Segurança de redes
Firewall

Gustavo Oliveira[1], Davison Giroldo[1] , André Oliveira[1] , Eduardo Noboru Sasaki[1]
[1] Ciência da Computação – Faculdades de Valinhos

Abstract.

There is users (home and office users) that access the internet and work with important datas, showing it. These datas must be strongly protected against badly intentioned attacks. Hackers can easily access the computers case it does not have any kind of firewall. The work shows solutions with a firewall, explaining how it work and how can protect personal computers without limit any data access to external and internal invaders.

Resumo.

Há usuários (domésticos e de escritório) que acessam a internet e trabalham com dados importantes, expondo-os. Tais arquivos devem ser fortemente protegidos contra ataques mal intencionados. Hackers podem facilmente acessar os computadores caso os mesmos não possuam nenhum tipo de firewall. O trabalho expõe soluções com firewall, explicando seu funcionamento e como é possível proteger os computadores pessoais sem fragilizar qualquer acesso aos dados para os invasores externos e internos.

1. Foco do trabalho

O trabalho foca segurança de redes baseado em soluções utilizando firewall, permitindo controle sobre computadores internos e acesso remoto ao computador de uma empresa ou domiciliar, bem como o monitoramento do tráfego de rede, minimizando as possibilidades de um ataque por spans e vírus.

2. Materiais de referência

São numerosas as fontes de pesquisa existentes relacionadas ao tópico aqui proposto. No entanto, o trabalho se restringe à pesquisas realizadas utilizando-se as seguintes fontes:

- CD-ROM
- Internet
- Periódicos
- Livros
- Monografias
- Artigos

3. Conceito de firewall

Um firewall proporciona um meio para que as organizações criem uma camada de tal forma que elas fiquem completamente isoladas de redes externas, como por exemplo a internet e estejam completamente conectadas a outras. Geralmente localizadas entre a rede interna e a rede externa de uma organização, um firewall provê uma forma de controlar o tamanho e o tipo de tráfego entre as duas redes.

Os firewalls evoluem com o passar dos anos e deixaram de ser somente um filtro de pacotes rudimentar para se tornarem sistemas sofisticados e com capacidade de filtragem cada vez mais avançados.

3.1. Filtro de pacote

Os mecanismos de filtragem implementados por roteadores possibilita que se controle o tipo de trafego de rede existente em qualquer seguimento de rede. Conseqüentemente pode-se controlar os tipos de serviços que podem existir no seguimento de rede. Serviços que comprometem a segurança da rede podem, portanto, ser restringidos.

É importante estarmos cientes de que um filtro de pacote não se encarrega de examinar nenhum protocolo de nível superior ao de transporte, como por exemplo o nível de aplicação, que fica a cargo dos proxy servers. Portanto, qualquer falha de segurança no nível da aplicação, não pode ser evitada utilizando somente um filtro de pacotes.

