

SEGURANÇA EM FIREWALL LINUX COM PROXY SERVER BASEADA NA NORMA DE SEGURANÇA BRASILEIRA ABNT NBR 17799

Wesley Mauricio Barboza dos Santos¹
Michel da Silva²

A internet é uma das ferramentas mais importante para as corporações nos dias de hoje. Porém para ter um uso efetivo, se faz necessário criar controles que evitem abusos. A informação é o maior bem que uma empresa pode possuir, exigindo cuidados especiais com a segurança de onde se armazena essas informações, principalmente em servidores com acesso a internet. Administradores de redes enfrentam algumas dificuldades com relação à segurança e controle de acesso à internet, devido utilização de programas como o ultrasurf e o freedom que ajudam os usuários a burlar bloqueios e regras de servidores firewalls com Proxy Server, dificultando o controle, fazendo com que os usuários percam tempo precioso com coisas inúteis. A idéia é apresentar uma solução para essas dificuldades enfrentadas com relação à segurança lógica dos firewalls com Proxy Server. Estudando métodos de ataques de hackers, crackers e o funcionamento do Ultrasurf e o Freedom, e estudando também técnica de Hardening, as ferramentas iptables, syslog, honeyd, aide, squid e o sarg que serão utilizados de acordo com uma política genérica de segurança baseada na norma ABNT NBR 17799. Para o desenvolvimento da proposta foi necessário um computador, simulando um servidor, com o sistema operacional Debian 5.0 e mais um computador para simular ataques e tentativas de usuários de burlar os controles e regras. Os resultados são satisfatórios, de acordo com a pesquisa é possível configurar as ferramentas com base na norma, neutralizando o ultrasurf e o freedom, sendo possível também fazer controle de acesso por usuário, com login e senha e ainda registrar eventos (logs) no servidor na qual a norma exige. Com os resultados obtidos, conclui-se que é possível configurar um firewall Linux com Proxy Server 95% seguro, seguindo alguns itens da norma, 95% pois não existe um sistema 100% seguro, existem outros fatores que deve ser levado em consideração, como por exemplo, o local onde esse servidor vai ficar e quem vai ter acesso diretamente nele, entre outros. A parte de segurança física também está na norma, mas não será falada neste trabalho.

Palavras-chave: Firewall.Segurança.Proxy

¹ Aluno do Curso de Sistemas de Informação. E-mail: wesleymauricio2002@yahoo.com.br

² Professor do Curso de Sistemas de Informação. E-mail: axel.2k@gmail.com