



中国移动
China Mobile

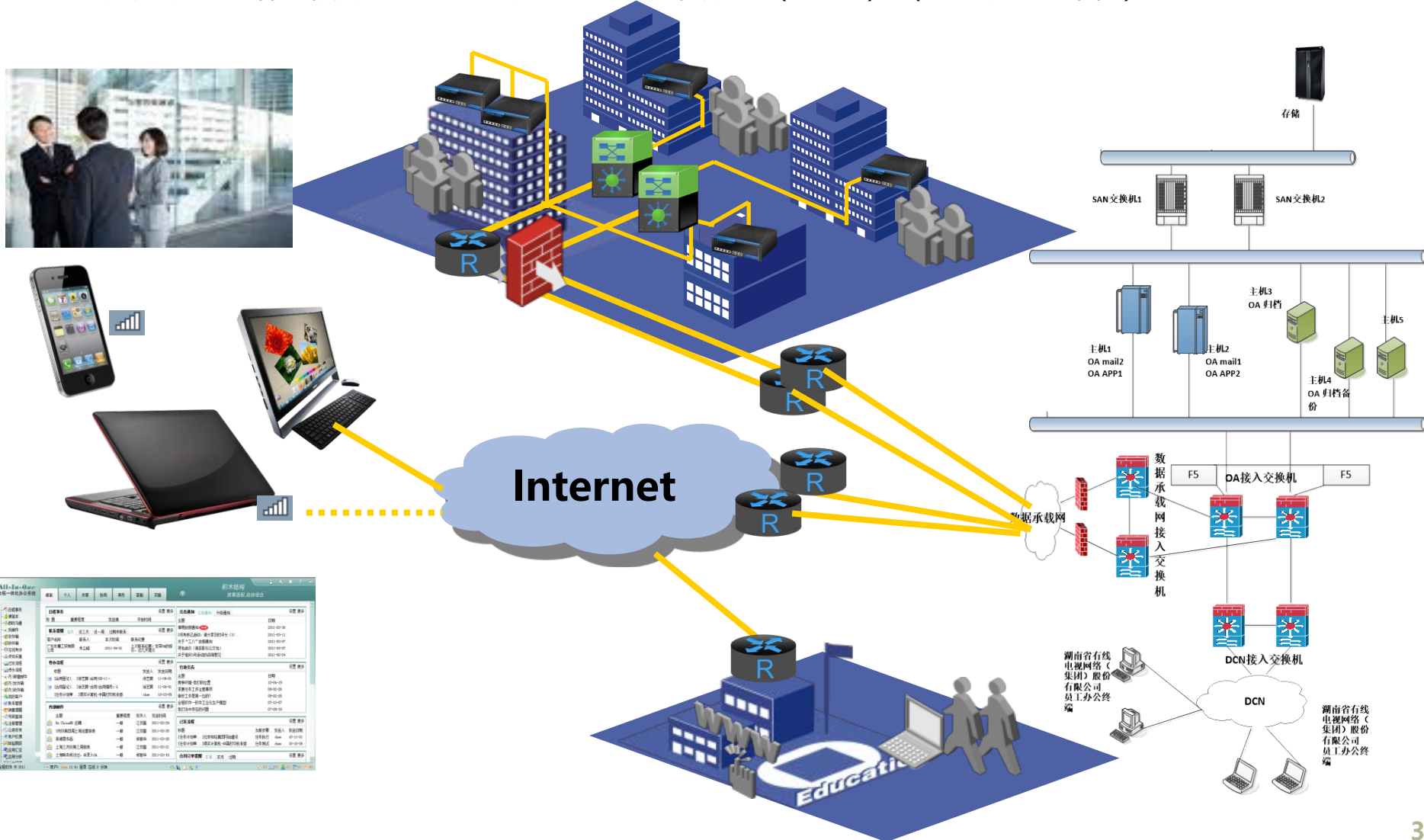
移动云SaaS产品介绍

www.10086.cn

1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

移动互联网时代，移动办公、分支互联对业务信息化提出安全要求

- 1、移动办公（SSL）：领导、出差员工移动办公的安全接入
- 2、分支机构网络互联实现协同办公或者共享系统和数据（IPSEC）（内部或者跨单位）



使用VPN（Virtual Private Network 虚拟专用网）技术来构建安全的业务网络

- VPN利用的是包括认证、加密、安全检测、权限分配、访问记录等一系列手段来构建安全的业务网络。
- 按照VPN的网络连接类型主要分为Site to Site 和End to Site两种类型。Site to Site 主要指的是网络和网络之间的VPN连接。而 End to Site 指的是移动终端到企业私有网络之间的VPN连接，而SSL VPN 就是 End to Site类型的VPN。
- 以OSI 模型参照标准，不同的VPN 技术可以在不同的OSI 协议层实现。

OSI层次		实现方式
应用层 Application	应用层 Application n	SSL
表示层 Presentation		
会话层 Session		
传输层Transport		
网络层Network		IPSec、GRE
数据链路层Data Link		PPTP&L2TP
物理层Physical Layer		专线

目前业界比较主流的是采用SSL和IPSec！

IPSec VPN

- IPSec（缩写IP Security）是保护IP协议安全通信的标准，它主要对IP协议分组进行加密和认证
- 常见产品：路由器或防火墙自带的VPN：主要是以一类传统的网络厂商为代表，如思科、Juniper、华为、迈普等。
- 试用场景：解决Site to Site（网对网）的安全问题，早期较流行的方式，多适用于分支互联。

SSL VPN

- SSL：安全套接字层（Secure Socket Layer，SSL）属于高层安全机制，广泛应用于Web 浏览程序和Web 服务器程序。在SSL中，身份认证是基于证书的。服务器方向客户方的认证是必须的，而SSL 版本3 中客户方向服务方的认证只是可选项，现在逐渐得到广泛的应用。试用场景：解决Site to Site（网对网）的安全问题，早期较流行的方式，多适用于分支互联。
- 试用场景：，SSL VPN的突出优势在于Web安全和移动接入，它可以提供远程的安全接入，而无需安装或设定客户端软件。多适用于移动办公及远程接入。

IPSec和SSL? 深信服提供SSL /IPSec 二合一VPN。

- IPSec VPN最初是为了解决Lan To Lan（网对网）的安全问题而制定的协议，因此在此基础上建立的远程接入方案在面临越来越多的End To Lan（点对网）应用情况下已经力不从心。。

IPSec VPN

- **客户端配置问题**：在每个远程接入的终端都需要安装相应的IPSec客户端，并且需要做复杂的配置。
- **IPSec VPN自身安全问题**：往往传统的IPSec 解决方案都没有很好的解决移动用户接入到私有网络的安全控制问题。
- **对网络的支持问题**：IPSec VPN对防火墙的安全策略的配置较为复杂（往往要开放一些非常用端口），因此客户端的网络适应性还是不能做到百分之百完美。
- **移动设备支持问题**：移动终端的种类将会越来越多，IPSec 客户端需要有更多的版本来适应这些终端。

SSL VPN

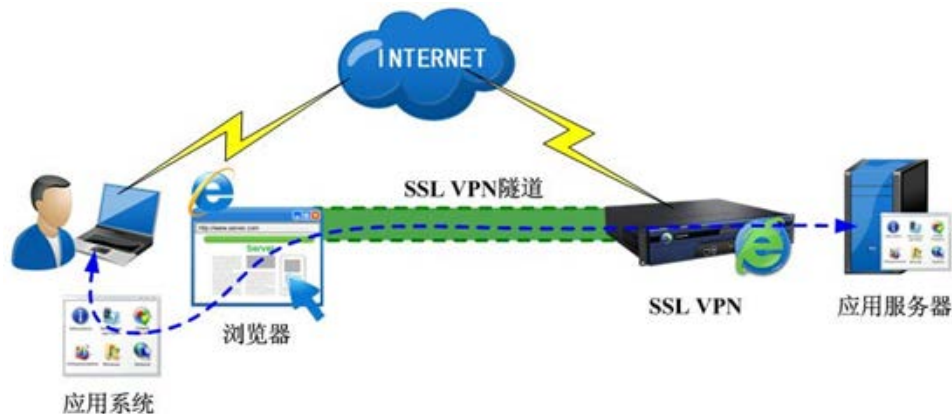
- **简单性**：不需要复杂配置，可以立即安装、立即生效。
- **无客户端**：不需要安装客户端，直接利用浏览器中内嵌的SSL协议就行。
- **兼容性好**：可以适用于任何的终端及操作系统。
- SSLVPN采用严谨的认证方式，高强度的加密模式，细致的权限分配和访问记录，实现对业务访问过程的全场护航，保证业务畅通无阻的同时规避网络安全风险。
- 两种技术目前应用在不同的领域，是可以进行互补的。SSL VPN考虑的是单点接入网络，是应用在点对网结构的接入模式；而IPSec VPN是在两个局域网之间通过Internet建立的安全连接，保护的是网对网之间的通信。。

深信服提供SSL /IPSec 二合一VPN！

若只针对移动办公的需求，基于SSL的方式更加便捷、安全。

1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

VPN 是在Internet 上临时建立的安全专用虚拟网络，类似在网络上建立一个“专用的隧道”



关键点

- 认证：“通道”对哪些人开放使用？
- 安全：“通道”中数据的安全性如何保障。
- 快捷：如何保障“通道”传输速度也不慢？
- 易用：如何实现良好的互操作性，监控管理、能否使用多种应用及操作系统？

- 深信服VPN利用的是包括认证、加密、安全检测、权限分配、访问记录等一系列手段来构建安全的业务网络。
- 良好的SSL VPN产品应该具有较好的互操作性，较为细致的访问控制能力，完善的日志和认证体系以及对应用的广泛支持。

