Faculdade Santa Maria
Curso de Bacharelado em
Sistemas de Informação

Firewall:
Requisitos e Primícias na escolha de sua Utilização.

por
Marcos Antonio de Souza Santos

Recife
2007

Marcos Antonio de Souza Santos

Firewall:
Requisitos e Primícias na Escolha de sua Utilização.

Monografia apresentada ao Curso de Sistemas de Informações da Faculdade Santa Maria como requisito para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Marcio Nogueira

Recife
2007

DEDICATÓRIA

Ao Deus maior, o pai altíssimo que me deu perseverança, força e paciência, lanterna que guia meus passos e luz que ilumina meu caminho, a Jesus fonte inesgotável de paz e refugio de meus momentos mais difíceis, fortaleza em meus temores e porto seguro nos momentos de turbulência.

A minha mãe Tânia, minha mãe Terezinha e minha mãe Maria Amara, sem vocês nada disso teria valido;

A minha esposa Waldcelma, pelo amor e dedicação de uma grande companheira, que me compreendendo nestes períodos de ausência e sempre me dando força para que não desistisse e concluísse mais uma etapa nesta vida;

A todos os colegas da minha turma pelos agradáveis momentos vividos e pelo grande elo de amizade formado.

.

AGRADECIMENTOS

A Deus por me ter oferecido a oportunidade de viver e ser um eterno aprendiz, dando-me força e coragem para continuar lutando, iluminando minha mente, me protegendo e abençoando, Yeshu lá Sabacktani Eloy lá hi la´lá Sabacktani;

Aos meus coordenadores Carlos Alexandre, Érika Medeiros e Kátia Garcia pelo acompanhamento e orientação pedagógica durante o curso;

A todos os meus professores pela dedicação e motivação durante o curso, tendo vocês a certeza de que tudo o que a mim foi transmitido será sempre de grande importância na minha formação e pratica profissional e pessoal;

Agradecimento especial aos professores Marcio Nogueira e Betânia Maciel, meus orientadores, pela paciência, empenho, simpatia e presteza na transmissão de seus conhecimentos para o desenvolvimento do tema e formatação deste projeto;

A minha Tia Terezinha e minha esposa Waldcelma pela maravilhosa ajuda na revisão ortográfica e gramatical deste trabalho;

A todos os meus amigos e parentes que me depositaram a confiança e credibilidade em minhas decisões.

RESUMO

Especificar o melhor tipo de Firewall, para utilização pessoal ou corporativa, requer antes de tudo, um breve conhecimento do cenário onde este ira atuar, definir quais riscos e quais falhas existem nestes dois ambientes, qual o perfil de trafego de dados e qual nível de segurança dever ser implementado.

Utilizar o Firewall adequado baseia-se em uma analise do que pode ser oferecido atualmente no mercado, relação custo e benéfico e se sua operacionalização é praticável, em que nível de segurança este oferece aos objetivos da situação do consumidor.

Através de analise comparativa demonstradas em gráficos de estudos de desempenho dos tipos de Firewall, serão apresentados os mais utilizados atualmente, corporativos ou residenciais.

É possível aproximar-se do que, dentro dos padrões mínimos de segurança serve em seus princípios a utilização da segurança e da privacidade.

Assim não existe no mercado propriamente definido o melhor Firewall, o que se propõe são Firewall de software e Firewall de hardwares, que são testados por ferramentas que definem dentro de um padrão mínimo o seu grau de segurança para sua utilização.

Palavras-chaves: Firewall, Grau de Segurança, Firewall de software, Firewall de hardwares, privacidade.

ABSTRACT

To specify the best type of Firewall, for personal or corporative use, requires before everything, a brief knowledge of the scene where this anger to act, to define which risks and which imperfections exists in these two environments, which the profile of passes through of data and which level of security to have to be implemented.
To use the adequate Firewall is based on one analyzes of that it can be offered currently in the market, relation cost and beneficial and if its operation is practicable, where security level this offers the objectives of the situation of the consumer. Through it analyzes comparative demonstrated in graphs of studies of performance of the types of Firewall, will be presented the most used currently, corporative or residential.
It is possible to come close itself of that, inside of the minimum standards of security it serves in its principles the use of the security and the privacy. Thus the best Firewall does not exist in the properly definite market, what it is considered are Firewall of software and Firewall of hardwares, that they are tested by tools that inside define of a minimum standard its degree of security for its use.

Key words: Firewall, Degree of Security, Firewall of software, Firewall of hardwares, privacy.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Prover um ambiente de utilização de dados e informação seguros e livres das investidas de invasores e criminosos digitais pode ser motivo de muita preocupação para alguns usuários ou departamentos tecnológicos, onde estes além de deter a entrada, tende a se preocupar como estes invasores agem e suas formas de pensar.

Baseado-se neste principio, existem muitos aplicativos e ferramentas capazes de minimizar estas investidas, que em muitos casos são bem ou maus sucedidas, isso depende muito da política utilizada dentro destes ambientes e suas diretrizes.

Entre estas ferramentas de segurança, faremos um estudo sobre Firewall, aplicativo este que visa regular o trafego de entrada e saída e dados, forma esta, que invasores utiliza para adentrar nos ambientes coorporativos ou residências com a finalidade de subtrair dados na sua forma bruta ou mesmo informações.

Definir um Firewall que atenda as necessidades de um usuário requer inicialmente um breve conhecimento da ferramenta em suas particularidades como, tipos e derivações, classificações e funcionalidades, nível de interatividade e um dos mais importantes pontos, o custo e beneficio, pode-se utilizar como termômetro de classificação de Firewall além dos testes e analises aplicadas no meio técnico, o grau de usabilidade postados em fóruns e enquêtes na internet.

Neste trabalho será dada ao leitor à oportunidade de entrar neste nível de conhecimento, e ao final o mesmo terá capacidade de identificar o Firewall que poderá ou não atender sua necessidade, baseando-se no conteúdo colhido desta pesquisa, além dos testes, gráfico e aplicativos apresentados para avaliação e definição da capacidade de defesa de um Firewall.

Não existe por definição técnica ou de capacidade “o melhor Firewall”, devido a este ser considerado melhor quando se adequa a necessidade do usuário, o que existe são inúmeros tipos e finalidade, pontos fortes e pontos fracos e nível de complexidade na utilização e manuseio.

Para um melhor desenvolvimento do tema, o projeto foi organizado em capítulos, que estão distribuídos da seguinte forma:

Capítulo 1 - Fundamentação Teórica: apresentação dos principais conceitos de Firewall que servirão de base para a compreensão do tema e conceitos relacionados ao

surgimento da motivação e utilização de Firewalls

Capítulo 2 - Invasores e Taxonomias de Ataque: elaboração da forma como crackers e outros crimes apresenta um potencial fator de riscos para uma rede interna.

Capítulo 3 - Requisitos e Primícias para Escolha do Firewall: Apresentação de um conjunto de conhecimentos que um usuário deverá ter, e uma análise dos Firewalls disponíveis.

Capítulo 4 - Tráfego de protocolos: análise de padrões e diretrizes sobre o que trafegará entre a rede externa e interna passando pelo Firewall.

Capítulo 5 - Comparativos entre firewall de software: demonstração do perfil dos firewalls de software para diversos usuários.

Capítulo 6 - Conclusão: apresentará os resultados obtidos pelo projeto, recomendações a partir destes resultados, críticas e considerações finais.

Capítulo 1 Fundamentação Teórica

1.1 Sobre Firewalls

1.1.1 Firewall

> *"É o nome dado ao dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão e ou recepção de dados nocivos ou não autorizados de uma rede a outra. Dentro deste conceito incluem-se, geralmente, os filtros de pacotes e os proxy de protocolos."* *Neto U.(2004)*

Segundo Ford L. (2002), "os firewalls é um dispositivo ou programa desenvolvido para detectar e proteger seu computador e rede contra ameaças internas e externas".

Como toda tecnologia é passiva a evolução não seria diferente a este sistema, pois junto a evoluções vêm as gerações.

> *"Os primeiros firewalls de segurança de redes surgiram no início dos anos 90. Eram dispositivos que possuíam um pequeno conjunto de regras do tipo: Alguém da rede A pode acessar a rede B, ou alguém da rede C não pode acessar a rede B. Esses firewalls eram efetivos, mas bastante limitados. Como exemplo, era muito difícil configurar as regras corretamente."* Walsh W. *(1997)*

1.2 O Gênesis do Firewall

1.2.1 A Primeira Geração - Filtro e Pacotes

Utiliza filtros de pacotes, controla somente a origem e o destino dos pacotes das mensagens mais rápido, atualmente, essa função pode ser implementada na maioria dos roteadores e é transparente para os usuários, as regras para aceitar ou recusar um pacote baseiam-se nas informação dos cabeçalhos dos pacotes de endereço ip de origem e destino, utiliza protocolo encapsulado (tcp, udp, icmp, etc) e porta tcp/udp de origem e destino, os tipo de mensagem icmp e screeningrouter (roteadorexaminador).

Podemos avaliar algumas vantagens como baixo custo, boa performance e ao mesmo tempo identificar as desvantagens que seriam função fácil de ser contornada com o uso de spoofing[1], outro problema é que roteadores não examinam todas as camadas de um pacote, não sendo capaz de decisões sofisticadas sobre conteúdo.

1.2.2 Segunda Geração - os Gateways e Proxys

Os gateways conectam as redes corporativas à internet através de estações seguras rodando aplicativos especializados para filtrar dados que permitem que usuários se comuniquem com os sistemas seguros através de um proxy que se dividem em duas categorias:

Gateways de circuito.

Usam as conexões tcp/ip como proxy(camada de sessão do modelo osi ou transporte no tcp/ip), de forma que toda a comunicação com a internet seja realizada por meio do gateway, não realiza qualquer filtragem ou processamento de pacotes individualmente.

Gateways de aplicações.

Examinam a comunicação entre as aplicações ip, pode oferecer um serviço, mas bloquear alguns comandos, impede tentativas de spoofinge permite o uso chaves de segurança, como senhas e pedidos de serviço, uma aplicação especial (servidor proxy) é

instalada no gateway para cada serviço desejado.

Podemos avaliar algumas vantagens como, oculta informações sobre a rede interna, oferece controle completo sobre cada serviço e permite analisar os conteúdos dos pacotes para verificar se são apropriados (pornografia) e seguros e a desvantagem sera acabar com a transparência para o usuário, pois os proxies introduzem perda de performance na rede, devido ao fato dos serviços serem processados duas vezes, no agente proxye e no servidor interno.

1.2.3 Terceira Geração, Statefulmulti-Layerinspection (Smli).

A tecnologia smli aplica o conceito de inspeção total de várias camadas do modelo osi, desde a rede (3) até a aplicação (7) e transporte , sem necessidade de processar a mensagem, usa algoritmos otimizados de verificação de dados na camada de aplicação, enquanto os pacotes são simultaneamente comparados a padrões conhecidos de pacotes amigáveis.

Podemos avaliar algumas vantagens como, oferece a velocidade de um filtro de pacotes com a segurança de um gatewayde aplicações porem a desvantagens seria expor os endereços ip das máquinas internas à rede, o que pode ser contornado com a adição de servidores proxy em conjunto.

1.2.4 A Necessidade de um Firewall

Sobre o Firewall , Segundo Ford L. (2002)

> *"A interner é uma mina de ouro de informações e oportunidades. Infelizmente tambem tem se tornado um campo de caça para individuos inescrupulosos com as ferramentas e o conhecimento para invadir seu computador e rouber suas informações financeiras e pessoais ou que simplismete se divertem com piadas sem imaginação ou causando danos deliberadamente a sistemas corporativo e compuatadores de outras pessoas."*

"*Uma dos grandes riscos para uma rede interna é o próprio usurário"*. Marcos A, Pitanga C. (2003).

O usuário por não conhecer ou negligenciar as regras internas de sua empresa ou

mesmo interessado em comprometer a segurança interna, expõe assim ao risco toda estrutura de segurança da rede e política traçada a ela.

Capítulo 2 Invasores e Taxonomias de Ataque

2.1 Crakers e Hackrs

2.1.1 Tipos de Invasores

Existe uma comunidade, uma cultura compartilhada, de programadores experts e gurus de rede cuja história remonta há décadas atrás, desde os primeiros minicomputadores de tempo compartilhado e os primeiros experimentos na ARPAnet. Os membros dessa cultura deram origem ao termo "hacker". Hackers construíram a Internet. Hackers fizeram do sistema operacional Unix o que ele é hoje. Hackers mantém a Usenet. Hackers fazem a World Wide Web funcionar. Se você é parte desta cultura, se você contribuiu a ela e outras pessoas o chamam de hacker, você é um hacker, Existe outro grupo de pessoas que se dizem hackers, mas não são. São pessoas (adolescentes do sexo masculino, na maioria) que se divertem invadindo computadores e fraudando o sistema telefônico. Hackers de verdade chamam essas pessoas de "crackers", e não tem nada a ver com eles. Hackers de verdade consideram os crackers preguiçosos, irresponsáveis, e não muito espertos, e alegam que ser capaz de quebrar sistemas de segurança torna alguém hacker tanto quanto fazer ligação direta em carros torna alguém um engenheiro automobilístico. Infelizmente, muitos jornalistas e escritores foram levados a usar, erroneamente, a palavra "hacker" para descrever crackers; isso é muito irritante para os hackers de verdade. A diferença básica é esta: “hackers constroem coisas, crackers as destroem”.

- **Scripti kiddies**

O script kiddie nada mais é do que alguém procurando por um alvo fácil. Este alguém não procura por informações ou companhias específicas. O seu objetivo é obter acesso à conta do administrador de uma máquina root[1] da maneira mais fácil possível. Assim, a técnica utilizada consiste em focalizar as ações em um pequeno número de falhas (exploits) e procurar pela Internet inteira, até que se consegue encontrar uma máquina que seja vulnerável, o que acontece mais cedo ou mais tarde. Alguns deles são usuários avançados, que desenvolvem suas próprias ferramentas e deixam para trás backdoors[2] sofisticadas. Outros sabem apenas superficialmente o que estão fazendo e limitam-se a digitar "go" na linha de comando. Embora o nível técnico deles possa diferir, todos usam uma estratégia comum: procurar, alternadamente, por falhas específicas, para que, mais a frente, elas possam ser exploradas.

- **Lammer**

Pouco conhecedor de sistemas é um repetidor de fórmulas de invasão assim como o Scripti kiddies, muitas vezes pego por sua arrogância onde deixa pichações eletrônicas e faz questão de afirma que foi ele que invadiu ou alterou algum layout de pagina na web.

- **Craker:**

O guru aquele que alem de ter conhecimentos profundos de um sistema por ter sido um hacker antes, conhece bastante de linguagem de maquina “assembler “e linguagem de programação em “C” dos sistemas operacionais como Unix e Windows, seu objetivo é conquistar uma informação sendo totalmente invisível na chegada e na saída sem ser percebido.

- **Carder**

Seu foco é o roubo de senhas de cartão de credito e troca de informações , vem sendo bastante combatido pela policia federal em tem seu numero aumentando cada vez mais no Brasil.

- **Pheaker**

Muito raro no nosso pais, por ser um individuo bastante conhecedor de sistemas de telefonia fixa e celular, utiliza seu conhecimento para gerar ligações internacionais sem nenhum custo para si, utilizando os sistemas de telefonia existente, sua especialidade é burlar sistemas telefônicos clonar linhas para roubar informações de usuários, um dos principais Pheakers kelvin Mitinick capturado e preso pelo FBI pelos mesmos crimes, embora confundido com um hacker erroneamente.

