.

Mesmo assim durante o tempo de pesquisa foram encontradas dificuldades na elaboração de formas de comprovação do problema de tráfego. Também na forma de utilização dos dados gerados pelos servidores de *Firewall/Proxy* da SATC, devido ao fato de estar lidando com um ambiente de produção. Tendo que de certa forma prejudicar o

funcionamento do serviço devido a fazer a cópia das bases de dados de testes para um local onde não influenciasse a disponibilidade do serviço.

Foram encontradas dificuldades também no sentido do monitoramento da interface tendo semanas interrompidas devido a feriados, ou volume de acessos diferenciados devido ao calendário da própria instituição.

Porém após superadas as dificuldades, os objetivos da pesquisa foram alcançados, devido ao emprego dos métodos estatísticos para confirmação do problema aliado aos relatórios apresentados pela ferramenta HEFESTO, torna-se possível a tomada de decisão dos administradores de rede, objetivando-se o ganho no desempenho do serviço nos horários que há queda.

É possível destacar também que a ferramenta foi aplicada no ambiente de rede da SATC, podendo ser utilizada com qualquer outro *Firewall/Proxy* que possua a funcionalidade de gerar os *logs* em bases de dados SQL.

Considerando os fundamentos aqui aplicados bem como os resultados apresentados, deixam-se aqui algumas sugestões para trabalhos futuros com intuito de aumentar o poder de auxílio do HEFESTO:

a) Efetuar o monitoramento por um período maior de tempo para que se consiga uma representatividade maior, diminuindo-se o erro amostral, objetivando-se assim um monitoramento mais representativo;
b) Colocar o HEFESTO para executar em conjunto com a aplicação portal do colaborador da instituição com a intenção de ter acesso a ela em qualquer lugar onde esteja disponível acesso a Internet;
c) Verificar a possibilidade de colocar o HEFESTO em ambiente de produção. Isto será possível por meio da configuração do ISA Server onde se pode gerar o arquivo de *log* em uma máquina da rede com o SQL Server instalado, sendo possível assim o acesso a informações em tempo real;
d) Verificar a possibilidade de salvar os relatórios gerados. Pois como o volume de dados é grande, otimizaria o espaço em disco utilizado. Por meio do salvamento dos relatórios não seria necessário o armazenamento da base de dados. Permanecendo no disco somente os últimos sete dias, com o objetivo de efetuar o desenvolvimento de novos relatórios;
e) Verificar junto à administração de rede a criação de novos relatórios de acordo com a necessidade da instituição;
f) Implementar métodos de busca dentro da aplicação, sendo possível a busca por um Cliente IP específico, ou um Usuário por exemplo;

REFERÊNCIAS

ABREU, Fabiano Rocha; PIRES, Herbert Domingues. **Gerência de Redes.** Disponível em: <http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf>. Acesso em: 23 out. 2008.

BARBETTA, Pedro Alberto. **Estatística Aplicada às ciências sociais.** 5. ed. Ver Florianópolis: Ed. UFSC, 2004. 340 p.

BARBETTA, Pedro Alberto. **Estatística aplicada às ciências sociais.** 7. ed. rev Florianópolis: Ed. UFSC, 2007. 315 p.

BARBETTA, Pedro Alberto; REIS, Marcelo Menezes; BORNIA, Antonio Cezar. **Estatística: para cursos de engenharia e informática.** 2. ed São Paulo: Atlas, 2008. 410 p.

BISQUERRA ALZINA, Rafael; CASTELLÃ SARRIERA, Jorge; MARTÍNEZ, Francesc. **Introdução à estatística:** enfoque informático com o pacote estatístico SPSS. Porto Alegre: Artmed, 2004. 255 p.

BLACK BOX. **Pocket Glossary of Conputer Terms.** 2. ed. Estados Unidos: Black Box, 1997.

CALLEGARI-JACQUES, Sidia M. **Bioestatística : princípios e aplicações.** Porto Alegre: Artmed, 2004. 255 p.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações.** 2.ed. São Paulo: SENAC/SP, 1999.

CARVALHO, Tereza Cristina Melo de Brito (Org.). **Arquiteturas de redes de computadores OSI e TCP/IP.** 2. ed. São Paulo: Makron Books, 1997. 695 p.

COMER, Douglas; STEVENS, David L. **Interligação em rede com TCP/IP**. Rio de janeiro: Ed. Campus, 1999. 2.v

COSTA NETO, Pedro Luiz de Oliveira. **Estatística.** São Paulo: Edgard Blücher, 1981. 264 p.

