UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

RUBEN BAMBI TSIMBA BAQUI

SEGURANÇA EM REDES LINUX COM FIREWALL

MONOGRAFIA

CURITIBA
2012

RUBEN BAMBI TSIMBA BAQUI

SEGURANÇA EM REDES LINUX COM FIREWALL

Monografia apresentada como requisito parcial para obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Kleber K. H. Nabas

CURITIBA

2012

“Façamos as coisas acontecer e não esperar que elas aconteçam”.

Ruben Baqui

AGRADECIMENTOS

Agradeço a Deus por estar sempre a minha frente em tudo, mostrando o caminho a seguir.

Aos nossos pais, demais familiares pois acredito que sem o apoio deles seria muito difícil vencer esse desafio, colegas de sala de aula e amigos pelo incentivo na elaboração desse projeto;

Aos Professores Augusto Foronda e Kleber Nabas, orientador deste projeto, pelo sabedoria, conhecimento, incentivo e principalmente pela dedicação com que me guiou nesta trajetória.

Enfim, a todos que acreditaram e me deram força para prosseguir adiante com o projeto.

Resumo

BAQUI, Ruben B. T. Segurança de Redes Linux com Firewall. 2012. 38f. Monografia (Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Centro Federal de Educação Tecnológica do Paraná. Curitiba, 2012.

Este trabalho tem como objetivo abordar formas de como assegurar as informações numa empresa dentro do contexto das redes de computadores com a utilização do firewall e também mostrar às principais ferramentas que podem ser utilizadas juntamente com os firewalls na segurança para *Linux* existentes atualmente nas áreas de varredura de vulnerabilidades, filtro de pacotes e monitoramento de servidores e serviços de rede (Nagios) e também o acompanhamento dos usuários da empresa, gerando relatórios de acesso do mesmo (Sarg).

Palavras-chave: Firewall. Segurança de Redes. Filtragem de Pacotes.

Abstract

BAQUI, Ruben B. T. Network Security Firewall with Linux. 2012. 38f. Monograph (Specialist in Configuring and Managing Servers and Network Equipment).Federal Center of Technological Education of Parana. Curitiba, 2012.

This work aims to address ways of how to ensure the information in an enterprise within the context of computer networks using the firewall and also show the main tools that can be used in conjunction with firewalls security for linux available today in the areas of scanning vulnerabilities, packet filtering and monitoring of servers and network services (nagios) and monitoring of enterprise users, generating reports access the same (sarg).

KEYWORDS: Firewall. **NETWORK SECURITY**. **PACKET FILTERING**.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

IP	Internet Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
NAT	Network Address Translators
PPP	Point-to-Point Protocol
SLIP	Serial Line Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

SUMÁRIO

1 INTRODUÇÃO

É fundamental as empresas atualmente serem acessadas por meia da Web, a fim de continuarem e de permanecerem competitivas perante o concorrido mercado globalizado. Neste caso atual, a informação nas empresas começa ser o alvo principal, devido a sua forma de fazer funcionar de maneira rápida e necessária que muita gente faça comércio o tempo todo, demonstrando assim que é possível o comércio eletrônico por intermédio de um clique.

Para muitos atualmente o mundo é uma sonho, até mesmo para os inventores do TCP/IP e da Internet quanto a sua ampliação desse plano, mais para muitos já é uma realidade por que a rede de Internet já oferece esse suporte, tornando a comunicação melhor e levando as pessoas que estão distantes a se manter em contato de forma fácil com menos custos e melhores benefícios, trazendo assim no mundo todo desenvolvimento o conhecimento digital.

O firewall é um dos principais componentes de segurança de uma empresa, como também o mais conhecido e antigo.

O nome firewall significa “barreira de fogo” que nas empresas é implantado para que os usuários da Internet não acessem dados das Intranets, ou seja, entre duas redes ele é a barreira que permite ou não o acesso de dados.

O conceito do firewall na Internet vem com a finalidade de limitar o acesso que a Internet ofereci, quebrando o modelo da “conectividade sem limites”. Porém, possuir um firewall não resolve os possíveis problemas de segurança, pois o componente sozinho não é uma barreira, mas suas configurações é que faz esta função ser atingida.

1.1 CONCEITO DE SEGURANÇA

Quanto ao conceito de segurança, segundo Jorge Caetano, diz que:

> Os conceitos de segurança para esta grande rede, pois o que seria apenas uma pequena rede militar, tornou-se a grande rede mundial. Os protocolos não foram criados para serem utilizados em tão larga escala em termos de segurança, pois apresentam diversas vulnerabilidades.
> Mas, é complicado mudá-los, pois é um padrão mundial. Se de um lado, temos a necessidade das organizações em dispor seus negócios de forma rápida, fácil e acessível, de outro temos estes problemas técnicos. (CAETANO, 2011).

Defender não é somente evitar, quando não for possível impedir uma invasão, o sistema deve estar apto à detectar e alertar o fato. A defesa completa de rede de computador vem da união entre o impedimento, prevenção e detecção de falhas. É preciso que seja criadas políticas e que decisões sejam tomadas com a maior rapidez possível. Criadas as regras de segurança, e então iniciando o processo de detecção a falhas e pontos críticos que devem ser vigiados para manter a confiabilidade entre os usuários dos serviços dependentes da redes de computadores.

1.2 FUNDAMENTOS

Este trabalho de conclusão de curso tem como objetivo fornecer conceitos importantes de segurança baseadas em Firewall dentro de um sistema operacional Linux, como soluções a serem introduzidas nos vários estados da Internet, com o propósito de se obter uma boa segurança das informações a um custo baixo.

A Internet tem o objetivo diferente, que é interligar todas as redes do mundo, porém, sem este trabalho de conclusão de curso tem algumas recomendações para que se possa disponibilizar informações pessoais ou comerciais na Web com mais segurança.

