

Universidade católica do Salvador
Curso: Informática
Matéria: Teleprocessamento e Redes
Professor: Marco Câmara

Trabalho sobre FIREWALL

Daniela Faria Carvalho
Abril - 2001

O que é firewall

"Antigamente, paredes de tijolos eram construídas entre construções em complexos de apartamentos de forma que se ocorresse um incêndio ele não

poderia se espalhar de uma construção para a outra. De uma forma completamente natural, as paredes foram chamadas de firewall". [Site da CLM]

Em redes de computadores, firewalls são barreiras interpostas entre a rede privada e a rede externa com a finalidade de evitar intrusos; ou seja, são mecanismos de segurança que protegem os recursos de hardware e software da empresa dos perigos aos quais o sistema está exposto. Estes mecanismos de segurança são baseados em hardware e software e seguem a política de segurança estabelecida pela empresa.

Atuantes como barreiras de segurança, firewalls são úteis em qualquer ponto estratégicos às redes ou sub-redes. Em algumas situações a empresa pode necessitar proteger partes da rede interna de outras partes da mesma rede corporativa. Neste caso, pode-se utilizar firewalls internos configurados de forma apropriada à segurança interna.

Quem Precisa?

Toda rede local com conexão dedicada à Internet precisa de proteção. É um engano pensar que somente as grandes corporações são alvo de hackers. Qualquer empresa com conexão dedicada à Internet é um alvo, pois as ferramentas automáticas de hackers atacam milhares de endereços por hora e penetram no primeiro site desprotegido.

A zona de risco é qualquer rede TCP/IP que pode ser diretamente acessada através da Internet. Deve-se ressaltar que os hosts que não estão conectados diretamente via TCP/IP não estão imunes aos ataques: se o atacante conseguir corromper a segurança de alguma máquina na rede TCP/IP privada, esta pode ser um ponto de acesso para que o atacante prossiga o seu ataque em outras máquinas que também não utilizem TCP/IP mas que estão diretamente conectadas à máquina invadida.

Riscos de Quem acessa a Internet

Há três principais perigos associados aos serviços fornecidos pela rede privada aos usuários externos na Internet:

- Hijacking: situação em que alguém rouba uma conexão depois que o usuário legítimo já realizou a sua autenticação;
- Packet Sniffing: situação em que alguém lê dados confidenciais enquanto eles transitam pela rede, sem interferir com a conexão;
- False authentication: situação em que alguém que não é um usuário válido convence o sistema de que ele é um usuário válido.

Quando se conecta à Internet, põe-se em risco três coisas: os dados; Os recursos (os próprios computadores) e a reputação da empresa.

Com relação aos dados, tem-se três características que precisam ser protegidas: O Segredo (privacidade); a Integridade e a Disponibilidade.

Mesmo que o intruso não danifique os dados, a simples utilização dos computadores (e demais recursos) pode ter conseqüências danosas: os recursos representam um substancial investimento da empresa, e o retorno financeiro depende da melhor utilização destes recursos, caso o atacante “compartilhe” tais recursos ele estará roubando tempo e dinheiro da empresa.

O que um firewall pode fazer

- Um firewall é um checkpoint; ou seja, ele é um foco para as decisões referentes à segurança, é o ponto de conexão com o mundo externo, tudo o que chega à rede interna passa pelo firewall;
- Um firewall pode aplicar a política de segurança;
- Um firewall pode logar eficientemente as atividades na Internet;
- Um firewall limita a exposição da empresa ao mundo externo.

O que um Firewall não pode fazer (até agora)

- Um firewall não pode proteger a empresa contra usuários internos mal intencionados;

- Um firewall não pode proteger a empresa de conexões que não passam por ele;
- Um firewall não pode proteger contra ameaças completamente novas: “qual será o próximo furo a ser descoberto?”
- Um firewall não pode proteger contra vírus.

Primeira geração - Filtros de pacotes

Esta geração inicial de firewall somente controlava a origem e o destino dos pacotes de mensagens da Internet. Atualmente, a filtragem de pacotes é implementada na maioria dos roteadores e é transparente aos usuários, porém pode ser facilmente contornada com IP Sniffers/Spoofers - técnicas usadas por hackers para iludir os roteadores, com a troca de endereços de origem. Por isto, o uso de roteadores como única defesa para uma rede corporativa não é aconselhável.