2.1.2 Técnicas mais Utilizadas para Invasão

“Após escolhido o alvo os ataques são definidos de acordo com a coleta de informações e fragilidades dos sistemas." Welch A, Deamon D (2002), assim apresentamos algumas taxonomias de ataque.

- **Fin scan, Ataque de captura ou levantamento de informações do alvo.**

Esse tipo de scanner utiliza um recurso muito interessante que parte do principio que as portas fechadas respondem com um RESET (reiniciar), e as portas abertas não enviam flag (sinalização) algum. Esta é uma das técnicas preferidas para o chamado modo stealh (oculto) de levantamento de informações.

- **Ataque de paralisação ou Sobrecarga de solicitações.**

Denial of service - De acordo com a definição do CERT (Computer Emergency Response Team), os ataques Dos (Denial of Service), também denominados Ataques de Negação de Serviços, consistem em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador. Para isso, são usadas técnicas que podem: sobrecarregar uma rede a tal ponto em que os verdadeiros usuários dela não consigam usá-la; derrubar uma conexão entre dois ou mais computadores; fazer tantas requisições a um site até que este não consiga mais ser acessado; negar acesso a um sistema ou a determinados usuários.

- **Ataque de comprometimento**

Buffer overflow, os programas que manipulam variáveis necessitam de buffers, que são áreas de memória onde são armazenados dados que estas mesmas variáveis recebem. Esta área normalmente é limitada e quando, em um determinado momento, há um estouro desta área por um excesso de informação ocorre o Buffer overflow.

Capítulo 3 Requisitos e Primícias na Escolha do Firewall

3.1 Escolhendo os Melhores Requisitos para um Firewall

3.1.1 Conhecendo Requisitos e Primícias nas Escolha de um Bom Firewall

Neste módulo Será apresentado como selecionar um Firewall adequado para a rede interna. Ele apresenta as diferentes classes de Firewall disponíveis e destaca os principais recursos. Ele também descreve as diretrizes de design que permitem determinar os seus próprios requisitos e selecionar o produto mais adequado, aplicando-se as tecnologias a seguir.

- **Produtos de firewall baseados em Ethernet/IP.**

Para entender este módulo, é necessário compreender sobre o protocolo TCP/IP e sobre a sua arquitetura de rede. Também é útil saber qual tráfego de entrada e saída que passa pelo firewall interno pode ser considerado válido e qual é inválido.

As diretrizes de design apresentadas neste módulo irão ajudá–lo a selecionar os recursos do firewall necessários, considerando os aspectos mais importantes, como crescimento e custo. Além disso, este módulo define diferentes classes de firewalls e, ao usar as diretrizes de design, você poderá selecionar a classe mais adequada para atender a seus requisitos. A partir das informações contidas neste módulo e da terminologia técnica, você poderá conversar com fabricantes de firewalls sobre os produtos que eles podem fornecer e avaliar a adequação deles a seus requisitos.

- **Diretrizes do design**

Este módulo considera os requisitos para um firewall interno em uma rede corporativa, os tipos de dispositivos que podem atender a esses requisitos e as opções disponíveis para a implantação. Infelizmente, as invasões em redes de usuários internos e externos têm se tornado um evento regular, o que significa que as empresas devem instalar uma proteção. O firewall tem o seu preço e cria um obstáculo ao fluxo do tráfego. Por isso, você deve certificar–se de que o firewall tenha sido criado para ser o mais econômico e eficiente possível.

- **Arquitetura de rede**

Geralmente, a arquitetura de rede de uma empresa possui três zonas as quais serão apresentadas a seguir.

- **Rede de limite**

Essa rede está voltada diretamente para a Internet por meio de um roteador que fornece uma camada de proteção inicial na forma de filtragem básica de tráfego de rede. Ela alimenta dados pela rede de perímetro por meio de um firewall de perímetro.

- **Rede de perímetro**

Essa rede geralmente chamada de DMZ (zona desmilitarizada) ou rede de borda, vincula usuários de entrada a servidores Web ou a outros serviços. Em seguida, os servidores Web os vinculam às redes internas por meio de um firewall interno.

- **Redes internas**

As redes internas vinculam os servidores internos, como o SQL Server e os usuários internos. Em uma empresa, normalmente existem dois firewalls diferentes: — o firewall de perímetro e o firewall interno. Embora as tarefas desses firewalls sejam semelhantes, a ênfase dada é diferente, já que o firewall de perímetro concentra–se no fornecimento de uma limitação aos usuários externos não confiáveis, enquanto o firewall interno se concentra em impedir que os usuários externos acessem a rede interna e em limitar as atividades dos usuários internos. Para obter mais informações sobre o design de firewall de perímetro, consulte "Design de firewall de perímetro".

As redes estão descritas na Figura 1

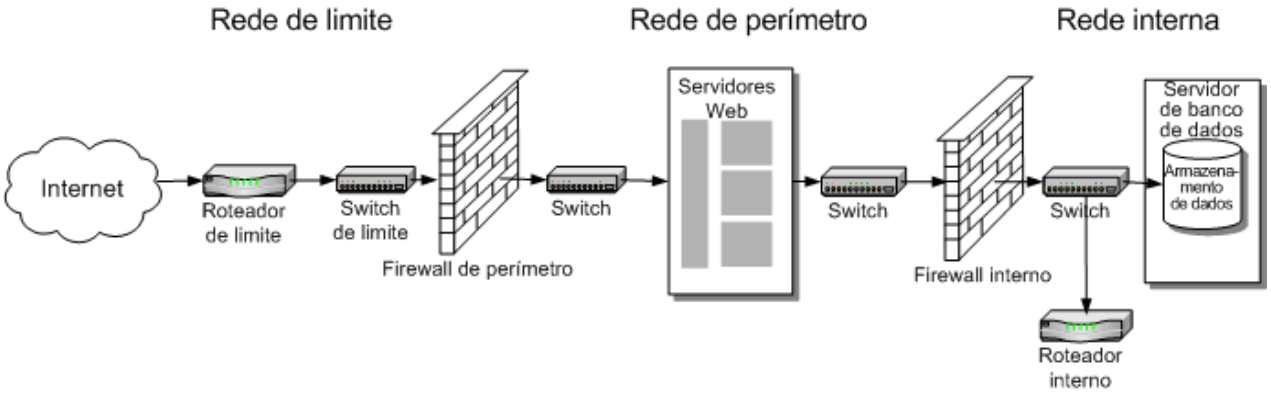

Figura 1: Arquitetura de rede de uma empresa
Fonte: Microsoft 2007

Ao se desenvolver um software é necessária à utilização de um destes modelos de processos, e esta escolha envolve vários fatores, que vai desde onde o software será aplicado, como será aplicado e até como será comercializado. Mas, seja qual for o modelo escolhido,

ele terá de determinar quais as atividades devem ser desenvolvidas, como serão executadas, quando serão e por quem. Comparando todos estes modelos, verifica-se que, mesmo apresentando denominações diferentes e estarem associados a paradigmas de desenvolvimentos distintos, todos eles apresentam características semelhantes nas atividades que serão desenvolvidas em cada modelo.

- **Entradas do design**

O firewall verifica os pacotes IP que chegam e bloqueia os que detecta como invasores. Alguns bloqueios podem ser feitos reconhecendo, por padrão, que determinados pacotes são ilegais. Uma outra opção é configurar o firewall para bloquear determinados pacotes. O protocolo TCP/IP foi criado há muitos anos, sem qualquer conceito de entrada ilegal ou invasão de computadores, portanto, possui muitos pontos fracos. Por exemplo, o protocolo ICMP foi projetado para ser um mecanismo de sinalização no TCP/IP, no entanto, está vulnerável a abusos, podendo ter problemas, como ataques DoS (Negação de Serviço).

Um Firewall interno possui requisitos mais precisos que um firewall de perímetro. Isso ocorre porque é mais difícil controlar o tráfego interno, uma vez que o seu destino legítimo pode ser qualquer servidor na rede interna.

Existem muitos tipos de firewall, diferenciados, em parte, pelo preço, mas também pelos recursos e pelo desempenho. Geralmente, o firewall mais caro é o que possui maior capacidade e mais recursos. Posteriormente, neste módulo, os firewalls serão agrupados em classes para serem diferenciados, no entanto, antes de escolher um firewall, você deve identificar quais são as suas necessidades. Observe as considerações a seguir:

- **Orçamento**

Qual é o orçamento disponível? Todos os firewalls do ambiente de rede devem oferecer um serviço da mais alta qualidade e ser, ao mesmo tempo, econômicos. No entanto, esteja ciente de como a sua empresa pode ser prejudicada se o firewall for muito limitado pelo fator preço. Considere o custo do tempo de inatividade na sua empresa caso o serviço seja suspenso devido a um ataque de negação de serviço.

- **Recursos existentes**

Existem recursos existentes que possam ser usados para reduzir custos? Talvez já existam firewalls no ambiente que possam ser reutilizados e roteadores que possam ter um conjunto de recursos de firewall instalado.

- **Disponibilidade**

A sua empresa precisa que o firewall esteja permanentemente disponível? Se você oferecer um recurso de servidor Web público que precise estar sempre disponível, será necessário que o firewall funcione ininterruptamente. Independentemente do firewall, sempre há uma probabilidade de falha. Então, como você pode minimizar esse problema? A disponibilidade de um firewall pode ser melhorada por meio de dois métodos:

- **Componentes redundantes**

A duplicação de alguns componentes com maior probabilidade de falha, como a fonte de alimentação, aumenta a resistência do firewall, uma vez que seu funcionamento não é afetado mediante a falha de um componente. Normalmente, os firewalls de baixo custo não dispõem de opções redundantes, pois estas, além de caras, não acrescentam nada ao seu poder de processamento.

Dispositivos duplicados: A duplicação do dispositivo do firewall proporciona um sistema totalmente resistente, mas novamente a um custo considerável, uma vez que ele também exige um cabeamento de rede totalmente duplicado e conectividade dupla nos roteadores ou switches aos quais o firewall se conecta. No entanto, dependendo do firewall, é possível duplicar a taxa de transferência para compensar. Teoricamente, todos os firewalls, do menor ao maior, podem ser duplicados, mas na prática é necessário um mecanismo de alternância de software que firewalls menores podem não conter.

- **Escalabilidade**

Quais são os requisitos de taxa de transferência dos firewalls? A taxa de transferência pode ser considerada em termos de bits por segundo e de pacotes transferidos por segundo. Se esta for a primeira vez que você lida com isso, talvez não saiba quais são as taxas de transferência e, mesmo que tudo dê certo, a taxa de transferência da Internet pode aumentar

rapidamente. Como você poderá lidar com um aumento? Você deve selecionar uma solução de firewall que possa aumentar de acordo com o aumento da taxa de transferência. O firewall pode aumentar com a adição de mais componentes ou você pode instalar outro firewall paralelamente?

- **Recursos necessários**

São necessários quais recursos de firewall? Com base em avaliações de risco relativas aos serviços prestados na empresa, você pode determinar quais tipos de recurso de firewall são necessários para proteger seus computadores. Há necessidade de VPNs (Redes Virtuais Privadas), já que o design é afetado?

3.1.2 Defesa e Ataques Contra o Sistema

Esta seção apresenta um resumo dos ataques ao sistema mais conhecidos, juntamente com as razões para usar o serviço do firewall como uma primeira linha de defesa.

- **Ataques externos**

Com freqüência, a Internet é usada como ferramenta por pessoas que desejam prejudicar empresas ou roubar segredos comerciais para obter vantagem competitiva. Se você instalar um firewall de perímetro e verificar o log de invasões, ficará surpreso pelo volume. A maioria das invasões é apenas para ver se a máquina responde e quais serviços estão sendo executados. Isso pode parecer inofensivo, mas se o atacante descobrir a sua máquina, ele poderá atacar o seu serviço e identificar seus pontos fracos.

- **Ataques internos**

Nem todos os ataques são provenientes da Internet. Você também deve proteger dados sigilosos de usuários internos que estão na rede corporativa. A maioria das empresas possui

dados sigilosos que devem ser protegidos contra determinados usuários na rede interna, inclusive funcionários, fornecedores, empreiteiros e clientes.

- **Ameaças de invasão**

As ameaças de invasão podem tomar muitas formas, e descrevê–las aqui serviria apenas a uma finalidade restrita, pois são criadas ameaças novas todos os dias. Algumas invasões, como efetuar ping em um endereço de servidor, podem parecer inofensivas. No entanto, depois de descobrir a presença de um servidor, o Cracker poderá tentar um ataque mais sério. Isso significa que todas as invasões devem ser consideradas potencialmente prejudiciais. Eis algumas das principais invasões:

- **Sniffers de pacotes**

Um sniffer é um aplicativo de software ou um dispositivo de hardware que se conecta à LAN e captura informações de quadros Ethernet. A intenção original desses sistemas foi solucionar problemas e analisar o tráfego da Ethernet ou investigar detalhadamente os quadros para examinar pacotes IP individuais. Os sniffers operam em modo promíscuo, ou seja, eles escutam todos os pacotes que passarem pelo cabo físico. Muitos aplicativos, como o Telnet, enviam informações sobre nome de usuário e senha em texto não criptografado que pode ser exibido pelos sniffers. Isso significa que um hacker pode acessar muitos aplicativos utilizando um sniffer.

A ação do sniffer não pode ser impedida por um firewall, uma vez que ele não gera tráfego de rede, e muitos dos invasores que podem estar utilizando um sniffer são os seus próprios usuários, dentro de um firewall. É possível baixar facilmente um software sniffer grátis pela Internet, e seus usuários podem executá–lo em PCs, examinando os pacotes à medida que passam. Se você estiver executando sistemas operacionais Microsoft® Windows® nos PCs, normalmente os usuários irão precisar de direitos de acesso de administrador para executar um sniffer, o que limita o número de usuários que podem tentar uma ação como essa. No entanto, os usuários com direitos de administrador, que podem ser muitos, conseguem executar um sniffer. Além do acesso a dados confidenciais, eles podem ver senhas em texto não criptografado, como mencionado anteriormente. Como muitas

pessoas usam a mesma senha para os aplicativos, os invasores podem deduzir quais serão as senhas codificadas e obter conseguir acesso. Existem várias medidas para combater a ação do sniffer. A principal medida é usar senhas criptografadas (mas este tópico não será abordado neste módulo).

- **Spoofing de IP**

O spoofing de IP ocorre quando o endereço de origem de um pacote IP é alterado para ocultar a identidade do remetente. O roteamento na Internet usa apenas o endereço de destino para enviar um pacote, ignorando o endereço de origem. Por isso, um hacker consegue enviar um pacote destrutivo para o seu sistema, ocultando a origem para que você não saiba de onde ele veio. O spoofing não é necessariamente destrutivo, mas sinaliza que uma invasão está próxima. O endereço pode estar fora de sua rede (para ocultar a identidade do invasor) ou pode ser um de seus endereços internos confiáveis com acesso privilegiado. O spoofing, em geral, é usado por ataques de negação de serviço, descritos posteriormente neste módulo.

- **Ataques de negação de serviço:**

Os ataques de DoS (negação de serviço) são um dos mais difíceis de evitar. Eles são diferentes dos outros tipos de ataque porque não causam dano permanente à rede. Em vez disso, eles tentam interromper o funcionamento da rede, bombardeando um computador específico (dispositivo de servidor ou de rede) ou degradando a taxa de transferência de conexões de rede até chegar ao ponto em que o desempenho é tão lento, que provoca irritação dos clientes e a perda de negócios para a empresa. O DDoS (ataque de negação de serviço distribuído) é um ataque iniciado em vários computadores, que concentra o bombardeamento no seu sistema. Os computadores de ataque não iniciam o ataque sozinho, mas se infiltram devido à vulnerabilidades em sua própria segurança.

