1.Segurança de portas

A **segurança de portas de rede** é um desafio comum em muitas organizações, abrangendo tanto conexões com fio quanto redes sem fio. Um dos métodos mais eficazes para garantir a proteção dessas conexões é a **autenticação baseada em portas**, que exige credenciais antes que um dispositivo possa acessar a rede. Esse tipo de segurança é frequentemente implementado em **switches e pontos de acesso Wi-Fi**, impedindo conexões não autorizadas.

O protocolo responsável por essa autenticação é o **EAP (Extensible Authentication Protocol)**, **uma estrutura flexível utilizada para gerenciar processos de autenticação em diversas tecnologias de rede**. O EAP é amplamente integrado ao padrão **IEEE 802.1X**, conhecido como **Network Access Control (NAC)** baseado em portas. Esse protocolo garante que um usuário ou dispositivo só possa acessar a rede após a validação de suas credenciais.

O processo de autenticação baseado em **802.1X** envolve três componentes principais:

1. **Supplicant (Solicitante)** – O dispositivo do usuário que solicita acesso à rede.
2. **Authenticator (Autenticador)** – O switch ou ponto de acesso que controla o acesso à rede.
3. **Authentication Server (Servidor de Autenticação)** – Um sistema, como **RADIUS, LDAP, TACACS+ ou Kerberos**, que valida as credenciais do usuário.

Quando um dispositivo se conecta a uma porta protegida por **802.1X**, o autenticador inicialmente bloqueia o tráfego e envia um **EAP request** ao solicitante, solicitando informações de login. O dispositivo responde com um **EAP response**, que é então encaminhado ao servidor de autenticação. Se as credenciais forem válidas, o servidor autoriza o acesso e instrui o autenticador a liberar a conexão.

Esse processo reforça a segurança da rede ao garantir que apenas usuários autenticados possam se conectar. Além disso, a integração com bancos de dados de autenticação permite um gerenciamento centralizado de permissões e políticas de acesso. Implementar **802.1X com EAP** é uma estratégia essencial para proteger redes corporativas contra acessos não autorizados e ataques cibernéticos.