UNIVERSIDADE ESTADUAL DE GOIÁS
UNIDADE UNIVERSITÁRIA ITABERAÍ
SISTEMAS DE INFORMAÇÃO

Adriano Cardoso Borges

Romario da Cunha Rodrigues

CONTROLE DE ACESSO À INTERNET EM AMBIENTES COORPORATIVOS

ITABERAÍ

NOVEMBRO DE 2011

ADRIANO CARDOSO BORGES

ROMARIO DA CUNHA RODRIGUES

CONTROLE DE ACESSO À INTERNET EM AMBIENTES COORPORATIVOS

Trabalho de conclusão de curso apresentado ao curso de Sistemas de Informação da Universidade Universitária Itaberaí – UEG, como parte dos requisitos para a obtenção do grau de Bacharel em Sistemas de Informação.
Orientador: Odiney Jacomini

ITABERAÍ

2011

ADRIANO CARDOSO BORGES

ROMARIO DA CUNHA RODRIGUES

CONTROLE DE ACESSO À INTERNET EM AMBIENTES COORPORATIVOS

Trabalho de conclusão de curso apresentada ao curso de Sistemas de Informação da Universidade Universitária Itaberaí – UEG, como parte dos requisitos para a obtenção do grau de Bacharel em Sistemas de Informação.
Orientador: Odiney Jacomini

Aprovada em _____/_____/_____.

Banca examinadora

_____

Odiney Candido Jacomini

_____

Rogério Alexandre Leite

Dedicamos este trabalho a Deus e a nossos familiares que estiveram sempre presentes nos apoiando nos momentos bons e ruins

Ao Prof. Odiney, pela paciência e pela orientação durante esta longa jornada, aos colegas de curso, que de forma silenciosa também são responsáveis por este trabalho e aos nossos familiares que contribuíram para que pudéssemos realizar mais esta etapa da nossa vida.

RESUMO

Este trabalho tem como objetivo apresentar uma proposta de implementação de uma solução eficaz no controle de acesso à Internet em ambientes coorporativos, apresentando um conjunto de ferramentas com funções específicas, no intuito de atingir um alto grau de segurança.

Palavras-chave: Segurança, Controle de Acesso, Squid.

ABSTRACT

This paper aims to present a proposal to implement an effective solution to control Internet access in corporative environments, presenting a set of tools with specific functions in order to achieve a high degree of safety.

Keywords: Security, Access Control, Squid.

LISTAS DE FIGURAS

SUMÁRIO

1 – INTRODUÇÃO

O crescimento e desenvolvimento tecnológico das empresas da atualidade são facilmente perceptíveis, e fica impossível pensar em tudo isso sem a presença da internet no seu cotidiano, porém temos que analisar como a internet está sendo empregada nessas organizações, pois ela não traz consigo apenas benefícios.

A maneira na qual seus colaboradores estão a utilizando é uma preocupação para os proprietários dessas organizações, pois o acesso as redes sociais no horário de trabalho para fins pessoais é muito grande, fazendo assim com que o rendimento seja diminuído e prejudicando o fluxo normal do trabalho da empresa, além do risco de expor dados confidenciais da empresa.

Tendo em vista estes problemas enfrentados, propomos o desenvolvimento de um servidor *proxy-cache*, utilizando a ferramenta *Squid* rodando sobre o sistema operacional *Debian*, ambos *software* livre.

Propomos a utilização do *cache* para que haja otimização do acesso à Internet, com economia de banda de rede, pois muitos conteúdos que são freqüentemente acessados ficam no *cache* do servidor, gerando assim uma otimização da navegação, disponibilizando mais recursos para atividades que exigem velocidade de acesso.

2 – CONCEITOS BÁSICOS

Neste capitulo estaremos explicando todas as necessidades, vantagens, desvantagens de se ter um sistema de controle de acesso à internet em ambientes corporativos, e para isso são necessários alguns conceitos.

2.1 – CONTROLE DE ACESSO

Quando falamos em internet independente do local em que se é empregada sabemos que teremos um longo e interessante assunto a ser discutido por ser uma ferramenta muito importante em nossas vidas atualmente. E ao analisarmos seu uso nas instituições e empresas no geral não é diferente. Sem duvida alguma a internet oferece diversos benefícios, benefícios esses que devem ser tratados com responsabilidade por parte das pessoas que estarão a utilizando. Sabemos também que atualmente é indispensável seu uso, mais temos que aproveitar o melhor que ela nos tem a oferecer.

Algumas empresas estabelecem políticas de segurança, esclarecendo ao colaborador as vantagens em se controlar e utilizar a internet de maneira responsável e benéfica para a empresa. Argumentos esses como: Minimizar os riscos de vírus, *trojans* e outras pragas da internet e aumentar a produtividade interna e externa da corporação. Mais mesmo com os relevantes argumentos apresentados muitas pessoas insistem em dizer que aos profissionais contratados por uma empresa tem direito a privacidade no acesso à internet. Muitas empresas optam por estabelecer um termo de compromisso que assinado pelo colaborador quando ele ingressa na empresa, termo esse que esclarece todo o procedimento de utilização da ferramenta por parte da empresa, estando ciente assim de suas responsabilidades e limites.

Mais por que as empresas têm essa necessidade de estar controlando o acesso a internet, quando buscamos saber os reais motivos desse importante controle estabelecido por elas passamos a ter uma visão completamente ampla sobre o assunto. Para iniciar uma discussão sobre esse assunto é fundamental deixar claro que o colaborador tem direito de utilizar as ferramentas virtuais tanto para uso pessoal quanto para uso profissional no âmbito empresarial. O colaborador,

por exemplo, pode realizar uma chamada por vídeo conferencia para fazer uma transação comercial por ordem do empregador através do MSN ou outro aplicativo, mais sabemos também que através do mesmo aplicativo o empregado pode, em vez de trabalhar, conversar com algum de seus contatos pessoais sobre futebol, novela ou outros assuntos particulares. É possível visualizar também que da mesma maneira que o empregado pode visitar diversos sites durante o expediente, sites relacionados com a empresa, ele pode também acessar sites que não tem nada a ver com seu trabalho como, por exemplo, sites relacionados a entretenimento como pornografia, esporte, filmes e outros. Não podemos esquece é claro das redes sociais que atualmente exerce um papel de destaque na vida das pessoas. Redes sociais como, Orkut, Facebook, Twitter e várias outras, redes sociais essas que podem ser utilizadas para assuntos pessoais e profissionais.

Então cabe ao empregador estabelecer um acordo entre seus colaboradores e também deixar claro que a navegação e utilização de ferramentas virtuais podem ser restringidas através de seu poder diretivo e regulamentar. Essas restrições podem ser estabelecidas no regulamento interno da empresa ou no contrato individual de trabalho do empregado. Essas restrições podem ser feitas através dessas determinações ou através de ferramentas que impossibilitem o acesso para fins particulares. Caso as determinações sejam desobedecidas por parte do empregado, o empregador tem o direito de penalizar o empregador dentro dos direitos legais.

No que diz respeito à fiscalização de conteúdo, ao permitir a utilização da internet para fins particulares o empregador não possui direito de fiscalizar o conteúdo dos e-mails e nem das mensagens instantâneas do empregado, se tratando assim da violação de correspondência, ferindo assim o direito de intimidade do empregado. O empregador nesse caso tem o direito de fiscalizar no âmbito eletrônico, o conteúdo em relação a vírus e pragas, tendo em vista que os riscos são evidentes. Quando se trata da utilização da internet para fins profissionais, o empregador tem total direito de fiscalizar todo conteúdo, de maneira que o colaborador nesse momento esta utilizando recursos disponibilizados pelo empregador e também sua imagem e tudo que ele executar em nome da empresa será de responsabilidade dela, ou seja, a empresa tem total direito de proteger sua imagem.

Ao utilizar um termo como fiscalização pode se ter uma primeira impressão

que ofende de certa maneira o colaborador, pois nos leva a pensar que eles sempre estão utilizando a internet para uso próprio ou de maneira irregular, mais precisamos como profissionais da atualidade analisar tudo de maneira amplamente inteligente e ter um real conhecimento dos riscos da má utilização da internet. Pois no mercado competitivo que vivenciamos, sabemos que muitos agem de má fé, aguardando uma falha para poder invadir o sistema ter acesso ao banco de dados enfim, ter acesso a tudo sobre a empresa, e utilizar esse conhecimento para seu beneficio, isso é bastante preocupante.

Não podemos deixar de citar as redes sociais quando falamos em bloqueio e fiscalização dentro das empresas, sabemos que no mundo em que vivemos atualmente é impossível pensar em uma empresa que não tenha um serviço de internet disponibilizado, cabe então aos gestores estarem analisando a melhor maneira de aplicar tal bloqueio. Pois algumas optam pelo bloqueio total das redes sociais, fazendo assim que todos fiquem focados no trabalho durante todo o horário de trabalho, mais sabemos que nem todos ficarão satisfeitos com essa medida, podendo prejudicar o clima interno da empresa sem as conversas sobre as novidades e também prejudicando a atratividade da empresa.

Outra medida a ser estabelecida é aplicar uma política interna de bom senso ao acesso a internet, estando assim o acesso totalmente livre, mais sabemos que não são todos que conseguem administrar a liberdade a eles concedida, podendo assim prejudicar o rendimento desse colaborador. Mais se for analisar por um lado em que todos ficarão satisfeitos com tal liberdade no acesso, a relação interna da empresa melhorara muito e se caso a instituição for ligada a algo que necessite de criatividade todos estando contentes conseguirão criar com mais facilidade, beneficiando assim a empresa, mais tudo tem que ser claramente especificado até que ponto as redes sociais contribuem para a produtividade e em que ponto ela começa a prejudicar o andamento normal da empresa.

As empresas podem também aplicar um acordo com os colaboradores, especificando os horários em que as redes sociais estarão disponíveis para acesso, por exemplo, antes do inicio do expediente, durante o almoço e depois do expediente, muitos acolherão a idéia. Visto que essa estratégia assim como as outras também não traz consigo apenas benefícios, claro que os funcionários estarão mais focados durante o horário de trabalho mais eles passaram a ficar mais tempo dentro das instituições, prolongando assim sua carga horária. Cabe então a

empresa deixa bem claro que eles só receberão pelas horas trabalhadas e não pelo tempo que ficaram a mais pra ter acesso às redes sociais resolvendo assuntos particulares.

Uma estratégia bastante utilizada também que tem dado certo é estabelecer horários durante o expediente em que o acesso é permitido, propiciando assim ao colaborador que ele se programe, mantendo o foco no serviço, pois sabe que terá acesso livre durante algum período para tratar questões pessoais. Assim como as demais opções, tudo deve ser monitorado, pois nem todos agirão de maneira coerente ao estabelecido. A responsabilidade de determinar esses horários fica para a área de TI da empresa, que devera tratar o assunto de maneira seria.

São diversas as opções que um supervisor de TI tem para poder resolver o problema de acesso a internet, mais cabe a ele analisar o perfil de sua equipe e aplicar o melhor método para o controle do acesso. Sabendo que as consequências do mau uso da ferramenta serão também dele.

O problema de controle de acesso é um problema mundial, por isso a grande necessidade de conhecer sobre o assunto e de dar a real importância a ele. Em uma pesquisa realizada.

Segundo o documento "*Internet Filtering Alternatives White Paper*" (*SOFTWARE*, 2003), que mostra os índices de abuso da internet é possível observar que:

- ✓ Acessos a sites com assuntos relacionados a sexo foram de 62%;
- ✓ Acesso à internet durante o horário de trabalho gera cerca de 30 a 40% de queda na produtividade;
- ✓ 32,6% dos colaboradores não tem um objetivo específico quando acessam a internet;
- ✓ Um em cada cinco homens e uma em cada oito mulheres admitem que usam como principal equipamento para acessar conteúdos relacionados a sexo, os computadores do serviço;
- ✓ Cerca de 70% de todo tráfego pornográfico na internet é realizado entre 9:00 e 17:00, ou seja, durante o horário que deveriam estar trabalhando e utilizando a internet para beneficiar a empresa.

