1. Firewall é uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo.
2. O Firewall tem função similar as portas e janelas de sua casa, pois “tranca” todas as portas e janelas só que do seu computador para que só os autorizados possam entrar e sair.
3. 1º Firewall : Filtragem de Pacotes – O firewall de filtro de pacotes controla o acesso à rede analisando os pacotes de saída e de entrada. Na prática, ele permite que um pacote passe ou seja bloqueado durante o caminho fazendo a comparação com critérios definidos antecipadamente.

2º Firewall : Firewall de Aplicação - Os Firewalls de servidor proxy são os tipos de firewall mais seguros. Eles podem proteger os recursos de rede de forma eficaz filtrando as mensagens, mascarando seu endereço IP e limitando os tipos de tráfego.

3º Firewall: Inspeção de estados - O Stateful Packet Inspection (SPI), conhecido também como inspeção de dados, é uma poderosa arquitetura de firewall que examina os fluxos de tráfego de ponta a ponta na rede.

4. 1º Arquitetura: Dual-Homed Host – Neste termo, há um computador dual-homed host que fica entre uma rede interna e a rede externa, normalmente a rede externa é a internet, seu nome deve-se ao fato deste host possuir ao menos duas interfaces de rede , uma para cada “lado”.

2º Arquitetura: 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.

3º Arquitetura: Screened Subnet – Esta arquitetura também conta com a figura do bastion host , mas ele fica dentro de uma área isolada com um nome peculiar, a DMZ sigla para Delimitarized Zone – Zona desmilitarizada, ela fica entre a rede interna e a rede externa.

5. Um firewall de hardware é um dispositivo externo que é conectado a um computador antes que ele se conecta à Internet. Um roteador de banda larga é um exemplo de um firewall de hardware . Geralmente eles são mais caros do que os firewalls de software e são normalmente usados em redes acessadas por vários computadores.

6. Algumas limitações do firewall no quesito segurança de rede são : O firewall não consegue impedir um ataque de rede cujo a origem e o destino sejam ambos a rede interna.

Também não conseguem impedir que os usuários acessem sites com códigos maliciosos , tornando necessário a conscientização do usuário.

Não conseguem barrar ou interceptar conexões que não passem por ele, por exemplo alguém tentando acessar a internet utilizando a internet móvel 3G.