

UNIVERSIDADE LUTERANA DO BRASIL

ULBRA – *CAMPUS* GUAÍBA

CURSO DE SISTEMAS DE INFORMAÇÃO



**DESENVOLVIMENTO DE SISTEMA  
PARA BLOQUEIO DE SITES  
TRABALHO DE CONCLUSÃO DE CURSO I**

CARLOS HENRIQUE SOARES DE SOUZA

André Peres  
Orientador

Guaíba, Novembro de 2007.

## **DADOS DE IDENTIFICAÇÃO**

Acadêmico: Carlos Henrique Soares de Souza.

E-mail: carloshss@hotmail.com

Professor Orientador: André Peres

E-mail: peres@guaiba.ulbra.tche.br

Título do Projeto: Desenvolvimento de Sistema para Bloqueio de Sites

Período de realização: agosto de 2007 até junho de 2008

## SUMÁRIO

1	INTRODUÇÃO.....	4
2	DEFINIÇÃO DO TEMA.....	5
2.1	Tema.....	5
2.2	Delimitação do Tema .....	5
3	SOLUÇÃO PROPÓSTA.....	6
4	OBJETIVOS .....	6
4.1	Objetivos Especificos .....	7
5	JUSTIFICATIVA .....	8
6	REFERENCIAL TEÓRICO .....	8
7	PROXY .....	8
8	SQUID.....	11
8.1	Funcionamento.....	11
8.2	Instalação.....	12
8.3	Configurando.....	13
8.4	ACLs – Listas de Acessos ( <i>Access Lists</i> ) .....	14
8.5	ACLs Especiais .....	17
8.6	Redirecionadores .....	17
8.7	O Squirm .....	17
8.8	IPTABLES .....	18
9	VLANS - REDES LOCAIS VIRTUAIS .....	18
10	CENÁRIO .....	21
10.1	Cenário Atual .....	21
10.2	Cenário Proposto .....	22
11	METODOLOGIA.....	23
12	RESULTADOS .....	25
13	TRABALHO DE CONCLUSÃO DE CURSO – II.....	25
14	CONCLUSÕES.....	26
15	REFERÊNCIAS .....	27

## 1 INTRODUÇÃO

A natureza do homem tem peculiaridades, e uma delas é a busca incessante pelo controle de tudo que lhe rodeia.

Uma entidade qualquer pode ter muitas qualificações específicas de seus negócios, no entanto, se não souber organizar e trabalhar adequadamente as Informações que possui e necessita, não terá sucesso em seus negócios.

Em um ambiente acadêmico, o serviço de ensino é considerado primordial, e para que este serviço seja efetivo, é necessário organização e controle no ambiente de aprendizagem. No caso de aulas em laboratórios de informática (Labin) o controle diz respeito também à manutenção da atenção dos alunos nos objetos de ensino.

Nem sempre determinados conteúdos de uma disciplina conseguem manter a atenção total de alguns alunos. Se há um ambiente que proporcione maior distração com relação ao assunto que incomoda o indivíduo, com certeza o mesmo fará a escolha visando àquilo que mais lhe agradará.

O controle a ser abordado diz respeito à restrição de acesso a páginas na internet. Sem este tipo de controle, os alunos podem dispersar sua atenção com consultas a páginas não relacionadas com a disciplina.

Essa situação ocorre durante algumas aulas. E devido a este fato, nem todos os alunos conseguem ter um aproveitamento ideal das disciplinas lecionadas nas salas dos laboratórios de informática.

Visando controlar estas situações e ter uma disseminação da informação com a adequada atenção dos alunos, será proposto um projeto de sistema que esta em questão neste trabalho.

Logo a seguir serão apresentados e definidos o tema e sua delimitação, a solução proposta, o objetivo e sua justificativa e o embasamento teórico para se chegar a solução para este trabalho.

## **2 DEFINIÇÃO DO TEMA**

### **2.1 Tema**

Este trabalho tem como tema a proposta de desenvolvimento de um Sistema para controle de acesso aos sites da internet no Labin da Ulbra - Guaíba

### **2.2 Delimitação do Tema**

Será desenvolvido um sistema para controle de acesso de sites durante determinados horários de acordo com as especificações dos professores. Este sistema fornecerá uma interface web e se comunicará com o servidor proxy do Labin. Esse sistema será planejado, testado, avaliado e implementado no Labin da ULBRA de Guaíba.

O tema abrangerá as seguintes áreas: desenvolvimento de software, redes de computadores e suas regras de segurança em proxy.

Para desenvolvimento de Software será abordado apenas o conceito de diagramação para melhor esboçar os processos da interface WEB e sua comunicação com o Proxy.

Sobre redes serão abordados os conceitos sobre criação de VLANs para subdivisão dos laboratórios, tendo em vista que atualmente se encontram em uma única subrede, e que esta separação é essencial para a aplicação de regras de acesso distintas para laboratório.

Será explanado o conceito de Proxy, suas configurações e a distribuição Squid, solução atualmente em uso no cenário abordado, bem como as regras que melhor se adequarão a solução do problema de bloqueio de sites da rede do Labin.

### **3 SOLUÇÃO PROPÓSTA**

Nessa primeira etapa, que é o TCC-I, será elaborado e documentado o Sistema onde será possível agendar quais sites estarão liberados e quais estarão bloqueados em determinadas salas do LABIN, de acordo com horários pré-determinados.

Há diversas possíveis abordagens para a implantação de um Sistema de Bloqueio de sites e uma rede, seja empresarial ou acadêmica. Neste trabalho, define-se uma proposta, conforme será apresentada a seguir.

As salas do Labin serão divididas em diferentes redes, assim formando diferentes VLANs para melhor estruturar cada regra de bloqueio dos sites e da rede.

