Componentes: Maria Francisca da Conceição Maciel Targino
Antonio Yves de Sousa Dantas

Disciplina: Segurança de dados

Resolução do questionário

01- O firewall é uma barreira de proteção que atua no bloqueio de acessos indevidos na rede. Além de ajudar a impedir tráfegos indevidos e indesejados sejam realizados e permite também que acessos ditos “confiáveis” sejam administrados como for necessário.
O firewall impede que seu computador seja invadido, não permite que dados indesejáveis entrem em uma máquina, como também bloqueia o envio de dados originários de uma máquina que não esteja devidamente especificados nas configurações.

02- No diagrama apresentado constata-se tais componentes: Router, Firewall, Switch, Server e dispositivos (Phones, PC’s e Workstation).

O Router, ou também conhecido como roteador, é um dispositivo de rede para outro com base nos endereços da camada 3 do OS, ou seja, é considerado um elemento intermediador em uma rede de computadores que permite o roteamento de dados entre redes separadas, de acordo com o conjunto de regras que formam a tabela de roteamento.

O Firewall é um controlador do fluxo de dados que trafegam na rede, no qual este controle é feito a partir dos requisitos de segurança, ou seja, ele julga quais os pacotes de dados é dita como “segura” ou “insegura”. Sendo “segura”, os dados são trocados ou trafegados pela rede normalmente; caso seja “ insegura”, a solicitação de tráfego é negada.

O Server, ou também chamado de servidor, é um sistema que fornece serviços a uma rede de computadores.

O Switch é um dispositivo de rede que move pacotes de rede de um dispositivo para o outro.

03- O firewall de hardware é um dispositivo físico ligado a um sistema de computador, já um software de firewall é um programa que se instala no dispositivo. Os de hardware tem a vantagem de proteger vários computadores em uma rede de computadores, visto que é um dispositivo externo que é conectado a um PC antes mesmo de ele se conectar à internet, ,já o de software pode ser utilizado de forma a atender às necessidades individualmente do usuário.

A cada vez que um pacote de dados chega, o firewall compara com cada regra até encontrar uma que corresponda a aquele pacote, assim que encontra, ele executa a ação correspondente à regra. Um firewall de software protege uma rede de computadore, já o firewall de hardware protege cada computador.

04- As policies são políticas de acesso, ou seja, são regras do firewall que tem como objetivo garantir quais pacotes são seguros e quais são ditos inseguro e logo colocá-los sob análise.
Essa análise utiliza regras acerca do tipo de pacote, endereço IP, portas, payload do pacote, dentre outros; quando cada pacote passa pelo firewall, ele recebe um status, seja ele: Aceito, desistente ou rejeitado.

Será “Aceito” quando os dados têm total liberdade no tráfego pelo firewall.
Será “Desistente” quando os dados não possuem tal permissão pelo firewall.
Será “Rejeitado” quando além de barrar os dados de tráfego, ainda emite um sinal de alerta.

05- Pra garantir a segurança do tráfego de dados de uma rede à outra, utiliza-se abordagens a exemplo da criação de blacklist. No tráfego, todos os pacotes são permitidos, exceto os pacotes com características da blacklist que logo são retidos para análise ou já são bloqueados automaticamente.

06- a) O firewall orientado a estado é aquele em que ocorre a filtragem de pacotes a partir de sua conexão, ou seja, o firewall conhece a conexão de onde o pacote está vindo com isso ele consegue validar ou não sua entrada, para realizar essa validação e ter conhecimento da origem dos pacotes ele usa tabelas de estado e endereços; O firewall não orientado a estado ele não utiliza as tabelas de validação, com isso qualquer pacote que passe pela rede ele será avaliado novamente, independe de ser uma nova conexão ou não.

b) O firewall orientado a estado conhece o pacote, com isso sua avaliação será bem mais rápida, porém pode haver o bloqueio de alguns pacotes devido o fato de suas regras serem estáticas; O firewall não orientado a estado permite que o administrador crie regras para cada cenário.