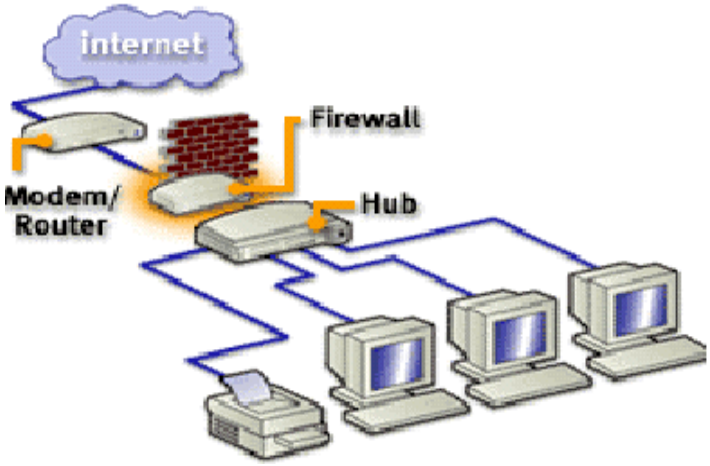
www.projetoderedes.com.br
Gestão da Segurança da Informação
Professor: Maurício
AULA 09 – Firewall

O que é Firewall

Um Firewall é um sistema para controlar o aceso às redes de computadores, desenvolvido para evitar acessos não autorizados em uma rede local ou rede privada de uma corporação. Esse sistema pode ser desempenhado por um dispositivo implementado em hardware ou software.

A RFC 2828 (Request for Coments nº 2828) define o termo firewall como sendo uma ligação entre redes de computadores que restringem o tráfego de comunicação de dados entre a parte da rede que está “dentro” ou “antes” do firewall, protegendo-a assim das ameaças da rede de computadores que está “fora” ou depois do firewall. Esse mecanismo de proteção geralmente é utilizado para proteger uma rede menor (como os computadores de uma empresa) de uma rede maior (como a Internet).



Um Firewall deve ser instalado no ponto de conexão entre as redes, onde, através de regras de segurança, controla o tráfego que flui para dentro e para fora da rede protegida. Pode ser desde um único computador, um software sendo executado no ponto de conexão entre as redes de computadores ou um conjunto complexo de equipamentos e softwares.

Deve-se observar que isso o torna um potencial gargalo para o tráfego de dados e, caso não seja dimensionado corretamente, poderá causar atrasos e diminuir a performance da rede. Os Firewalls oferecem as seguintes funcionalidades:

- Capacidade para direcionar o tráfego para sistemas internos mais confiáveis;

- Proteção de sistemas vulneráveis ou críticos, ocultando informações de rede como nome de sistemas, topologia da rede, identificações dos usuários, etc;

- Mecanismo de defesa que restringe o fluxo de dados entre redes podendo criar um “log” do tráfego de entrada e saída da rede;

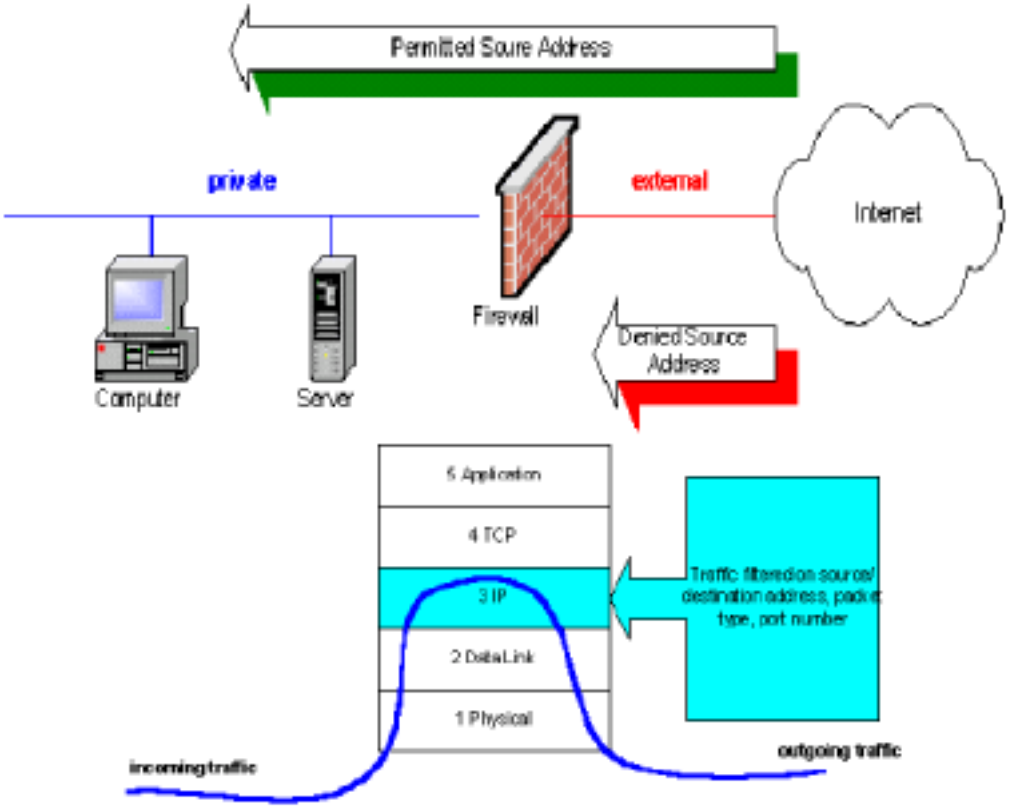
- Concentrar os problemas de segurança em um único ponto;