Será constituído um sistema para controle de acesso aos sites da internet e para esse Sistema, que funcionara via WEB, estarão disponíveis as seguintes funcionalidades:

- Cadastro de professor para o agendamento;
- Cadastro das salas a serem utilizadas;
- Modulo LOGIN de usuário;
- Modulo de agendamento para cadastros de sites permitidos e sites bloqueados.

A apresentação do Sistema nesse projeto será feita com os diagramas de UML, ficando assim mais detalhada suas funcionalidades e estrutura [UML01].

Na segunda etapa que é o TCC-II, será implementado, instalado e avaliado o Sistema desta proposta.

### **4 OBJETIVOS**

O Principal Objetivo deste TCC é desenvolver um projeto centrado nas necessidades de melhorias do atual sistema de bloqueio da rede em determinadas salas do LABIN.

Esse projeto visa empregar as disciplinas do curso no trabalho de conclusão para desenvolver um sistema de bloqueio de sites via WEB. Esse sistema atuará no

Labin, e os professores cadastrados poderão agendar, por data, hora e sala do LABIN, quais sites irão bloquear e quais sites irão permitir.

#### **4.1 Objetivos Específicos**

Durante o desenvolvimento deste projeto foram executadas as seguintes atividades: Reunião inicial, Definição do Tema e Elaboração da Proposta, Entrega da Proposta, Análise de Requisitos, Projeto Estrutural, Redação do Artigo, Revisão e Entrega do Artigo, redação do volume final, entrega do volume.

- Análise de Requisitos: Neste início de projeto será coletado o máximo de informações possíveis sobre necessidades específicas dos professores com relação ao sistema;
- Projeto Estrutural: através desta etapa foram definidos os softwares mais adequados a serem trabalhados Conforme os resultados da Análise de Requisitos;
- Redação do trabalho: foi redigida a Documentação que relatara a implementação do alvo desta proposta.

Para a segunda etapa do TCC ficam programadas as atividades práticas como o desenvolvimento do sistema, instalação do sistema, testes e avaliação do sistema, sendo as etapas:

- Desenvolvimento do Sistema: neste momento serão programadas as linhas de código fonte do sistema.
- Instalação do Sistema: juntamente com o acompanhamento do professor orientador será colocado em funcionamento no servidor o sistema de bloqueio de sites para adequá-lo ao ambiente do Labin.
- Testes e avaliação: nesta fase serão testadas as funcionalidades do sistema e avaliada sua aceitação com relação ao público alvo, nesse caso os professores.

## 5 JUSTIFICATIVA

Foi verificada a necessidade, por parte dos professores do curso de Sistemas de Informação, na ULBRA Guaíba, de desenvolver um sistema que possibilitasse, aos professores, bloquear alguns sites e liberar outros para o bom andamento da aula. No entanto, o bloqueio desses teria efeito sobre todo o LABIN enquanto o necessário seria apenas em determinadas salas.

No momento, o mecanismo mais eficiente para tal bloqueio é a remoção do cabo de energia do *switch*, e tão logo fosse necessária a utilização da rede o mesmo era religado.

O desligamento do switch interrompe a comunicação das estações com a rede. Sem a comunicação, os alunos perdem a capacidade de autenticação (login) nas estações, e o acesso recursos de servidor de arquivos, auto-atendimento, ou qualquer tipo de acesso que não seja a própria estação.

Havendo a necessidade de resolver este problema, será trabalhado e planejado o Sistema para o Bloqueio de Sites por agendamento.

## 6 REFERENCIAL TEÓRICO

Para o desenvolvimento deste projeto, será necessário utilizar conhecimentos adquiridos nas áreas que integram o curso de Sistemas de Informação.

Apresenta-se a seguir a fundamentação teórica para se chegar ao objetivo proposto neste trabalho. Isto se dá a partir de uma abordagem sobre Redes e regras de Proxy, apresentando seus conceitos e definições básicas; logo a seguir a sumária apresentação sobre Proxy, seu funcionamento e a distribuição Squid, juntamente com a apresentação sobre VLANs e do ambiente Labin.

## 7 PROXY

Servidor Proxy é um servidor HTTP com características especiais de filtragem de pacotes. O Proxy aguarda por uma requisição de dentro do Firewall, a repassa para um servidor remoto do outro lado do Firewall, recebe a resposta e a envia de volta a uma estação cliente [MAR03].

A principal vantagem dos proxies é a capacidade de armazenamento temporário de documentos. Numa estação que utiliza um Proxy para acessar uma página da Internet, uma cópia da página acessada é colocada no chamado cache do Proxy (Figura 1), que é uma área com um tamanho especificado pelo administrador e que contém as requisições ao sistema. Se um outro usuário acessa esta mesma página de outra estação, o proxy irá verificar com o servidor http que contém a página, se a mesma não foi modificada. Caso não tenha sido alterada, o Proxy descarrega no navegador do usuário a página contida em seu cache. Isto aumenta a performance dos acessos à Internet.

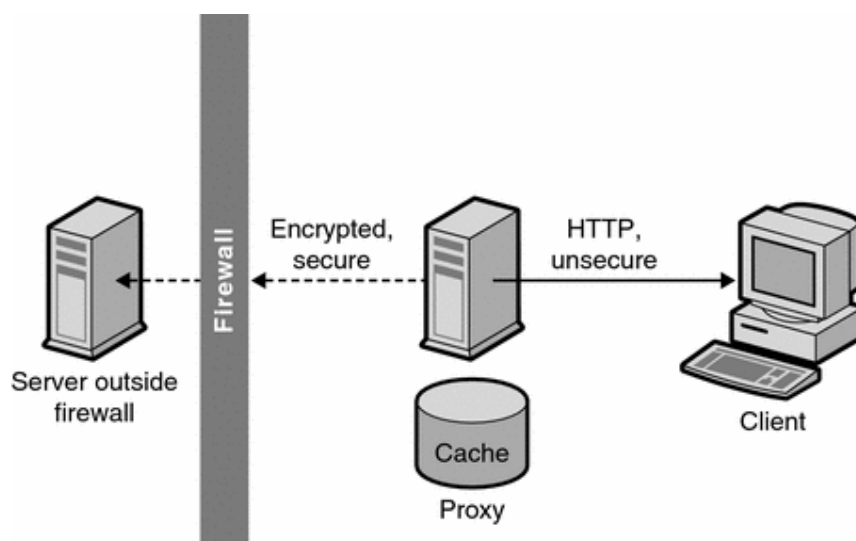


Figura 1 – Proxy Cache

O Proxy ainda pode criar regras de acesso, permitindo ou não acessos a sites. Isto é importante para evitar a navegação em sites com conteúdo explícito (pornográfico), salas de Chat, etc.

