Seminário de Sistemas Operacionais

Leandro Gomes de Souza
Matheus Felipe Krol

Firewall

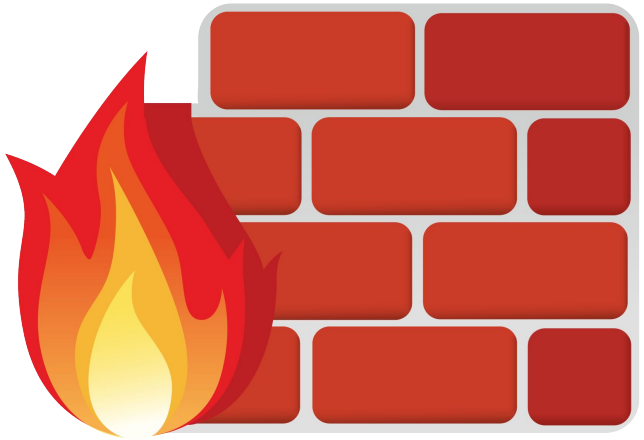
Histórico

Os sistemas firewall nasceram no final dos anos 80, fruto da necessidade de criar restrição de acesso entre as redes existentes, com políticas de segurança no conjunto de protocolos TCP/IP.

Nesta época a expansão das redes acadêmicas e militares, que culminou com a formação da ARPANET e, posteriormente, a Internet e a popularização dos primeiros computadores tornando-se alvos fáceis para a incipiente comunidade hacker.

Histórico

Casos de invasões de redes e fraudes em sistemas de telefonia começaram a surgir, e foram retratados no filme Jogos de Guerra ("War Games"), de 1983. Em 1988, administradores de rede identificaram o que se tornou a primeira grande infestação de vírus de computador e que ficou conhecido como Internet Worm. Em menos de 24 horas, o worm escrito por Robert T. Morris Jr disseminou-se por todos os sistemas da então existente Internet (formado exclusivamente por redes governamentais e de ensino), provocando um verdadeiro "apagão" na rede.



Primeira geração - Filtros de pacotes

- A tecnologia foi disseminada em 1988 através de pesquisa sustentada pela DEC;
- Bill Cheswick e Steve Bellovin da AT&T desenvolvem o primeiro modelo para *Prova de Conceito*;
    - O modelo tratava-se de um filtro de pacotes responsável pela avaliação de pacotes do conjunto de protocolos TCP/IP;
    - Apesar do principal protocolo de transporte TCP orientar-se a um estado de conexões, o filtro de pacotes não tinha este objetivo inicialmente (uma possível vulnerabilidade)

Primeira geração - Filtros de pacotes

Até hoje, este tipo de tecnologia é adotada em equipamentos de rede para permitir configurações de acesso simples (as chamadas "listas de acesso"). O *ipchains* é um exemplo recente de um *firewall* que utiliza a tecnologia desta geração. Hoje o "ipchains" foi substituído pelo iptables que é nativo do Linux e com maiores recursos.

Regras típicas na 1ª geração

- Restringir tráfego baseado no endereço IP de origem ou destino
- Restringir tráfego através da porta (TCP ou UDP) do serviço.

Segunda Geração - Filtros de Estado de Sessão

- A tecnologia foi disseminada a partir de estudo desenvolvido no começo dos anos 90 pelo Bell Labs

- Pelo fato de o principal protocolo de transporte TCP orientar-se por uma tabela de estado nas conexões, os filtros de pacotes não eram suficientemente efetivos se não observassem estas características

- Foram chamados também de firewall de circuito.

Regras Típicas na 2ª Geração

- Todas as regras da 1ª Geração
- Restringir o tráfego para início de conexões (NEW)
- Restringir o tráfego de pacotes que tenham sido iniciados a partir da rede protegida (ESTABLISHED)
- Restringir o tráfego de pacotes que não tenham número de sequência corretos.

Regras Típicas na 2ª Geração

Firewall Stateful: Armazena o estado das conexões e filtra com base nesse estado.
Existe três estados para uma conexão:

- NEW: Novas conexões
- ESTABLISHED: Conexões já estabelecidas
- RELATED: Conexões relacionadas a outras existentes.