- Autenticação de usuários na rede.

Implementação

Existem várias técnicas usadas na implementação de firewalls, dentre as quais pode-se citar:

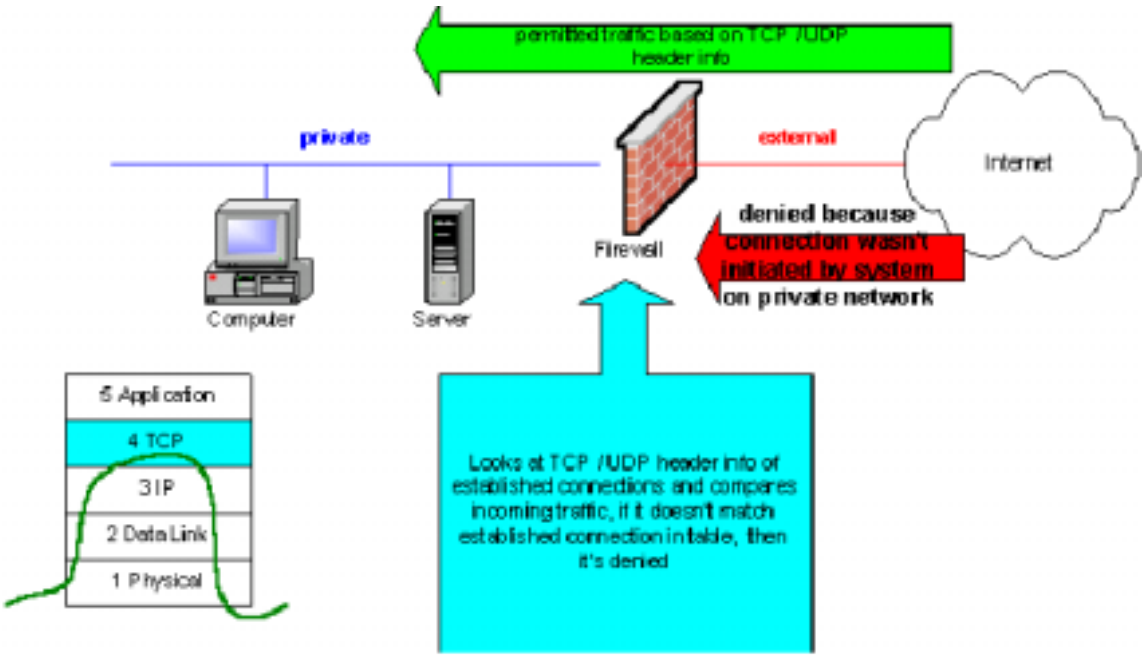
- **Filtragem de pacotes**: Mais simples, porém menos segura, a técnica permite ou não o acesso baseado no endereço origem / destino ou na porta origem / destino do protocolo de comunicação utilizado. Utiliza-se de uma relação de endereços confiáveis para permitir ou não o acesso. Por filtrar apenas os endereços, está sujeito a ataques de spoofing Trabalha na terceira camada do modelo OSI (IP);



