Trabalho sobre Firewall para Infraestrutura e Segurança na Internet, Faculdade ALFA de Umuarama

Enzo Filipe Abbade Antunes – 4827, Professor Márcio Alves.

Trabalho sobre FireWall Crie uma conta no github e crie um repositório com o nome de “infraestrutura\_seguranca”. Responda as questões em um documento DOC ou DOCX e faça o upload deste documento no novo repositório.

Envie um email com o link do seu repositório para marciockalves@gmail.com

**1.** O que é FireWall?

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

**2.** Como um FireWall funciona?

Firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede mas também a confidencialidade deles.

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

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.

2- Firewall de aplicação (proxy services)

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.

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

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.

**Screened Host:**

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.

**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.

**5.** Explique sobre FireWalls de 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 capazes 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.