Utilização de um Firewall com Controle de Acesso no Instituto Federal Farroupilha – Campus Júlio de Castilhos

Diogo Otto Kunde[1], Marcos Paulo Konzen[2]

[1]Instituto Federal Farroupilha – Campus Júlio de Castilhos – RS - Brasil
Caixa Postal 38 – 98.130-000 – Júlio de Castilhos, RS – Brazil

[2]Instituto Federal Farroupilha – Campus Alegrete – RS - Brasil
Caixa Postal 118 – 97.555-000 – Alegrete, RS – Brazil
diogokunde@hotmail.com, marcos.konzen@iffarroupilha.edu.br

Abstract. *In educational institutions, the Internet has become a great ally, enabling a breaking down of barriers to access to information. However, despite the benefits it can present many risks for its users as well as the user itself can pose a risk to the system where they are connected, accessing sites with inappropriate content or committing irregularities, for example. Considering the academic environment, information security becomes essential, and for this you need to determine a way to keep the network and its users safe. The adoption of a firewall is the most widely used solution and may represent a good layer of protection*

Resumo. *Dentro das instituições de ensino, a Internet tornou-se um grande aliado, possibilitando uma quebra de barreiras para o acesso à informação. Contudo, apesar dos benefícios, ela pode apresentar diversos riscos para seus usuários, assim como o próprio usuário pode representar um risco para a rede em que está conectado, acessando sites com conteúdos impróprios ou cometendo irregularidades, por exemplo. Considerando o ambiente acadêmico, a segurança da informação se torna indispensável e, para isso é necessário determinar uma forma de manter a rede e seus usuários seguros. A adoção de um Firewall é a solução mais utilizada, podendo representar uma boa camada de proteção.*

1. Introdução

Tendo como base o ambiente extremamente dinâmico da Internet, Ponte e Vieira (2008) colocam-na como um elemento-chave para educação, onde ela funciona como uma espécie de ferramenta para igualdade entre as diferentes classes sociais, visto que a mesma informação está ao acesso de todos.

Atualmente, o acesso à Internet pelos alunos do IF-Farroupilha JC é constituído por dez Laboratórios de Informática e pelos pontos de acesso sem fio distribuídos pelo Campus, em que os alunos utilizam os seus próprios dispositivos para se conectar à Internet. Esse acesso pode ocorrer tanto através da LAN (*Local Area Network*), quanto pela WLAN (*Wireless Local Area Network)*.

Mesmo já utilizando o *pfSense* como *Firewall* para a rede acadêmica, este se mostra pouco explorado, não atendendo certos requisitos de segurança. Dentre os requisitos não atendidos, está a filtragem do tráfego indesejado, que pode ser definido como "[...] qualquer tipo de tráfego de rede não requisitado e/ou inesperado, cujo único propósito é consumir recursos computacionais da rede, desperdiçar tempo e dinheiro dos usuários e empresas [...]" (FEITOSA; SADOK; SOUTO, 2008, p. 15). Além do tráfego indesejado, existe a

falta de mecanismos de autenticação, permitindo com que qualquer pessoa que esteja ao alcance de uma das redes sem fio possa utilizá-la sem a necessidade de identificação.

Assim, espera-se resolver essas deficiências com a adição de uma camada de autenticação, através do *Captive Portal,* e da ampliação do uso de mecanismos de filtragem de conteúdo, através da utilização do *Firewall* (*pfSense*) em conjunto com o *Squid* (*proxy)* e *SquidGuard* (filtro de conteúdo).

2. Referencial Teórico

Atualmente, a Internet funciona através do Modelo de Referência TCP/IP, que é divido nas seguintes camadas: camada física, de enlace, de rede, de transporte e de aplicação. Este estudo abordará, principalmente, questões relacionadas a camada de rede, transporte e de aplicação. A camada de rede está diretamente ligada a transferência dos pacotes entre origem e destino, incluindo os protocolos de roteamento e também o IP (*Internet Protocol*). A camada de transporte permite a comunicação entre as diferentes máquinas, ou seja, faz o transporte das mensagens enviadas por elas*,* de modo que o que foi enviado pelo remetente seja entregue ao destinatário. Já a camada de aplicação contém os protocolos de níveis mais altos, atuando diretamente nas aplicações da rede, como é o caso do HTTP, FTP, etc (TANENBAUM; WETHERALL, 2011).