A falta de segurança efetiva de empresa, quanto ao controle das informações, podem causar danos graves na operacionalização dos trabalhos internos da empresa. Uma rede sem firewall não transmite a segurança na rede interna das redes externas, tornando assim a rede vulnerável para os invasores. Não havendo

uma boa segurança na rede, os resultados não serão coerentes e confiáveis da parte lógica da rede da empresa, no processamento e outros, ficam prejudicadas, pois pode existir o excesso ou a falta de informações e que podem causar prejuízo financeiro e/ou social.

2. FIREWALL

2.1 DEFINIÇÃO DE FIREWALL

O firewall é um dos principais componentes de segurança de uma empresa, como também o mais conhecido e antigo.

O nome firewall significa “barreira de fogo” que nas associações é inserido para que os usuários da Internet não acessem dados das Intranets, limitando o caminho das informações, como as permissões de cada um, ou seja, entre duas redes ele é a barreira que permite ou não o acesso de dados.

Existem duas explicações exemplares e mais antigas e aceitas, dadas por dois atores que diz:

> “Firewall é um ponto entre duas ou mais redes no qual circula todo o tráfego. A partir deste tráfego é possível controlar e autenticar o tráfego, além de registrar por meio de logs, todo o tráfego da rede, facilitando sua auditoria. É um dos maiores destaques para hackers, pois se o mesmo conseguir acessá-lo, pode alterar suas permissões e alcançar o bem mais valioso das empresas – a informação”. A outra definição é de Chapman e define firewall como um componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre conjuntos de redes”.(CHESWICK, STEVEBELLOVIN, 2011).

2.2 SEGURANÇA EM FIREWALL

A idéia do firewall na Internet vem com o objetivo de restringir a comunicação que a Internet oferece, quebrando o modelo da “conectividade sem limites”. Mas, possuir um firewall não dá solução aos problemas de segurança, pois ele por si só não é um obstáculo, mas suas configurações é que faz esta função ser atingida.

Os primeiros firewalls foram inseridos em roteadores, no final da década de 80, por estarem em posição privilegiada – conectando redes distintas. As regras de filtragem eram baseadas na origem, destino e tipo de pacote. Com o advento da Web, foi necessário separar as funcionalidades do firewall dos roteadores.

Nesta nova situação houve uma necessidade maior em se prestar atenção nos assuntos de segurança e também um aumento de dificuldade, aparecendo varias tecnologias, tais como: filtro de pacotes, proxies, híbridos e adaptativos. Outras funcionalidades foram inseridas, como o firewall reativo e individual.

Atualmente, a inclinação é de serem acrescentados mais serviços aos firewalls, mesmo não estando diretamente ligado à segurança, como por exemplo, gerenciamento de banda, balanceamento de cargas, Proxy, entre outros.

2.3 A FUNCIONALIDADE DO FIREWALL E SUA COMPOSIÇÃO

Um firewall é um sistema ou conjunto de sistemas que influência um plano de segurança de dados existente entre uma empresa e possíveis usuários inseridos fora da mesma, restritamente os de origem na Internet, criando uma barreira inteligente por meio da qual só passa o tráfego autorizado.

A solução certa para a construção de um firewall é dificilmente formada de uma única técnica. É um conjunto de diferentes técnicas para resolver diferentes problemas. Os problemas que devem ser solucionado dependem de quais serviços a empresa planeja fazer disponíveis e de quais riscos esta considera aceitáveis.

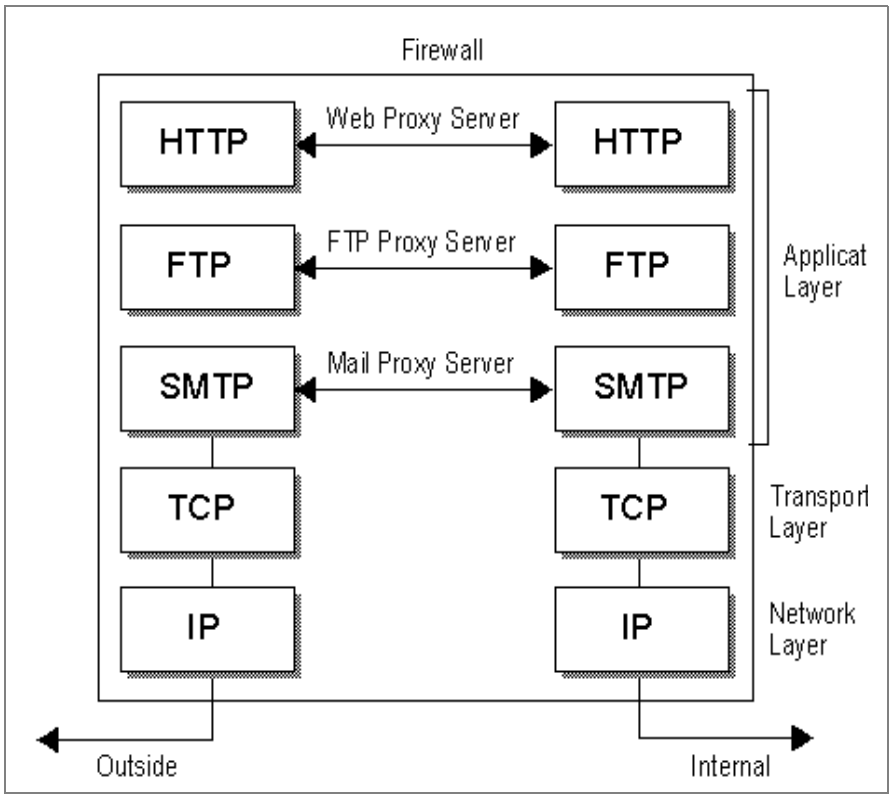
Por outra, as técnicas a serem aplicadas para a solução destes problemas dependem do tempo, recursos financeiros e conhecimento técnico disponível na empresa.

