Redes de Computadores II – Firewall Resumo

Daniel Veiga da Silva Antunes

Um firewall trata-se de um dispositivo de segurança de rede que monitora o tráfego de entrada e saída, aceitando-o, rejeitando-o ou descartando-o com um conjunto de regras definidas. Desta forma, estabelecendo uma barreira de proteção entre redes internas e externas.

Antes este controle era realizado através de uma lista de controle de acesso no roteador (ACL), porém era incapaz de determinar o tipo do pacote bloqueado e de manter ameaças fora da rede. Como hoje a comunicação com a internet é imprescindível para as empresas é necessário garantir a segurança da rede contra tráfego não autorizado.

O firewall toma decisões de ações no tráfego de rede com base num conjunto de regras definido em sua tabela. Quando uma regra é atendida, a ação associada a ela é aplicada. Este tráfego pode ser de entrada ou saída e o firewall possui um conjunto de regras separadas para ambos os casos, porém, definir uma regra de saída é sempre melhor para garantir mais segurança e assim evitar comunicações indesejadas. Já o tráfego de entrada é tratado de forma diferente. Em sua maioria, são do tipo TCP, UDP ou ICMP. Todos eles possuem um endereço de origem e destino, além de os tipos TCP e UDP possuírem os números de porta e o ICMP usar o código de tipo.

Por ser difícil cobrir todas as regras em totalidade, o firewall deve sempre ter uma política padrão, consistindo em apenas em uma ação: aceitar, rejeitar ou descartar.

Podemos categorizar os firewalls com base em sua geração. Começando pelo **firewall de filtragem de pacotes**, atuando principalmente as primeiras 3 camadas, é utilizado para controlar o acesso à rede monitorando os pacotes de saída e de entrada e permitindo que eles passem ou parem com base no endereço IP de origem e destino, protocolos e portas. Em seguida temos o **firewall de inspeção de estado de segunda geração**, que são capazes de determinar o estado de conexão do pacote, ao contrário do anterior. O **firewall de camada de aplicativo** pode inspecionar e filtrar os pacotes em qualquer camada OSI, até a camada de aplicativo, podendo bloquear conteúdo específico e reconhecer quando certos aplicativos e protocolos estão sendo mal utilizados. Por fim, temos os **firewalls de próxima geração (NGFW)**, sendo implantados atualmente para impedir violações de segurança modernas, como ataques avançados de malware e ataques na camada de aplicativos.

Temos dois tipos de firewalls, os baseados em host e os baseados em rede. No caso do primeiro tipo, o firewall é instalado em cada nó da rede que controla cada pacote de entrada e saída, protegendo o host de ataques e acessos não autorizados. Já no segundo tipo, filtram todo o tráfego de entrada e saída na rede, protegendo a rede interna e filtrando o tráfego usando regras definidas no firewall.