1.Infraestrutura de rede

A segmentação de redes é uma estratégia essencial para aumentar a segurança e o controle do tráfego entre dispositivos. Uma abordagem extrema dessa segmentação é o uso de um **air gap**, **que cria um isolamento físico entre dispositivos ou redes, impedindo que um atacante mova-se de um sistema para outro através de conexões digitais**. Esse método é usado em sistemas críticos, como redes governamentais, militares e infraestruturas industriais.

Um exemplo prático de **air gap** ocorre em **provedores de serviços gerenciados**, que mantêm redes separadas para diferentes clientes. Isso significa que mesmo que um invasor comprometa um sistema de um cliente, ele não poderá acessar os sistemas de outro. No entanto, essa abordagem exige **múltiplos switches físicos**, tornando-se inviável em grandes escalas.

Para contornar essa limitação, utiliza-se **VLANs (Virtual Local Area Networks)**, que permitem criar redes isoladas dentro do mesmo switch físico. Dispositivos em VLANs separadas não podem se comunicar diretamente, a menos que haja um roteamento intencional entre elas. Isso reduz custos e melhora a eficiência, mantendo a segurança semelhante à de um air gap físico.

Além da segmentação, é essencial entender os **três planos de operação** dentro de dispositivos de rede, especialmente em ambientes de **Software Defined Networking (SDN)**:

1. **Plano de Dados** – Responsável por encaminhar pacotes entre dispositivos, realizando funções como **trunking, NAT (Network Address Translation) e criptografia de tráfego**.
2. **Plano de Controle** – Gerencia tabelas de roteamento, protocolos dinâmicos e políticas de tráfego, decidindo como os pacotes serão entregues.
3. **Plano de Gerenciamento** – Permite a configuração e monitoramento da rede por meio de **SSH, SNMP ou APIs**, influenciando as regras aplicadas ao plano de controle.

Com a ascensão da **nuvem e redes virtualizadas**, a SDN separa esses planos de operação e permite que dispositivos de rede sejam **definidos por software**, tornando a infraestrutura mais flexível e escalável. Em um ambiente tradicional, um firewall físico pode ser necessário para segmentar servidores. Em um ambiente SDN, a mesma funcionalidade pode ser implementada virtualmente, adicionando ou removendo firewalls com poucos cliques.

A capacidade de gerenciar redes por software possibilita arquiteturas dinâmicas, como a criação instantânea de **firewalls virtuais** para controlar o tráfego entre **servidores web, balanceadores de carga e bancos de dados**. Esse modelo melhora a

segurança, pois permite ajustes rápidos na configuração da rede sem necessidade de mudanças físicas.

Ao utilizar **segmentação lógica, VLANs e SDN**, organizações podem otimizar a segurança e a eficiência da rede, minimizando riscos de movimentação lateral de invasores e garantindo controle granular sobre o tráfego de dados.