# Redes Windows

* Topologia: As redes Windows geralmente seguem a topologia cliente-servidor, onde existem servidores que gerenciam as autenticações dos usuários e as políticas de segurança. Os clientes se conectam aos servidores para realizar as autenticações e acessar recursos de rede.
* Protocolos de segurança envolvidos: A autenticação em redes Windows é baseada no protocolo Kerberos, que fornece autenticação forte e criptografia de dados. Além disso, o protocolo LDAP é usado para consultar o diretório ativo e obter informações sobre os usuários e grupos.

# Redes Linux

* Topologia: As redes Linux podem seguir diferentes topologias, como cliente-servidor ou ponto a ponto. Geralmente, existem servidores que gerenciam as autenticações e os clientes se conectam a esses servidores para realizar autenticações e acessar recursos de rede.
* Protocolos de segurança envolvidos: A autenticação em redes Linux pode ser realizada através de diferentes protocolos, como o PAM (Pluggable Authentication Modules) e o LDAP. O protocolo SSH (Secure Shell) também é amplamente utilizado para autenticação e comunicação segura.

# API Authy (Google)

* Topologia: A API Authy é uma plataforma de autenticação em nuvem, que pode ser utilizada por diferentes tipos de aplicações. A topologia pode variar dependendo da forma como a API é integrada à aplicação cliente.
* Protocolos de segurança envolvidos: A API Authy utiliza criptografia de ponta a ponta para garantir a segurança dos dados. Além disso, utiliza diferentes protocolos de segurança, como o SSL/TLS para criptografia de dados em trânsito e o OTP (One-Time Password) para autenticação.

# Google Autenticador em 2 fatores com PHP

* Topologia: O Google Autenticador é uma aplicação móvel que gera códigos de autenticação em 2 fatores. A integração com PHP pode ser realizada de diferentes formas, como através de bibliotecas e APIs específicas.
* Protocolos de segurança envolvidos: A autenticação em 2 fatores com o Google Autenticador é baseada no protocolo OTP, que utiliza códigos únicos e temporários para autenticação. Além disso, a comunicação entre o servidor e o aplicativo pode ser criptografada utilizando o protocolo HTTPS.