"A segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizados, alterações indevidas ou sua disponibilidade." (SÊMOLA, 2014, p. 41). Quando o assunto é segurança de redes de computadores, uma propriedade que pode ser destacada é a autenticação. No dia a dia, as pessoas realizam autenticação de diversas formas, reconhecendo a voz e aparência física de outras pessoas, por exemplo. No ambiente de redes, a autenticação é muito importante, pois através dela é possível gerenciar autorizações e realizar auditorias (KUROSE; ROSS, 2013).

Para controlar o tráfego de uma rede, ferramentas como *firewalls* são as aplicações mais utilizadas. *Firewall* é um conjunto de *hardware* e *software* que tem por objetivo manter uma rede interna protegida da Internet (rede externa). Ele possui três princípios básicos: todo tráfego, tanto de dentro para fora quanto de fora para dentro, da rede deve passar por ele; o tráfego autorizado é o único que poderá passar por ele sem ser bloqueado; o *Firewall* deve ser impenetrável (KUROSE; ROSS, 2013).

3. Metodologia

O presente estudo visa aplicar controles de segurança sobre a rede utilizada pelos alunos para acesso à Internet no Instituto Federal Farroupilha – Campus Júlio de Castilhos, de maneira que, além de fornecer maior segurança a eles a partir da adição de uma camada de autenticação e da filtragem de conteúdos acessados, bloqueie sites considerados impróprios. A metodologia do trabalho pode ser divida em duas fases: fase de testes e implantação.

Na fase testes foram utilizadas máquinas virtuais (VM's). As máquinas virtuais foram criadas utilizando-se *Oracle Virtualbox,* ferramenta gratuita para virtualização de sistemas. Através dela é possível simular o ambiente de rede de computadores. Utilizando um ambiente virtual é possível realizar modificações e experimentos que não seriam possíveis em ambiente real, pois comprometeria o funcionamento da rede, prejudicando a conectividade dos usuários. Nesse ambiente (Figura 1) foram criadas duas máquinas virtuais com a função de servidor, um *firewall* (*gateway*) e um servidor *Radius* (que também será como servidor *web*), além de uma máquina para simular as ações do usuário.

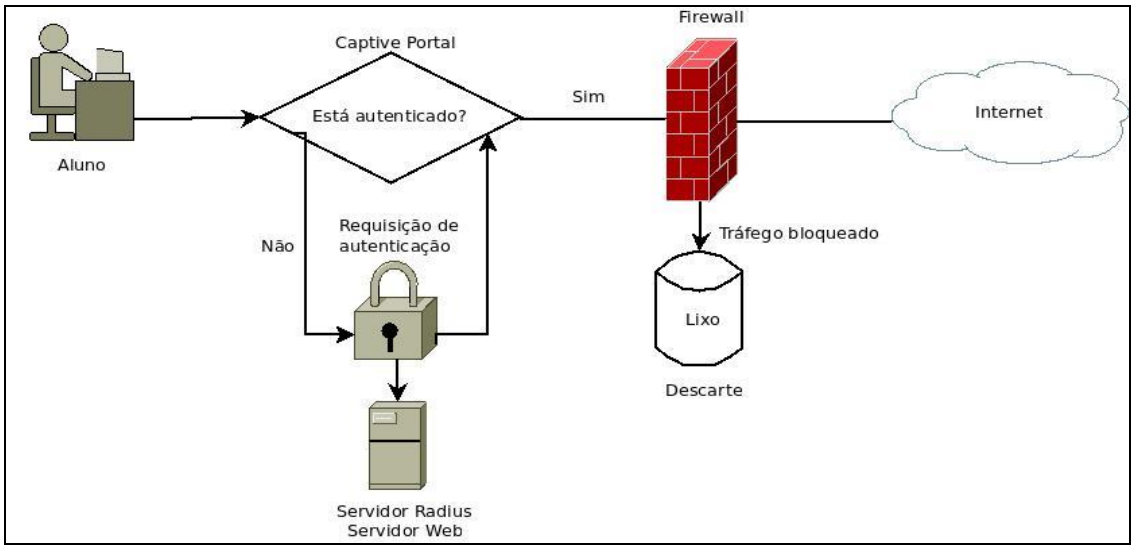

Figura 15. Ambiente Virtual

O projeto *pfSense* é um software livre, licenciado sob a Licença BSD, baseado no sistema operacional *FreeBSD,* personalizado para trabalhar como *Firewall. P*orém, suas funcionalidades vão muito além das de um simples *Firewall,* podendo exercer o papel de roteador, trabalhar com VPN's, Sistemas de Detecção de intrusão, e muito mais. Como *Firewall,* ele pode desempenhar a função de Filtro de Pacote e *Gateway* de Aplicação (*proxy)* (PFSENSE, 2015).