深信服VPN解决方案

-安全、便捷、快速、易管理的远程接入



- 深信服SSL VPN采用严谨的认证方式，高强度的加密模式，细致的权限分配和访问记录，实现对业务访问过程的全场护航，保证业务畅通无阻的同时规避网络安全风险。

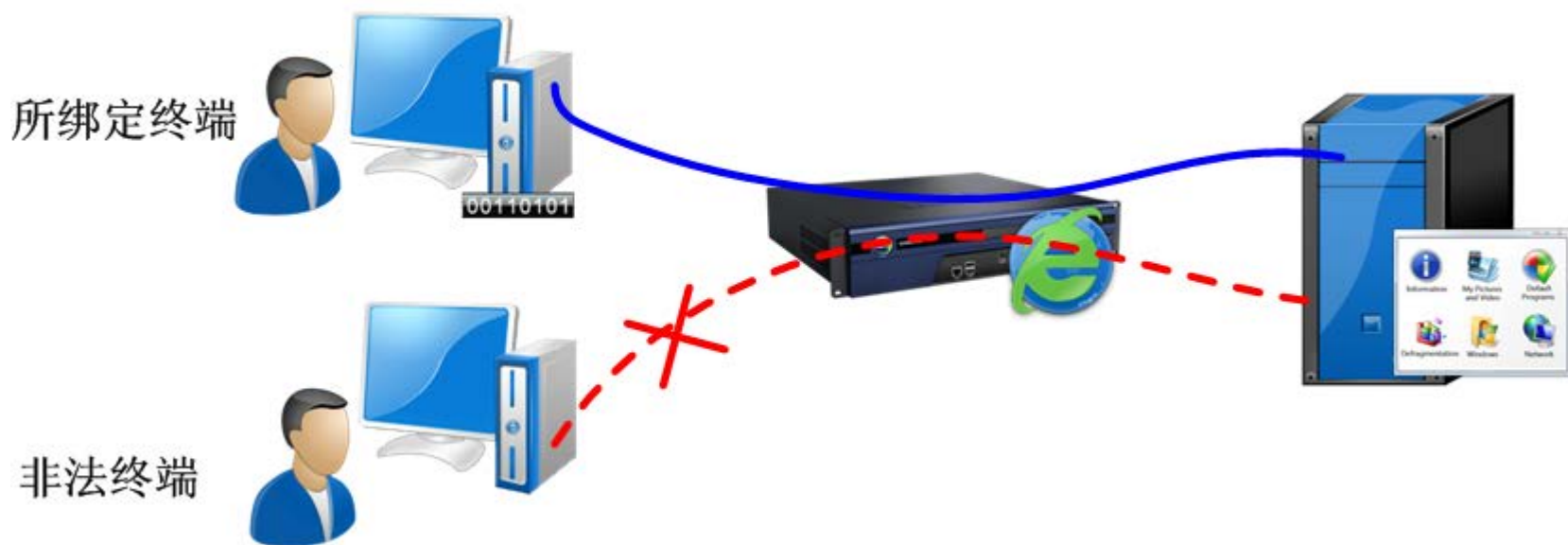


深信服VPN解决方案 -安全（身份安全）



- 传统的认证方式通过单一用户名密码认证，存在方式单一，易遭冒用，密码安全强度弱，隐患重重，受键盘监听器、爆破软件威胁等安全问题，威胁核心重要应用安全。
- 在SANGFOR SSL VPN安全网关支持LocalDB、LDAP/AD、Radius、第三方CA、自建CA、Dkey、短信认证（短信猫和短信网关）、硬件特征码、动态令牌多种安全认证方式，最大限度地保证了接入用户的合法性。
- 深信服创新性提出**混合认证**，针对上面提到的用户名和密码、CA数字证书、LDAP/AD、Radius、Dkey、硬件特征码、短信认证**可以进行五个因素以上的捆绑认证**，这几种认证方式必须同时满足才能够接入SSL VPN系统。

硬件特征码认证



- 绑定CPU、硬盘、网卡等硬件信息，防止非法终端接入。
- 支持用户的多硬件特征码绑定，支持自动审批，减轻管理员维护工作。

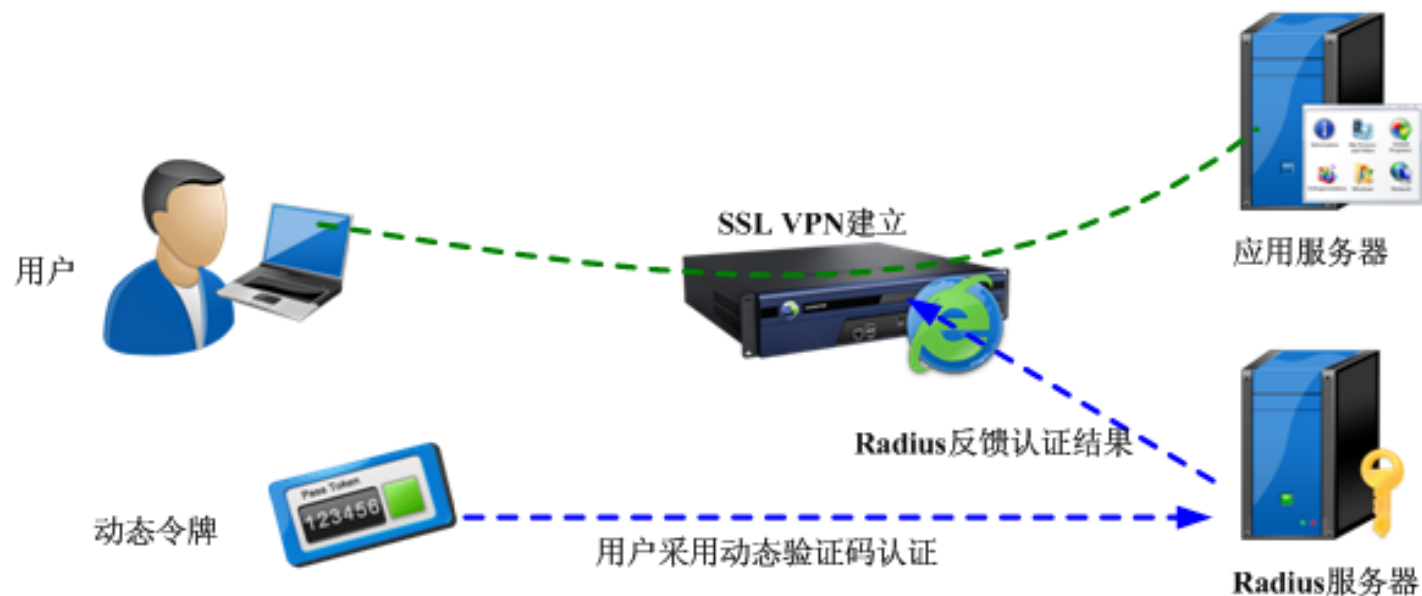
短信认证

- 支持短信猫
- 支持与运营商短信网关结合



动态令牌认证

- 一次性动态口令认证，杜绝密码爆破、盗窃，加强身份安全
- 支持基于时间、基于事件的动态令牌



CA认证

自建CA认证

- 设备内置CA中心，节省采购第三方CA的高昂成本
- 支持颁发设备证书、用户文件证书、用户KEY证书

与第三方CA结合

- 与原有CA进行无缝接合，支持各种证书格式
- 支持OCSP和自动更新CRL

与LDAP结合认证

- 以LDAP作为用户统一管理平台，提高管理效率
- 设备用户组结构与LDAP OU结构一致，方便管理
- 可结合LDAP实现短信认证、虚拟IP绑定、角色管理、权限分配



与Radius结合认证

- 与已有的Radius认证做结合，用户统一管理平台
- 可与SQL Server、My SQL、ORACAL、Access等用户管理数据库进行结合，读取用户认证信息、用户组分组、手机号码、虚拟IP等设置



密码安全保障

密码强度

- 多重密码安全策略
- 软键盘
- 图形校验码

密码防暴

- 基于用户名防暴破保护
- 基于IP的防暴破保护

本地密码认证设置

密码安全策略

☒ 启用密码安全策略 (注意: 密码策略只对本地密码认证的私有用户有效!)

☐ 密码不能包含用户名

密码认证选项设置

用户登录时校验选项

☒ 启用软键盘 (防止木马记录键盘输入信息)

☐ 字母键随机变化

☐ 数字键随机变化

☒ 启用图形校验码 (防止暴力破解登录密码)

防止暴力破解选项

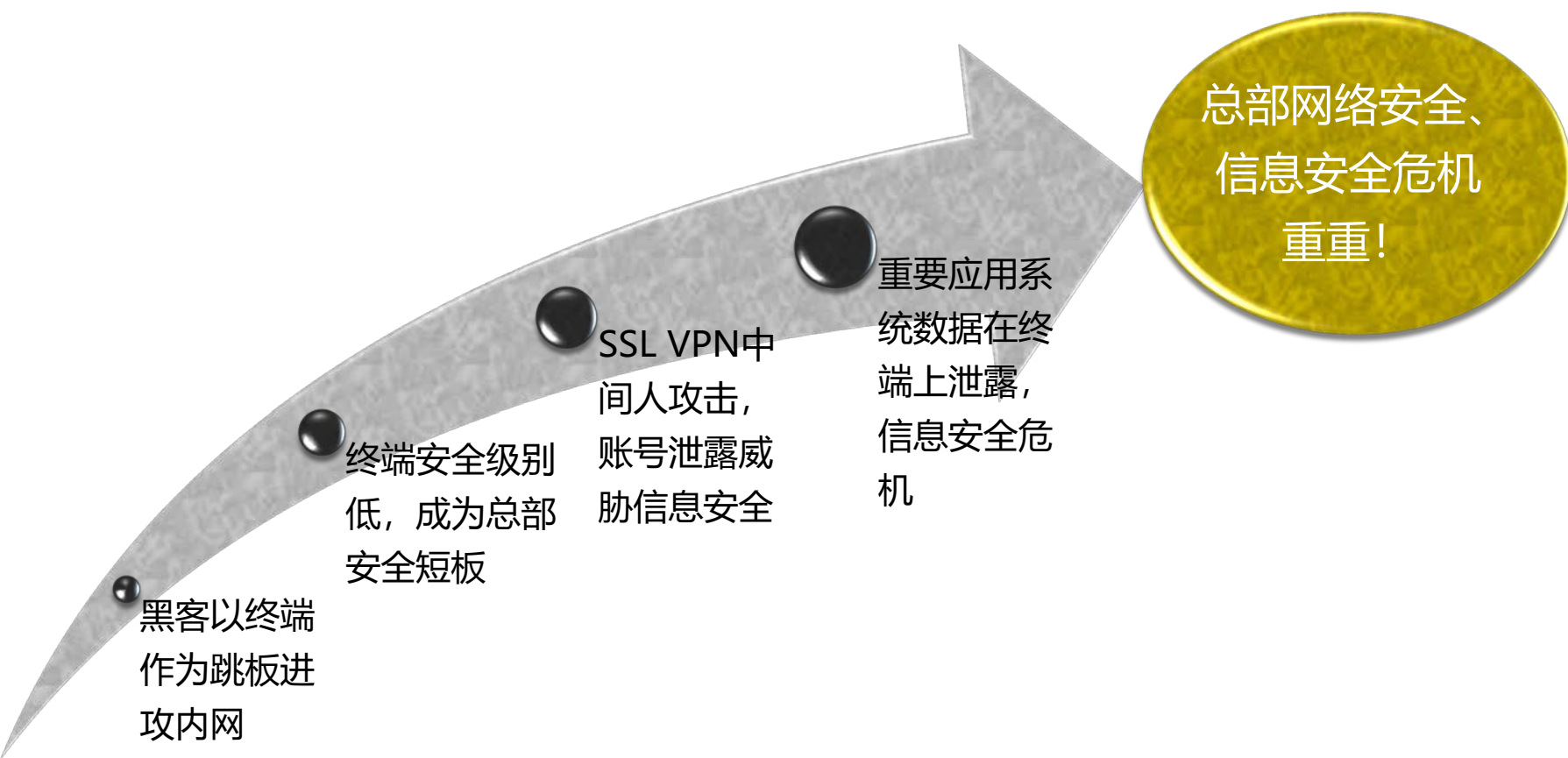
同名用户登录连续出错 (1-32)次后锁定用户 (30-1800)秒后恢复正常状态

