Firewall

- Firewall é um sistema de proteção de redes internas contra acessos não autorizados originados de uma rede não confiável (Internet), ao mesmo tempo que permite o acesso controlado da rede interna à Internet
- Normalmente envolve hardware e/ou software
- Existem diversos níveis de proteção diferentes (pacotes, e-mails, navegação, etc.)

Características de Firewalls

- Todo tráfego entre a rede interna e a externa (entrada e saída) deve passar pelo Firewall
- Somente o tráfego autorizado passará pelo Firewall, todo o resto será bloqueado
- O Firewall em si deve ser seguro e impenetrável

Controles do Firewall

- Controle de Serviço: determina quais serviços Internet (tipos) estarão disponíveis para acesso
- Controle de Sentido: determina o sentido de fluxo no qual serviços podem ser iniciados
- Controle de Usuário: controla o acesso baseado em qual usuário está requerendo (tipicamente os internos, ou externo via VPN)
- Controle de Comportamento: controla como cada serviço pode ser usado (ex: anti-spam)

Recursos do Firewall

- O Firewall define um ponto único de ligação que oferece proteção a uma rede interna
  - Pelo fato de ser um ponto único, o gerenciamento dessa tarefa de proteção é mais fácil
- O Firewall provê uma localização para o monitoramento de eventos relacionados com segurança
  - Através de auditorias, históricos e alarmes

Recursos do Firewall

- O Firewall é uma plataforma conveniente também para:
  - NAT (Tradução de Endereço de Rede)
  - Proxy de Web
  - Gateway de email
- O Firewall pode servir como plataforma para VPN
  - Pode implementar Ipsec, ou outro protocolo

Limitações de um Firewall

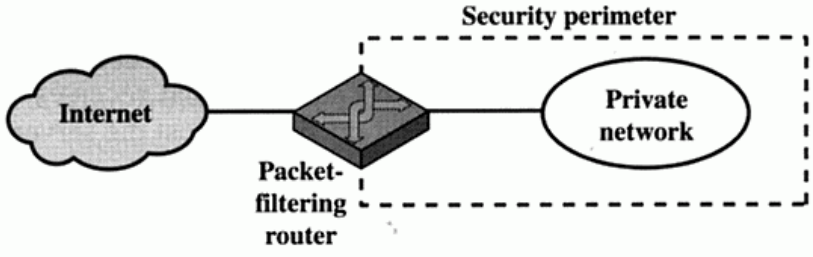
- O Firewall não protege contra ataques vindos de outras fontes:
  - conexões diretas (ex: modem) de máquinas internas para ISPs
  - modems de entrada não passando pelo firewall
- O Firewall não protege contra ameaças internas
- O Firewall não protege contra transferência de arquivos infectados por vírus
  - Seria impraticável analisar o conteúdo de tudo que trafega

Tipos de Firewall

- Existem três tipos de Firewall:
  - Filtragem de pacotes
  - Gateways de aplicação
  - Gateways a nível de circuito

Filtragem de Pacotes

- Proteção é baseada na filtragem de pacotes entre as redes externa e interna



Filtragem de Pacotes

- 2 políticas de aplicação de regras aplicáveis aos pacotes IP:
  - Padrão = Descartar: tudo o que não é expressamente permitido, é proibido (**+ seguro**)
  - Padrão = Encaminhar: tudo o que não é expressamente proibido, é permitido
- Pacotes não autorizados são descartados
- As regras são criadas pelo administrador
- Regras baseadas nos campos dos pacotes transmitidos (normalmente IP, TCP e UDP)

Filtragem de Pacotes

- Exemplo:
  - bloqueia qualquer conexão com SPIGOT
  - permite receber conexões na porta 25 (SMTP) para o host OUR-GW
  - Permite o uso do servidor de envio de e-mail, exceto quando o outro servidor é SPIGOT

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Filtragem de Pacotes

- Exemplo:
  - permite conexões para fora na porta 25 (SMTP) em qualquer host

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

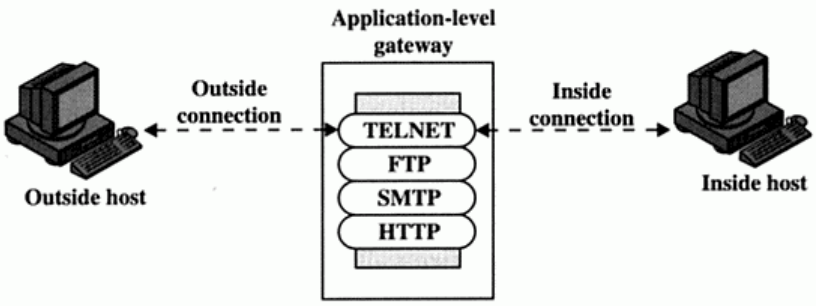
Filtragem de Pacotes

- Exemplo melhorado:
  - permite conexões para fora na porta 25 (SMTP) em qualquer host
  - permite receber pacotes TCP de ACK (somente confirmação) na porta 25 (SMTP)