Segunda geração - Gateways e Proxies

Gateways para circuitos e aplicações conectam as redes corporativas à Internet através de estações seguras rodando aplicativos especializados para filtrar dados. Estes gateways permitem que usuários se comuniquem com os sistemas seguros através de um proxy, o qual esconde os arquivos e os servidores da ação dos hackers.

Terceira Geração - Stateful Multi-Layer Inspection

O Firewall de terceira geração, suporta a tecnologia SMLI- Stateful Multi-Layer Inspection ou seja: Inspeção de Estado Multi-Camada. Esta moderna tecnologia permite que o firewall examine cada pacote em todas suas camadas do modelo OSI, desde o transporte até a aplicação, sem necessidade de processar a mensagem.

Com a tecnologia SMLI o firewall usa algoritmos de verificação de tráfego otimizados para altas velocidades de inspeção. Simultaneamente, os pacotes são comparados a padrões conhecidos de pacotes amigáveis. Desta maneira a SMLI oferece a velocidade de um filtro de pacotes junto com a segurança de um gateway de aplicações, sendo totalmente transparente aos usuários e permitindo ao administrador adicionar novos serviços Internet em poucos minutos.

Estratégias de Segurança

Estas estratégias não são exclusivas de ambientes de sistemas de computação, são estratégias de segurança de uma forma geral mas são muito úteis quando consideradas em toda a sua extensão:

Least Privilege

O princípio do mínimo privilégio significa que qualquer objeto (usuário, administrador, programa, sistema, etc) deveria ter somente os privilégios que ele precisa para realizar as suas tarefas.

Mínimo privilégio é um princípio importante para limitar a exposição aos ataques e para limitar os danos causados por ataques. Deve-se explorar meios para reduzir os privilégios requeridos para as operações.

Há alguns problemas com a estratégia do privilégio mínimo, eis alguns:

- Pode ser complexo implementar caso os programas e ou protocolos não permitam estabelecer privilégios;
- Pode-se acabar implementando algo que tenha menos privilégios do que o mínimo estabelecido, acarretando em uma série de aborrecimentos por parte dos usuários

Choke Point

Esta estratégia força os atacantes a utilizarem um “canal estreito”, o qual pode ser monitorado e controlado. O firewall quando é o único ponto de acesso a rede privada, constitui-se em um choke point porque os atacantes necessariamente devem passar por ele.

Todos os choke points devem ser amplamente conhecidos e monitorados. Não adianta uma empresa ter um ótimo firewall se ela permite que funcionários conectados a uma rede TCP/IP interna acessem a Internet via linhas discadas. Caso isto ocorra, os atacantes terão portas abertas sem precisar enfrentar a grande muralha do firewall.

Defense in depth

De acordo com este princípio, não se deve depender de apenas um mecanismo de segurança não importando quão forte ele pareça ser. Ao invés disso, recomenda-se que sejam utilizados múltiplos mecanismos de segurança e que estes estejam configurados no nível mais alto possível de segurança e redundância. A estratégia

principal é fazer com que o ataque seja significativamente arriscado e caro ao atacante que se espera encontrar.

Weakest Link

"Uma corrente é tão segura quanto a mais fraca de suas argolas e uma parede é tão forte quanto o seu ponto mais fraco". Esta é uma noção fundamental à segurança dos sistemas de computação. Deve-se eliminar os pontos fracos, observando-se que o perigo ainda é maior quando uma ligação fraca também é um choke point.

Fail Safe

A Falha Segura estabelece que se um sistema falhar ele falha de tal forma que é negado o acesso ao atacante, não permitindo que ele entre. A falha também pode resultar que os usuários legítimos não tenham acesso até que os reparos sejam realizados, mas isso é bem melhor do que permitir que alguém (o intruso) entre e destrua tudo.

A principal aplicação desse princípio em segurança de redes está em escolher a postura do site com respeito a segurança. As duas principais posturas são:

- Postura padrão de negação: Especificar apenas o que é permitido e proibir o resto;
- Postura padrão de permissão: Especificar somente o que é proibido e permitir o resto.

