XIV INIC Encontro Latino Americano de Iniciação Científica
X EPG Encontro Latino Americano de Pós Graduação
IV INIC Jr Encontro Latino Americano de Iniciação Científica Júnior

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: um estudo comparativo sobre os programas e sistemas de *firewall*

Mônica Gonçalves de Mendonça, Edson Aparecida de Araújo Querido Oliveira, Vilma da Silva Santos, Paulo Cesar Ribeiro Quintairos

Universidade de Taubaté – UNITAU, Programa de Pós-graduação em Gestão e Desenvolvimento Regional– Rua Visconde do Rio Branco, 210. Centro – 12020-040 – Taubaté – SP – Brasil. monica@ita.br; edson@unitau.br; vilma70@gmail.com; quintairos@gmail.com.

Resumo- A crescente utilização de computadores, para uso pessoal e profissional, aliada à popularização do acesso à *internet,* por meio de conexões de banda larga acarreta a crescente preocupação com a segurança dos sistemas de informação. Essas ameaças fomentam o mercado de produtos de segurança, especialmente os sistemas *firewall* e os programas de antivírus; o *firewall* físico ou baseado somente em *software* é um dos dispositivos mais utilizados como sistema de segurança. Neste trabalho serão apresentados os resultados de uma pesquisa exploratória e descritiva, realizada a partir de um levantamento bibliográfico e documental, sobre os tipos de *firewall* disponíveis no mercado brasileiro de segurança de informação. O objetivo é construir um quadro comparativo dos produtos analisados, a partir de documentos de acesso público. Os resultados apresentados indicam que a grande variedade de produtos é devida às diferentes necessidades dos clientes. Os fatores que recomendam as escolha das diversas soluções disponíveis, nem sempre são considerados por um número significativo de usuários.

Palavras-chave: Segurança em Sistemas de Informação, *Firewall*.
Área do Conhecimento: Ciências Sociais Aplicadas.

Introdução

Os rápidos avanços tecnológicos permitiram a fusão da infra-estrutura dos meios de telecomunicações e a *Internet,* criando as bases do setor usualmente denominado TIC — Tecnologia da Informação e Comunicações. A rede mundial de computadores possibilita a conexão entre sistemas e redes em ambientes corporativos e distribuídos (CAMEIRA, 2007).

Apesar dos muitos benefícios e possibilidades devidos à inovação tecnológica e às novas e tecnologias interconectadas, através da *Internet,* a segurança dos sistemas baseados em TI tem sido um grave problema para gestores e usuários de computadores. O termo segurança refere-se à proteção contra acessos indevidos de usuários não habilitados a um sistema, programa ou rede de computadores; implica a aquisição de informações a quem não é de direito (TANENBAUM, 2003).

Há diversos sistemas criados com o intuito de garantir a segurança dos sistemas de informação, ou ao menos de tornar os computadores e as redes menos vulneráveis. Dentre os sistemas de segurança, observa-se que uma medida inicial é a implantação de um *firewall*. Estes sistemas contribuem para resolver problemas de acessos internos e externos não autorizados a uma rede conectada à Internet. De acordo com O´brien (2004), os *firewalls* se tornaram componentes essenciais das organizações que se conectam com a *Internet*, tendo-se em vista a vulnerabilidade e a falta de segurança da *Internet.*

Neste trabalho apresentam-se os resultados de uma pesquisa cujo objetivo foi construir um quadro comparativo dos tipos de *firewall* disponíveis no mercado brasileiro. Tal quadro possibilita a escolha do produto mais adequado às diferentes condições de uso e aos diferentes orçamentos.

Metodologia

O presente trabalho de pesquisa tem caráter descritivo-exploratório. Trata-se de uma pesquisa bibliográfica e documental, tendo sido desenvolvido a partir da análise qualitativa de dados obtidos em documentos de acesso público.

Resultados

O NIST (2002) define *firewall* como sendo o conjunto de dispositivos ou programas que ajudam as organizações a protegerem suas redes e sistemas de informação. Ele também permite que usuários protejam seus computadores de ataques hostis, tentativas de invasão e *softwares* maliciosos. *Firewalls* são, portanto, dispositivos ou programas que controlam o fluxo de tráfego de entre redes ou hosts que empregam diferentes políticas de segurança.