同IP用户登录连续出错 (64-2048)次后

☐ 启用图形校验码认证

☒ 暂时拒绝同IP登录

并在 (30-1800)秒后恢复正常状态



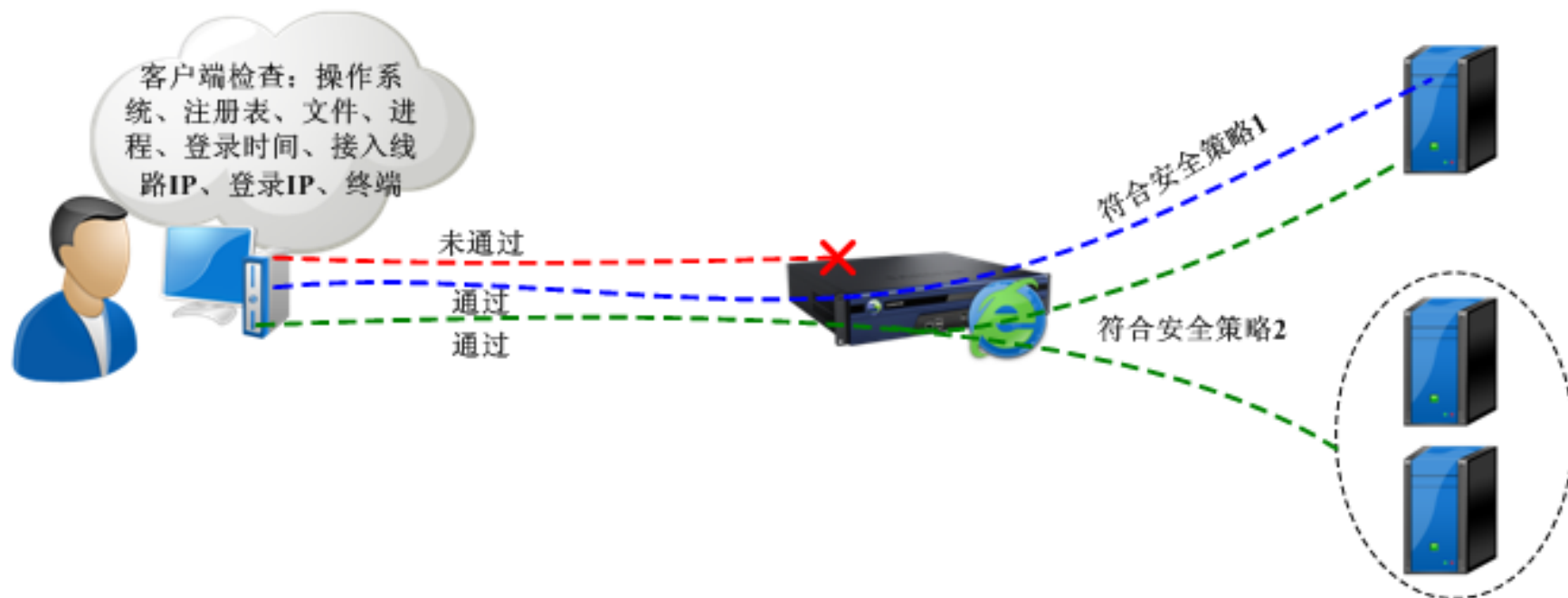
沙盒技术

- 启用安全桌面对重要的应用进行保护，防止数据在终端上遭泄露
- 安全桌面内，用户无法通过本地保存、外设拷贝打印、局域网传输、互联网通信等方式将受保护应用数据外泄
- 用户退出SSL VPN之后，安全桌面
- 内所有应用数据将被销毁