2.2 – FILTRO DE CONTEÚDO

O serviço de *Proxy* funciona como o esperado na sua utilização, atendendo as necessidades para as quais foi criado, por exemplo, intermedia requisições entre clientes e os servidores de destino além de controlar o acesso através de listas através de filtros, visando bloquear o acesso a sites determinados pela empresa.

Porém a proibição ao acesso a determinados sites não pode ser implementado somente através dos proxies, é necessário a utilização de filtros de conteúdos, que são ferramentas que auxiliam no controle de acesso. Essas ferramentas por sua vez tem a função de percorrer cada pagina antes de disponibilizá-la, analisando todo o conteúdo, verificando termos, palavras, frases relacionadas a base de dados que é considerada irregular.

A maioria dessas aplicações oferece ao administrador condições onde ele poderá estabelecer tudo o que irá conter nessas listas, o que será considerado indevido no acesso, e também permite a ele acrescentar e retirar qualquer termo do filtro de conteúdo.

Filtros de Conteúdo são implementados principalmente para:

- ✓ Impedir que o usuário ao acessar uma pagina contraia *malwares* (vírus, cavalo de tróia, *worms*) para a rede interna da empresa.
- ✓ Impedir que o usuário perca tempo e produtividade passando horas em redes sociais ou em bate papos.
- ✓ Impedir acesso a determinados sites como os de pornografia.
- ✓ Garantir que um usuário não utilize toda a banda de internet sozinho.
- ✓ Impedir que o usuário acesse sites de *phishing*.

3 – CONHECENDO AS FERRAMENTAS

Neste capítulo mostraremos a configuração das ferramentas utilizadas, definindo e detalhando o funcionamento de cada uma delas, com o objetivo de, efetivamente, controlar o acesso a Internet dos usuários da rede corporativa.

3.1 – SQUID

3.1.1 – DEFINIÇÃO

O *Squid* surgiu de um projeto de servidor HTTP que também incluía *Proxy* e *Cache* em meados dos anos 90. Tendo sido desenvolvido pelo Internet *Research Task Force Group on Resource Discovery* (IRTF-RD) através do projeto *Harvest*. E, atualmente, vem sendo melhorado por um grupo considerável de desenvolvedores, foi escrito originalmente para rodar em sistema operacional tipo Unix, mas ele também funciona em sistemas Windows desde sua versão 2.6.*STABLE4*.

É uma ferramenta que aceita requisições HTTPS e HTTP de usuários e capaz de efetuar requisições FTP, HTTP e Gopher para servidores, além do poder de implantar várias outras características úteis em ambientes empresariais:

- ✓ Controle de banda (velocidade) no acesso à rede local e Internet;
- ✓ Redução do consumo da Internet no carregamento de páginas;
- ✓ Relatórios e estatísticas do tráfego na Internet proveniente da rede;
- ✓ Bloqueio de sites com conteúdo inapropriado;
- ✓ Proteção de máquinas internas de acessos externos uma vez que as requisições a sites externos são efetuadas pelo *Proxy*.

3.1.2 – FUNCIONAMENTO

O *Squid* foi desenvolvido com uma característica de portabilidade, sendo assim ele roda nos principais sistemas operacionais Unix, como: Linux, BSD/OS, FreeBSD, NetBSD, OpenBSD, Solaris, HP-UX, OSF/DUNIX/TRU-64, Mac OS/X, IRIX e AIX, além de funcionar em ambientes Microsoft *Windows*.

Para se implantar o *Squid* os requisitos de equipamentos ou *hardware* necessários são modestos. A memória é o principal recurso, pois pouca quantidade de memória condena consideravelmente o desempenho. Espaço em disco é um outro fator muito importante, pois mais espaço em disco significa mais objetos no *cache* e, portanto, menores tempos de resposta.

Sendo um *Proxy* o *Squid* pode intervir as transações entre usuários e servidores. Ele aceita requisições de usuários, processa e as encaminha ao servidor desejado. Estas requisições podem ser registradas, rejeitadas e modificadas antes do encaminhamento.

Se tratando também como c*ache*, a ferramenta armazena em disco local o conteúdo de páginas acessadas freqüentemente com o objetivo de reutilizá-las, aumentando assim a performance e a diminuição do tempo de resposta.

As ACL's - (*Access Control Lists*) ou listas de controle de acesso, tornam o *Squid* eficiente e flexível. É através delas que se podem criar regras para controlar o acesso à Internet das mais diferentes formas. Praticamente todo o processo de controle do *Squid* é feito com o seu uso.

A configuração das listas de controle de acesso é a princiapl parte de um servidor *proxy Squid*, as ACL's bem definidas podem trazer um alto nível de segurança para a rede. Entretanto se mal defindas podem ter o resultado oposto, já que além da falsa sensação de segurança não será aproveitada a principal funcionalidade do Squid.

As ACL's são definidas da seguinte forma:

acl nome tipo string | "arquivo"

onde:

- ✓ acl é a palavra identificadora de uma acl;
- ✓ nome é o identificador para cada acl;
- ✓ tipo é a funcionalidade da acl;
- ✓ string é um conjunto de palavras que farão parte do grupo definido pela acl;
- ✓ arquivo é o endereço de um arquivo que conterá as palavras que farão parte do grupo definido pela acl.

Existem vários tipos de ACL que podem ser utilizadas. Detalharemos aqui as principais e suas funções.

src – tem a função de indicar endereços IP de origem. Podendo ser um endereço de rede, um endereço de *host*, ou uma faixa de endereços;

dst - semelhante ao **src**, mas está relacionada ao endereço de destino;

url_regex - Percorre o endereço completo do site (URL) a procura da expressão regular especificada. Para que seja *case-insensitive* deve ser usada a opção -i. É o tipo mais comum de ACL dada a flexibilidade proporcionada pelo uso de expressões regulares;

urpath_regex - Procura a expressão regular na URL sem levar em conta o nome do servidor e o protocolo, a procura vai ser feita apenas na parte da URL após o nome do servidor, como por exemplo, na URL http://www.acbinfo.net/netsystem/sexo.html a procura será realizada apenas na parte /netsystem/sexo.html. Ela é também *case-sensitive*, para que seja *case-insensitive* deve ser usada a opção -i;

port - Realiza o controle pela porta de destino do servidor, neste tipo deve ser especificado o número da porta;

proto - Serve para especificar o protocolo, como por exemplo FTP ou HTTP;

method - Especifica o tipo de método usado na requisição, como por exemplo GET, CONNECT ou POST;

proxy_auth - Tipo usado para implementar autenticação de usuários no *Proxy*. Neste trabalho não utilizaremos nenhum tipo de autenticação de usuários

Se as ACLs do *Squid* são as listas que definem as configurações do *Squid*, os operadores HTTP_ACCESS são as relações com as ACLs, que vão resultar no bloqueio ou liberação do acesso.

Existem muitos outros operadores, no entanto, como estes são os mais importantes, apenas eles serão detalhados.

A ordenação das HTTP_ACCESS é o ponto chave para que o *Squid* funcione de modo confiável e seguro. Sua colocação de forma ilógica poderá trazer

resultados indesejados como bloqueios não necessários, e liberação de acessos inapropriados.

Para ter uma melhor compreensão da ordenação de uma HTTP_ACCESS é necessário entender seu funcionamento. Sua estrutura é:

http_access allow | deny acl1 acl2 acl3 ...

O *Squid* utiliza as regras a seguir para analisar as ACL's:

1. As regras são lidas em seqüência "de cima para baixo";
2. Se a regra for atendida não haverá a analise das demais, não havendo possibilidade de utilização de redirecionamento de uma regra para outra;
3. As ACL's são "*case sensitive*", uma simples diferença entre minúsculas e maiúsculas anulará a regra;
4. Se acontecer de nenhuma regra ser atendida, a regra geral será o inverso da última regra, assim, se nenhuma regra for atendida e a última regra for permitida (*allow*) o *Squid* procederá a um acesso negado (*deny*) e vice versa.

Vejamos, a seguir, um pequeno exemplo:

Supondo que uma empresa cuja política de acesso a internet libera o acesso aos sites das principais empresas de publicidade do país, mas impede o acesso a qualquer *site* de conteúdo pornográfico. Seu squid.conf poderia estar configurado da seguinte forma:

```
# define o arquivo que nomina os domínios das empresas de publicidade
acl publicidade url_regex –i "/etc/squid/bloqueios/publicidade.domains"

# define o arquivo que nomina os domínios pornôs bloqueados
acl porno url_regex –i "/etc/squid/bloqueios/porno.domains"

# regras de acesso
http_access deny porno
http_access allow publicidade
http_access deny all
```

3.2 – SARG

3.2.1 – DEFINIÇÃO

O SARG (*Squid Analisys Report Generator*) é um analisador de *logs* do *Squid* que informa ao administrador em um formato bem simplificado, e que pode ser personalizado, por onde os usuários navegaram.

3.2.2 – FUNCIONAMENTO

A leitura dos *logs* do *Squid* é feita por meio de um agendamento que deve ser configurado pelo administrador. Normalmente executado diariamente no mesmo horário.

Um arquivo de texto é gerado contendo informações úteis sobre a navegação na Internet durante o período encontrado no arquivo de *log*.

Um *script* é encarregado de transformar as informações dos arquivos txt em formato Web com o objetivo de facilitar a visualização dos relatórios conforme pode ser visto na ***Figura 1***.

Na visualização na Web, gráficos dos acessos também podem ser mostrados conforme ***Figura 2***.

3.2.3 – CARACTERÍSTICAS ADICIONAIS

- ✓ Disponível em várias línguas, entre elas o português;
- ✓ Pode também analisar os *logs* do *ISA Server*, *Proxy Server* da Microsoft;
- ✓ Os relatórios poder ser customizados com informações consideradas importantes como, por exemplo: sites mais visitados, sites visitados por determinado usuário, tempo de acesso de cada usuário, etc.

Squid Analysis Report Generator

Squid User Access Reports

Period: 2008Dec11-2008Dec11
User: 10.5.1.251
Sort: BYTES, reverse
User Report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME	
dl2.avgate.net	29	19.14M	93.31%	0.00%	100.00%	00:01:19	79.29K	46.44%	
www.microsoft.com	120	519.29K	2.53%	0.00%	100.00%	00:00:48	48.26K	28.27%	
notifier.avira.com	4	179.96K	0.88%	98.92%	1.08%	00:00:01	1.06K	0.62%	
db2.stb00.s-msn.com	19	136.27K	0.66%	0.00%	100.00%	00:00:02	2.74K	1.61%	
db2.stb01.s-msn.com	18	83.42K	0.41%	0.00%	100.00%	00:00:02	2.97K	1.74%	
estb.msn.com	5	80.71K	0.39%	0.00%	100.00%	00:00:00	978	0.57%	
db2.stc.s-msn.com	27	52.93K	0.26%	0.00%	100.00%	00:00:03	3.68K	2.16%	
debian.dom-sln.local	1	48.73K	0.24%	100.00%	0.00%	00:00:00	91	0.05%	
estc.msn.com	18	44.20K	0.22%	0.00%	100.00%	00:00:02	2.14K	1.26%	
db2.stj.s-msn.com	2	34.90K	0.17%	0.00%	100.00%	00:00:00	757	0.44%	
www.google.fr	8	34.05K	0.17%	46.97%	53.03%	00:00:02	2.90K	1.70%	
estj.msn.com	14	30.21K	0.15%	0.00%	100.00%	00:00:01	1.38K	0.81%	
fr.msn.com	3	23.09K	0.11%	0.00%	100.00%	00:00:00	632	0.37%	
ll.atdmt.com	1	13.48K	0.07%	0.00%	100.00%	00:00:00	172	0.10%	
error:unsupported-request-method	9	10.62K	0.05%	100.00%	0.00%	00:00:00	211	0.12%	DENIED
voiture.fr.msn.com	2	9.83K	0.05%	0.00%	100.00%	00:00:00	453	0.27%	
stj.msn.com	1	8.26K	0.04%	0.00%	100.00%	00:00:00	173	0.10%	
analytics.live.com	4	7.13K	0.03%	0.00%	100.00%	00:00:01	1.09K	0.64%	
clients1.google.com	11	5.61K	0.03%	5.45%	94.55%	00:00:03	3.32K	1.95%	
est.msn.com	5	4.62K	0.02%	0.00%	100.00%	00:00:00	604	0.35%	
msnportal.112.2o7.net	6	4.46K	0.02%	0.00%	100.00%	00:00:02	2.69K	1.58%	
go.microsoft.com	6	4.21K	0.02%	0.00%	100.00%	00:00:02	2.49K	1.46%	
xml.fr.msn.com	3	2.83K	0.01%	0.00%	100.00%	00:00:00	468	0.27%	
images.windowsmedia.com	2	2.72K	0.01%	0.00%	100.00%	00:00:00	314	0.18%	
rad.microsoft.com	1	2.66K	0.01%	0.00%	100.00%	00:00:00	292	0.17%	
beta.update.microsoft.com	6	2.64K	0.01%	33.64%	66.36%	00:00:01	1.04K	0.61%	
c.msn.com	4	2.55K	0.01%	0.00%	100.00%	00:00:00	895	0.52%	
m.webtrends.com	3	2.39K	0.01%	0.00%	100.00%	00:00:01	1.09K	0.64%	

