



SIMPsOn: Interface Squid para Gerenciamento de Perfis

Thales Nicolai Tavares¹, Vinícius Fülber Garcia¹, Brenda Salenave Santana¹,
Luisa Perin Lucca¹, Guilherme de Freitas Gaiardo¹, Maurício Matter Donato¹,
Nilton Camargo Batista da Silva¹, Anderson Monteiro da Rocha¹

¹NoSTRUn - Networks Technologies Research Nucleus

Universidade Federal de Santa Maria (UFSM)

av. Roraima nº 1000 – 97.105-900 – Santa Maria – RS – Brazil

{bsantana, tntavares, vfulber, llucca}@inf.ufsm.br

{ggaiardo, mdonato, nbatista, amonteiro}@inf.ufsm.br

Abstract. *Access control in computer networks is an increasingly necessary alternative and present in companies and educational institutions, after all, it becomes ideal to have tools that can manage and monitor access to the Internet, quickly and intuitively. Therefore, we present the SIMPsOn tool, which uses the Squid tool integrated to an intuitive graphical interface.*

Resumo. *O controle de acesso nas redes de computadores é uma alternativa cada vez mais necessária e presente nas empresas e instituições de ensino, afinal, torna-se ideal que se tenham ferramentas que possa gerir e monitorar o acesso à internet, de forma rápida e intuitiva. Sendo assim, apresentamos a ferramenta SIMPsOn, a qual utiliza a ferramenta Squid integrada a uma interface gráfica intuitiva.*

1. Introdução

Com o advento da Internet, o acesso à grande rede e a popularização das mesma, cada vez mais esta se apresenta como uma ferramenta de trabalho e estudo [de Oliveira et al. 2013]. No caso das empresas e instituições de ensino, cabe ao responsável pela rede fazer o controle do acesso à Internet visando a segurança da rede local, realizando possíveis bloqueios de sites indesejados, de downloads, protocolos, aplicações, entre outros [Siewert 2007].

Segundo [Kunde and Konzen 2015], uma das preocupações que deve ser abordada na política de segurança consiste no controle de acesso, ou seja, o que o usuário pode ou não estar executar na utilizando a rede. De acordo com [Yeu and Fedel 2016], os mecanismos para realizar controle não devem ser abordados pela política de segurança, mas devem ser implementados de maneira que se faça cumprir o que nela é determinado [Silva and Uchôa 2015].

Ainda, [Marcelo 2006] ressalta que o controle de acesso nas redes de computadores é uma alternativa cada vez mais necessária e presente nas empresas e instituições de ensino, afinal, segundo [Tavares et al. 2016] é fundamental que se tenham ferramentas que possa gerir e monitorar o acesso à internet, de forma rápida e intuitiva.

O Squid [Spare 2001] é um poderoso servidor de *proxy/cache* que oferece suporte para os principais sistemas operacionais baseados em UNIX, dentre eles FreeBSD,



OpenBSD, SunOS, HP-UX e AIX. O Squid é largamente utilizado para compartilhamento de acesso a WEB.

Nesse contexto apresentamos a interface SIMPsOn, o qual provê uma interface gráfica para a utilização da ferramenta Squid. Esta solução torna possível monitorar e administrar o acesso à internet tendo como meta a criação de perfis de controle individuais. De modo geral, cada perfil irá conter uma lista de sites desejados para bloqueio, que será aplicada durante um período de tempo, informada pelo criador desse perfil. Desse modo, objetiva-se a implementação de uma interface intuitiva, onde é possível criar e gerenciar seus perfis de acesso apropriados para diferentes situações, de forma a restringir o conteúdo inapropriado para determinados momentos e locais.

O restante desse artigo está organizado como se segue: a Seção 2 demonstra o funcionamento das principais ferramentas similares a proposta. A Seção 3 apresenta uma visão geral, bem como o funcionamento do sistema SIMPsOn. A Seção 4 traz os testes realizados e os resultados obtidos. Finalmente, a Seção 5 conclui o trabalho.

Para realizar a avaliação do sistema utiliza-se um cenário hipotético. Este cenário está situado na área educacional onde um professor de determinada escola necessita de um mecanismo de controle de acesso rígido para um grupo de alunos que utiliza um laboratório informatizado.

2. Trabalhos Relacionados

Esta seção apresenta os principais trabalhos correlatos que abordam o uso de Squid aliado a interfaces gráficas.