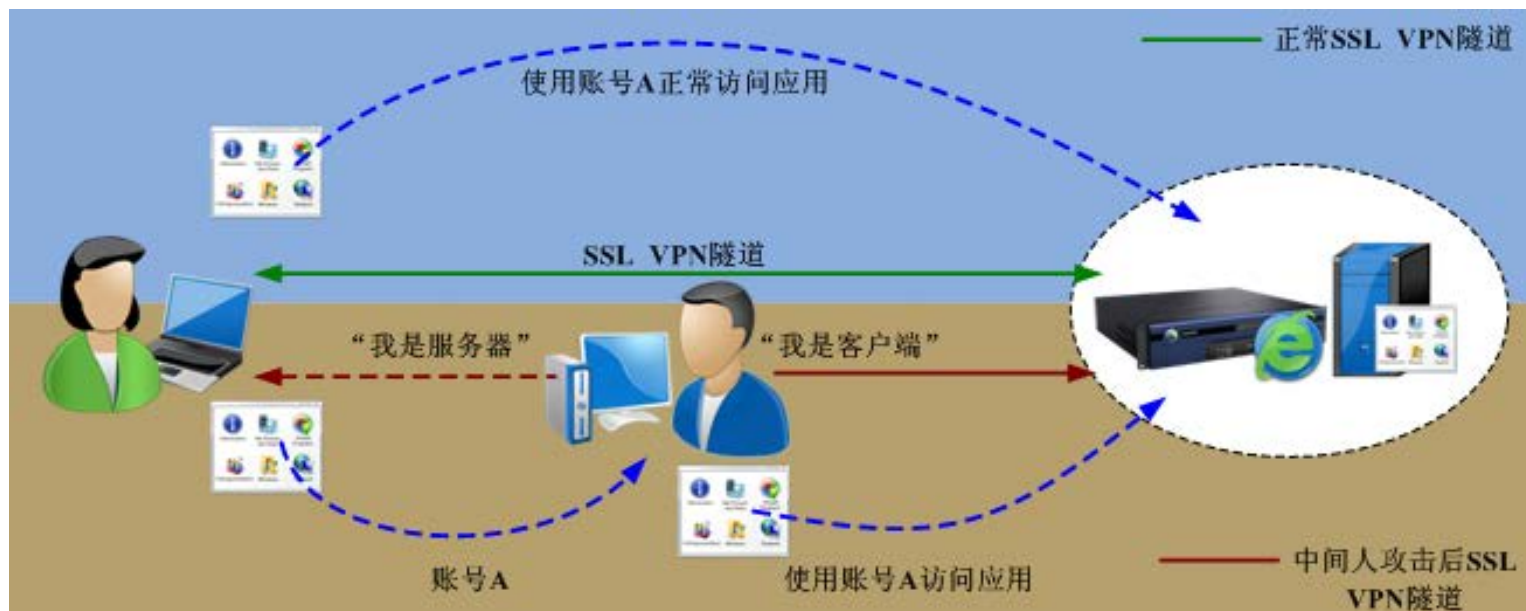
客户端安全检查

- 基于角色实现客户端准入、授权
- 可检查：操作系统及版本、注册表、文件、



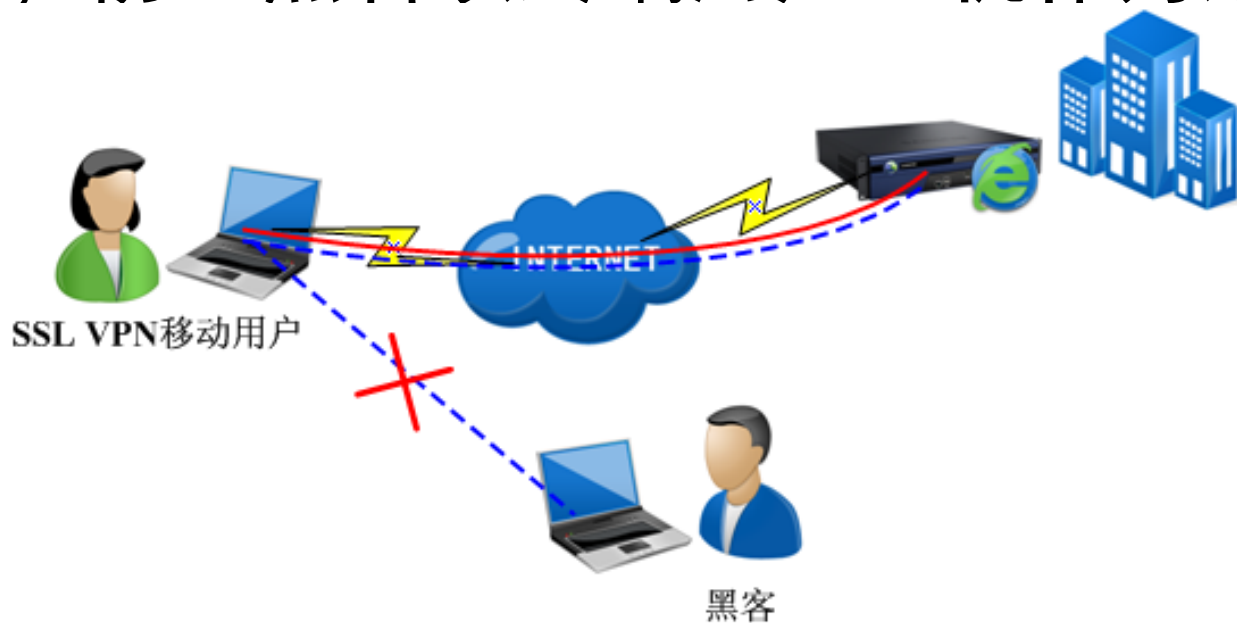
防中间人攻击

- 针对劫持会话伪造证书、SSLStrip等中间人攻击进行检测
- 对客户端进行告警，防止信息泄露



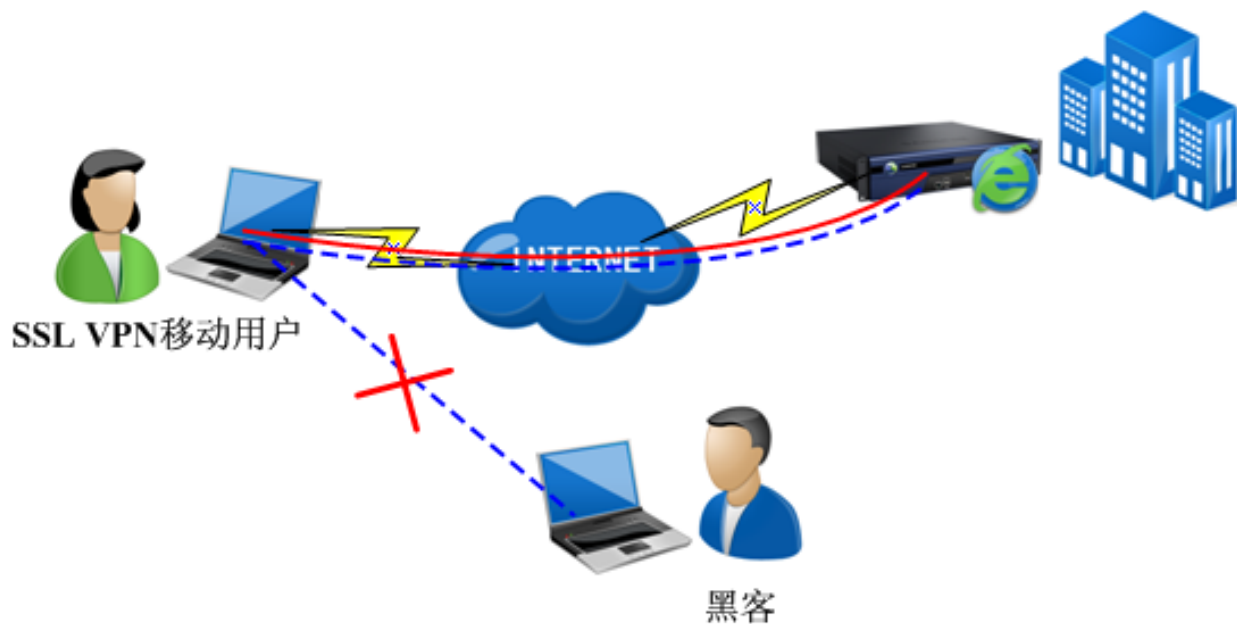
VPN虚拟专线

■ 用户接入SSL VPN后自动断开其余所有互联网链接，防止黑客以终端用户主机作为进攻内网



VPN虚拟专线

■ 用户接入SSL VPN后自动断开其余所有互联网链接，防止黑客以终端用户主机作为进攻内网的跳板



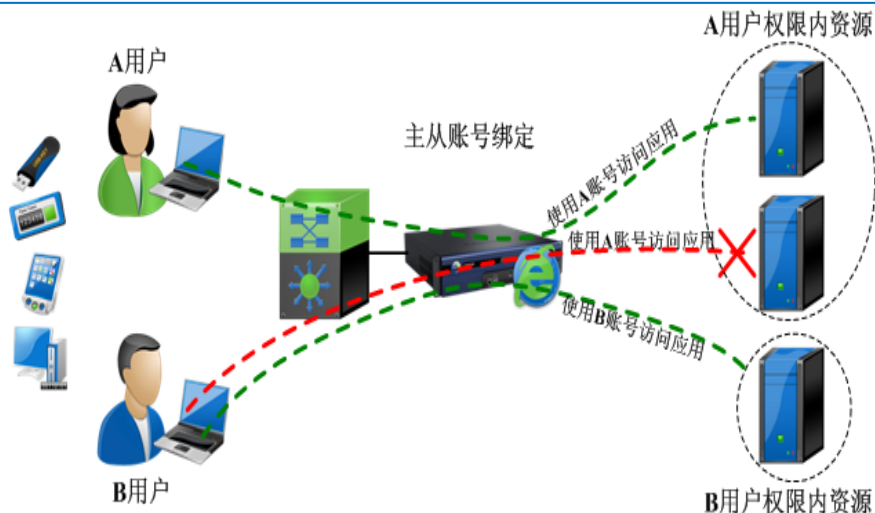
- 标准SSL协议，安全性保障
- 支持多种国际标准加密算法及摘要算法，如AES、3DES、DES、RSA、DH、RC4、SHA-1、MD5
- 可扩展国密加密算法SCB2



- 角色细粒度授权，URL级别授权
- 主从账号绑定
- 服务器地址伪装、资源隐藏
- 基于客户端安全级别的授权

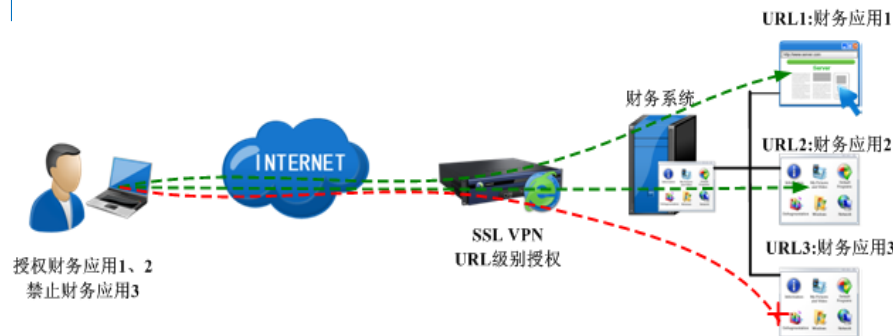
主从账号绑定

- SSL VPN登录账号与应用账号对应绑定
- 防止越权访问行为，加强应用系统安全



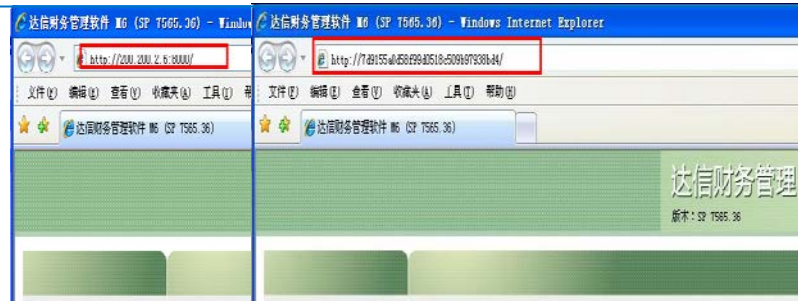
URL级别授权

- 基于角色对用户组/用户进行应用授权
- 针对B/S资源，支持URL级别授权，细致到应用、页面



URL级别授权

- B/S应用服务器地址伪装
- TCP应用、L3VPN应用IP地址隐藏
- 资源完全隐藏

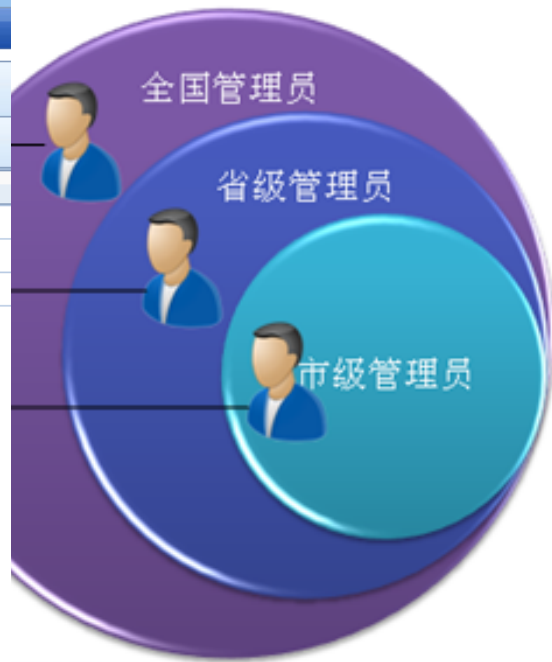
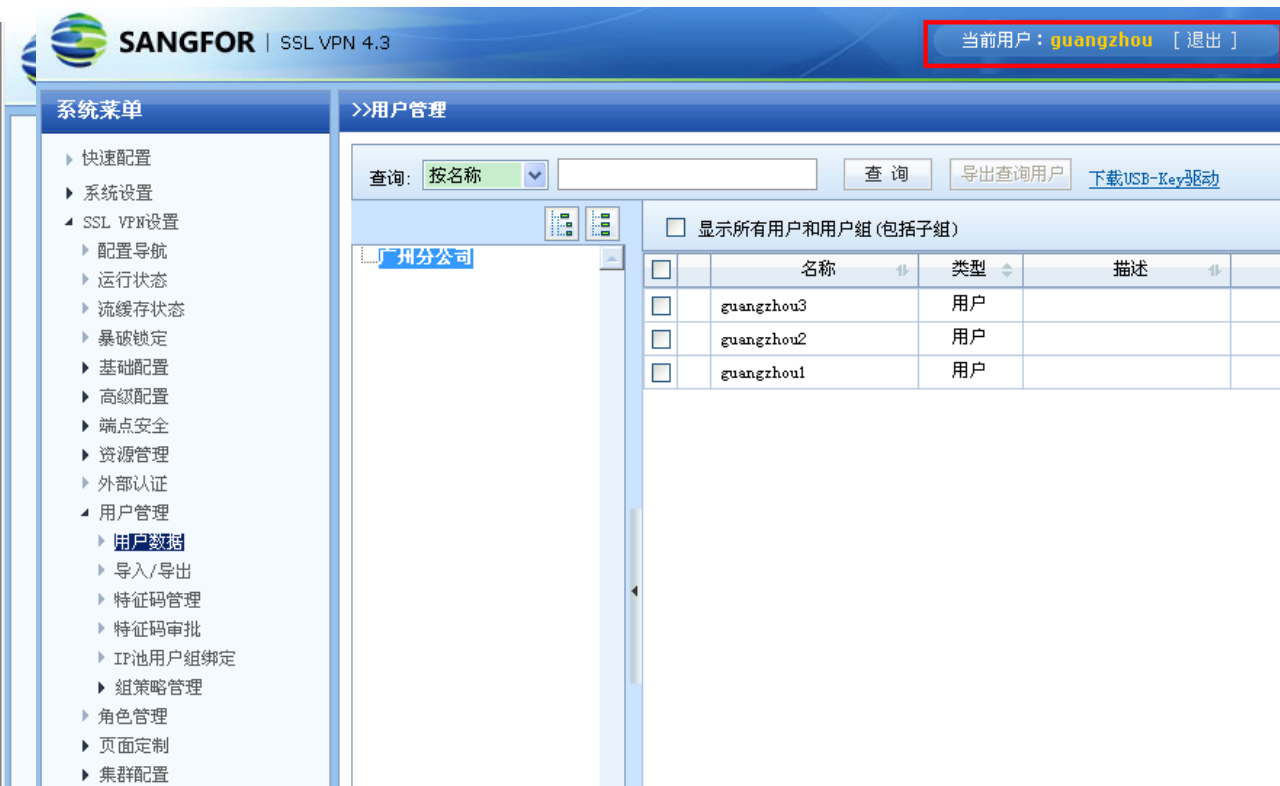


- 管理员16级分级分权限管理，保证管理安全
- 设备内置管理日志、服务日志
- 独立日志中心提供用户、管理、系统、告警等详尽日志及报表



管理员16级分级分权限管理

- 16级树形管理员分级分权限管理，支持权限继承
- 配置模块、用户、角色、资源权限的划分
- 配置和查看权限划分



独立日志中心

- 实时同步，海量日志存储，不影响网关性能
- 支持Syslog、SNMP
- 管理员权限与控制台同步，防止日志滥用



零痕迹访问

- SANGFOR SSL VPN在用户结束访问以后，拔出DKEY后将自动注销，同时会自动清除Cookie，临时文件等遗留在客户端计算机上的信息，实现“零痕迹”访问，避免安全隐患。

图形码验证

- SANGFOR SSL VPN安全网关提供图形码校验功能

软键盘功能

- SANGFOR SSL VPN安全网关提供了软键盘功能，用户在输入密码的时候可以使用界面上提供的软键盘，这样木马程序就无法采用截获用户键盘输入的方法来窃取密码了。

会话超时控制功能

- SANGFOR SSL VPN安全网关特别加入了不活动检测引擎，当检测到客户端在指定时间内没有任何访问内网资源的流量时，SSL VPN网关将自动弹出对话框，提示用户“SSL连接会在X秒内超时关闭，继续还是注销？”若用户在该时间内仍未选择相应动作，则SANGFOR SSL VPN安全网关将自动注销，中断会话并重新返回登录界面。

关键文件保护

- 保护应用系统关键文件，防止恶意修改，保障系统安全

集成企业级状态防火墙

- SANGFOR SSL VPN安全网关集成了企业级的状态检测防火墙。拥有企业级防火墙所具备的基本功能如：管理员权限分级、URL过滤、NAT功能、访问监控、上网控制、用户认证、流量控制、QOS、DHCP服务、自动拨号等。