O objetivo dos firewalls é formar uma linha fechada de defesa projetado para proteger os bens internos de uma empresa. Para tal, deve atender a algumas condições:

- Deve ser parte integrante da política global de segurança da organização, de modo a evitar ser contornado facilmente por meios disponíveis a qualquer dos usuários internos;
- Todo o tráfego de dados para dentro ou para fora da rede corporativa deve passar obrigatoriamente pelo firewall, para poder ser inspecionado;
- Deve permitir apenas a passagem do tráfego especificamente autorizado (política conservadora - "o que não for expressamente permitido é proibido"), bloqueando imediatamente qualquer outro;

> • Deve ser imune à penetração, uma vez que não pode oferecer nenhuma proteção ao perímetro interno uma vez que um atacante consiga atravessá-lo ou contorná-lo. (NAKAMURA, 2002).

Um firewall, como se pode ver na figura 1, funciona como uma barreira que controla o tráfego entre duas redes. O mais seguro dos firewalls é aquele que bloqueia todo o tráfego com rede externa, mas isto terminaria com o propósito de fazer ligação com redes exterior. O passo seria permitir tráfego com o a rede exterior, mas manter severo controle sobre ele, de forma segura. Portanto, o firewall pode ser visto como um processo de funcionamento: um existe para bloquear tráfego e o outro existe para permiti-lo. Qualquer das duas estratégia é baseada numa plano total de segurança da empresa.



Firewall / Proxy típico

Figura 1 - Um firewall típico (Senna Junior, 2008)

O firewall gerencia todo acesso entre a rede interna e a Internet, sem ele a interna estaria vulnerável a ataques externos e, portanto, necessitaria usufruir das

capacidades de segurança determinadas. Não só isso, como também o estado da segurança total da rede interna seria decidido, pelo meio mais "fraco" desta rede.

2.4 VANTAGENS DO USO DE UM FIREWALL

O firewall facilita ao administrador da rede criar um ponto único de controle, pelo qual pode bloquear os acessos não autorizados, não permitir que serviços e dados fortemente vulneráveis saiam da rede interna e conceber proteção contra diversos tipos de ataques, pelo conjunto de energia e tecnologias de meio seguro neste único ponto. Outra vantagem do uso de um firewall é a possibilidade de monitoração centralizada e criação de alarmes de invasão. De modo geral, pode-se dizer que, para uma empresa que conserva conexões permanentes com a Internet, a questão não é se os ataques ocorrerão, mas sim quando ocorrerão. Os administradores de rede devem dispor de ferramentas adequadas para gerar relatórios de segurança e verificar o estado de suas defesas (Silva, 2003). Se o administrador de rede não tiver meios de saber que houve uma tentativa de invasão e se foi ou não bem sucedida, não precisaria ter um firewall.

> Um outro benefício do uso de firewalls é que estes tornaram-se os locais ideais para a colocação de Tradutores de Endereços de Rede (NAT –. *Network Address Translators*), essenciais para aliviar a crescente escassez de endereços IP registrados Assim, a organização necessita ter apenas um endereço IP conhecido e fornecido por um ISP (*Internet Service Provider*), sendo os demais criados internamente e geridos pelo NAT. O firewall é composto por diversos componentes, que isoladamente são responsáveis por algum tipo de serviço específico, que de acordo com o tipo disponível, vai definir o papel do firewall e seu nível de segurança.(SILVA, 2003).

Logo, o uso do firewall numa empresa se torna indispensável, pelo fato de garantir a segurança das informações da mesma.

2.5 LIMITAÇÕES NO USO DE FIREWALL

Um firewall só pode defender uma rede interna de ataques que passem por ele. Se o uso de canais de discagem por parte dos usuários da rede for ilimitado, usuários internos realizarão conexões diretas do tipo PPP (*Point to Point Protocolo*) ou SLIP (*Serial Line Internet Protocol*), que contornam as barreiras de segurança do firewall e proporcionam significativo risco de ataques por trás, como pode ser mostrado na figura 2.

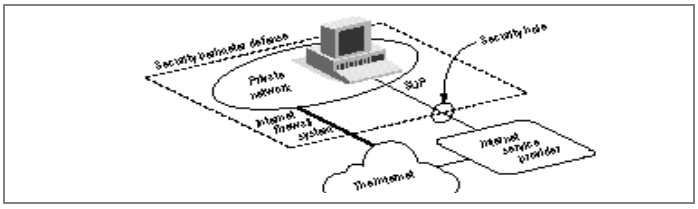


Figura 2– Uma conexão SLIP controlando o firewall (Senna Junior, 2008)

Outra proteção que o firewall não pode prover é caso a redes interna seja infetada a partir de dentro pelos usuários internos agindo propositadamente ou por displicência. Usuários podem remover dados secretos por meio de pen drives, cartões de notebooks ou serem vítimas de hackers disfarçando-se de administradores de sistemas e procurando que revelem uma senha, por exemplo.

O mesmo que se diz quanto à multiplicação de vírus de computador: as empresas devem predispor de softwares anti-vírus em toda a rede interna, por segurança. Um outro meio de ataque contra a qual os firewalls não são completamente eficientes são ataques movimentados por dados. Nestes caso, dados disfarçando ser puros são incluídos no interior da rede interna, seja através de email ou cópia de arquivos.

2.6 SEGURANÇA DE UMA REDE CONECTADA Á Internet

De uma maneira avaliada pode-se dividir os firewalls em quatro grandes grupos que são:

- Roteadores com filtragem de pacotes;
- Gateways de circuitos;
- Gateways de aplicação;
- Firewalls com inspeção de estado multi-camadas.

As aplicações de firewall chega desde a camada de rede (camada 3 no modelo OSI, ou camada de Internet, no modelo TCP/IP) até a camada de aplicação (camada 7 no modelo OSI, ou camada 4 no modelo TCP/IP).

Os firewalls que executam no nível da rede geralmente fundamentam suas decisões nos endereços de origem e destino e nas portas que existem em pacotes IPs individuais. Um roteador simples é a forma mais peculiar de um firewall funcionando no nível da rede. Um roteador não é competente ao ponto de tomar decisões sofisticadas sobre o conteúdo ou a origem de um pacote. Por outro lado, este tipo de firewall é muito rápido e evidente para os usuários.