Figura 1 - Relatório de informações de navegações

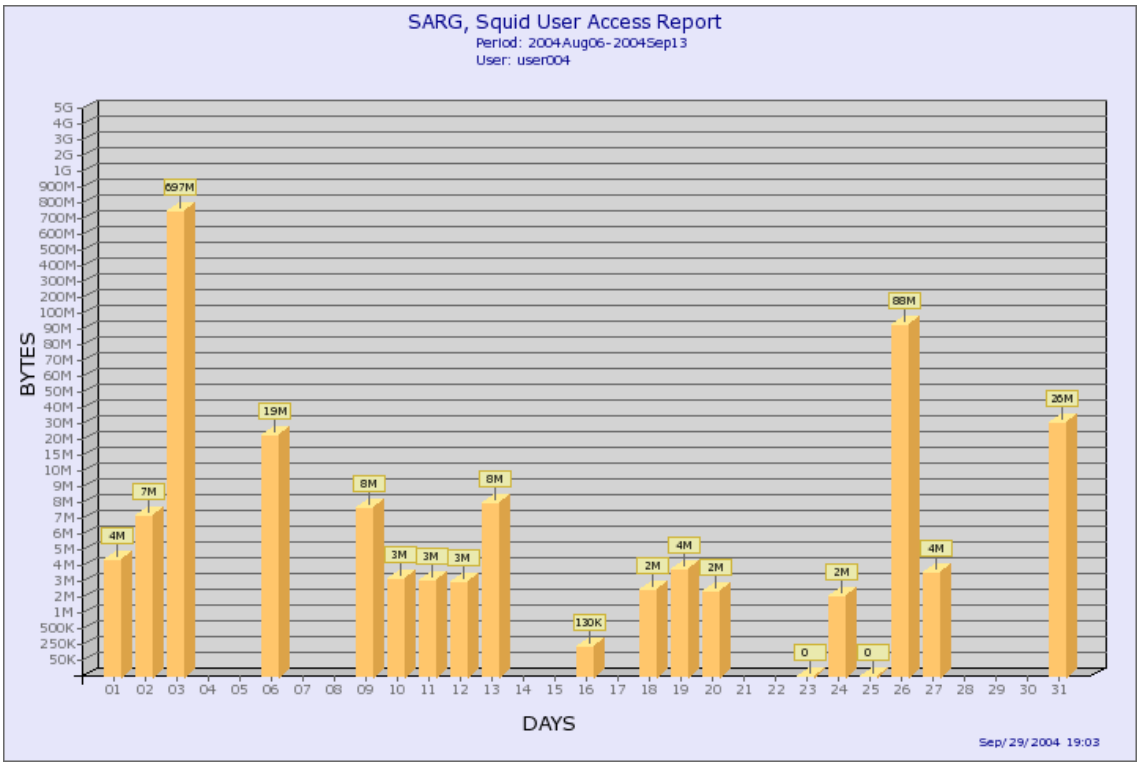


Figura 2 – Gráfico dos acessos diários

3.3 – SAMBA

3.3.1 – DEFINIÇÃO

Os ambientes de redes de computadores atualmente têm uma variedade enorme de sistemas operacionais; UNIX, Windows, FreeBSD, Linux são exemplos. Essa heterogeneidade faz os serviços de compartilhamento de arquivos e impressoras tornar-se algo complexo.

O Samba é um conjunto de aplicações *Open Source* que permitem aos usuários de sistemas operacionais *Windows* trocarem arquivos com Linux e vice-versa.

O Samba pode prover serviços tais como:

- ✓ Compartilhamento de vários sistemas de arquivos;
- ✓ Compartilhamento de impressoras;
- ✓ Visualização de estações na rede;
- ✓ Autenticação de usuários;

3.3.2 – FUNCIONAMENTO

O Samba é composto por dois programas principais: o smbd e o nmbd.

O smbd fica com a responsabilidade de prover os serviços de compartilhamento de arquivos e de impressão. Autorizando e autenticando através de dois modos: *user* e *share*. Esses dois modos são utilizados para proteger os serviços de compartilhamento e impressão através do uso de senhas. No modo *share*, uma senha é dada a qualquer usuário que possa acessar o compartilhamento. No modo *user*, a autenticação se dá por usuário através de nome de usuário e senha.

O nmbd está envolvido com o gerenciamento e a distribuição de listas de nomes NetBIOS. Este servidor entende e responde a solicitações de resolução de nomes NetBIOS sobre IP.

As ferramentas do pacote contêm outras funcionalidades úteis, tais como:

- ✓ **smbtar**, capaz de efetuar cópias de segurança de determinado compartilhamento;
- ✓ **smbpasswd**, da ao gestor da rede o poder para criar e/ou modificar senhas usadas pelo Samba;
- ✓ **smbstatus**, mostra as conexões ativas nos compartilhamentos do Samba;
- ✓ **testparm**, valida o arquivo de configuração do Samba;
- ✓ **testprns**, testa quando várias impressoras são reconhecidas pelo smbd.

4 – PROPOSTA DE IMPLEMENTAÇÃO

Este capítulo propõe uma solução para o controle de acesso à Internet em um ambiente coorporativo.

4.1 – DEFINIÇÕES DO CACHE

A seguir, serão mostradas as principais características no *Squid* para que o *cache* de páginas funcione de forma eficaz.

- **cache_mem 1500 MB**
  Informa o tamanho de 1500MB para armazenamento na memória principal (RAM).

- **maximum_object_size_in_memory 512 KB**
  Limita a 512KB o tamanho máximo de cada objeto alocado na memória principal.

- **maximum_object_size 300 MB**
  Limita a 300MB o tamanho máximo dos objetos a serem gravados na memória secundária (disco rígido).

- **minimum_object_size 0 KB**
  Informa o tamanho mínimo dos objetos a serem gravados na memória secundária.

- **cache_dir ufs /var/spool/squid 10000 16 256**
  Determina onde, tamanho e como será feito o *cache*.

- **cache_access_log /var/log/squid/access.log**
  Determina onde será gravado o *logs* do *Squid*, posteriormente usados pelo sarg.

- **cache_swap_low 80**
- **cache_swap_high 85**

  Estipulam o total de informações que o *Squid* vai trabalhar, ou seja, o diretório especificado nunca será preenchido completamente e sempre trabalhará entre 80% à 85%.

4.2 – DEFINIÇÕES DAS ACL'S

A seguir, será mostrado um conjunto de regras necessárias para que haja controle efetivo no acesso à Internet.

4.2.1 – ACL´S CRIADAS DURANTE A INSTALAÇÃO, ÚTEIS PARA REGRAS DE SEGURANÇA.

- **acl all src 0.0.0.0/0.0.0.0**

  Identifica todos os endereços IPs.

- **acl localhost src 127.0.0.1/255.255.255.255**

  Identifica o computador local, no caso o computador onde o *Proxy* está instalado.

- **acl Safe_ports port 80 81 21 443 563 70 85 210 1022 1021 1025-65535**

  Identifica as portas consideradas seguras que poderão ser acessadas pelo *Proxy*.

4.2.2 – ACL QUE IDENTIFICA A REDE EXISTENTE

- **acl RedeLocal src 192.168.10.0/255.255.255.0**

  Define o range de IPs da rede principal.

4.2.3 – ACL´S COM OS GRUPOS DE ARQUIVOS

- **acl MaqLiberadas src "/etc/squid/MaquinasLiberadas.txt"**

Define as máquinas que terão acesso irrestrito à Internet.

- **acl MaqBloqueadas src “/etc/squid/MaquinasBloqueadas.txt”**
  Define o grupo de máquinas que não terão acesso a internet.

- **acl SitesLiberados dstdomain “/etc/squid/liberados.txt”**
  Define o arquivo com os sites que não serão bloqueados.

- **acl SitesBloqueados dstdomain "/etc/squid/bloqueados.txt"**
  Define o arquivo com os sites que serão bloqueados a todas as máquinas.

- **acl SitesAdultos url_regex "/etc/squid/adultos.txt"**
  Define o arquivo com palavras que identifiquem os endereços de sites com conteúdo adulto ou inapropriado.

- **acl Negadownload urlpath_regex -i "/etc/squid/negadownload.txt”**
  Define extensões de tipos de arquivos que deverão ser bloqueados para *download*. O arquivo deverá ter a seguinte estrutura:
  \.mp3$
  \.exe$
  \.mpg$
  \.avi$

Note que a barra antes da extensão do arquivo não é parte do nome real do arquivo. Porém, a precaução é necessária, pois o ponto é identificado pelo *Squid* como um metacaracter, e a utilização da barra força sua interpretação de modo literal.

4.2.4 – ACL COM O GRUPO DE DOMÍNIO LOCAL

- **acl DominiosLocais dst 192.168.10.0/255.255.255.0**
  Define os endereços que serão acessados sem utilização do *Proxy*.

4.3 – DEFINIÇÃO DAS REGRAS DE ACESSO

A seguir, será definido o conjunto de regras de acesso que utilizarão as ACL's criadas anteriormente.

4.3.1 – REGRAS DE SEGURANÇA PADRÃO DO SQUID

- **http_access allow manager localhost**
  Permite acesso ao "*cache*" ao computador local (*Proxy*).

- **http_access deny !Safe_ports**
  Impede a utilização de portas não seguras.

4.3.2 – REGRA DE ACESSOS A SITES INTERNOS

Determina que os acessos a sites localizados na rede local não utilizem o *Proxy*.

- **always_direct allow DominiosLocais.**

4.3.3 – REGRAS DE BLOQUEIOS PRIORITÁRIAS.

São definidas antes de qualquer regra de liberação que não sejam as regras de segurança do *Squid* e a regra de redirecionamento dos sites da rede interna. São regras que não possuem exceções.

- **http_access deny !RedeLocal**
  Nega o acesso à Internet aos endereços IPs que não estão definidos na ACL "RedeLocal".

- **http_access deny MaqBloqueadas**
  Impede o acesso dos computadores cujos IPs estão definidos no arquivo "MaquinasBloqueadas.txt".

4.3.4 – REGRAS DE LIBERAÇÕES ESPECÍFICAS

Estas regras devem ser obrigatoriamente definidas após as regras de bloqueio prioritárias.

- **http_access allow MaqLiberadas**
  Libera totalmente o acesso dos computadores cujos IPs estão definidos no arquivo “MaquinasLiberadas.txt”.

- **http_acces allow SitesLiberados**
  Libera os sites que estão definidos no arquivo “liberados.txt”

4.3.5 – REGRAS GERAIS DE BLOQUEIOS

Estas são as regras de bloqueio que serão aplicadas em todos os casos que não estejam definidos anteriormente nas regras de liberação específicas. Em geral, aqui são definidas as principais regras da empresa.

- **http_acess deny SitesBloqueados**
  Bloqueia o acesso aos sites cujos endereços foram definidos no “bloqueados.txt”.

- **http_access deny SitesAdultos**
  Bloqueia o acesso aos sites cujos endereços contenham palavras listadas no arquivo “adultos.txt”.

- **http_access deny Negadownload**
  Bloqueia o download de todos os arquivos cujas extensões estejam listadas no arquivo “negadownload.txt”.