- **Ataques contra a camada de aplicativo**

Os ataques à camada de aplicativo normalmente são os mais divulgados e, geralmente, aproveitam os pontos fracos já conhecidos de aplicativos, como em servidores Web e de bancos de dados. O problema, particularmente para os servidores Web, é que eles são criados para serem acessados por usuários públicos desconhecidos e não confiáveis. A maioria dos

ataques é feita contra deficiências já conhecidas no produto. Isso significa que a melhor defesa é instalar as últimas atualizações dos fabricantes. O terrível worm Slammer do SQL (Structured Query Language) afetou 35.000 sistemas em muito pouco tempo desde seu lançamento em janeiro de 2003. O worm explorou um problema conhecido no Microsoft® SQL Server™ 2000, para o qual a Microsoft tinha emitido uma correção em agosto de 2002. Esse worm aproveitou o fato de que muitos administradores não haviam aplicado a atualização recomendada e não tinham adquirido firewalls adequados (que poderiam descartar os pacotes destinados à porta usada pelo worm). O firewall é apenas uma barreira nessas situações. Os fabricantes recomendam que as atualizações sejam aplicadas a todos os produtos, particularmente para impedir ataques à camada de aplicativo.

- **Varredura de rede**

A varredura de rede é a verificação de redes para descobrir endereços IP válidos, nomes DNS (Sistema de Nome de Domínio) e portas IP antes de se iniciar um ataque. A varredura de rede em si não é prejudicial. No entanto, descobrir quais endereços estão em uso pode ajudar alguém a iniciar um ataque hostil. Se você procurar um firewall nos logs, verificará que a maioria das invasões é dessa natureza. As investigações comuns incluem o exame das portas de escuta dos protocolos TCP e UDP, bem como de outras portas de escuta bastante conhecidas, como as usadas pelo Microsoft SQL Server, NetBIOS, HTTP e por servidores SMTP. Todas essas investigações buscam uma resposta, que informa ao hacker que o servidor existe e executa um desses serviços. Muitos desses exames podem ser impedidos pelo roteador de limite ou um firewall, mas desligar alguns dos serviços pode restringir a capacidade de diagnóstico de rede.

- **Definição do dispositivo**

Um firewall é um mecanismo para controlar o fluxo do tráfego IP entre duas redes. Os dispositivos de firewall costumam operar no L3 do modelo OSI, embora alguns modelos também possam operar em níveis superiores. Um firewall interno, em geral, proporciona os seguintes benefícios: Defender os servidores internos contra ataques de rede. Aplicar restrições às diretivas de uso e acesso à rede. Monitorar o tráfego e gerar alertas ao detectar padrões suspeitos É importante observar que os firewalls reduzem apenas alguns tipos de

riscos de segurança. Um firewall geralmente não evita o dano que pode ser causado a um servidor com uma vulnerabilidade de software . Os firewalls devem ser implementados como parte da ampla arquitetura de segurança de uma empresa.

3.1.3 Recursos de Firewall

Dependendo dos recursos que um firewall pode suportar, o tráfego será permitido ou bloqueado por meio de várias técnicas. Essas técnicas oferecem diferentes graus de proteção com base na capacidade do firewall. Os recursos de firewall a seguir estão listados em ordem crescente de complexidade:

- **Filtros de entrada de adaptador de rede**
- **Filtros estáticos de pacotes**
- **NAT (Conversão de Endereço de Rede)**
- **Inspeção com informações de estado**
- **Inspeção no nível de circuito**
- **Filtragem da camada de aplicativo**

Em geral, os firewalls que oferecem recursos complexos também oferecem suporte para os recursos mais simples. No entanto, você deve ler atentamente as informações do fornecedor ao escolher um firewall, pois podem existir diferenças sutis entre a capacidade implícita e a real de um firewall. A seleção de um firewall normalmente envolve o questionamento sobre os recursos e o teste para garantir que o produto possa de fato ter um desempenho segundo as especificações.

- **Filtros de entrada de adaptador de rede**

A filtragem de entrada do adaptador de rede examina os endereços de origem ou de destino e outras informações no pacote de entrada, assim como bloqueia ou permite que esse pacote prossiga. Essa filtragem aplica–se apenas ao tráfego de entrada e não pode controlar o

tráfego de saída. Ela compara os endereços IP e os números de porta para UDP e TCP, bem como o protocolo do tráfego, TCP, UDP e GRE (Generic Routing Encapsulation). A filtragem de entrada para o adaptador de rede permite uma negação rápida e eficiente de pacotes de entrada padrão que atendem aos critérios configurados no firewall. No entanto, ela pode ser facilmente contornada, uma vez que compara apenas os cabeçalhos do tráfego IP e trabalha com base na hipótese básica de que o tráfego sendo filtrado segue os padrões IP e não é capaz de escapar da filtragem.

- **Filtros estáticos de pacotes**

Os filtros estáticos de pacotes são parecidos com os filtros de entrada de adaptador de rede no sentido de que eles simplesmente fazem correspondência com cabeçalhos de IP para determinar se será ou não permitida a passagem do tráfego pela interface. No entanto, os filtros estáticos de pacotes permitem o controle sobre as comunicações de entrada e de saída com uma interface. Além disso, normalmente os filtros estáticos de pacotes permitem uma função adicional sobre a filtragem do adaptador de rede que é a de verificar se o bit ACK (Acknowledged) está definido no cabeçalho IP. O bit ACK informa sobre a possibilidade de o pacote ser uma solicitação nova ou uma solicitação de retorno de uma solicitação original. Ele não verifica se o pacote foi originalmente enviado pela interface que o recebe, apenas verifica se o tráfego que chega à interface parece ser de retorno com base nas convenções dos cabeçalhos IP.

Essa técnica aplica–se apenas ao protocolo TCP e não ao UDP. Assim como a filtragem de entrada do adaptador de rede, a filtragem estática de pacotes é muito rápida, mas sua capacidade é limitada, podendo ser evitada por um tráfego com habilidades específicas.

- **Conversão de endereço de rede**

No intervalo de endereços IP mundial, determinados intervalos são designados como endereços particulares. Esses intervalos de endereços devem ser usados na empresa e não possuem significado na Internet. Como o tráfego destinado a qualquer um desses endereços IP não pode ser roteado pela Internet, a atribuição de um endereço particular a seus dispositivos

internos oferece–lhes alguma proteção contra invasões. No entanto, esses dispositivos internos freqüentemente precisam acessar a Internet e, por isso, a NAT converte o endereço particular em um endereço da Internet.

Embora a NAT não seja estritamente uma tecnologia de firewall, ocultar o endereço IP real de um servidor impede que os atacantes obtenham informações valiosas sobre o servidor.

- **Inspeção com informações de estado.**

Na inspeção com informações de estado, todo o tráfego de saída é registrado em uma tabela de estado. Quando o tráfego de conexão volta para a interface, a tabela de estado é verificada para garantir que o tráfego tenha sido originado nessa interface. A inspeção com informações de estado é um pouco mais lenta do que a filtragem estática de pacotes. No entanto, ela garante que o tráfego poderá passar apenas se corresponder aos requisitos do tráfego de saída. A tabela de estado contém itens como endereço IP de destino, endereço IP de origem, a porta que está sendo chamada e host originador.

Determinados firewalls podem armazenar mais informações (como os fragmentos IP enviados e recebidos) na tabela de estado enquanto outros armazenam menos. O firewall pode verificar se o tráfego é processado quando todas ou somente algumas informações fragmentadas retornam. Cada fornecedor de firewall implementa o recurso de inspeção com informações de estado de forma diferente. Por isso, você deve ler atentamente a documentação do firewall. O recurso de inspeção com informações de estado geralmente ajuda a reduzir o risco causado pelo reconhecimento de rede e pelo spoofing de IP.

- **Inspeção no nível de circuito.**

Com a filtragem no nível de circuito é possível inspecionar sessões em oposição às conexões ou pacotes. Uma sessão pode incluir várias conexões. Assim como a filtragem dinâmica de pacotes, as sessões são estabelecidas apenas em resposta à solicitação de um usuário. A filtragem do nível de circuito oferece suporte embutido para protocolos com

conexões secundárias, como FTP e fluxo de mídia. Normalmente, ela ajuda a reduzir o risco apresentado pelo reconhecimento de rede, DoS e ataques de spoofing de IP.

- **Filtragem da camada de aplicativo.**

O nível mais sofisticado de inspeção do tráfego de firewall é a filtragem no nível do aplicativo. Filtros de aplicativo de boa qualidade permitem a análise do fluxo de dados de um determinado aplicativo e fornecem um processamento específico ao aplicativo. Esse processamento inclui a inspeção, a triagem ou o bloqueio, o redirecionamento e a modificação de dados à medida que passam pelo firewall. Este mecanismo é usado para proteger contra, por exemplo, comandos SMTP sem segurança ou ataques contra DNS interno. Normalmente, podem ser adicionadas ao firewall ferramentas de terceiros para triagem de conteúdo, como detecção de vírus, análise léxica e categorização de sites.

O firewall na camada de aplicativo pode inspecionar muitos protocolos diferentes com base no tráfego que passa por ele. Diferentemente de um firewall de proxy que em geral inspeciona o tráfego na Internet, como HTTP, download de FTP e SSL, o firewall na camada de aplicativo possui um controle muito maior sobre a maneira como qualquer tráfego passa por ele. Por exemplo, um firewall de camada de aplicativo pode permitir somente a passagem do tráfego de UDP que se origina no limite do firewall. Se for preciso que um host da Internet examine a porta em relação a um firewall com informações de estado para ver se ele permitiu o tráfego DNS no ambiente, o exame da porta provavelmente mostrará que a famosa porta associada ao DNS estava aberta, no entanto, uma vez que o ataque é armado, o firewall com informações de estado recusará as solicitações porque não foram originadas internamente. Um firewall na camada de aplicativo pode abrir portas de forma dinâmica com base na possibilidade de o tráfego se originar internamente.

O recurso do firewall na camada de aplicativo ajuda a reduzir o risco apresentado pelo spoofing de IP, DoS, alguns ataques na camada de aplicativo, reconhecimento de rede e ataques de vírus e cavalos de Tróia. A desvantagem de um firewall na camada de aplicativo é que ele exige uma capacidade de processamento muito maior e, normalmente, são mais lentos na passagem do tráfego do que os firewalls com informações de estado ou de filtragem estática. O mais importante ao usar firewalls na camada de aplicativo é determinar sua atividade nessa camada.

A filtragem de camada de aplicativo é amplamente usada para proteger os serviços

expostos publicamente. Se a sua empresa possuir uma loja online que coleta números de cartão de crédito e outras informações pessoais sobre os clientes, será prudente tomar as precauções de mais alto nível para proteger esses dados. O recurso de camada de aplicativo garante que o tráfego que está passando por uma porta seja apropriado. Diferentemente dos firewalls de filtro de pacote ou de inspeção com informações de estado, que simplesmente verificam a porta e os endereços IP de origem e de destino, os firewalls que oferecem suporte ao recurso de filtragem de camada de aplicativo podem inspecionar os dados e os comandos que passam de um lado para o outro.

A maioria dos firewalls que oferecem suporte ao recurso de camada de aplicativo possui apenas a filtragem de camada de aplicativo para o tráfego de texto não criptografado, como um serviço de mensagens com reconhecimento de proxy, HTTP e FTP. É importante lembrar que um firewall que oferece suporte a esse recurso pode controlar o tráfego que entra e sai do ambiente. Outra vantagem desse recurso é a capacidade de inspecionar o tráfego DNS para que procure comandos específicos ao DNS à medida que passa pelo firewall. Essa camada adicional de proteção garante que os usuários ou os invasores não irão dissimular informações em tipos de tráfego permitidos.

Esta fase determina como realizar as funções do software . Aspectos como a arquitetura do software, as estruturas de dados, os procedimentos a serem implementados, a forma como o projeto será transformado em linguagem de programação, a geração de código e os procedimentos de teste devem ser encaminhados nesta fase.

3.1.4 Classes de Firewall

A seção a seguir apresenta várias classes de firewalls, cada uma fornecendo determinados recursos de firewall. É possível usar classes de firewall específicas para responder a solicitações específicas no design de uma arquitetura de TI.

O agrupamento de firewalls em classes permite a abstração do hardware em relação às solicitações do serviço. As solicitações de serviço podem ser comparadas aos recursos da classe. Contanto que um firewall se encaixe em uma classe específica, ele poderá oferecer suporte a todos os serviços dessa classe de firewalls.

As diversas classes são as seguintes:

- ***Classe 1 – Firewalls pessoais***
- ***Classe 2 – Firewalls de roteador***
- ***Classe 3 – Firewalls de hardware low–end***
- ***Classe 4 – Firewalls de hardware high–end***
- ***Classe 5 – Firewalls de servidor high–end***

É importante compreender que há sobreposição de algumas dessas classes. Isso ocorre naturalmente porque a sobreposição permite que um tipo de solução de firewall estenda várias classes. Muitas classes também podem ser atendidas por mais de um modelo de hardware do mesmo fornecedor, de modo que a empresa possa escolher um modelo adequado às suas necessidades atuais e futuras. Além do preço e do conjunto de recursos, os firewalls podem ser classificados com base no desempenho (ou taxa de transferência). No entanto, os fabricantes não fornecem nenhum dado de taxa de transferência para a maioria das classes de firewalls. Nos locais em que eles são fornecidos (geralmente para dispositivos de firewall de hardware), nenhum processo de medida padrão é adotado, o que dificulta a comparação entre os fabricantes. Por exemplo, uma medida é o número de bps (bits por segundo), mas como o firewall na verdade está transportando pacotes IP, essa medida não terá sentido se o tamanho do pacote usado para medir a taxa não for incluído.

3.1.5 Classe 1 - Firewall Pessoal

Um firewall pessoal é definido como um serviço de software executado em um sistema operacional que oferece ao PC (Computador Pessoal) a capacidade de um firewall simples. Com o crescimento do número de conexões permanentes com a Internet (em oposição às conexões dial–up), o uso de firewalls pessoais aumentou.

Embora o firewall pessoal tenha sido criado para proteger um único computador pessoal, ele também é capaz de proteger uma rede pequena, se o computador no qual ele

estiver instalado compartilhar a conexão de Internet com outros computadores da rede interna.

No entanto, o desempenho de um firewall pessoal é limitado e degradará o desempenho do computador pessoal no qual se encontra instalado. Os mecanismos de proteção normalmente são menos eficientes do que uma solução de firewall dedicada, pois eles, em geral, se limitam a bloquear endereços IP e de porta, embora a necessidade de proteção em um computador pessoal seja menor.

Os firewalls pessoais podem vir gratuitamente em um sistema operacional ou a um custo muito baixo. Eles são adequados para a finalidade pretendida, mas não devem ser considerados para uso corporativo, mesmo que para pequenas filiais satélite, devido à limitação de desempenho e funcionalidade. No entanto, eles são ideais para usuários móveis em computadores laptop.

A tabela a seguir mostra os recursos que podem estar disponíveis em firewalls pessoais. Eles podem variar muito no que se refere a capacidade e preço. No entanto, a falta de um recurso específico, especialmente em um laptop, pode não ter muita importância.