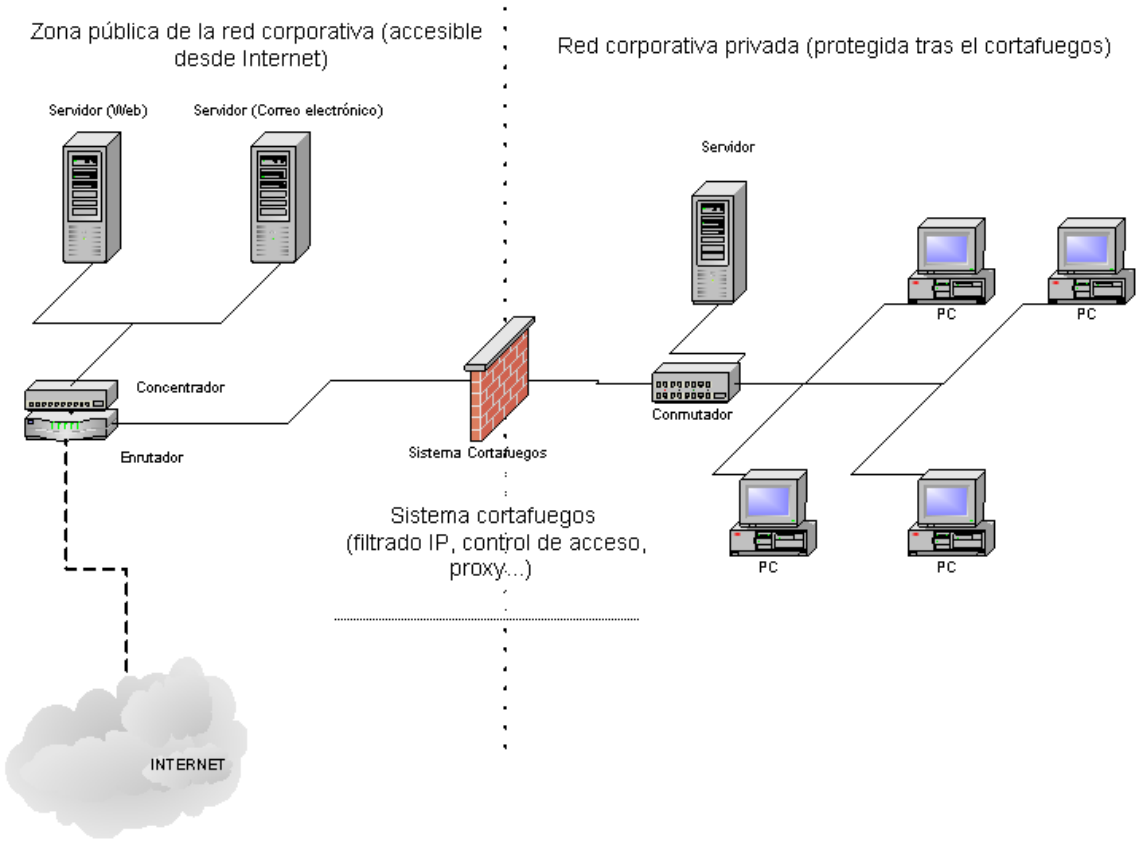

Figura 1. Exemplo de rede protegida por firewall

4. Estratégias de segurança

Abaixo são mostrados alguns exemplos de estratégias de segurança, de uma forma geral, não exclusivas de ambientes de sistemas de computação, porém muito úteis quando consideradas em sua extensão:

- Least Privilege : O principio desta estratégia significa que qualquer objeto (usuário, administrador, sistema, etc) deveria ter somente os privilégios realmente necessários para cumprimento de suas tarefas. Mínimo privilégio é um principio importante para limitar a exposição aos ataques e danos causados por estes. Principais problemas envolvidos à estratégia do privilegio mínimo: 1) Pode ser complexo de implementar

caso os programas e/ou protocolos não permitam estabelecer privilégios. 2) Pode-se acabar implementando algo que tenha menos privilégios do que o mínimo estabelecido.

- Defenser in depth: Este principio determina que não se deve depender de apenas um mecanismo de segurança, não importando quão forte ele pareça ser. Ao invés disso, recomenda-se que sejam utilizados múltiplos mecanismos de segurança e que estes estejam configurados no nível mais alto possível de tolerância a falhas e redundância.

5. Tipos de firewall e uso adequado

Há basicamente dois tipos de firewall que podem ser utilizados:

- Uso caseiro (Personal Firewall): Como exemplo o Norton Internet Security e Zone Alarm:

Figura 2. Norton Internet Security

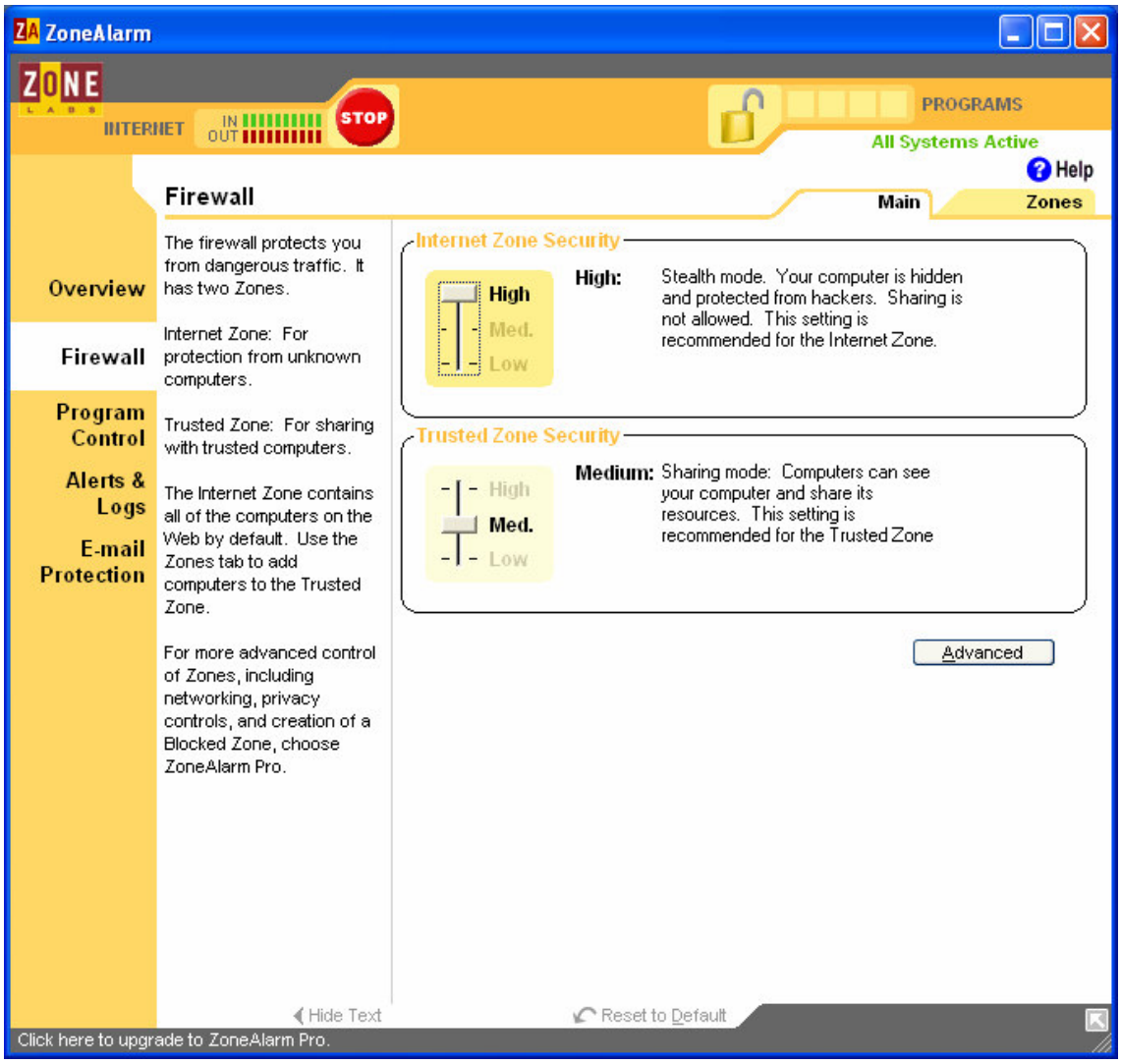

Figura 3. Zone Alarm

- Uso em servidores: Utilizado para garantir a segurança dos servidores de maneira a garantir a integridade dos dados e operações que neles são realizados. Como exemplo temos o Firehol, programa de firewall utilizado em servidores Linux, que pode substituir com apenas uma linha de comando diversos comandos de iptables.

6. Bibliografia

Segurança – Firewall para personal computers e servidores, através do site www.symantec.com

Segurança – Firewall de doméstico, porém também utilizado em empresas – www.zonelabs.com