CRESPO, Antônio Arnot. **Estatística fácil.** 18. ed. São Paulo: Saraiva, 2002.

DIMARZIO, J. F. **Projeto e arquitetura de redes.** Rio de Janeiro: Campus, 2001. 370 p.

FARREL, Adrian. **A Internet e seus protocolos: uma análise comparativa.** Rio de Janeiro: Elsevier, 2005. 572 p.

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI: o dicionário da língua portuguesa.** 3.ed. Rio de Janeiro: Nova Fronteira, 1999. 2128 p.

FONTES, Edison. **Segurança da informação: o usuário faz a diferença.** São Paulo: Saraiva, 2006.

GARCIA, Luís Fernando Fortes. **RPC - Remote Procedure Call.** Disponível em: <http://penta.ufrgs.br/rc952/trab1/rpc.html>. Acesso em: 01 nov. 2008.

JESUS, Fabricio Cardoso de. **ANÁLISE DA REDE SOB O PONTO DE VISTA DO CONTROLE DE INFORMAÇÕES E TRÁFEGO ESTUDO DE CASO: TSA QUÍMICA DO BRASIL.** 2008. 85 f. Trabalho de Conclusão de Curso (Graduação) - Universidade do Extremo Sul Catarinense - Unesc, Criciúma, 2008.

KIMBALL, Ralph; MERZ, Richard. **Data WebHouse:** Construindo o data warehouse para a web. Rio de Janeiro: Campus, 2000.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down.** 3. ed São Paulo: Pearson Addison Wesley, 2006. 634 p.

LEVINE, David; BERENSON, Mark L.; STEPHAN, David. **Estatística: teoria e aplicações usando Microsoft Excel.** Rio de Janeiro: LTC, 2000.

MARTINS, Paulo João. **Comparação dos paradigmas cliente/servidor e agentes móveis:** um estudo em gerência de redes. 2002. 90 f. Dissertação (Mestrado) - Universidade Federal de Santa Catarina, Florianópolis, 2002.

MILONE, Giuseppe. **Estatística:** geral e aplicada. São Paulo: Thomson, 2004. 483 p.

MORAES, Luís Felipe M. de; VILELA, Guilherme S.. **Uma metodologia de classificação para os fluxos de comunicação.** Disponível em: <http://www.lbd.dcc.ufmg.br:8080/colecoes/sbrc/2006/st12_3.pdf>. Acesso em: 12 out. 2008.

MURHAMMER, Martin W.; GAERTNER, Jussara Licinia Souza. **TCP/IP: tutorial e técnico.** São Paulo: Makron Books, 2000. 690 p. TANENBAUM, Andrew S. Redes de computadores. Rio de Janeiro: Campus, 2003. 945 p.

NASCIMENTO, Marcelo Brenzink do; TAVARES, Alexei Corrêa. **Roteadores e Switches - Guia de Configuração para Certificações CCNA.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

OLIVEIRA, Mauro et al. **Introdução à Gerência de Redes ATM.** XVI Simpósio Brasileiro de Redes de Computadores Rio de Janeiro, maio de 1998. Disponível em: <http://www.cefetce.br/Ensino/Professores/Publicacoes/livrogerencia.pdf>. Acesso em: 23 out. 2008.

PELLIN, Alex Fabio . **Um monitor de transações de serviços Internet.** 2002. 111 f. Dissertação (Mestrado) - Universidade Federal do Rio Grande do Sul - Ufrgs, Porto Alegre, 2004.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores das LANs, MANs e WANs às Redes ATM.** 2. ed. Rio de Janeiro: Ed. Campus, 1995. 704 p.

SOUSA, Lindeberg Barros de. **Redes de computadores: dados, voz e imagem.** 4.ed. Rio de Janeiro: Érica, 2001.

STALLINGS, William. **Redes e sistemas de comunicação de dados.** Rio de Janeiro: Elsevier, 2005. 449 p.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3 and RMON 1 AND 2.** 3. ed. Reading: Addison-Wesley, 1999. 619 p.

TANENBAUM, Andrew S. **Redes de computadores.** 5.ed. Rio de Janeiro: Campus, 1997. 923 p.

TANENBAUM, Andrew S. **Redes de computadores.** Rio de Janeiro: Campus, 2003. 945 p.

TEIXEIRA JUNIOR, José Helvécio. **Redes de computadores: serviços, administração e segurança.** São Paulo: Makron Books, 1999.

THE INTERNET ENGINEERING TASK FORCE. **RFC 1561:** Use of ISO CLNP in TUBA Environments. 1993.

TORRES, Gabriel. **Redes de computadores: curso completo.** Rio de Janeiro: Axcel Books do Brasil, 2001. 664 p.

