



# 北京网络安全大会

## SDP如何帮助企业安全上云

——零信任安全的实践与探索

**NO.1** 软件定义边界（SDP）介绍

**NO.2** 深云SDP的落地实践探索

**NO.3** 深云SDP的技术实践探索



## 云深互联 (北京) 科技有限公司

云深互联取名自 **“只在此山中，云深不知处”** 古诗。旨在通过新一代SDP（软件定义边界）网络隐身技术，让企业数据“隐身”于互联网之中，让黑客无从发起攻击，从而有效保护企业的数据资产。**让每一家企业的数据可以安全上云并高效地互联互通。**



## 国际云安全联盟（大中华区）SDP工作组

<https://www.c-csa.cn/ruanjiandingyibianjieSDP.html>

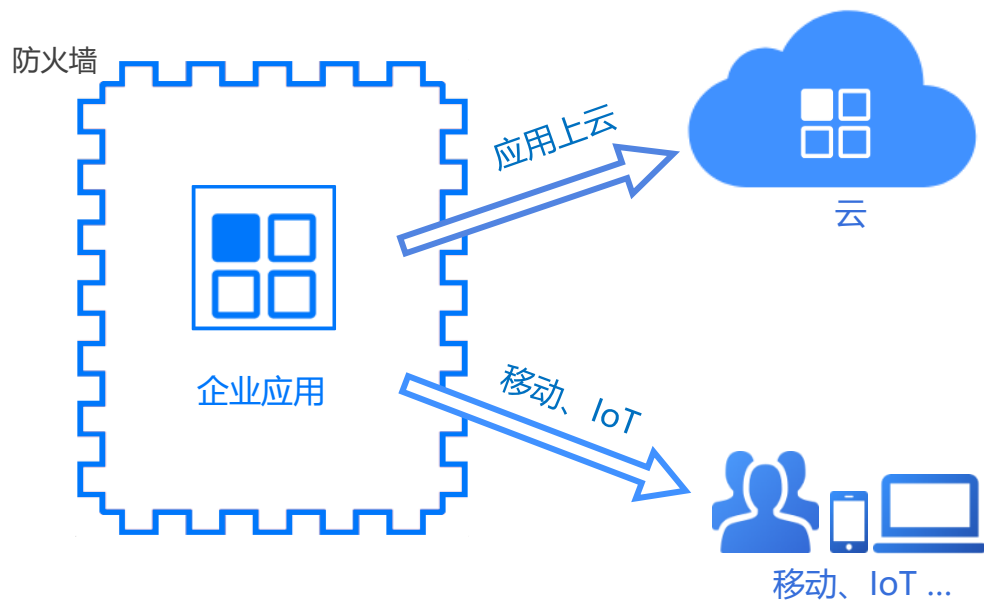
Software Defined Perimeter（软件定义边界，即SDP）安全模型由国际云安全联盟CSA于2014年提出，已经在海外广泛成功应用，有效地帮助企业解决上云的安全问题。

为了提高SDP安全模型在中国的实践和创新，中国市场CSA大中华区于2019年3月成立SDP工作组，首批参与单位有：阿里云、腾讯云、京东云、奇安信、深信服、绿盟科技、Ucloud、顺丰科技、天融信、云深互联、中宇万通、华云数据、三未信安、上元信安、安全狗、易安联、联软科技、上海云盾、缔盟云等30多家企业。[云深互联](#)担任组长单位。

## 进入万物互联时代，企业安全无法再100%依赖防火墙

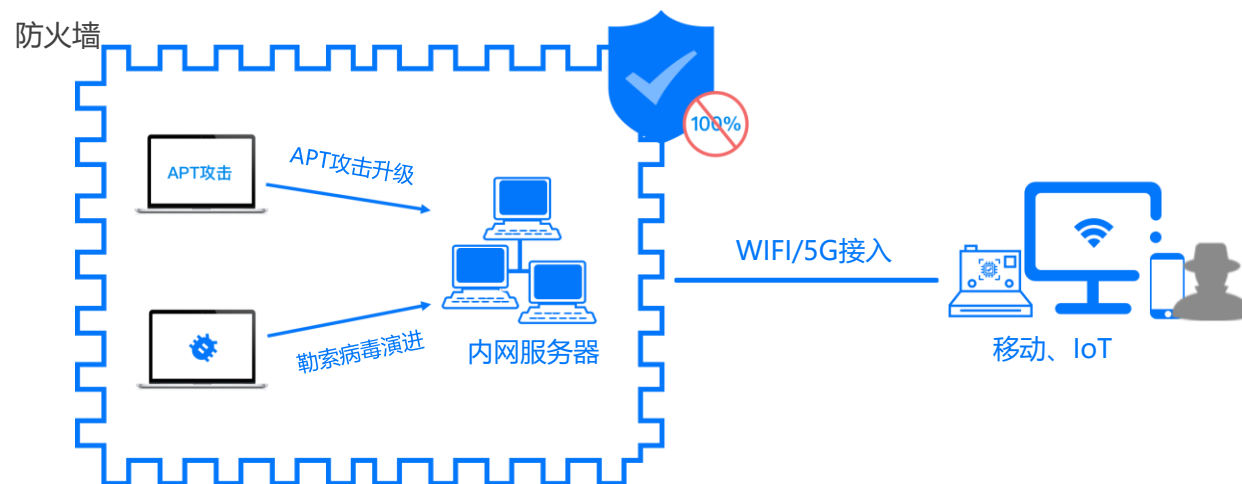
### 变革1：数据开始“出墙”