O uso mais genérico está em evitar que usuários externos acessem recursos particulares de uma rede de computadores. Uma das tarefas de um firewall é garantir que as comunicações de / para a Internet estejam de acordo

com preceitos de segurança. Da mesma maneira devem ser colocados Firewalls dentro da rede local de computadores de forma a proteger os dados da corporação (financeiros, pessoais, de pesquisas, etc) contra invasões internas.
Todavia, um Firewall não poderá proteger uma rede contra conexões que não passam por ele ou contra novas ameaças que não estejam previstas na sua programação.

- **Stateful Packet Inspection** (Inspeção de Estado de Pacote): permite ou não o acesso, analisando não apenas as informações utilizadas na filtragem de pacotes, mas também analisa o cabeçalho de cada pacote de informação que chega, verificando se pertence a uma conexão interna. Ou seja, se chegar ao firewall um pacote que não foi solicitado por algum terminal de dentro da área protegida, o pacote é bloqueado. Trabalha na quarta camada do modelo OSI (TCP);



- **Proxy Firewall:** nesse tipo de implementação, toda a comunicação é direcionada ao firewall. Este, recebendo uma solicitação de pacote para ser enviada a rede externa, examina suas políticas de segurança. Se o pacote atendê-las, envia-o para o destino, mas, com o endereço IP do firewall, protegendo o verdadeiro endereço de origem da solicitação. Ao receber um pacote de respostas, examina seu conteúdo e em seguida verifica se o pacote pertence a uma solicitação interna. Em caso positivo, repassa-o então ao solicitante. Trabalha na quinta camada do modelo OSI.

