SENAI-SP

IPTables

SENAI
SÃO PAULO

Firewall

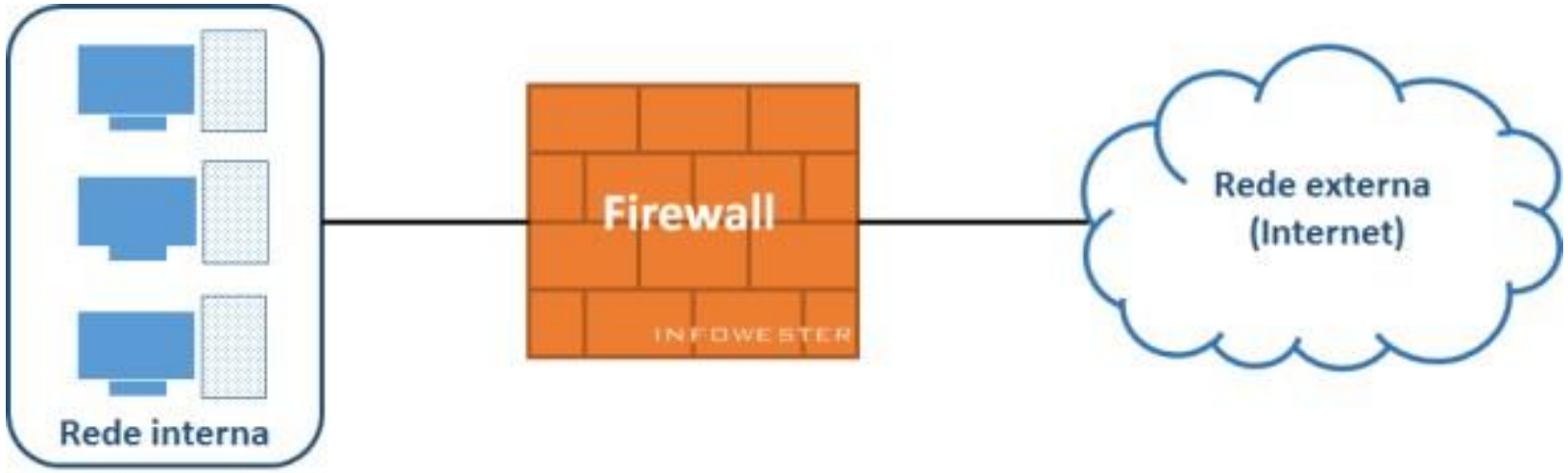
Definição

- Firewall é uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

- "Parede de fogo", a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa.

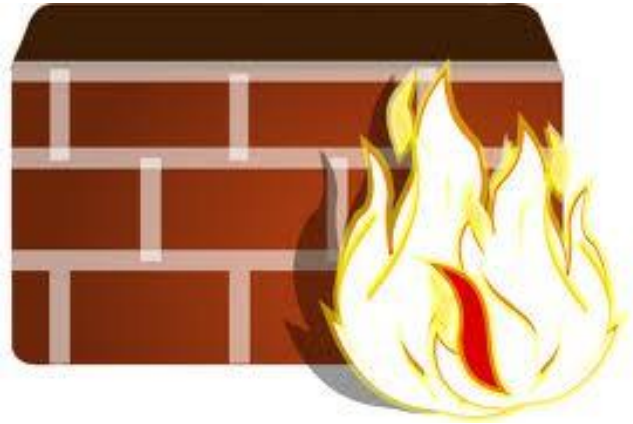
Definição

- A sua missão, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejados e liberar acessos bem-vindos.



Tipos de Firewall

- Existem basicamente dois tipos de firewalls:
  - Filtragem de pacotes (packet filtering)
  - Firewall de aplicação ou proxy de serviços (proxy services)



SENAI-SP

SENAI SÃO PAULO

Filtragem de Pacotes (Packet Filtering)

- Este tipo de firewall toma as decisões baseadas nos parâmetros do pacote, como porta, endereço de origem/destino, estado da conexão e outros parâmetros do pacote.
- O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT).