云计算、移动互联网、IoT物联网等新技术出现和采用，让企业数据不再局限在内网



### 变革2：内网不再100%安全

APT攻击、勒索病毒等黑客技术的发展，以及企业WIFI/5G等无线方式接入，让黑客更容易渗透进内网



传统“城墙”安全理念已经过时，“零信任”才是未来



“Never Trust  
Always Verify”

All resources are accessed in a secure manner regardless of location.

Access control on a “need-to-know” basis should be strictly enforced.

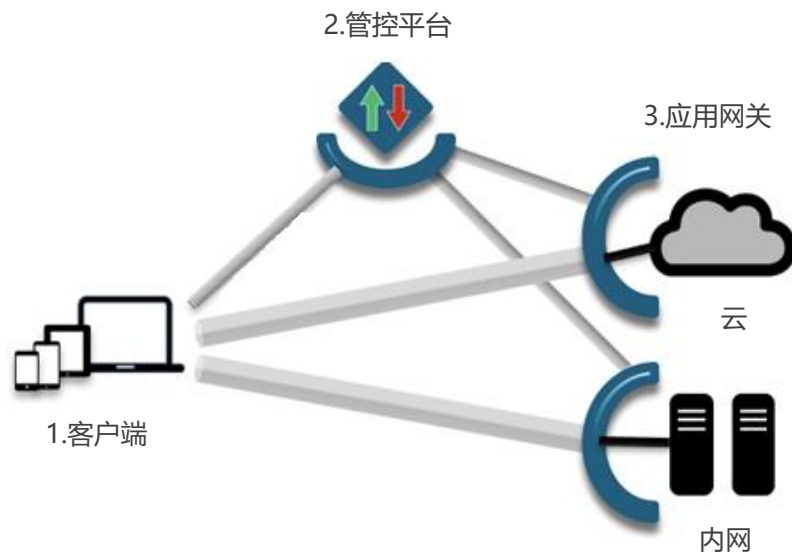
Inspect and log all traffic



零信任理念落地方案：国际云安全联盟CSA定义了SDP安全模型

## SDP: Software-Defined-Perimeter (软件定义边界)

### SDP安全模型架构图



#### 三大组件

1. Client: 设备、身份验证
2. Controller: 配置策略, 管理连接
3. Gateway: 网络隐身, 访问控制

### SDP核心优势

#### 网络隐身 Information Hiding

隐藏服务器地址、端口, 使之不被扫描发现

#### 预验证 Pre-authentication

在连接服务器之前, 先验证用户和设备的合法性

#### 预授权 Pre-authorization

用户只能看到被授权访问的应用 (最小权限原则)

