Jonathan Ribeiro R.A: 8610

1. O que é FireWall?

R: Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

2. Como um FireWall funciona?

R: Ele funciona como uma alfândega ou filtro que restringe a passagem dos dados recebidos e enviados pelo seu computador.

3. Cite e descreva os tipos de FireWall.

#### R:

#### 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. Servidores proxy podem oferecer recursos adicionais, como armazenamento em cache e segurança de conteúdo ao evitar conexões diretas de fora da rede. No entanto, isso também pode afetar a capacidade de taxa de transferência e as aplicações que eles podem comportar.

#### 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. As decisões de filtragem são tomadas de acordo com as regras definidas pelo administrador e com o contexto, o que significa o uso de informações de conexões e pacotes anteriores que pertencem à mesma conexão.

#### 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. Ele também pode incluir serviços adicionais e, às vezes, gerenciamento em nuvem

#### Firewall de próxima geração (NGFW)

#### Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção stateful. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.

4. Cite e descreva as arquiteturas do FireWall.

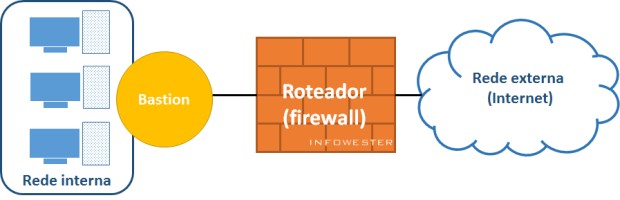
R:

### 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

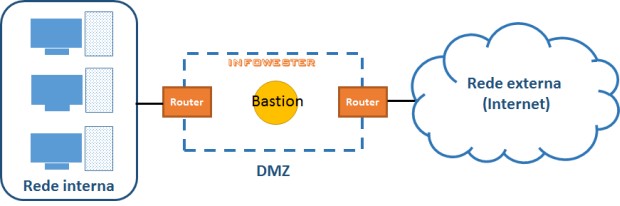
Na arquitetura **Screened Host**, em vez de haver uma única máquina servindo de intermediadora entre a rede interna e a rede externa, há duas: uma que faz o papel de roteador (screening router) e outra chamada de bastion host.



### 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.

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. Explique sobre FireWalls de hardware.

R:

É possível encontrar, por exemplo, roteadores ou equipamentos semelhantes a estes que exercem a função em questão função. Neste caso, o objetivo normalmente é o de proteger uma rede com tráfego considerável ou com dados muito importantes.

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

R:

* 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.