2.1. Carraro Dashboard

O Carraro DashBorad [Carraro 2011] é uma ferramenta web que tem como principal objetivo o auxílio na administração dos servidores Linux. Esta administração dos servidores pode ser vista no gerenciamento do *proxy* Squid, testes de conectividade, NMAP, DHCP, bem como de status de serviços.

Esta ferramenta foi desenvolvida em PHP, que interage com alguns *shell scripts*, e possui certa facilidade no momento da criação das regras de bloqueio para o *proxy* Squid. Entretanto, o usuário que fará uso da ferramenta deverá possuir conhecimento específico do assunto, pois, a regra e o grupo em que esta será aplicada deverão ser inseridos manualmente.

2.2. SquidGuard Manager

A ferramenta web SquidGuard Manager [Darold 2015] é desenvolvida pelo Gilles Darold e disponibilizada sob os termos *GNU General Public License*. Nela é possível configurar e gerenciar o software SquidGuard através da leitura de seu arquivo de configuração, o *squidGuard.conf*. Dentre algumas de suas funcionalidades podemos destacar a configuração de datas e horários para bloqueio de listas, redirecionamentos de URLs desejadas, criação e aplicação de filtros de controles através da utilização de listas cadastradas, gerenciamento dessas listas por meio de inclusão ou exclusão de domínios e URLs e a edição ou inserção de novas ACLs.



Por fim, após modificar qualquer configuração disponível na ferramenta, será necessário reiniciar o Squid e, para isso, é disponibilizada uma opção no menu chamada “Restart Squid”.

3. SIMPsOn

Para o desenvolvimento do SIMPsOn foram utilizadas as seguintes tecnologias: servidor de páginas web Apache, *HyperText Markup Language* (HTML), *Common Gateway Interface* (CGI), *HyperText PreProcessor* (PHP) e um banco de dados. O emprego destas tecnologias melhora a interação do usuário através de uma ferramenta visual para manipulação do arquivo de configuração *squid.conf* do servidor Squid, que é onde as políticas, grupos de usuários e regras de acesso à Internet são determinadas.

3.1. Controle de acesso

O servidor Squid foi configurado de maneira a liberar todo e qualquer acesso. Sendo assim, o controle desse acesso será feito de forma individual, tendo como base o perfil selecionado. Uma vez que determinado usuário acessar um site, este será adicionado ao arquivo de acessos do laboratório, esse registro contém o site acessado e sua categoria.

A categoria indicada é o retorno da comparação do site acessado com o conjunto de *blacklists* utilizadas pelo *proxy* Squid. Desse modo, é possível gerenciar individualmente o perfil aplicado ao laboratório, possibilitando a inclusão ou exclusão desse site para bloqueio. A Figura 1 possibilita compreender o modo como o professor poderá gerenciar seu perfil, de acordo com os bloqueios e liberações que efetuar, bem como definir *blacklists* para o laboratório selecionado. Também é possível visualizar um relatório completo dos acessos ao servidor *proxy* Squid.

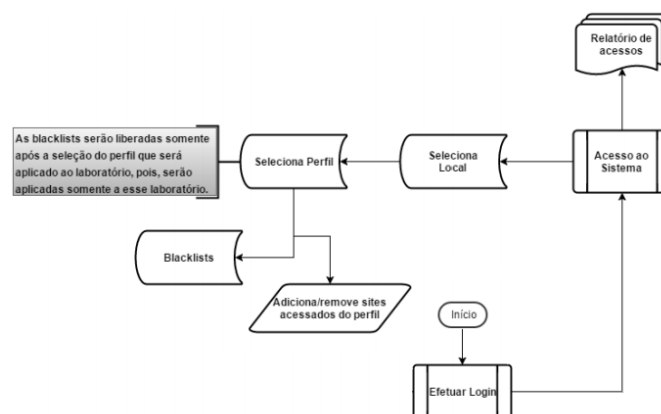


Figura 1. Fluxograma de gerenciamento de perfil

3.2. Base de dados

O sistema de banco de dados surgiu da necessidade de obter um controle mais efetivo dos dados armazenados garantindo a integridade dos mesmos. Desse modo, este sistema irá verificar os dados inseridos no banco, as ligações entre as tabelas através de chaves estrangeiras e as informações referentes aos usuários cadastrados. Na figura 2 observa-se a estrutura do banco de dados utilizado para esse trabalho.

