# 铠盾零信任访问服务应用场景

## 场景：远程办公

- 越来越多的企业开始采用WFH(Work From Home)，需要员工或者合作伙伴用自己的终端设备通过互联网访问部署在私有云上的IT服务
- 铠盾零信任访问服务能为远程办公提供安全可靠的零信任远程访问服务：
  - 在私有云的服务器上安装ZTAS-VENUS程序，对服务器上的IT服务进行零信任保护
  - 域管理员在平台上为企业员工创建域账号
  - 在私有云上部署ZTAS-EARTH(零信任安全网关)，为终端设备提供安全隧道
  - 企业员工用域账号在终端设备(Windows/Linux/Mac)上用ZTAS-MARS程序注册MARS设备
  - 域管理员根据实际需要对员工的MARS设备进行IT服务授权
  - 企业员工通过ZTAS-MARS跟ZTAS-EARTH建立安全隧道，依据授权访问私有云上的IT服务

# 常见网络安全防护技术

## 防火墙

- 技术原理：通过对入栈、出栈的数据包分析包内的IP地址、端口，看IP地址和端口是否符合预先设定的安全策略，并根据策略对数据包做出放行或者丢弃动作
- 缺点和不足：
  - 防火墙不能抵御最新的未设置策略的攻击漏洞
  - 防火墙的并发连接限制容易导致拥堵或者溢出，成为性能瓶颈
  - 防火墙对服务器合法开放的端口的攻击，无法阻止
  - 防火墙对内部主动发起的攻击一般无法阻止
  - 无法做到设备级的安全策略