CSA GCR cloud security alliance GREATER CHINA REGION ®

封闭还是开放

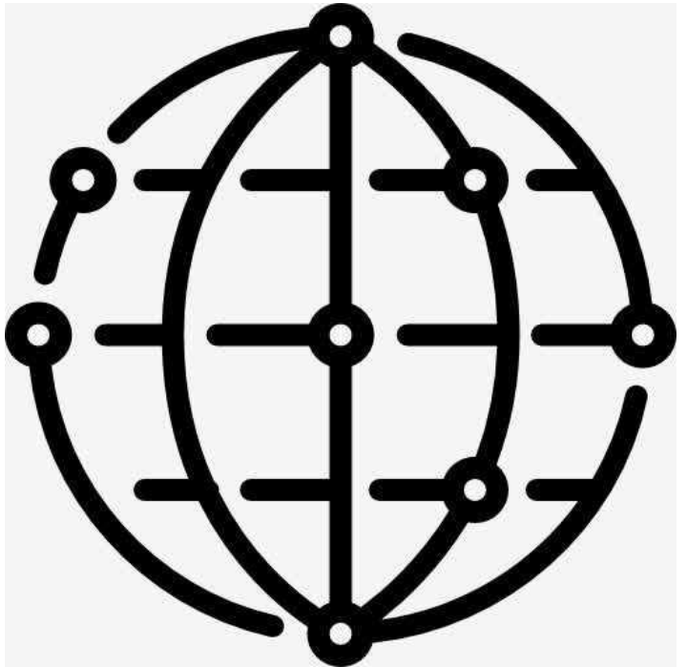
——谈零信任落地

YOUNG

所有的实名应用访问都需要“零信任”