> No outro extremo, firewalls que atuam no nível da aplicação, são geralmente computadores executando servidores Proxy, que não permitem fisicamente a existência de tráfego entre redes, e que efetuam elaboradas operações de verificação nos dados que por eles trafegam. Além disso, firewalls deste tipo são excelentes também como tradutores de endereços de rede (NAT), já que o tráfego "entra" por um lado e "sai" por outro, depois de passar por uma aplicação que efetivamente mascara a origem da conexão inicial. Este tipo de firewall é certamente menos transparente para os usuários e pode até causar alguma degradação no desempenho. (ANONYMOUS, 2000).

3. O FUNCIONAMENTO DO FILTRO DE PACOTE

Os firewalls que trabalham com sistemas de filtragem de pacotes entre computadores internos e externos à rede corporativa cumprem esta tarefa de forma selecionada. Um roteador é um dispositivo que envia para outra rede pacotes recebidos de uma rede. Um roteador com filtragem de pacotes é conhecido como *screening router* (roteador examinador). Seu propósito é decidir se aceita ou recusa o tráfego de cada pacote que recebe. Para tal, testa cada pacote para ordenar se atende a alguma de suas regras de filtragem de pacotes.

Estas regras firmam-se na informação que consta nos cabeçalhos dos pacotes, que é baseado nos seguintes itens:

• Endereço IP da origem;

• Endereço IP do destino;

• Protocolo encapsulado (TCP, UDP ou ICMP);

• A porta de origem TCP/UDP;

• A porta de destino TCP/UDP;

• O tipo de mensagem ICMP.

Se as informações coincidirem e a regra aceitar a entrada do pacote, este é encaminhado conforme a informação da tabela de roteamento. Se, por outro lado, coincidirem, mas a regra determinar a rejeição do pacote, o mesmo é rejeitado. Se não coincidirem, um parâmetro padrão definirá se possuirá rejeição ou aceitação do pacote.

Eis aqui algumas regras típicas de filtragem que são:

- Permitir entrada de sessões Telnet somente para determinada lista de computadores internos;

- Permitir entrada de sessões FTP somente para determinada lista de computadores internos;
- Permitir saída de todas as sessões Telnet;
- Permitir saída de todas as sessões FTP;
- Rejeitar todas as conexões de sistemas externos à rede corporativa, exceto para conexões SMTP (para a recepção de e-mail);
- Rejeitar todo tráfego de entrada e saída oriundo de determinadas redes externas.

> Para entendermos como funciona a filtragem de pacotes, precisamos atentar para a diferença entre um roteador comum e um *screening router*. Um roteador comum simplesmente observa o endereço de destino de cada pacote e decide qual o melhor caminho para enviar o pacote ao seu destino. Então, a decisão de como tratar o pacote é baseada somente no endereço de destino. Existem, então, duas possibilidades: ou o roteador sabe como enviar o pacote ao seu destino, e o faz, ou não sabe, e retorna-o à origem, com uma mensagem ICMP para o destino inalcançável. (ULBRICH, 2002).

Um *screening router*, por outro lado, observa as características do pacote mais detalhadamente. Além de determinar se pode ou não rotear o pacote ao seu destino, também determina o que deve ser feito, de acordo com as regras de segurança que o roteador deve fazer cumprir. Na figura 3, observa-se a posição típica de um *screening router* num sistema.

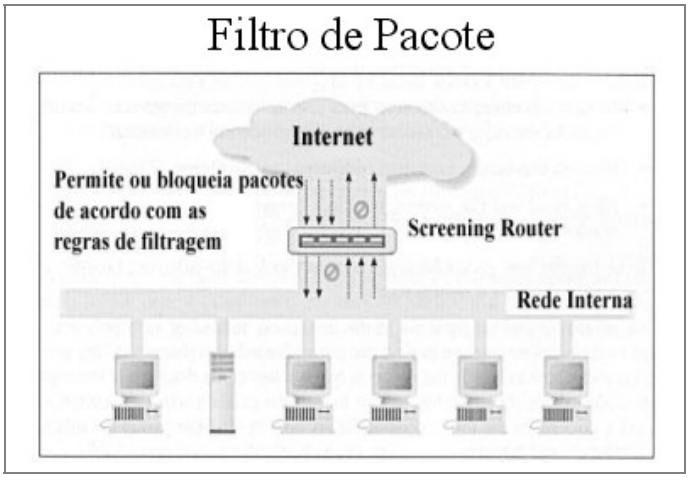


Figura 3 - Usando um screening router para a filtragem de pacotes.(Senna Junior, 2008)

4. GATEWAY DE CIRCUITO

Um gateway de circuito é uma função especializada que pode ser realizada por um gateway de aplicação (uma estação segura - um computador - que permite aos usuários se comunicarem com a Internet por meio de um servidor Proxy, código especial que aceita ou recusa características ou comandos exclusivo de certas aplicações, ou mesmo aceita ou recusa a própria aplicação).

Este tipo de firewall opera na camada de sessão do modelo OSI (camada 5), ou camada de transporte, no modelo TCP/IP (veja na figura 4). Este firewall usa as conexões TCP/IP como Proxy, pois um circuito Proxy é instalado entre o roteador da rede e a Internet. É este Proxy que comunica-se com a Internet, em lugar da própria rede local, e só o seu endereço IP é tornado público na Internet.