TRIOLA, Mario F. **Introdução à estatística.** Mario F. Triola, tradução de Alfredo Alves de Farias; revisão de Eliana Farias e Soares; colaboração de Vera Regina L. F. Flores M. 7. ed Rio de Janeiro: LTC, 1999.

TROMBIM, Diordgenes. **DIAGNÓSTICO DO TRÁFEGO DE REDE DE LABORATÓRIOS DE INFORMATÍCA. ESTUDO DE CASO: UNIVERSIDADE DO EXTREMO SUL CATARINENSE.** 2006. 116 f. Trabalho de Conclusão de Curso (Graduação) - Universidade do Extremo Sul Catarinense, Criciúma, 2006.

ZACKER, Craig; DOYLE, Paul. **Redes de computadores : configuração, manutenção e expansão.** São Paulo: Makron Books, 2000. 1056 p.

ZAKI, M.; DARWISH, M. G.; OSMAN, G.. GBF: a grammar based filter for Internet applications. **Journal Of Network And Computer Applications,** Amsterdã, p. 229-257. 23 mar. 2003.

REFERÊNCIAS COMPLEMENTARES

BEIGHLEY, Lynn. . **Use a cabeça SQL= Head first SQL**. Rio de Janeiro: Alta Books, 2008. 454p.

OLIVEIRA, Celso Henrique Poderoso de. **SQL :curso prático**. São Paulo: Novatec, 2002. 272 p.

PLEW, Ronald R.; STEPHENS, Ryan K. **Aprenda em 24 horas SQL**. Rio de Janeiro: Ed. Campus, 2000. 394 p.

APÊNDICE A - TABELA COM OS DADOS UTILIZADOS COMO COLETA BASE EFETUADA EM 08/04/2009.

	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum	
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second
8/4/2009 23:00 - 00:00	318464,38	724,71	147710,89	336,14	466175,26	1060,85
8/4/2009 22:00 - 23:00	169096,74	384,80	145242,23	330,52	314338,97	715,32
8/4/2009 21:00 - 22:00	1254702,47	2855,24	256680,39	584,11	1511382,85	3439,35
8/4/2009 20:00 - 21:00	1144346,63	2604,10	306847,67	698,27	1451194,30	3302,37
8/4/2009 19:00 - 20:00	1008632,47	2295,26	247687,18	563,64	1256319,65	2858,91
8/4/2009 18:00 - 19:00	1311542,20	2984,58	253135,85	576,04	1564678,05	3560,62
8/4/2009 17:00 - 18:00	1159558,34	2638,72	347171,32	790,03	1506729,66	3428,75
8/4/2009 16:00 - 17:00	2556844,66	5818,39	545554,02	1241,47	3102398,68	7059,86
8/4/2009 15:00 - 16:00	2726740,81	6205,01	502902,67	1144,41	3229643,48	7349,42
8/4/2009 14:00 - 15:00	2894602,93	6587,01	486923,88	1108,05	3381526,81	7695,07
8/4/2009 13:00 - 14:00	2843703,06	6471,17	444690,86	1011,94	3288393,92	7483,11
8/4/2009 12:00 - 13:00	1161333,51	2642,77	292351,33	665,29	1453684,84	3308,06
8/4/2009 11:00 - 12:00	2154890,27	4903,68	375993,24	855,61	2530883,51	5759,29
8/4/2009 10:00 - 11:00	1735792,49	3950,01	374566,33	852,37	2110358,82	4802,39
8/4/2009 09:00 - 10:00	3192830,83	7265,63	404245,41	919,90	3597076,24	8185,53
8/4/2009 08:00 - 09:00	2035345,18	4631,68	318949,37	725,81	2354294,55	5357,49
8/4/2009 07:00 - 08:00	1108236,62	2521,92	288764,22	657,12	1397000,84	3179,04
8/4/2009 06:00 - 07:00	57622,29	131,13	64534,99	146,86	122157,28	277,98
8/4/2009 05:00 - 06:00	8965,93	20,40	57738,81	131,39	66704,74	151,80
8/4/2009 04:00 - 05:00	8745,31	19,90	86412,46	196,64	95157,77	216,54
8/4/2009 03:00 - 04:00	25226,48	57,41	39244,13	89,31	64470,61	146,71
8/4/2009 02:00 - 03:00	456,08	1,04	1226,98	2,79	1683,06	3,83
8/4/2009 01:00 - 02:00	6881,32	15,66	5510,21	12,54	12391,53	28,20
8/4/2009 00:00 - 01:00	218215,62	496,58	68376,49	155,60	286592,11	652,17
Total Volume	29102776,62		6062460,91		35165237,54	