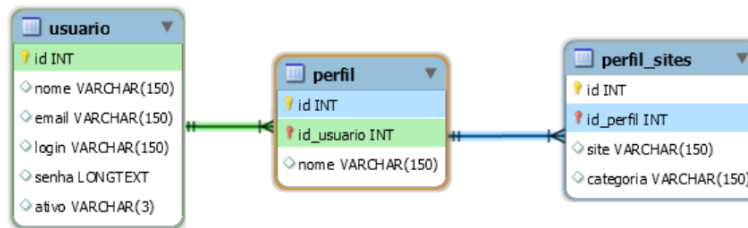


Figura 2. Estrutura do banco de dados

3.3. Interface Web do SIMPsOn

Através da interface web do SIMPsOn é possível efetuar um gerenciamento direto e efetivo do *proxy squid*, independente do nível de experiência do usuário. A interface possibilita que, no caso apresentado, o professor visualize suas ações de forma mais intuitiva através dos avisos sobre as operações efetuadas.

A primeira página visualizada é a de login conforme apresentada na Figura 3, para dispor das funcionalidades fornecidas pela interface web o professor deverá efetuar o acesso nessa página e consequentemente será redirecionado para a página inicial do sistema.

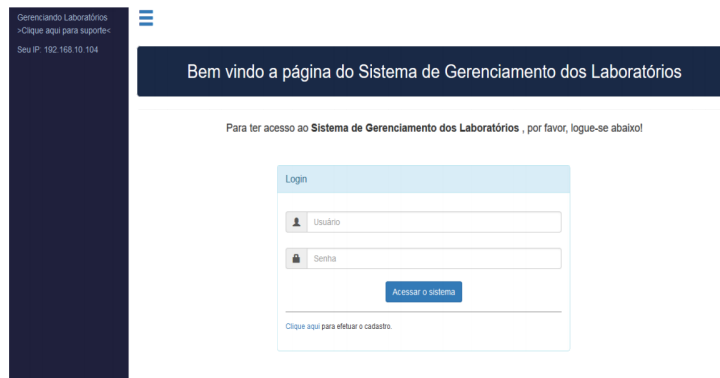


Figura 3. Tela de autenticação do usuário

A página inicial do sistema ilustrada na Figura 4 contém um breve roteiro de utilização da ferramenta web, esta informa o conteúdo existente em cada opção do menu lateral, conforme apresenta a Figura ???. O acesso à interface não necessita ser necessariamente realizadas via *desktops* ou *notebooks*, pois esta se adapta aos dispositivos que requisitarão seus serviços, tornando-se uma interface responsiva permitindo uma utilização eficiente em dispositivos móveis.

Nas opções de menu é possível verificar os laboratórios que estão disponíveis para gerenciamento. A lista de laboratórios é pré-cadastrada pelo administrador do servidor, conforme a figura 5. Cada laboratório possui um conjunto de IPs que devem ser configurados no *squidguard*, garantindo corretude nos bloqueios realizados.

Após realizada a seleção do laboratório por parte do professor, uma nova página é apresentada. Esta, por sua vez, possuirá campo para que o cadastrado um novo perfil seja

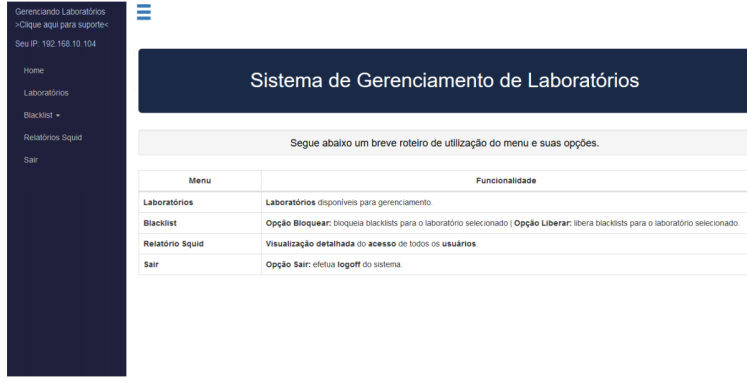


Figura 4. Página inicial



Figura 5. Lista de laboratórios

efetuado. Caso o professor possua um perfil cadastrado anteriormente, este é disponibilizado para seleção.