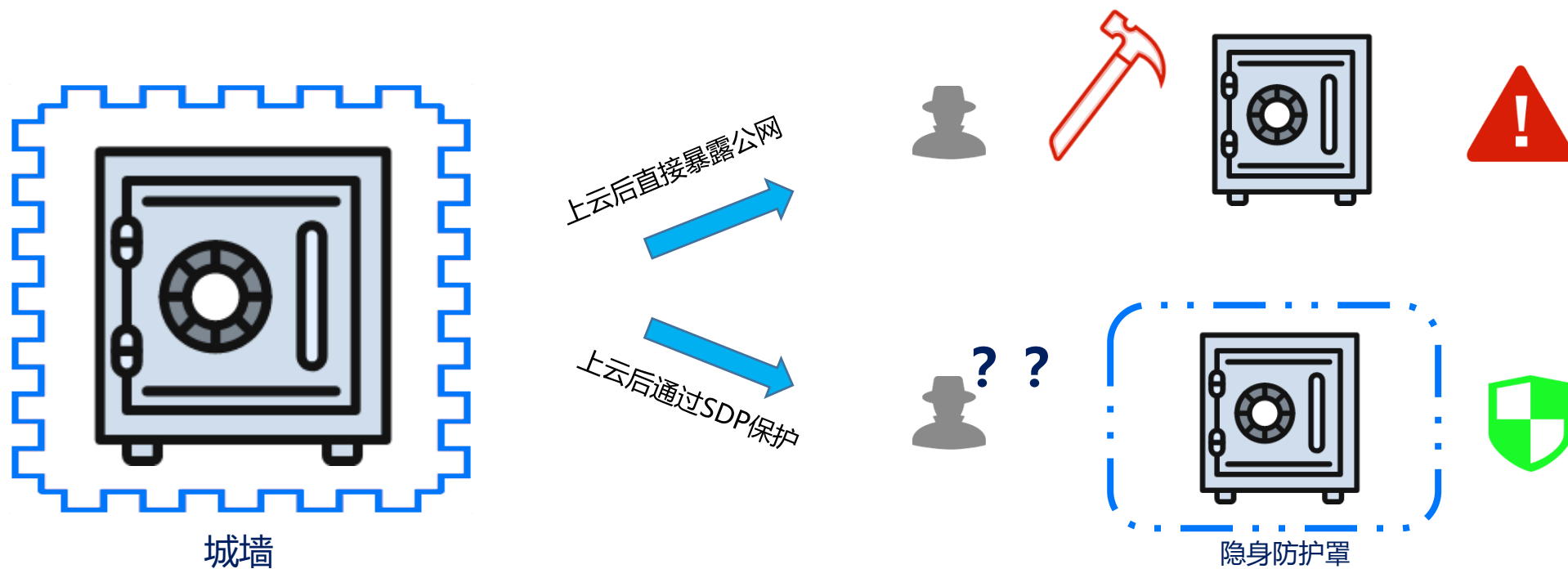
#### 应用级的访问准入 Application Layer Access

用户只有应用层的访问权限, 无网络级的访问

#### 扩展性 Extensibility

基于标准协议, 可以方便与其它安全系统集成

SDP通过网络隐身和用户身份控制，帮助企业安全上云



**类比：**服务器上云就好像把保险箱从“家里”被移动到了“室外广场”，暴露在公众视野下，将经受7x24的黑客攻击，再坚固的保险箱都可能被击破，因为天下没有无漏洞的程序。SDP就好像给保险箱加上一层网络隐身“隐身罩”，黑客没法攻击看不见的东西。



## SDP（软件定义边界）已经在国外成功广泛应用

### SDP有效防止12大安全威胁中的

#### 10大安全威胁\*

1. 数据泄露
2. 弱身份、密码与访问管理
3. 不安全的界面 和API 接口
4. 系统和应用程序漏洞
5. 账号劫持
6. 内部恶意人员威胁
7. 高级持续威胁攻击 (APTS)
8. 数据丢失
9. DDoS拒绝服务
10. 共享技术问题

\* 来自云安全联盟CSA白皮书《SDP for IaaS》

- **RSA Conference**

连续4年举办SDP黑客破解大赛，无人攻破

- **Gartner**

SDP入选《2017年11大信息安全技术》，《2018最应投入的10大安全项目》，Gartner《网络服务隔离指南》：“到2021年底，60%的企业将用SDP取代VPN”



美国硅谷SDP创业公司**Zscaler**于2018年纳斯达克上市，市值已超过100亿美金。以色列SDP创业公司**Safe-T**也于2018年在以色列股市上市。



Google内部孵化的SDP项目BeyondCorp已经成功应用于谷歌大多数员工的日常办公



国外众多老牌安全产商、CDN产商、电信运营商都推出自己的SDP产品

## 软件定义边界(SDP)- 入围Gartner2019行业报告推荐产商

## Gartner定义云安全趋势：零信任网络访问ZTNA（即SDP）

**云深互联成为中国区唯一入选ZTNA市场指南的产商，同时入选的还有美国对标Zscaler和OKTA，以及巨头微软、Google、思科、赛门铁克等**

Gartner.

This research note is restricted to the personal use of the individual user.

Market Guide for Zero Trust Network Access


Published : 29 April 2019

Zero trust network access replaces traditional perimeter-based security models which require companies to extend external networks to employees and partners to connect and collaborate. Security and risk management leaders should plan for employee/partner-facing applications.

Table 2. Representative Vendors of Stand-Alone ZTNA

Vendor	Product or Service Name
CyberArk	AppGate SDP
Google Cloud Platform (GCP)	Cloud Identity-Aware Proxy (Cloud IAP)
Microsoft (Windows only)	Azure AD Application Proxy
Pulse Secure	Pulse SDP
Safe-T	Software-Defined Access Suite
Unit42	Stealth
Waverly Labs	Open Source Software Defined Perimeter
Zeniter Systems	Cloud-Over-IP (COIP) Access

Source: Gartner (April 2019)