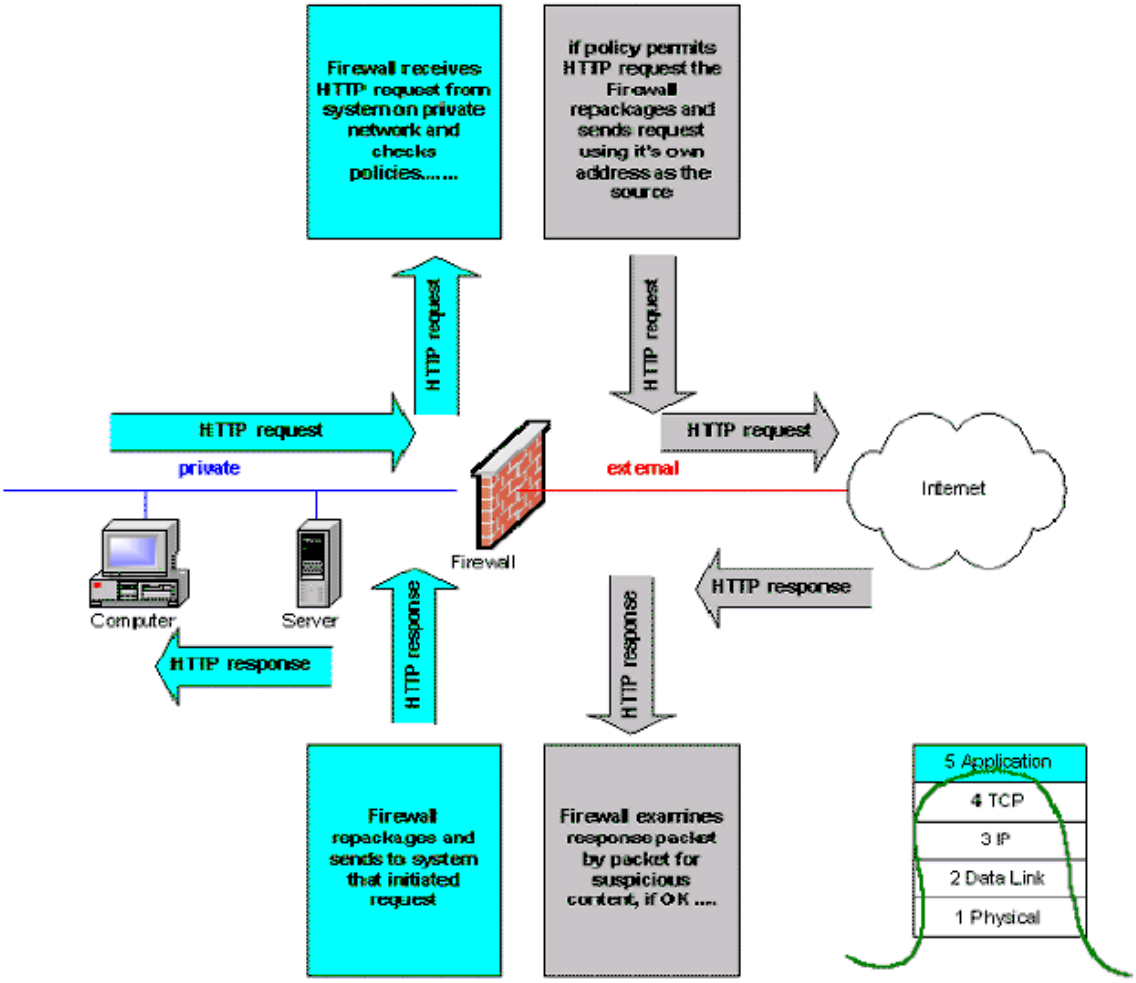


Figura 1 - Esquema de Firewall Proxy

Categorias de Firewall

Os sistemas de Firewall disponíveis comercialmente se diferenciam de duas maneiras: quanto ao seu conjunto de características e quanto à sua arquitetura básica.

Quanto às características, os Firewalls geralmente são divididos em duas categorias:

1. Firewall em nível de aplicação

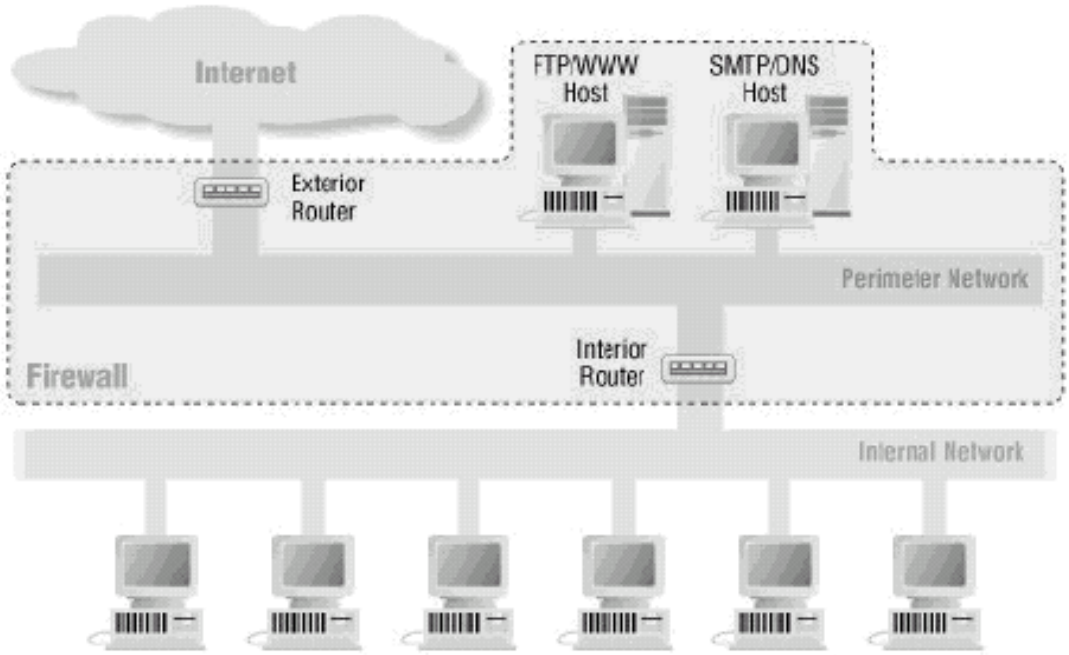
Um Firewall de aplicação (Application-level ou "proxy" server), também conhecido como Bastion Host (gateway de aplicação) não permite que nenhum pacote passe diretamente da rede externa para a rede corporativa. A RFC 2828 (Request for Coments nº 2828) define como sendo um computador fortemente protegido contra ataques, podendo ser parte de um firewall, sendo o único

computador da rede que pode ser acessado diretamente pelo lado de fora do firewall. Geralmente, está localizado no perímetro da rede entre a parte interna e protegida e a Internet, por exemplo.