封闭与开放

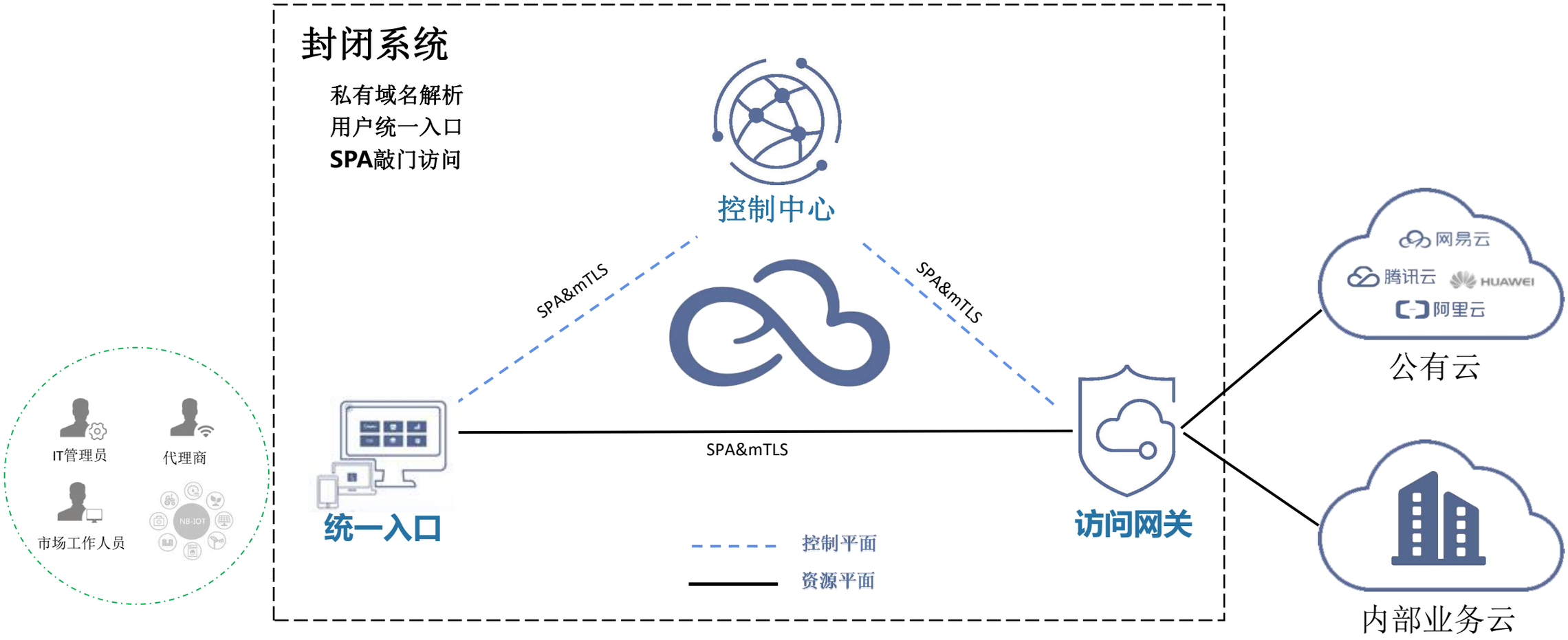
封闭：最小化攻击面



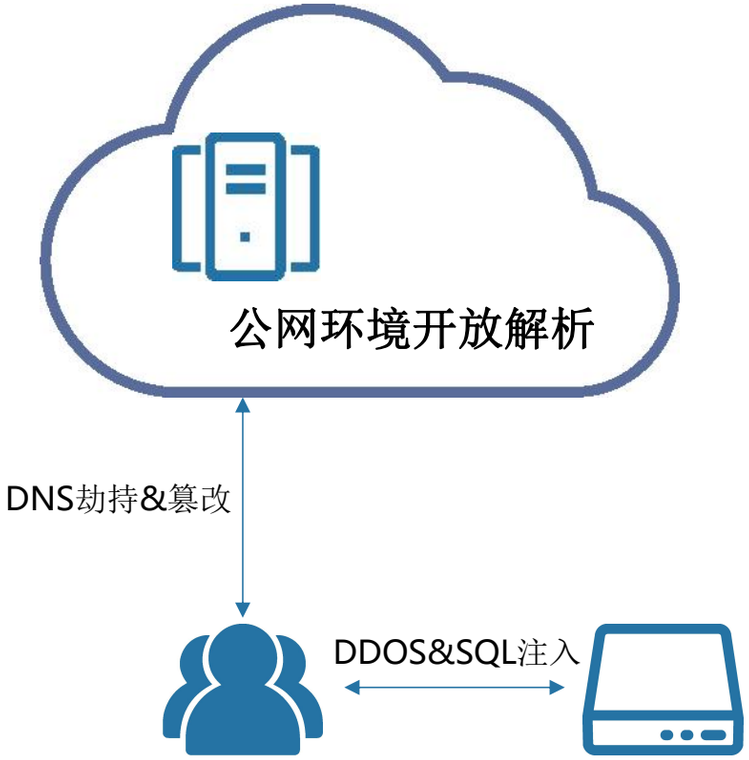
开放：更符合互联网宗旨

如何基于应用场景权衡和取舍二者的平衡

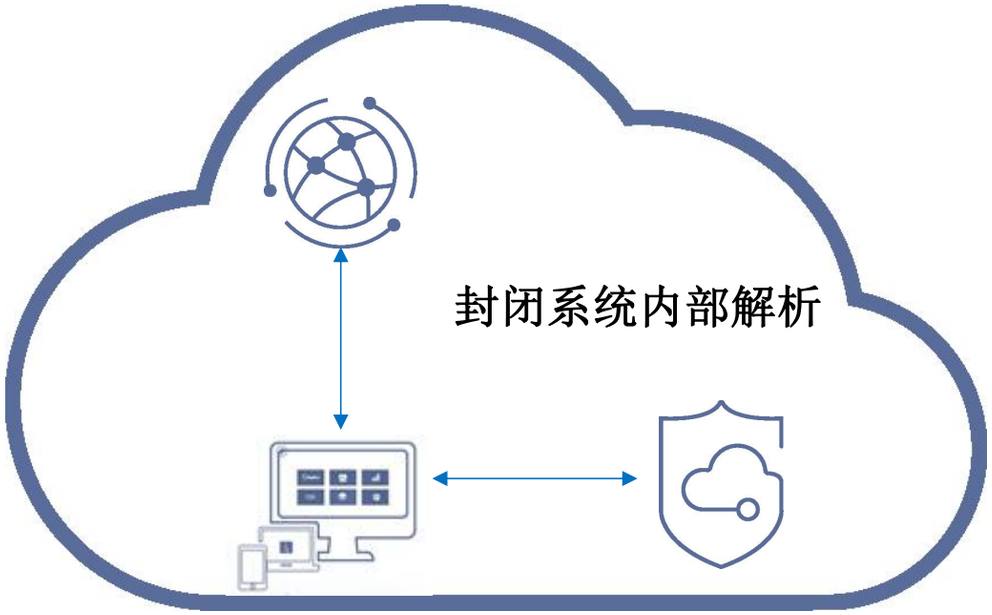
零信任SDP封闭网络安全架构



互联网开放DNS解析和零信任私有域智能引流

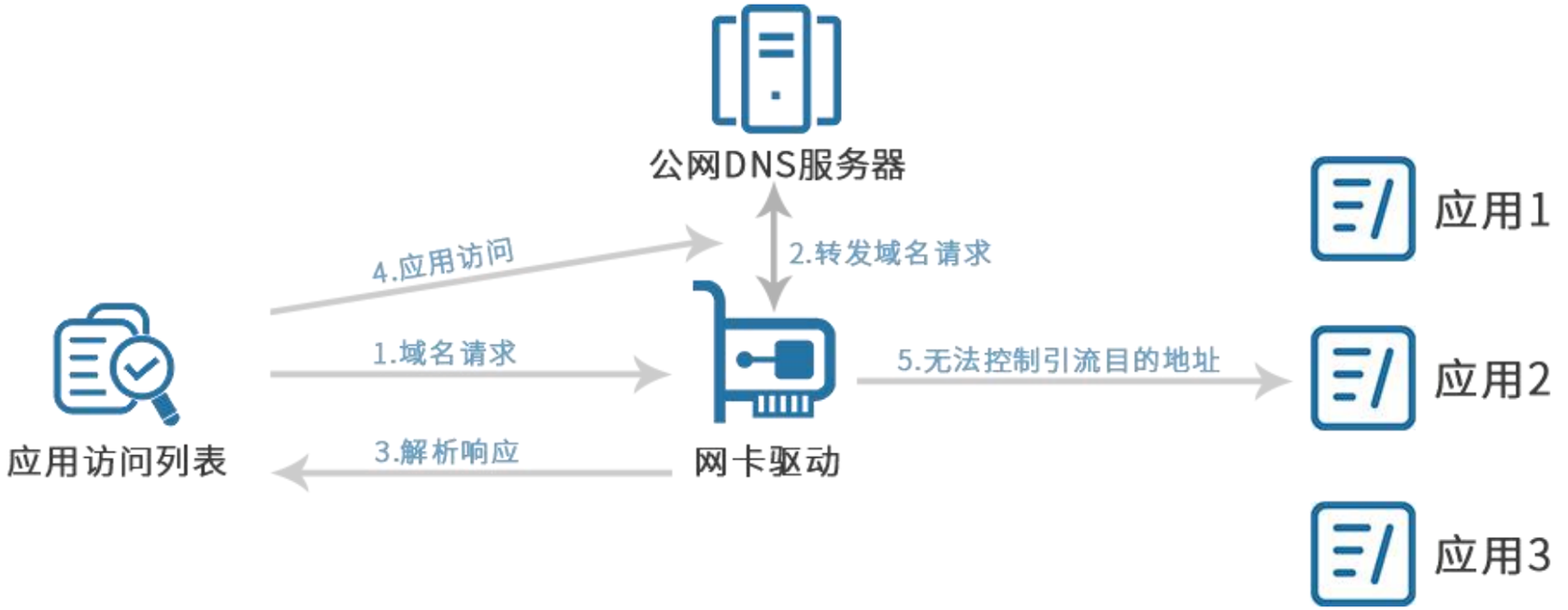


- 公网DNS解析
- 互联网开放访问
- 暴露应用端口

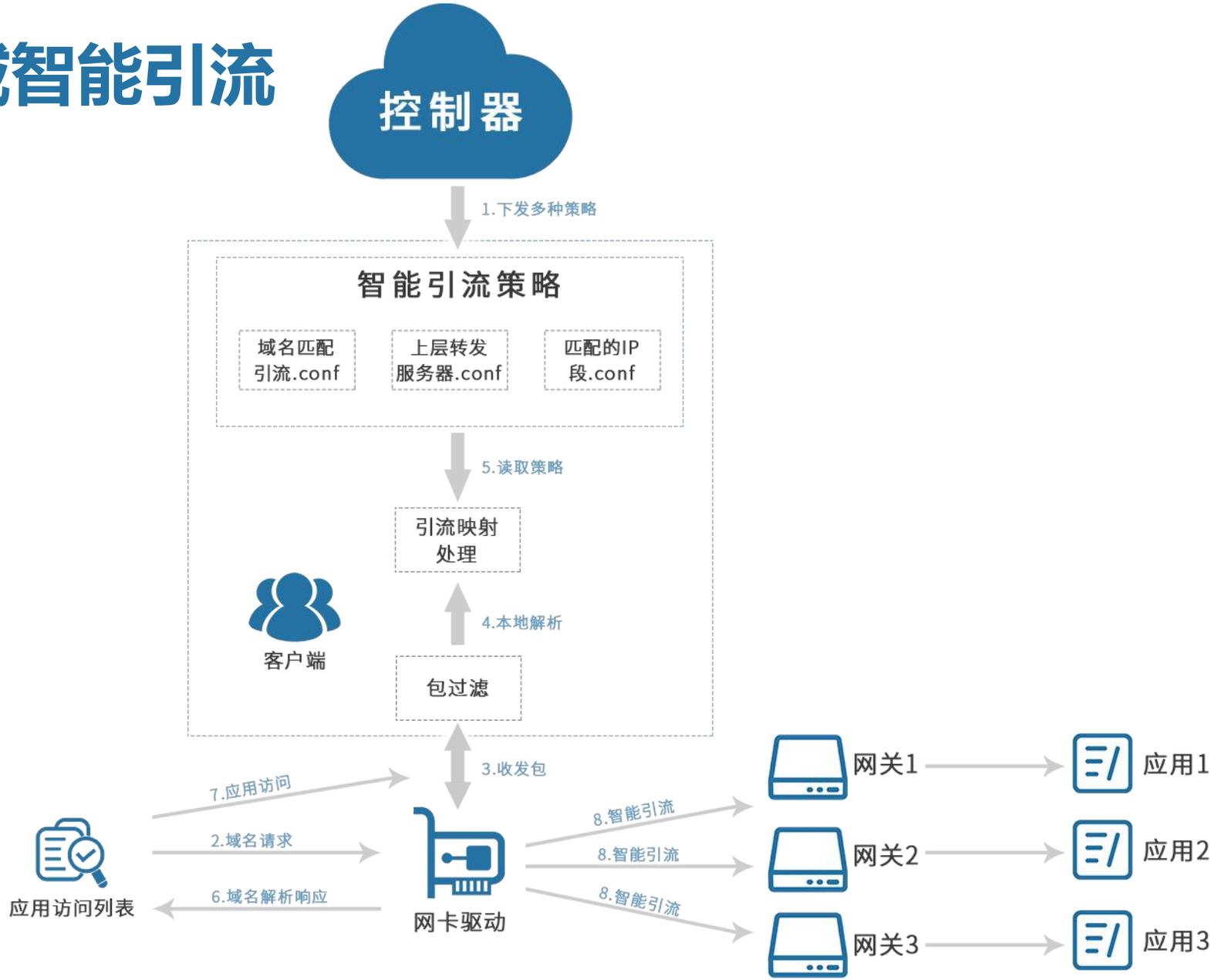


- 私有域名解析
- 统一企业入口
- 封闭智能引流

互联网开放DNS解析

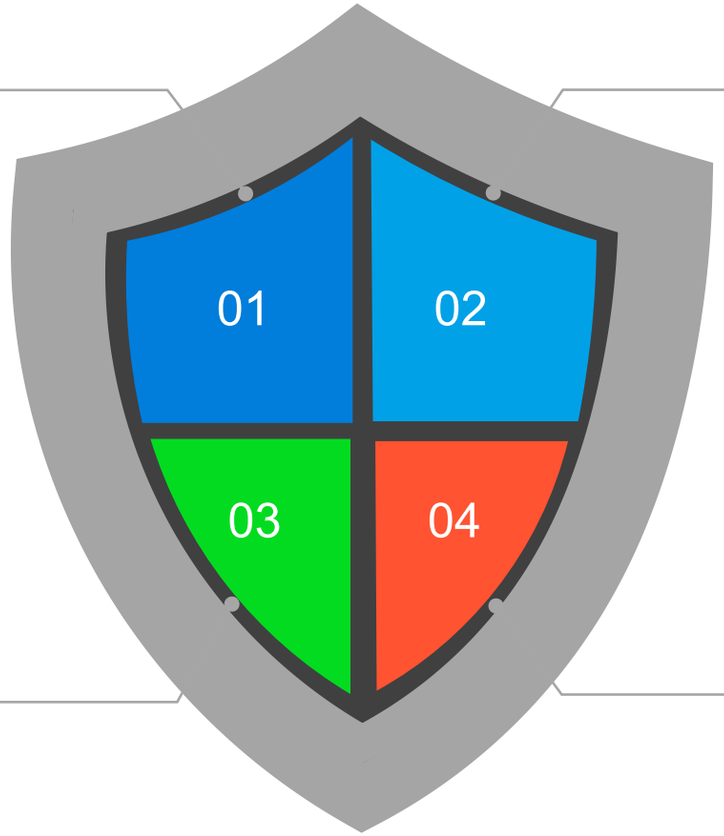