深云SDP  
DeepCloud

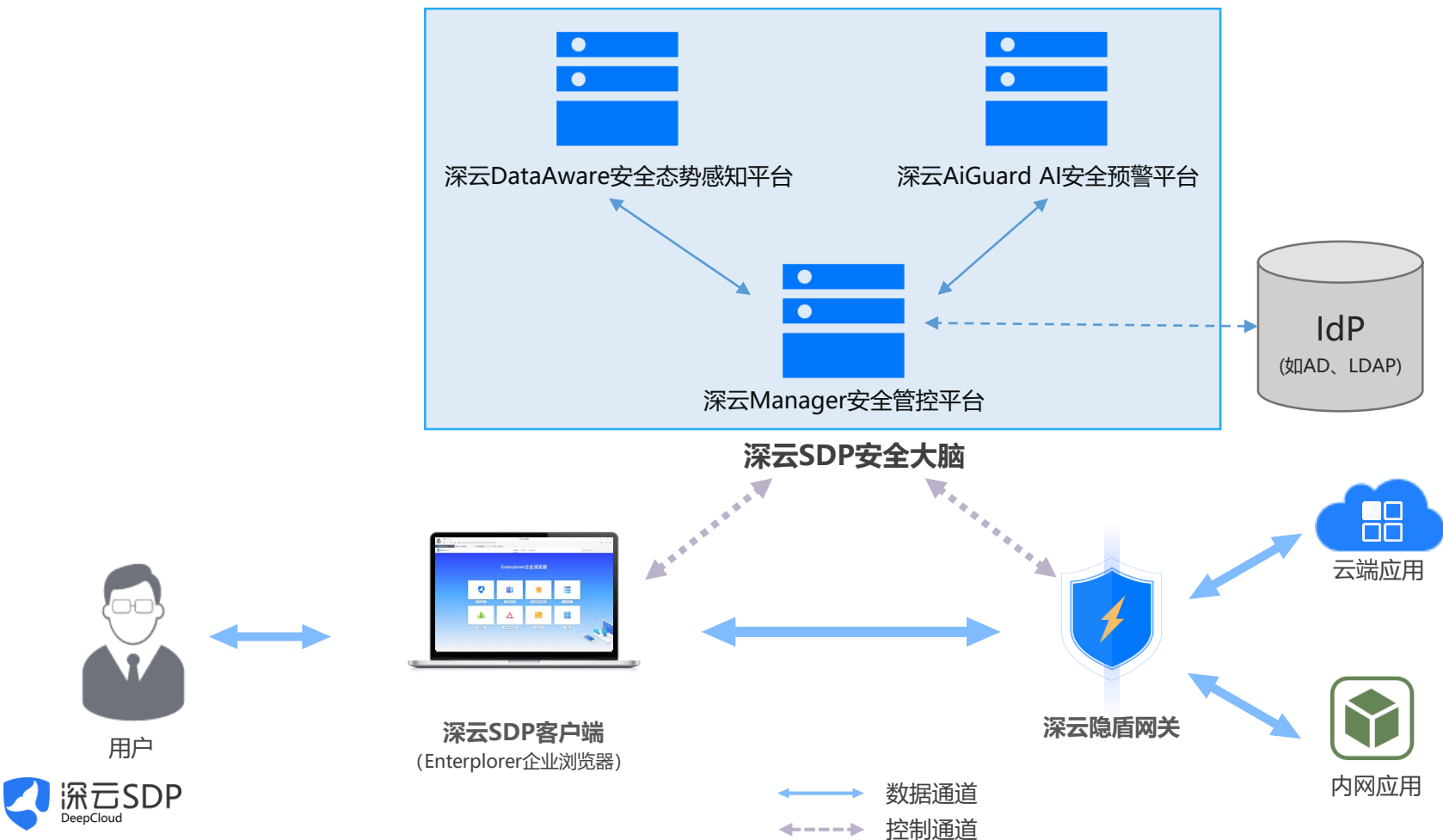
- As a service from the cloud
- As a stand-alone offering that the customer is responsible for support

As-a-service offerings (see Table 1) require less setup and maintenance. As-a-service offerings typically require provisioning at the end-user or service through the vendor's cloud for policy enforcement. Stand-alone offerings require customers to deploy and manage all elements of the product. In addition, cloud providers offer ZTNA capabilities for their customers.

Table 1. Representative Vendors of ZTNA as a Service

Vendor	Product or Service Name
Akamai	Enterprise Application Access
Cato Networks	Cato Cloud
Cisco	Duo Beyond (acquisition by Cisco)
CloudDeep Technology (China only)	DeepCloud SDP
Cloudflare	Cloudflare Access
InstaSafe	Secure Access
Meta Networks	Network as a Service Platform
New Edge	Secure Application Network
Okta	Okta Identity Cloud (Acquired ScaleFT)
Perimeter 81	Software Defined Perimeter
SAIFE	Continuum
Symantec	Luminate Secure Access Cloud (acquisition by)
Verizon	Vidder Precision Access (acquisition)
Zscaler	Private Access

## 深云SDP：中国领先的SDP平台



### 深云SDP隐盾网关

- 应用服务器的隐身防护罩

### 深云SDP客户端

- Enterplorer企业浏览器：企业B/S应用的统一安全入口

### 深云SDP安全大脑

- 深云Manager安全管控平台
  - 用户身份管理与安全验证
  - 设备管理与安全验证
  - 应用管理与权限控制
  - 数据防泄密控制
- 深云DataAware安全态势感知平台
  - 安全办公态势大屏
  - 用户行为审计
  - 数据统计报表
- 深云AiGuard AI安全预警平台  
(研发中)