4.3.6 – REGRAS DE BLOQUEIO TOTAL

- **http_access deny all**

Bloqueia todos os outros casos não previstos anteriormente. Bloqueia qualquer acesso que não tenha sido liberado nas regras anteriores.

5 – UML - UNIFIED MODELING LANGUAGE

5.1 – LISTA DE REQUISITOS

Interesse	Motivo	Quem Solicita?	Data	Ator Responsável
Manter cadastro de computadores com acesso irrestrito	Manter atualizado os computadores com acesso irrestrito a internet	Administrador da Rede	31/05/2011	Administrador da Rede
Manter cadastro de computadores sem acesso a internet	Manter atualizado os computadores sem acesso a internet	Administrador da Rede	31/05/2011	Administrador da Rede
Manter cadastro de domínios da internet que podem ser acessados	Manter atualizado os domínios da internet que podem ser acessados	Administrador da Rede	31/05/2011	Administrador da Rede
Manter cadastro de domínios da internet que não podem ser acessados	Manter atualizado os domínios da internet que não podem ser acessados	Administrador da Rede	31/05/2011	Administrador da Rede
Manter cadastro de sites que serão bloqueados pela URL	Manter atualizado os sites que não poderão ser acessados	Administrador da Rede	31/05/2011	Administrador da Rede
Manter cadastro dos tipos de downloads que não poderão ser feitos	Manter atualizado os tipos de downloads bloqueados	Administrador da Rede	31/05/2011	Administrador da Rede

5.2 – EMBASAMENTO TEÓRICO

As técnicas orientadas a objeto permitem que o software seja construído de objetos que tenham um comportamento especifico. Os próprios objetos podem ser construídos a partir de outros, os quais, por sua vez, podem ainda ser construídos de outros. A orientação a objetos está ligada diretamente a classificação, organização e abstração de dados.

A análise de sistemas no mundo orientado a objeto é feita analisando-se os objetos e os eventos que interagem com esses objetos. O projeto de software é feito reusando-se classes de objetos existentes e quando necessário, construindo-se novas classes.

Técnicas orientadas a objeto podem ser usadas para simplificar o projeto de sistemas complexos. O sistema pode ser visualizado como uma coleção de objetos, estando cada um dos objetos em um determinado estado. Os objetos são construídos a partir de outros objetos.

A análise e o projeto orientados a objeto modelam o mundo em termos de objetos que tem propriedades e comportamentos e eventos que disparam operações que mudam o estado dos objetos. Os objetos interagem com outros objetos.

A modelagem e o projeto orientados a objeto são os paradigmas que devem integrar todas as ferramentas e técnicas poderosas para a criação de software. Estratégia de desenvolvimento baseada no conceito de que o sistema deve ser construído a partir de componentes reutilizáveis, chamados de objetos.

A UML (Unified Modeling Language ou Linguagem de modelagem Unificada) é uma linguagem visual utilizada para modelar sistemas computacionais por meio do paradigma de Orientação a Objetos.

Nos últimos anos essa linguagem tornou-se uma linguagem padrão para desenvolvimento de software adotado internacionalmente pela indústria de Engenharia de software.

Mas é preciso deixar bem claro que a UML não é uma linguagem de programação e sim uma linguagem de modelagem, que auxilia os engenheiros de software, tais como seus requisitos, comportamentos, sua estrutura lógica e outros.

A UML surgiu com a união de três métodos de modelagem, o método Booch, OMT e o OOSE, que eram uma linguagem de modelagem de dados

orientada a objetos mais populares na década de noventa.

É importante ressaltar a importância de que todo sistema deve ser modelado antes de sua implementação, porque os sistemas de informação frequentemente costumar possuir a propriedade de “crescer”, isto é, aumentar em tamanho, complexidade e abrangência. Porque na verdade é como se eles nunca estivessem finalizados, por serem dinâmicos.

Para estar modelando esses sistemas a UML disponibiliza de várias ferramentas como:

Levantamento e analise de requisitos, é uma das primeiras etapas de engenharia de um software, na qual é a principal etapa da modelagem. Pois é nessa etapa em que o engenheiro de software vai compreender as necessidades do usuário, ou seja, aquilo que ele espera que o sistema realize. Levantamento esse que acontece através de entrevistas onde o engenheiro irá compreender o sistema informatizado em uso e o que o novo software irá fornecer.

Para uma melhor representação do que esta sendo desenvolvido a UML utiliza uma serie de diagramas no qual estaremos apresentando agora.

Após a o levantamento de requisitos e possível utilizar demais ferramentas que irão auxiliar na documentação do software.

Diagrama de caso de uso é o diagrama mais geral e informal da UML, pois ele utilizado normalmente na fase de levantamento de requisitos mais também posteriormente para construção de novos diagramas e também para consultas. Tem a função de dar uma visão externa geral do sistema, onde apresenta um ator que representa o usuário e a função, em uma elipse, a ser executada pelo software, e suas relações são ligadas por setas. Apesar de ser de fácil entendimento o diagrama de caso de uso possui varias particularidades. No geral pode se associar um caso de uso a uma tela do sistema, mais vale lembrar que ele representa melhor o negocio.

A documentação de um Caso de Uso costuma descrever, por meio de uma linguagem bastante simples, suas funções, quais atores interagem com o mesmo, quais etapas devem ser executadas pelo ator e pelo sistema para que a função seja executada. Mas não existe nenhum formato especifico para a documentação do caso de uso. Mas recomenda-se optar por algo que seja de fácil entendimento que um usuário leigo possa entender.

Diagrama de Classes é com certeza, o mais importante e o mais utilizado da

UML. Porque sua principal função é estar demonstrando as classes que estarão compondo o sistema com seus respectivos atributos e métodos, como elas se relacionam, transmitem informações entre si. Este diagrama mostra uma visão estática de como as classes estão organizadas, dando atenção a como definir a estrutura lógica das mesmas. E também esse diagrama servirá de bases para a construção dos demais diagramas da UML.

Na verdade esse o diagrama de classe é uma evolução do modelo entidade relacionamento para as classes persistentes.

As classes são compostas por atributos que armazenam os objetos da classe, além de métodos que são as funções que cada função pode executar. Os valores dos atributos podem variar de uma instancia para outra. Devido a essa característica é possível identificar cada objeto individualmente.

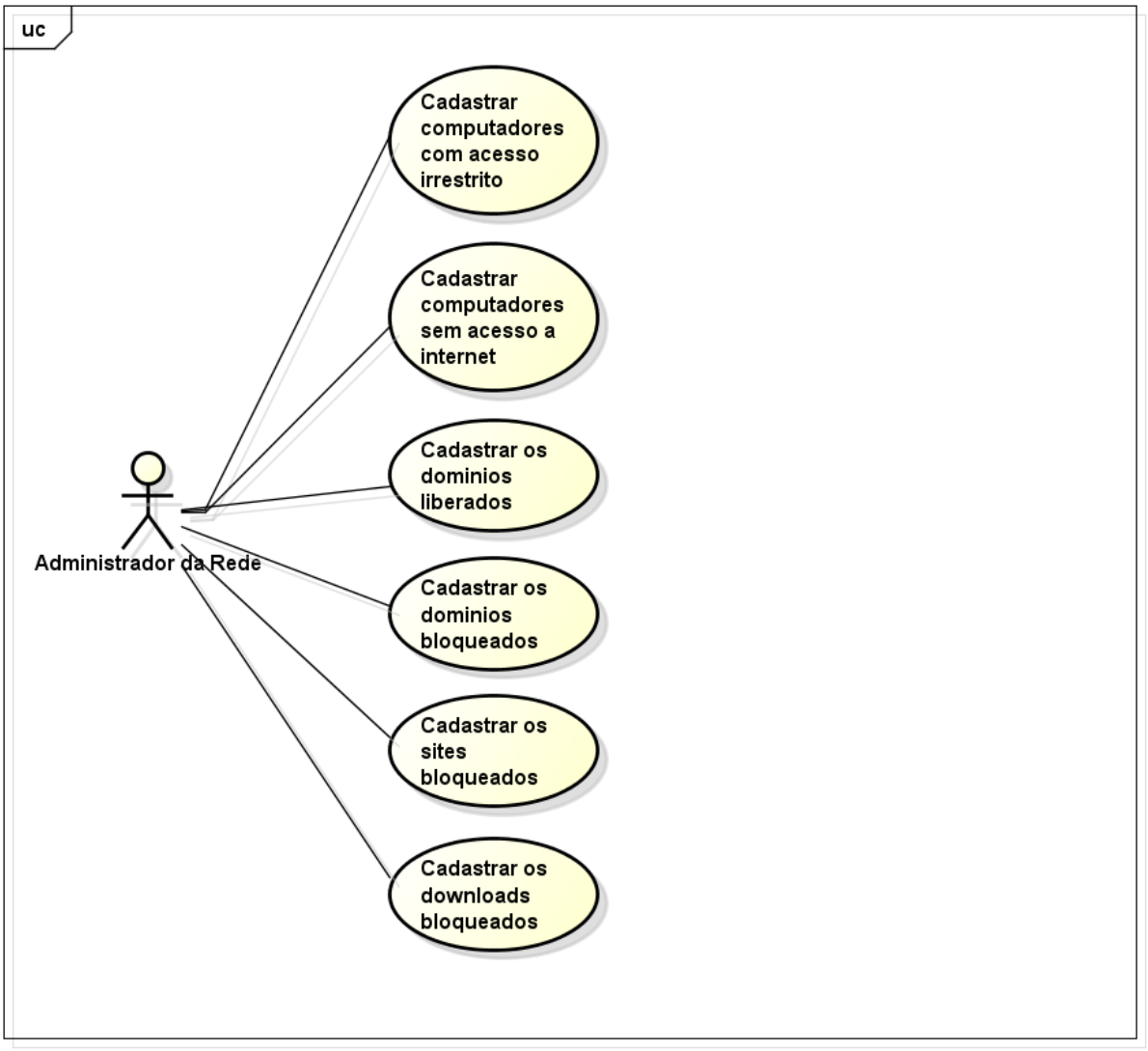
As classes têm relacionamentos entre si para compartilharem informações e colaborarem umas com as outras para permitir a execução dados diversos processos executados pelo sistema. Para fazer estes relacionamentos são utilizados vários meios como associação, agregação, composição, especialização, generalização dependência e outros.

Seguindo, o diagrama de objetos é como um complemento do diagrama de classes. Seu objetivo é fornecer uma visão dos valores armazenados pelos objetos das classes definidos no diagrama de classes.

Diagrama de sequência, este diagrama procura determinar a sequência de eventos que ocorrem em um determinado processo, ou, seja, quais condições devem ser satisfeitas e quais métodos devem ser disparados entre os objetos envolvidos e em que ordem durante um processo específico. Esse diagrama baseia-se no diagrama de caso de uso. No entanto, deve-se ter em mente que o fato de haver normalmente um único diagrama de casos de uso não significa em absoluto que haverá um único diagrama de sequência.

