铠盾零信任访问服务

基本概念

- 域(Domain)：每个企业在平台里都有一个唯一的域，域之间的网络是完全隔离的。每个域有一个域管理员（Admin），负责管理当前域的所有零信任访问功能的配置
- 域用户(Domain User)：域管理员可以为当前域注册用户，将用户的令牌分享给对应的用户，用户凭该令牌在ZTAS-MARS程序登录，生成Mars设备，域管理员可以为每个Mars设备设置IT服务的访问权限
- 数据中心(Datacenter)：数据中心是同一局域网内能互相访问的IT设备的集合，一个域，可以包含任意多个数据中心，可以来自公有云，私有云
- Venus设备：运行在Linux设备上的ZTAS-VENUS程序，会采集宿主设备的特征，生成独一无二的设备指纹，生成Venus设备，每台Venus设备由该设备指纹标识

铠盾零信任访问服务

基本概念

- VENUS程序：运行在Linux宿主机上的核心程序，依据对应Venus设备的零信任安全规则，通过内核模块对宿主设备上的TCP会话进行零信任保护
- 零信任安全规则：对Venus设备上的TCP会话进行零信任保护的指令，包含方向(Ingress/Egress），源IP地址/端口，目标IP地址/端口，指纹，以及保护策略（Accept/Reject/ZTP）
- 东西向访问保护(East/West Protection, EWP)：用于保护VENUS设备之间访问IT服务的安全
- Mars设备：指域用户在特定的终端设备（Windows/Linux/Darwin）上通过ZTAS-MARS程序登录后，由程序采集终端设备的特征信息，结合用户的ID，生成独一无二的指纹，从而生成Mars设备，不同的用户在同一台设备上有不同的指纹。Mars设备是一种多重信任因素认证机制，确保用户只能在特定的设备上依据零信任策略访问IT服务