

CENTRO UNIVERSITÁRIO FEEVALE

LEÔNIDAS KLEIN SALDANHA

*Firewalls* de Baixo Custo

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo, maio de 2007.

LEÔNIDAS KLEIN SALDANHA

leonidas-klein@feevale.br

*Firewalls* de Baixo Custo

Centro Universitário Feevale  
Instituto de Ciências Exatas e Tecnológicas  
Curso de Ciência da Computação  
Anteprojeto de Trabalho de Conclusão

Professor orientador: Msc. Vandersílvia da Silva

Novo Hamburgo, maio de 2007.

## RESUMO

O trabalho apresentará a comparação de dois *firewalls* GPL (*General Public License*) voltados para o segmento SOHO (*Small Office/Home Office*, Pequenos escritórios/escritórios em casa) de empresas. Como a insegurança na Internet cresce cada vez mais, esse segmento tende a ser mais vulnerável a ameaças. Seus níveis de segurança são relativamente baixos, atraindo a atenção dos *crackers*, os quais têm a tendência de voltar-se para este segmento pela fragilidade de seus sistemas de proteção, quando existentes. Sendo assim a preocupação com a falta de segurança destas redes não pode ser esquecida. Os cuidados que elas devem ter com seus dados é crucial para que diminua as chances de algum indivíduo mal intencionado causar alguma forma de prejuízo. As pequenas empresas muitas vezes não possuem alguém especializado para definir uma política de segurança consistente ou para administrar sua rede. Da mesma maneira não dispõem de capital para investir em *firewalls* de alto custo. Por esse motivo o estudo será embasado em duas ferramentas que não possuem custo inicial, possibilitando a aquisição do mesmo de uma maneira simplificada. Serão estudadas características comuns e métricas de comparação, e posteriormente explicadas para o bom entendimento do funcionamento desta tecnologia indispensável nos dias de hoje. Após estes estudos será elaborada a forma de comparação para averiguar qual das ferramentas melhor se enquadra para este segmento empresarial.

Palavras-chave: *Firewall*. Segurança de Pequenas Empresas. Segurança com custo baixo.

## SUMÁRIO

MOTIVAÇÃO.....	5
OBJETIVOS.....	8
METODOLOGIA.....	9
CRONOGRAMA .....	10
BIBLIOGRAFIA .....	11

## MOTIVAÇÃO

Dadas as atuais circunstâncias nas quais as pequenas empresas são submetidas por estarem conectadas na Internet, as SOHO (*Small Office/Home Office*, Pequenos escritórios/escritórios em casa) devem se manter protegidas da melhor forma possível. Uma ferramenta indispensável nos dias de hoje é o *firewall*, ele mantém (na medida do possível) a rede interna em segurança contra a rede externa (Internet). É instalado na fronteira com a Internet, fazendo o roteamento de pacotes com base na política de segurança aplicada. Os benefícios trazidos por esta ferramenta são muitos: restrição de acesso à rede interna, controle sobre o tráfego da Internet, relatórios de segurança por meio de *logs*, filtro de conteúdo indevido...

Todo o tráfego entre a rede privada e a Internet deve necessariamente passar pelo *firewall*, assim ele pode analisar os pacotes e permitir ou não a passagem dos mesmos nos dois sentidos (entrada e saída). “*Achamos que um firewall é qualquer dispositivo, software, arranjo ou equipamento que limita o acesso à rede. Ele pode ser uma caixa que você compra ou constrói ou uma camada de software em alguma outra coisa*”.(CHESWICK, BELLOVIN e RUBIN, 2005, p.177)

Quando atua na fronteira com a Internet poupam-se recursos dos computadores, pois sem ele cada estação de trabalho teria de se proteger sozinha. Outro ponto positivo é a centralização dos serviços de proteção, contra perigos externos, em uma máquina preparada para trabalhar nesta tarefa. Em contrapartida o *firewall* cria um canal estreito por onde passa toda a informação que sai ou entra na rede, mas é um pequeno preço que deve ser pago pela segurança. (STREBE e PERKINS, 2002).