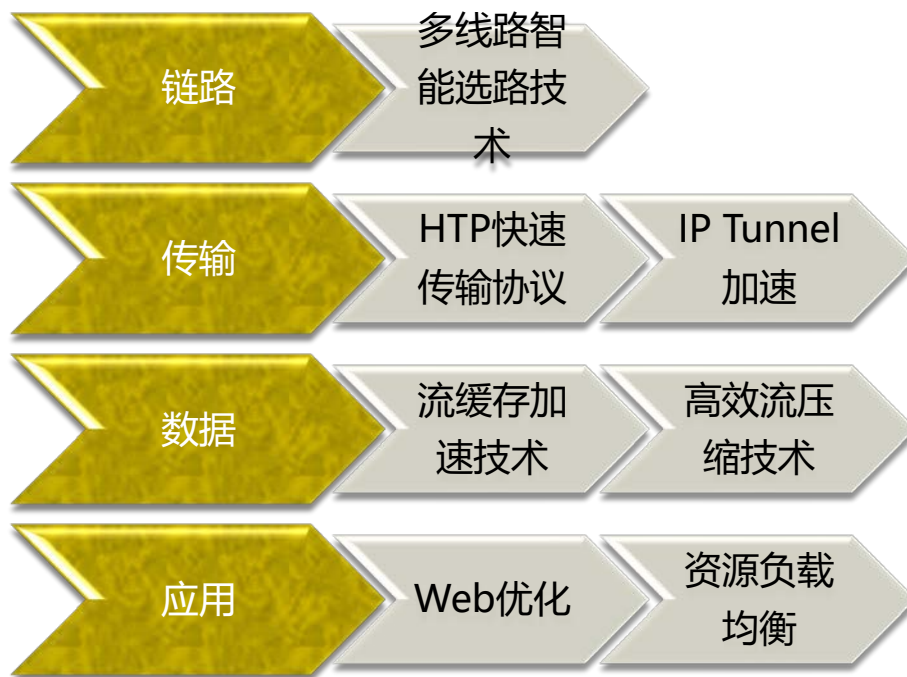


影响速度的因素

- 跨运营商访问速度瓶颈
- 跨国、偏远地区访问等造成高丢包、高延时、质量低下
- 数据本身冗余度高，多次重复读取相同或细微改动数据，冗余量大
- PDA、智能手机等终端采用GSM、CDMA、EDGE、3G接入速度慢
- 分担同一应用的多台服务器负载分配不均，高负载服务器用户速度慢

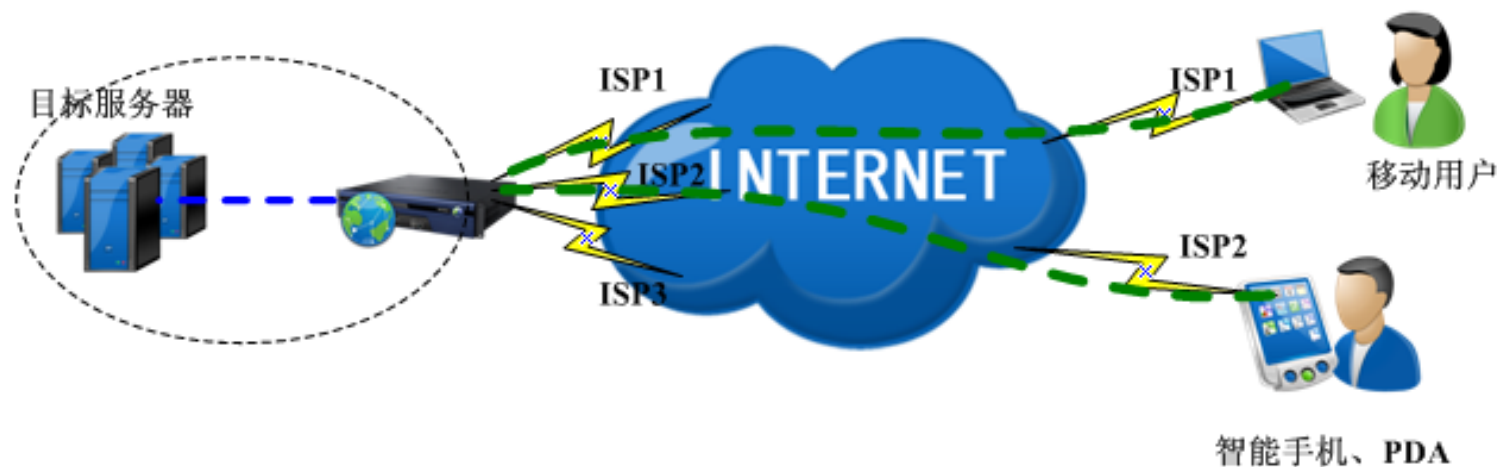
更快的SSL VPN提升业务办公效率

- SSLVPN实现了便捷而又安全的办公同时，也受到了互联网的环境制约，办公效率会被互联网的链路质量所影响。
- 为了帮助客户更好利用互联网技术提升业务效率，深信服致力于开发最快的业务访问模式，利用多种广域网加速技术，提升系统的响应速度。



多线路智能选路

- 通过速度实时探测，选择响应最快的线路接入，避免跨运营商访问
- 支持多线路备份，登录SSL VPN后实时探测总部线路效果，若当前线路不稳定，立即将用户切换到另一条较稳定度的线路上，保证用户SSL VPN畅顺使用



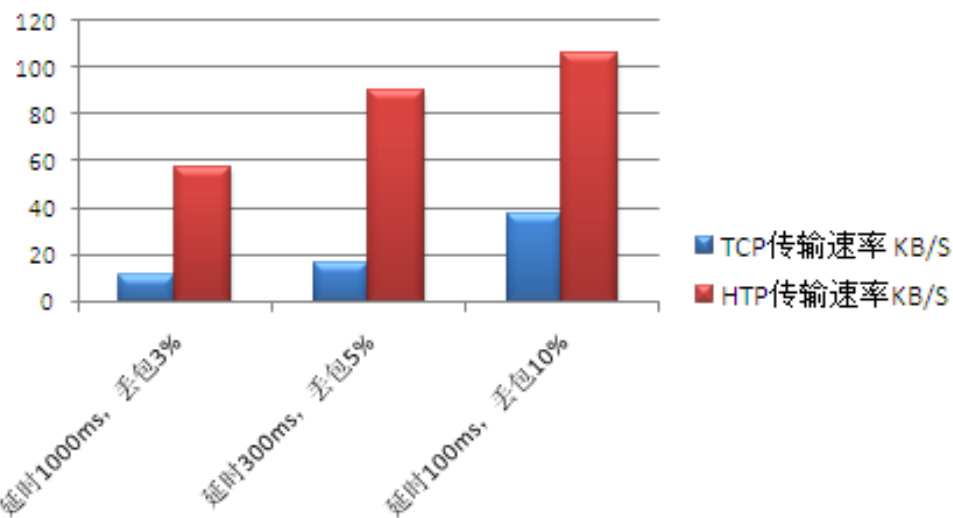
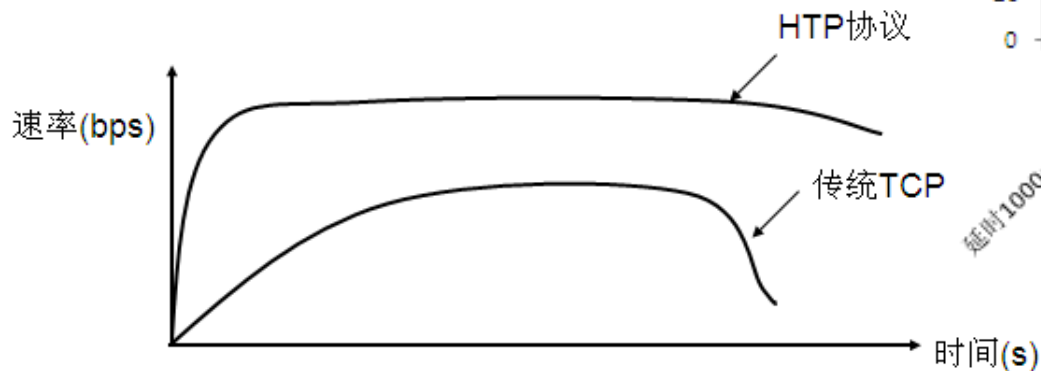
HTP快速传输协议

■ 解决网络高丢包、高延时造成的应用访问速度缓慢的问题

■ 优化传统TCP传输，恶劣网络环境下大幅加速

- ◆ 基于UDP的可靠传输
- ◆ 快速重传
- ◆ 选择性重传
- ◆ 拥塞机制优化

■ -滑动窗口优化



流缓存加速

■ 基于码流特征，进行数据包分片、数据更新校验、标签、缓存及数据重组，保证数据更新实时性的同时大幅削减传输数据量，提高速度

■ 实际测试表明，流缓存加速最高可削减80%的流量，速度大跨越

■ 可在客户端、控制台查看流缓存效果



高效流压缩

- 采用LZO、GZIP高效流压缩算法，削减冗余数据量
- 全面优化各种B/S、C/S应用
- 动态压缩策略，采用最佳压缩策略，获取系统负载与压缩比之间最佳平衡



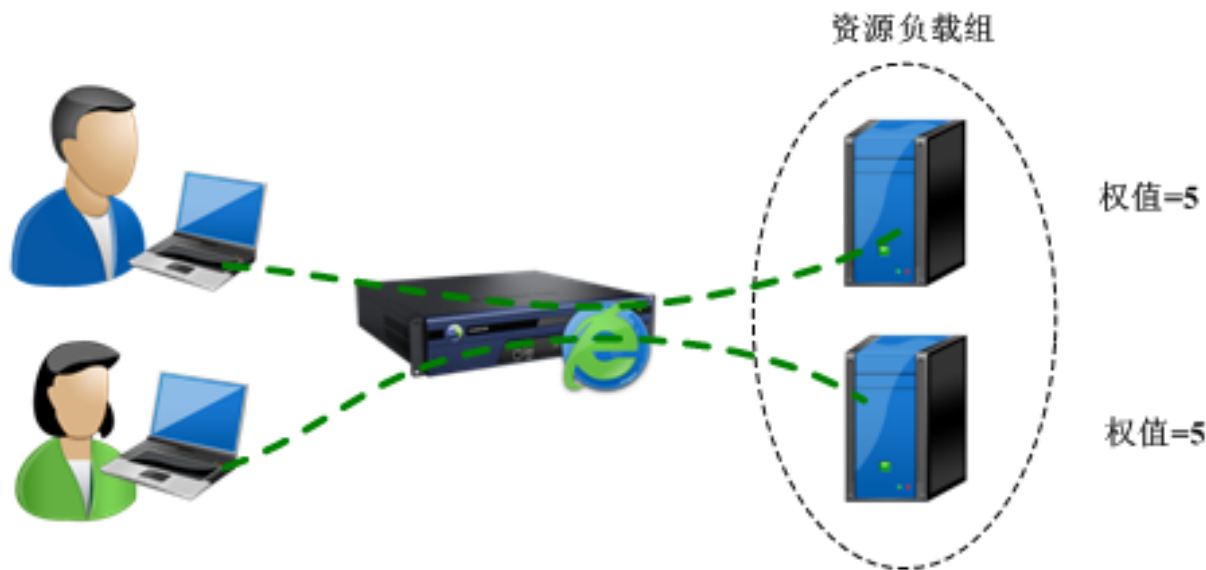
WEB优化

- 通过图片过滤、缩小、模糊化策略实现对于图片的优化处理，提高不同WEB资源、不同网络环境用户访问WEB资源的体验
- 传输数据量削减，应用访问加速



资源负载均衡

- 一个应用由多台服务器承载，需要动态负载接入服务器
- 根据预设的权限值动态的将用户连接分配 服务器上
- 提升用户访问体验，提高服务器利用率



深信服VPN解决方案 -易用



管理员

- 零客户端、零配置，管理维护量小
- 页面定制便利，打造专属应用平台
- 智能递推，防止资源漏访
- 用户组16级分级管理

用户

- 完整支持Windows、Linux、MAC OS等主流操作系统，完整支持IE、Firefox、Opera、Safari、Chrome等浏览器
- 远程应用发布
- 虚拟门户
- B/S、C/S应用单点登录
- 文件共享Web化