A postura padrão de negação é uma postura fail safe. Entretanto, nem sempre a política de segurança agrada aos usuários do sistema. É necessário que se estabeleça uma relação amistosa entre o pessoal da administração da segurança e os usuários, esclarecendo estes acerca das medidas tomadas.

A postura padrão de permissão certamente não se enquadra como fail safe. Os únicos que de fato se beneficiam desta postura são os intrusos, porque o administrador do firewall não pode tapar todos os buracos nos serviços disponíveis e naqueles que surgem no correr do tempo. Enquanto ele está ocupado tentando resolver alguns problemas com algum serviços os atacantes se deliciam atacando em outros pontos.

Universal Participation

É necessário que os usuários da rede tenham consciência da necessidade dos mecanismos de segurança adotados. Esta consciência deve ser construída de uma forma polida, mostrando ao usuário que as medidas vêm em benefício deles e de toda a corporação. Para que haja participação, ou pelo menos não haja oposição, a compreensão dos usuários deve ser conquistada de forma voluntária. Qualquer inimigo dentro da empresa pode ser a grande brecha na segurança da corporação.

Diversity of Defense

Através da estratégia defense in depth se acrescenta segurança através de um certo número de diferentes sistemas. Analogamente, com a estratégia de diversity of defense, adiciona-se segurança utilizando um número de diferentes tipos de sistemas.

A idéia por detrás desta estratégia é que utilizando sistemas de segurança de diferentes fornecedores pode reduzir as chances de existir um bug ou erro de configuração comum aos diferentes sistemas. No exemplo citado anteriormente, caso os dois packet filters utilizados sejam do mesmo tipo, fica mais fácil para o atacante pois ele poderá explorar o mesmo problema da mesma forma em ambos.

É importante que se tenha cuidado com diferentes sistemas configurados pela mesma pessoa (ou grupo de pessoas) pois é provável que os mesmos erros cometidos em um sistema estejam presentes nos outros devido a compreensão conceitual errada sobre alguns aspectos.

Simplicidade

Simplicidade é uma estratégia de segurança por duas razões:

- Coisas simples são mais fáceis de serem compreendidas (se não se compreende alguma coisa, não se pode realmente saber se ela é ou não segura);
- A complexidade proporciona esconderijos de todos os tipos de coisas (é mais fácil proteger uma sala do que todo um prédio).

Type Enforcement

Type enforcement é um mecanismo de segurança que atribui a todo programa no sistema permissão para fazer somente aquelas coisas que ele precisa fazer para executar o seu trabalho. Isto é chamado least privilege e aplica a programas, arquivos e Sistemas Operacionais. Entretanto, este mecanismo também aborda as estratégias defense in depth e fail safe porque caso algum programa seja comprometido proposital ou acidentalmente a falha não se propagará além do

ambiente restrito onde o programa estiver executando; ou seja, além de se poder investir na segurança do próprio serviço, tem-se a redundância na segurança a nível de sistema operacional e se garante que a falha não permitirá maiores danos ao sistema.

Arquiteturas de Firewall

O Firewall consiste em um conjunto de componentes organizados de uma forma a garantir certos requisitos de segurança. Os componentes básicos para a construção de um firewall são:

- Packet Filter: são responsáveis pela filtragem (exame) dos pacotes que trafegam entre dois segmentos de rede.
- Bastion Host: computador responsável pela segurança de um ou mais recursos (serviços) da rede.

Determinadas arquiteturas recebem denominações especiais e servem como referência para a construção de uma infinidade de variantes. As arquiteturas Screened Subnet e Screened Host podem ser consideradas clássicas. Destacam-se porque são resultantes de uma disposição básica dos componentes packet filter e bastion host.

Packet Filters

Como um primeiro passo ao se implementar uma barreira de segurança em uma rede de computadores, é fundamental que se conheça os detalhes dos protocolos de comunicação utilizados. Na Internet, a atenção deve ser voltada aos protocolos IP, TCP, ICMP e UDP. Estes são os principais protocolos a nível de rede e transporte (Modelo OSI) que são considerados e examinados ao se estabelecer regras de filtragem em um packet filter para a Internet. Este mecanismo de filtragem a nível de roteador possibilita que se controle o tipo de tráfego de rede que pode existir em qualquer segmento de rede; conseqüentemente, pode-se controlar o tipo de serviços que podem existir no segmento de rede. Serviços que comprometem a segurança da rede podem, portanto, ser restringidos.

