Mateus G S Cassandri RA: 8133

Trabalho sobre Firewall

1. O que é Firewall?

R: 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.

1. Como um Firewall funciona?

R: Ele funciona como uma alfândega ou filtro que restringe a passagem dos dados recebidos e enviados pelo seu computador. O antivírus é necessário porque mesmo as comunicações consideradas seguras pelo Firewall podem trazer ameaças à máquina, geralmente devido à operação incorreta do PC pelo usuário.

1. Cite e descreva os tipos de Firewall.

R: 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.

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.

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.

1. Cite e descreva as arquiteturas do Firewall.

R: Screening Router: É a arquitetura mais simples utilizada, caracteriza-se pela presença de um roteador de filtro de pacotes entre a rede interna e a internet. Nessa arquitetura existe comunicação direta entre múltiplos servidores internos e múltiplos servidores externos. A sua zona de risco é proporcional ao número de servidores na rede interna e os tipos de serviço de tráfego permitidos pelo roteador. Para cada tipo de serviço permitido a zona de risco aumenta consideravelmente. Controle de danos é igualmente difícil, já que o administrador da rede teria que verificar cada servidor a procura de traços de invasão regularmente. No caso de destruição do firewall tende a ficar muito complicado rastrear ou até mesmo notar a invasão. Já a facilidade de uso entretando é bem alta, já que o usuário pode acessar diretamente os serviços da internet. Essa configuração é um caso de "Aquilo que não é expressamente proibido é permitido".

Screened Host: Em geral, arquiteturas desse tipo são altamente seguras. porém não muito simples de se implementar. Tipicamente, configura-se um servidor principal com segurança reforçada, sendo ele o único ponto de comunicação entre a rede interna e a internet, esse servidor é chamado de Bastion Host. Entre o Bastion Host e a internet, utiliza-se a arquitetura do Screening router. A zona de risco é restrita somente ao Bastion Host e o roteador. A estância básica dos Screened Hosts é determinada 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, geralmente chamada de Perimiter Network ou DMZ (Demilitarized Zone), que isola a rede interna da externa, sendo ela a responsável por toda a comunicação entre as redes, além da criação do Bastion Host. Sendo asssim, uma Screened Subnet é formada por um Bastion Host isolado pela sub-rede, um roteador responsável pela comunicação entre a rede interna e o bastion host e outro responsável pela comunicação entre o bastion host e a rede externa(internet). Para invadi-lo o ataque teria que passar por ambos os roteadores.Sendo assim, a zona de risco é reduzida drasticamente. A estância básica pode variar, porém como na maioria dos casos necessita-se alto nível de segurança utiliza-se a estância "Aquilo que não é expressamente permitido é proibido".

1. Explique sobre Firewalls de hardware.

R: 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 .

1. Quais são as limitações de um Firewall.

R: 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.