**Aluno:Eduardo Migliorini RA:8321**

**1.O que é FireWall?**

Tipo de se segurança baseado em um conjunto de regras ou instruções. • “Parede de fogo” sua função é determinar quais transmissões ou recepções de dados serão permitidas. Pode evitar uma série de problemas, malware que se instala por uma porta desprotegida, programas maliciosos que enviem dados para a internet, tentativas de acesso de computadores externos desconhecidos, etc.

**2. Como um FireWall funciona?**

Através das políticas é regras de um firewall varias configurações podem ser feitas:

• Aguardar autorização do usuário administrador.

• Permitir determinados tipos de dados bloqueando outros.

• Essas políticas como se percebe se baseia em:

• Trafego bloqueado, exceto o permitido.

• Trafego permitido, exceto o bloqueado.

• Alguns podem

**3. Cite e descreva os tipos de FireWall**.

• Filtragem por pacotes onde os cabeçalhos do pacotes são analisados, a transmissão feita porTCP/IP comumente filtrando a camada de rede e de transporte:

• Filtro estático; são bloqueados e liberados com base nas regras, sem observar a ligação com outros pacotes.

• Filtro dinâmico; os filtros consideram o contexto em que os pacotes estão inseridos para "criar" regras que se adaptam a certo cenários temporários.

• Firewall de aplicação ou proxy de serviço ou proxy.

• É uma segurança que atua como intermediário entre um computador ou uma rede interna e outra rede, externa (normalmente a internet).

• pode registrar o tráfego de dados em um arquivo de log, conteúdo muito utilizado pode ser guardado em uma espécie de cache.

• Determinados recursos podem ser liberados apenas mediante autenticação do usuário.

• Proxy transparente.

• Inspeção de estados (stateful inspection).

• Firewalls pessoais.

• Firewall de hardware.

**4. Cite e descreva as arquiteturas do FireWall.**

**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".

**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.

**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.

**5. Explique sobre FireWalls de hardware.**

A vantagem de um firewall de hardware 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 (por conta de uma falha em outro software, por exemplo).

**6. Quais são as limitações de um FireWall.**

seguintes limitações:

Um firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede (ou mesmo de um computador). 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;

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 (justamente para burlar as restrições da rede, talvez), o firewall não conseguirá interferir.