Com o exposto acima, fica evidente que um packet filter não se encarrega de examinar nenhum protocolo de nível superior ao nível de transporte, como por exemplo o nível de aplicação que fica como tarefa dos application gateways (proxy servers). Portanto, qualquer falha de segurança a nível de aplicação não pode ser evitada utilizando somente um packet filter.

Bastion Host

Bastion host é qualquer máquina configurada para desempenhar algum papel crítico na segurança da rede interna; constituindo-se na presença pública na

Internet, provendo os serviços permitidos segundo a política de segurança da empresa.

Um bastion host deve ter uma estrutura simples, de forma que seja fácil de garantir a segurança. É importante que se esteja preparado para o fato de que o bastion host seja comprometido, considerando que ele provavelmente (dependendo do site) será alvo de ataques.

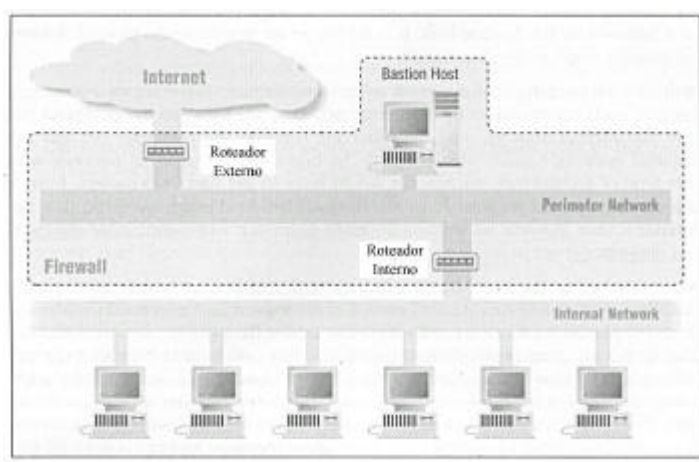
O bastion host tem responsabilidades diferentes do packet filter, dependendo do seu tipo. Alguns autores enfatizam que enquanto o packet filter atua em um nível mais baixo o bastion host se encarrega de todos os níveis (referentes ao modelo OSI). Na realidade, um host pode acumular tanto as funções de filtragem de pacotes como também pode prover alguns serviços; neste caso, ele seria um packet filter e bastion host simultaneamente (exemplo: dual homed host). Independentemente de qual seja a nomenclatura adotada, o que se deve ter em mente é o papel que estes dois componentes desempenham: filtragem e provedor de serviços. Traçando um paralelo destes dois componentes em relação ao modelo OSI, o packet filter realiza algum exame dos pacotes até o nível 4 (transporte) enquanto que o bastion host se encarrega basicamente dos níveis superiores (fundamentalmente o de aplicação, nível 7).

Screened Subnet

Composta por componetes mais básicos (packet filters e bastion hosts) esta é uma arquitetura que apresenta múltiplos níveis de redundância e provê um bom esquema de segurança, constituindo-se em um exemplo clássico de arquiteturas de firewall. Os componentes deste tipo de firewall incluem os seguintes:

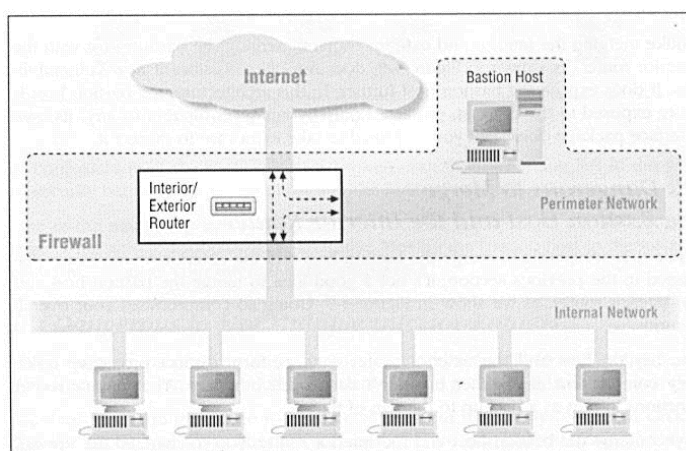
- Perimeter Network: constitui-se numa sub-rede situada entre a rede interna e a rede externa (Internet);
- Roteador externo: diretamente conectado à Internet e à perimeter network;
- Roteador interno: diretamente conectado à rede interna e à perimeter network;
- Bastion hosts residentes na perimeter network.