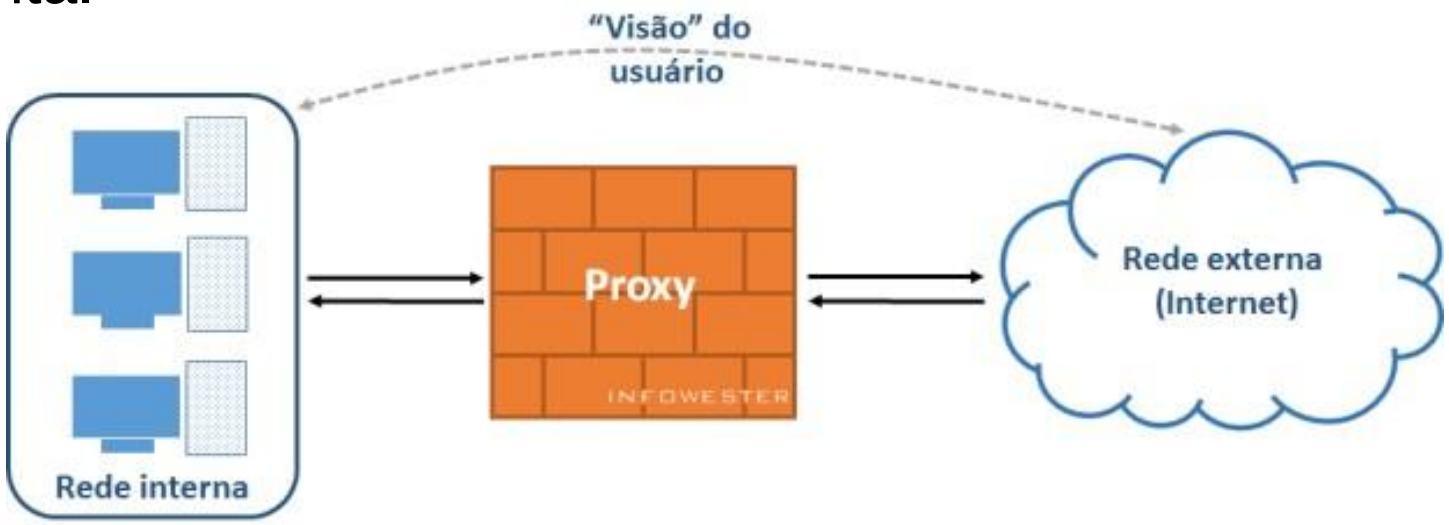
Firewall de Aplicação ou Proxy de Serviços (Proxy Services)

- Este tipo de firewall analisa o conteúdo do pacote para tomar suas decisões de filtragem.

- Firewalls deste tipo são mais intrusivos (pois analisam o conteúdo de tudo que passa por ele) e permitem um controle relacionado com o conteúdo do tráfego.

Firewall de Aplicação ou Proxy de Serviços (Proxy Services)

- Alguns firewalls em nível de aplicação combinam recursos básicos existentes nos firewalls em nível de pacotes, combinando as funcionalidade de controle de tráfego/controle de acesso em uma só ferramenta.



Aplicação

- **IPTABLES**

  - Funciona através da comparação de regras para saber se um pacote tem ou não permissão para passar.

  - Em firewalls mais restritivos, o pacote é bloqueado e registrado para que o administrador do sistema tenha conhecimento sobre o que está acontecendo em seu ambiente.

Aplicação

- Por intermédio de regras, fazemos com que pacotes possam ou não serem recebidos por toda uma rede, somente uma máquina, uma interface ou até mesmo uma porta de comunicação.
- As regras do iptables são compostas de uma **Tabela, Opção, Chain, Dados e Ação.** Através destes elementos, podemos especificar o que fazer com os pacotes, seguindo a estrutura:

iptables [-t tabela] [opção] [chain] [dados] -j [ação]

Características - IPTables

- Especificação de portas/endereço de origem/destino;
- Suporte a protocolos TCP/UDP/ICMP (incluindo tipos de mensagens icmp);
- Suporte a interfaces de origem/destino de pacotes;
- Manipula serviços de proxy na rede;
- Permite um número ilimitado de regras por chain;
- Muito rápido, estável e seguro;
- Possui mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados;

Características - IPTables

- Suporte a módulos externos para expansão das funcionalidades padrões oferecidas pelo código de firewall;
- Permite especificar exceções para as regras ou parte das regras;
- Suporte a detecção de fragmentos;
- Redirecionamento de portas;
- Masquerading;
- Suporte a SNAT;
- Suporte a DNAT;
- Limitação de passagem de pacotes/conferência de regra (muito útil para criar proteções contra, syn flood, ping flood, DoS, etc).

Tabelas (Tables)

- São os locais usados para armazenar os “chains”. As tabelas são referenciadas em uma regra *iptables* com a opção "-t tabela“.

- Existem 3 tabelas disponíveis:

  - **filter** - tabela padrão, usada no tráfego de dados comum;
  - **nat** - usada quando há ocorrência de NAT (geração de outra conexão);

Tabelas (Tables)

- **mangle** - raramente usada, utilizada para alterações especiais de pacotes (como modificar o tipo de serviço (TOS)).