- **Firewalls pessoais**

Recursos básicos que contam com suporte onde a maioria dos firewalls pessoais tem suporte para filtros estáticos de pacotes, nat e de inspeção com informações de estado, enquanto alguns têm suporte para filtragem de inspeção no nível de circuito ou na camada de aplicativo, sua configuração é automática (opção manual também disponível), pode bloquear ou permitir endereços ip, números de protocolo ou de porta mensagens icmp de entrada, controlar o acesso de saída, alguns possuem proteção do aplicativo alem de alertas audíveis ou visíveis, arquivo de log de ataques e depende do produto alertas em tempo real, geralmente não dão suporte a vpn nem gerenciamento remoto o suporte do fabricante varia muito (depende do produto) não possui opção de alta disponibilidade e seu número de sessões simultâneas suporta de 1 a 10 com uma capacidade de atualização modular (hardware ou software), sua faixa de preço é acessível (gratuito em alguns casos)

- **Vantagens**

As vantagens dos Firewalls pessoais são

- **Preço acessível:**

Quando for necessário apenas um número limitado de licenças, os firewalls pessoais

serão uma opção econômica. Um firewall pessoal está integrado a versões do Windows XP.

Produtos adicionais que funcionam com outras versões do Windows ou outros sistemas operacionais estão disponíveis gratuitamente ou a um preço acessível.

Fáceis de configurar

Os produtos de firewall pessoal tendem a ter configurações básicas que funcionam facilmente, com opções de configuração simples e diretas.

- **Desvantagens**

Difíceis de gerenciar de modo centralizado Os firewalls pessoais precisam ser configurados em cada cliente, o que adiciona sobrecarga ao gerenciamento.

A configuração tende a ser uma combinação de filtragem estática de pacotes e bloqueio baseado em permissões somente de aplicativos.

Limitações de desempenho

Os firewalls pessoais são criados para proteger um único PC. Usá–los em um computador pessoal que serve como roteador para uma pequena rede levará a uma degradação do desempenho.

3.1.6 Classe 2 - Firewall de Roteador

Os roteadores geralmente oferecem suporte a um ou mais recursos de firewall abordados anteriormente; eles podem ser subdivididos em dispositivos low–end criados para conexões com a Internet e em roteadores tradicionais high–end. Os roteadores low–end oferecem recursos básicos de firewall para bloquear e permitir endereços IP específicos e números de portas, bem como usar NAT para ocultar endereços IP internos. Eles geralmente oferecem o recurso de firewall como padrão, otimizado para bloquear invasões da Internet e, embora não precisem de configuração, eles podem ser refinados com mais configurações.

Os roteadores high–end podem ser configurados para restringir o acesso impedindo as invasões mais óbvias, como os pings, e implementando outras restrições de endereço IP e de porta por meio do uso de ACLs (Listas de Controle de Acesso). Outros recursos de firewall podem estar disponíveis para proporcionar uma filtragem de pacote com informações de estado em alguns roteadores. Em roteadores high-end, a capacidade do firewall é semelhante

ao de um dispositivo de firewall de hardware, a um custo menor, porém, também com baixa taxa de transferência.

- **Recursos Técnicos**

Recursos básicos que contam com suporte e a maioria dos firewalls de roteador oferecem suporte e filtros estáticos de pacotes. Normalmente, os roteadores low-end têm suporte para nat, e os roteadores high-end podem ter suporte para a filtragem de inspeção com informações de estado ou na camada de aplicativo, sua configuração geralmente é automática em roteadores low-end (com opções manuais). Freqüentemente manual em roteadores high-end pode bloquear ou permitir endereços ip, números de protocolo ou de porta mensagens icmp de entrada controlar o acesso de saída alguns possuem proteção do aplicativo geralmente alertas audíveis ou em muitos casos arquivo de log de ataques, alertas em tempo real suporte para vpn em roteadores low-end, não tão comum em roteadores high-end. há disponibilidade de servidores ou dispositivos separados. dedicados a esta tarefa.

Possui gerenciamento remoto, o suporte do fabricante normalmente limitado em roteadores low-end e bom em roteadores high-end. com opção de alta disponibilidade, número de sessões simultâneas entre 10 e1.000, capacidade de atualização modular (hardware ou software) limitado faixa de preço baixo a alto.

- **Vantagens**

As vantagens dos firewalls de roteador são:

- **Solução de baixo custo:**

A ativação de um recurso de firewall de roteador existente não pode adicionar nenhum custo ao preço do roteador e não requer hardware adicional

A configuração pode ser consolidada .A configuração de firewalls de roteador pode ser realizada quando o roteador for configurado para operações normais, minimizando assim o esforço de gerenciamento. Essa solução é ideal para escritórios satélite, já que o hardware de rede e o gerenciamento são simplificados.

- **Proteção do investimento**

A configuração e o gerenciamento de firewalls de roteador são conhecidos pela equipe operacional, não exigindo um novo treinamento. O cabeamento da rede é simplificado porque nenhum outro hardware foi instalado, o que também simplifica o gerenciamento da rede.

- **Desvantagens**

As desvantagens dos firewalls de roteador são: Funcionalidade limitada em geral, os roteadores low–end oferecem somente recursos básicos de firewall. Normalmente, os roteadores high–end oferecem recursos de firewall de nível superior, porém, pode ser necessária uma configuração significativa. Muito dessa configuração se faz pela adição de controles que são facilmente esquecidos, dificultando, de alguma forma, a configuração correta.

- **Possuem somente controle básico**

A configuração tende a ser uma combinação de filtragem estática de pacotes e bloqueio baseado em permissões somente de aplicativos.

- **Impacto no desempenho**

O uso de um roteador como um firewall prejudica o desempenho do roteador e torna a função de roteamento lenta, o que é sua principal tarefa.

Desempenho do arquivo de log

O uso de um arquivo de log para capturar atividades incomuns pode reduzir drasticamente o desempenho do roteador, especialmente quando ele já estiver sendo atacado.

3.1.7 Classe 3 - Firewall de Hardware Low–End

No ponto mínimo do mercado de firewall de hardware encontram–se as unidades Plug and Play, exigindo uma configuração menor ou nenhuma configuração. Esses dispositivos freqüentemente incorporam uma funcionalidade de switch e/ou de VPN. Os firewalls de hardware low–end são adequados para as pequenas empresas e para uso interno em empresas maiores. Eles costumam oferecer recursos de filtragem estática e funcionalidade básica de gerenciamento remoto. Os dispositivos oferecidos por fabricantes maiores podem executar o mesmo software que os dispositivos high–end, proporcionando um caminho de atualização, caso necessário.

- **Recursos Técnicos**

Recursos básicos que contam com suporte onde a maioria dos firewalls de hardware low–end tem suporte para filtros estáticos de pacotes e nat e pode ter suporte para a filtragem

de inspeção com informações de estado e/ou na camada de aplicativo.

Configuração automática (opção manual também disponível) pode bloquear ou permitir endereços ip, números de protocolo ou de porta mensagens icmp de entrada. Possui controle de acesso de saída e geralmente não possui proteção do aplicativo, alertas audíveis ou visíveis, arquivo de log de ataques, alertas em tempo real, pode fornecer suporte para vpn, gerenciamento remoto e tem suporte do fabricante limitada. Geralmente não possui opção de alta disponibilidade disponível, número de sessões simultâneas entre 10 e 7500 e limitada capacidade de atualização modular (hardware ou software) sua faixa de preço e acessível

- **Vantagens**

As vantagens dos firewalls de hardware low–end são:

Baixo custo :Os firewalls low–end podem ser adquiridos por um baixo custo

Configuração simples: Quase nenhuma configuração é necessária

- **Desvantagens**

As desvantagens dos firewalls de hardware low–end são:

Funcionalidade limitada: Em geral, os firewalls de hardware low–end oferecem somente funcionalidades básicas de firewall. Eles não podem ser executados ao mesmo tempo devido à redundância.

- **Taxa de transferência baixa**

Os firewalls de hardware low–end não foram criados para lidar com conexões com alta taxa de transferência, o que pode causar gargalos.

Suporte limitado do fabricante: Como são itens de baixo custo, o suporte do fabricante costuma ser limitado a Emails e/ou a um site.

- **Capacidade de atualização limitada:**

Geralmente, não pode haver atualizações de hardware, embora normalmente existam atualizações periódicas de firmware disponíveis.

3.1.8 Classe 4 - Firewall de Hardware High–End

No ponto máximo do mercado de firewall de hardware, existem produtos altamente resistentes e de alto desempenho, adequados à empresa ou ao provedor de serviços. Em geral, eles oferecem a melhor proteção, sem afetar o desempenho da rede.

A resistência é alcançada adicionando–se um segundo firewall, executado como uma unidade de espera ativa que mantém a tabela das conexões atuais por meio da sincronização automática com informações de estado.

Redes conectadas à Internet precisam usar firewalls, pois as invasões são constantes. A tentativa de ataques DoS, roubos e corrupção de dados ocorrem o tempo todo. Deve–se considerar a implantação de unidades de firewall de hardware high–end em escritórios centrais ou matrizes.

- **Recursos Técnicos**

Possui recursos básicos que contam com suporte, a maioria dos firewalls de hardware high–end tem suporte para filtros estáticos de pacotes e nat e pode ter suporte para a filtragem de inspeção com informações de estado e/ou na camada de aplicativo. configuração geralmente manual, pode bloquear ou permitir endereços ip, números de protocolo ou de porta, mensagens icmp de entrada, o acesso de saída. proteção do aplicativo potencial, alertas audíveis ou visíveis, arquivo de log de ataques, alertas em tempo real, suporte a vpn, gerenciamento remoto bom suporte do fabricante e opção de alta disponibilidade número de sessões simultâneas entre 7500 e 500.000 com capacidade de atualização modular (hardware ou software) sua faixa de preço é bastante elevado.

- **Vantagens**

As vantagens dos firewalls de hardware high–end são:

- **Alto desempenho**

Os produtos de firewall de hardware foram criados para uma única finalidade e oferecem altos níveis de bloqueio contra invasões, juntamente com uma degradação mínima do desempenho.

- **Alta disponibilidade:**

Os firewalls de hardware high–end podem ser conectados uns aos outros para obter a disponibilidade e o balanceamento de carga ideais.

- **Sistemas modulares:**

O hardware e o software podem ser atualizados de acordo com os novos requisitos. As atualizações de hardware podem incluir portas Ethernet adicionais, ao passo que as atualizações de software podem incluir a detecção de novos métodos contra invasão.

- **Gerenciamento remoto:**

A funcionalidade de gerenciamento remoto dos firewalls de hardware high–end é melhor que a de seus equivalentes low–end

- **Resistência**

Os firewalls de hardware high–end podem ter recursos de disponibilidade e resistência, como o modo de espera ativo com uma segunda unidade.

- **Filtragem de camada de aplicativo:**

Diferentemente dos firewalls low–end, que em geral fazem apenas a filtragem na camada 3 e, possivelmente, na camada 4 do modelo OSI, os firewalls de hardware high–end fornecem filtragem nas camadas de 5 a 7 para os aplicativos já conhecidos.

- **Desvantagens:**

As desvantagens dos firewalls de hardware high–end são:

- **Alto custo**

Os firewalls de hardware high–end costumam ser caros. Embora possam ser adquiridos por $100, o custo de um firewall corporativo é muito superior e, com freqüência, tem como base o número de sessões simultâneas, a taxa de transferência e os requisitos de disponibilidade.

- **Configuração e gerenciamento complexos:**

Como esta classe de firewalls conta com capacidade muito maior do que os firewalls low–end, sua configuração e seu gerenciamento também são mais complexos.

3.1.9 Classe 5 - Firewall de Servidor High–End

Os firewalls de servidor high–end adicionam capacidade de firewall a um servidor high–end,

fornecendo proteção robusta e rápida em sistemas de hardware e software padrão. Esta abordagem se beneficia do uso de hardware ou software conhecido. Isso proporciona um número reduzido de itens de inventário, treinamento e gerenciamento simplificados, confiabilidade e capacidade de expansão. Muitos firewalls de hardware high–end são implementados em plataformas de hardware com padrão de mercado que executam sistemas operacionais padrão (porém ocultos) e, portanto, possuem pouca diferença, tecnicamente e em desempenho, com relação a um firewall de servidor. No entanto, como o sistema operacional ainda está visível, o recurso de firewall de servidor pode ser atualizado e ficar mais resistente por meio de técnicas como o agrupamento.

Como o firewall de servidor é executado em um sistema operacional normalmente usado, é possível adicionar mais software , recursos e funcionalidade ao firewall de vários fornecedores (não de apenas um, como ocorre com o firewall de hardware). O conhecimento do sistema operacional também pode proporcionar uma proteção de firewall mais eficaz, pois para algumas das outras classes é preciso ter bastante experiência para executar a configuração de forma total e correta.

Esta classe é adequada caso haja grande investimento em uma determinada plataforma de hardware ou software , pois usar a mesma plataforma para o firewall simplifica seu gerenciamento. O recurso de cache dessa classe também pode ser muito eficaz.

- **Recursos Técnicos**

Recursos que contam com suporte onde a maioria dos firewalls de servidor high–end tem suporte para filtros estáticos de pacotes e nat e pode ter suporte para a filtragem de inspeção com informações de estado e/ou na camada de aplicativo, configuração geralmente manual, pode bloquear ou permitir endereços ip, números de protocolo ou de porta mensagens icmp de entrada, controlar o acesso de saída potencial proteção do aplicativo, alertas sonoros/visuais e arquivo de log de ataques, alertas em tempo real suporte a vpn, gerenciamento remoto, bom suporte do fabricante e opção de alta disponibilidade, sessões simultâneas acima de 50.000 (em vários segmentos de rede) com capacidade de atualização modular (hardware ou software) faixa de preço elevado.

- **Vantagens**

As vantagens dos firewalls de servidor são:

- **Alto desempenho:**

Quando executados em um servidor de tamanho adequado, esses firewalls podem oferecer altos níveis de desempenho.

- **Integração e consolidação de serviços:**

Os firewalls de servidor podem usar os recursos do sistema operacional no qual são executados. Por exemplo, o software de firewall executado no sistema operacional do Windows Server™ 2003 pode aproveitar a funcionalidade do balanceamento de carga de rede embutida no sistema operacional. Além disso, o firewall pode servir como servidor VPN, usando novamente a funcionalidade do sistema operacional do Windows Server 2003.

- **Disponibilidade, resistência e escalabilidade:**

Como esse firewall é executado em um hardware de PC padrão, ele possui todos os recursos de disponibilidade, resistência e escalabilidade da plataforma do PC no qual é executado.

- **Desvantagens**

As desvantagens dos firewalls de servidor são:

- **Exigem hardware high–end :**

Para obter um alto desempenho, a maioria dos produtos de firewall de servidor exige hardware high–end no que se refere à CPU (unidade de processamento central), memória e interfaces de rede.

- **Suscetíveis a vulnerabilidades:**

Como os produtos de firewall de servidor são executados em sistemas operacionais conhecidos, eles estão suscetíveis às vulnerabilidades presentes no sistema operacional e em outros software s executados no servidor. Embora esse também seja o caso dos firewalls de hardware, seus sistemas operacionais geralmente não são tão conhecidos pelos invasores quanto a maioria dos sistemas operacionais de servidor

3.1.10 Uso do firewall interno

Um firewall interno existe para controlar o acesso a e proveniente da rede interna. Os

tipos de usuário são:

- **Confiáveis:**

Funcionários da empresa, que podem ser usuários internos saindo para a zona de perímetro ou para a Internet; usuários externos, como os funcionários de filiais; usuários remotos ou usuários que trabalham em casa.