APÊNDICE B - CÁLCULOS DE ESTATÍSTICA ESTRATIFICADA EFETUADOS APÓS COLETA BASE

	Cálculos Estatísticos					
	E (Estrato)	P (População)	p (% representativa do valor do estrato diante da População)	t (tamanho da amostra para cada hora)	f (tempo de monitoramento para cada amostra (h))	Tempo Monitoramento (min)
8/4/2009 23:00 -	466175,26	35165237,54	0,0132567073	466175,262	0,0132567073	0,80
8/4/2009 22:00 -	314338,97	35165237,54	0,0089389122	314338,972	0,0089389122	0,54
8/4/2009 21:00 -	1511382,85	35165237,54	0,0429794581	1511382,854	0,0429794581	2,58
8/4/2009 20:00 -	1451194,30	35165237,54	0,0412678657	1451194,299	0,0412678657	2,48
8/4/2009 19:00 -	1256319,65	35165237,54	0,0357261812	1256319,648	0,0357261812	2,14
8/4/2009 18:00 -	1564678,05	35165237,54	0,0444950229	1564678,049	0,0444950229	2,67
8/4/2009 17:00 -	1506729,66	35165237,54	0,0428471344	1506729,658	0,0428471344	2,57
8/4/2009 16:00 -	3102398,68	35165237,54	0,0882234529	3102398,677	0,0882234529	5,29
8/4/2009 15:00 -	3229643,48	35165237,54	0,0918419356	3229643,48	0,0918419356	5,51
8/4/2009 14:00 -	3381526,81	35165237,54	0,0961610684	3381526,811	0,0961610684	5,77
8/4/2009 13:00 -	3288393,92	35165237,54	0,0935126322	3288393,924	0,0935126322	5,61
8/4/2009 12:00 -	1453684,84	35165237,54	0,0413386897	1453684,844	0,0413386897	2,48
8/4/2009 11:00 -	2530883,51	35165237,54	0,0719711764	2530883,513	0,0719711764	4,32
8/4/2009 10:00 -	2110358,82	35165237,54	0,0600126422	2110358,817	0,0600126422	3,60
8/4/2009 09:00 -	3597076,24	35165237,54	0,1022906850	3597076,236	0,1022906850	6,14
8/4/2009 08:00 -	2354294,55	35165237,54	0,0669494853	2354294,553	0,0669494853	4,02
8/4/2009 07:00 -	1397000,84	35165237,54	0,0397267567	1397000,837	0,0397267567	2,38

APÊNDICE C - TEMPO DE MONITORAMENTO PARA SEGUNDA-FEIRA DIA 27/04/2009

Intervalo	Duração	Min Monitorados	SOMA		
12:00 - 13:00	0:02:38	27/04/2009 12:46 - 12:47	20.957		
		27/04/2009 12:45 - 12:46	23.632		
		27/04/2009 12:44 - 12:45	33.029	Total	77.619
13:00 - 14:00	0:06:01	27/04/2009 13:55 - 13:56	50.660		
		27/04/2009 13:54 - 13:55	45.265		
		27/04/2009 13:53 - 13:54	39.467		
		27/04/2009 13:52 - 13:53	46.952		
		27/04/2009 13:51 - 13:52	63.237		
		27/04/2009 13:50 - 13:51	64.264	Total	309.844
17:00 - 18:00	0:04:32	27/04/2009 17:44 - 17:45	33.531		
		27/04/2009 17:43 - 17:44	40.434		
		27/04/2009 17:42 - 17:43	32.338		
		27/04/2009 17:41 - 17:42	24.682		
		27/04/2009 17:40 - 17:41	27.045	Total	158.030

APÊNDICE D - TEMPO DE MONITORAMENTO PARA TERÇA-FEIRA DIA 28/04/2009

Intervalo	Duração	Min Monitorados	SOMA		
10:00 - 11:00	0:04:00	28/04/2009 10:30 - 10:31	63.130		
		28/04/2009 10:29 - 10:30	42.654		
		28/04/2009 10:28 - 10:29	65.335		
		28/04/2009 10:27 - 10:28	78.834	Total	249.952
20:00 - 21:00	0:02:48	28/04/2009 20:10 - 20:11	35.859		
		28/04/2009 20:09 - 20:10	38.896		
		28/04/2009 20:08 - 20:09	36.635	Total	111.390
21:00 - 22:00	0:02:58	28/04/2009 21:19 - 21:20	50.976		
		28/04/2009 21:18 - 21:19	53.351		
		28/04/2009 21:17 - 21:18	64.274	Total	168.601