Os *Firewalls* são freqüentemente avaliados no contexto da Internet e da conectividade, pois eles também podem ter aplicabilidade em outros ambientes de rede. Por exemplo, muitas redes corporativas utilizam *firewalls* para restringir a

conectividade da rede interna a funções mais particulares tal como contabilidade ou pessoal.

Nakamura e Geus (2008) afirmam que embora os sistemas de *firewall* possam ser considerados como uma tecnologia antiga, ela ainda não adquiriu a estabilidade necessária tendo em vista que continua em constante processo de evolução. Isso se deve ao aumento da complexidade das redes nas organizações, que adicionam cada vez mais características e funcionalidades que precisam ser protegidas.

Chapman (1995 apud Nakamura e Geus 2008) define *firewall* como sendo um componente ou conjunto de componentes que restringe o acesso de um host situado em uma rede protegida e a Internet, ou entre outros conjuntos de redes.

A empresa Cyclades (2003) define que *firewall* é um conjunto de medidas tomadas para garantir o máximo de segurança, incluindo filtros de pacotes, *softwares* de monitoramento, detecção de intrusos e até mesmo a maneira que seus dados devem ser acessados remotamente.

De acordo com Kurose e Ross (2003), as empresas empregam o *firewall* por algumas razões:

- Impedir que intrusos interfiram na operação diária da rede interna, sendo um concorrente da organização ou mesmo algum usuário esperto querendo se divertir.
- Impedir que intrusos apaguem ou modifiquem informações armazenadas na rede interna.
- Impedir que intrusos obtenham informações sigilosas.

O autor relata ainda que o *firewall* mais simples consiste em um filtro de pacotes, e *firewalls* mais sofisticados consistem em combinações de filtros de pacotes e *gateways* de aplicação.

Atualmente existem diversos tipos de *firewall*. Em uma rede de computadores, um *firewall* pode se apresentar como um dispositivo de *hardware*, *software* ou híbrido que tem como principal objetivo a proteção das informações e ou filtro de acesso as mesmas, podendo servir ainda como elemento de interligação entre duas redes distintas (MARCELO, 2003).

- DISPOSITIVO DE *HARDWARE* - Equipamentos como roteadores, placas especiais ou mesmo computadores.
- DISPOSITIVO DE *SOFTWARE* – São programas especializados, instalados em computadores ou roteadores.
- DISPOSITIVOS HÍBRIDOS - É uma mescla de dispositivos de *hardware* e *software*

Um software de *firewall* deve ser instalado e utilizado em qualquer sistema operacional do computador e sempre atualizados. Os firewalls baseados em *softwares* são utilizados para complementar a proteção fornecida por *firewalls* baseados em *hardware*. Os sistemas de *firewall* podem ser adquiridos com ou sem custo para o usuário. Segundo a empresa Microsoft (2004) há vantagens e desvantagens sobre o uso de cada um deles, como representado a seguir.

Firewall Tipo	Vantagens	Desvantagens
Software	- Nenhum Hardware adicional; - Não exige instalação de cabos; - Boa opção para computadores autônomos.	- Custo adicional: a maioria custa caro; - Instalação e configuração podem ser necessárias para iniciar seu uso; - Necessária uma licença para cada computador.
Hardware	- Possuem várias portas, que permitem conectar vários dispositivos simultaneamente. - Um único equipamento oferece proteção para várias máquinas.	- Exige conexão de cabos, podendo sobrecarregar a área de trabalho. -Custo elevado, pois utiliza hardware dedicado.

Quadro 1 – Comparativo entre *Firewalls por Software* e por *Hardware*. Fonte: Microsoft *Inc*.

Para a RNP (Rede Nacional Pesquisa, 2002) o *Personal Firewall* ou *Firewall* pessoal é classificado como um aplicativo que intercepta as conexões de entrada e saída de um computador, baseando-se em regras padrão definidas pelo usuário, mas não permitem uma solução abrangente para todos os problemas de segurança, servindo apenas como uma fonte adicional de proteção.

Dentre alguns sistemas desta categoria, pode-se citar aplicativos *freeware tais como*: o *ZoneAlarm,* que tem sua inicialização automática ao ligar o computador e interface interativa com o usuário; e o *Tiny Personal Firewall* que tem como ponto forte a permissão para que sejam criadas regras de acesso na medida em que os aplicativos vão necessitando de conexão com a *Internet*, permitindo também a administração remota.