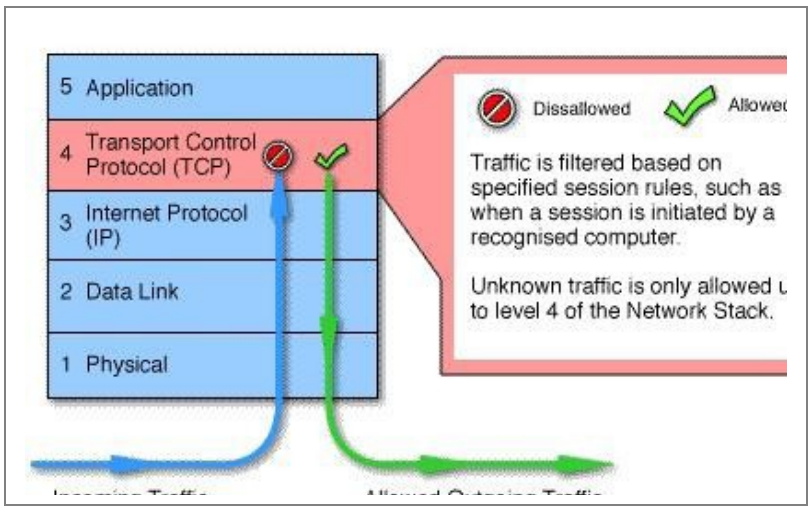


Figura 4: A posição de um firewall baseado em um gateway de circuito, como vista pelo modelo de camadas TCP/IP (Senna Junior, 2008)

Os gateways de circuito monitoram a troca de informações entre pacotes para definir se uma determinada sessão que está sendo verificada é legítima ou não. As

informações passadas a um computador remoto através de um gateway de circuito parecem ser originárias do próprio gateway. Com isto, ocultam-se informações mais detalhadas sobre a rede interna. Todavia, neste tipo de firewall ainda não acontece qualquer filtragem ou processamento de pacotes individualmente. Suas aplicações características são as ligações de saída, quando os usuários internos que as utilizam são considerados "confiáveis". Desta forma, uma configuração muito utilizada é um computador (o *bastion host*, um sistema especificamente configurado e protegido para resistir aos ataques externos) que opera como gateway de aplicação para conexões entrando no sistema e como gateway de circuito, para as que saem. Isto torna o sistema firewall mais transparente e fácil de usar para os usuários internos que anseiam o acesso direto à Internet, enquanto fornecer as funções necessárias à proteção da rede interna contra o tráfego que vem da Internet (FRASER, 1997).

A figura 5 mostra a operação de uma típica conexão Telnet através de um gateway de circuito. Este simplesmente transmite as informações, sem nenhum exame ou filtragem dos pacotes. Todavia, como a conexão parece, aos usuários externos, gerada e gerenciada no gateway de circuito, informações sobre a rede interna não estão disponíveis. Só o endereço IP do gateway é conhecido.

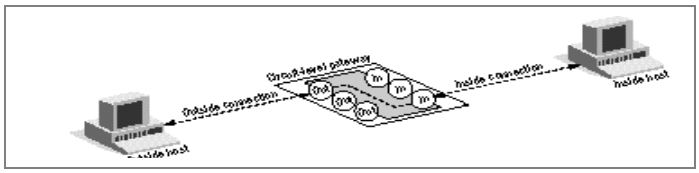


Figura 5: Uma conexão Telnet através de um gateway de circuito (Senna Junior, 2008)

5 GATEWAY DE APLICAÇÃO

Um gateway no nível (ou camada) de aplicação permite ao administrador de redes implementar uma política de segurança muito mais restritiva do que um roteador. Ao invés de contar com uma ferramenta genérica de filtragem de pacotes para gerenciar o fluxo de serviços da e para a Internet, uma aplicação especial (servidor Proxy) é instalada no gateway para cada serviço desejado. Se o servidor Proxy para uma dada aplicação não for instalado, o serviço não estará disponível e os pacotes correspondentes não atravessarão o firewall. Além disso, o servidor Proxy pode ainda ser configurado para permitir que apenas algumas características da aplicação sejam oferecidas, a critério do administrador.

A filtragem de pacotes num servidor Proxy continua, então, sendo efetuada, com a diferença de que, como o servidor examina intensivamente os pacotes recebidos no nível da aplicação (camada 7 do modelo OSI, ou camada 5 do modelo TCP/IP - veja figura 6), pode filtrar comandos específicos desta, o que seria impossível para um roteador. Assim, por exemplo, um serviço http pode estar sendo oferecido, mas determinados comandos, como http:post e http:get, podem ser bloqueados.

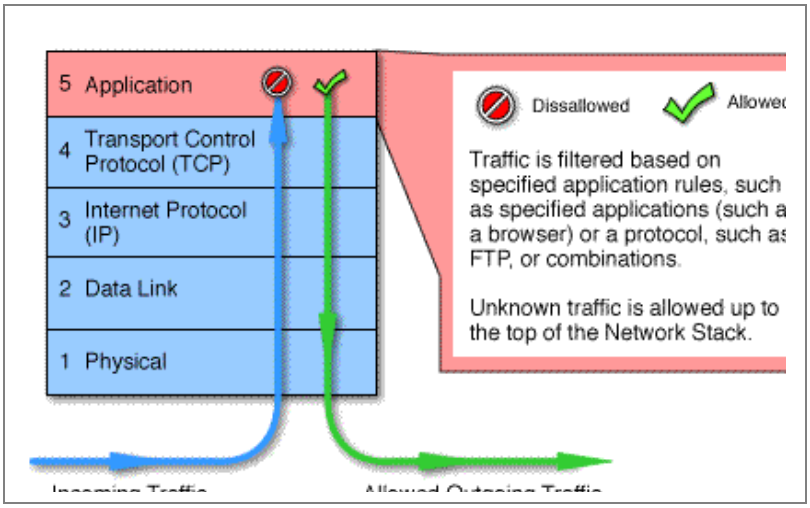


Figura 6: A posição da filtragem de pacotes usando um gateway de aplicação, como vista pelo modelo de camadas TCP/IP (Senna Junior, 2008).

Um esquema que esclarece a posição ocupada pelo servidor Proxy na filtragem de pacotes pode ser visto na figura 7. Com a presença do servidor Proxy, não há comunicação direta entre a rede interna e a Internet; a rede interna conecta-se ao computador que age como um gateway (ou portão de acesso) e este conecta-se à Internet, o que reduz as chances de um ataque externo e ainda permite a inspeção dos dados que passam através do firewall. Este computador é muitas vezes conhecido por *bastion host,* porque é o sistema especificamente projetado para suportar ataques externos.

