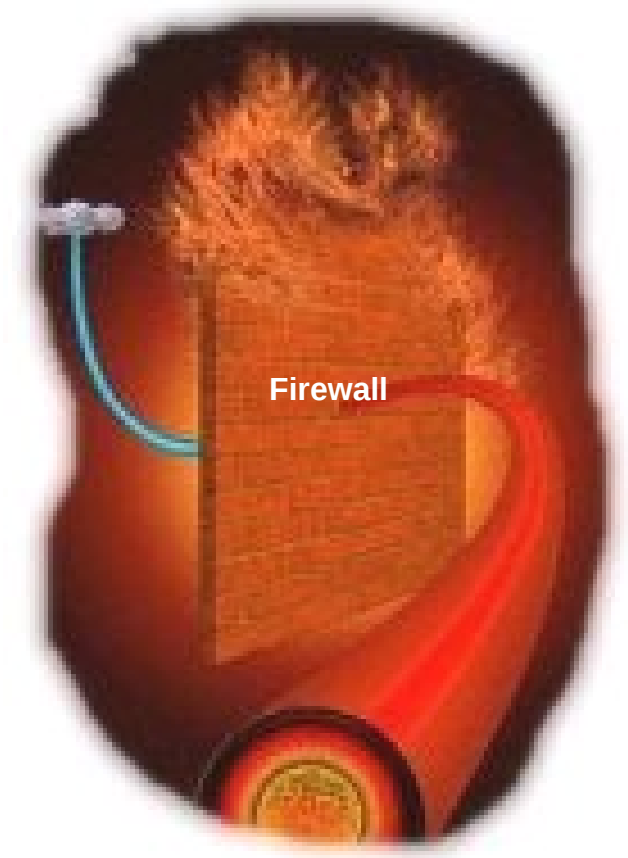
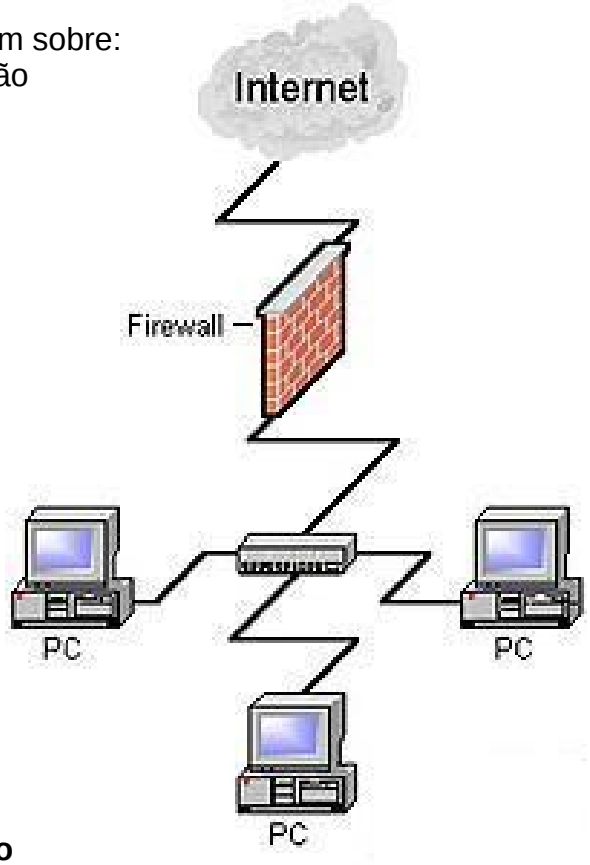
David Júnior



Pouso Alegre
2006.

Firewall é o nome dado ao dispositivo de rede que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede a outra. É utilizado para evitar que o tráfego não autorizado possa fluir de um domínio de rede para o outro. Apesar de se tratar de um conceito geralmente relacionado a proteção contra invasões, o firewall não possui capacidade de analisar toda a extensão do protocolo, ficando geralmente restrito ao nível 4 da camada OSI.

Podemos falar também sobre:
- Firewall de aplicação
- Filtros de pacotes
- Proxy firewall
- Stateful firewall



Firewall de aplicação

Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc.) são instalados geralmente em computadores servidores e são conhecidos como Proxy. Este tipo não permite comunicação direto entre a rede e a Internet. Tudo deve passar pelo firewall, que atua como um intermediador. O Proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um Proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim, uma solução é criar um "Proxy genérico", através de uma configuração que informa que determinadas aplicações usarão certas portas. Essa tarefa só é bem realizada por administradores de rede ou profissionais de comunicação qualificados.

O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre a rede e outra rede).
É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

Componentes de um firewall:

Filtro de pacotes
Base de um firewall
Dados utilizados
Ips
Tipo de protocolo (udp/tcp)
portas
interface de chegada/saída do pacote
flags (syn,ack,...)