Terceira Geração - Gateway de Aplicação

- Baseado nos trabalhos de Gene Spafford (co-autor do livro Practical Unix and Internet Security), Marcos Ranum (fundador da empresa TIS), e Bill Cheswick

- Também são conhecidos como "Firewall de Aplicação" ou "Firewall Proxy"

- Foi nesta geração que se lançou o primeiro produto comercial em 13 de Junho de 1991—o SEAL da DEC;

Terceira Geração - Gateway de Aplicação

- Diversos produtos comerciais surgiram e se popularizaram na década de 90, como os firewalls Raptor, Gauntlet (que tinha sua versão gratuita batizada de TIS) e Sidewinder, entre outros

- Não confundir com o conceito atual de "Firewall" de Aplicação: firewalls de camada de Aplicação eram conhecidos desta forma por implementarem o conceito de Proxy e de controle de acesso em um único dispositivo (o Proxy Firewall), ou seja, um sistema capaz de receber uma conexão, decodificar protocolos na camada de aplicação e interceptar a comunicação entre cliente/servidor para aplicar regras de acesso

Regras Típicas na 3ª Geração

- Todas as regras das gerações anteriores
- Restringir acesso FTP a usuários anônimos
- Restringir acesso HTTP para portais de entretenimento
- Restringir acesso a protocolos desconhecidos na porta 443 (HTTPS).

Quarta Geração e subsequentes

- O firewall consolida-se como uma solução comercial para redes de comunicação TCP/IP
  - Stateful Inspection para inspecionar pacotes e tráfego de dados baseado nas características de cada aplicação, nas informações associadas a todas as camadas do modelo OSI (e não apenas na camada de rede ou de aplicação) e no estado das conexões e sessões ativas
  - Prevenção de Intrusão para fins de identificar o abuso do protocolo TCP/IP mesmo em conexões aparentemente legítimas
  - Deep Packet Inspection associando as funcionalidades do Stateful Inspection com as técnicas dos dispositivos IPS

Quarta Geração e subsequentes

- A partir do início dos anos 2000, a tecnologia de Firewall foi aperfeiçoada para ser aplicada também em estações de trabalho e computadores domésticos (o chamado "Firewall Pessoal"), além do surgimento de soluções de firewall dedicado a servidores e aplicações específicas (como servidores Web e banco de dados), ou mesmo usuários.

Classificação

- **Filtros de Pacotes**
- **Proxy Firewall ou Gateways de Aplicação**
- **Stateful Firewall (ou Firewall de Estado de Sessão)**
- **Firewall de Aplicação**

Tipos de Firewall

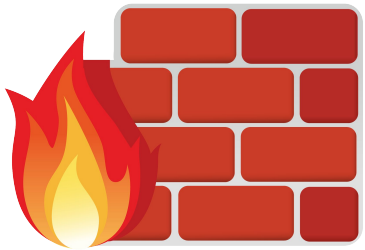
- **Firewall de Proxy:** é um dos tipos de firewall mais antigos comercialmente e funciona como a passagem de uma rede para outra de uma aplicação específica. Servidores proxy podem oferecer recursos adicionais, como armazenamento em cache e segurança de conteúdo ao evitar conexões diretas de fora da rede. No entanto, isso também pode afetar a capacidade de taxa de transferência e as aplicações que eles podem comportar.

Tipos de Firewall

- **Firewall de inspeção de estado:** é o firewall tradicional que conhecemos, este tipo permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo. Ele monitora toda a atividade desde o momento em que uma conexão é aberta até que ela seja fechada. As decisões de filtragem são tomadas de acordo com as regras definidas pelo administrador e com o contexto.
- **Firewall UTM (*Unified Threat Management*):** é uma evolução do firewall tradicional, que unifica em um único dispositivo: funcionalidades convencionais de firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais de rede.

Tipos de Firewall

- **Firewall NGFW (*Next Generation Firewall*):** assim como o firewall UTM, o NGFW engloba todas as funcionalidades padrão de firewall em conjunto com funcionalidades adicionais, tais como: IPS (*Intrusion Prevent System*), inspeção SSL, inspeção profunda (*deep inspection*), detecção de malware e URL baseada em reputação. Os recursos específicos são destinados a impedir o crescente número de ataques de aplicativos ocorrendo entre as camadas 4-7 do modelo OSI.



Fireball