Firewall é uma barreira de segurança do nosso computador, ele nos ajuda contra conteúdo malicioso, imagine uma sala com 350 computadores sem um firewall, todos esses computadores podem ser acessados por qualquer pessoa, dessa forma o firewall aplica um conjunto de regras na rede para decidir se permite ou nega determinado acesso.

Com a internet todo mundo tem acesso rápido a muitos programas e conteúdo, porem existem portas abertas, que expões suas informações e seus conteúdos, o firewall fecha as portas para sua segurança e ele já sabe qual programa pode fazer ou entrar em tal coisa qual é seguro ou não.

Existem dois tipos de firewall, o de hardware e o de software, os de hardware são os mais utilizados, são os que vem em roteadores, já os de software o Windows no caso já vem com um firewall instalado para sua segurança, para você instalar outro firewall na sua máquina você precisa desativar o seu do Windows para instalar outra e colocar com suas próprias configurações para melhor segurança.

Screening Router é a arquitetura mais simples e utilizada, caracteriza por um roteador na rede e um filtro de pacotes entre a rede interna na internet.

Screenned Host é considerara altamente segura porém não muito simples, a característica é um servidor principal com segurança reforçada sendo ele o único ponto entre a rede interna e a internet.

Screenned Subnet é considerada a mais segura, pois ela adiciona mais uma camada de segurança, como se fosse uma sub-rede geralmente chamada de DMZ que isola a rede interna da externa.

Firewall de hardware são equipamentos específicos para este fim, são mais utilizados em empresas, a vantagens de usar esse tipo de equipamentos é que ele é dedicado em vez de utilizar conteúdo de outro aplicativo, desse jeito ele pode tratar mais requisições e filtros de maneira rápida.

O firewall é completamente perfeito porem para que isso seja verdadeiro todos os dados devem ser passados por ele, e isso causa algumas limitações, por exemplo ele não consegue impedir ataques cuja a origem seja da rede interna pois os dados não passam por ele, ele também não reforça as senhas nem previnem o uso inadequado delas, ele não previnem o uso de sites maliciosos, os usuários tem que ter consideração nisso, ele não compromete o desempenho da rede nem o do computador pois o tamanho dele aumenta para que seja possível ele superar os problemas, as políticas de segurança devem ser revisadas sempre para que nenhum crack ou malware tenha descoberto alguma falha nele e esteja se aproveitando.