Composto de listas de regras
input
output
forward

Filtro de pacotes
Stateless Packet Inspection
Cada pacote é analisado isoladamente
não há correlação com outros pacotes
tipo mais comum de filtro

Statefull Packet Inspection
considera o histórico de conexões
considera o relacionamento entre pacotes
está sendo cada vez mais utilizado

Network Address Translation (NAT)
Modifica endereços IP e portas
Surgiu como solução para a falta de endereço IP

NETWORK ADDRESS Translation (NAT)
Source NAT (S-NAT)
Destination NAT (D-NAT)

Network Address Translation (NAT)
Alem da economia de endereço...
Limita a exposição da rede interna
Interferem no funcionamento das VPNs
* IPSec com AH

Proxy
Trata nível de alicação
* Realiza logs mais detalhados (específicos)
* verifica características especificas de cada aplicação
Pode realizar caching

Proxy
Cada serviço requer um Proxy especifico
Nem sempre é transparente

O que um firewall pode fazer e o que não pode fazer por uma rede

O que o Firewall não pode fazer

Proteger a rede de usuários internos mal intencionados - O firewall pode evitar que certas informações saiam de uma companhia através da conexão de rede, mas não pode impedir que um usuário copie os dados num disquete e os carregue consigo. Atacantes internos requerem medidas de segurança interna, como segurança de host e educação de usuários.

Proteger contra conexões que não passam por ele - O firewall pode apenas controlar o trafego que passa por ele. Se o seu site disponibilizar acesso discado para sistemas internos atrás do firewall, não há nada que o firewall possa fazer para prevenir que intrusos tenham acesso a sua rede por esta via.

Proteger contra novas ameaças - Firewalls são projetados para proteger contra ameaças conhecidas.

Proteger contra vírus - Embora o firewall verifique todo o trafego que entra na rede interna, esta verificação é feita basicamente checando os endereços fonte e destino e os números de porta, não verificando os dados em si.

O que o Firewall pode fazer

Eis algumas tarefas cabíveis a um firewall:

- 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.

- Tipos de Firewall
  - – Filtragem de pacotes
  - – NAT
  - – Servidores Proxy

Filtragem de pacotes é o bloqueio ou liberação da passagem de pacotes de dados de maneira seletiva, conforme eles atravessam a interface de rede. O critério usado ao inspecionar pacotes são baseados nos cabeçalhos da Camada 3 (IPv4 e IPv6) e Camada 4 (TCP, UDP, ICMP, e ICMPv6). Os critérios mais usados são endereços de origem e destino, porta de origem e destino e protocolo.

Regras de filtragem especificam o critério em que o pacote deve se enquadrar e a ação resultante, que pode ser bloqueio ou liberação, tomada quando o pacote casa com a regra. As regras de filtragem são avaliadas em seqüência da primeira a última. A não ser que o pacote encontre uma regra contendo a palavra-chave quick, o mesmo será avaliado contra *todas* as regras de filtragem antes da ação final ser tomada. A última regra a casar é a "vencedora" e dita qual ação tomar. Existe um pass all implícito no início das regras de filtragem, que significa que caso o pacote não case com nenhuma regra a ação resultante será pass.

Servidor Proxy

Proxy Server x Firewall

Inicialmente precisamos definir o que é um Servidor Proxy. Proxy é uma palavra em inglês que, segundo o Michaelis, significa:

Proxy - procuração, procurador, substituto, representante.

Portanto Servidor Proxy é, em essência, um equipamento que presta um serviço de procurador de um computador de uma rede em outra rede, evitando que o endereço IP do computador seja conhecido na outra rede. O Serviço de Proxy age como representante de um usuário que precise acessar um sistema do outro lado do Servidor Proxy.

Isto coloca o Servidor Proxy como um dos três tipos clássicos de Firewall. E o que é Firewall? Segundo Michaelis é *Firewall – parede, muro, guarda-fogo.*

Então, um Firewall é um equipamento e / ou programa que funciona como muro de proteção de uma rede de dados de acessos não desejados, oriundos de outras redes ou equipamentos. Qualquer equipamento que controle o tráfego por razões de segurança pode ser chamado Firewall.

Os Firewall se dividem em três tipos básicos: Roteador de Barreira, Gateway Servidor de Proxy e Técnicas de inspeção de estado.

