CENTRO UNIVERSITÁRIO INTERNACIONAL UNINTER
ESCOLA SUPERIOR POLITÉCNICA
TECNOLOGIA EM ANALISE E DESENVOLVIMENTO DE SISTEMAS
DISCIPLINA DE SEGURANÇA EM SISTEMAS DA INFORMAÇÃO

ATIVIDADE PRÁTICA

ALYSSON DUMA – RU: 3050279

CURITIBA – PARANÁ
2021

1 - Descrição dos tipos de firewall

O Firewall é um modelo de programa que filtra o que entra e o que sai de uma rede privada. Com essa tecnologia é possível monitorar pacotes e analisar se existe algum tipo de ameaça, como um ataque DDoS entre outros.

-(Stateless) Packet Filtering (PF)

Responsável por controlar o acesso de rede analisando os pacotes de entrada e saída permitindo que um pacote passe ou que seja bloqueado. Esse bloqueio pode ser definido por regras de firewall que variam bastante das configurações que podem ser diversas. Exemplos de configurações: IP de destino e IP de origem, tipo do pacote, protocolo ou o número de porta de acesso que esse pacote está sendo enviado, técnica essa que é ideal para redes pequenas, pois ficaria bem complexa implementada em redes maiores, podendo sobrecarregar o servidor do firewall ou deixar a rede lenta por conta dessa filtragem, porque tudo passa por ele antes de sair ou entrar na rede. Esse firewall não tem como impedir de todos os tipos de ataque, não tendo a capacidade de distinguir ataques que usam vulnerabilidades nas camadas de aplicativos, por exemplo.

- Statefull packet filtering (SPF)

Rastreia o estado operacional e as características das conexões de rede que o atravessam. O firewall está configurado para distinguir pacotes legítimos para diferentes tipos de conexões. Somente os pacotes que combinam a conexão ativa conhecida podem passar pelo firewall. A inspeção dos estados dos pacotes (SPI), também referida como filtragem de pacotes dinâmicos, é uma característica de segurança que muitas vezes é incluída nas redes das empresas.

- Application gateways (AG)

Definida como uma porta de ligação de uma rede interna com a rede externa. É um servidor específico de aplicação através do qual todos os dados da aplicação (que entram e que saem) devem passar. Os pacotes de dados enviados por um dispositivo de uma rede local devem passar pelo gateway padrão para chegar a um dispositivo que faça parte de outra rede externa.

2 – Facilidades de firewall

-Access Control Lists (ACLs)

A característica principal das ACLs é filtrar por pacotes IP, por opções do UDP, TCP (podendo analisar alguns Flags).

Compromete em respeitar uma determinada regra que foi estabelecida, baseado em um quesito estático no qual permite ou não o tráfego de informações.

-Intrusion Detection System (IDS)

Pode ser um hardware ou software de monitoramento de rede que detecta sinais de atividade maliciosa na internet ou computador, que detém de recursos para examinar o tráfego, afim de identificar e prevenir os acessos não autorizados na rede.

É um sistema de monitoramento que atua como parte principal do sistema. Ele consulta através de regras preestabelecidas o gerenciamento de pacotes para efetuar uma eventual análise. Se houver um pacote a ser analisado, o gerenciador de análise compara o pacote com as assinaturas requeridas ao gerenciador de assinatura. Caso haja uma confirmação das características do pacote a serem descritas por alguma assinatura, o gerenciador de análise aciona o gerenciador de medidas de defesa (IPS) para que a ameaça detectada seja combatida.

3 - Solução em software e em hardware.

- Firewall em forma de software (ZoneAlarm) - É uma aplicação de segurança dos computadores. Hoje em dia, os computadores pessoais já vêm com softwares de firewall. Usam um conjunto de regras para fazer o controle do tráfego de informações do aparelho. Essas regras podem ser customizáveis, o que aumenta ou diminui a segurança do seu computado. Assim, é possível dar parte do controle também do usuário, que configura o firewall da forma que achar melhor. É muito utilizado em computadores pessoais.
- Firewall em forma de hardware (Watchguard) - É um verdadeiro equipamento que servirá como suporte de segurança para outros aparelhos. É muito procurado pelas empresas, que precisam garantir que seus dados estão seguros sob a proteção desse aparelho. A vantagem do uso de equipamentos desta categoria é que o hardware é exclusivo, em substituição do compartilhamento de recursos com outros aplicativos. Assim, o firewall pode ser capaz do tratamento de mais requisições e aplicar filtros com mais agilidade.

Referências

https://blog.starti.com.br/tipos-de-firewall/
https://blog.algartelecom.com.br/gestao/conheca-3-tipos-de-firewall-e-as-suas-diferencas/
https://dicasdeinfra.com.br/8-tipos-de-firewalls-guia-para-profissionais-de-seguranca-de-ti/
https://ostec.blog/seguranca-perimetro/firewall-stateful-stateless/
https://www.gta.ufrj.br/grad/00_2/bruno/newpage2.htm

Declaro para todos os fins de direito, sob as penas da lei, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, declarando ainda a inexistência plágio ou cópias sem os respectivos créditos aos autores, isentando o CENTRO UNIVERSITÁRIO INTERNACIONAL UNINTER ESCOLA SUPERIOR POLITÉCNICA e o respectivo orientador de toda e qualquer responsabilidade acerca do conteúdo deste trabalho.

Alysson Duma.