APÊNDICE E - TEMPO DE MONITORAMENTO PARA QUARTA-FEIRA DIA 29/04/2009

Intervalo	Duração	Min Monitorados	SOMA		
08:00 - 09:00	0:04:02	29/04/2009 08:41 - 08:42	89.243		
		29/04/2009 08:40 - 08:41	90.016		
		29/04/2009 08:39 - 08:40	90.440		
		29/04/2009 08:38 - 08:39	87.970	Total	357.669
15:00 - 16:00	0:05:51	29/04/2009 15:51 - 15:52	104.807		
		29/04/2009 15:50 - 15:51	107.934		
		29/04/2009 15:49 - 15:50	113.966		
		29/04/2009 15:48 - 15:49	117.861		
		29/04/2009 15:47 - 15:48	109.043		
		29/04/2009 15:46 - 15:47	104.184	Total	657.795
16:00 - 17:00	0:05:29	29/04/2009 16:06 - 16:07	95.715		
		29/04/2009 16:05 - 16:06	94.117		
		29/04/2009 16:04 - 16:05	100.484		
		29/04/2009 16:03 - 16:04	109.175		
		29/04/2009 16:02 - 16:03	99.473		
		29/04/2009 16:01 - 16:02	92.027	Total	590.991

APÊNDICE F - TEMPO DE MONITORAMENTO PARA QUINTA-FEIRA DIA 30/04/2009

Intervalo	Duração	Min Monitorados	SOMA		
09:00 - 10:00	0:06:14	01/05/2009 09:34 - 09:35	1.612		
		01/05/2009 09:33 - 09:34	11.323		
		01/05/2009 09:32 - 09:33	2.219		
		01/05/2009 09:31 - 09:32	2.064		
		01/05/2009 09:30 - 09:31	1.140		
		01/05/2009 09:29 - 09:30	1.475		
		01/05/2009 09:28 - 09:29	1.011	Total	20.844
14:00 - 15:00	0:06:17	30/04/2009 14:34 - 14:35	72.075		
		30/04/2009 14:33 - 14:34	70.197		
		30/04/2009 14:32 - 14:33	85.410		
		30/04/2009 14:31 - 14:32	81.222		
		30/04/2009 14:30 - 14:31	78.266		
		30/04/2009 14:29 - 14:30	88.468		
		30/04/2009 14:28 - 14:29	66.255	Total	541.893
18:00 - 19:00	0:03:07	30/04/2009 18:08 - 18:09	6.192		
		30/04/2009 18:07 - 18:08	12.755		
		30/04/2009 18:06 - 18:07	41.950		
		30/04/2009 18:05 - 18:06	25.301	Total	86.199

APÊNDICE G - TEMPO DE MONITORAMENTO PARA SEXTA-FEIRA DIA 08/05/2009

Intervalo	Duração	Min Monitorados	SOMA		
07:00 - 08:00	0:02:48	08/05/09 07:42 - 07:43	65.125		
		08/05/09 07:41 - 07:42	74.513		
		08/05/09 07:40 - 07:41	94.159	Total	233.797
11:00 - 12:00	0:02:57	08/05/09 11:19 - 11:20	100.769		
		08/05/09 11:18 - 11:19	99.800		
		08/05/09 11:17 - 11:18	99.930	Total	300.499
19:00 - 20:00	0:02:14	08/05/09 19:15 - 19:16	75.939		
		08/05/09 19:14 - 19:15	71.710		
		08/05/09 19:13 - 19:14	61.811	Total	209.460

APÊNDICE H - VALORES DE *d* PARA CÁLCULO DE VARIÂNCIA DA VARIÁVEL BANDWIDTH TRAFFIC IN

x	*d*	di^2
318464,38	-894151,32	799506575308,43
169096,74	-1043518,95	1088931800400,46
1254702,47	42086,78	1771296657,96
1144346,63	-68269,06	4660664780,85
1008632,47	-203983,22	41609153905,58
1311542,20	98926,51	9786454644,58
1159558,34	-53057,35	2815082353,65
2556844,66	1344228,97	1806951516618,04
2726740,81	1514125,12	2292574864883,18
2894602,93	1681987,23	2829081056460,30
2843703,06	1631087,37	2660445999874,38
1161333,51	-51282,18	2629861951,36
2154890,27	942274,58	887881382857,81
1735792,49	523176,79	273713957082,55
3192830,83	1980215,14	3921251982203,21
2035345,18	822729,49	676883812618,69
1108236,62	-104379,07	10894991228,27
57622,29	-1154993,41	1334009767133,49
8965,93	-1203649,76	1448772751167,52
8745,31	-1203870,38	1449303898261,99
25226,48	-1187389,21	1409893135232,83
456,08	-1212159,61	1469330931428,84
6881,32	-1205734,37	1453795375018,41
218215,62	-994400,07	988831498553,07