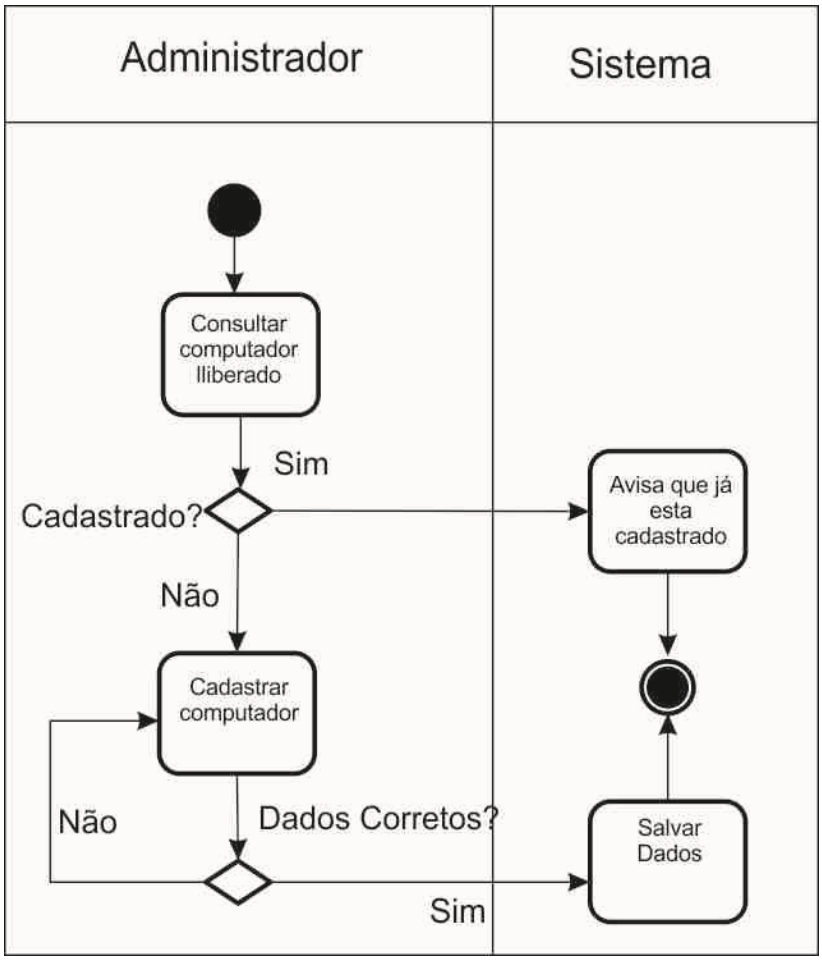
O diagrama de atividades preocupa-se em descrever os passos a serem percorridos para a conclusão de um método ou algoritmo específico e não de um processo complexo como e a do diagrama de sequência, por exemplo. Este diagrama define passos como estado inicial, estado final, transições e outros.

5.3 – DIAGRAMA DE CASO DE USO DE SOFTWARE

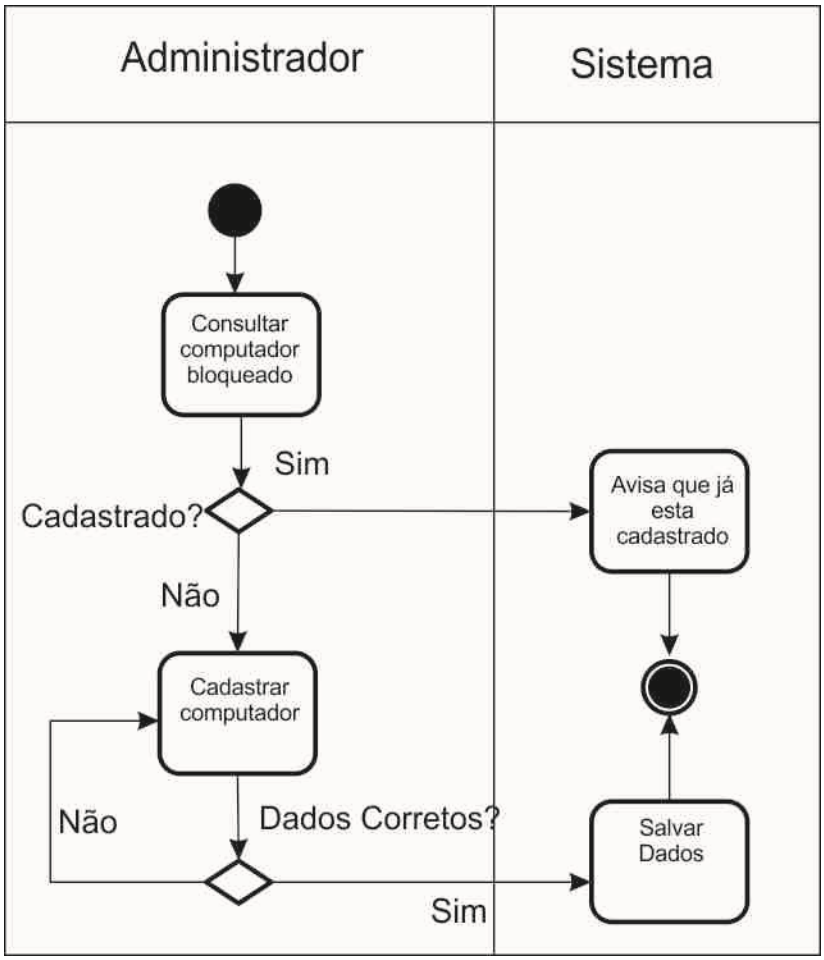


5.4 - DIAGRAMA DE ATIVIDADE

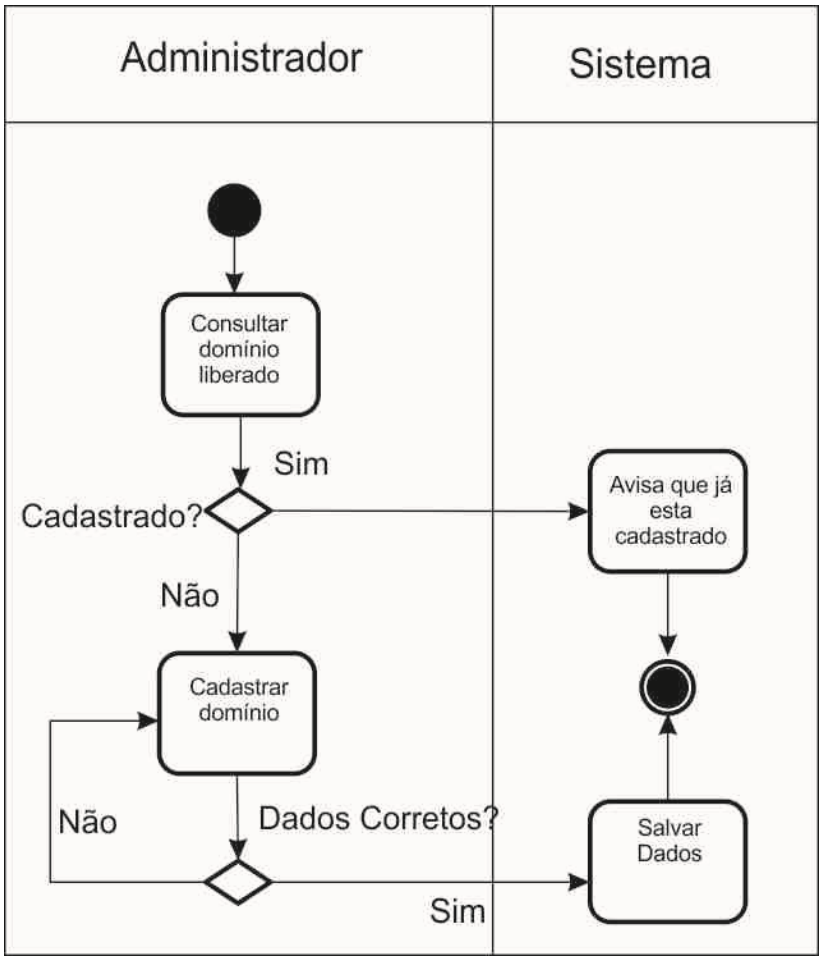
5.4.1 – CADASTRAR COMPUTADORES LIBERADOS



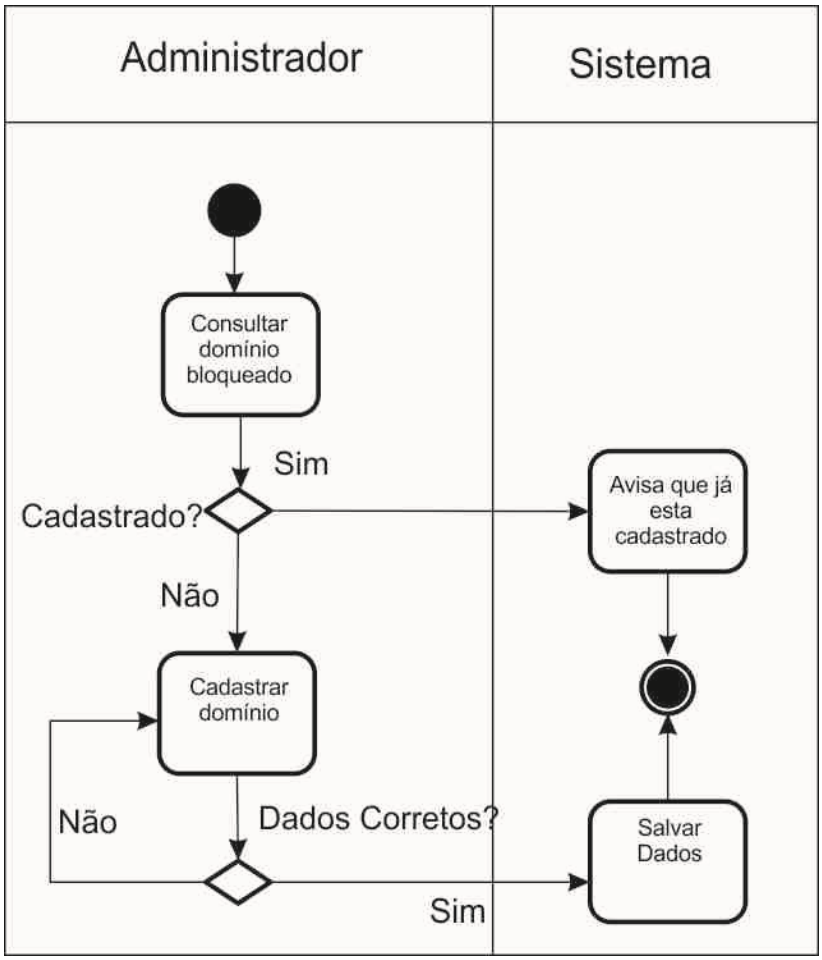
5.4.2 – CADASTRAR COMPUTADORES BLOQUEADOS