Primeiramente verifica se um pedido de acesso realizado por um usuário a um site ou serviço disponível na Internet é permitido – validação de usuário e senha para acesso, por exemplo, de sites de pornografia ou serviço de ICQ, por exemplo. Todos os pacotes são enviados a um servidor de proxy. O proxy determina quando se deve ou não estabelecer a conexão e deve conhecer a aplicação e, se uma nova aplicação for necessária na rede, deve obter com o fornecedor um novo código que a contemple. Se o acesso é autorizado, o firewall realiza o papel de intermediário, realizando a conexão com o site ou serviço na Internet conforme solicitado pelo usuário, repassando-o as páginas, imagens e outras informações provenientes da Internet.

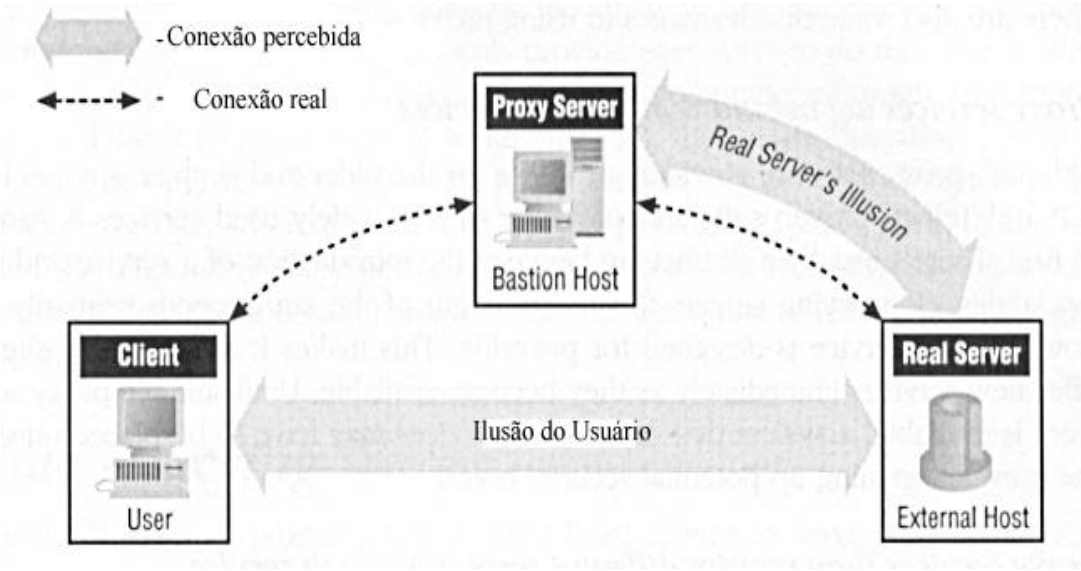
Um firewall ou um roteador funcionando como bastion host, pode ser projetado com a finalidade de ser um servidor Web, servidor FTP, dentre outras funções que estiverem disponíveis a usuários de fora da proteção da interna da rede. Também pode ser projetado como chamariz para crackers, também conhecidos como honey pot. Sua função é justamente atrair a atenção dos invasores com vulnerabilidades propositadamente deixadas para que se possam coletar dados de eventuais tentativas de invasão e posterior proteção.

A sua configuração é totalmente diferente de um computador comum. Devido ao seu papel específico dentro da rede, todos os protocolos, programas e portas são removidos se não forem estritamente necessários ao funcionamento. A figura seguinte representa uma rede protegida por dois bastion hosts, um com a função de servidor WWW e FTP e outro com a função de servidor SMTP e DNS.


Internet
FTP/WWW
Host
SMTP/DNS
Host
Exterior
Router
Perimeter Network
Interior
Router
Firewall
Internal Network

As características principais de um Bastion Host são as seguintes:

- Gateway de aplicação (verifica protocolos da camada de aplicação);
- Papel crítico na segurança da rede interna, funcionando como intermediário entre o cliente da rede interna e o servidor remoto;
- Recurso de controle de acesso;
- Registro do tráfego.