- **Parcialmente confiáveis**

Parceiros comerciais da empresa para os quais existe um nível de confiança maior do que para usuários não confiáveis. No entanto, este com freqüência é um nível inferior de confiança do que o existente para os funcionários da empresa.

- **Não confiáveis**

Por exemplo, usuários do site público da empresa, os usuários não confiáveis da Internet devem, teoricamente, acessar apenas os servidores Web na sua zona de perímetro. Caso precisem acessar seus servidores internos para, por exemplo, verificar os níveis de estoque, o servidor Web confiável fará a pesquisa em nome deles. Portanto, os usuários não confiáveis nunca devem ter permissão para ultrapassar o firewall interno.

Há vários pontos que devem ser considerados ao selecionar a classe de firewall a ser usada nessa capacidade. A tabela a seguir realça essas questões.

- **Recursos Técnicos**

Capacidades de firewall necessárias, conforme especificado pelo administrador de segurança em um equilíbrio entre o grau de segurança necessário versus o custo do recurso e a degradação potencial do desempenho que o aumento na segurança pode causar. Enquanto muitas empresas desejam aproveitar a máxima segurança oferecida por um firewall que atende a esta capacidade, outras não querem aceitar a redução no desempenho associada. Para sites que não sejam de comércio eletrônico com volume muito alto, por exemplo, são permitidos níveis inferiores de segurança com base nos níveis superiores de taxa de transferência obtidos pelo uso de filtros estáticos de pacotes em vez da filtragem na camada de aplicativo. O dispositivo será um dispositivo físico dedicado, oferecerá outra funcionalidade ou será um firewall lógico em um dispositivo físico Depende do desempenho exigido, da confidencialidade dos dados e da freqüência da necessidade de acesso pela zona de perímetro. Requisitos da capacidade de gerenciamento para o dispositivo de acordo com o especificado pela arquitetura de gerenciamento da empresa Normalmente, usa–se alguma forma de registro; no entanto, um mecanismo de monitoramento de evento também é necessário. Você pode optar por não permitir a administração remota aqui para impedir que

um usuário mal–intencionado administre o dispositivo remotamente. Os requisitos de taxa de transferência provavelmente serão determinados pelos administradores de rede e de serviços na empresa

Eles irão variar para cada ambiente, mas a capacidade do hardware no dispositivo ou servidor e os recursos de firewall usados irão determinar a taxa geral de transferência de rede. Os Requisitos de disponibilidade Novamente, este ponto depende dos requisitos de acesso dos servidores Web. Se eles devem principalmente manipular as solicitações de informações atendidas pelo fornecimento de páginas da Web, o fluxo para as redes internas será lento. No entanto, altos níveis de disponibilidade serão necessários no caso do comércio eletrônico.

- **Regras para firewall interno**

Os firewalls internos monitoram o tráfego entre as zonas de confiança de perímetro e as internas. Os requisitos técnicos para os firewalls internos são consideravelmente mais complexos do que aqueles para os firewalls de perímetro, devido à complexidade dos tipos de tráfego e dos fluxos entre essas redes.

Esta seção faz referência aos "bastion hosts". Bastion hosts são servidores localizados na rede de perímetro que fornecem serviços a usuários internos e externos. Exemplos de bastion hosts incluem os servidores Web e os servidores VPN. Normalmente, o firewall interno necessitará da implantação das seguintes regras, por padrão ou por configuração:

Bloquear todos os pacotes por padrão.

Na interface do perímetro, bloqueie os pacotes de entrada que parecem ter sido originados a partir de um endereço IP interno para impedir o spoofing.

Na interface interna, bloqueie os pacotes de saída que parecem ter sido originados a partir de um endereço IP externo para restringir um ataque interno.

Permitir consultas baseadas em UDP e respostas dos servidores DNS internos para o bastion host do DNS Resolver.

Permitir consultas baseadas em UDP e respostas do bastion host do DNS Resolver para os servidores DNS internos.

Permitir consultas baseadas em TCP dos servidores DNS internos ao bastion host do DNS Resolver, inclusive as respostas para essas consultas.

Permitir consultas baseadas em TCP do bastion host do DNS Resolver para os servidores DNS internos, inclusive as respostas para essas consultas.

Permitir transferências de zonas entre o bastion host do servidor DNS externo e os hosts de servidores DNS internos.

Permitir Email de saída do servidor de Emails SMTP interno para o bastion host SMTP de saída.

Permitir Email de entrada do bastion host SMTP de entrada para o servidor de Emails SMTP interno

Permitir que o tráfego que se origina no back–end nos servidores VPN alcancem os hosts internos e as respostas retornem para os servidores VPN

Permitir o tráfego de autenticação para os servidores RADIUS na rede interna e que as respostas retornem aos servidores VPN.

Permitir que o acesso de saída da Web dos clientes internos passe por um servidor proxy e as respostas retornem a eles.

Suportar tráfego de autenticação de domínio do Microsoft Windows 2000/2003 entre segmentos de rede tanto para o domínio de perímetro como para o domínio interno.

Suportar pelo menos cinco segmentos de rede.

Realizar inspeção de pacotes com informações de estado entre todos os segmentos de rede que unem (firewall na camada de circuito – camadas 3 e 4).

Suportar recursos de alta disponibilidade como failover com informações de estado

Rotear tráfego por todos os segmentos de rede conectados sem usar a conversão de endereço de rede

- **Requisitos do hardware**

Os requisitos de hardware para um firewall são diferentes para firewalls baseados em software e em hardware, da seguinte forma:

Firewalls baseados em hardware

Esses dispositivos geralmente executam código especializado em uma plataforma de hardware personalizada. Esses firewalls são, em geral, escalados (com preço determinado) com base no número de conexões que podem aceitar e na complexidade do software que devem executar.

3.1.11 Firewalls Baseados em software

Também são configurados com base no número de conexões simultâneas e na complexidade do software de firewall. Existem calculadoras que podem computar a velocidade do processador, o tamanho da memória e o espaço em disco necessário para um

servidor com base no número de conexões suportadas. Você deve considerar outro software que possa ser executado no servidor do firewall, como o software de balanceamento de carga e VPN. Além disso, considere os métodos para colocar o firewall em escala para cima e para fora. Esses métodos incluem o aumento da capacidade do sistema ao adicionar mais processadores, memória e placas de rede e, ainda, ao usar vários sistemas e o balanceamento de carga para espalhar a tarefa do firewall em todos eles. Alguns produtos utilizam o SMP (Multiprocessamento Simétrico) para aumentar o desempenho. O serviço de Balanceamento de carga de rede do Windows Server 2003 pode oferecer tolerância a falhas, alta disponibilidade, eficiência e aprimoramentos no desempenho para alguns produtos de firewall.

- **Disponibilidade**

Para aumentar a disponibilidade do firewall, este pode ser implementado como um único dispositivo de firewall com ou sem componentes redundantes ou como um par redundante de firewalls, incorporando algum tipo de failover e/ou mecanismo de balanceamento de carga. As vantagens e desvantagens dessas opções são apresentadas nas subseções a seguir.

Firewall único sem componentes redundantes

A figura a seguir apresenta a descrição de um firewall único, sem componentes redundantes:

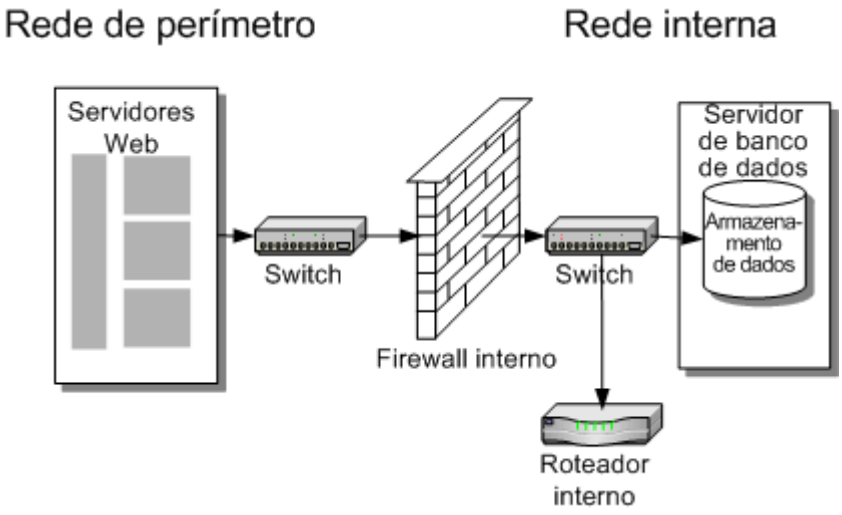

Figura 2: Firewall único, sem componentes redundantes

Fonte: Microsoft 2007

- **Vantagens:**

As vantagens de se ter um firewall único incluem:

- **Baixo custo:**

  Como existe somente um firewall, os custos de hardware e licenciamento são baixos.

  Gerenciamento simplificado:

  O gerenciamento é simplificado, pois há somente um firewall para o site ou para a empresa.

- **Uma única fonte de log:**

  Todo o log de tráfego é centralizado em um dispositivo.

- **Desvantagens**

  As desvantagens de um firewall único sem redundância são:

- **Ponto único de falha:**

  Existe um ponto único de falha para o acesso de entrada e/ou saída.

- **Possibilidade de gargalo no tráfego:**

  Um firewall único poderia causar um gargalo no tráfego, dependendo do número de conexões e da taxa de transferência necessária.

3.1.12 Firewall Único com Componentes Redundantes:

A figura a seguir apresenta a descrição de um firewall único com componentes redundantes:

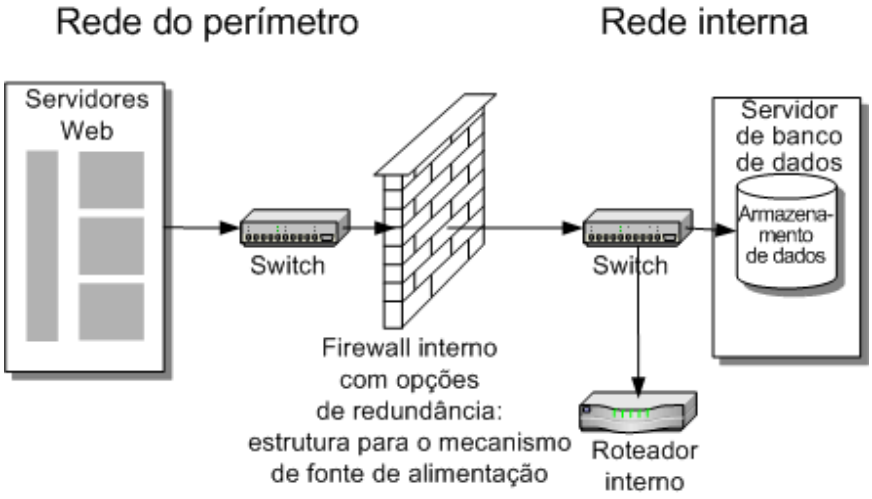

Figura 3: Firewall único, com componentes redundantes.

Fonte: Microsoft 2007

- **Vantagens:**

  As vantagens de se ter um firewall único incluem:

- **Baixo custo:**

Como existe somente um firewall, os custos de hardware e licenciamento são baixos. O custo dos componentes redundantes, como uma fonte de alimentação, não é alto.

- **Gerenciamento simplificado:**

O gerenciamento é simplificado, pois há somente um firewall para o site ou para a empresa.

- **Uma única fonte de log**

  Todo o log de tráfego é centralizado em um dispositivo

- **Desvantagens**

  As desvantagens de se ter um firewall único incluem:

- **Ponto único de falha**

Dependendo do número de componentes redundantes, pode ainda existir um ponto único de falha para o acesso de entrada e saída.

- **Custo**

  O custo é mais alto do que o de um firewall sem redundância e também pode exigir uma classe superior de firewall para poder conseguir incorporar a redundância.

- **Possibilidade de gargalo no tráfego**

Um firewall único poderia causar um gargalo no tráfego, dependendo do número de conexões e da taxa de transferência necessária.

3.1.13 Firewalls Tolerantes a Falhas

Um conjunto de firewall tolerante a falhas inclui um mecanismo para duplicar cada firewall como na figura a seguir.

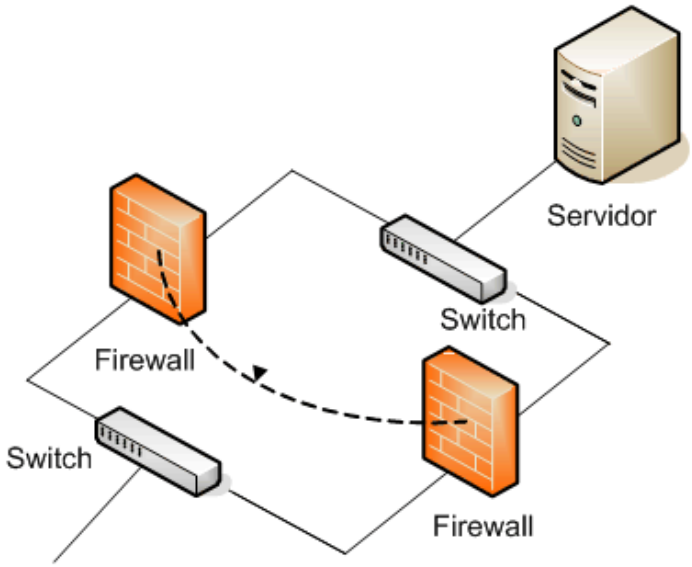

Figura 4: Firewalls tolerantes a falhas.
Fonte: Microsoft 2007

- **Vantagens**

  As vantagens de um conjunto de firewalls tolerantes a falhas são:

- **Tolerância a falhas**

  Usar pares de servidores ou dispositivos pode ajudar a fornecer o nível necessário de tolerância a falhas.

- **Log de tráfego central**

  O log de tráfego é mais confiável quando um ou ambos firewalls podem registrar atividade para o outro parceiro ou para um servidor separado

- **Possibilidade de compartilhamento de estado**

  Dependendo do produto, os firewalls nesse conjunto conseguem compartilhar o estado de sessões.

- **Desvantagens**

  As desvantagens de um conjunto de firewalls tolerantes a falhas são:

- **Maior complexidade**

A instalação e o suporte deste tipo de solução são mais complexos devido à natureza de vários caminhos do tráfego de rede.

- **Configuração complexa**

Os conjuntos separados de regras de firewall podem levar a falhas de segurança e problemas de suporte se não forem configurados corretamente

- **Maior custo**

Como há a necessidade de pelo menos dois firewalls, o custo aumenta no conjunto de um único firewall.

- **Configurações do firewall tolerante a falhas**

Ao implementar um conjunto de firewalls tolerantes a falhas (geralmente conhecido como cluster), existem duas abordagens principais, conforme descrito nas seções a seguir. Conjunto ativo/passivo de firewall tolerante a falhas Em um conjunto ativo/passivo de firewall tolerante a falhas, um dispositivo (também conhecido como nó ativo) manipula todo o tráfego, enquanto o outro dispositivo (o nó passivo) não encaminha o tráfego nem executa a filtragem, mas permanece ativo, monitorando o estado do nó ativo. Normalmente, cada nó comunica a sua disponibilidade e/ou o estado da sua conexão ao nó parceiro. Geralmente, essa comunicação recebe o nome de pulsação, pois cada sistema avisa o outro, várias vezes por segundo, para garantir que as conexões estejam sendo manipuladas pelo nó parceiro. Se o nó passivo não receber uma pulsação do nó ativo em um intervalo específico superior ao definido pelo usuário, indicando que o nó ativo falhou, então, o nó passivo assumirá a função de ativo. A figura a seguir apresenta a descrição de um conjunto ativo/passivo de firewall tolerante a falhas.