Ao selecionar o perfil e inserir o tempo de sua aplicação, todos os sites acessados no laboratório na data corrente são listados, conforme é possível visualizar na figura 6. O processo de bloqueio de endereços é realizado de forma direta, através de cliques para seleção e confirmação.

Após a aplicação das normas e bloqueios desejados, informações sobre os mesmos relacionados a cada perfil podem se acessados através da seleção dos mesmos. Logo a relação dos bloqueios se da pelos perfis, os perfis se relacionam diretamente aos laboratórios pode ser visualizada genericamente

Feita a seleção dos endereços e a inserção dos mesmos ao perfil aplicado, será visualizada uma informação que os sites foram bloqueados, e estes serão adicionados automaticamente para bloqueio no laboratório selecionado.

Feita a seleção dos sites e a inserção dos mesmos ao perfil aplicado, através do botão bloquear, será visualizada uma informação que os sites foram bloqueados, e estes serão adicionados automaticamente para bloqueio no laboratório selecionado.

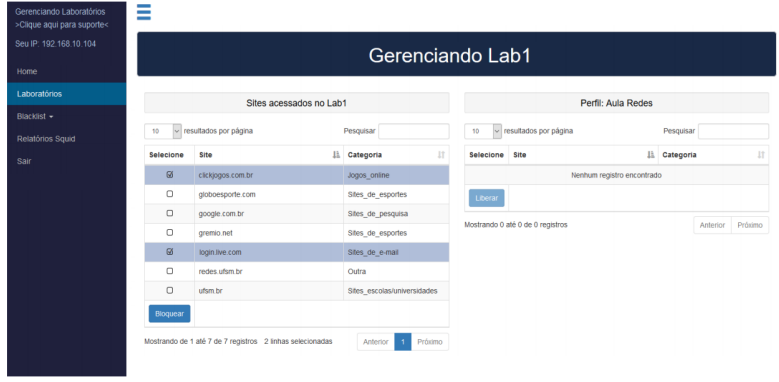


Figura 6. Lista de sites acessados

4. Avaliação e Resultados

Os testes realizados simulam um laboratório utilizado um usuário virtualizado e o mesmo efetuando acessos a internet através do *proxy*. A ferramenta web mostrou-se eficiente na interação com as configurações de grupos pré-determinadas no Squid, no bloqueio *deblacklists* para o laboratório selecionado e também o bloqueio dos sites inseridos nos perfis. Para simular um laboratório em uso foi utilizado uma máquina virtual com o sistema operacional Windows XP, e configurado seu endereço de IP no arquivo de configuração do *squidguard*, conforme a figura 7.

```

GNU nano 2.2.6 Arquivo: squidGuard.conf
src lab1 {
    ip 192.168.1.101-192.168.1.120
}

#
# DESTINATION CLASSES:
#
dest lab1bloq {
    domainlist labs/Lab1
}
  
```

Figura 7. Arquivo de configuração do squidguard

Finalizado a inserção de sites para bloqueio através da interface SIMPsOn, foi realizado a tentativa de acessar os sites inseridos no perfil de bloqueio e outros quaisquer que não estivessem inseridos. A Tabela 1 descreve os sites bloqueados e liberados para acesso.

Usuários	IP	Sites bloqueados
Computador	192.168.1.122	comcerva.com.br objetivas.com.br

Tabela 1. Permissões e bloqueios de sites

Após a tentativa de acesso do usuário a três páginas WEB, como mostra a Figura 8, uma página foi permitida (a qual não havia definição de bloqueio) e duas bloquea-

das (como definido através da ferramenta), demonstrando o funcionamento esperado das definições realizadas através da interface SIMPsOn.

