1.Seguranças de infraestrutura

A arquitetura de redes pode variar bastante dependendo do setor em que é aplicada, mas alguns princípios fundamentais de segurança permanecem constantes. A segmentação da rede por meio de **firewalls** ajuda a manter **atacantes externos isolados**, permitindo apenas tráfego legítimo entre dispositivos. Além dos firewalls, outras tecnologias como **honeypots, jump servers, sensores de rede e balanceadores de carga** contribuem para um ambiente mais seguro.

Uma abordagem essencial na segurança de redes é o uso de **zonas de segurança**. Diferente de sub-redes ou faixas de IP, **as zonas de segurança segmentam dispositivos e recursos com base em seu nível de acesso e uso**. Uma rede pode ser dividida em **zonas confiáveis e não confiáveis**, permitindo controle mais granular sobre quais dispositivos podem se comunicar. Exemplos comuns incluem zonas **internas, externas, de servidores e de banco de dados**.

Esse modelo permite criar **regras de segurança claras**. Por exemplo, pode-se autorizar tráfego da zona confiável para a não confiável, mas restringir o inverso. Outra abordagem comum envolve a utilização de uma **zona intermediária** (screened zone), onde servidores acessíveis pela internet, como web servers, podem ser isolados para reduzir riscos.

A proteção contra invasões exige a análise da **superfície de ataque**, que representa todos os pontos vulneráveis de uma rede. Atacantes podem explorar **códigos de aplicação inseguros, portas abertas em servidores, autenticação fraca e erros humanos** para obter acesso. Mesmo um **único erro na configuração do firewall** pode permitir invasores dentro da rede.

Reduzir a superfície de ataque envolve práticas como:

- **Auditar códigos e aplicações** antes da implementação.
- **Fechar portas desnecessárias** em servidores e dispositivos de rede.
- **Monitorar o tráfego em tempo real** para detectar atividades suspeitas.

Outro aspecto importante é a **segurança do cabeamento de rede**. Em muitas empresas, os cabos de rede ficam expostos e podem ser fisicamente acessados. Se um invasor conseguir conectar-se diretamente ao cabeamento, poderá capturar pacotes e monitorar o tráfego sem precisar comprometer um dispositivo. Para mitigar esse risco, são recomendadas **proteções físicas e criptografia de tráfego**, garantindo que dados capturados por terceiros permaneçam inacessíveis.

Para conexões remotas e interligações entre filiais, o uso de **criptografia em nível de rede** é essencial. Tecnologias como **túneis IPsec e VPN concentrators** garantem que comunicações externas sejam protegidas contra interceptações.

A implementação de zonas de segurança, segmentação de tráfego e criptografia adequada fortalece a proteção da rede contra ameaças, dificultando invasões e minimizando riscos operacionais.