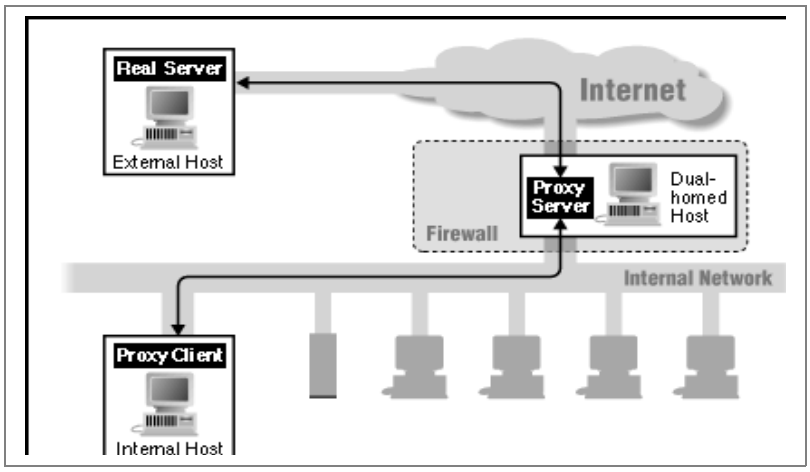


Figura 7: Um servidor Proxy entre a Internet e a rede interna (Senna Junior, 2008).

5.1 FIREWALL COM INSPEÇÃO DE ESTADO MULTI-CAMADA

Considerada a terceira geração dos firewalls, esta tecnologia de Inspeção de estado multicamada permite examinar cada pacote em todas as suas camadas do modelo OSI, desde a rede (camada 3) até a aplicação (camada 7), sem a necessidade de processar a mensagem. Com a tecnologia SMLI, o firewall usa algoritmos de verificação de dados da camada de aplicação (ao invés de executar

servidores Proxy específicos para cada aplicação), otimizados para altas velocidades de inspeção, enquanto os pacotes são simultaneamente comparados a padrões conhecidos de pacotes amigáveis. Por exemplo, ao ter acesso a algum serviço externo, o firewall armazena informações sobre a requisição de conexão original, tais como o número da porta, o endereço de destino e o de origem. No retorno da informação, o firewall compara os pacotes recebidos com as informações armazenadas, para determinar se serão admitidos na rede interna. Desta maneira, a SMLI oferece a velocidade e a transparência ao usuário típicas de um filtro de pacotes, aliadas à segurança e à flexibilidade de um gateway de aplicação.

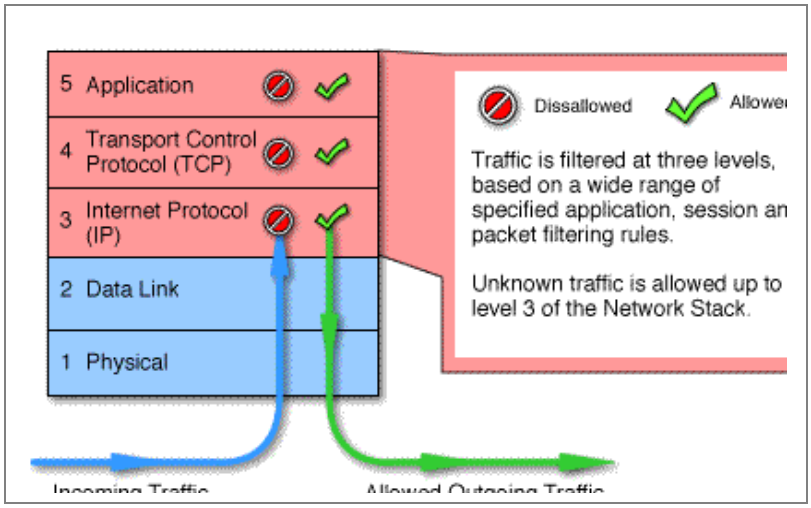


Figura 8: A posição da Inspeção de Estado Multi-Camada, como vista pelo modelo de camadas TCP/IP (Senna Junior, 2008).

A principal limitação desta tecnologia é que ela expõe os endereços IP das máquinas internas à rede, já que permite que os pacotes internos alcancem a Internet. Esta limitação pode ser contornada com a adição de servidores Proxy em conjunto, o que eleva ainda mais a segurança.

5.2 BASTION HOSTS

Os *bastion hosts* são os equipamentos que prestam serviços à Internet. Por estarem em contato direto com conexões externas, devem estar protegidos da melhor maneira possível. Estar protegido significa que um *bastion host* deve executar SOMENTE os serviços e aplicativos essenciais, bem como ter a última versão de atualizações e *patches* de segurança instalados em sua configuração, assim que disponibilizado ao mercado.

O *bastion host* é a ponte de interação com a zona desmilitarizada, pois os serviços disponíveis à DMZ devem ser impreterivelmente instaladas nestes equipamentos protegidos.

5.3 EXEMPLOS DE ARQUITETURAS DE FIREWALL

O sistema mais comum de firewall consiste em nada mais que um roteador com filtragem de pacotes, instalado entre a rede interna e a Internet, executando a tradicionais funções de rotear o tráfego de pacotes entre redes e usar regras de filtragem para aceitar ou não este tráfego. Neste arranjo, os computadores da rede interna têm acesso direto à Internet, enquanto os externos só dispõem de acesso limitado à rede interna. A política de segurança mais adotada nesta arquitetura é "tudo o que não for especificamente proibido é permitido fazer ".