完整的支持

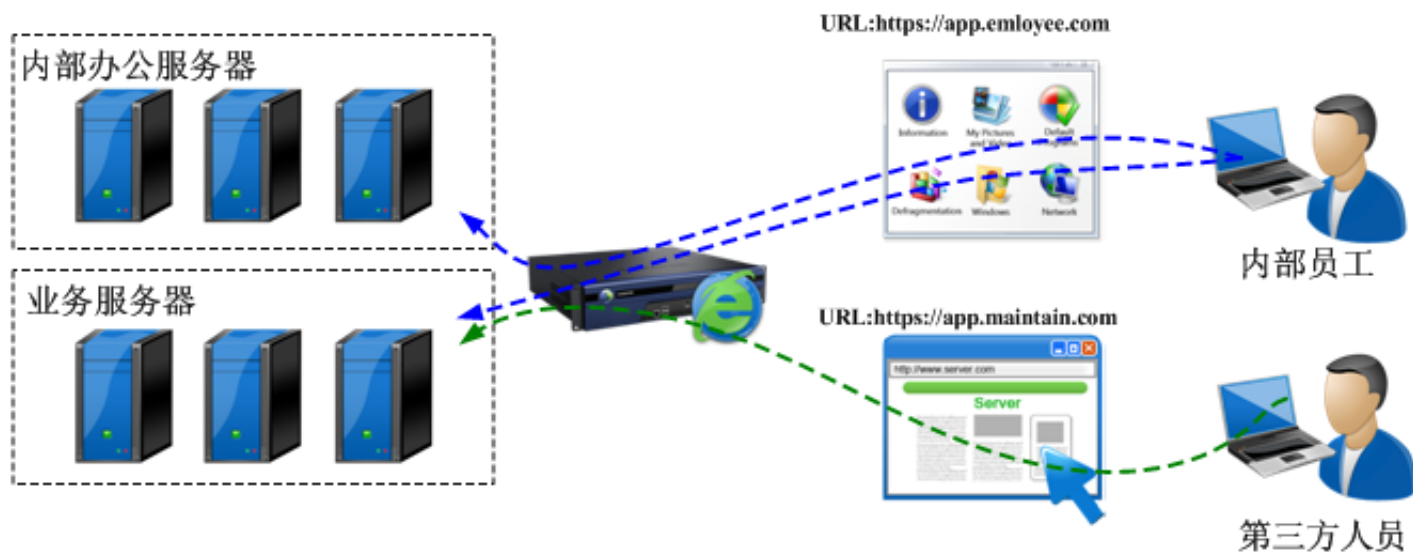
- 完整支持Windows、LINUX、MAC OS等主流操作系统
- 完整支持IE、Firefox、Opera、Safari、Chrome等主流浏览器



Safari

虚拟门户

- 不同部门、不同运用平台采用不同的Portal
- 各Portal可拥有独立的地址、界面、应用资源、管理员



远程应用发布

- 用户终端发布应用窗口，使用体验相同
- 用户终端无需安装客户端，可正常使用C/S应用
- 网络中仅传输鼠标、键盘、显示数据



WEB文件共享

- Web应用方式发布文件共享
- 避免传统网上邻居CIFS协议小包频繁交互，提高使用速度
- 可结合域进行权限控制，可进行文件夹访问权限控制



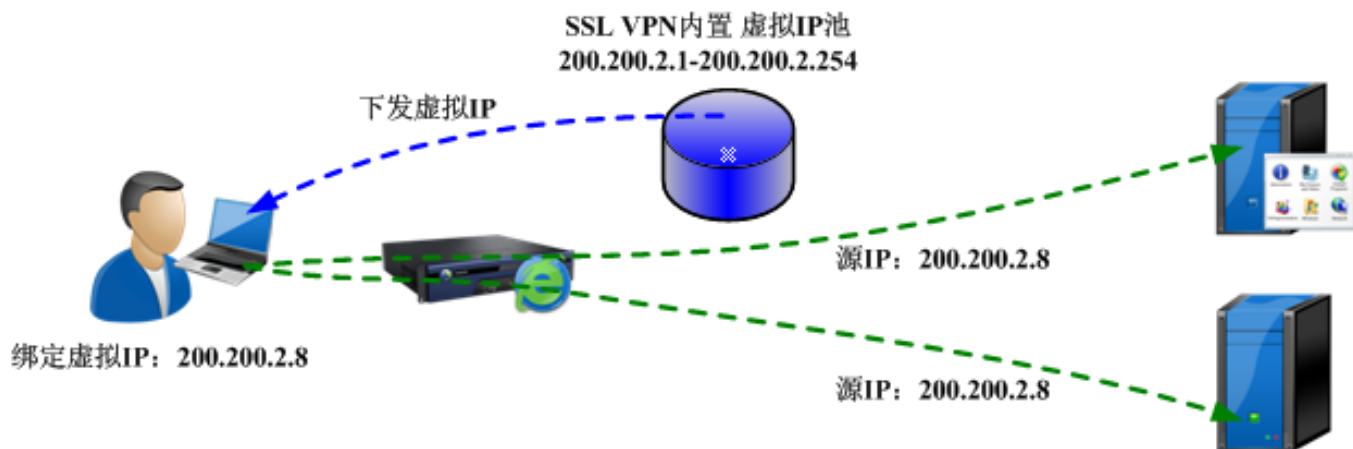
单点登录 (SSO)

- 登录SSL VPN后，可直接点击应用直接访问，无需再次认证，提供工作效率
- 支持B/S、C/S应用单点登录
- 支持FROM、NTLM、BASIC方式单点登录



虚拟IP绑定

- 可自定义设置多虚拟IP池
- 支持用户组虚拟IP池绑定、用户虚拟IP绑定
- L3VPN应用支持路由模式、SNAT模式、反向连接
- Web应用、TCP应用支持虚拟IP绑定



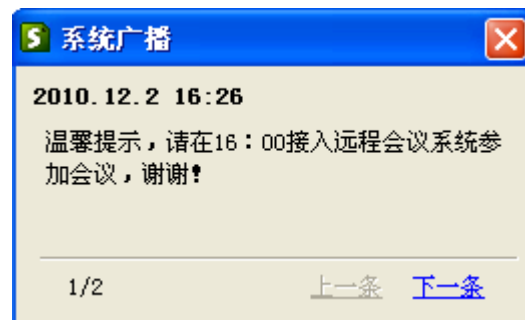
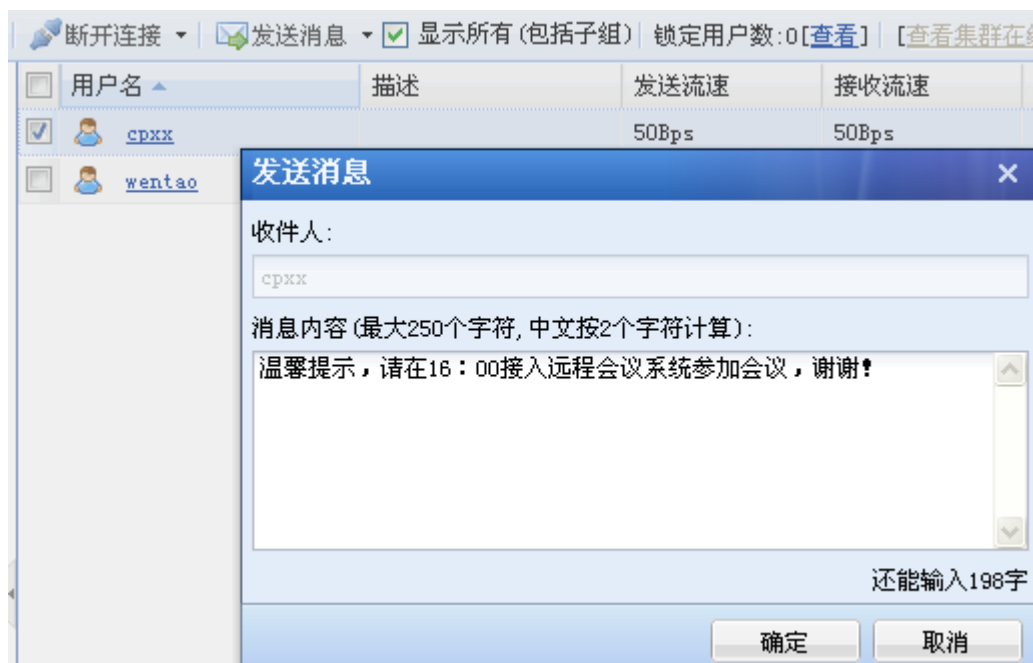
自定义页面