Dentre as versões comerciais para uso pessoal, pode-se citar o *Norton Personal Firewall,* que permite controle de privacidade, um bom assistente de configuração, sendo a interface com o usuário interativa e o *BlackIce Defender,* que também apresenta uma configuração bem simples e um bom reconhecimento de ataques.

Dentre estes *softwares* apresentados cada um apresenta um determinado tipo de utilização, segundo a RNP (2002).

- Usuário que necessita de maior controle sobre quais aplicativos se conectam à internet: *ZoneAlarm.*
- usuário que deseja se aprofundar e conhecer mais sobre os ataques de que está sendo alvo: *BlackIce Defender.*
- usuário que deseja o aplicativo mais simples e funcional: *Tiny Firewall.*
- usuário que deseja uma solução mais completa com inclusive controle de privacidade: *Norton Personal Firewall.*

Quanto as funcionalidade, os *firewalls* apresentam uma série de componentes, sendo que cada um tem uma funcionalidade diferente, desempenhando um papel que influi diretamente no nível de segurança do sistema (Nakamura e Geus, 2008). Essas funcionalidades formam os chamados componentes clássicos de um *firewall*, que foram definidos por Chapman (1995):

- Filtros, *proxies*, *bastion hosts*, zonas desmilitarizadas.
- NAT (*Network Address Translation*), (VPN) Rede Privada Virtual.
- Autenticação/certificação.

Um *firewall* pode ajudar a aumentar o nível de segurança de uma rede de computadores, pois ele se tornou o centro para tomada de decisões, por se localizar no ponto de entrada/saída de uma rede. Para que um *firewall* seja eficiente, todo o tráfego entre a *Internet* e a rede local terá que passar através dele, sendo então inspecionado, permitindo somente a passagem do tráfego autorizado (CAMY, SILVA RIGHI, 2003).

A função fundamental de um *firewal*l é restringir o fluxo de informação entre duas redes. Todo o tráfego de, e para a *Internet*, pode ser direcionado ao *firewal*l, dando a ele a capacidade de verificar se o tráfego é aceitável ou não. Para configurá-lo, é necessário que sejam definidos quais os tipos de dados que poderão circular pela rede e quais não poderão, constituindo então uma política para o *firewall*. Existem duas políticas básicas para um *firewall*:

- *Default Permit*: Onde se define o conjunto de condições que irão resultar no bloqueio dos dados. Qualquer host ou protocolo não coberto pela política será permitido.
- *Default Deny*: Especifica-se o que poderá passar pelo *firewall*, ou seja, os *hosts* e os protocolos, o que não estiver especificado terá acesso negado na rede.

Analogamente, os *firewalls* agem como portas que permitem a algumas conexões entrar ou sair da rede, enquanto bloqueia as demais. Normalmente, as conexões originadas de dentro de uma rede são permitidas, enquanto as originadas de fora da rede são bloqueadas; (MCCARTHY, 2004).

Um *firewall* não protege a rede contra usuários internos, conexões que não passam por ele, contra ameaças completamente novas, pois ele é projetado para proteger contra ameaças conhecidas, não protege contra vírus, pois para este tipo de problema somente utilizando *softwares* específicos. (CAMY, SILVA RIGHI, 2003) .

O NIST (2002) relata que o desempenho do *firewall* e seus componentes devem ser identificados e monitorados para que as questões de recursos potenciais sejam identificadas e abordadas antes que o desempenho seja comprometido.

Nakamura e Geus (2008) descrevem que quando a maturidade do mercado de *firewalls* é analisada, verifica-se que no início o mercado era formado por simples filtros nos *gateways*, mas que como todo mercado emergente, diversas e novas empresas passaram a oferecer seus produtos.

Com a demanda crescente, grandes fabricantes entraram no mercado, resultando em maiores opções de compra e na diminuição dos preços. O mercado de *firewall* pode ser dividido nos seguintes seguimentos:

- Provedor de serviços (*Internet Service Provider*-IPS), com maior capacidade de filtragem de pacotes.
- Corporativo, são clássicos que se tornaram fáceis de gerenciar, mas precisam de um profissional de segurança para gerenciamento.
- *Small and Midsize Bussiness,* considerados *plug and play*, com poucas opções de configuração.
- *Small Office Home Office*, com múltiplos serviços integrados, específicos para organizações com poucos recursos técnicos, porém podendo trazer problemas de segurança, devido ao aumento das funcionalidades.