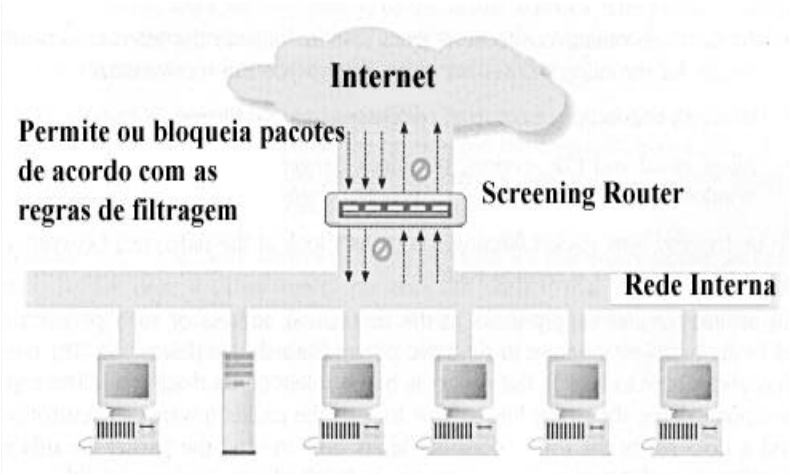
As características principais do Proxy Server são as seguintes:

- Atua como um procurador;
- Cliente não necessita DNS;
- Cliente deve suportar Proxy;
- Geralmente implementa recurso de Cache;
- Necessidade de somente um IP válido;
- Pode possuir recursos para verificação de vírus.

2. Firewall em nível de rede

Um Firewall de Rede (Network-level ou "packet-filtering" firewall) também conhecido como Packet Filter (filtro de pacotes) atua ao nível de rede examinando as informações solicitadas pelos usuários da Internet, servindo como intermediário entre a corporação e a Internet. No seu projeto, os dados (pacotes IP) chegam até ele. Dependendo de regras de filtragem embutidas em seu sistema operacional, ele decide se os deixa passar ou não para a rede local.

Cada solicitação é examinada, e, quando solicitações ilícitas são realizadas, essas são bloqueadas, para que não sejam encaminhadas para a estrutura interna da organização, evitando danos aos dados existentes na estrutura da empresa bem como a disponibilização de informações confidenciais da corporação à Internet.



Um filtro de pacotes atua até a camada de transporte e pode filtrar:

- Endereço de origem e destino;
- Protocolos: TCP, UDP ou ICMP;
- Portas de origem e destino: TCP ou UDP;
- Tipo de mensagem ICMP;
- Interface de rede de entrada e saída;
- TCP Flags (Ex. flag ACK)

As características desejáveis em um Screening Router são:

- Boa performance na filtragem;

- Hardware dedicado;

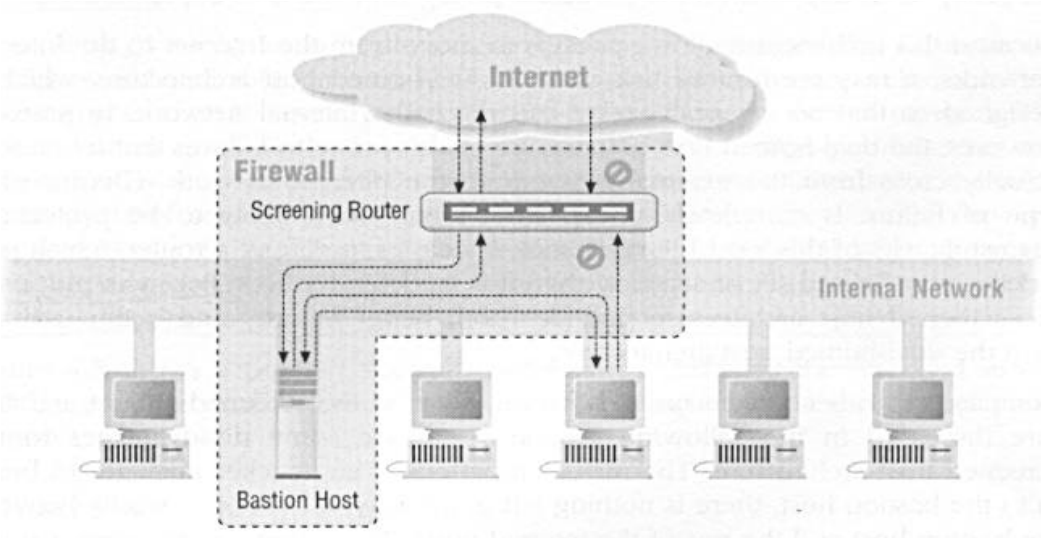
- Permitir especificação de regras;