Os *firewalls* podem possuir serviços dentre os quais se destacam: filtro de pacotes, NAT e *proxy*. A maioria deles também tem a capacidade de realizar outros dois serviços: autenticação criptografada e VPN (STREBE e PERKINS, 2002).

A necessidade de utilizar ou não os recursos apresentados acima varia, existem casos em que a empresa não precisará de todos. Isto depende do ramo de atividade, do tamanho da empresa e de outras variáveis.

As pequenas empresas possuem características distintas das atividades, o que gera necessidades de proteção diferenciadas. Seus gestores devem averiguar a importância de seus dados e tomar as providências.

Observando-se que o custo das conexões de alta velocidade com a Internet vem diminuindo ao longo dos anos, cada vez mais as SOHO as utilizam, o que agrava as vulnerabilidades: pelo fato da exposição à Internet durar longos períodos de tempo, pela falta de política de segurança e pelo investimento em segurança da informação ser limitado.

Não utilizar um *firewall* em uma pequena empresa é um agravante para a baixa segurança. Em ambos os casos (utilizar ou não um *firewall*) ainda existem algumas medidas que devem ser tomadas como: manter as atualizações dos sistemas operacionais em dia e colocar um antivírus em cada estação; atualizando-o regularmente. Se o sistema operacional usado for o Windows XP o mesmo contém um simples *firewall* que somente filtra pacotes e bloqueia portas, mas deve estar ativado. No caso de conexão por ADSL, outra medida de segurança seria adotar modems roteadores que possuam filtro de pacotes, desta maneira os mesmos podem ser configurados para aumentar a segurança da rede prevenindo alguns protocolos ou conexões que possam ocasionar risco para a empresa.

Mesmo que as SOHO não sejam alvos comuns, por muitas vezes não possuem dados que interessem a outros, a segurança não pode ser deixada de lado. Ao contrário destas, existem empresas pequenas que lidam com dados sigilosos como: clínicas médicas, escritórios de advocacia, contabilidade, etc. Isso deve ser levado em conta na hora de configurar o nível de segurança e ou bloqueio que o *firewall* irá oferecer.

Ainda assim uma pequena empresa pode atrair um *craker*, a tendência é que ele seja impulsionado a invadi-la pelo motivo da baixa segurança. As grandes empresas comumente se preocupam com a segurança da informação e possuem capital para altos investimentos: novos equipamentos, novos programas e contratam uma pessoa ou uma equipe responsável por esse assunto. Isso as torna menos atrativas para o *craker*, muitas vezes por incapacidade do mesmo de invadir empresas com altos níveis de segurança. (ZMOGINSKI, 2006)

“Como regra geral, quanto mais visível é uma organização, maior é a probabilidade de ela atrair um hacker que a coloca em sua agenda” (STREBE e PERKINS, 2002, p. 186).

Os gestores das pequenas empresas podem não possuir o conhecimento devido sobre a necessidade de proteção da informação. Também pelo motivo do capital ser baixo, não é possível um investimento elevado em segurança.

O presente trabalho pretende comparar duas soluções de *firewalls*. Ambas serão aplicáveis às pequenas empresas, ou seja, o produto não terá um alto custo.

Ao fim, as pequenas empresas terão uma avaliação de qual é o *firewall* – dentre os dois – mais recomendado para seu segmento, desta forma poderão se munir de mais uma ferramenta para ajudar no aumento da segurança em seu ambiente de rede.

## OBJETIVOS

Objetivo geral: Fazer a comparação entre dois *firewalls* de baixo custo, destinados a pequenas empresas com restrições de orçamento.