APÊNDICE I – VALORES DE *d* PARA CÁLCULO DE VARIÂNCIA DA VARIÁVEL BANDWIDTH TRAFFIC OUT

x	*d*	di^2
147710,89	-104891,65	11002258877,81
145242,23	-107360,31	11526235957,52
256680,39	4077,85	16628852,13
306847,67	54245,13	2942534124,20
247687,18	-4915,36	24160784,00
253135,85	533,31	284416,31
347171,32	94568,78	8943253575,40
545554,02	292951,48	85820569023,87
502902,67	250300,13	62650157560,16
486923,88	234321,35	54906493171,73
444690,86	192088,33	36897924969,47
292351,33	39748,79	1579966541,64
375993,24	123390,70	15225265329,77
374566,33	121963,79	14875166792,78
404245,41	151642,87	22995560009,20
318949,37	66346,83	4401902243,60
288764,22	36161,68	1307667169,73
64534,99	-188067,55	35369401498,00
57738,81	-194863,73	37971872506,30
86412,46	-166190,08	27619142039,50
39244,13	-213358,41	45521809855,36
1226,98	-251375,56	63189669672,51
5510,21	-247092,33	61054620553,79
68376,49	-184226,05	33939237882,41

ANEXO A - PLANO AMOSTRAL DAS INTENÇÕES DE VOTO PARA PREFEITO DA CIDADE DE CRICIÚMA – 23/09/2008

Dados com base do TRE com atualização em 01/08/2008

Total de Eleitores: 132.007

Amostra: 737 questionários

Erro Amostral (%): 3,60

Sexo	População	%	Quest.
Masculino	**63.317**	**47,96**	**354**
Feminino	**68.690**	**52,04**	**383**
Total	132.007	100,00	737

Idade	População	%	Quest.
16 a 24	**26.082**	**19,76**	**146**
25 a 44	**56.981**	**43,17**	**318**
45 a 69	**42.516**	**32,21**	**237**
Acima de 69	**6.428**	**4,87**	**36**
Total	132.007	100,00	737

Grau de Instrução	População	%	Quest.
Analfabeto, lê, ensino fundamental Incompleto	**54.442**	**41,24**	**304**
Ensino Fundamental Completo, Ensino Médio Incompleto	**47.540**	**36,01**	**266**
Ensino Médio Completo, Ensino Superior Incompleto	**24.254**	**18,37**	**135**
Ensino Superior Completo	**5.771**	**4,37**	**32**

Total	132.007	100,00	737

Área Física da Realização do Trabalho

Bairros	População	%	Quest.
Ana Maria	**1.766**	**1,34**	**10**
Brasília	**3.238**	**2,45**	**18**
Capão Bonito	**214**	**0,16**	**1**
Centro	**11.965**	**9,06**	**67**
Cidade Mineira Velha	**2.507**	**1,90**	**14**
Colonial	**1.144**	**0,87**	**6**
Comerciário	**3.461**	**2,62**	**19**
Floresta 1	**1.131**	**0,86**	**6**
Jardim Montevidéu	**398**	**0,30**	**2**
Jardim União	**5.296**	**4,01**	**30**
Laranjinha	**1.100**	**0,83**	**6**
Linha Anta	**711**	**0,54**	**4**
Linha Batista	**1.109**	**0,84**	**6**
Lote Seis	**438**	**0,33**	**2**
Mãe Luzia	**686**	**0,52**	**4**
Maria Céu	**824**	**0,62**	**5**
Metropolitana	**2.266**	**1,72**	**13**
Michel	**5.246**	**3,97**	**29**
Milanesi	**1.005**	**0,76**	**6**
Mina Brasil	**1.225**	**0,93**	**7**
Mina do Mato	**2.807**	**2,13**	**16**
Mina do Toco	**654**	**0,50**	**4**
Morro Estevão	**1.902**	**1,44**	**11**