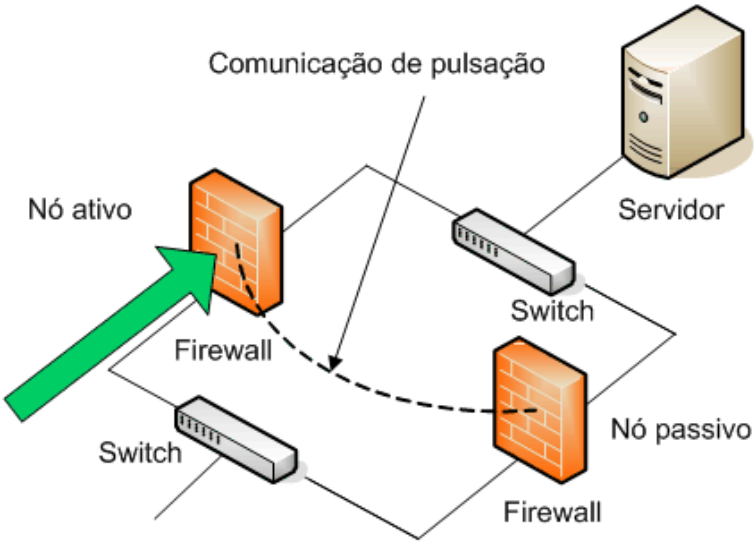

Figura 5: Conjunto ativo/passivo de firewall tolerante .

Fonte: Microsoft 2007

- **Vantagens**

As vantagens de um conjunto ativo/passivo de firewall tolerante a falhas são:

- **Configuração simples**

Esta configuração é mais simples de se fazer e solucionar do que a opção a seguir, ativo/ativo, porque apenas um único caminho de rede está ativo a todo o momento.

- **Carga de failover previsível**

Como toda a carga de tráfego alterna para o nó passivo em failover, o tráfego que o nó passivo deve gerenciar poderá ser facilmente planejado

- **Desvantagens**

As desvantagens de um conjunto ativo/passivo de firewall tolerante a falhas são:.

- **Utilização ineficiente**

O conjunto ativo/passivo de firewall tolerante a falhas é ineficiente porque o nó passivo não fornece uma função útil à rede durante a operação normal e não aumenta a taxa de transferência.

- **Conjunto ativo/ativo de firewall tolerante a falhas**

Em um conjunto ativo/ativo de firewall tolerante a falhas, dois ou mais nós ouvem ativamente todas as solicitações enviadas para um endereço IP virtual que cada nó compartilha. A carga é distribuída entre os nós por meio de algoritmos exclusivos para o mecanismo de tolerância a falhas em uso ou por meio de uma configuração estática baseada no usuário. Qualquer que seja o método, o resultado é que cada nó filtra ativamente um tráfego diferente. No caso de um nó falhar, os nós sobreviventes distribuem o processamento da carga que tinha sido assumida anteriormente pelo nó que falhou. A figura a seguir apresenta a descrição de um conjunto ativo/ativo de firewall tolerante a falhas:

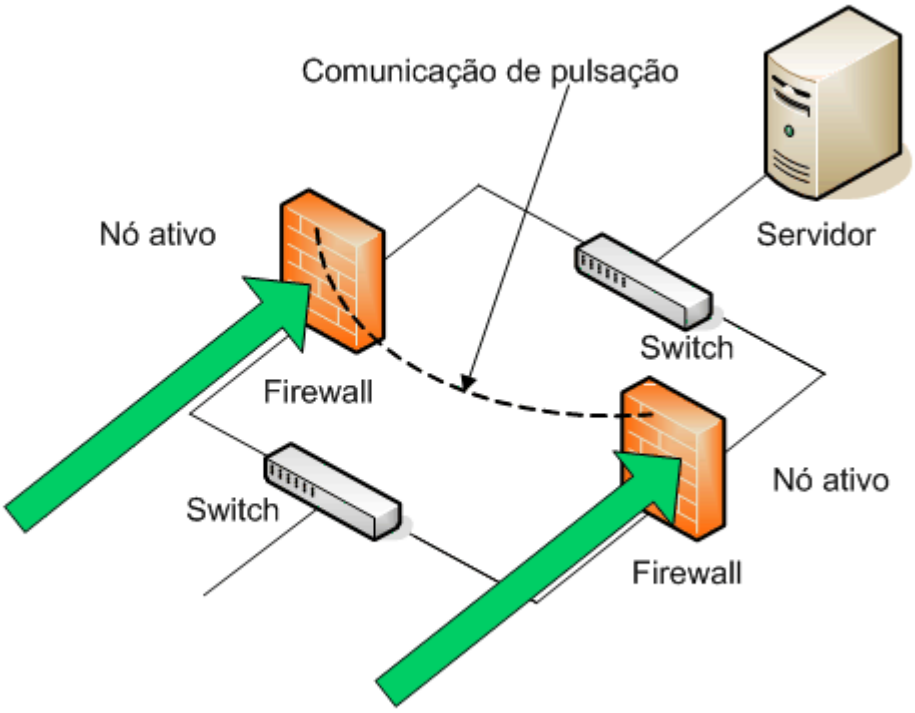

Figura 6: Conjunto ativo/ativo de firewall tolerante a falhas

Fonte: Microsoft 2007

- **Vantagens**

  As vantagens de um conjunto ativo/ativo de firewall tolerante a falhas incluem:

- **Maior eficiência**

  Como todos os firewalls estão fornecendo um serviço à rede, o uso deles é mais

eficiente.

- **Taxa de transferência maior**

Durante a operação normal, esta configuração pode manipular níveis superiores de tráfego se comparada à configuração ativo/passivo, já que todos os firewalls podem fornecer o serviço à rede simultaneamente.

- **Desvantagens**

As desvantagens de um conjunto ativo/ativo de firewall tolerante a falhas são:

- **Sujeito a possíveis sobrecargas**

Se um nó falhar, os recursos de hardware no(s) nó(s) restante(s) poderão ser insuficientes para atender ao requisito de taxa de transferência total. É importante planejar-se adequadamente para isso, entendendo que a degradação do desempenho provavelmente irá ocorrer, já que os nós sobreviventes assumem a carga de trabalho adicional, quando um nó falha.

- **Maior complexidade**

Como o tráfego de rede pode passar por várias rotas, a solução de problemas torna–se mais complexa.

- **Segurança**

A segurança de produtos de firewall é de suma importância. Embora não existam padrões para a segurança de firewall, o fornecedor independente ICSA (International Computer Security Association) executa um programa de certificação para testar a segurança de produtos de firewall disponíveis comercialmente. A ICSA testa um número significativo de firewalls disponíveis no mercado atual. Para obter mais informações, consulte a seguinte URL: www.icsalabs.com (em inglês)

É preciso ter cuidado para garantir que um firewall alcance os padrões de segurança necessários e uma maneira para fazer isso é escolher um firewall que conquiste a certificação ICSA. Além disso, deve existir um histórico para o firewall escolhido. Há vários bancos de dados de vulnerabilidade de segurança disponíveis na Internet. Você deve verificá–los para obter informações sobre as vulnerabilidades do produto que pretende comprar. Infelizmente, todos os produtos (baseados em hardware e software) têm bugs. Além de determinar a quantidade e a gravidade dos bugs do produto que pretende comprar, também é importante avaliar a capacidade de resposta do fornecedor para as vulnerabilidades expostas.

- **Escalabilidade**

Essa seção trata sobre o requisito de escalabilidade de uma solução de firewall. A

escalabilidade de firewalls é determinada basicamente pelas características de desempenho dos dispositivos usados. É prudente selecionar um tipo de firewall que será escalado para atender às situações que enfrentará na prática. Há duas maneiras básicas para se alcançar a escalabilidade:

- **Escala vertical (ascendente)**

Se o firewall for um dispositivo de hardware ou uma solução de software executada em um servidor, a variação de graus de escalabilidade poderá ser atingida com o aumento da quantidade de memória, da capacidade de processamento da CPU e da taxa de transferência de interfaces de rede. No entanto, há um limite para cada dispositivo ou servidor no que se refere à distância em que pode ser escalada verticalmente. Por exemplo, se você comprar um servidor com suporte para quatro processadores e começar com dois, será possível adicionar apenas mais dois processadores.

- **Escala horizontal (lateral)**

Uma vez que um servidor tenha sido escalado verticalmente até o seu limite, a escala horizontal passará a ser importante. A maioria dos firewalls (baseados em hardware e software) pode ser escalada lateralmente usando alguma forma de balanceamento de carga.

Em uma situação como essa, vários servidores são organizados em um cluster e vistos como um pelos clientes na rede. Esse caso é essencialmente o mesmo do cluster ativo/ativo descrito na seção "Disponibilidade", neste módulo. A tecnologia usada para oferecer essa funcionalidade pode ou não ser a mesma que a descrita anteriormente, e dependerá do fornecedor.

A escala vertical de firewalls pode ser difícil. No entanto, alguns fabricantes de firewall de hardware oferecem soluções de escala lateral por meio das quais os seus dispositivos podem ser empilhados para operar como uma única unidade de carga equilibrada.

Alguns software s baseados em firewalls foram criados para fornecer uma escala ascendente, usando vários processadores. O multiprocessamento é controlado pelo sistema operacional subjacente, e o software de firewall não precisa conhecer os demais processadores. No entanto, é possível que nem todos os benefícios dos vários processadores sejam alcançados a menos que o software de firewall possa operar em um modo de multitarefas. Esta abordagem permite uma escala em dispositivos simples ou redundantes em oposição aos firewalls baseados em hardware ou do tipo dispositivo, que normalmente devem seguir as limitações de hardware neles embutidas no momento da fabricação. A maioria dos firewalls do tipo dispositivo é classificada pelo número de conexões simultâneas que os

dispositivos podem manipular. É freqüente a necessidade de substituição dos dispositivos de hardware se os requisitos de conexão excederem o que está disponível para o modelo de escala fixa do dispositivo.

Como já foi abordado, a tolerância a falhas pode estar embutida em um sistema operacional de servidor de firewall. Para um firewall de hardware, a tolerância a falhas representará, provavelmente, um custo extra.

- **Consolidação**

Consolidação significa incorporar o serviço de firewall em outro dispositivo ou incorporar outros serviços no firewall. Os benefícios da consolidação são:

- **Preço de compra menor**

Ao incorporar o serviço de firewall em outro serviço, por exemplo, em um roteador, o custo de um dispositivo de hardware será evitado, embora ainda seja necessário comprar o software de firewall. Da mesma forma, se for possível incorporar outros serviços no firewall, o custo de hardware adicional será evitado.

- **Custos reduzidos de inventário e gerenciamento**

A redução no número de dispositivos de hardware faz com que os custos operacionais sejam reduzidos. Uma vez que a necessidade de atualizações de hardware é menor, o cabeamento fica simplificado e o gerenciamento torna–se mais simples.

- **Melhor desempenho**

Dependendo da consolidação alcançada, o desempenho pode ser melhor. Por exemplo, a incorporação de cache de servidor Web no firewall pode afastar a necessidade de dispositivos adicionais e os serviços se comunicam em alta velocidade, e não por um cabo Ethernet.

- **Entre os exemplos de consolidação, estão:**
- **Adição de serviços de firewall a um roteador**

A maioria dos roteadores pode ter um serviço de firewall incorporado. Os recursos desse serviço de firewall podem ser muito simples em roteadores de baixo custo, mas os roteadores high–end geralmente terão um serviço de firewall muito eficiente. É provável que você tenha pelo menos um roteador conectando os segmentos da Ethernet na sua rede interna.

Você economizará com a incorporação do firewall nele. Mesmo que você implemente dispositivos de firewall específicos, a implantação de alguns recursos de firewall nos roteadores poderá ajudar a limitar as invasões internas.

- **Adição de serviços de firewall ao switch interno**

Dependendo do switch interno selecionado, é possível adicionar o firewall interno como "blade", reduzindo custos e melhorando o desempenho.

Ao considerar a consolidação de outros serviços no mesmo servidor ou dispositivo que ofereça o serviço de firewall, você deverá ter cuidado para garantir que o uso de um determinado serviço não comprometa a disponibilidade, a segurança ou a facilidade de gerenciamento do firewall. Também é importante considerar o desempenho, já que a carga gerada por serviços adicionais irá degradar o desempenho do serviço de firewall.

Uma abordagem alternativa para consolidar serviços no mesmo dispositivo ou servidor que hospeda o serviço de firewall é consolidar um dispositivo de hardware de firewall como uma "blade" em um switch. Essa abordagem normalmente custa menos do que um firewall autônomo de qualquer tipo e pode aproveitar os recursos de disponibilidade do switch, como as fontes de alimentação duplas. Uma configuração como essa também é mais fácil de ser gerenciada por não envolver um dispositivo separado. Além disso, esta solução normalmente é executada com mais rapidez porque usa o barramento no switch, que é mais veloz que um cabeamento externo.

Capítulo 4 Tragefo de Protocolos

4.1 Sobre Pacotes

4.1.1 Padrões e diretrizes

A maioria dos protocolos de Internet que usa a versão 4 do protocolo IP (IPv4) pode ser protegida por um firewall. Isso inclui os protocolos de nível inferior, como o TCP e o UDP, e os protocolos de nível superior, como o HTTP, o SMTP e o FTP. Ao analisar o produto de firewall que pretende adquirir, verifique se ele realmente oferece suporte ao tipo necessário de tráfego. Alguns firewalls também podem interpretar o GRE, que é o protocolo

de encapsulamento para o protocolo PPTP (Point–to–point Tunneling Protocol), usado em algumas implementações de VPN.

Alguns firewalls têm filtros da camada de aplicativo embutidos para protocolos, como HTTP, SSL, DNS, FTP, SOCKS v4, RPC, SMTP, H. 323 e POP (Post Office Protocol).

Deve–se considerar também o futuro do protocolo TCP/IP e IPv6, bem como se esse será um requisito obrigatório para qualquer firewall, mesmo se o IPv4 estiver sendo usado no momento.

Capítulo 5 Comparativos entre firewall de software

5.1 Comparativos entre firewall de softwer:

5.1.1 Pontos positivos e negativos de Firewall de software

Serão relacionados os principais pontos positivos e pontos negativos para cada um dos aplicativos que foram analisados.

5.1.2 Zone Alarm

- **Pontos positivos**

Possui botão de emergência para terminar as conexões; a interface com o usuário é bastante interativa; permite desconectar o computador com inatividade ou proteção de tela; possui diferentes configurações para rede local e rede externa; permite controle de senha para cada aplicativo cadastrado; diferencia aplicativos que funcionam como servidor; permite que as regras sejam exportadas/importadas.

- **Pontos negativos:**

Não possui controle de senha para a configuração desejada; realiza controle de versão dos aplicativos apenas se o serviço TrueVector estiver executado, caso contrário não identifica a mudança da versão; não permite que os logs sejam enviados para um loghost; só

permite a criação de regras para IPs.

5.1.3 Tiny Firewall

- **Pontos positivos**

Faz controle de versão dos aplicativos; apresenta baixo consumo de memória; a interface é simples; é inicializado antes do processo de autenticação do Windows; boa interface de criação das regras; permite que os logs sejam enviados para um loghost.