### Objetivos específicos

- Estudar o funcionamento dos componentes comuns de *firewalls*
- Pesquisar métricas de comparação.
- Definir métricas a serem aplicadas
- Definir dois *firewalls* GPL para a comparação
- Aplicar métricas sobre os *firewalls* em um ambiente controlado
- Avaliar resultados e definir o melhor *firewall*

## METODOLOGIA

A metodologia que se propõe prevê a elaboração da pesquisa em dois semestres:

### Primeiro semestre (TC1)

1. Realizar pesquisa bibliográfica em artigos, livros, revistas e trabalhos de conclusão de curso
2. Elaborar o anteprojeto com base na pesquisa realizada
3. Estudar o funcionamento do *firewall* em geral
4. Estudar o funcionamento de cada componente de um *firewall*
5. Pesquisar métricas de comparação
6. Definir dois *firewalls* GPL para a comparação
7. Definir as métricas que serão utilizadas
8. Elaborar o trabalho escrito de TC I

### Segundo Semestre (TC2)

9. Preparar um ambiente para comparação dos *firewalls*
10. Instalar os dois *firewalls* com políticas de segurança padrão
11. Aplicar métricas escolhidas sobre os *firewalls* no ambiente controlado
12. Analisar os resultados
13. Elaborar o trabalho escrito de TC II, incluindo toda a pesquisa, procedimentos e resultados
14. Criar uma apresentação para a banca contemplando os dois semestres

## CRONOGRAMA

### Trabalho de Conclusão I

Etapas	Meses			
	Março	Abril	Maio	Junho
Etapa 1				
Etapa 2				
Etapa 3				
Etapa 4				
Etapa 5				
Etapa 6				
Etapa 7				
Etapa 8				

### Trabalho de Conclusão II

Etapas	Meses			
	Agosto	Setembro	Outubro	Novembro
Etapa 9				
Etapa 10				
Etapa 11				
Etapa 12				
Etapa 13				
Etapa 14				

## BIBLIOGRAFIA

- BORSCHIED, Régis Maciel. **Protótipo de Aplicação Web Para Gerenciamento de Firewall Linux**. Blumenau: 2005. p 18-26. Monografia (Bacharelado em Ciências da Computação) – Centro De Ciências Exatas e Naturais, Universidade Regional de Blumenau, 2005.
- CHESWICK, William R; BELLOVIN, Steven M; RUBIN, Aviel D. **Firewalls e Segurança na Internet: Repelindo o Hacker Ardiloso**. 2ª edição. Porto Alegre: Artmed, 2005. 400 p.
- FERRETTO, Luiz Filipe Fagundes et al. **Implementações Básicas de Segurança Para Ambientes com Processamentos Críticos**. Brasília: 2002. 118 p. Monografia (Especialização em Redes de Computadores) - Estudos, Pesquisa, Pós-graduação e Extensão (COPEX), UNEB, 2002.
- HARE, Chris; SIYAN, Karanjit. **Internet Firewalls and Network Security**. Indianópolis, Estados Unidos da América: New Riders, 1996. p 201-354
- HENMI, Anne et al. **Firewalls Polices and VPN Configurations**. Canada: Syngress, 2006. 504 p
- LAET, Pert De; SCHAUWERS, Gert. **Network Security Fundamentals**. Indianópolis, Estados Unidos da América: Cisco Press, 2004. 480 p.
- MAIWALD, Eric. **Networ Security: A Beginner's Guide**. Estados Unidos da América: Osborne, 2001. 441 p.
- NOONAN, Wes; BRAWSKY, Ido. **Firewall Fundamentals**. Indianópolis, Estados Unidos da América: Cisco Press, 2006. 408 p.
- PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence. **Security in Computing**. 4ª edição. Massachusetts, Estados Unidos da América: Prentice Hall, 2006. 880 p
- STREBE, Matthew; PERKINS Charles. **Firewalls**. São Paulo: Makron Books, 2002. 411 p.
- ZMOGINSKI Felipe. **Crackers preferem PCs de pequenas empresas**. Brasil: 2006. Disponível em: <<http://info.abril.com.br/aberto/infonews/112006/21112006-3.shl>>. Acesso em: 01 de maio de 2007.