**Trabalho de Infraestrutura Seguranca**

**1. O que é FireWall?**

Firewall é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

**2. Como um FireWall funciona?**

Em termos mais técnicos, o Firewall é o responsável pelo controle dos dados transferidos de e para o seu computador através da internet, além de prevenir que informações pessoais ou confidenciais sejam transmitidas pelo seu computador para a internet e impedir a invasão da máquina por software malicioso.

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

3.1. Filtragem de pacotes (packet filtering)

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, como:

* Endereços IP permitidos;
* Tipo de pacote;
* Número de porta para acesso.

3.2. Firewall de aplicação (proxy services)

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.

Eles fornecem uma análise de segurança completa e com reconhecimento dos protocolos que suportam. Para as grandes empresas, os firewalls de aplicação oferecem a melhor experiência na internet e resultam nas melhorias de desempenho da rede.

3.3. Inspeção de estados (stateful inspection)

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. Esses firewalls inteligentes e rápidos usam uma maneira inteligente de evitar o tráfego não autorizado, analisando os cabeçalhos dos pacotes e inspecionando o estado de cada um.

Esses firewalls funcionam na camada de rede e por isso são mais seguros do que os modelos básicos de filtragem de pacotes.

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

4.1. Dual-Homed Firewall

É um *host* que tem no mínimo duas interfaces de rede, conectadas cada uma a segmentos diferentes de rede. Um computador que fica entre duas redes pode ser um *Dual-Homed Gateway* , já que este actua como um *router* desactivado, o que impede que se faça o *routing* de pacotes de uma rede directamente para outra, não permitindo a comunicação directa entre a rede interna, que se quer proteger, e a rede externa.

4.2. Screened Host Firewall

Nesta arquitectura não há uma sub-rede de segurança entre a *Internet* e a rede interna. Existe apenas um *screening router* e um *bastion host* situado junto à rede interna.

O *screening router* é responsável por bloquear os pacotes de serviços que não deseja que passem pelo *Firewall,* pacotes que tenham rotas *IP* definidas ou que tenham como destino a sua rede interna.

O *bastion host* executa servidores *proxy* possibilitando aos utilizadores da sua rede interna usar serviços na rede externa. Este, ainda, actua como um servidor de correio electrónico .

Esta arquitectura é bastante segura porque existem dois níveis de protecção, na camada de rede através do *screening router*e na camada de aplicação através do *bastion host*. No caso de ocorrer uma falha existe a protecção do outro. A configuração e a manutenção deste tipo de *Firewall* é relativamente fácil.

4.3. Screened Subnet Firewall

É uma arquitectura que combina um *Screened Host* com um *Screening Router* e um *Bastion Host,*formando uma sub-rede segura entre as redes internas e externa, também conhecida como *DMZ (De-Militarized Zone).*

*4.4. Multiple Gates*

Este tipo de *Firewall*é bastante similar aos já apresentados, sendo a diferença o uso de vários *gates,* cada um para um determinado protocolo.  Apresenta a vantagem de tornar o *gate* mais fácil para o administrador da rede, pois há um controle individual de cada máquina. Como existem mais máquinas que devem ser vigiadas contra actividades “suspeitas”, a sua gerência  torna-se mais difícil, além do custo ser mais elevado.

4.5. Internal Firewall

A utilização deste *Firewall*difere dos outros tipos de *Firewall* já referidos anteriormente. Este tipo de *Firewall*, visa proteger algumas subredes da empresa de outras. Na instalação destas máquinas, são criadas subredes independentes que comunicam entre si através de canais de comunicação que passam pelo *Internal Firewall*, usando algum tipo de encriptação para evitar que os dados sejam entendidos por pessoas não autorizadas.

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

hardwall e software firewalls proteger os computadores , bloqueando o tráfego suspeito da internet. Uma firewall de hardware é uma parte física do equipamento ligado a um sistema de computador , enquanto que um software de firewall é um programa instalado no computador . Os firewalls de hardware têm o benefício de proteger vários computadores em uma rede, enquanto firewalls de software pode ser adequada para as necessidades de um usuário individual. Firewall Hardware

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

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

*Firewalls* são componentes cruciais na segurança de uma rede. Porém, eles não são completamente perfeitos. Porém, para que seu funcionamento seja pleno, é necessário que todos o fluxo de dados passe pelo *firewall*. Por isso, diversos problemas não podem ser resolvidos através do uso de um *firewall*. Vejamos alguns deles:

* Um *firewall* não consegue impedir um ataque cuja origem e destino seja a rede interna, pois os dados não passarão por ele, tornando-o ineficaz nesse tipo de ataque.
* *Firewalls* não aumentam força de senhas e nem previnem o uso inadequado das mesmas. Da mesma forma, eles são ineficazes em ataques não- técnicos como Engenharia Social.
* *Firewalls* não conseguem impedir que usuários acessem sites com códigos maliciosos, tornando necessária a conscientização dos usuários neste sentido.
* A política de segurança do *firewall* deve ser revista periodicamente, de modo a garantir o bom funcionamento do mesmo. Além disso, é importante fiscalizar o funcionamento do mesmo com certa periodicidade para garantir que nenhum *Malware* ou *Cracker* tenha descoberto e esteja explorando alguma falha do mesmo.
* *Firewalls* não são capazer de interceptar conexões que não passem por ele, como por exemplo um usuário que acesse a internet usando um modem 3G.
* *Firewalls* podem comprometer o desempenho da rede (ou do computador), demandando uma ampliação na infraestrutura para que seja possível superar o problema.