- **Pontos negativos**

Não possui botão de emergência; os alertas são pouco detalhados; as regras não podem ser exportadas/importadas; não permite controle dos aplicativos com senha.

5.1.4 Sygate Firewall

- **Pontos positivos**

Possui botão de emergência; permite execução de aplicativos dentro de períodos pré-determinados; permite o envio de logs por e-mail; oferece opções de logs bem complexas; permite acessar o conteúdo de pacotes suspeitos; permite testar a configuração do firewall.

- **Pontos negativos**

Não realiza controle de versão dos aplicativos; não permite controle dos aplicativos com senha; não permite que os logs sejam enviados para um loghost; as regras não podem ser exportadas/importadas.

5.1.5 Norton Firewall

Pontos positivos:

Permite controle de privacidade além do firewall em si, possui bom assistente de configuração; a interface com o usuário é bastante intuitiva.

- **Pontos negativos:**

Não realiza controle de versão dos aplicativos; não possui botão de emergência; exige um sistema com mais memória; não possui senha para controle de configuração; os logs possuem limitação de tamanho; logs não podem ser enviados para um loghost; não distingue entre rede local e rede externa.

5.1.6 BlackIce Defender

- **Pontos positivos**

Possui o melhor reconhecimento de ataques; a configuração é bastante simples; está mais para sistema IDS do que para Personal Firewall.

- **Pontos negativos**

Não possui bloqueio de saída; não controla versão dos aplicativos; não possui controle por senha da configuração; não permite o envio dos alertas para um loghost (somente disponível com um pacote adicional); não possui botão de emergência.

5.1.7 Escolhendo o firewall de software mais adequado.

A escolha do firewall de software a ser utilizado deve levar em conta uma série de fatores:

- **Nível de proteção desejada**

Deve-se escolher entre controle por protocolos, aplicativos, privacidade, conteúdo;

- **Funcionalidades mais desejadas**

Deve-se escolher qual função é mais interessante. Por exemplo, o controle de versão de aplicativos;

- **Facilidade de utilização:**

Pode-se escolher por um pacote completo que possua um antivírus e um firewall, ou pode-se escolher aquele cuja configuração e utilização sejam mais fáceis;

- **Familiarização com terminologias e conceitos de firewalls**

Alguns aplicativos podem exigir um maior conhecimento sobre o funcionamento de um firewall para que seja possível tirar total proveito das funcionalidades, outros aplicativos possuem opção de configuração automática e auxiliadores de configuração;

- **Preço x funcionalidades**

Deve-se considerar a compra de um firewall de software se as funcionalidades desejadas somente existirem na versão comercial;

- **Recursos computacionais necessários:**

Deve-se considerar versões mais simples e que exijam menos memória e capacidade de processamento para computadores cujos recursos sejam limitados;

- **Suporte disponível**

É desejável possuir acesso ao suporte especializado para sanar eventuais problemas com alguma aplicação especifica que pode eventualmente deixar de funcionar com a instalação de um firewall de software;

- **Disponibilidade de novas versões e correções**

É obrigatório escolher um software que forneça correções e atualizações; Tipo de conectividade (modem, adsl, cablemodem): deve-se considerar que alguns tipos de conectividade possuem taxas de transmissão de dados muito superiores do que outras firewall de softwer escolhido deve ser capaz de manter a funcionalidade. Alguns aplicativos possuem a funcionalidade de realizar uma desconexão após períodos estabelecidos de inatividade.

- **Comparativo entre Firewalls**

A escolha de um firewall de software não é definitiva, pois as ferramentas evoluem, agregam novas funcionalidades e surgem, sempre, novas alternativas. O usuário que já estiver habituado a utilizar um firewall de software deve, inclusive, testar alternativas para verificar se as suas necessidades particulares são atendidas.

5.1.8 Analise de aplicativos

Dos cinco aplicativos analisados de acordo com seus pré-requisitos antes analisados é possível fazer a seguinte observação na utilização sua utilização

- **ZoneAlarm**

Usuário que necessita de maior controle sobre quais aplicativos se conectam à internet.

- **BlackIce Defender.**

Usuário que deseja se aprofundar e conhecer mais sobre os ataques de que está sendo alvo.

- **Tiny Firewall**

Usuário que deseja o aplicativo mais simples e funcional.

- **Norton Firewall**

Usuário que deseja uma solução mais completa com inclusive controle de privacidade.

- **Sygate Firewall**

Usuário que deseja desenvolver regras e realizar configurações especificas.

Como todo software, os firewalls de software estão sujeitos a basicamente dois tipos de problemas: erros relacionados a programação do código e erros conceituais.

A grande aceitação destas ferramentas e sua proliferação atraíram também a curiosidade de muitos usuários sobre eventuais problemas que os Firewall de software poderiam ter.

Os usuários, não só ao Firewall de software , mas de qualquer software , devem sempre estar atentos a atualizações e correções que possam surgir pois uma sensação de falsa segurança por estar utilizando um programa com uma vulnerabilidade conhecida pode ser desastrosa.

Ao longo do ano de 2001, foram apresentadas publicamente várias vulnerabilidades dos principais produtores de Firewall de softwares, que por sua vez lançaram atualizações para corrigir estes problemas. Um ponto que sempre deve ser levado em conta na utilização de um software é se existe um desenvolvimento contínuo ou se o software foi abandonado, o famoso abandonware. Um aplicativo que não tem continuidade deve ser descartado como opção de utilização.

Outro ponto a ser considerado na utilização de um Firewall de software é que ele inibe a realização de uma auditoria remota. A utilização de um Firewall de software deve sempre ser comunicada/solicitada aos responsáveis pela área de segurança ou suporte para que seja possível desabilitar a aplicação durante um processo de auditoria.

Capítulo 6 Conclusão

Neste projeto foi apresentado um método prático para a seleção bem–sucedida de produtos de firewall. Esse método abrange todos os aspectos do design de firewall, inclusive os diversos métodos de avaliação e classificação necessários para escolher uma solução.

Nenhum firewall é 100% seguro. A única maneira de se garantir que a rede não será atacada eletronicamente pelo lado de fora é implementar uma barreira entre ele e todos os outros sistemas e as outras redes. O resultado seria uma rede segura quase inutilizável. Os firewalls permitem implementar um nível adequado de segurança, quando sua rede é conectada a uma rede externa ou são unidas duas redes internas.

As estratégias do firewall e os processos de design apresentados neste projeto devem ser considerados apenas como parte de uma estratégia geral de segurança. Um firewall sólido possui valor limitado se existirem pontos fracos em outras partes da rede. A segurança deve ser aplicada em todo componente da rede e uma política de segurança também.

Atentar para pontos fracos e conhecer o próprio nível de usabilidade reforça a idéia que o Firewall ideal é aquele que atende sua necessidade, no mercado existem inúmeros produtos para este modulo da segurança que devem ser analisados conforme todos os princípios aqui apresentados.

Nos teste apresentados será demonstrado o que atualmente o mercado oferece podendo o leitor baseado neste documento analisar e por sua vez chegar a uma conclusão daquilo que procura dentro de um Firewall.

REFERÊNCIAS BIBLIOGRÁFICAS

Ford. L. **Manual Compelto de Firewall Pessoal**, 1ª ed. Sao Paulo: Personal Education do Brasil ,2002 .244p.

Antonio M. , Pitanga C. **Hoenypots: a Arte de Iludir Hackers**, 1ªed. Rio de Janeiro:Brasport, 2003. 153p.

Neto U. Dominando **Linux Firewall Iptables**, 1ª ed. Rio de Janeiro: Ciência Moderna, 2004. 112p.

Welch A, Deamon D. **Check Point Firewall – 1 Essencial**, Sao Paulo: Campus BB, 2002. 560p.

Walsh W. **Firewall – Iran contra Conspiracy end Cover-up**, 1ª ed. São Paulo:WW Norton, 1997. 277p.

Paulo N. **Introdução ao estudo de Direito,** 28ª ed, São Paulo: Forense, 2007.450p.

Howto Y. **Como se tornar um hacker , Chester county, Pesnilvania,** Disponível em**:** <http://www.ccil.org/~esr/faqs/hacker-howto.html>. Acesso em 03 de Abr.2007.

Eric S. **Como se tornar um hacker , Chester county, Pesnilvania,** Disponível em**:** <http://gul.linux.ime.usp.br/~rcaetano/docs/hacker-howto-pt.html>. Acesso em 03 de Abr.2007.

Madeira.F, **historia do firewall**, São Paulo (SP). Disponível em: <http://www.imasters.com.br/artigo/4583/seguranca/a_historia_do_firewall/>. Acesso em: 15 Mai.2007.

Alecrim.E. Ataques **DoS (Denial of Service) e DDoS (Distributed oS)**, Ifowester, São Paulo, disponível em:< http://www.infowester.com/col091004.php>. Acesso em : 18 Abr.2007.

http://www.net.ohio-state.edu/security/talks.shtml - Forensic Computer

Australian Institute of Criminology. **Australian Institute of Criminology**. Austrália, mai.2005. Disponível em <http://www.aic.gov.au >. Acesso 12 Mar. 2007.

Carnegie Mellon , CERT(Computer Emergency Response Team). Disponível em <http://www.cert.org>. Acesso em 01de Jun.2007.

Firewalls Leak test. **Teste de Qualidade de Firewall de Software versus Aplicativos Leaktest**. EUA Jan 2003 Disponível em < http://www.firewallleaktester.com/tests.php>. Acesso em 17 de Jun.2007.

ANEXOS

Anexo A - Testes de avaliação de segurança dos firewalls de Software.

Serão apresentadas nesta parte do estudo para fim de conclusão do trabalho a descrição e informações técnicas das ferramentas que testam a capacidade de defesa de firewall de software.

Explanação da pontuação na defesa da terminação de firewall.

Nesta parte do trabalho apresentado ate aqui, será dada uma vista geral das avaliações de teste e informação adicional sobre estes, para saber, antes de olhar os resultados ,é necessário conhecer os símbolos que estão dispostos durante o teste.

: Este ícone significa que o Firewall está obstruindo o método utilizado, e adverte possivelmente o usuário sobre ele. Este é o resultado é o mais seguro.

: Este ícone significa qualquer um uma das seguintes possibilidades:

- a relação e / ou o serviço do firewall foram terminados com sucesso parcial, e a proteção da rede é considerada de médio risco.

Windows estava parando ou deixado de funcionar. Este resultado é ainda "médio risco". Alguns Firewall quando terminados inesperadamente, não libera enm etrada nem saídas de trafego de dados.

Este ícone significa que o o serviço testado é falho, e é segurança da rede é totalmente comprometida. Uma vez que este método nao seja aprovado qualquer programa maliscioso pode emitir dados para fora ou para dentro sem nenhum controle do firewall como um malware que pode incapacitar o firewall,.

Este ícone é dado a um firewall aprovado numa faixa de 70% a 100 % dos testes.

Este ícone é dado a um firewall que é aprovado nos teste dentro de uma faixa de 30% a 70%

Este ícone é dado a um firewall que ano é aprovado nos requisitos mínimos que varia de 0% a 30%

1. Tipos de Testes

1.1. Leaktest:

Este aplicativo renomeia arquivos maliciosos para arquivos e processos validos, para driblar regras do Firewall, assim substituindo a passagem destes com o nome de um arquivo permitido para trafego de entrada e saída.

- Informações Técnicas

Web site: http://grc.com/lt/leaktest.htm
Autor: Steve Gibson (Gibson Pesquisa Corporation)
Data: (primeira liberação versão atual do fim 2000) 07/11/2005
Categoria: substituição de nome de arquivo
Download: leaktest1.2.exe
Sistema Operacional : Windows 9x/Millenium/NT4/2000/XP

1.2. Tooleaky:

Este teste simula o envio de senhas de conta e cartão pela porta 80 com trafego entre sua maquina e a de origem do programa maliscioso.

- Informações Técnicas

  Web site: http://tooleaky.zensoft.com/
  Autor: Bob Sundling
  Data: 11/05/2001
  Categoria: trafego de dados pela porta 80
  Download: tooleaky.exe
  Sistema Operacional: Windows 9x/Millenium/NT4/2000/XP

1.3. Firehole:

O uso de um FireHole opta pelo utilização do browser, para transmitir dados a um anfitrião remoto. Para isto, instala uma DLL (com função do interception para dentro) no computador do usuário.

Após carregar esta DLL juntamente aos processos em execução se utiliza a aplicação

apontada, assim o FireHole tem grande probabilidade de alcançar o stealthly (modo oculto) à Internet.

- Informações Técnicas

  Website : http://keir.net/firehole.html

  Autor : Robin Keir

  Data: 03/25/2002

  Categoria: launcher, DLL injection

  Download: firehole.exe

1.4. Yalta:

Yalta tem dois testes, um clássico e um avançado.

O teste clássico: permite envio de pacotes UDP por portas como 53 (DNS), 21(FTP) entre outras.

O teste avançado envia seus pacotes diretamente à relação da rede sob a camada de TCP/IP – processo também conhecido como calha de passagem.

- Informações Técnicas

  Web site: http://www.soft4ever.com/security_test/En/index.htm

  Autor: Soft4ever

  Data: novembro 2001

  Categoria: relação de rede sobre camada TCP/IP

  Download: yalta.zip

  Sistema Operacional: Windows NT4/2000/XP,modalidade avançada dos yalta de 9x/Millenium.

1.5. OutBound :

OutBound emite pacotes diretamente à relação da rede que tenta contornear o Firewall. O que difere o outBound dos makes e dos outros leaktests é o uso dos pacotes do TCP com poucas bandeiras permitidas, tentando fazê-las vistas como uma conexão estabelecida. Muitos Firewalls não filtram este tipo do pacote, para manter recursos seguros do processador central e do sistema.

- Informações Técnicas

  Web site: http://www.hackbusters.net/ob.html

  Autor: HackBusters

  Data: dezembro 2001

  Categorias: alcançar direto da relação da rede.

  Download: outbound.exe (vista EULA)

  Sistema Operacional: Windows 9x/Millenium

1.6. PCAudit:

Injeção de DLL dos usos de PCAudit, com código (como um DLL) na aplicação autorizada em vez de lançá-la no alvo diretamente.

Se a aplicação apontada tiver o acesso direto, o pcaudit irá funcionar sem problemas. Para testar corretamente PCaudit, configure o Firewall para advertir que, tentativas de conexões através do Explorer.exe à Internet devem ser informadas. Tente então outra vez, e se seu Firewall não lhe mostrar um alerta sobre pcaudit.exe, significando vulnerabilidade.

- Informações Técnicas

  Web site: http://www.pcinternetpatrol.com/

  Autor: Alliance da Segurança do Internet

  Data: março 2002

  Categoria: injeção do DLL

  Download: PCaudit.exe (vista EULA)

  Sistema Operando-se: 2000/XP,

1.7. AWFT

AWFT oferece 10 testes ao seu Firewall:

Um: tentativas de carregar uma cópia do browser com defeito e de corrigir na memória antes executar. Derrota o PFs mais fraco.

Dois: gera uma linha em uma cópia carregada no browser com defeito. Na maioria dos Firewalls ainda falha.

Três: gera uma linha no explorador do Windows. Firewalls ainda falham neste ponto.

