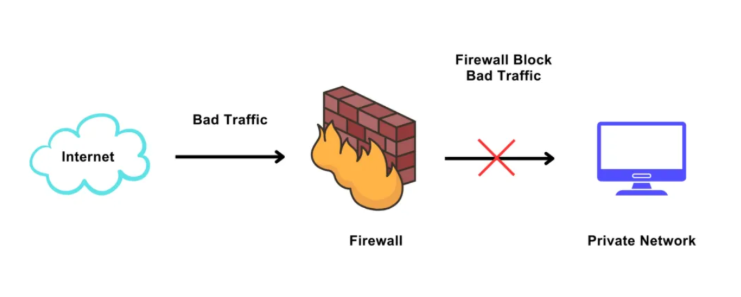
SO

FIREWALL

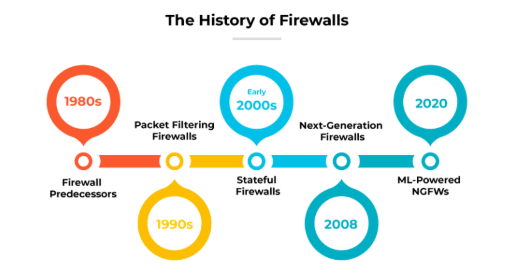
**O que é?**

* Sistema de segurança de rede
* Controla tráfego de entrada e saída
* Barreira entre rede confiável e não confiável
* Bloqueia tráfego malicioso da internet



**História**

* Anos 80 – Crescimento da internet
* “Como proteger nossos sistemas?”



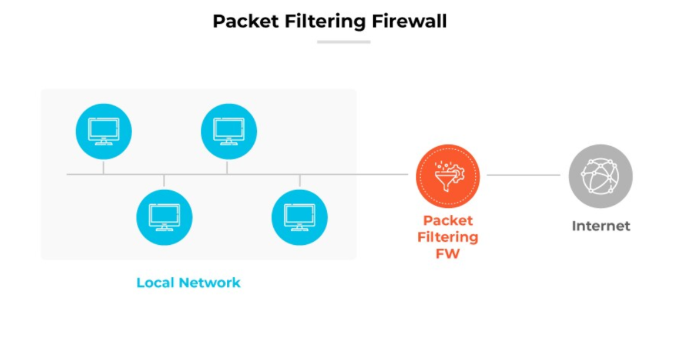
**Firewall com Filtragem de Pacotes**

Durante a década de 90 surgiu a primeira geração de Firewalls, os Packet Filtering Firewalls. A principal

característica desse tipo de firewall é a inspeção de pacotes de forma individual, onde.

Ele avalia os pacotes com base em regras predefinidas que consideram endereços de IP de origem e destino, números de porta e o protocolo utilizado, como TCP ou UDP.

O processo era semelhante ao processo de entrega de encomendas, onde é verificado apenas o endereço do pacote, e não o conteúdo.



**Firewall com Estado**

No início dos anos 2000 surgiram os firewalls de segunda geração, que possuem **estado**.

Eles trouxeram uma grande evolução em relação a primeira geração, sendo capaz de monitorar o estado das conexões ativas e determinando o contexto do tráfego de rede.

O **conceito** **principal** desse tipo de firewall é baseava-se em que **nem todos os pacotes são entidades independentes**; muitos fazem parte de uma comunicação maior entre hosts.

Os firewall com estado são capazes de rastrear o estado das conexões de rede (como fluxos TCP ou comunicação UDP) mantendo uma tabela de estados.

Essa tabela registra todas as conexões em andamento e podia verificar se um pacote recebido fazia parte de uma sessão estabelecida.

**Firewall de Aplicação**

Ainda em 2000, surgiu o Firewall de Aplicação. Com a crescente necessidade de segurança em nível de aplicação devido ao aumento de ataques sofisticados baseados na WEB.

Eles aprimoraram o Firewall de Estado com recursos adicionais para analisar e filtrar o tráfego com base nos dados da aplicação, levando à criação dos sistemas de Gerenciamento Unificado de Ameaças (**UTM**).

**UTM**

Os UTMs combinavam uma série de recursos do firewal com antívirus de gateway, detecção de intrusão e filtragem de spam

A inspeção de pacotes com estado dos UTMs permitia o tráfego de entrada e saída na rede, enquanto um proxy web filtrava o **conteúdo** e fazia a varredura com serviços antivírus.

