**FIREWALL**

1. Firewall é uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisao tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executada. Firewall se enquadra em uma espécie de barreira de defesa, sua função é bloquear tráfego de dados indesejado e liberar acessos confiáveis.
2. Firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede. É baseado em dois principios: todo o tráfego é bloqueado, exceto o que está explicitamante autorizado; todo tráfego é permitido, exceto o que está explicitamente bloqueado.
3. **Filtragem de pacotes** : Firewall analisa informações de acordo com as regras estabelecidas para liberar ou não o pacote, podendo também executar alguma tarefa relacionada, como registrar o acesso em um arquivo de log.

**Filtragens estática e dinâmica** : Na filtragem estática, os dados são bloqueados ou liberados meramentecom boas regras, não importando a ligação que cada pacote tem com outro. Na filtragem dinâmica, os filtros consideram o contexto em que os pacotes estão inseridos para criar regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente.

**Firewall de aplicação ou proxy de serviços** : É uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e outra rede externa normalmente, a internet.

**Proxy Transparente** : É uma alternativa para estes casos porque as máquinas que fazem parte da rede não precisam saber de usa existência, dispensando qualquer configuração específica.

1. **Arquitetura Dual-Homed Host** : Há um computador com esse nome que fica entre uma rede interna e a rede externa, normalmente a internet.

**Screened Host** : Há duas máquinas servindo de intermediadora entre a rede interna e a rede externa. Uma faz papel de roteador e a outra chamada de bastion host.

**Screened Subnet** : Também conta com o bastion host, mas fica dentro de uma área isolada de nome DMZ.

1. O objetivo normalmente é o de proteger uma rede com tráfego considerável ou com dados muito importantes. É preparedo para lidar com grandes volumes de dados e não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional.
2. . Um Firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede. Esta situação pode gerar mais gastos para uma ampliação de infraestrutura capaz de superar o problema;

. A verificação de políticas tem que ser revista periodicamente para não prejudicar o funcionamento de novos serviços;

. 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.