## 1、深云SAAS平台（上架公有云市场）

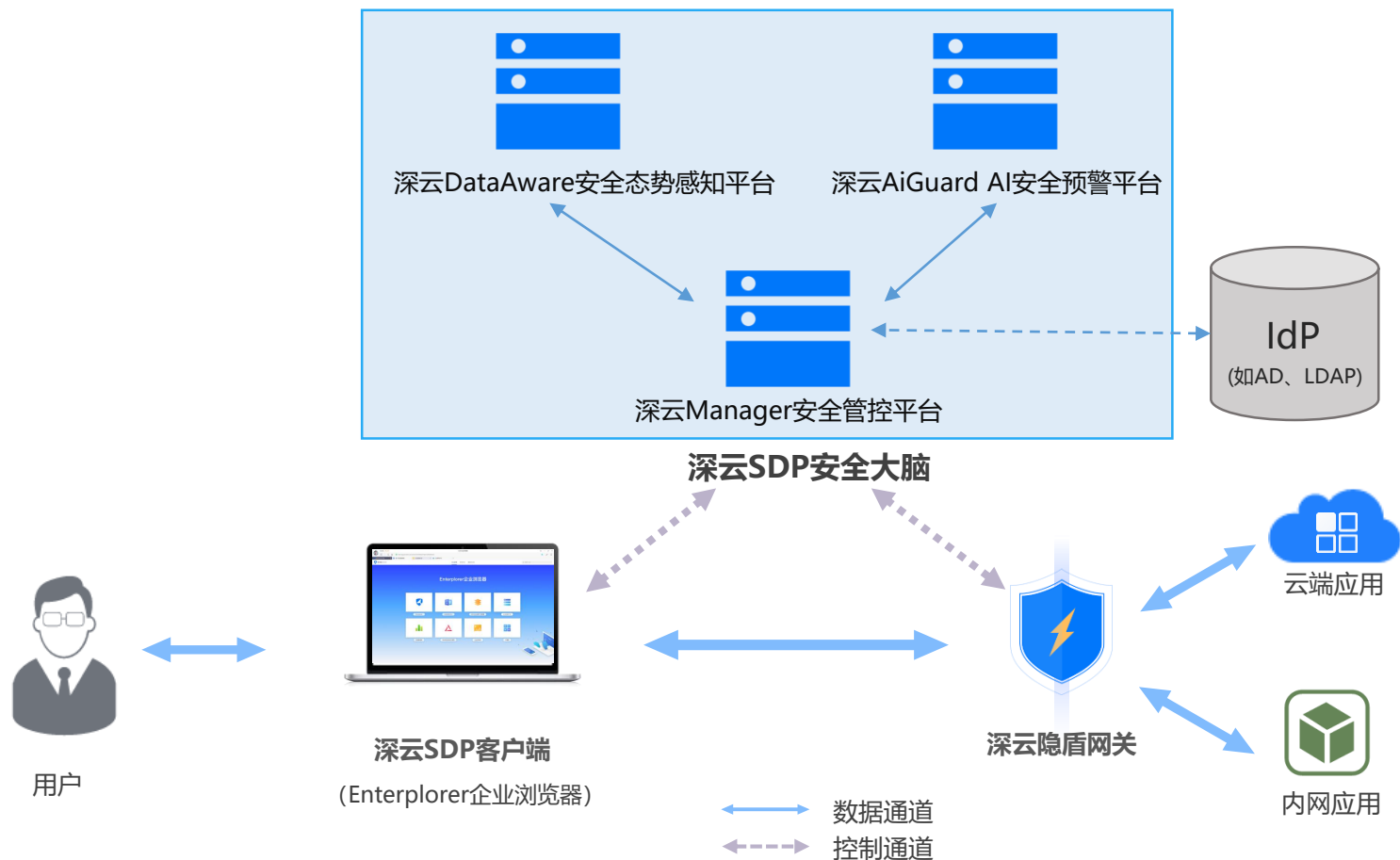


## 2、深云安全一体机（私有部署）



包含深云SDP安全大脑、隐盾网关等全套软硬件平台，**开箱即用！**

## 产品三大组件：网关、企业浏览器、大脑



## 深云SDP的落地实践探索

**场景：**企业上云

**需求：**企业分支机构（门店、营业厅）访问企业业务支撑系统



## 场景:

营业厅日常访问业务支撑系统十余个:

翼工程、网络运营一体化平台、2/3G移动客户体验管理平台 (CEM)、4G移动客户体验管理平台 (CEM)、综合外呼平台系统、渠道销售实况监控、县支局长工作台、门店承包助手、代理商4.0、BSS3.0等。

## 营业厅特点:

- (1) 位置分散: 20个地级市级分公司、90个县级分公司
- (2) 人员复杂: 直营店、合作网点、代理网点多种类型
- (3) 变化频繁: 100+个直营店、200+个合作/代理网点