Tipos de Proxy

Existem basicamente dois tipos de **Proxy: o Proxy Transparente e o Proxy Controlado. Veja a seguir as diferenças:**

Proxy Transparente

N**ele é simplesmente feito um repasse de pacotes vindos da internet para uma máquina que está na rede interna.**

Proxy Controlado

Essa é a categoria dos softwares especializados em agir como **servidores Proxy, como o próprio Squid. Eles possuem mais opções que o Proxy transparente para facilitar o controle de quem pode ou não utilizar o**

Proxy, solicitação de autenticação, Proxy para SSL e o uso de listas de controles de acesso (ACL's) que nós veremos mais à frente.

Vantagens e desvantagens

Claro que dependendo do seu caso como um administrador de redes, você vai ter que decidir qual tipo de Proxy você vai utilizar. Vão existir casos que um Proxy transparente vai lhe oferecer o suficiente para fazer o que você quer fazer e vão existir casos em que você vai precisar de funções que somente um Proxy controlado está disposto **a lhe oferecer.**

Conheça aqui algumas vantagens do Proxy transparente e do Proxy controlado:

Proxy Transparente

É mais simples de ser configurado quando já está habilitado no **Kernel, o cliente é obrigado a passar pelo Proxy, programas como ICQ funcionam plenamente com ele e não precisa que as máquinas clientes sejam configuradas.**

Proxy Controlado

Com ele você pode utilizar listas de controles de acesso (ACL's) **para controlar quem usa e quem não usa o seu Proxy, pode ser utilizado para uso com SSL, pode servir para liberação de internet mediante autenticação do usuário e, principalmente, possui um sistema de caching, possuindo um desempenho na rede geralmente melhor.**

Agora as desvantagens:

Proxy Transparente

Possui menos recursos que um Proxy Controlado, precisa de configurações **no Kernel e, em alguns casos, é necessária a recompilação do Kernel do sistema, não possui nenhuma segurança de acesso e não possui um sistema de caching, o que o torna mais lento em uma rede.**

Proxy Controlado

Programas como ICQ e o protocolo SMTP não funcionam muito bem com ele, **pode ocorrer dos usuários removerem as configurações do Proxy assim que você tiver saído da sala e sua configuração é mais complicada.**

Tipos de ataques e Técnicas Hacking

Source Routing

Source routing é a habilidade de lidar com um pacote de modo que este seja direcionado a certos roteadores sem que passe pelos roteadores convencionais. Tipicamente, utiliza-se source routing quando um roteador executa o bloqueio de algum tipo de tráfego que o invasor deseja explorar, onde

o roteamento é alterado na tentativa de burlar o dispositivo de conectividade. Hoje em dia, no ambiente Internet, não existe motivos legítimos que levariam alguém a necessidade de ditar o caminho que o pacote deverá percorrer até chegar ao seu destino. Desde que o roteamento é feito apenas de e para uma respectiva rede privada, deve-se atentar para o cuidado de não aceitar pacotes no roteador de borda que instruam este roteador a encaminhar pacotes para outra rede.

É necessário desabilitar o source routing com o comando "no ip source-route".

Ip spoofing

No contexto de redes de computadores, ip spoofing e a técnica de subversão de sistemas informáticos que consiste em mascarar (spoof) pacotes ip com endereços remetentes falsificados.

Devido às características do protocolo IP, o re-encaminhamento de pacotes é feito com base numa premissa muito simples: o pacote deverá ir para o destinatário (endereço-destino); não há verificação do remetente — o router anterior pode ser outro, e ao nível do IP, o pacote não tem qualquer ligação com outro pacote do mesmo remetente. Assim, torna-se trivial falsificar o endereço de origem, i.e., podem existir vários computadores a enviar pacotes fazendo-se passar pelo mesmo endereço de origem, o que representa uma série ameaça para os velhos protocolos baseados em autenticação pelo endereço IP.

Esta técnica, utilizada com outras de mais alto nível, aproveita-se, sobretudo, da noção de confiabilidade que existe dentro das organizações: supostamente não se deveria temer uma máquina de dentro da empresa, se ela é da empresa. Mas isto não é bem assim, como indica o parágrafo anterior. Por outro lado, um utilizador torna-se também confiável quando se sabe de antemão que estabeleceu uma ligação com determinado serviço. Esse utilizador torna-se interessante, do ponto de vista do atacante, se ele possuir (e estiver a usar) direitos privilegiados no momento do ataque.

Bom, mas resta a interação com as aplicações, além de que as características do protocolo IP permitem falsificar um remetente, mas não lhe permitem receber as respostas — essas irão para o endereço falsificado. Assim, o ataque pode ser considerado cego.

Por outro lado, ao nível das aplicações, este protocolo é frequentemente acoplado ao TCP, formando o TCP/IP. Isto quer dizer que existe encapsulamento do TCP dentro do IP (e os dados dentro do TCP), o que remete ao atacante a necessidade de saber que dados TCP incluir no pacote falsificado. Essa técnica é conhecida por desvio de sessão TCP, ou TCP session hacking em inglês.