Após instalado, o *pfSense* pode ser configurado através de uma interface *web*. Atualmente possui dezenas de pacotes de *software* livre de terceiros para funcionalidades adicionais, como, por exemplo, o *Squid* (*proxy*).

Para realizar autenticação dos usuários na rede, o próprio *pfSense* conta com uma ferramenta pré-instalada, o *Captive Portal.* O *Captive Portal* faz a captura da conexão através do *Firewall,* com o objetivo de garantir que o usuário não possua acesso à Internet caso não esteja autenticado. Para isso foi utilizada a opção de servidor *Radius,* que armazenará os dados de autenticação dos usuários. Para administrar os dados de usuário no servidor *Radius*, foi desenvolvido um sistema *web.* Esse sistema é responsável pelo cadastro de novos usuários, edição dos dados cadastrais e recuperação de senha.

O *Squid* e *SquidGuard* são responsáveis, respectivamente, pelos papéis de *proxy* e filtro de conteúdo. O *Squid* tem o papel de servidor *proxy*, interceptando as conexões e armazenando o cache das páginas acessadas. Ele foi configurado em modo transparente, o que evita ter que configurar o navegador cliente para utilizá-lo.

Já o *SquidGuard* desempenhará a tarefa de filtro de conteúdo, através da criação de ACL's (*Acess Control List)*. A utilização do *SquidGuard* permite utilizar *Blacklists* (metodologia onde as URLs são armazenadas em um banco de dados e relacionadas com suas categorias, conforme seu conteúdo) em suas ACL's. A função *Times* permite criar diferentes horários, conforme a necessidade, de modo que é possível determinar um período de tempo para o funcionamento e relacioná-lo com uma ACL. Por exemplo, uma ACL que bloqueie redes sociais pode permanecer ativa durante o período de aula, mas ficar inativa durante os períodos de intervalo, permitindo o acesso somente nesses horários.

As regras (*rules*) são utilizadas para controlar o tráfego, através delas que se gerenciam as portas e serviços acessíveis pela rede. Também podem ser utilizadas para bloquear sites específicos, o que acaba suprindo a deficiência do pacote *Squid* instalado no

pfSense, que não realiza a filtragem de conteúdo em sites que utilizam HTTPS. Com a criação de *aliases,* essa torna-se uma ótima opção.

4. Considerações Finais

O trabalho encontra-se no início de sua implantação em ambiente real. Foi realizada a importação dos dados de autenticação dos alunos do ambiente virtual de aprendizado, o *Moodle,* para o servidor *Radius.* Essa integração é um passo importante para que os alunos não tenham que criar novos usuários para autenticação no *Captive Portal.* Futuramente, espera-se também utilizar o servidor *Radius* para autenticação do próprio ambiente virtual, de modo que ocorra a integração e unificação desses dados de usuário.

Por fim, com a implantação espera-se alcançar melhorias no acesso à Internet, destacando-se o aumento na questão de segurança da informação para promover eficiência na utilização das tecnologias de informação no processo de aprendizagem.

Referências

FEITOSA, E. L.; SOUTO, Eduardo; SADOK, Djamel. Tráfego Internet não Desejado: Conceitos, Caracterização e Soluções. Livro-Texto dos Minicursos do VIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, p. 91-137, 2008..

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a Internet: uma abordagem top-down. Tradução Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

PFSENSE. Disponível em:<http:///www.pfsense.org>. Acesso em: 05 set. 2015.

PONTE, C.; VIEIRA, N. Crianças e Internet, riscos e oportunidades. Um desafio para a agenda de pesquisa nacional. In: Comunicação e Cidadania. Actas do 5º Congresso da SOPCOM. 2008. p. 2732-2741.

SÊMOLA, M. Gestão da Segurança da informação: uma visão executiva. Elsevier Brasil, 2014.

TANENBAUM, A. S; WETHERALL, D. J. Redes de Computadores. 5. Ed. São Paulo: Pearson Prentice Hall, 2011.