Naspolini	**797**	**0,60**	**4**
Nossa Senhora da Salete	**5.561**	**4,21**	**31**
Operária Nova	**3.240**	**2,45**	**18**
Pinheirinho	**8.670**	**6,57**	**49**
Pio Correa	**4.016**	**3,04**	**22**
Primeira Linha	**1.375**	**1,04**	**8**
Próspera	**7.204**	**5,46**	**40**
Quarta Linha	**3.096**	**2,35**	**17**
Renascer	**1.488**	**1,13**	**8**
Rio Maina	**8.042**	**6,09**	**45**
Sangão	**861**	**0,65**	**5**
Santa Augusta	**959**	**0,73**	**5**
Santa Bárbara	**4.518**	**3,42**	**25**
Santa Catarina	**1.480**	**1,12**	**8**
Santa Luzia	**6.461**	**4,89**	**36**
Santo Antônio	**2.603**	**1,97**	**15**
São Cristóvão	**1.463**	**1,11**	**8**
São Defende	**1.847**	**1,40**	**10**
São Domingos	**258**	**0,20**	**1**
São Francisco	**4.554**	**3,45**	**26**
São Luiz	**3.544**	**2,68**	**20**
São Marcos	**950**	**0,72**	**5**
São Roque	**342**	**0,26**	**2**
São Sebastião	**2.312**	**1,75**	**13**
São Simão	**1.440**	**1,09**	**8**
Verdinho	**885**	**0,67**	**5**
Vila Rica	**995**	**0,75**	**6**

Vila Zuleima	**1.953**	**1,48**	**11**
Total	132.007	100,00	737

Intervalo de Confiança.

O presente trabalho será realizado por intermédio de pesquisa aleatória usando-se a técnica de amostragem aleatória proporcional com confiança de 95% e margem de erro de 3,6%.

Estatístico Responsável

Antonio Fernando Noceti Bahia
CONRE 8441

ANEXO B - POSSIVEIS REGISTROS DO ARQUIVO DE WEBPROXY LOGGING DO MICROSOFT ISA SERVER 2006

Campo	Descrição
Client IP	Endereço IP do Cliente
Client Username	Conta de usuário que fez a solicitação. Um ponto de interrogação (?), ao lado do nome do usuário indica que o nome do usuário foi enviado, porém o mesmo não foi autenticado pelo ISA Server. Se o ISA Server não está configurado para controle de acesso por usuários, o mesmo é listado como Anonymous.
Client Agent	Nome e Versão do aplicativo cliente enviada pelo próprio cliente no cabeçalho HTTP. Quando foi utilizado o cache do ISA Server, é utilizado o próprio ISA Server neste campo.
Authenticated Client	Este valor indica se o cliente foi ou não autenticado. Podendo apresentar os valores Y ou N.
Log Date	Refere-se a data em que o evento de autenticação ocorreu. No formato MSDE tanto a data como a hora local são incluídas num único campo logTime. E os dados são colocados em ambos os campos.
Log Time	A hora local quando ocorreu o evento de autenticação.
Service	O nome do serviço que ficou registrado. Por exemplo fwsrv representa do serviço do Microsoft *Firewall*.
Server Name	Nome do computador onde está instalado o ISA Server.
Referring Server	URL do recurso que forneceu a URL para o cliente, indicado no cabeçalho da requisição.
Destination Host Name	O nome do computador de destino que forneceu o serviço para a conexão atual. Um hífen (-) neste campo pode indicar que o objeto solicitado foi concedido pelo cache local.
Destination IP	Endereço IP do computador de destino que forneceu o serviço para a conexão atual.
Destination Port	O número da porta fornecido pelo computador de destino para a conexão atual. Utilizado pelo aplicativo cliente no momento da requisição.
Processing Time	Total de tempo, em milisegundos, que foi necessário para o ISA Server processar a conexão atual. Sendo contado a partir do momento que se inicia a conexão até quando o cliente recebe todos os dados e fecha a conexão.
Bytes Received	Total de bytes recebidos pelo computador remoto, vindo do cliente.
Bytes Sent	Total de bytes enviados do computador remoto para o cliente.
Protocol	Protocolo utilizado pela conexão, no nível de aplicação.
Transport	Protocolo utilizado pela conexão, no nível de transporte.
HTTP Method	Método HTTP utilizado, podendo ser GET, PUT, POST e HEAD.