Um Proxy também serve como um firewall baseado em um protocolo (HTTP, por exemplo) e que filtra estes acessos vindos de clientes na rede interna na qual faz papel de um canal de saída. Os proxies não necessitam de nenhum tipo de hardware especial, apenas uma máquina com uma boa quantidade de memória (64 Mbytes para uma rede com cerca de 100 máquinas) e um bom espaço em disco (100 Mbytes para começarmos é o ideal) [MAR03].

O Proxy em si possui algumas vantagens inerentes interessantes. A mais comum é como um filtro de IPs, permitindo ou não acessos a sites da web. De um outro ponto de vista, um Proxy é uma excelente ferramenta de auditoria de acessos, já que tem a capacidade de armazenar em seus arquivos de log todas as conexões feitas através do mesmo.

Agora, o Proxy possui algumas desvantagens que vários autores abordam dentro de seus livros e artigos técnicos. Os aspectos mais relevantes seriam [MAR03]:

- Poucos serviços suportados - Nem todos os serviços são suportados pelos proxies mais comuns do mercado. A relação entre um cliente e um servidor Proxy deve ser muito bem estruturada e, no caso de muitos sistemas operacionais, isto não ocorre.
- Grande trabalho de atualização em clientes - Existe uma carga muito grande de atualização/modificação de clientes, que em muitas situações se torna extremamente desvantajosa. Em ambientes mistos, o problema pode ser muito mais grave.
- Problemas de segurança em protocolos/aplicações - O Proxy não protege uma estação de possíveis falhas de segurança nos protocolos, ou em aplicações, por exemplo, um *buffer overflow* contra um determinado aplicativo não será bloqueado pelo Proxy. Este tipo de problema é o mais grave.

Normalmente um Proxy trabalha em conjunto com um filtro de pacotes, completando assim a segurança do site em diversos aspectos importantes no que diz respeito aos acessos e às tentativas de invasão. É muito interessante este dueto de mecanismos de segurança, já que cria uma dificuldade maior para o invasor.

Os proxies são programas importantes no que diz respeito à aceleração e à performance de uma conexão à Internet. Por ser um tipo de firewall simples, é interessante que trabalhe em conjunto com um outro filtro de pacotes, com regras e políticas bem definidas. Importante ressaltar que apenas uma configuração bem definida, planejada e estruturada terá sucesso no sistema de segurança.

## 8 SQUID

O Squid é um servidor Proxy em software livre. Apresenta-se como um dos melhores softwares para a função do mercado. É projetado principalmente para ser executado em sistemas operacionais LINUX

O Squid está em desenvolvimento faz muito tempo, por isso, é completo, robusto, confiável, e tem seu código aberto com licença GNU GPL. Squid é um Proxy-cache de alto desempenho para clientes WEB. É apoiado por muitos protocolos, embora seja principalmente usado para gopher, HTTP e FTP. Também tem suporte para TLS, SSL e HTTPS. O Squid tem se tornado obrigatório na instalação dos provedores de qualquer empresa que deseja garantir um bom desempenho de sua conexão ou criar regras de acesso (ACLs, *Access Lists*) para servidores web [SQU01].

Esse software teve seu começo através do projeto Harvest da ARPA e foi fruto dos esforços de Duane Wessels e uma série de colaboradores espalhados pelo mundo.

O Squid pode ser executado nas seguintes plataformas: Linux, FreeBSD, AIX, NetBSD, BSDI, HP-UX, OSF, Digital Unix, IRIX, SunOS/Solaris, NextStep, SCO Unix, OS/2 e Windows NT [SQU02].

Apesar de sua estabilidade o Squid esta em constante atualização e é um dos mais populares.

### 8.1 Funcionamento

O principal arquivo de configuração é o squid.conf que encontra-se no diretório /etc/squid. É um arquivo muito extenso, contém aproximadamente 3000 linhas, porém para deixá-lo funcional, basta configurar apenas algumas linhas.

O Squid mantém meta dados e especialmente objetos armazenados na RAM, fazendo um cache de buscas de DNS. Implementa, também, um cache negativo de falhas de requisições ou requisições falhas [SQU01].

## 8.2 Instalação

Esse software vem nativo na maioria das distribuições Linux, necessitando apenas ser inicializado e configurado. Para as demais distribuições, o Squid deve ter seus arquivos descompactados na máquina que fará o papel de servidor Proxy. Depois de efetuar o download do pacote do Squid em <http://www.squid-cache.org>, se devem executar os seguintes comandos [SQU01]:

```
# tar -xzf squid-2.5.STABLE1-src.tar.gz
# ./configure
# make all
# make install
```

Será criado o diretório `/usr/local/squid`, com os principais arquivos do Squid. Dentro deste diretório serão criados três subdiretórios: o `/etc` com os arquivos de configuração, o `/bin` com os binários do Squid e o `/logs` para futuras atividades do log do sistema.

Na seqüência deve-se criar um usuário (por exemplo: squid). Este usuário atuara como uma espécie de administrador do Squid. Na realidade é um usuário que o Squid utilizará para gerenciamento de seus arquivos de serviços e configuração.