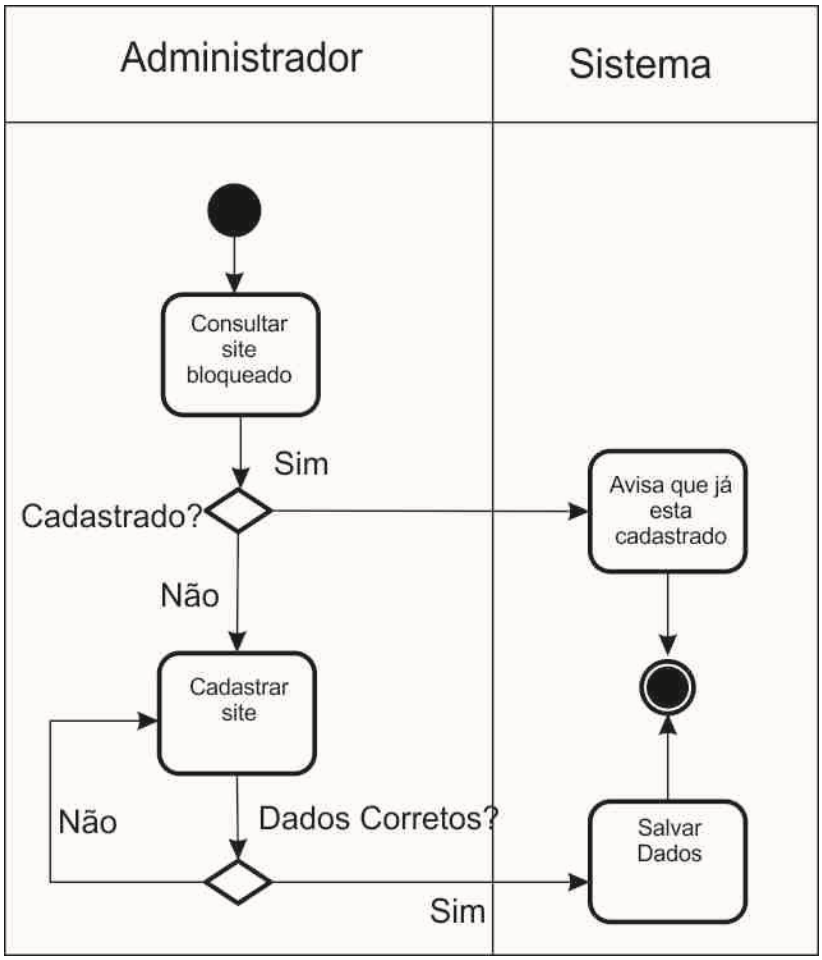
5.4.3 – CADASTRAR DOMÍNIOS LIBERADOS



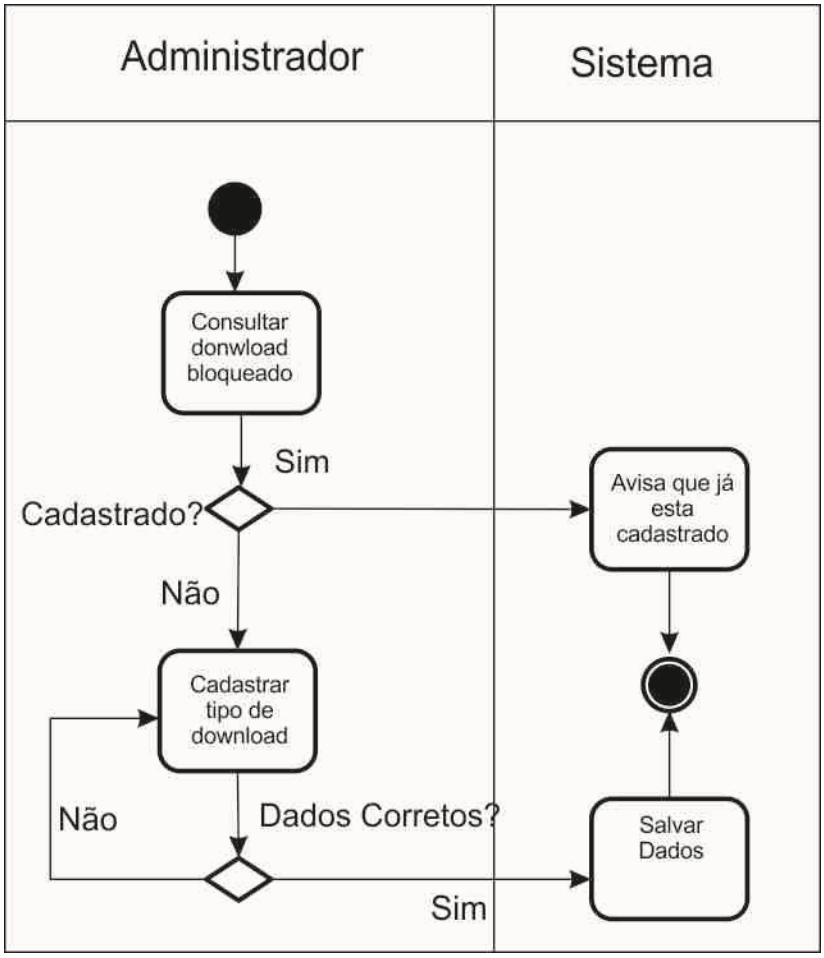
5.4.4 – CADASTRAR DOMÍNIOS BLOQUEADOS



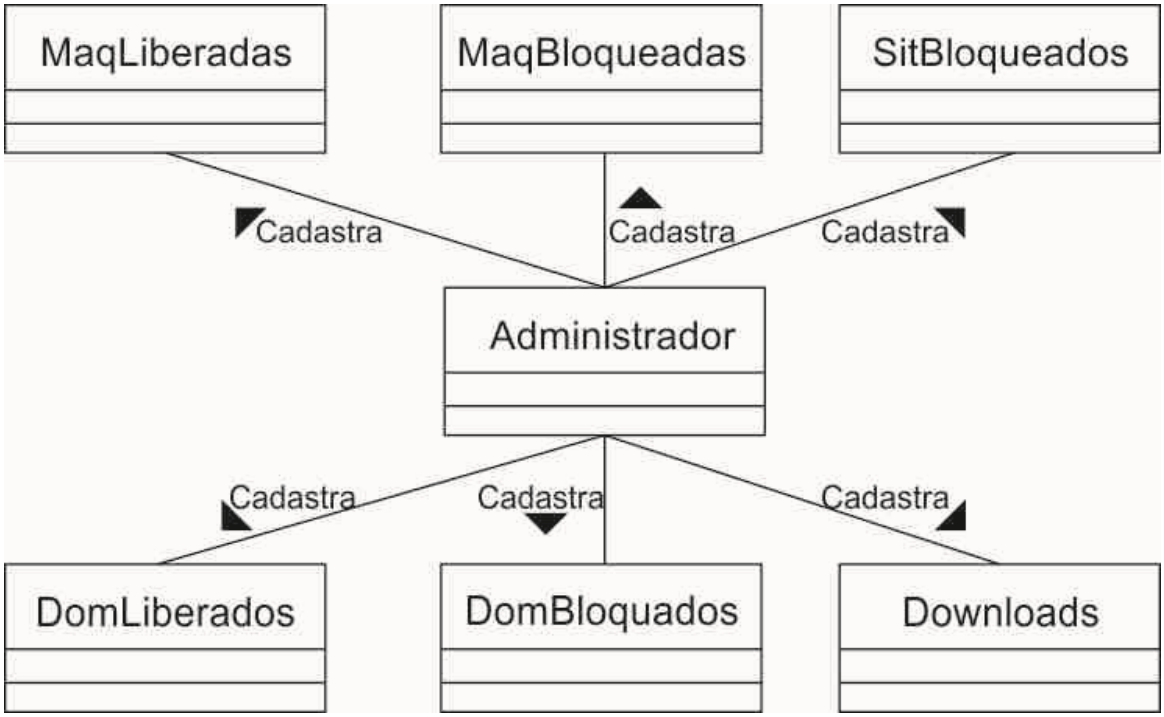
5.4.5 – CADASTRAR SITES BLOQUEADOS



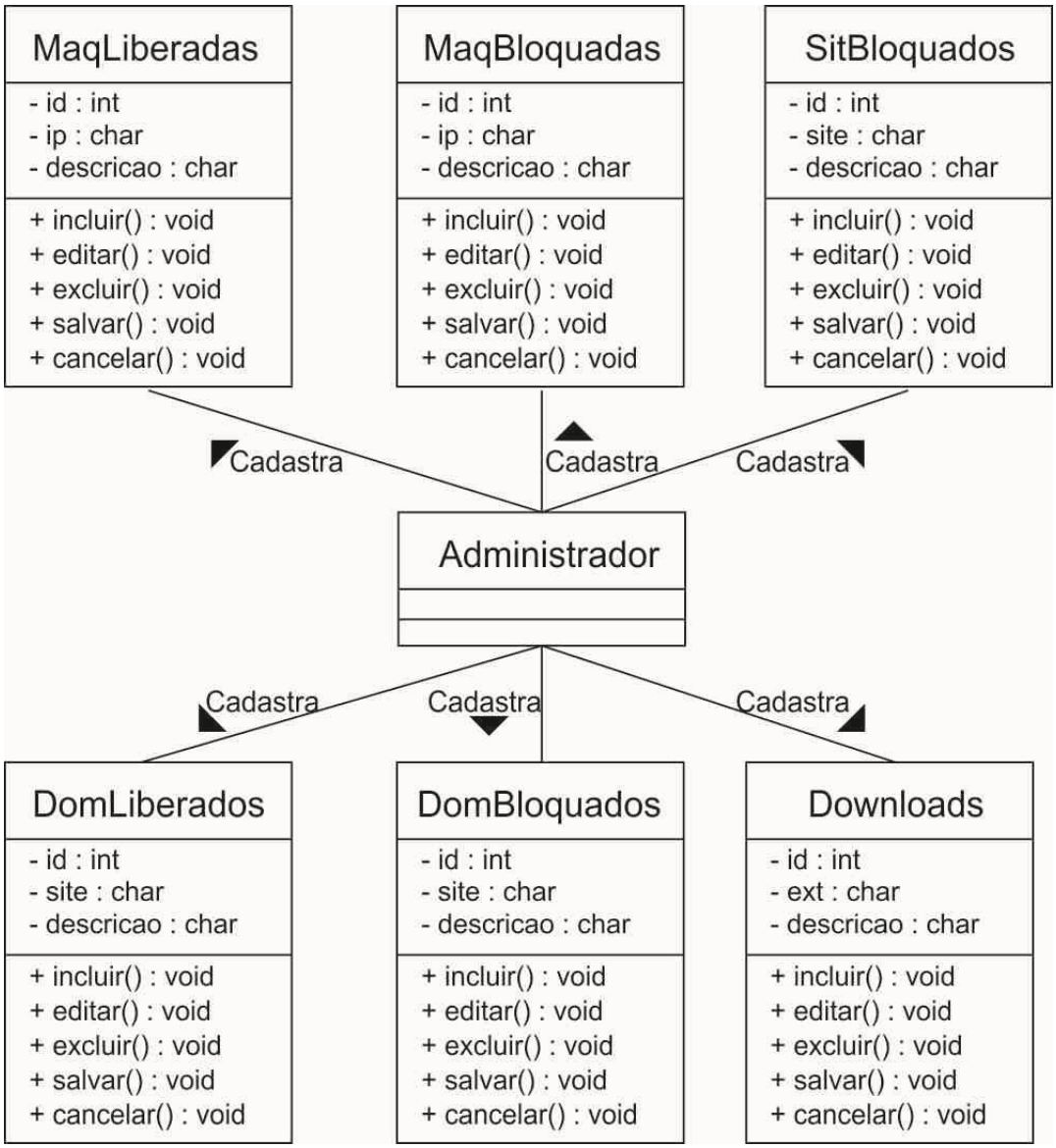
5.4.6 – CADASTRAR DOWNLOADS BLOQUEADOS



5.5 – MODELO DE DOMÍNIO



5.6 – DIAGRAMA DE CLASSE



6 – FERRAMENTAS UTILIZADAS PARA DESENVOLVIMENTO DO SISNET

6.1 – ASTAH PROFISSIONAL

Versão completa da ferramenta de modelagem UML, desenvolvida pela empresa Change Vision. Intuitiva e fácil de usar, permite ao desenvolvedor elaborar modelos dos vários diagramas da UML.

6.2 – MICROSOFT ACESS

Sistema de gerenciamento de banco de dados da Microsoft, incluído no pacote do *Microsoft Office* Professional, que combina o *Microsoft Jet Database Engine* com uma interface gráfica do utilizador (*graphical user interface*). Ele permite o desenvolvimento rápido de aplicações que envolvem tanto a modelagem e estrutura de dados como também a interface a ser utilizada pelos usuários.

6.3 – DELPHI

O Delphi é muito utilizado no desenvolvimento de aplicações desktop, aplicações multicamadas e cliente/servidor, compatível com os bancos de dados mais conhecidos do mercado. O Delphi pode ser utilizado para diversos tipos de desenvolvimento de projeto, abrangendo desde Serviços a Aplicações Web e CTI.