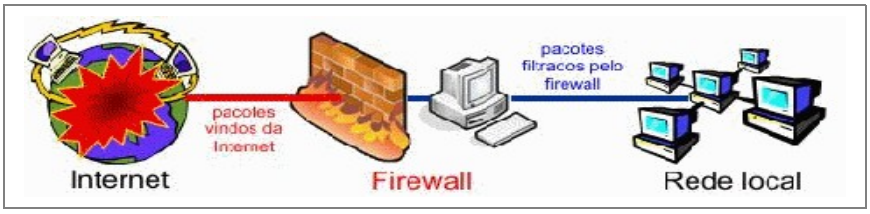


Figura 9: Roteador com filtragem de pacotes (Senna Junior, 2008)

Suas vantagens são o baixo custo e a transparência para os usuários. Por outro lado, apresenta as seguintes desvantagens:

• Exposição a ataques por configuração inadequada dos filtros;

• Exposição a ataques praticados através de serviços permitidos (já que não há exame do conteúdo dos pacotes);

• Necessidade de segurança adicional e autenticação de usuários para cada computador acessível a partir da Internet;

• Exposição da estrutura da rede interna (já que a troca de pacotes entre usuários internos e externos é permitida, há a exposição dos endereços IP internos);

• Se o roteador for atacado, toda a rede interna fica desprotegida.

O segundo exemplo de arquitetura emprega a filtragem de pacotes, que aliada a um computador especificadamente projetado e protegido contra ataques externos, o *bastion host*. Esta arquitetura provê maior grau de segurança porque implementa tanto a filtragem de pacotes, em primeira instância, quanto o fornecimento de serviços através de servidores Proxy (aplicações com finalidades especiais, instaladas no *bastion host*, que intermediam a comunicação entre os meios interno e externo, impedindo a direta troca de pacotes entre eles).

Neste assunto, um roteador com filtragem de pacotes é instalado entre o *bastion host* e a Internet. As regras de filtragem de pacotes só admitem que o tráfego externo tenha acesso ao *bastion host*; o tráfego dirigido a qualquer outro computador da rede interna é bloqueado.

Como os sistemas internos residem na mesma rede que o *bastion host*, a política de segurança determina se os sistemas internos terão acesso direto à Internet ou se deverão utilizar os serviços de Proxy concentrados no *bastion host*, o que pode ser reforçado pelo bloqueio de todo o tráfego de saída que não se origine no *bastion host.*

As vantagens deste arranjo são: um servidor público (que forneça serviços Web ou FTP, por exemplo) pode ser colocado no mesmo segmento da rede situado

entre o *bastion host* e o roteador, permitindo acesso direto de usuários externos sem comprometer a rede interna (protegida pelo *bastion host*); ou o mesmo servidor pode situar-se após o *bastion host* e estar disponível apenas através de serviços Proxy, tanto para usuários internos quanto externos.

5.4 FIREWALL ANFITRIÃO SELECIONADO

Um arranjo ainda mais seguro, visto na seguir, pode ser construído com um *bastion host* que apresenta duas interfaces de rede: uma com a rede interna e outra com a Internet, passando pelo roteador. Neste arranjo, conhecido por *dual-homed bastion host,* não há mais nenhuma possibilidade de acesso direto entre os sistemas da rede interna e a Internet; todo o tráfego é bloqueado no *bastion host* e o uso dos serviços de Proxy passa a ser compulsório mesmo para os usuários internos. Deve-se, entretanto, evitar que usuários externos tenham a possibilidade de efetuar um login diretamente ao *bastion host*, sob pena de comprometer a segurança obtida com este arranjo.

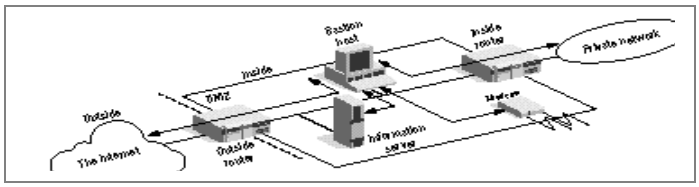


Figura 10: Firewall anfitrião selecionado (Senna Junior, 2008)

Este arranjo aplica ainda um *bastion host* e um roteador para acesso à Internet, mas adiciona um segundo roteador interno (na interface *bastion host* - rede interna), criando o que se convencionou chamar de "zona desmilitarizada", ou DMZ. Este arranjo é o que de mais seguro se pode gerar em termos de arquiteturas de firewall, pois aplica conceitos de segurança desde a camada de rede até a de aplicação, além de limitar o acesso a tudo o que é público (*bastion host*, servidores públicos, modems, etc.) a uma área restrita, a zona desmilitarizada. Esta funciona como se fosse uma pequena rede isolada, situada entre a Internet e a rede interna.

O tráfego direto através desta é proibido e os sistemas, tanto os internos quanto os externos, só têm acesso limitado à zona desmilitarizada.

Para o tráfego externo, o roteador mais externo oferece proteção contra os ataques externos mais comuns, bem como gerencia o acesso da Internet à sub rede DMZ. Somente o *bastion host* (ou, às vezes, o servidor público, dependendo da rigidez da política de segurança deste) está disponível para acesso. Já o roteador interno provê uma segunda linha de defesa, gerenciando o acesso da sub rede DMZ à rede interna, aceitando somente o tráfego originado no *bastion host*.

Para o tráfego de saída, as regras são semelhantes. Os sistemas internos à rede privada somente têm acesso ao *bastion host*, através do controle exercido pelo roteador interno. E as regras de filtragem do roteador externo exigem o uso de serviços Proxy para o acesso à Internet, ou seja, só permitem o tráfego externo que se origina do *bastion host.*

Este arranjo traz diversos benefícios importantes: três níveis de segurança (roteador externo, *bastion host* e roteador interno) separam a Internet do meio interno; somente a sub rede DMZ é conhecida na Internet, de modo que não há meio de se conhecerem rotas de acesso à rede interna; da mesma forma, somente a sub rede DMZ é conhecida para a rede interna e não existem rotas diretas para o acesso à Internet.