## 当前方案:

将营业厅10多个业务支撑系统迁移到电信云上, 方便访问

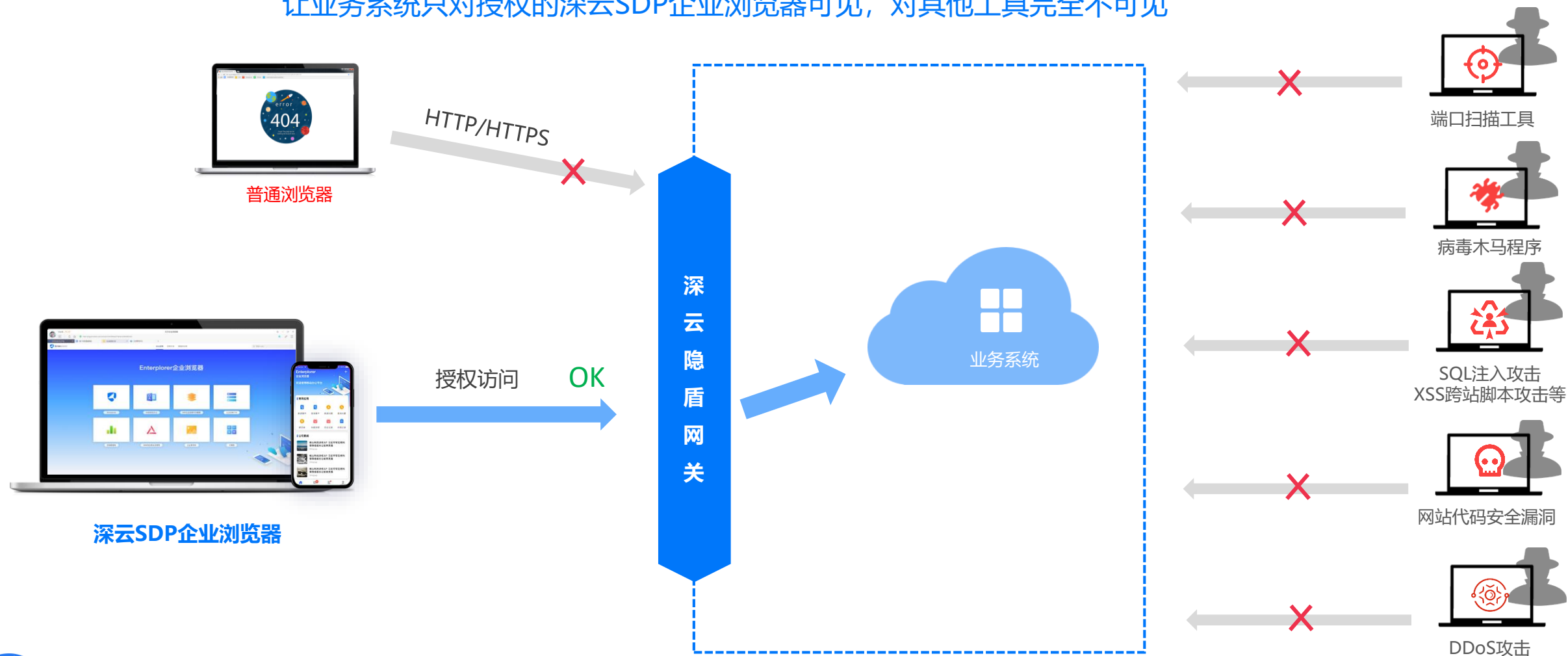
## 痛点:

核心业务支撑系统暴露在公网上, 经常受到黑客扫描和攻击



## 深云SDP解决企业上云的安全问题

让业务系统只对授权的深云SDP企业浏览器可见，对其他工具完全不可见



## 上线结果:

- 10个业务系统从互联网上彻底“隐身”
- 只有授权深云SDP企业浏览器能够访问
- 营业厅业务人员只需要安装，并登录企业浏览器就可以办公
- 通过短信验证、硬件设备绑定等功能，使原来业务系统的身份验证更加安全

NSFOCUS			
绿盟科技“远程安全评估系统”安全评估报告-主机报表			
目录			
1.主机概况			
主机风险	 非常安全 (1.0分)		
IP地址	222.83.4.37	漏洞扫描检查模板	全部漏洞扫描
系统版本	V6.0R02F04SP04	漏洞风险评估分	1.0分
插件版本	V6.0R02F01.1411	主机风险评估分	1.0分
扫描起始时间	2019-05-25 22:40:07		
扫描结束时间	2019-05-25 22:55:59		

## 上线结果：XX省电信营业厅实拍图





深云SDP数字大屏展现全局安全态势，及时发现安全威胁



实时掌握业务系统的使用情况

- 访问次数最多的应用
- 访问次数最多的用户

实时发现异常访问情况

- 访问量突然飙升的应用（可能正在被攻击）
- 活跃度飙升的用户（可能账号被盗或者有意盗取公司机密）
- 访问地图显示异常的登录（可能遭受攻击或者账号盗取）

全局掌握公司的数字办公情况

- 当日活跃用户数
- 实时在线用户数
- 总访问流量
- 总激活用户数
- 总激活办公设备数

## 深云SDP的落地实践探索

**场景：**企业业务系统上云，方便分支机构（门店、营业厅、上下游合作伙伴）

访问业务支撑系统

**需求：**既要方便，又要安全

**解决方案：**深云SDP帮助上云的系统实现网络隐身，避免黑客攻击，同时又让

授权的用户可以很方便地访问系统

## 深云SDP

### 七层零信任安全架构





## 深云SDP的技术实践探索：网络隐身

1

私有DNS

隐藏域名

2

SPA敲门协议

隐藏端口

## 私有DNS：保护企业网络隐私，同时免遭DNS劫持威胁

通过私有DNS，可以在互联网上隐藏DNS信息，消除网络攻击风险，避免近年频发的大规模DNS劫持事件影响

### 深云私有DNS原理



### 近年来DNS劫持事件频发，急需DNS保护方案

著名以太坊钱包Myetherwallet在18年4月24日发生了一起事故，两个小时内，众多用户钱包被清空。调查发现原因并非自身安全问题，而是由于Amazon的DNS遭到劫持所导致。

