1.Firewalls

Um firewall baseado em rede é um dispositivo que fica em linha na sua infraestrutura e toma decisões sobre permitir ou bloquear o tráfego. Essas decisões podem ser feitas com base em números de porta, como acontece nos **firewalls tradicionais**, ou no próprio aplicativo que está sendo utilizado, o que é característico dos **firewalls de próxima geração**. Esses dispositivos não são apenas mecanismos de segurança que filtram tráfego; eles também podem executar diversas outras funções dentro da rede.

Muitos firewalls modernos atuam como terminais ou concentradores de VPN, permitindo conexões seguras entre diferentes locais ou acessos remotos. Além disso, eles podem funcionar como roteadores de camada 3, sendo posicionados nos pontos de entrada e saída da rede, onde ocorre a comunicação entre redes internas e externas. Como são roteadores, eles podem realizar **tradução de endereços de rede (NAT)**, **roteamento dinâmico** e outras funções avançadas de gerenciamento de tráfego.

Um dos tipos mais comuns de firewall encontrados nas redes atuais é o **firewall de próxima geração (NGFW - Next-Generation Firewall)**. Esse tipo de firewall pode analisar detalhadamente o tráfego que passa por ele e identificar os aplicativos específicos que estão sendo utilizados. A partir dessa análise, o firewall pode decidir se determinado aplicativo deve ou não ser permitido.

Os firewalls de próxima geração são frequentemente chamados de **Application Layer Gateway (ALG)**, **dispositivos de inspeção multi-camadas com estado** ou **dispositivos de inspeção profunda de pacotes (DPI - Deep Packet Inspection)**. Diferente dos firewalls tradicionais, que tomam decisões com base apenas nos números de porta, os NGFWs precisam capturar os pacotes, categorizá-los corretamente e depois decidir como o tráfego deve ser tratado.

Nos firewalls tradicionais, não há compreensão sobre quais aplicativos estão trafegando na rede. Eles apenas sabem quais portas estão sendo utilizadas para comunicação entre dois pontos e aplicam regras de segurança com base nessas portas. No entanto, os firewalls de próxima geração proporcionam muito mais flexibilidade, pois reconhecem os aplicativos e ainda podem utilizar números de porta como critério adicional para tomada de decisões.

Por exemplo, um firewall tradicional pode permitir ou bloquear tráfego web analisando se ele ocorre nas portas **80 (HTTP)** ou **443 (HTTPS)**. Já um firewall de próxima geração pode identificar aplicativos específicos, como **Facebook**, **YouTube** ou **Skype**, e decidir se esses aplicativos devem ser permitidos ou bloqueados independentemente das portas utilizadas. Isso se aplica a protocolos como **SSH (porta 22)**, **Remote Desktop Protocol - RDP (porta 3389)** e **DNS (porta 53, UDP)**.

Os firewalls de próxima geração também podem criar regras com base em categorias de aplicativos, listas de URLs ou qualquer outro critério definido pelo administrador. **Ao definir uma política de segurança, é possível especificar regras para permitir ou bloquear tráfego com base na origem, no destino, em endereços IP, serviços e identidade do usuário.**

Geralmente, os firewalls seguem um fluxo de regras em ordem hierárquica. Isso significa que as regras mais específicas devem ser posicionadas no topo da lista para que sejam processadas primeiro, enquanto regras mais genéricas podem ser aplicadas mais abaixo. A maioria dos firewalls também possui uma regra de **negação implícita** (implicit deny) **no final da lista, garantindo que qualquer tráfego não correspondido por regras anteriores seja automaticamente bloqueado**.

O conjunto de regras de um firewall pode ser descrito como uma **Lista de Controle de Acesso (ACL - Access Control List)**. Cada regra dentro da ACL pode incluir parâmetros como endereço IP de origem e destino, número de porta, protocolo, horário do dia e nome do aplicativo.

Para entender como um firewall toma decisões sobre o tráfego, podemos analisar um exemplo de regras configuradas. No caso de um firewall configurado para permitir SSH, HTTP, HTTPS, RDP e DNS, cada regra define o tráfego permitido com base nas portas específicas. Se houver uma tentativa de tráfego ICMP (ping), e a regra não permitir esse protocolo, o firewall bloqueará a solicitação.

Muitas organizações posicionam seus firewalls no **ponto de entrada e saída da rede**, onde ocorre a separação entre a internet e a infraestrutura interna. Em algumas arquiteturas, há um segmento de rede adicional chamado **sub-rede filtrada (screened subnet)**, **que contém serviços que precisam ser acessíveis pela internet, como servidores web e servidores de e-mail. Essa configuração impede que qualquer tráfego vindo da internet tenha acesso direto à rede interna da empresa**.

Além dos firewalls, muitas empresas implementam **Sistemas de Prevenção de Intrusões (IPS - Intrusion Prevention System)**, que podem estar integrados aos NGFWs. O IPS monitora o tráfego em tempo real e utiliza assinaturas de ameaças conhecidas para identificar e bloquear atividades maliciosas.

Os IPSs utilizam um conjunto de regras para detectar ataques. Por exemplo, um IPS pode ter uma assinatura específica para identificar o **worm Conficker**, verificando padrões específicos no tráfego de rede. Se o tráfego corresponder a essa assinatura, o IPS pode bloquear automaticamente a conexão. Além das assinaturas, os IPSs também podem detectar **anomalias** no tráfego e impedir ataques mesmo que não exista uma assinatura específica para eles.

Os IPSs contêm milhares de assinaturas, permitindo que os administradores decidam quais delas devem ser aplicadas ou ajustadas. Em alguns casos, as assinaturas

podem ser agrupadas para facilitar a gestão. Um exemplo seria a criação de um grupo para **invasões em bancos de dados**, garantindo que qualquer tentativa de injeção SQL seja bloqueada imediatamente.

Com tantas regras e assinaturas, os IPSs podem ocasionalmente gerar **falsos positivos**, bloqueando tráfego legítimo por engano. Por isso, muitas empresas ajustam suas configurações para equilibrar segurança e funcionalidade.

O IPS também pode identificar malwares, ataques contra serviços FTP e outras ameaças em tempo real. Quando configurado corretamente, ele se torna uma ferramenta essencial para proteger a rede contra invasões, ataques de negação de serviço (DDoS) e tentativas de exploração de vulnerabilidades.

A combinação de **firewalls de próxima geração** e **sistemas de prevenção de intrusões** cria uma defesa robusta para redes corporativas, garantindo que apenas tráfego legítimo e seguro tenha acesso aos sistemas internos da organização.