Para Nakamura e Geus (2008) é preciso tomar cuidado com relação a diversos produtos que estão no mercado, pois os fabricantes estão aproveitando a força do termo "*firewall*" e vendendo produtos como se fossem a solução para todos os problemas de segurança das organizações.

Em um ambiente cooperativo, há a necessidade de uma estratégia de segurança bem definida, que começa pelo uso do *firewall* para a proteção do perímetro, mas na realidade o que vai garantir a eficiência da segurança necessária é uma política de segurança definida e uma correta implementação por parte dos administradores (NAKAMURA; GEUS, 2008).

O produto mais adequado para uma organização é aquele que melhor permite a implementação de uma política de segurança bem definida e que melhor se ajusta à experiência e capacidade do profissional.

Diversos aspectos devem ser levados em consideração na escolha do *firewall* mais adequado para uma organização, tais como:

- Fabricante/fornecedor – A estabilidade financeira e relacionamento do fornecedor com outros clientes.
- Suporte Técnico – o suporte deve atender a escala de 24x7
- Tempo – O prazo para funcionamento do firewall é essencial para a escolha do sistema ao qual será instalado.
- Projeto – Atender consideravelmente aspectos de implementação, como a defesa de ataques clássicos.
- *LOGS* – Apresentar uma boa capacidade de armazenamento de logs a fim de facilitar o registro de tentativas a possíveis ataques.
- Desempenho – Aliar o desempenho com a segurança.
- Gerenciamento – Facilidade e eficiência para configuração remota
- Teste do *Firewall* – Testes são essenciais para determinar a efetividade do que foi implantado.
- Capacitação de Pessoal – Operação e manutenção requerem profissionais com visão em segurança e capacidade comprovadas.

Considerações Finais

Os resultados apresentados neste trabalho permitiram construir um quadro comparativo dos principais aspectos que devem ser considerados para a escolha do sistema de *firewall* mais adequado a um sistema, visando atender aos requisitos de segurança tanto para o usuário pessoal quanto para as organizações.

Foram descritas as principais arquiteturas de firewall utilizadas, bem como, os aspectos técnicos mais importantes para decisão na escolha da solução mais apropriada para cada caso. Foram apresentados alguns indicadores sobre o custo envolvido na aquisição, instalação e operação das diversas soluções mencionadas.

No entanto, apesar de serem componentes tecnológicos imprescindíveis para garantir a segurança das informações, deve-se ressaltar que os sistemas de *firewall* são apenas uma parte da solução.

Para alcançar um estágio de maior segurança das informações, diversos outros fatores devem ser considerados. Dentre eles destacam-se os aspectos culturais e motivacionais que os usuários dos sistemas devem possuir, pois como em todo sistema, a segurança geral do conjunto será tão eficiente quanto o seu elo mais fraco.

Referências

- CAMEIRA, R. F. A Indústria de Telecomunicações e o Setor Informacional Multimídia Emergente. Rio de Janeiro: Quartet, 2007.

- CAMY, A. R., SILVA, E. R. N., RIGHI, R. Seminário de Firewalls, Florianópolis. 2003. Disponível em <http://svn.assembla.com/svn/odinIDS/Egio/artigos/Firewall/Firewall.pdf>. Acesso em Agosto de 2010.

- Cyclades Brasil. Guia Linux de Conectividade. São Paulo: Cyclades Brasil, 2003.

- Kurose , J. F.; Ross, W. K. Rede de Computadores e a Internet: uma nova abordagem. São Paulo: Adddison Wesley, 2003.

- Marcelo, A. Firewalls em Linux para pequenas corporações. Rio de Janeiro: Brasport, 2003.

- MCCARTHY, M. Conceitos básicos sobre Firewall. 2004. Disponível em <http://www2.dcc.ufmg.br/~mlbc/cursos/internet/firewall. index.html.>. Acesso em Agosto 2010.

-MICROSOFT. Disponível em: <http:// www.microsoft.com/brasil/security/viruses/fwbenefits.mspx>. Acesso em Agosto 2010.

NIST- National Institute of Standards and Technology. Disponível em <http://csrc.nist.gov/publications/nistbul/Oct2009_firewall-bulletin.pdf.> Acesso em Agosto 2010.

-RNP – Rede Nacional de Pesquisa. Disponível em <http://www.rnp.br/newsgen/0201/firewall-pessoal.html>. Acesso em Agosto 2010.