Digitando o comando para sua criação e atribuição de senha:

```
# adduser squidadm
# passwd squid
# group add squid
```

Os profissionais da área de informática ressaltam a importância de nunca se executar o Squid pelo usuário root. Por motivos de segurança, até mesmo contra invasões, sempre se deve criar um usuário para administrar a execução do serviço.

Logo após a criação do usuário é necessário criar o diretório cache. Dentro deste diretório ficarão armazenadas as páginas de cache do Squid.

```
# cd /usr/local/squid
# mkdir cache
```

É necessário mudar o proprietário do arquivo para o usuário squidadm, pois o mesmo deverá ser o responsável por uma série de configurações importantes.

```
# chown squid cache
```

No diretório cache o Squid criará a área de armazenamento das páginas html visitadas pelos usuários do sistema. Este diretório terá uma série de subdiretórios, de acordo com a configuração feita no sistema.

### 8.3 Configurando

O arquivo squid.conf é o responsável por todas as configurações. Neste arquivo é que serão criadas as listas de acesso (ACLs, *Access Lists*) e onde deverão ser feitas as inserções, modificações e exclusões de parâmetros importantes no sistema [SQU02].

```
# NETWORK OPTIONS
#-----
# TAG: http_port
#     The port number where Squid will listen for http cliente requests.
#     Default is 3128, for httpd-accel mode use port 80.
#     May be overridden with -a on the command line.
#     You may specify multiple ports here, but, they MUST all be on a single line.
http_port 3128
```

http\_port 3128 – Indica em que porta TCP o Squid receberá requisições para acesso à Internet. Grande parte dos usuários do Squid utiliza este número, 3128, de porta como padrão. Normalmente através desta porta é que os usuários irão se conectar ao Proxy e acessar a web com todas as suas restrições ou não [SQU02].

```
#TAG: cache_dir
#     Usage:
#     cache_dir Directory-Name Mbytes Level - 1 Level2
#     You can specify multiple cache_dir lines to spread the cache among different disk
partitions.
Cache_dir /usr/local/squid/var/cache 100 64 64
```

Cache\_dir /usr/local/squid/var/cache 100 64 64 – Especifica o diretório para o armazenamento do cache do Squid. Nesse caso, o mesmo diretório criado durante a instalação. O número 100 indica o tamanho em Megabytes do arquivo de cache e o 64 64 indica o número de subdiretórios que serão abertos dentro do diretório /cache. O padrão é vir com 16 256, ou seja, 16 diretórios com 256 subdiretórios dentro de cada um deles. O padrão de 64 64 é utilizado para otimizar o tratamento dos diretórios de cachê [SQU02].

Existe uma controvérsia no que diz respeito aos arquivos de cache. Normalmente um espaço de 100 Mbytes em disco é o suficiente para o

armazenamento dos arquivos temporários, sem a necessidade de uma atualização muito grande pelo Proxy. Contudo, deve-se ter em consideração que isto, no caso de uma grande rede, pode se tornar insuficiente. É altamente recomendado que, durante o período de implantação do sistema, seja feito um acompanhamento dos logs do Squid. Caso exista a necessidade de um aumento do cache isto deverá ser implementado[SQU01].

Para executar o Squid deve-se fazer logon com o usuário criado durante a fase de instalação. Logo após serão executados alguns comandos a partir do diretório */usr/local/squid/bin*:

```
#!/squid -z
#!/RunCache
```

Se o funcionamento estiver correto, o Squid gerará um arquivo chamado *squid.out*. Este arquivo representa um log do processo de inicialização do Squid, e é aconselhável visualizar, pois em caso de problemas o mesmo os apontará. O script *RunCache* é que inicializa o Squid para as futuras requisições à Internet. A opção *squid -z* cria os subdiretórios de cache do Squid. É interessante que o proprietário do *squid.out* seja o usuário *squidadm*, para acompanhar e corrigir problemas no Squid. Para tornar o usuário *squidadm* owner do arquivo, é necessário o seguinte comando no diretório do Squid:

```
# chown squidadm squid.out
```

Iniciando o Squid a partir do *rc.local*:

Para finalizar a instalação e iniciar o Squid a partir do boot de um servidor Linux, é necessário acrescentar a seguinte linha de comando no arquivo */etc/rc.d/rc.local*:

```
#su squidadm /usr/local/squid/bin/./RunCache&
```

Com isto o Squid não precisará mais ser iniciado manualmente toda vez que o sistema for desligado.

#### **8.4 ACLs – Listas de Acessos (Access Lists)**

Uma das características mais interessantes do Proxy não é só o cache, mas principalmente a restrição de acesso a sites não autorizados. Isto inibe os usuários a acessarem sites pornôns, ou sites de jogos, ou qualquer outro tipo de site que

possa desviá-los do seu trabalho do dia a dia. As ACLs também podem ser utilizadas para regular acessos por hora e data. Em uma grande empresa, em muitos casos, esta situação se torna obrigatória [MAR03].

No arquivo squid.conf existe um parâmetro ligado às ACLs. No exemplo abaixo é possível verificar uma lista de acesso por máquinas:

```
# ACCESS CONTROLS
#-----
#TAG: acl
#   Defining as Access List
#   acl aclname acltype string1 . . .
#   acl aclname acltype "file" . . .
#
#   when using "file", the file should contain one item per line
#
```

Existem várias opções explicativas neste parâmetro, mas que realmente interessam são as seguintes:

```
Acl all src 0.0.0.0/0.0.0.0
Acl manager proto cache_object
Acl localhost src 127.0.0.1/255.255.255.255
Acl SSL_ports port 443 563
Acl Safe_ports port 80 21 443 563 70 210 1025 65535
Acl CONNECT method CONNECT
```

Os parâmetros citados criam uma série de listas, como por exemplo:

```
Acl all src 0.0.0.0/0.0.0.0
```

Nesta linha criou-se uma lista de acesso chamada all onde os endereços Ips válidos são todos os da Internet (0.0.0.0/0.0.0.0). Por exemplo, para criar uma lista da diretoria de uma empresa, seria colocada uma lista com o seguinte conteúdo:

```
Acl diretoria scr 10.0.0.2 10.0.0.3 10.0.0.4
```

Nesta lista, as máquinas com os endereços IP anteriormente mostrados, farão parte da acl diretoria.