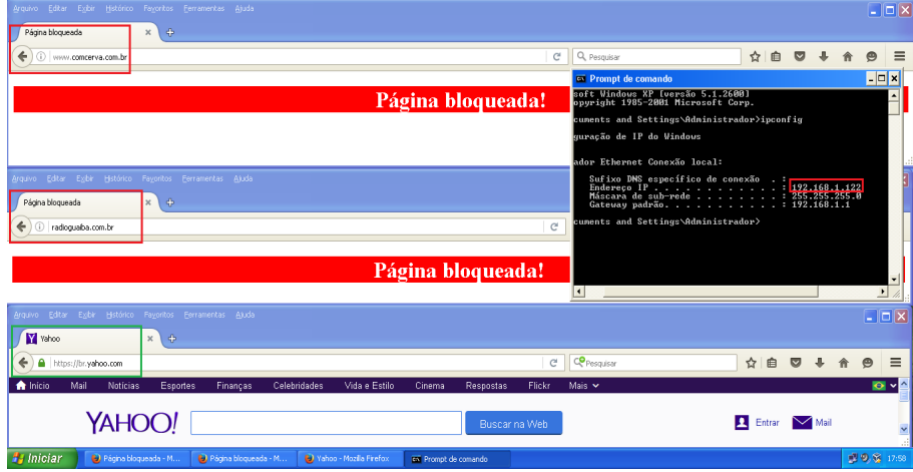


Figura 8. Acesso do usuário

Uma importante vantagem identificada nessa ferramenta web em comparação a ferramenta Carraro Dashboard é a forma como se efetua o bloqueio do acesso, o cadastro dos sites é realizado individualmente para os grupos pré-definidos ou para usuários que farão parte desse bloqueio. Em comparação a ferramenta SquidGuard Manager, a ferramenta web desenvolvida apresenta uma visão mais privilegiada e menos técnica, uma vez que a SquidGuard Manager exige uma verificação das regras configuradas e das listas aplicadas as estas, bem como uma reinicialização manual toda vez que forem alteradas, possibilitando assim, que o utilizador cometa um erro ao esquecê-la.

5. Conclusão

O crescimento e popularização das redes de computadores demandam cada vez mais controle pela parte dos administradores da mesma. Laboratórios escolares, ambientes de rede compartilhada ou locais contendo dados sensíveis devem atentar ainda mais para a segurança e a liberdade de acesso de seus usuários. Nesse contexto, SIMPsOn é uma interface para manipulação do *proxy* Squid que objetiva facilitar e tornar intuitivo o trabalho de configuração do mesmo.

A ferramenta apresentada neste trabalho obteve resultados satisfatórios considerando que atendeu ao objetivo proposto. Através de uma simulação de monitoramento e controle dos acessos em um laboratório, possibilitou-se que o usuário gerencia-se o acesso ao conteúdo, disponibilizado na internet, tendo como forma de controle de acesso a utilização de seus perfis através da interface SIMPsOn.

Como proposta para realização de trabalhos futuros encontram-se a aplicação da ferramenta em um ambiente real, como laboratórios de aulas, de modo que se obtenha uma avaliação qualitativa por parte de usuários comuns através de testes de usabilidade. Ainda, pretende-se realizar a criação de *whitelists* contendo sites que terão o acesso permitido, possibilitando a utilização de um processo de bloqueio inverso ao apresentado.



Referências

- Carraro, M. (2011). Carraro dashboard. <https://github.com/marcoscarraro/Carraro-Dashboard>.
- Darold, G. (2015). Squidguard manager. <http://squidguardmgr.darold.net/news.html>.
- de Oliveira, S. A. et al. (2013). Interface gráfica para administração de rede com software livre. *Anais SULCOMP*, 6.
- Kunde, D. O. and Konzen, M. P. (2015). Utilização de um firewall com controle de acesso no instituto federal farroupilha–campus júlio de castilhos. *Anais do EATI - Encontro Anual de Tecnologia da Informação*.
- Marcelo, A. (2006). *Squid-Configurando o Proxy para Linux (5a edição)*. Brasport.
- Siewert, V. C. (2007). Ferramenta web para administração do servidor proxy squid.
- Silva, A. M. d. and Uchôa, J. Q. (2015). Uma implementação de alta disponibilidade em firewall linux.
- Spare, I. (2001). Deploying the squid proxy server on linux. *Linux Journal*, 2001(83es):5.
- Tavares, T. N., Fischer, I. A., Duarte, F., and Preigschadt, R. (2016). Desenvolvimento de uma ferramenta para monitoramento de dispositivos em rede sem fio. *Anais do EATI - Encontro Anual de Tecnologia da Informação*.
- Yeu, Y. C. and Fedel, G. S. (2016). Aceleração no acesso à internet: estudo sobre o servidor proxy/cache squid. *Revista Tecnológica da Fatec Americana*, 2(1):23.