公网DNS服务器
4.应用访问
2.转发域名请求
1.域名请求
5.无法控制引流目的地址
3.解析响应
应用访问列表
网卡驱动
应用1
应用2
应用3

零信任私有域智能引流


控制器
1.下发多种策略
智能引流策略
域名匹配
引流.conf
上层转发
服务器.conf
匹配的IP
段.conf
5.读取策略
引流映射
处理
4.本地解析
客户端
包过滤
3.收发包
7.应用访问
2.域名请求
6.域名解析响应
应用访问列表
网卡驱动
8.智能引流
8.智能引流
8.智能引流
网关1
网关2
网关3
应用1
应用2
应用3

企业级浏览器，打造统一的应用访问可信入口

所有的访问只给合法用户使用



缩小攻击面

- ✓单包授权，保护服务端口
- ✓封闭内部引流系统
- ✓应用访问白名单机制，拒绝非授权的URL访问
- ✓应用路径默认隐藏和授权推送

数据安全保护

- ✓企业数据不落盘
- ✓文档水印保护
- ✓国密传输保护

终端可信

- ✓终端与账号绑定，避免非法设备接入
- ✓配置参数防篡改，避免恶意软件攻击

统一入口

- ✓WEB/WEB终端/CS应用统一入口

SPA机制隐藏应用

只有合法用户能访问进来

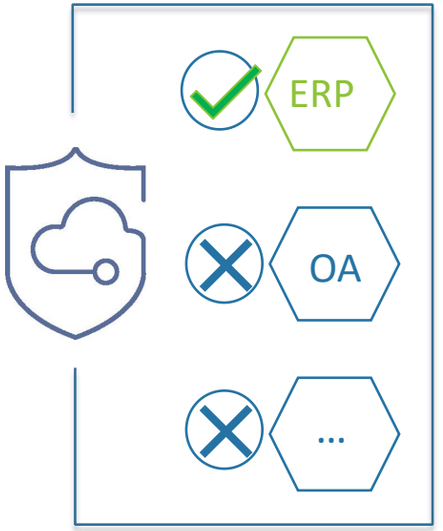
可信身份+设备，才可以触发SPA

经过SPA认证后，在特定时间段内开放端口等待连接，超时自动关闭

默认关闭所有TCP端口, UDP端口只接收不响应，隐藏业务

基于单次请求连接加密

应用级控制，每次访问都需要敲门



封闭是为了更安全，安全是为了更方便

安全和方便并不矛盾，我们追求的是既安全、又方便

面向大众用户的应用场景

- **不改变使用习惯**，保护个人隐私；
- 减少咨询和投诉，降低客户维护成本；
- 抵御常见的攻击，提升系统稳定性。

面向企业用户的应用场景

- **统一入口**，**提高**应用访问**效率**；
- 客户端自动更新，减少管理员维护工作；
- 内/外网同样的安全保护，缓解管理员压力。

零信任可落地所有实名认证的业务场景

金融/证券

手机银行
证券交易

互联网/运营商

网上商城
移动营业厅

企业/政府

内网防护
远程办公

教育/传媒

在线学习
资料下载

封闭还是开放，安全还是方便，我们如何选择

所有的实名访问都需要逐步升级到基于“零信任”的安全框架下，那么我们如何去权衡封闭与开放，安全与便利的关系，如何在保障应用访问安全的同时，给予用户最便利的访问方式。

1. 如何权衡**基于零信任的封闭**和**基于互联网的开放?**

2. 如何对**零信任的封闭**制定**统一的产业标准?**

VS

THANK YOU

零信任十周年峰会