Logo abaixo, estão definidas as restrições e algumas regras serão mostradas:

```
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny!Safe_ports
http_access deny CONNECT!SSL_ports
#
```

Para uma boa estrutura de regras é indicado que sempre se comece com as regras que têm o parâmetro *allow*, ou seja, de autorização, em seguida sempre as de proibição *deny*. No próximo exemplo estão liberados acessos a acl diretoria e negado a acesso aos endereços restantes.

```
#INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow diretoria
http_access deny all
```

Para bloqueio de sites de conteúdo explícito é necessário criar uma acl da seguinte maneira:

```
Acl porno url_regex
"/usr/local/squid/etc/porno"
```

Onde *porno* é um arquivo que é possível editar com palavras que podem aparecer no endereço web de um site, como por exemplo: <http://www.sosexo.com>.

Dentro do arquivo a palavra *sexo* deverá existir digitada, para ser possível criar uma lista de restrição. No arquivo, as palavras deverão estar uma embaixo da outra. É possível, também, criar outra lista com o conteúdo não pornográfico, mas que envolva termos que lembrem este tipo de assunto, como por exemplo:

```
Acl naoporno url_regex
"/usr/local/squid/etc/naoporno"
```

E a segurança ficaria da seguinte forma:

```
http_access allow naoporno all
http_access deny porno
```

Este tipo de filosofia pode ser usado para sites de jogos, bate-papo, entre outros, bastando o administrador da rede definir suas listas de acessos a sites não permitidos.

## 8.5 ACLs Especiais

Existem muitas regras que podem ser criadas nas ACLs do Squid. No entanto, para este trabalho, se apresentara apenas a necessária na resolução do principal problema apresentado neste TCC.

Por Hora: Existem outros tipos de situações para as quais o Squid pode contribuir, e muito, com o controle de acesso em uma rede.

Supondo que uma empresa só permita o acesso à Internet após o expediente, ou então, na hora do almoço. Para isso, seria criada uma lista de acesso na hora do almoço para todos os usuários em uma intranet numa rede 10.0.0.0. Seria criada uma regra com o seguinte formato [MAR03]:

```
Acl users src 10.0.0.0/0  
Acl almoço time MTWHF 12:00-13:30  
http_access allow users almoço  
http_access deny user
```

É importante observar na regra acima que as letras MTWHF são os dias da semana em inglês e que assim são interpretados pelas ACLs do Squid: (Monday, Tuesday, etc...).

## 8.6 Redirecionadores

Os redirecionadores são definidos por um tipo de ferramenta importante na configuração de qualquer Proxy. No caso do Squid, existem vários softwares voltados exclusivamente para o mesmo. Dentre esses softwares, destaca-se o Squirm[MAR03].

O redirecionador é um programa que permite ao administrador controlar as URLs destinos de seus usuários. Um exemplo é quando um usuário digita em um navegador <http://www.páginaporno.com.br> e o Squid o redireciona para uma página inofensiva. No FAQ do Squid, ele recomenda a utilização do Squirm, por ser um programa de fácil instalação e configuração.

## 8.7 O Squirm

O Squirm foi desenvolvido por Chris Foote e, como todo software para Linux, é gratuito e de fácil instalação.

O Squirm pode ser obtido através do endereço <http://www.senet.com.au/squirm/squirm-1.0betab.tar>. e sua instalação é feita através do seguinte conjunto de comando:

```
#tar -xvf squirm-1.0betab.tar
```

## 8.8 IPTABLES

O Iptables é um programa que como objetivo proteger a máquina contra acessos indesejados, tráfego indesejado, proteger serviços que estejam rodando na máquina e bloquear a passagem de outros que se não deseja receber (como conexões vindas da Internet para a rede local, evitando acesso aos dados corporativos de uma empresa ou a seus dados pessoais). No kernel do Linux 2.4, foi introduzido o filtro de pacotes iptables (também chamado de netfilter) que substitui o ipchains dos kernels da série 2.2. Este firewall tem como vantagem ser muito estável (assim como o ipchains e ipfwadm), confiável, permitir muita flexibilidade na programação de regras pelo administrador do sistema, fornece mais opções disponíveis ao administrador para controle de tráfego, controle independente do tráfego da rede local/entre redes/interfaces devido a nova organização das etapas de roteamento de pacotes [IPT01].

## 9 VLANS - REDES LOCAIS VIRTUAIS

Definem-se redes locais como um sistema de comunicação de dados confinado a uma área geográfica limitada, possuindo altas taxas de transmissão, de acordo com a tecnologia utilizada. Entretanto, diz-se que uma LAN é "um único domínio *broadcast*". Ou seja, é o grupo de todos os dispositivos que receberão os quadros de *broadcast* originários de qualquer dispositivo que pertença a este mesmo grupo. Os domínios de *broadcast* são tipicamente delimitados por roteadores, já que estes não encaminham quadros deste tipo [VLA01].

As VLANs são uma solução alternativa ao uso de roteadores para conter o tráfego *broadcast*, já que estas segmentam as redes locais em diferentes domínios desta natureza. Elas aumentam tanto o desempenho, conservando a largura de banda, quanto a segurança de uma rede local, limitando o tráfego a domínios específicos.