- **OBS:** Se nenhuma tabela for citada na regra (deixar em branco a opção [-t tabela]), a tabela usada será a filter.

Tabelas (Tables)

- **FILTER**
  - Tabela padrão, usada no tráfego de dados comum. Esta contém 3 chains padrões:
    - **INPUT** - consultada para dados que chegam ao servidor;
    - **OUTPUT** - consultada para dados que saem do servidor;
    - **FORWARD** - consultada para dados que são redirecionados para outra interface de rede ou outra máquina.

Tabelas (Tables)

- **NAT**
  - Usada para concentrar o fluxo de varias conexões, saindo para uma única. Possui
  - 3 chains padrões:
    - **PREROUTING** - Consultada quando os pacotes precisam ser modificados logo que chegam ao firewall. É a chain ideal para realização de DNAT e redirecionamento de portas.

Tabelas (Tables)

- **OUTPUT** - Consultada quando os pacotes gerados localmente precisam ser modificados antes de serem roteados. Esta chain somente é consultada para conexões que se originam de IP's de interfaces locais.

- **POSTROUTING** - Consultada quando os pacotes precisam ser modificados após o tratamento de roteamento. É a chain ideal para realização de SNAT e IP Masquerading.

Tabelas (Tables)

- **MANGLE**
  - Utilizada para alterações especiais de pacotes (como modificar o tipo de serviço (TOS)).

    - **INPUT** – entrada.
    - **FORWARD** - repasse.
    - **PREROUTING** - Consultada quando os pacotes precisam ser modificados logo que chegam.

Tabelas (Tables)

- **OUTPUT** - Consultada quando pacotes gerados localmente precisam ser modificados antes de serem roteados.

- **POSTROUTING** - Consultada quando os pacotes precisam ser modificados após o tratamento de roteamento. É o chain ideal para realização de SNAT e IP Masquerading.

Regras

- **Parâmetros para as CHAINS**

-L List (Listar as Regras existentes)

-A Append (Adicionar novas Regras às existentes)

-I Insert (Inserir uma nova Regras)

-R Replace (Substituir Regras)

-D Delete (Apagar Regras)

Regras

-P Policy (Define uma regra Padrão)

-N New (Criar nova Chain)

-E rEname (Renomeia a Chain Criada por -N)

-F Flush (Apaga todas as Regras)

-X eXtract(Limpar Chain Criada por -N)

-Z Zero (Zerar Regras específicas)

Regras

- **Parâmetros para o complemento das regras**

-s especifica a origem do pacote. Origem que pode ser informada como:

endereço IP completo (-s 192.168.1.1);

hostname (-s ubuntu);

endereço fqdn (-s www.ubuntu.com);

par rede/máscara (-s 200.200.200.0/255.255.255.0 ou -s 200.200.200.0/24).

-d especifica um destino para o pacote, com a mesma sintaxe descrita acima por ***-s***.

Regras

-i identifica a interface de entrada do pacote, podendo ser placa de rede, modem ou interface de conexão:

-i eth0

-i eth1

-i ppp0

-o identifica a interface de saída do pacote, com a mesma sintaxe descrita anterior em ***-i***.

OBS: A interface de entrada (-i) nunca poderá ser especificada em um chain OUTPUT e a interface de saída (-o) nunca poderá ser especificada em um chain INPUT.

Regras

-p especifica o protocolo usado na regra, podendo ser:

-p tcp

-p udp

-p icmp

-sport ou **--source-port** especifica uma porta ou faixa de portas de origem. Deve sempre ser acompanhado por **-p tcp** e **-p udp**.

-dport ou **--destination-port** especifica uma porta ou faixa de portas de destino. Deve sempre ser acompanhado por **-p tcp** e **-p udp**.

! exclui determinado argumento (exceção).

-j Join (Aplica a Regra)

Regras

- **Especificando um alvo**

ACCEPT (Aceita o pacote processado pela CHAIN)

DROP (Barra o pacote processado pela CHAIN)

REJECT (Rejeita, com a mensagem "icmp-port-unreachable")

REDIRECT (Redireciona o pacote processado pela CHAIN)

MASQUERADE (Mascaramento do ip de origem do pacote)

LOG (Registra a atividade de um pacote)

Regras

- **Estado da conexão**

NEW (Confere pacotes que criam novas conexões)

ESTABLISHED (Confere pacotes de conexões já estabelecidas)

RELATED (Confere pacotes relacionados indiretamente a uma conexão)

INVALID (Confere pacotes que não puderam ser identificados)