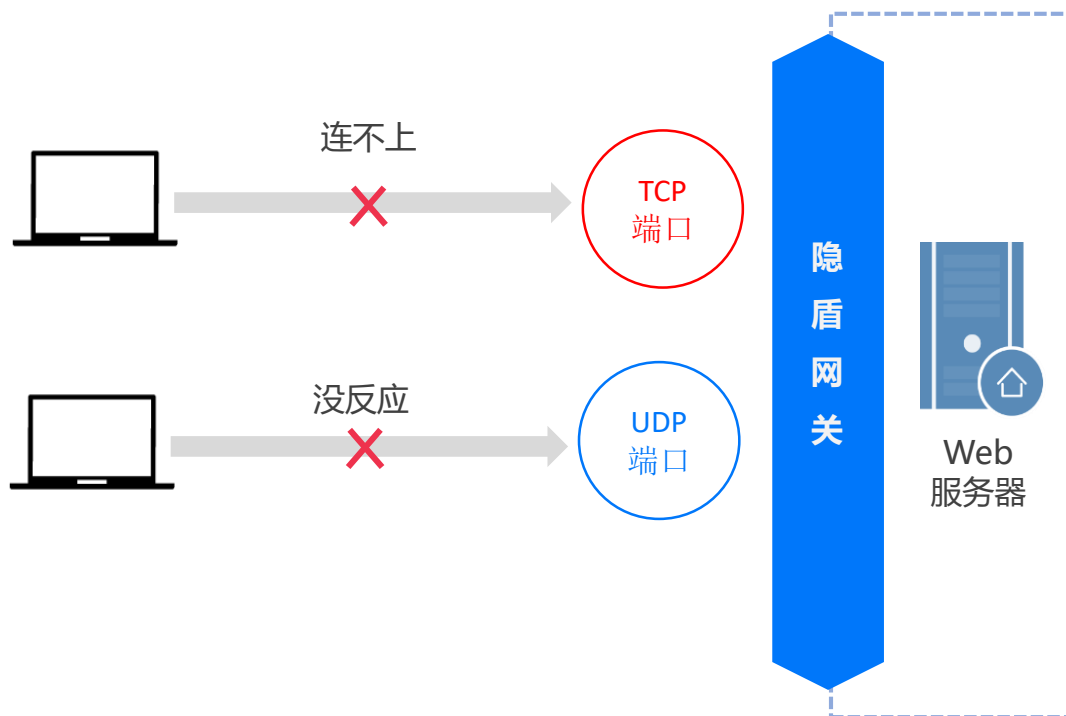


2019年1月，美国网络安全公司FireEye发现了一波DNS劫持活动，该活动已经影响到了中东、北非、欧洲和北美的政府、电信和互联网设备实体的数十个域名。在此期间，一个可疑的伊朗团体通过他们自己的恶意服务器重定向全球各地公司的流量，记录公司凭证以备将来的攻击。

## 深云隐盾网关：服务器的隐身防护罩

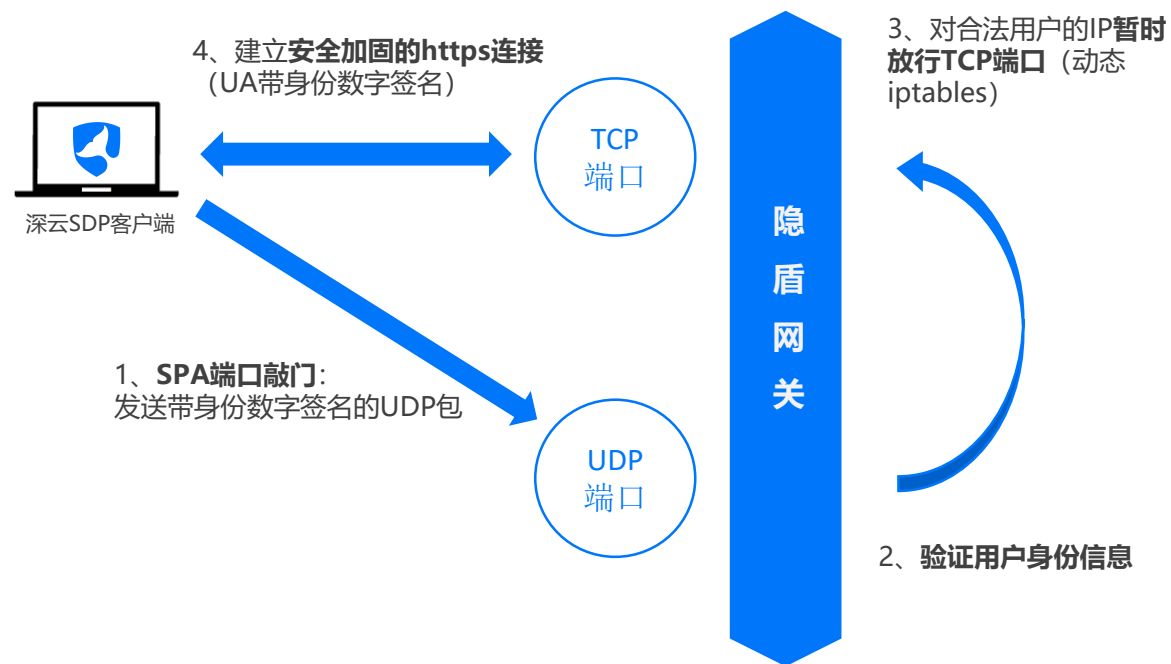
原理：“Deny all”与“Only you”