Quanto a forma de identificação, as redes locais virtuais podem ser classificadas como VLANs baseadas e:

- Portas (camada 1): Os membros de uma VLAN podem ser definidos de acordo com as portas da ponte/switch utilizado. Por exemplo, em um switch com dez portas, as portas 1, 2, 3 e 8 pertencem a VLAN 0. Já as portas 4, 9 e 10 fazem parte da VLAN 1. As demais pertencem a VLAN 2. Este método vem sendo o mais utilizado na implementação de VLANs, pois sua configuração é rápida e simples. No entanto, caso um usuário se mova para um local diferente, fora da ponte/switch onde estava conectado, o administrador da rede deve reconfigurar a VLAN. Esta é a principal desvantagem deste método. Além disso, deve se ressaltar que ao conectar um repetidor, um hub ou outro switch a uma porta pertencente a uma VLAN, todas as estações conectadas e este dispositivo se tornaram membros desta VLAN.
- Endereço MAC (*Media Access Control*, camada 2): Neste caso os membros da rede virtual são identificados pelo endereço MAC (*Media Access Control*) da estação de trabalho. O switch reconhece o endereço MAC pertencente a cada VLAN. Quando uma estação de trabalho é movida, não é necessário reconfigurá-la para que esta continue pertencendo a mesma VLAN, já que o endereço MAC faz parte da sua placa de interface de rede. Isto é uma vantagem em relação as VLANs baseadas em portas, onde a tabela de membros tem de ser reconfigurada. O grande problema deste método é que um membro de uma VLAN deve ser inicialmente especificado,

obrigatoriamente. Em redes com milhares de usuários isto não é uma tarefa simples. Os membros de uma VLAN camada 2 também podem ser identificados de acordo com o campo "tipo de protocolo" encontrado no cabeçalho da camada 2.

- Endereço IP (*Internet Protocol*, camada 3): Neste método os membros pertencentes a uma VLAN são determinados pelo cabeçalho da camada 3. O endereço IP pode ser usado nesta classificação. Embora um membro seja identificado por uma informação da camada 3, este processo não é realizado pelo roteador e também não há nenhuma relação com o roteamento nesta rede. Neste método, o endereço IP é usado somente como um mapeamento para determinar os usuários de uma VLAN. Em VLANs camada 3, os usuários podem mover suas estações de trabalho sem reconfigurar os seus endereços de rede. O único problema é que geralmente o tempo para o encaminhamento de pacotes usando informações da camada 3 é maior do que utilizando o endereço MAC.

## 10CENÁRIO

Há uma necessidade por parte dos professores em bloquear alguns sites em determinados dias, pelo período de aula em cada sala do Labin.

O problema é enfrentado por grande parte dos professores que lecionam no Labin. Apesar da necessidade de utilizar os computadores no período de aula, os alunos acabam se dispersando com outros conteúdos na Internet.

### 10.1 Cenário Atual

Atualmente as salas do Labin utilizam endereçamento de IP dinâmico. O que dificulta o controle de acessos direcionado por salas. Neste caso, as regras de filtragem do Proxy atuam em todo o Labin com as mesmas regras (Figura 2).

Até o momento as configurações do proxy Squid, que estão atuando nas salas do Labin, vigoram em um regime de 24x7, ou seja, 24 horas por dia e 7 dias da semana. As regras de bloqueio dos sites parte de um arquivo nomeado "Bloq.txt". Esse arquivo tem sites fixados e alguns são liberados e outros são bloqueados, dependendo do estudo de caso de uso de cada um deles por parte do administrador da rede.

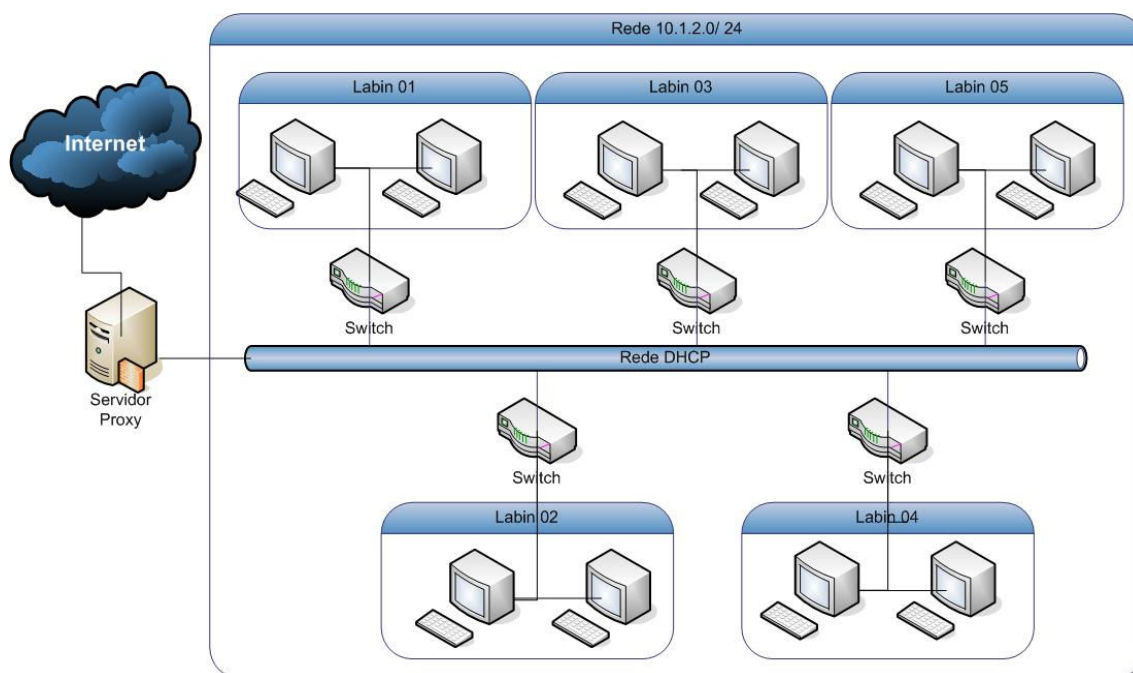


Figura 2 - Cenário Atual

## 10.2 Cenário Proposto

O cenário proposto envolve a divisão lógica das redes entre as salas do Labin e a adição de um sistema via WEB que fará as regras de bloqueios baseadas nos parâmetros indicados pelos professores.

