Nome: Giovanni Bússola RA: 8233

1. O que é Firewall?

É uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, sem impedir que os dados que precisam transitar continuem fluindo.

1. Como um Firewall funciona?

Ele “tranca” as portas de conexão do computador, permitindo somente conexões autorizadas a “passar” por essas portas.

1. Cite e descreva os tipos de Firewall

* Firewall de Proxy:

Pode fornecer funcionalidades adicionais, como armazenamento em cache em conteúdo e segurança, impedindo conexões de fora da rede.

* Firewall de Inspeção com Estado:

É considerada a “tradicional”, permite ou bloqueia o tráfego de rede com base no estado, porta e protocolo, monitorando todas as atividades desde o início da conexão até que ela seja fechada.

* Firewall de Gerenciamento Unificado de Ameaças (UTM)

Acopla as funções do Firewall de Inspeção com Estado (modelo tradicional) com prevenção de intrusões e antivírus. Pode ter gerenciamento de nuvem e concentra-se na facilidade de uso.

* Firewall de Última Geração

Serve para bloquear ameaças modernas, como malware avançado e ataques na camada de aplicativos. Possui:

Recursos de firewall padrão, como inspeção stateful, Prevenção de intrusão integrada, Conscientização e controle de aplicativos para ver e bloquear aplicativos arriscados, Caminhos de atualização para incluir feeds de informações futuras e Técnicas para lidar com as ameaças de segurança em evolução

1. Cite e Descreva as Arquiteturas de Firewall

Screening Router:

É um modelo simples onde um roteador ou switch recebe as informações da internet, filtra eles e passa para a intranet. Porém esse modelo é pouco seguro

Screened Host:

O roteador ou switch recebe as informações da internet, e passa para um servidor chamado de “Bastion Host”, a filtragem das informações é realizada pelo software utilizado no Bastion Host.

Screened Subnet:

É considerada a mais segura, pois adiciona uma nova camada de segurança à arquitetura Screened Host, baseia-se na criação de uma sub-rede chamada de “Demilitarezed Zone”, que isola a rede interna da externa. Assim a rede fica um roteador exterior que recebe as informações, passa para o Bastion Host e o mesmo passa para um roteador interior que espalha a informação na intranet.

1. Explique Sobre Firewalls de Hardware

Os firewalls em forma de hardware são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais. A vantagem de usar equipamentos desse tipo é que o hardware é dedicado em vez de compartilhar recursos com outros aplicativos. Dessa forma, o firewall pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

1. Cite as Limitações do Firewall

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 podem comprometer o desempenho da rede (ou do computador), demandando uma ampliação na infraestrutura para que seja possível superar o problema

Firewalls não conseguem impedir que usuários acessem sites com códigos maliciosos, tornando necessária a conscientização dos usuários neste sentido, ou bloqueio do site se caso for de conhecimento do administrador de redes

Referências:

<https://www.gta.ufrj.br/grad/15_1/firewall/limitacoesdofirewall.html>

<https://www.gta.ufrj.br/grad/08_1/firewall/architectures.html>

<https://www.tecmundo.com.br/seguranca/3329-como-funciona-o-firewall-.htm>

<https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm>

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>