7 – PROTOTIPAGEM

SisNet

7.1 – TELA DE LOGIN

Figura 3 – Tela de Login do SisNet

7.2 – MENU PRINCIPAL

Figura 4 – Tela principal do SisNet

7.3 – COMPUTADORES COM ACESSO IRRESTRITO A INTERNET

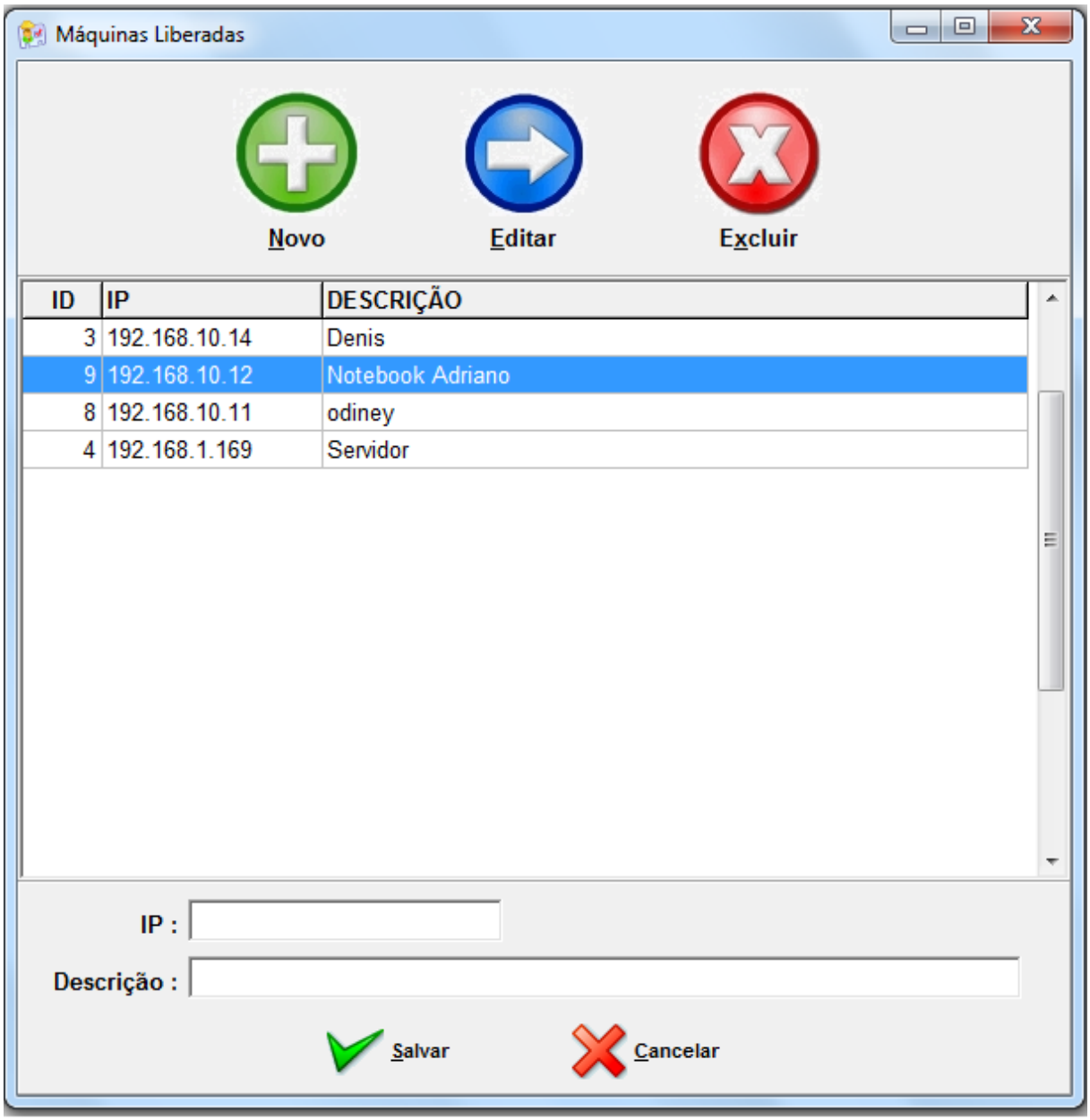


Figura 5 – Tela de cadastro dos computadores com acesso ilimitado à internet

7.4 – COMPUTADORES SEM ACESSO A INTERNET

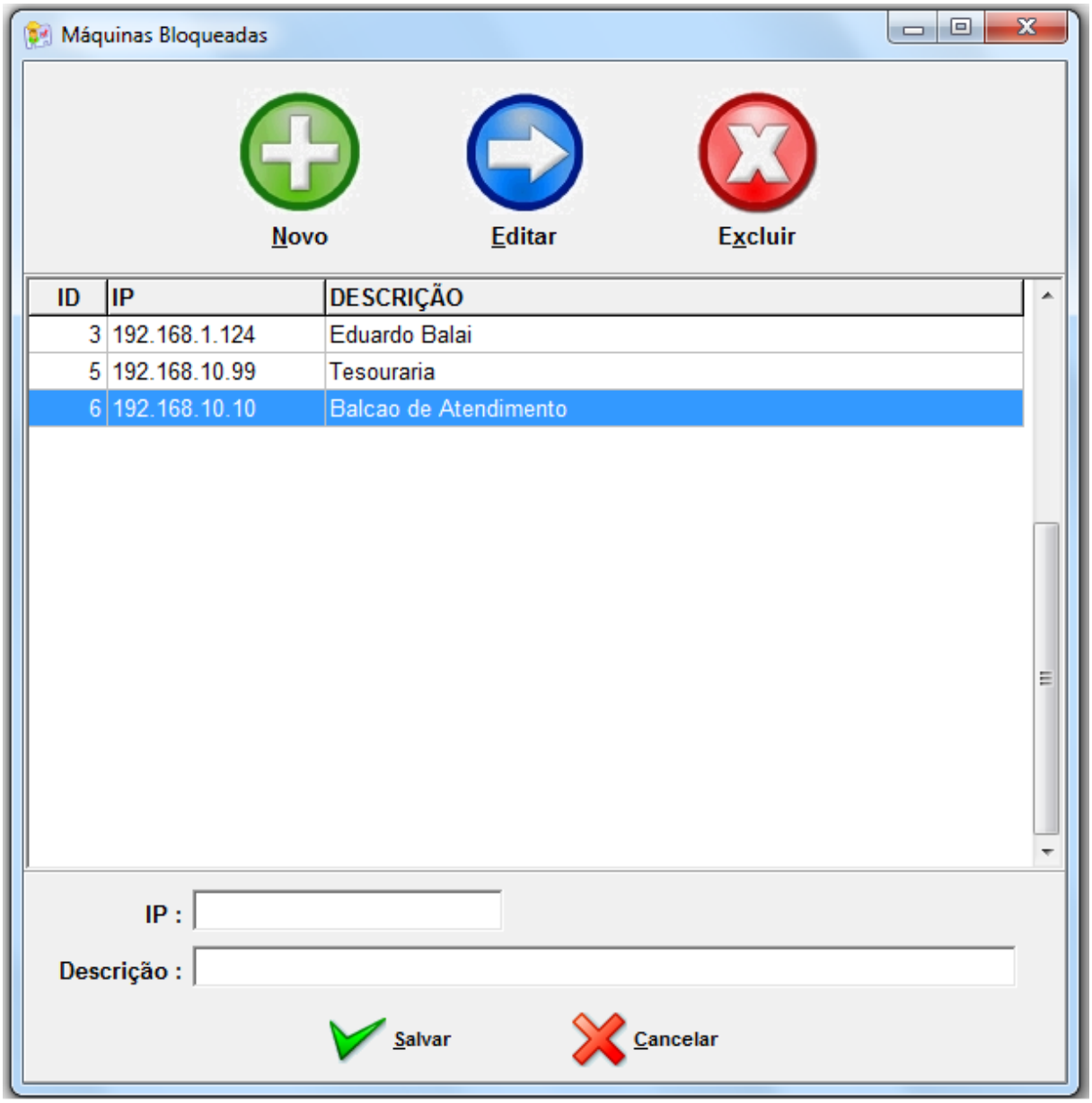


Figura 6 – Tela de cadastro dos computadores sem acesso à internet

7.5 – DOMÍNIOS LIBERADOS PARA ACESSO

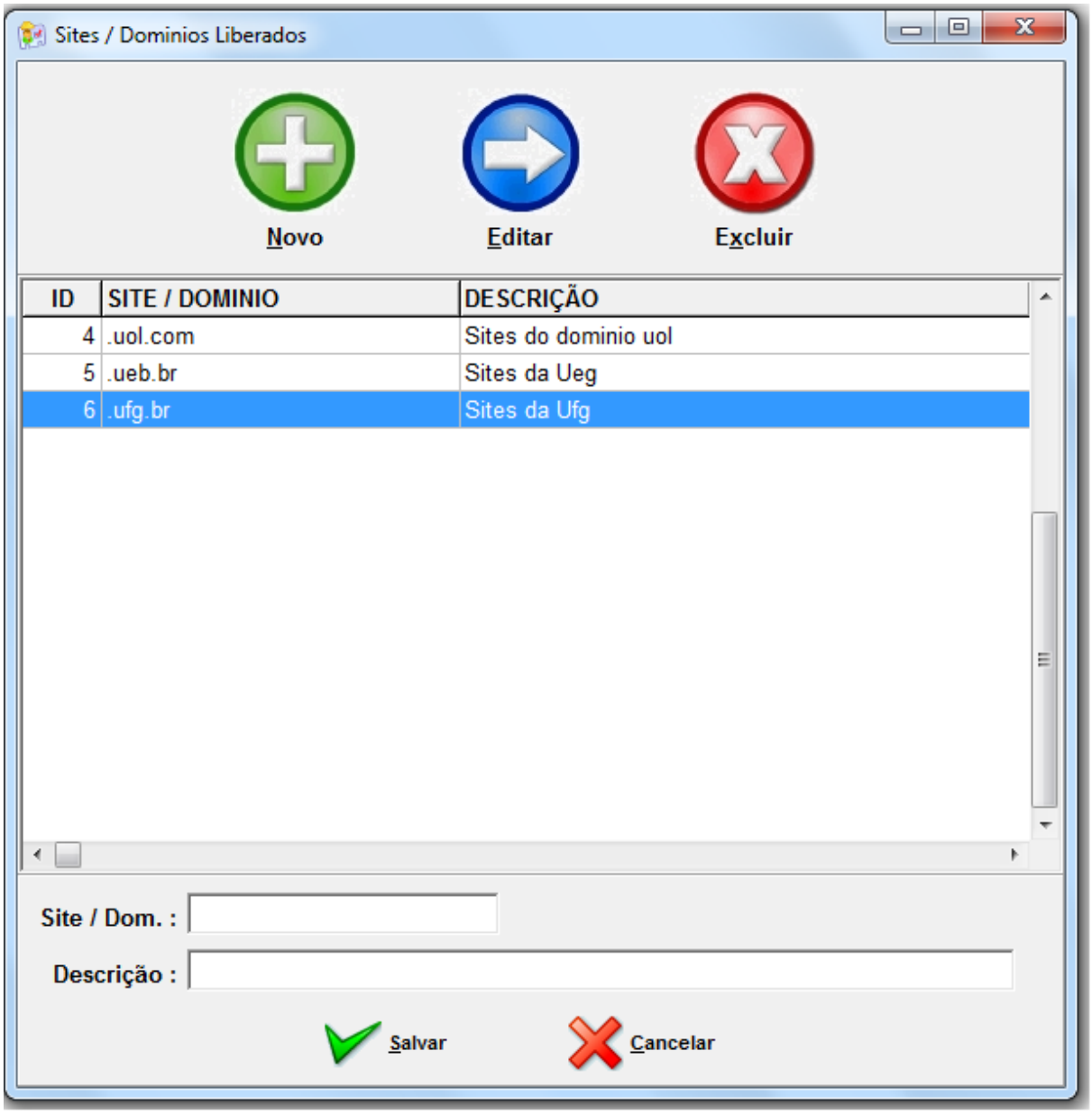


Figura 7 – Tela de cadastro dos domínios liberados para acesso

7.6 – DOMÍNIOS BLOQUEADOS

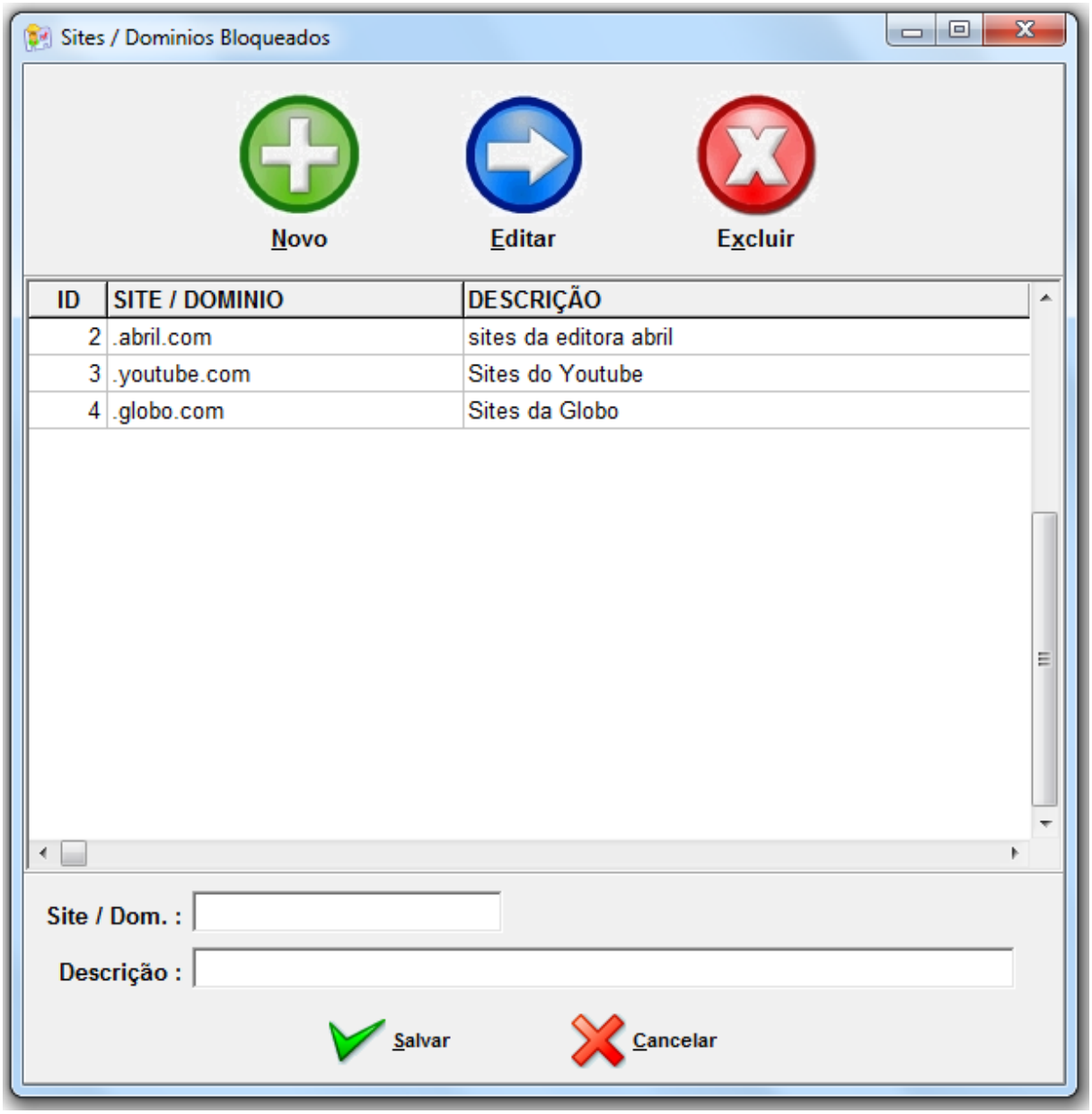


Figura 8 – Tela de cadastro dos domínios proibidos para acesso

7.7 – SITES BLOQUEADOS POR URL

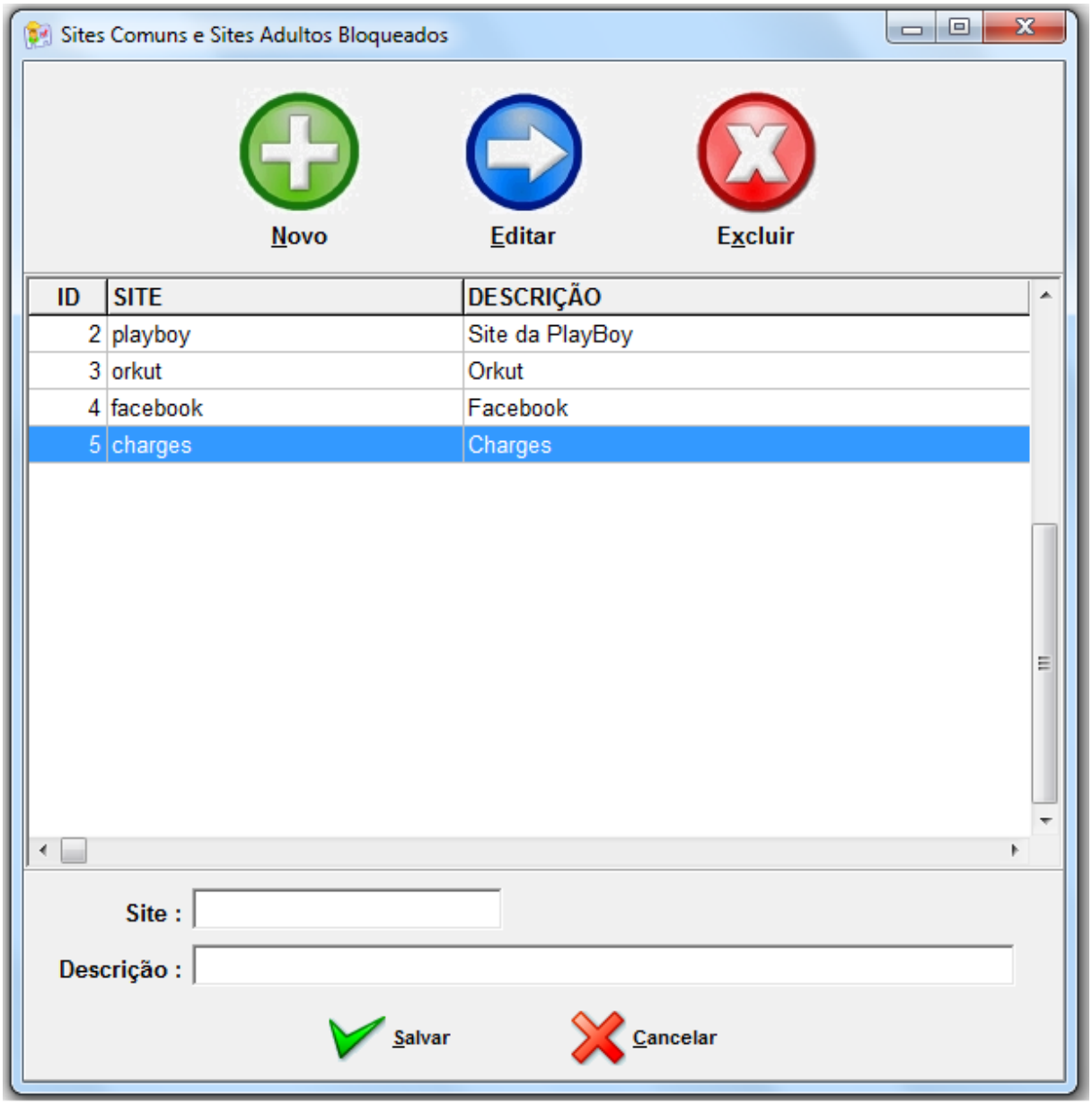


Figura 9 – Tela de cadastro dos sites bloqueados pela url

7.8 – TIPOS DE DOWNLOADS BLOQUEADOS

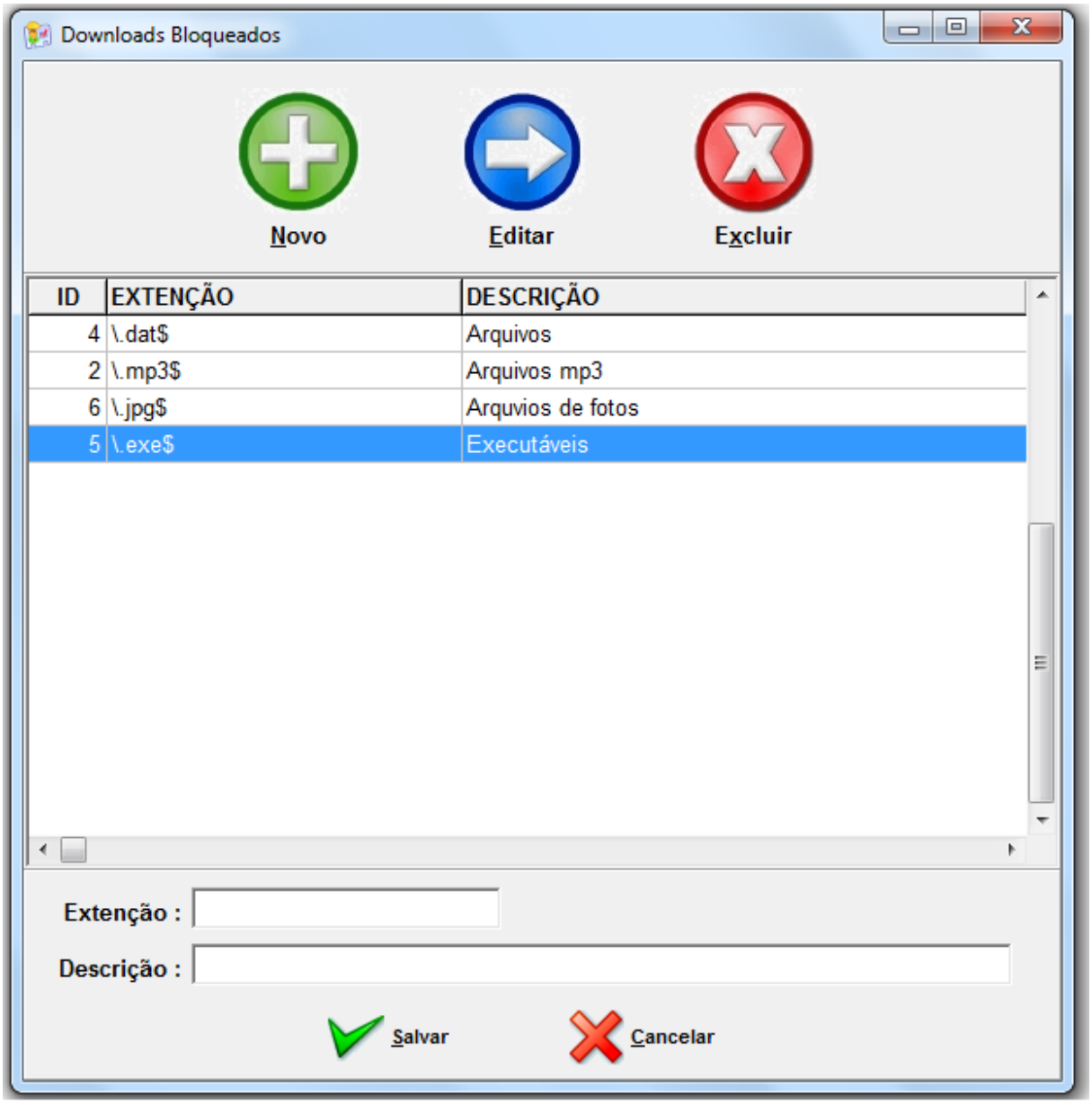


Figura 10 – Tela de cadastro dos tipos de downloads bloqueados

8 – CONSIDERAÇÕES FINAIS

O acesso constante à Internet nas empresas é um fato, entretanto, controlar esse acesso é uma tarefa que exige cuidados especiais. O controle deve ser feito por meio da definição e aplicação de políticas de seguranças. Diante disso, é necessário buscar soluções alternativas capazes de permitir o acesso à rede mundial de computadores com restrições eficazes.

