

# Desenvolvimento de Sistema para Bloqueio de Sites

Carlos Henrique Soares de Souzal<sup>1</sup>, André Peres<sup>2</sup>

<sup>1</sup> Acadêmico do Curso de Sistemas de Informação da ULBRA Guaíba  
< carloshss@hotmail.com >

<sup>2</sup> Professor Orientador do Curso de Sistemas de Informação da ULBRA Guaíba  
< peres@guaiba.ulbra.tche.br >

*Resumo: Este artigo tem como objetivo apresentar a proposta para o desenvolvimento de um sistema de bloqueio de sites através de regras de Proxy e divisões de redes em VLANs. Serão apresentados conceitos sobre Proxy, Squid e VLANs, juntamente com as respectivas configurações que serão utilizadas, concluído com a explanação do cenário atual e as próximas atividades.*

*Abstract: This paper has as objective to present the proposal for the development of a system of blockade of sites through rules of Proxy and divisions of nets in VLANs. Concepts on Proxy, Squid and VLANs will be presented, together with the respective configurations that will be used, concluded with the communication of the current scene and the next activities.*

## 1 - INTRODUÇÃO

O Principal Objetivo deste artigo é apresentar uma proposta para o desenvolvimento de um projeto centrado nas necessidades de melhorias do atual sistema de bloqueio da rede do Labin em determinadas salas e dias.

Este artigo está organizado conforme segue: A seção 2 contém uma introdução sobre a definição de Proxy, apresentando seus conceitos e o que será utilizado sobre o trabalho; Na seção 3 apresentam-se noções sobre a utilização do Squid e como suas configurações irão atuar sobre o bloqueio; Na seção 4 contém uma introdução sobre VLANs, seus conceitos e definições, bem como a mesma será utilizada na criação do sistema; por fim, tem-se a descrição da solução proposta juntamente com a conclusão, que nortearam a continuidade do projeto.

## 2 - PROXY

Marcelo (2003) considera que 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.

O Proxy pode criar regras de acesso, permitindo ou não acessos a sites. Isto é importante para evitarmos navegação em sites com conteúdo explícito (pornográfico), salas de Chat, ou qualquer outro conteúdo impróprio para o local ou momento.

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. 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.

Normalmente um Proxy trabalha em conjunto com um firewall, 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 firewall, com regras e políticas bem definidas. Importante ressaltar que apenas uma configuração bem definida, planejada e estruturada terá sucesso no sistema de segurança.

O Proxy tem muitas funcionalidades interessantes, no entanto será utilizado, para este trabalho, apenas sua capacidade de filtragem e de criar regras. Existem muitos softwares que fazem o papel de um Proxy, todavia, será utilizado, para o desenvolvimento do sistema, o Squid.

### 3 - SQUID

Marcelo (2003) considera que o Squid é um servidor Proxy em software livre, ou seja, gratuito. Apresenta-se como um dos melhores softwares para a função do mercado. É projetado principalmente para rodar em sistemas operacionais LINUX

O Squid<sup>1</sup> 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 alta performance 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 uma boa performance de sua conexão ou criar regras de acesso (ACLs, Access Lists) para servidores web.

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.

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

#### 3.1 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 cachê de buscas de DNS. Implementa, também, um cachê negativo de Falhas de requisições ou requests falhos.

---

<sup>1</sup> Pode ser obtido através de download do site <http://www.squid-cache.org>.

### 3.2 Instalação

Esse software vem nativo<sup>2</sup> 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.

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.

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.

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

### 3.3 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.

```
# 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

---

<sup>2</sup> Nativo: já programado para ser instalado junto com o sistema operacional.

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.

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.

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

Uma das características mais interessantes do Proxy não é só o cachê, 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.

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 cachê_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 de Labin01, seria colocada uma lista com o seguinte conteúdo:

```
Acl Labin01 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 Labin01.

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
#
```

No primeiro grupo de regras foram relacionadas com as ACLs padrão criadas. 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 Labin01 e negado a acesso aos endereços restantes.

```
#INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow Labin01
http_access deny all
```

### 3.4.1 ACLs Especiais

Existem muitas regras que podem ser criadas nas ACLs do Squid. No entanto, para este trabalho, se apresentaram apenas as necessárias 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 Universidade só permita o acesso à Internet após a aula, ou então, na hora de intervalo. Para isso, seria criada uma lista de acesso na hora do intervalo para todos os usuários numa rede 10.0.0.0. Seria criada uma regra com o seguinte formato:

```
Acl users src 10.0.0.0/0
Acl intervalo time MTWHF 20:45-21:00
http_access allow users intervalo
http_access deny user
```

É importante observar na regra acima que as letras MTWHF são os dias da semana em inglês: (Monday, Tuesday, e os demais).

## 4 - VLANs - REDES LOCAIS VIRTUAIS

Tanenbaum (2002) Define 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.

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 em:

#### **4.1 VLANs baseadas em:**

As VLANs podem ser criadas de diversas formas utilizando as camadas OSI, no entanto apenas uma dessas divisões é inerente ao trabalho.

Endereço IP (Internet Protocol, camada 3): Neste método (CAN03) 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.

## **5 - CENÁRIO**

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.

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.

## **6 - SOLUÇÃO PROPOSTA**

A proposta deste trabalho é dividir as salas do Labin em VLANs. Essa divisão será utilizada na criação de regras para o Proxy. As regras também irão utilizar os sites indicados e as datas necessárias para o bloqueio.

Para isso, será elaborado um sistema via web, que será acessado pelos professores cadastrados, que crie um arquivo contendo as regras para o bloqueio. Este bloqueio terá como parâmetro, para criação das regras, os sites e a data que serão indicados pelo professor no momento do agendamento.

Na etapa de desenvolvimento serão utilizadas as linguagens de programação PHP e HTML e seus editores mais apropriados. A página fará o cadastro dos professores autorizados a agendar os bloqueios.

O Proxy será configurado, para reiniciar suas regras, todos os dias indicados, antes do início da aula.

Para demonstrar o sistema a ser desenvolvido, serão elaborados diagramas UML.

## **7 - CONCLUSÃO**

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 do Proxy. Utilizando-se do conjunto de parâmetros, informados pelo professor, através do sistema de bloqueio de sites, será possível bloquear os sites que dispersão a atenção do aluno com relação a aula.

Na segunda etapa do TCC, será desenvolvido, implementado, testado e avaliado o sistema proposto para a solução do problema acima descrito.

## 8 - BIBLIOGRAFIA

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

Tanenbaum (2002) TANENBAUM, Andrew S: **Redes de computadores** [2002]

(MAN01) Acessado em 13/10/2007

<<http://www.linuxman.pro.br/squid/node/1/node/1/#toc27>>

(FOC02) Acessado em 07/10/2007 <<http://focalinux.cipsga.org.br/guia/avancado/ch-fw-iptables.htm>>

(CAN03) Acessado em 02/10/2007 <<http://www.candelatech.com/~greear/vlan.html>>