- 处于管理的需要，需要保持跟公司原有风格的一致
- 支持3套模板选择
- 支持自定义LOGO、公告、页面标题
- 支持页面完全自定义



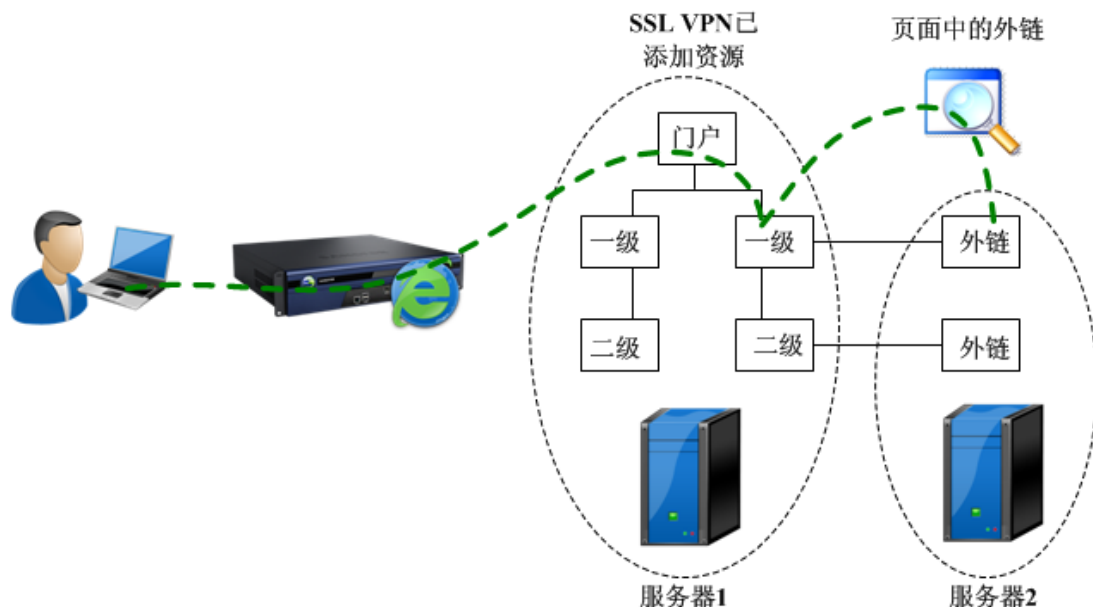
即时消息

- 可查看在线用户流速、流量、IP、接入时间、并发会话等接入状况
- 可向指定用户、所有用户发送即时广播



智能递推

- 内部应用门户上含多级链接，添加资源时易漏导致用户资源漏访
- 多级链接中含变化IP链接，一旦IP变化需重新添加资源，维护量大
- 自动探测页面上未添加为资源的链接，根据IP+端口、域名自动将其添加为资源，防止资源漏访



便捷使用

- 点击资源可直接启动所关联的C/S客户端
- 系统托盘，防止页面误关操作导致的SSL VPN连接中断
- 开机自动登录SSL VPN、桌面快捷方式启动SSL VPN



SJJ1007远程安全办公系统

资源组列表资源

默认资源组

管理组

秘书组

行政组

财务组

销售组

技术组

地址:



内部论坛

[192.200.40.143]:[80 - 80]

内部BBS论坛



财务系统

[192.200.40.143]:[80 - 80]

公司财务管理系统



Remote desktop

[10.0.0.2]:[3389 - 3389]

远程桌面管理



windows messenger

[10.0.0.2]:[1863 - 1863]

内部MSN通信



客户关系管理系统

[192.200.40.143]:[80 - 80]

客服客户关系管理系统



邮件系统

[192.200.40.143]:[80 - 80]

内部办公邮件系统



LotusNote

[10.0.0.2]:[1352 - 1352]

IBM办公系统



RTX

[10.0.0.1]:[8000 - 8000]

企业腾讯通系统

资源图标方式

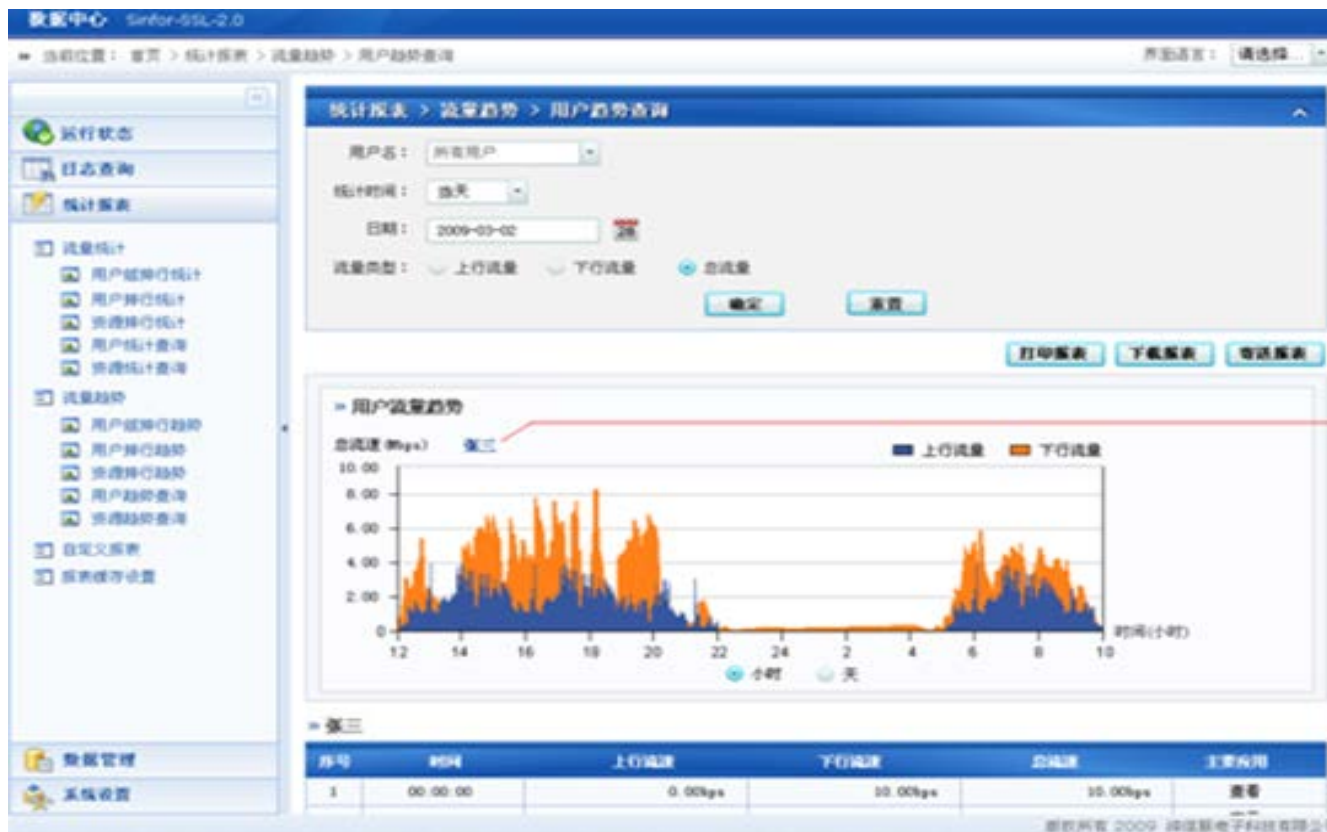
系统托盘

深信服VPN解决方案 - 管理性



强大的实时监控能力

通过远程监控平台，管理员可以实时地监控用户的接入情况，实时观察SSL VPN安全网关的运行情况。通过SSL VPN丰富的系统日志，可以及时定位故障，并实施远程维护。通过Web界面，管理员还可以随时查看每个在线用户的情况，可以随时中断可疑会话，方便快捷。还可以实现告警的短信通知，及时通知到终端用户。



丰富的日志信息

- SANGFOR SSL VPN通过独立的第三方日志服务器，用户可以按照系统日志和用户日志两大类日志进行查询。
- 管理员可对指定时间范围内的日志以及日志的级别如：错误、告警、信息、调试和进程类型进行查询。
- 管理员可按照饼图、柱状图、曲线图等多种显示方式对服务的被访问次数、被拒绝次数，用户的登录次数、告警次数等进行直观显示，并可直接打印和导出。S



提供最细致的权限管理

SANGFOR SSL VPN内置有多种用户和资源管理方式，可以自建用户，也可以从第三方导入，支持LDAP/AD、RADIUS等第三方认证，可以根据用户、用户组、公用账号、私有账号等多种方式对用户进行管理。管理员可根据角色、Web资源、C/S资源、IP资源等权限划分方式，为远程接入用户分配细致的访问权限控制用户组认证方式、属性配置继承，管理方便。