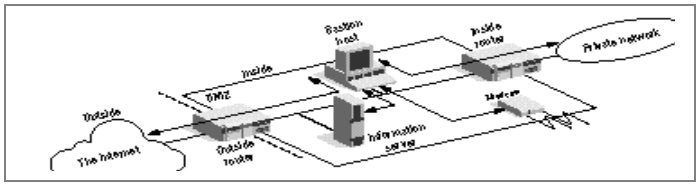


Figura 11: Selecionados sub-firewal (Senna Junior, 2008)**.**

6. A IMPLANTAÇÃO

Para impantação de sistema firewall com inspeção em multi-camadas na empresa, se faz necessário estruturar a rede interna de forma que a mesma venha a ter um ponto de saída para Internet, no caso o próprio firewall, e todo o tráfego com a Internet seja feito por um servidor Proxy, também fazendo com que a saída para Internet seja única, segura e também monitorável.

Também necessita-se de uma estação ou microcomputador para preparar esta versão do sistemas operacional com o novo firewall, portanto define-se uma máquina padrão de marca DELL, com microprocessador Pentium IV com velocidade de 2.26 GHz, com memória RAM de 1 Gbyte. É utilizado também um HD de 80 Gbytes, uma unidade de CD-ROM. Para contemplar o projeto também necessita-se que a estação incorporada à mothermoard da estação e outras do padrão PCI da marca 3COM.

Depois de verificados e configurados os quipamentos para estação, procedeu-se então com a instação do sistema operacional Linux Red Hat Versão 9. A instalação é feita através da unidade de CD-ROM da estação onde se faz necessário definir as partições do HD e os respetivos pontos de montagem.

- Uma partição de Swap (usado como memória) com tamanho de 1024 Mbytes e com formato de participação do tipo Linux Swap;

- Uma partição de Boot com tamanho de 1024 Mbyetes e com formato de partição do tipo ext3 (*third extended file system*);

- Uma partição Raiz (*/*)com o restante do tamanho do disco rígido e com formato de particão do tipo ext3.

Após a definição das partições, é instalado o sistema Linux, neste momento muitos administradores de rede preferem customizar a instalação do sistema retirando ou colocando alguns pacotes de instalação, mais neste caso foi escolhido uma instalação do tipo completa onde todos os pacotes necessários serão

instalados e não há necessidade de modificações futuras devido à falta de um pacote ou outro que seja necessário à implantação de algum outro serviço (CAETANO, 2011).

Finalizado a instalação, deve-se em seguida fazer a ligação de novo firewall ao ambiente de rede, estruturando a mesma conforme mostrada na figura 12.

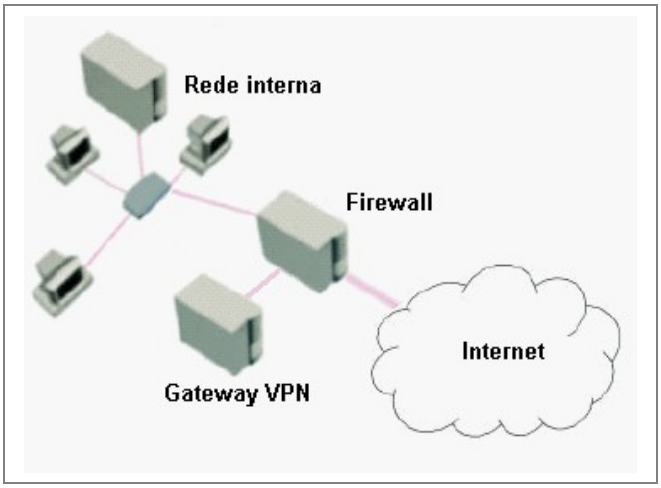


Figura 12 – Diagrama de ligação do novo Firewall à Rede (José Pinheiro, 2004*)*.

Após serem feitas todas a ligações do firewall à rede, procedeu-se agora à parte da configuração do mesmo para o funcionamento em multi-camadas, partindo então para configuração do L7-Filter, aplicando, todos os patches necessários.

CONCLUSÃO

Firewall vêm protegendo redes locais privadas de intrusos hostis a partir da Internet, de modo que o número de LANS hoje conectadas à Web é muito maior do que se esperaria, dados os riscos de segurança envolvidos. Estes sistemas permitem aos administradores de redes oferecerem acesso a serviços especificos da Internet a usuários internos selecionados, como parte de uma política de gerenciamento de informação que envolve que envolve não apenas a proteção da informação interna como também o conhecimento de quem acessa o quê na Web.

Logo a melhor solução de projeto de firewall para a redes dependerá de varios fatores, como a politica de segurança total da empresa, o conhecimento técnico do administrador da rede, o custo e o nível percebido de ameaças externas. A solução unirá estes fatores com o requisitos de serviços a oferecer externamente e aos usuários internos o grau de dificuldade no acesso que se imporá a estes.

REFERÊNCIAS

ANONYMOUS. Tradução Furmankiewicz, Edson e Figueiredo, Joana. Segurança máxima para Linux. Rio de Janeiro: Campus, 2000.

CAETANO, Jorge. Manual do linux red hat 9.0 Disponivel em: <http://www.linuxit.com.br/article2848.html>Acesso em 10 Out.2011.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. Segurança de redes em ambientes cooperativos. São Paulo: Berkeley, 2002.

PIRES. Fabiano. Implementando seu firewall com Layer 7. Disponível em: http://www.vivaolinux.com.br/artigo/verArtigo.php?codigo=4446. Acesso em 14 out.2011.

PINHEIRO. José. Projeto de Gateway VPN. Disponível em: http://www.projetoderedes.com.br/tutoriais/tutorial_projeto_de_gateway_vpn_01.ph. Acesso em 08 mar.2012.

SILVA, Lino Sarlo da. VPN – Virtual Private Network. São Paulo: Novatec, 2003.

SILVA, Lino Sarlo da. VPN – Public key Infrastruture – PKI. São Paulo: Novatec, 2004.

SENNA JUNIOR, Clovis. Segurança de redes com firewall. 2008. 39 f. : Monografia (Especialização) - Universidade Tecnológica Federal do Paraná. Curso de Especialização em Teleinformática e Redes de Computadores, Curitiba, 2008.

ULBRICH, Henrique César; VALLE, James Della. Universidade Hacker. São Paulo: Digerati, 2002.