**Paulo Henrique Nunes da Silva RA:5792**

**1 -** Um firewall é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

**2 -** Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet. Um firewall pode ser um hardware, software ou ambos.

**3 – Tipos de Firewall**

* **Firewall de proxy -** Um firewall de proxy é um dos primeiros tipos de firewall e funciona como a passagem de uma rede para outra de uma aplicação específica.
* **Firewall com inspeção de** estado - Atualmente conhecido como o firewall tradicional, um firewall com inspeção de estado permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo. Ele monitora toda atividade desde o momento em que uma conexão é aberta até que ela seja fechada.
* **Firewall de Gerenciamento unificado de ameaças (UTM)** - Normalmente, um dispositivo UTM combina, de maneira flexível, as funções de um firewall com inspeção de estado e prevenção contra intrusões e antivírus.
* **Firewall de próxima geração (NGFW)** – Seria o novo tipo de firewall no qual deve incluir os seguintes criterios, Recursos padrão de firewall, como inspeção stateful, Firewall de próxima geração (NGFW)Prevenção de invasão integrada, Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos, Atualização de caminhos para incluir feeds futuros de informação, Técnicas para lidar com as ameaças à segurança em evolução.

## **4 - Arquitetura dos firewalls**

* Arquitetura Dual-Homed Host - Nesta modalidade, há um computador chamado dual-homed host que fica entre uma rede interna e a rede externa normalmente, a internet. O nome se deve ao fato de este host possuir ao menos duas interfaces de rede, uma para cada lado. Não há outro caminho de comunicação, portanto, todo o tráfego passa por este firewall
* Screened Host - Na arquitetura Screened Host, em vez de haver uma única máquina servindo de intermediadora entre a rede interna e a rede externa, há duas: uma que faz o papel de roteador (screening router) e outra chamada de bastion host.O bastion host atua entre o roteador e a rede interna, não permitindo comunicação direta entre ambos os lados.
* Bastion host - O roteador normalmente trabalha efetuando filtragem de pacotes, sendo os filtros configurados para redirecionar o tráfego ao bastion host. Este, por sua vez, pode decidir se determinadas conexões devem ser permitidas ou não, mesmo que tenham passado pelos filtros do roteador.
* Screened Subnet -A arquitetura Screened Subnet também conta com a figura do bastion host, mas este fica dentro de uma área isolada de nome interessante: a DMZ, sigla para Demilitarized Zone - Zona Desmilitarizada. A DMZ, por sua vez, fica entre a rede interna e a rede externa. Acontece que, entre a rede interna e a DMZ há um roteador que normalmente trabalha com filtros de pacotes. Além disso, entre a DMZ e a rede externa há outro roteador do tipo.

**5 – Firewall de Hardware** – o firewall de hardware nada mais é do que um equipamento com um software de firewall instalado, onde a sua vantagem é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para lidar com grandes volumes de dados e não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional.

6 – Limitações de Firewalls

* Um firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede.
* A verificação de políticas tem que ser revista periodicamente para não prejudicar o funcionamento de novos serviços;
* Novos serviços ou protocolos podem não ser devidamente tratados por proxies já implementados;
* Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede interna;
* Um firewall pode não ser capaz de identificar uma atividade maliciosa que acontece por descuido do usuário - quando este acessa um site falso de um banco ao clicar em um link de uma mensagem de e-mail, por exemplo;
* Firewalls precisam ser "vigiados". Malwares ou atacantes experientes podem tentar descobrir ou explorar brechas de segurança em soluções do tipo;
* Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma [conexão 3G](https://www.infowester.com/3g4g.php) (justamente para burlar as restrições da rede, talvez), o firewall não conseguirá interferir.