Emerson R Zandonadi

RA: 8130

1. O que é FireWall?

R: Na tradução é parede de fogo, que é uma barreira de proteção que ajuda a bloquear acessos de dados maliciosos, sem impedir que dados que precisam seguir continuem seguindo.

1. Como um FireWall funciona?

R: São equipamentos ou aplicativos que ficam entre um link de comunicação checando e filtrando todo o fluxo de dados, protegendo a integridade dos dados na rede e a confidencialidade deles. Usam regras de segurança, fazendo com que somente pacotes de dados que estejam dentro das regras sejam aprovados.

1. Cite e descreva os tipos de FireWall.

R: Os sistemas operacionais modernos já devem possuir o software de FireWall. Nos computadores em redes de uma empresa, pode ser usado um computador da rede como FireWall, específico para este fim, é dedicado em vez de compartilhar recursos com outros aplicativos, pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

1. Cite e descreva as arquiteturas do FireWall.

R:

**Screening Router**: arquitetura mais simples utilizada. 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. 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:** São altamente seguras, porém não muito simples de se implementar. 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:** Considerada a mais segura, 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: 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: Pode permitir conexões entre máquinas que foram iniciadas por qualquer máquina, conhecidas como conexões bidirecionais, entretanto, isso pode expor o Servidor Tivoli a conexões ilícitas por máquinas não autorizadas que se posicionam como clientes legítimos.