URL	URL solicitada pelo cliente.
MIME Type	Tipo de Multipurpose Internet Mail Extensions utilizado pelo objeto atual. Podendo apresentar hífen (-) quando não utilizado.
Object Source	Tipo de fonte utilizada para recuperar o objeto atual. Uma lista de objetos pode ser verificar no link http://msdn.microsoft.com/pt-br/library/aa503433(en-us).aspx#_isa_object_source_values
Result Code	Códigos para possíveis erros, sendo erros do Windows valores entre 0 e 100, erros HTTP valores entre 100 e 1.000, erros winsock com valores entre 10.004 e 11.031 e erros do ISA Server que podem ser consultados por meio deste link http://msdn.microsoft.com/pt-br/library/aa503433(en-us).aspx#_isa_result_code_values
Cache Info	Número que reflete o estado do objeto, indicando o armazenamento ou não do objeto. Retrata a soma dos valores de todas tentativas de armazenamento. Sendo possível consultar os possíveis valores em http://msdn.microsoft.com/pt-br/library/aa503433(en-us).aspx#_isa_cache_info_values
Rule	A regra utilizada para liberação ou negação do acesso perante a requisição. Podendo assumir as seguintes possibilidades: • Se a requisição for permitida, o ISA Server mostra a regra pelo qual a permissão foi concedida; • Se o pedido foi negado, é mostrado a regra que bloqueou o pedido; • Se for negado por um política geral, é mostrado a política do servidor web que restringiu o acesso. • Se o ISA Server bloquear o acesso por algum motivo não explicitado em regras, colocará um hífen (-) no local da regra.
Filter Information	Contém informações fornecidas por filtros da WEB. Por exemplo, se o HTTP Filter rejeitou um pedido, este campo contém o motivo da rejeição.
Source Network	A rede do qual o pedido foi originado.
Destination Network	A rede a qual o pedido foi enviado.
Error info (ErrorInfo)	Contém informações adicionais caso seja detectado algum erro. Objetiva-se por meio deste campo fornecer a fonte do erro. As possíveis ocorrências destes campos podem ser verificadas em http://msdn.microsoft.com/pt-br/library/aa503433(en-us).aspx#_isa_error_info_bit_fields
Action	Ação tomada pelo ISA Server
GMT Log Time	A data e hora em formato de tempo universal (UTC)
Authentication Server	O nome do servidor LDAP ou RADIUS utilizado para autenticação.

ANEXO C - DOCUMENTO ASSINADO PELA ADMINISTRAÇÃO DE REDE DA SATC

Termo de Responsabilidade

Os relatórios apresentados pelo Protótipo da Ferramenta HEFESTO estão de acordo com o que é necessário para uma melhor administração de rede da Instituição. Desta forma declaro para os devidos fins que os relatórios descritos a seguir estão de acordo com o que foi pedido pelo administrador de rede da instituição. Podendo ser utilizado como ferramenta de auxílio à administração de rede. E assim realizar a possível reavaliação das políticas de acesso ao serviço de Internet da SATC.

Base Corporativa	Base Acadêmica
Site mais acessado	Site mais acessado
Cliente IP que mais acessou	Cliente IP que mais acessou
Usuário que mais acessou	Laboratório que mais acessou
Protocolos utilizados	Protocolos utilizados
Gráfico de Fluxo de dados por hora	Gráfico de Fluxo de dados por hora
Gráfico de Requisições por hora	Gráfico de Requisições por hora
Relatório de uso por hora	Relatório de Uso por hora

_____

Valter Blauth Junior
Coordenador de Informática

ANEXO D – TABELA DOS VALORES PARA *t*

Valores da distribuição *t de Student*								
Bicaudal	**0,2**	**0,1**	**0,05**	**0,02**	**0,01**	**0,002**	**0,001**	**Nível de significância**
Unicaudal	**0,1**	**0,05**	**0,025**	**0,01**	**0,01**	**0,001**	**0,0005**	
X	3,078	6,314	12,71	31,82	63,66	318,3	637	1
X	1,886	2,92	4,303	6,965	9,925	22,33	31,6	2
X	1,638	2,353	3,182	4,541	5,841	10,21	12,92	3
X	1,533	2,132	2,776	3,747	4,604	7,173	8,61	4
X	1,476	2,015	2,571	3,143	3,707	5,893	6,869	5
X	1,440	1,943	2,447	3,143	3,707	5,208	5,408	6
X	1,415	1,895	2,365	2,998	3,499	4,785	5,408	7
X	1,397	1,860	2,306	2,896	3,355	4,501	5,041	8
X	1,383	1,833	2,262	2,821	3,25	4,297	4,781	9
X	1,372	1,812	2,228	2,764	3,169	4,144	4,587	10
X	1,325	1,725	2,086	2,528	2,845	3,552	3,85	20
X	1,31	1,697	2,042	2,457	2,75	3,385	3,646	30
	1,303	1,684	2,021	2,423	2,704	3,307	3,551	40
X	1,302	1,682	2,018	2,418	2,698	3,296	3,538	42
X	1,301	1,68	2,015	2,414	2,692	3,286	3,526	44
X	1,300	1,679	2,013	2,410	2,687	3,277	3,515	46