É possível visualizar na figura abaixo (Figura 3) que o proposto neste trabalho é manter a condição de rede que utiliza endereçamento de IP Dinâmico, separando as salas em subredes diferentes através de VLANs na camada 1 (por portas no switch).

Para este cenário que está se propondo no projeto, o Squid estará sendo configurado com a retenção independente da rede de cada sala. Essa filtragem será definida conforme os parâmetros informados por cada professor. Portanto, poderão ser programadas por horário e data.

Estará disponível para o professor consultar, cada vez que o mesmo for programar um bloqueio, a lista com os sites bloqueados e os permitidos. Essa consulta será feita em um arquivo onde serão geradas as referidas listas de bloqueios e apresentadas através da interface web disponibilizada ao professor. O sistema irá converter as informações definidas pelos professores em ACLs para o proxy.

O proxy irá consultar estas ACLs e atualizar a política de acesso a páginas no momento a política de acesso a páginas no momento do cadastro. A ACL irá controlar o acesso no período definido pelo professor no sistema.

O sistema será seguro com relação a fraudes de liberações e de bloqueios. Apesar de trabalhar via web, que não tem segurança concreta, a mesma será definida por utilizar a linguagem de programação web PHP, que por sua vez fará as consultas todas no servidor ao contrario das outras que fazem a consulta no cliente e enviam os resultados via rede.

Entretanto, é importante ressaltar que apesar de toda a tecnologia empregada ainda é possível usufruir da melhor forma possível dos recursos empregados. E dessa forma é que será estabelecido o sistema de retenção que fará a filtragem dos sites utilizados durante as aulas. Com isso, serão melhor aproveitados os equipamentos do Labin e haverá um aumentando da atenção dos alunos, que atualmente é dispersa, durante as aulas nos Laboratórios.

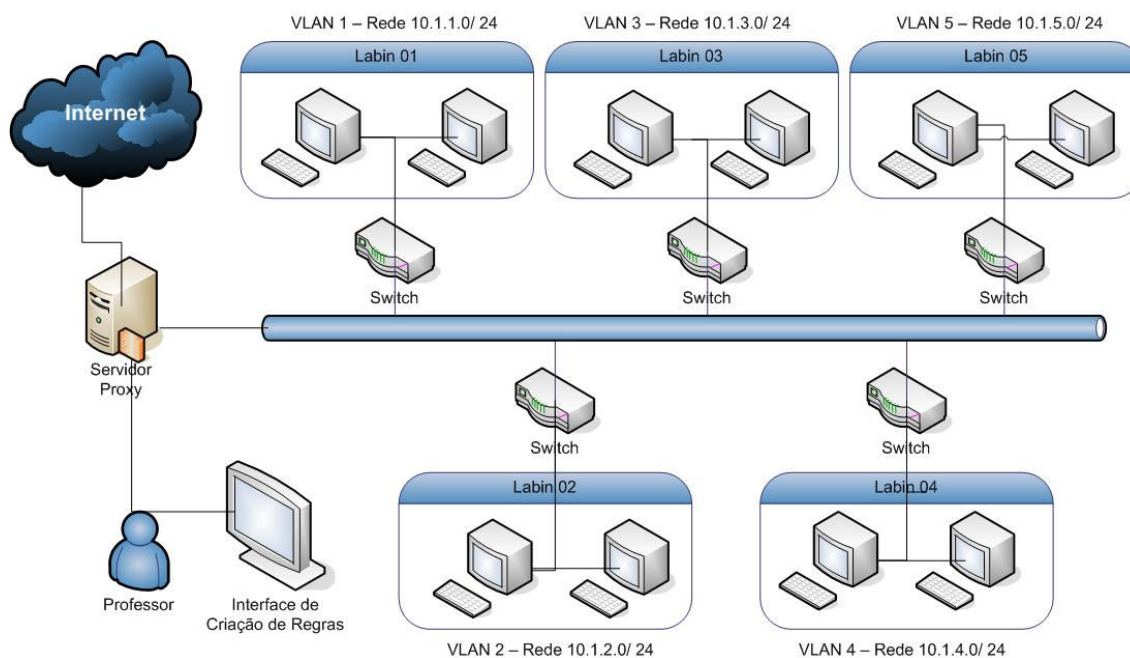


Figura 3 – Cenário Proposto

## 11 METODOLOGIA

A metodologia para elaboração deste projeto terá várias etapas, que envolvem a pesquisa de bibliografia, livros, sites que tratem dos assuntos relacionados. Após pesquisa e seleção de bibliografias têm-se um processo de leitura para conceituar os assuntos abordados. As informações referentes aos parâmetros de acesso as regras do Proxy serão obtidas através de reunião com o administrador do servidor. Paralelo a isso, serão realizadas modificações de rede do Labin, transformando cada sala em uma VLAN. Para elaboração da interface, também será necessário estudo das linguagens de programação WEB PHP e HTML [PHP01].

Porque PHP e HTML?

Porque estas linguagens de programação têm seus funcionamentos básicos voltados para desenvolvimento WEB. As funcionalidades da linguagem PHP proporcionam maior segurança ao utilizar a aplicação a ser implementada.

O diagrama de caso de uso é utilizado na figura 4 para demonstrar amplamente os personagens relacionando seus processos [UML01].