隐盾默认关闭所有TCP端口，拒绝一切TCP连接，  
让服务器从网络上“隐身”

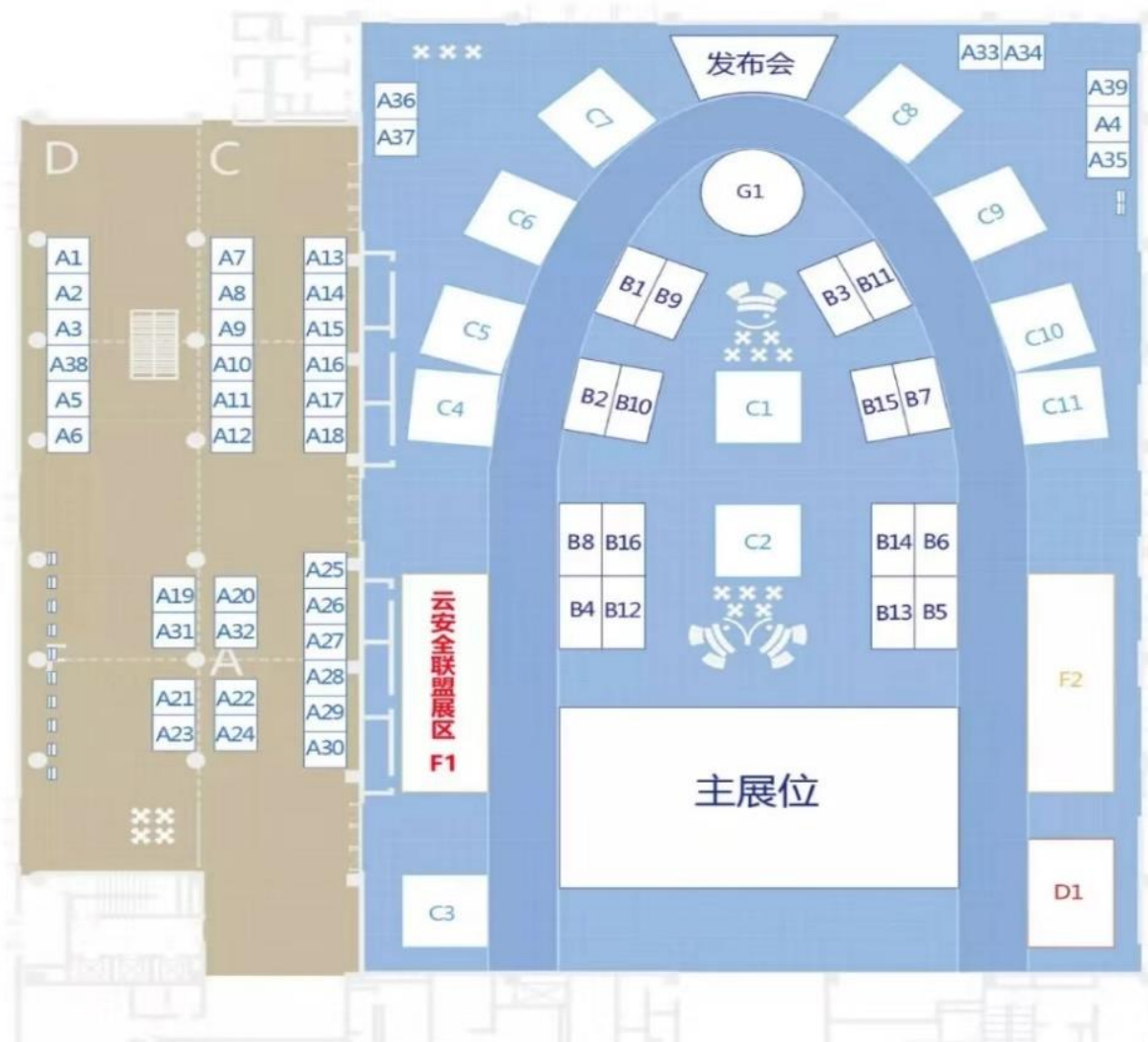


只有合法用户知道怎么连接

基于SPA敲门协议以及动态防火墙iptables的多层安全防护







关于SDP技术资料  
请到**F1**展台领取



# THANKS

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



[www.deepcloudsdp.com](http://www.deepcloudsdp.com)

软件定义边界 (SDP) 解决方案



400-069-0309