Existem métodos para evitar estes ataques, como a aplicação de filtros de pacotes, filtro ingress nos gateways; faz sentido bloquear pacotes provindos da rede externa com endereços da rede local. Idealmente, embora muito negligenciado, usar um filtro egress — que iria descartar pacotes provindos da rede interna com endereço de origem não-local que fossem destinados à rede

externa — pode prevenir que utilizadores de uma rede local iniciem ataques de IP contra máquinas externas.

Existem outros ataques que utilizam esta técnica para o atacante não sofrer os efeitos do ataque: ataques SYN (SYN flooding) ou ataques smurf são exemplos muito citados.

Ataque man in the middle

Um ataque man-in-the-middle (mitm) é um ataque no qual o atacante é capaz de ler, inserir e modificar, mensagens entre duas entidades sem que estas tenham conhecimento que a ligação entre ambas esta comprometida. Tipicamente o atacante insere-se no maio da comunicação entre dois pontos, fazendo parte de um canal de comunicação.

Esse tipo de ataque é porventura aquele mais difícil de detectar e de prevenir, sendo também o exemplo clássico de segurança informática, estando na base de técnicas de hacking, de descoberta de password, desvio de tráfego, ataque de imitação, injeção de pacotes, modificação de pacotes,etc.

Tiny fragment

Tiny fragment é um tipo de ataque que utiliza a fragmentação de pacotes ip para criar fragmentos extremamente pequenos e assim forçar o cabeçalho tcp de informar a ser um fragmento de pacote separado. O ataque é designado para evitar as regras de filtragem da política de segurança da rede; espera-se que a filtragem implementada no roteador examine somente o primeiro fragmento do pacote transmitido, permitindo assim a passagem dos restantes.

Esse ataque pode ser evitado descartando-se aqueles pacotes em que o tipo de protocolo é o tcp e o parâmetro ip fragmentOffset, especificando no cabeçalho.

Ateque syn

SYN flood ou ataque SYN é uma forma de ataque de negação de serviço (também conhecido como Denial of Service - DoS) em sistemas computadorizados, na qual o atacante envia uma seqüência de requisições SYN para um sistema-alvo.

Quando um cliente tenta começar uma conexão TCP com um servidor, o cliente e o servidor trocam um série de mensagens, que normalmente são assim:

O cliente requisita uma conexão enviando um SYN (synchronize) ao servidor.

O servidor confirma esta requisição mandando um SYN-ACK de volta ao cliente.

O cliente por sua vez responde com um ACK, e a conexão está estabelecida.

Isto é o chamado aperto de mão em três etapas (Three-Way Handshake).

Um cliente malicioso pode não mandar esta última mensagem ACK. O servidor irá esperar por isso por um tempo, já que um simples congestionamento de rede pode ser a causa do ACK faltante.

Esta chamada conexão semi-aberta pode ocupar recursos no servidor ou causar prejuízos para empresas usando softwares licenciados por conexão. Pode ser possível ocupar todos os recursos da máquina, com pacotes SYN. Uma vez que todos os recursos estejam ocupados, nenhuma nova conexão (legítima ou não) pode ser feita, resultando em negação de serviço. Alguns podem funcionar mal ou até mesmo travar se ficarem sem recursos desta maneira.

Inundação icmp

O icmp floof ou inundação icmp é o ato de enviar o número máximo de pacotes no menor espaço de tempo possível a fim de tornar a conexão de um usuário lenta(leg), desconectando-o da rede. o ataque icmp flood pode ser dividido em duas categorias: usuários de modem e usuários de rede.

Um usuário que esteja conectado via modem a 14.400bps de sua casa dificilmente conseguirá atacar alguém com um icmp flood, pois não tem velocidade para o envio de pacotes suficiente para derrubar alguém, e, ao mesmo tempo, pode ser um alvo para outro usuário que esteja conectado a 28.800bps, por exemplo.

Para proteger-se do ataque ICMP Flood deve-se usar um programa de ICMP Check que irá lhe dizer de onde estão vindo os pacotes, pois o ICMP não estabelece conexão e, por esse motivo, programas como o netstat, não conseguem identificar a origem do ataque.

Também um bom firewall para bloqueio de pacotes ICMP vindos de qualquer lugar é uma possível proteção.

Um bom programa é o Conseal PC Firewall, da Signal9, que também atua no caso de ataques utilizando outros protocolos, como TCP, UDP e SYN.

Sempre o cliente q tiver a maior conexão consegue derrubar o que tiver a menor conexão: cliente com shell t3, derruba shell t2, que derruba shell t1, derruba modem 56k.....