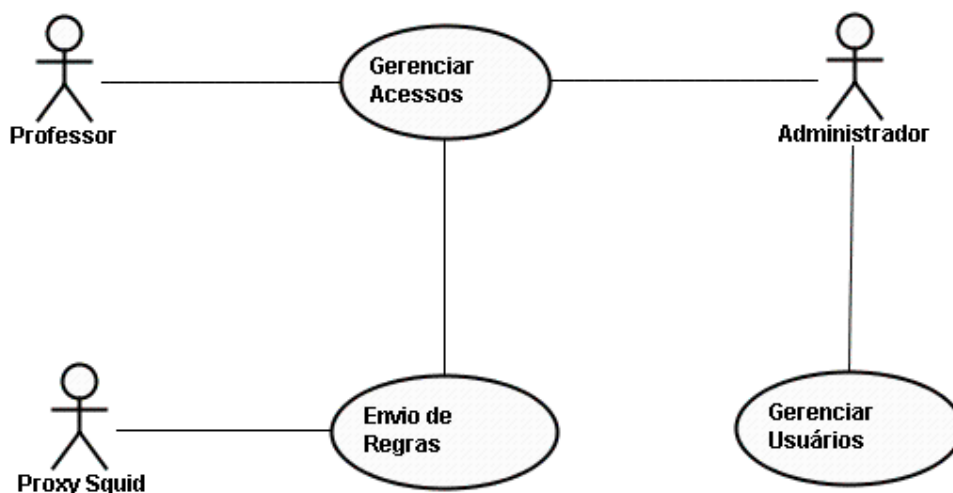


Figura 4 – Caso de Uso.

**Gerenciar Acessos:** no referido processo tanto o Administrador quanto o Professor, que é o personagem principal, podem interagir. Neste, o professor fará seus agendamentos, consultando no banco que contem as sugestões de sites, para encurtar sua pesquisa. No momento de criação da regra o professor também devera especificar qual sala ira lecionar e em qual data fará as devidas restrições.

**Envio de Regras:** o envio de regras é um processo que será feito após o processo de gerência de acessos. Nesse, após criadas regras com base nos parâmetro definidos pelo professor, será enviada para o servidor proxy Squid, que por sua vez processará as regras conforme pré-estabelecido em sua programação de atualização.

**Gerenciar Usuários:** o processo de gerenciar usuários irá interagir apenas com o Administrador do sistema. Este, por sua vez, criará usuários para cada professor ou irá apagar aqueles que não estiverem sendo utilizados.

## **12 RESULTADOS**

Conforme apresentado no referencial teórico e na solução proposta, têm-se os subsídios necessários para o desenvolvimento da aplicação, que terá como resultado a interface entre os Professores e as Regras a serem criadas.

## **13 TRABALHO DE CONCLUSÃO DE CURSO – II**

Diante do objetivo específico apresentado para o trabalho e tendo como referencia as atividades e conclusões do atual trabalho conclusão de curso (TCC-I), ficam especificadas as seguintes atividades para o TCC-II, a fim de alcançar-se o objetivo proposto:

- Desenvolvimento do Sistema: neste momento serão programadas as linhas de código fonte do sistema.
- Criação das VLANs: será feita a divisão das salas do Labin em diferentes redes, criando assim as VLANs o que possibilitará o controle direcionado a cada sala;
- Instalação do Sistema: juntamente com o acompanhamento do professor orientador será colocado em funcionamento no servidor o sistema de bloqueio de sites para adequá-lo ao ambiente do Labin.
- Testes e avaliação: nesta fase serão testadas as funcionalidades do sistema e avaliada sua aceitação com relação ao público-alvo, nesse caso os professores.

## 14 CONCLUSÕES

Foram aplicados os conhecimentos adquiridos nas disciplinas do curso de Sistema de Informação para elaboração e para a futura efetivação desse trabalho, assim contribuindo para a melhor compreensão das mesmas.

Com base no que foi apresentado neste projeto, mais especificamente nos objetivos, referencial teórico e nos resultados, é possível concluir a documentação de um trabalho que irá diferenciar a utilização dos meios disponíveis nos laboratórios de informática da Ulbra no *campus* Guaíba. Essa diferenciação irá aprimorar a aprendizagem dos alunos e facilitará, para os professores, o ensino, daqueles que utilizarem os laboratórios de informática.

No entanto, é interessante que o único beneficiado com trabalho não seja apenas o aluno, com a assimilação sobre os conteúdos abordados neste, mas também o *campus* da Ulbra Guaíba.

Sendo assim, dentre os beneficiados com este trabalho têm-se os professores, que receberão uma ferramenta adicional, a qual agregará melhores resultados aos seus trabalhos, o aluno que apresenta este projeto e emprega seus conhecimentos, e por fim, os alunos que utilizam os laboratórios de informática, pois se concentrarão mais no momento da aula, obtendo, com isso, um maior aproveitamento dos recursos disponibilizados nos laboratórios para serem utilizados de acordo com aula.

## 15 REFERÊNCIAS

[MAR03] MARCELO, Antonio – **SQUID - Configurando o Proxy para Linux**. 2. ed. Rio de Janeiro: Brasport, 2003.

[PHP01] CONVERSE, Tim e PARK, Joyce – **PHP, A Bíblia 2ª Edição** [2003]

[SQU02] LUNARDI, Marco, Agisander – **Squid – Prático e Didático** [2005]

[TAN02] TANENBAUM, Andrew S - **Redes de computadores** [2002]

[UML01] GUEDES, Gilleanes T. A. – **UML – Uma abordagem Prática** [2004]

[VLA02] OSTERLOH, Heather - **IP Routing – Primer PLUS** [2001]

[IPT01] Acessado em 07/10/2007  
<<http://focalinux.cipsga.org.br/guia/avancado/ch-fw-iptables.htm>>

[SQU01] Acessado em 13/10/2007  
<<http://www.linuxman.pro.br/squid/node/1/node/1/#toc27>>

[VLA01] Acessado em 02/10/2007  
<<http://www.candelatech.com/~greear/vlan.html>>

[VLA03] Acessado em 02/10/2007  
<<http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=4997&pagina=3>>