铠盾零信任访问服务应用场景

公有云/私有云之间实现零信任访问

- 企业在公有云上的IT服务暴露到互联网上，私有云通过互联网访问公有云上的IT服务，这些IT服务容易遭到嗅探和攻击，需要将这些IT服务隐藏起来，对互联网不可见，仅允许私有云上特定的设备才能访问这些IT服务
- 铠盾零信任访问服务的实施过程：
  - 在ZTAS-MERCURY管理端，创建公有云/私有云的数据中心
  - 在公有云数据中心，定义好对应的IT服务记录，并创建NAT记录
  - 在公有云/私有云的服务器上，分别部署ZTAS-VENUS程序
  - 在ZTAS-MERCURY管理端，以私有云上的ZTAS-VENUS为源，公有云上的IT服务为目标，创建EWP(东西向保护)记录，保证私有云上指定的ZTAS-VENUS设备能访问公有云上的IT服务
- 效果：
  - 互联网没法嗅探到公有云里暴露到互联网上的IT服务，达到IT服务隐形效果，私有云上经过授权的VENUS设备能正常访问公有云上的IT服务

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