Um sistema de prevenção de intrusão (IPS) separado detectava e bloqueava tráfego malicioso.

**Firewall de Próxima Geração**

Em 2008 a **Palo Alto Networks** lançou o primeiro firewall de próxima geração (NGFW) do setor.

Nessa nova era na segurança os firewall não se limitavam mais a filtrar portas e endereços de IP, mas também eram capazes de realizar inspeções mais profundas para tomada de decisões.

Os NGFWs introduziram sistemas integrados de prevenção de intrusão (IPS), visibilidade completa da pilha e a capacidade de aplicar políticas de segurança com base em aplicativos, usuários e conteúdo.

**Firewall de Hardware**

Os roteadores domésticos modernos (como TP-Link, D-Link, Intelbras, etc.) normalmente já vêm com um firewall embutido, que faz o que chamamos de filtragem de pacotes. Isso funciona de forma parecida com o firewall "packet filtering" que vimos antes.

**Firewall Nativo do SO**

Um firewall nativo de sistema operacional é um software de segurança integrado diretamente ao sistema operacional (SO) de um computador ou dispositivo.

Sua principal função é monitorar e controlar o tráfego de rede de entrada e saída, com base em um conjunto predefinido de regras de segurança.

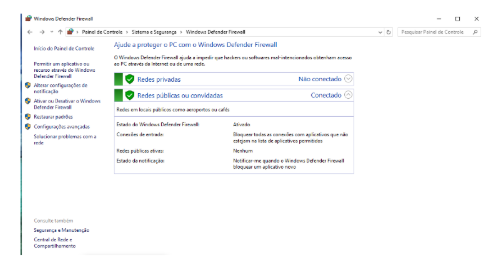
**Aplicação do Firewall Windows**

* As principais aplicações do Windows Defender são:
* Proteger o sistema contra acessos não autorizados;
* Controlar quais programas podem se comunicar pela rede/internet
* Definir restrições específicas para portas, endereços de IP, protocolos ou aplicativos;

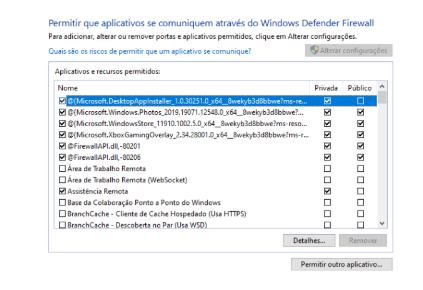
**Prática – Windows Defender**

Vamos conhecer um pouco mais sobre o Windows Defender.

Acessem o firewall pelo painel de controle do Windows ou digitando “Firewall” no menu iniciar



Na primeira opção temos um local onde definimos se os aplicativos vão poder se comunicar com o Firewall do Windows. Normalmente isso é feito de forma automática quando usamos um aplicativo que vai utilizar a rede.



**Configurações Avançadas**

Passando para configurações avançadas podemos testar algumas coisas.

Aqui podemos definir manualmente regras de entrada e saída.

* Regras de Entrada: Controlam o tráfego que chega no computador.
  + Exemplo: Autorizar ou bloquear conexões para um servidor de jogo que você está hospedando.
* Regras de Saída: Controlam o tráfego que sai do computador.
  + Exemplo: Bloquear um navegador de acessar a internet

**Como funcionam as regras?**

As regras do firewall podem ser definidas com base em:

* Programa (aplicativo): A regra se aplica a um software específico;
* Porta: A regra se aplica a uma porta de comunicação, por exemplo permitir conexões na porta 80 (http);
* Protocolos (TCP e UDP): As regras também podem especificar o tipo de protocolo de rede ou para ambos.

**Prática - Vamos definir algumas regras!**

Agora vamos definir uma regra que vai nos impedir de realizar pings, bloqueando o protocolo ICMPv4 que é o responsável por transmitir mensagens de controle e identificar problemas de rede entre os dispositivos.

Agora vamos realizar o ping no mesmo IP que pegamos anteriormente.

**Exercício**

Para o exercício ligue duas máquinas virtuais, defina uma regra de entrada para uma das duas restringindo o protocolo ICMPv4, após definir esta regra tente realizar o ping da outra VM para que está restringida.

* Não esqueça de verificar se a placa de rede está em modo bridge;
* Ative a descoberta de rede;
* Realize o ping para testar se está funcionando
* Aplique a regra de entrada para um dos computadores