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Gateways de Aplicação



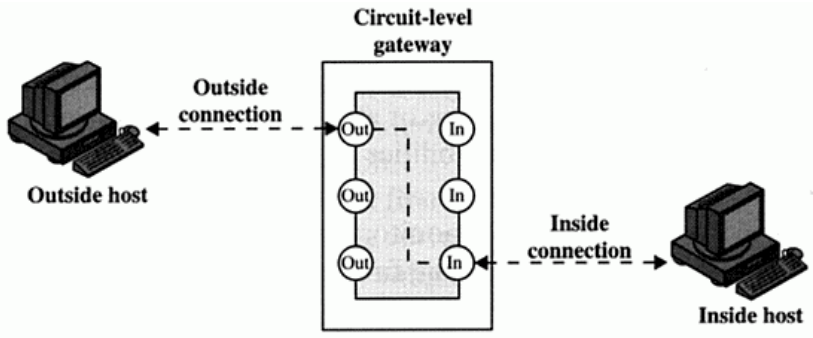
Gateways de aplicação

- O gateway de aplicação recebe uma conexão para uma aplicação suportada
- Autentica o usuário externo através de senha
- Para usuários válidos uma segunda conexão para um servidor interno é estabelecida
- Todo tráfego é roteado entre ambas conexões
- Funciona somente em aplicações "conhecidas"

Gateways de Aplicação

- Firewall gateways de aplicação tendem a ser mais seguros que filtros de pacote
- Ao invés de filtrar pacotes com base em regras que cercam inúmeras possibilidades, permitem conexões desde que sejam de aplicações permitidas
- A grande desvantagem é o trabalho extra de identificação feito pelo gateway em cada conexão

Gateways a Nível de Circuito



Gateways a Nível de Circuito

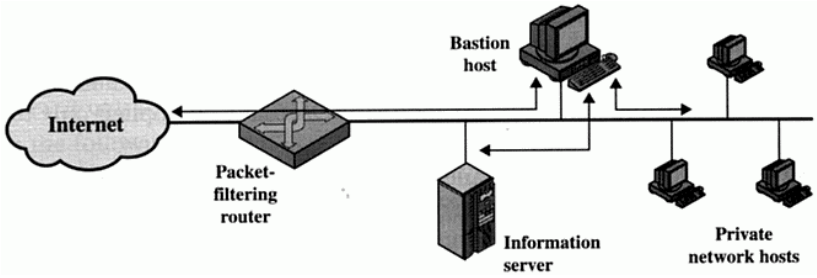
- O Firewall não permite que conexões TCP sejam estabelecidas diretamente através dele
- Para cada conexão até o Firewall, o mesmo cria uma segunda até o destino
- O tráfego não é monitorado
- A segurança vem do fato de que nem todas as conexões são permitidas
- O SOCKS é um Firewall a nível de circuito

Estação Bastião

- Estação bastião é uma máquina segura instalada em um ponto crítico da rede
- Executa um sistema operacional estável e serguro e um conjunto mínimo, seguro e controlado de serviços
- Pode ser plataforma para Firewalls gateways de aplicação ou a nível de circuito
- Normalmente é proxy de serviços Internet
- Pode ser usado conectado a uma rede, duas ou como subrede

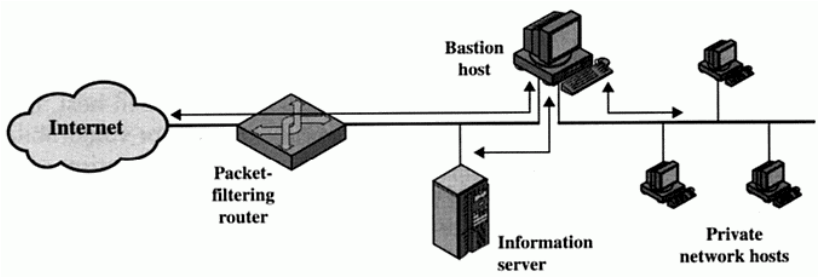
Bastião em uma Rede

- Não existe isolamento a nível de rede do bastião para as máquinas protegidas
- O filtro de pacotes permite conexão de/para Internet apenas entre ela e o bastião



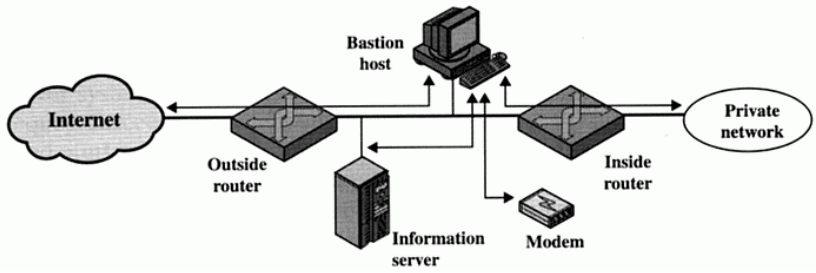
Bastião em duas redes

- O acesso para a rede protegida passa obrigatoriamente pelo bastião
- A segurança do fluxo não depende somente do filtro de pacotes



Bastião em outra sub-rede

- A rede interna é protegida por outro Firewall
- Define sub-rede restrita entre os roteadores
- A Internet só enxerga a sub-rede. A rede interna também



Atualização de Firewall

- Os principais recursos de firewall normalmente são software (mesmo quando está instalado em um hardware específico)
- Software tem falhas que são descobertas com o tempo
- É essencial que o software do Firewall seja constantemente atualizado
- Análise permanente dos logs também é muito importante