- Aplicar regras na ordem especificada;
- Aplicar as regras nos pacotes que chegam e partem em cada interface de rede;

- Registros de pacotes aceitos e/ou rejeitados, bloqueando os que não satisfazem nenhuma regra.

Firewall Híbrido

Também são conhecidos como Screened Host. Embora o projeto de um Firewall de filtro de pacotes seja considerado o mais rápido e flexível em comparação com o Firewall de aplicação, muitas organizações combinam as vantagens de ambos para obterem um nível maior de segurança e performance em suas redes.



Arquitetura Básica

Os sistemas de Firewall disponíveis oferecem combinações de características variadas. Algumas são essenciais, outras necessárias apenas em circunstâncias especiais. A seguir serão apresentadas as básicas que um Firewall deve apresentar em sua configuração:

- **Controle de acesso básico**: controlar o acesso à rede. Alguns Firewalls oferecem controles de acesso fáceis de administrar e difíceis de burlar;

- **Serviços suportados**: Protocolos (ao nível de aplicação) que o Firewall reconhece. Um Firewall ao nível de aplicação deve ter um serviço de proxy para cada aplicação. Os Firewalls filtros de pacotes suportam todos os serviços conhecidos (DNS, Finger, FTP, Gopher, ICMP, IRC, Mail, Telnet, WWW);

- **Autenticação de usuários**: Os Firewalls ao nível de aplicação normalmente utilizam esse conceito, interrompendo aplicações e exigindo aos usuários que se autentiquem antes de continuarem a conexão no destino requisitado;

- **Redes privadas virtuais:** Como o Firewall é a porta de entrada da corporação nada mais natural do que utilizá-lo como servidor VPN e ser o responsável pela autenticação dos usuários;

- **Administração**: Oferecer uma interface gráfica com recursos de auxilio ao operador que permitam que mesmo uma pessoa não especializada possa gerenciá-lo facilmente;

- **Auditoria e alarmes:** os administradores de Firewall devem ser notificados quando da tentativa de uma invasão;

- **Alta performance:** Firewalls lentos podem ser um sério gargalo na rede;

- **Mapeamento de endereços:** Alguns Firewalls trocam (dinamicamente) os endereços ilegais pelos endereços legais quando os pacotes saem para a Internet em uma operação chamada NAT;

- **Controle de conexões permitidas**: Essa característica ajuda a evitar ataques do tipo sobrecarga da rede ("flooding attacks")

Vantagens na utilização de Firewall

Vários objetivos para a segurança de uma rede de computadores podem ser atingidos com a utilização de Firewalls. Dentre eles destacam-se:

- **Segurança**: Evitar que usuários externos, vindos da Internet, tenham acesso a recursos disponíveis apenas aos funcionários da empresa autorizados. Com o uso de firewalls de aplicação, pode-se definir que tipo de informação os usuários da Internet poderão acessar (somente servidor de páginas e correio eletrônico, quando hospedados internamente na empresa);

- **Confidencialidade**: Pode ocorrer que empresas tenham informações sigilosas veiculadas publicamente ou vendidas a concorrentes, como planos de ação,

metas organizacionais, entre outros. A utilização de sistemas de firewall de aplicação permite que esses riscos sejam minimizados;

- **Produtividade**: É comum que os usuários de redes de uma corporação acessarem sites na Internet que sejam improdutivos como sites de pornografia, piadas, chat, etc. O uso combinado de um firewall de aplicação e um firewall de rede pode evitar essa perda de produtividade;

- **Performance**: O acesso a Internet pode tornar-se lento em função do uso inadequado dos recursos. Pode-se obter melhoria de velocidade de acesso a Internet mediante controle de quais sites podem ser visitados, quem pode visitá-los e em que horários serão permitidos. A opção de geração de relatórios de acesso pode servir como recurso para análise dos acessos.