Este trabalho resultou do estudo de ferramentas de *software* livre que pudessem controlar de forma eficaz o acesso à Internet. A utilização das ferramentas aqui expostas, e configuradas da forma que foi sugerida neste estudo, permitirá um controle de acesso seguro e eficiente à Internet para redes de diversos tamanhos, e com baixos custos devido à utilização exclusiva de *softwares* livres.

9 – REFERÊNCIAS BIBLIOGRÁFICAS

1. RICCI, B. **Squid – Solução Definitiva**. Editora Ciência Moderna, 2006.

2. TANEMBAUM, Andrew S. **Redes de Computadores**. 4. ed. Editora Campus, 2003.

3. CISNEIROS, H. Gerando relatórios do Squid com o SARG. 2003. **http://www.devin.com.br/eitch/sarg/**. Visitado em Agosto de 2011.

4. ORSO, P. Squid Analysis Report Generator. **http://sarg.sourceforge.net/**. Visitado em Agosto de 2011.

5. SOFTWARE, S. B. Internet Filtering Alternatives White Paper. 2003. **http://www.stbernard.com/products/docs/Internet_Filtering_Alternatives.pdf**. Visitado em Julho de 2011.

6. **http://www.cert.br/stats/incidentes/**. Visitado em Julho de 2011.