Firewall

Uma segurança necessária

O que é Firewall?

O termo firewall é cada dia mais comum no nosso meio, pois vivemos hein uma era digital onde a segurança é primordial para que tenhamos boas experiências nesse meio. Você certamente já deve estar familiarizado com ele, mas sabe o que é um firewall ou o que ele faz?

Pararede de fogo (do inglês “firewall”), é o nome das portas antichamas ou barreiras contra fogo usadas nas casas, automóveis, passagens para as escadas em prédios e edifícios que impedem o fogo se espalhar antes que os bombeiros consigam detê-lo. Na tecnologia esse termo “firewall” é usado para dar nome a aplicativos ou equipamentos que protegem tanto uma rede empresarial quanto uma rede domiciliar, checando e filtrando todo o fluxo de dados protegendo assim, não só a integridade dos dados mas também a confidencialidade deles.

Quais tipos de Firewalls?

São muitos os tipos de firewalls, seu trabalho poderá ser realizado de diferentes formas, isso depende de critérios do desenvolvedor, estrutura de rede, necessidades específicas do usuário ou características do sistema operacional que mantém o firewall. Citarei alguns deles que considero os mais importantes:

- **Filtro de Pacotes**

Este tipo de firewall controla o tráfego de uma rede bloqueando ou autorização os pacotes; este bloqueio é feito com políticas especificadas através de endereços IP, protocolos de rede (portas) e tcp syn. Sua função é filtrar e fazer o controle de entrada e saída na camada de rede e transporte. As regras desse tipo de firewall são estáticas e contêm: endereço de origem/destino, protocolos, portas de origem/destino e mensagens ICMP. Cada pacote é tratado isoladamente, não guardam o estado e nem a qual conexão o pacote pertence, por isso são também chamados de “stateless firewall”. Esses firewalls são filtros de controle simples, por isso não tem um alto índice de confiabilidade, são vulneráveis a ataques hackers (ex. exploits), e não oferecerem autenticação.

- **Filtro de Pacotes com Estado**

Este firewall realiza as mesmas tarefas que o filtro de pacotes, porém também mantem o estado das conexões, possibilita o bloqueio de varreduras, controla o fluxo de dados, faz tratamento do cabeçalho TCP e identifica possíveis ataques. Assim como no filtro de pacotes, existe uma inspeção dos pacotes, porém o estado de cada conexão e monitorado e os pacotes são bloqueados ou permitidos de acordo com as políticas de segurança do firewall. Também chamado de “stateful firewall”, ele monitora as conexões através de uma tabela de estado, que incluem: IP de origem, IP de destino, números de portas e estado da conexão. Cada tentativa de conexão é verificada, uma nova entrada é adicionada à tabela caso sejam aceitas pelas regras do firewall, desta forma uma nova conexão será estabelecida.

- **Proxy Firewall**

Este tipo de firewall é considerado um dos mais seguros, também conhecido como “application firewall” ou “gateway firewall” ele filtra mensagens na camada de aplicação, solicita pedidos no lugar dos clientes e devolve respostas no lugar do servidor, desta forma, um proxy firewall trabalha como intermediador entre a rede local e a rede externa(internet), com intuito de monitorar o trafego e proteger a rede contra possíveis ameaças. Este proxy possui um endereço IP próprio, assim ele impede que servidores externos tenha contato direto com a rede interna, além de fazer inspeções nos protocolos FTP e HTTP da camada de aplicação. Nem todos os protocolos são suportados por ele, diminuindo assim as aplicações que se conectarão a rede local, e também, quando um pacote é enviado ou recebido uma nova conexão é estabelecida,

criando assim um certo gargalo na rede, essas são umas das desvantagens desse tipo de firewall.

Facilidades dos Firewalls

São muitas as tecnologias utilizadas pelos firewalls, como por exemplo as ACL (do inglês Access Control List), que são listas que determinam qual usuário terá acesso a um sistema ou serviço. Antes de fornecer acesso a uma solicitação na rede, o servidor consulta essas listas para determinar se quem está solicitando tem permissão para fazê-lo. Alguns critérios e atributos são usados para conceder as permissões como: id do usuário, horário e local de acesso, nome de arquivo e endereço IP.

Outra tecnologia muito utilizada nos firewalls é o IDS (do inglês Intrusion Detection System), sistema de detecção de intrusão que trabalha em modo passivo; em modo inline é também conhecido como IPS (do inglês Intrusion Prevetion System) que faz detecção de intrusão em tempo real, ou seja, o IDS gera alertas quando são detectados pacotes que possam fazer parte de um eminente ataque. São muitos os tipos de IDS, mas basicamente eles analisam os pacotes na rede e comparam com as assinaturas de ataques ou anomalias semelhantes, prevenindo assim danos a rede e aos computadores.

Soluções de Firewalls

Os firewalls também podem ser em software ou em hardware, as soluções em software são mais fáceis de se implementar e consequentemente mais baratas ou até freeware (software livre de custos). Hoje qualquer sistema operacional moderno já integram aplicações com a função de firewall, como por exemplo o firewall do Windows 10; também é comum as empresas usarem computadores específicos com aplicações de firewall, como é o caso do iptables do Linux que é um sistema operacional open source (software de código fonte aberto). Já as soluções em hardware, são equipamentos específicos para essa finalidade e são mais usados geralmente em empresas. A maior vantagem desse tipo de equipamento é de o hardware ser exclusivo para esse fim, não havendo compartilhamento de recursos de hardware com outros aplicativos; assim o firewall usa todo esse recurso para tratar de mais requisições e aplicar os filtros com mais agilidade. Por serem hardware exclusivo, são mais caros, porém existem tipos mais acessíveis; um exemplo são os roteadores domiciliar que geralmente possuem algum tipo de aplicação de firewall que além de proteger os dispositivos conectados, também protegem o WI-FI para não ser usado sem permissão.

Conclusão

Os firewalls são uma solução de segurança necessária, que evitam vários tipos de ataques à rede, porém quando se trata de um sistema conectado a internet, devemos ter um cuidado especial, pois nunca estará completamente seguro. Existem uma infinidade de falhas que podem ser exploradas por hackers para um suposto ataque. A evolução da tecnologia sempre será para ambos os lados, por tanto, se novos firewalls são desenvolvidos para garantir a segurança, novas vulnerabilidades também serão exploradas em novos ataques hackers.

Referências Bibliográficas

MACHADO, Jonathan. O que é firewall?. Tecmundo, 2012. Disponível em: https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm. Acesso em: 28 nov. 2020

PIZZOLATO, Rafael. Quais os tipos de Firewall e suas diferenças?. Starti, 2017. Disponível em: https://blog.starti.com.br/tipos-de-firewall. Acesso em: 28 nov. 2020

MACÊDO, Diego. Tipos de Firewall. Diego Macêdo, 2012. Disponível em: https://www.diegomacedo.com.br/tipos-de-firewall. Acesso em: 29 nov. 2020

IDS. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2016. Disponível em: https://pt.wikipedia.org/w/index.php?title=IDS&oldid=45655712. Acesso em: 04 dez. 2020.

LISTA DE CONTROLE DE ACESSO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation,2018. Disponível em: https://pt.wikipedia.org/w/index.php?title=Lista_de_controle_de_acesso&oldid=52517514. Acesso em: 04 dez. 2020.

Firewall em Forma de Software ou Hardware. SISGRACOM, [S.l] [2015?]. Disponível em: https://www.sisgracom.com.br/protecao-de-firewall-software-ou-hardware-e-seu-funcionamento. Acesso em 04 dez. 2020.