**IP Adress spoofing**

O envio e recebimento de pacotes IP é a regra da comunicação pela internet e segue um procedimento simples. Cada pacote tem um cabeçalho que contém informações para o roteamento. Em um pacote confiável, o endereço de origem que está indicado no cabeçalho é o endereço do remetente real.

Porém, se um atacante consegue forjar o endereço IP, o endereço de origem indicado no cabeçalho será de outro dispositivo

Utilizando o IP Spoofing, um agente malicioso pode:

* Passar despercebido pelos sistemas de detecção de IP (a origem do ataque não poderá ser identificada);
* Evitar alertas dos sistemas baseados em assinaturas de reputação de IP (whitelists, blacklists).

**Como prevenir?**

* **Proteção contra IP Spoofing por Zona de Rede (Zone Protection)**: Garante que o sistema só aceite pacotes com endereços IP originados da Zona de Rede conhecida;
* **Firewall Autenticado**: As políticas que exigem que um usuário esteja autenticado no firewall para trafegar na rede.

***Spoofing* (alteração ou repetição  de informações de roteamento)**

Esse tipo de ataque pode causar *loops* na rede, atrair ou repelir tráfego, gerar mensagens de erro de rota falsas, dividir a rede, dentre outros danos. Tudo por ter como alvo principal os pacotes de controle responsáveis pelas informações de roteamento, através de repetições ou modificações dos mesmos.

**SSL Hijacking**

O Session ocorre quando o criminoso online se coloca entre o computador e o servidor do site sem revelar a identidade de ambos os pontos finais, obtém acesso à informação personificando-se.

Algumas maneiras de se proteger contra esse tipo de ataque são o uso do protocolo **https** e o uso de VPNs.