Quatro: tentativas de carregar uma cópia no browser com defeito dentro do explorador do Windows e de corrigir na memória antes da execução. Derrota PFs que requerem a

autorização para uma aplicação (sucedendo na técnica 1) - o explorador do Windows é autorizado normalmente. Este teste sucede geralmente, a menos que o browser com defeito seja obstruído para alcançar a Internet.

Cinco: Executa uma busca heurística por proxys e outros softwares autorizados. A fim de alcançar a Internet pela porta 80, carrega uma cópia e corrige na memória antes da execução dentro de uma linha no explorador do Windows.

Seis: executa uma busca heurística por proxys e o outros softwares autorizados. Para alcançar a Internet pela porta 80, pede ao usuário que selecione um deles, em seguida gera uma linha nos processos.

- Informações Técnicas
  Web site: http://www.atelierweb.com/awft/
  Autor: José Pascoa
  Data: 2005, v3.2
  Categoria: carrega teste no browser
  Download: awft32.zip (Vista EULA)
  Sistema Operacional: Windows NT4/2000/XP/Server 2003

1.8. Thermite

Ao contrário de outros leaktests que injetam código em outros processos através de DLL, o Thermite injeta diretamente o código no processo alvo, criando uma linha maliciosa adicional dentro desse processo, totalmente invisível ao firewall.

Com o Thermite, a injeção do código é diretamente no aplicativo, que já esta sendo processado sem criar uma linha adicional no browser, impedindo assim, que seja descoberto pelo Firewall.

- Informações Técnicas
  Web site: email: oliverlavery@hotmail.com
  Web site: http://mc.webm.ru/
  Autores: Oliver Lavery e bugsbunny@e-mail.ru
  Data: 02/20/2003
  Categoria : injeção processo direto no aplicativo alvo
  Download: thermite.exe

Informação de Leaktest

Download: copycat.exe

Sistema Operacional: Windows NT4/2000/XP

Obs: Detectado por antivirus como exploit.win32.copycat.b, este não é um vírus é um arquivo protegido por senha (passagem = mais leaktest)

1.9. Outbound MBtest

Envia diretamente ao NIC seus pacotes ao tentar contornar o Firewall. Emitindo tipos diferentes de pacotes de size/protocoles/type.

Usa bibliotecas de Winpcap, não sendo necessária instalação pelo usuário.

- Informações Técnicas

  Web site: email: mbcx8nlp@hotmail.com

  Autor: mbcx8nlp (entalhe)

  Data: 07/05/2003

  Categoria: alcançar direto da relação da rede

  Download: mais leaktest nse: mbtest.exe

  Todas as linhas + fontes: mbtest.zip (pacote original do autor)

  Linhas de Winpcap:files.rar (linhas de Winpcap necessitadas para o teste)

  Sistema Operacional: Windows 2000/XP

Obs: este leaktest não trabalha em todo computador, devido ao fato que está codificado de encontro a uma língua específica (testes padrões em sua língua nativa). Por exemplo: não trabalhará em computadores franceses.

Como um workaround, você deve editar a fonte para ajustar o seu computador.

Para testar, é necessário codificar o Adress MAC, entre outras coisas.

1.10. WallBreaker

Primeiro teste: o WallBreaker usa o explorer.exe para alcançar a Internet, e assim, uma janela abre outra, . Os Firewalls atuais podem ver as aplicações tentando alcançar diretamente a Internet: uma aplicação que lança outra para alcançar a Internet.

Segundo teste: é um gracejo trivial, utiliza o Internet Explorer diretamente, mas de uma maneira não segura para Firewall, visto que é uma maneira a mais de escapar. Muitos Firewall não o vêem.

Terceiro teste: é uma variante do primeiro teste, utilizando o cmd.exe que executa então o explorer.exe, e finalmente iexplore.exe:

Wallbreaker - > cmd - > explorador - > iexplore (vitória 2000/XP somente).

Quarto teste : é uma extensão do terceiro teste, Wallbreaker ajusta uma tarefa programada usando "AT.exe" que por sua vez executará a tarefa através do "svchost": Wallbreaker - > EM - > svchost - > cmd - > explorador - > iexplore

Este teste cría uma linha de grupo (extensão do "bat") com um nome de arquivo aleatório em seu diretório, ele deve manualmente ser suprimido pelo usuário na extremidade do teste. Para que este teste seja executado, o serviço do scheduler de tarefa do Windows deve ser inicializado (mantenha na mente que um Trojan real poderia fazer para você.)

- Informações Técnicas

  Web site: http://www.firewallleaktester.com

  Autor: eu mesmo: Guillaume Kaddouch

  Data: Outubro 2004 (v4.0)

  Categoria : lançador

  Download: WallBreaker.exe

  Sistema Operacional: Windows 9x/Millenium/NT4/2000/XP

1.11. PCAudit V2

PCAudit usa a injeção do DLL no código da aplicação autorizada em vez de lançá-la diretamente na aplicação.

Se a aplicação apontada tiver o acesso livre, o pcaudit irá fucnionar sem problemas. Para testar corretamente PCaudit, configure o Firewall a advertir que tentativas de execução do Explorer.exe. Tente então outra vez, e se seu Fiewall não lhe mostrar um alerta sobre pcaudit.exe, significando vulnerabilidade.

PcAudit V2 usa uma maneira diferente do que sua versão anterior contorna a proteção de DLLs pelo Firewall.

- Informações Técnicas

  Web site: http://www.pcinternetpatrol.com/

  Autor: Alliance de Segurança da Internet

  Data: não disponível

Categoria: Injeção do DLL

Download: pcaudit2(6.3).exe

Versão Antiga: 4.0.1.0: pcaudit2(4.0.1.0). exe

Sistema Operacional: 95(WinsockV2) /98/Millenium/NT/2000/XP

1.12. DNS

Usado geralmente quando um aplicativo faz acesso a Internet, o Firewall usa o Windows API para recuperar o pai PID e o nomear (os executáveis que utilizam a aplicação confiada) e quando a têm, a congelam (travando no sistema) e lhe pedem o que fazer (allow/deny).

Para impedir de ser visto, gera um ghost. Uma vez que deu a informação para emitir ao browser com defeito, a mudança de solicitação de serviços dos processos travados, será derrubada, shuting (derrubar) e reinicia-se para continuar a emitir dados.

Tentativa do ghost de alcançar uma página que feche uma conexão. Pelo defeito em alguns sistemas operacionais como Windows NT, e janelas no Windows 2000, um serviço cliente de Windows no DNS estará funcionando e assegurará todos os pedidos do DNS. Assim, todo o DNS solicita a vinda de várias aplicações poderão ser transmitidas ao cliente no DNS (SVCHOST.EXE sob XP).

Este comportamento pode ser usado para transmitir dados a um computador remoto, um pedido especial do DNS sem a observação dos Firewall. Certamente, o serviço das janelas do cliente do DNS deve ser permitido para conexão a Internet. DNSteste usa este tipo de pedido recursivo do DNS contornando o seu Firewall.

Para usar DNSteste, você deve permitir o serviço de janelas do cliente no DNS (um Trojan real poderia fazer para você).

- Informações Técnicas

  Web site: http://www.firewallleaktester.com

  Autor: Guillaume Kaddouch,

  Data: julho 2004 (v1.1)

  Categoria: lançador, ataque cronometrado.

  Download: Ghost.exe

  Sistema Operacional: Windows 9x/Millenium/NT4/2000/XP

  Web site: http://www.klake.org/~jt/dnshell/

Autor: Jarkko Turkulainen

Data: abril 2004 (v1.0)

Categoria: pedido recursiva

Download: dnstester.exe (vista EULA)

(fontes: dnstester.zip)

Sistema Operacional: Windows 2000/XP/2003

Obs: detectado por antivirus como trojan.win32.agent.pc. Este não é um vírus arquivo protegido senha do download (passagem = mais leaktest).

1.13. Surfe

Chama o Internet Explorer a dar-lhe parâmetros. Para evitar que, o surfer crie um IE escondido no desktop como tambem lançamento dentro de nenhuma URL e assim nenhum acesso de rede, lança então um outro exemplo de I.E, e fecha primeiro. Então usa o protocolo do DDE (troca de dados direta).

O DDE é um protocolo antigo para troca de dados inter-process (muito similar a OLE). A netscape desenvolveu uma relação de DDE para seu browser e todas principais estão inclusas no IE.

- Informações Técnicas

  Web site: nenhuma ligação

  Autor: Jarkko Turkulainen

  Data: agosto 2004 (v1.1)

  Categoria: lançador

  Download: surfer.exe

  (fontes: surfer.zip)

  Sistema Operacional: Windows 2000/XP

1.14. Breakout

O breakout emite à barra do endereço do IE e o URL ao lançamento, através do SendMessage Windows API. Nenhum código é injetado.

- Informações Técnicas

  Web site: hoster: http://www.dingens.org

Autor: Volker Birk

Data: não disponivel

Categoria: lançador, messaging de Windows

Download: Versão inglesa do IE: breakout-en.exe

Versão inglesa de Firefox: breakout-mozilla-firefox.exe

fontes: http://www.dingens.org/breakout-en. http://www.dingens.org/breakout-mozilla-firefox.c

Sistema Operacional: Windows 2000/XP

Obs: Detectado por antivirus como trojan-clicker.win32.small.ip. arquivo protegido por senha de download (passagem = mais leaktest)

1.15. Jumper.

Os métodos usuais de desvio de Firewall, tais como a injeção de DLL e a injeção de linha, estão agora no espaço dos Firewall , e alguns deles fornecem uma proteção genérica de encontro de tal atividade.

Em vez de modificar diretamente a memória do processo alvo, a ligação está fazendo o alvo carregar a DLL. Assim escreve à entrada no registro do AppInit_DLLs, e ele mata então o processo do explorer.exe que é recarregado automaticamente pelo Windows.

Uma vez dentro e lançado diretamente no IE dando-lhe a linha de comando e parâmetros. O DLL modifica a entrada do registro da página do começo do IE com todos os dados que quer transmitir (em nosso caso URL + as informações pessoais), e lança então no IE.

Na extremidade, o IE previsto no Windows, é o processo final do alvo. O Internet Explorer, não é modificado nem é atacado.

- Informações Técnicas

  Web site: http://www.firewallleaktester.com

  Autor: Guillaume Kaddouch

  Data: março 2006 (v1.0)

  Categoria: lançador, injeção do DLL, registro de injeção

  Download: Jumper.exe

  Sistema Operacional: 2000/XP

1.16. Cpil

Este teste tenta encontrar o explorer.exe e alterar sua memória. Então com o explorer.exe infectado, tenta transmitir dados aos usuários remotos através do browser com defeito.

- Informações Técnicas
  Web site: http://www.personalfirewall.comodo.com
  Autor: COMODO
  Data: Abril 2006
  Categoria: Injeção do DLL
  Download: cpil.exe
  Sistema Operacional: 2000/XP

1.17. PCFlankLeaktest.exe

PCFlank's Leaktest usa uma técnica especial, chamada automatização de OLE do controle da aplicação, verifica como seu Firewall comporta-se perante a situação onde um programa tenta controlar o comportamento de um outro programa, que seu Firewall foi reconfigurado.

- Informações Técnicas
  Web site: http://www.pcflank.com/pcflankleaktest.htm
  Autor: PCFlank
  Data: Maio 2006
  Categoria: Messaging de Windows
  Download: PCFlankLeaktest.exe
  Sistema Operacional: 2000/XP

1.18. Teste de Qualidade de Firwall de Software versus Aplicativos Leaktest .

Nas próximas paginas serão apresentado alguns testes que avaliam a capacidade de defesa do Firewall dentro de todos os contextos aqui apresentados.

1.19. Pontuação dos Testes de Ferramentas Leaktest.

Highest Settings *(last update : March 11 2006)*

Firewall	ver(build)	LeakTest	TooLeaky	FireHole	Yaltas	PCAudit	AWFTester	Thermite	CopyCat	MBtest	WBreaker	PCAudit2	Gnoci	DNStester	Surfer	Breakout1	Breakout2	Jumper	Immunity	Score	block
KIS6	6.0.0.297f	✓	✓	+	✓	+	5.5/10 +	+	+	✗	+	+	✓	✗	✓	✗	✓	+	✓	18/27	15/18
Zone Alarm Pro	6.1.737.000	✓	✓	✓	✓	✓	8/10 +	+	+	✗	✗	✓	✓	✗	✓	✓	✗	+	✓	19.5/27	14/18
Zone Alarm Free	6.1.737.000	✓	✗	✗	✓	✗	1/10 ✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	4/27	3/18
Sunbelt Kerio	4.2.3.912	✓	+	✓	✓	+	4/10 +	+	+	✓	✗	+	+	✗	✗	✗	✗	✗	✗	11/27	11/18
Outpost	3.5.641.6214 (458)	✓	✓	✓	✓	✓	10/10 ✓	+	+	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	20/27	12/18
LookNStop	2.05p3	✓	✓	✓	✓	✓	10/10 ✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	20/27	11/18
Norton	2006 (9.0.0.73)	✓	✓	✓	✓	✓	9/10 ✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	19/27	11/18
Jetico	1.0.1.61	✓	✓	✓	✓	✓	10/10 ✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	23/27	14/18
Filseclab Pro	3.0.0.8686	✓	✗	✗	✓	✗	1/10 ✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	3/27	2/18
PrivateFirewall	5.0.3.9	✓	✓	✓	✗	+	5.5/10 +	+	+	✗	✗	+	✗	✓	✓	+	+	+	✓	15/27	14/18
Netveda	3.61.0002	✓	✓	✓	✓	✗	1/10 ✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	5/27	4/18
NetOp	3.0.0.180	✓	✓	✓	✓	✗	1/10 ✗	✗	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	9/27	8/18
Personal Firewall Plus	7.0.152	✓	✓	✓	✗	✗	1/10 ✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	5/27	4/18
Desktop Firewall	8.5(260)	✓	✗	+	✓	✗	5/10 +	+	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	9/27	8/18
Comodo	1.1.005	✓	✓	✓	✓	✗	3/10 +	✗	✗	✗	✗	✗	+	✗	+	✗	✗	+	✓	9.5/27	9/18
Windows Firewall (SP2)	-	✗	✗	✗	✗	✗	0/10 ✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0/27	0/18
Firewall	ver(build)	LeakTest	TooLeaky	FireHole	Yaltas	PCAudit	AWFTester	Thermite	CopyCat	MBtest	WBreaker	PCAudit2	Gnoci	DNStester	Surfer	Breakout1	Breakout2	Jumper	Immunity	Score	block

Please read the NEWS N°51 annoucing the update of these tests and giving more information.

1.20. *Gráficos Demonstrativos de Percentuais de Segurança dos Firewalls.*

Firewall	Ver(build)	Score (100% - % of leaktests failed)	Place
KIS6	6.0.0.297f	83,3%	1
Jetico	1.0.1.61	77,8%	2
Zone Alarm Pro	6.1.737.000	77,8%	2
PrivateFirewall	5.0.3.9	77,8%	2
Outpost	3.5.641.6214(458)	66,7%	3
Look'n'Stop	2.05p3	61,2%	4
Norton	2006 (9.0.0.73)	61,2%	4
Sunbelt Kerio	4.2.3.912	61,2%	4
Comodo	1.1.005	50%	5
NetOp	3.0.0.180	44,4%	5
Desktop Firewall	8.5(260)	33,4%	6
Personal Firewall Plus	7.0.152	22,2%	7
Netveda	3.61.0002	22,2%	7
Zone Alarm Free	6.1.737.000	16,7%	8
Filseclab Pro	3.0.0.8686	11,1%	9
Windows Firewall (SP2)	-	0%	-