Screened Subnet:



Ao invés de se utilizar dois roteadores, o que pode ser muito caro dependendo dos recursos disponíveis, pode-se utilizar um único roteador com três interfaces de rede mas que possibilite aplicar as regras de filtragem em cada interface em ambos os sentidos. Neste caso, a solução seria um pouco mais complexa porque teria de se executar uma junção dos dois conjuntos de filtragem adotados no roteador externo e interno, agora substituídos por um único roteador.

Screened Subnet utilizando um único roteador:



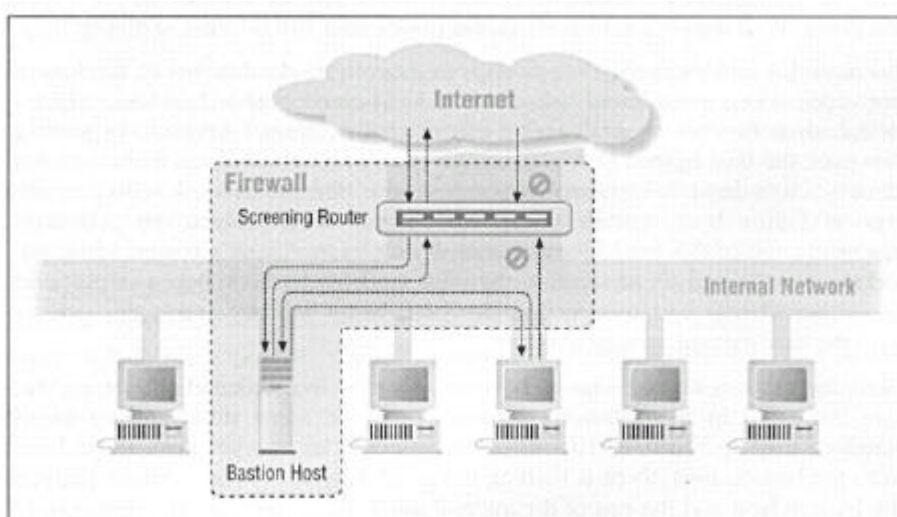
Há alguns servidores secundários localizados na rede interna, fazendo para com alguns servidores primários localizados nos bastion hosts (mail servers, news servers, DNS servers, etc).

Definidos os serviços a serem providos, pode-se elaborar as regras de filtragem para os roteadores externo e interno. Vale ressaltar que um pouco de redundância sempre ajuda e, como alternativa, repete-se algumas das regras de filtragem

adotadas no roteador externo também no roteador interno, de forma que o interno ainda se configure como uma barreira caso o externo seja atacado com sucesso.

Screened Host

Nesta arquitetura não há uma sub-rede de segurança (perimeter network) entre a Internet e a rede Interna. Existem apenas um screening router e um bastion host situado junto à rede interna. Esta não é uma arquitetura muito segura.



Conclusão

Hoje em dia já se tornou indispensável o uso do FIREWALL. Não tem como se construir uma rede sem proteção

Bibliografia:

- Sites da Internet

Questões Comentadas:

1. Explique o que se entende por Firewall.

Firewall é um mecanismo que protege a rede interna de invasores, que conseguem entrar via redes externas diretamente conectadas a essas redes internas.

ex: Internet

2. Quais os componentes necessários para se construir um firewall?

O Packet Filter, que são responsáveis pela filtragem (exame) dos pacotes que trafegam entre dois segmentos de rede.

O Bastion Host que é computador responsável pela segurança de um ou mais recursos (serviços) da rede.

3. Porque é importante conhecer a política de segurança da empresa, antes de se construir um firewall?

Porque para cada caso em particular tem-se arquiteturas compatíveis com cada necessidade. Tanto visando a economia, quanto a maior segurança.