1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

深信服统一安全接入平台

新的时代，应运而生

业界最快、最安全、最好用的
VPN远程接入解决方案



移动信息化时代
创新加入多种智能终端接入方式

1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

全面的安全特性

多维度保障单位数据安全

身份安全

支持多达8种认证方式，支持认证方式的灵活组合
多重密码安全保障

终端安全

防中间人攻击
客户端安全检查
SSL专线
客户端零痕迹

传输安全

标准加密算法

应用权限安全

角色授权、URL级别授权
主从账号绑定
服务器地址伪装、应用隐藏

审计安全

独立日志中心
日志中心管理员权限分级



安全特性技术优势



身份认证

主从账号绑定

国际加密算法



快速特性

逐层级保障用户畅快接入



链路

- 多线路智能选路

传输

- HTTP高速传输协议

数据

- 流缓存加速技术
- 流压缩加速技术

应用

- Web优化
- 资源负载均衡

快速特性技术优势



单边加速

不用单独做任何配置

用户使用速度提升30%



多线路智能选路

选择最快的运营商线路接入

为用户提供最快的接入速度



流缓存

削减65%-95%冗余数据

提升网络传输效率

稳定特性

保障业务连续运行不中断

设备自身稳定性

支持多达253台服务器做非对称集群
保证设备自身的稳定
扩容规模 随心所欲



业务系统稳定性

支持对设备发布的业务进行资源负载均衡
为用户保证业务连续性
发挥服务器集群最大性能

卓越的易用特性

关注最终用户使用感知

全面支持主流操作系统
包括Win10、Win8、
Win7的32/64位系统
MAC最新版本
Linux最新版本

全面支持主流浏览器
包括IE6-11、
非IE内核如Safari、
chrome、firefox

全面支持主流移动智能终
端接入，包括最新的
Iphone、Ipad及各类
Android手机、平板。

完整支持
解决用户接入难题

虚拟门户
带给用户专属感知

不同部门的用户登录
地址不同、界面不同

断线重连
适应移动网络状态

短暂性断网后自动恢
复
免除手动重连的麻烦

优秀的易管理特性

减少管理员运维管理压力

用户分组管理

16级用户组织架构
根据组织架构分配权限

管理员权限分级

不同部门分级管理
运维工作方式灵活、压力分散



用户流量管理

接入用户带宽分配
为用户提供更佳体验

独立日志中心

保留管理员/用户访问日志
为管理员提供溯源依据

1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

统一业务安全接入平台



PC端安全接入
SSL VPN/Easyconnect

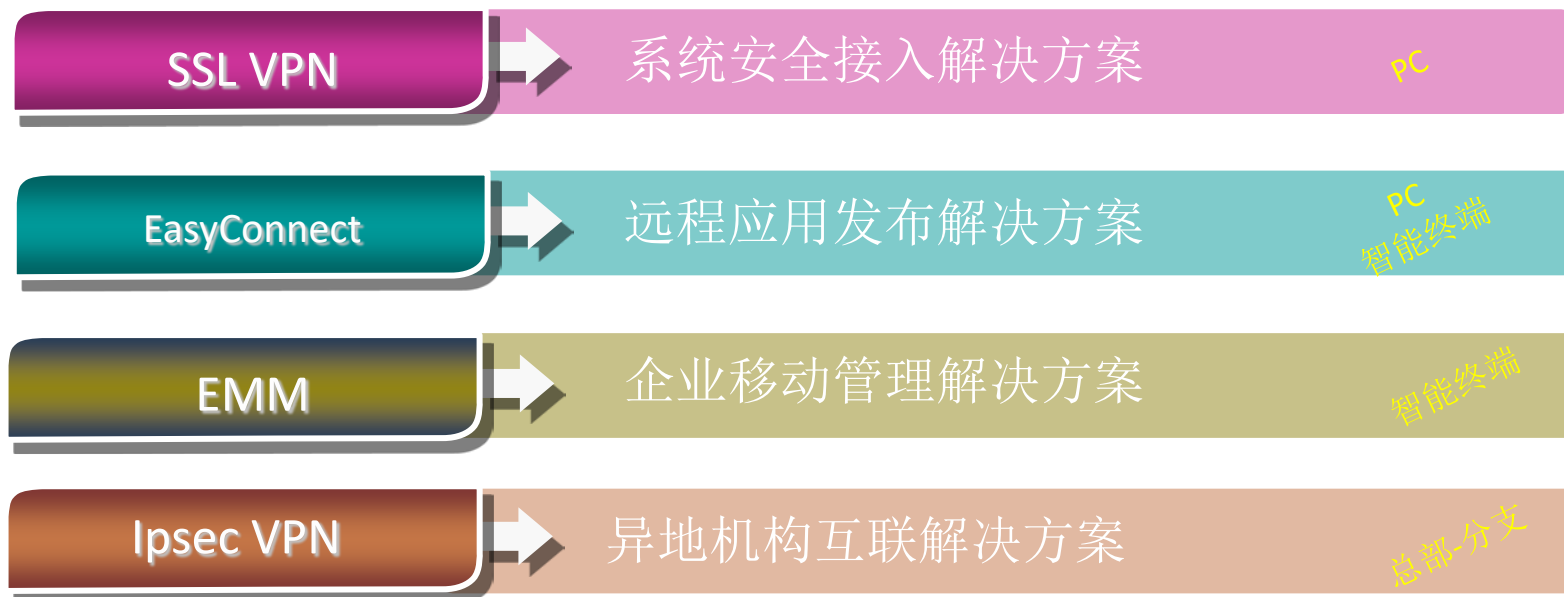


智能终端安全接入
Easyconnect/EMM



分支安全接入
IPSEC VPN

深信服统一安全接入平台应用场景简介



SSL VPN系统安全接入应用场景

核心业务系统接入

系统安全接入
系统安全加固

移动用户远程接入

领导外出出差
员工在家加班

Easyconnec远程应用发布应用场景

移动办公

对智能终端移动办公提供支持，例如政府移动执法、金融移动展业

应用加速

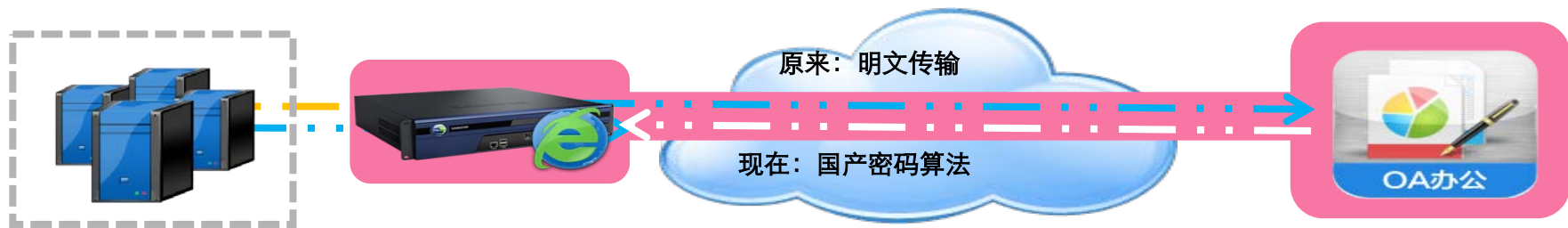
对中小分支、跨国机构访问业务系统慢的情况进行应用加速

数据防泄密

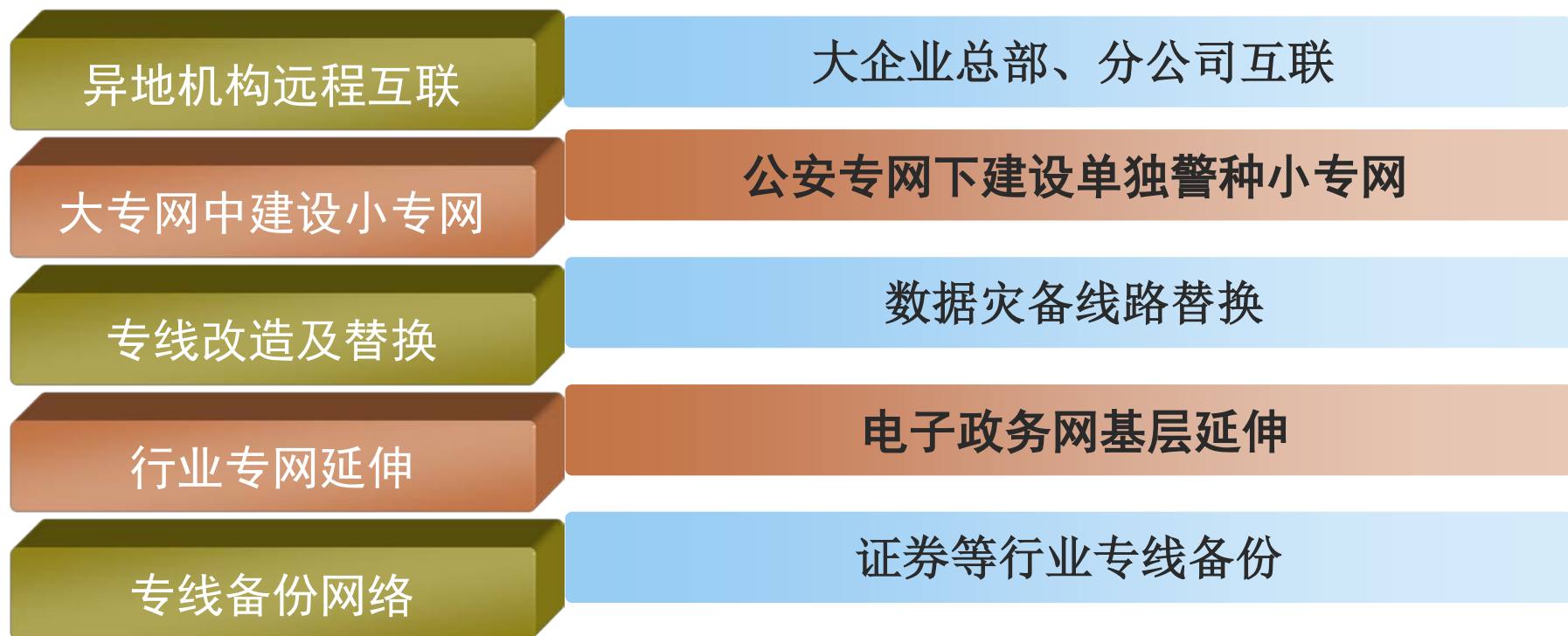
对防泄密要求高的客户提供便捷，对核心机密数据进行不落地保护

EasyAPP手动/自动封装应用场景

- 将用户真实服务器隐藏在SSL VPN设备后，保护服务器自身安全
- 在APP中集成VPN安全接入代码，增加认证方式及传输加密机制
- 用户正在开发移动办公APP——手动封装安全接入SDK
- 用户使用已经开发完成的APP——自动封装安全接入SDK



Ipsec VPN异地机构远程互联应用场景



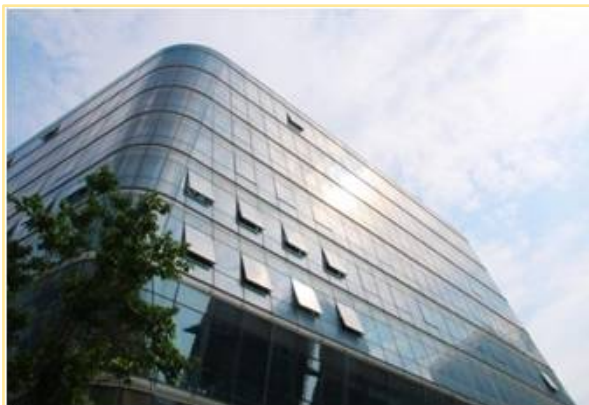
1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

完善的服务支撑体系



200坐席CTI

深圳、长沙、吉隆坡



50+个城市

设立备品备件中心
设有原厂工程师



6500+名认证工程师

100余名资深行业专家
组成的专业团队

快速响应的服务机制



7*24小时
400电话咨询和远程调试



社区：人工智能在线服务，
24小时在线，365天无休



服务可视化
手机端及时推送信息



通过ISO9001质量管理

1. 产品概述
2. 功能介绍
3. 技术架构
4. 产品特点
5. 应用场景
6. 售后支撑
7. 客户案例

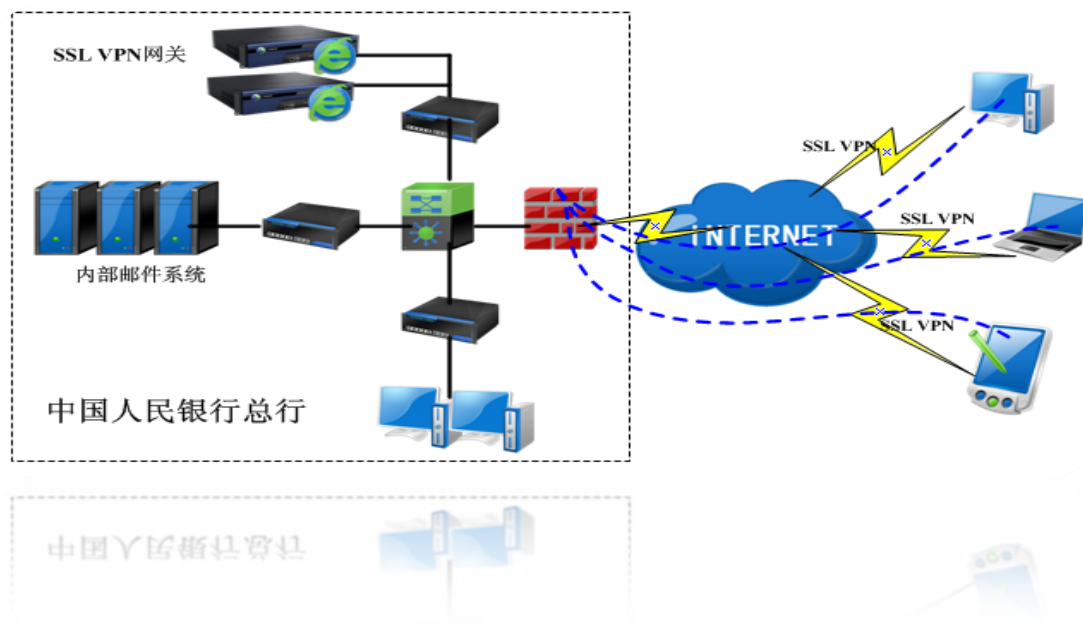
中国人民银行总行 ——SSL VPN远程移动办公接入

客户需求：

- ✓员工外出期间安全、便捷的访问移动办公

应用效果：

- ✓多因素身份认证方式，实现了静态认证和动态认证的混合模式身份认证体系
- ✓数据经过SSL VPN加密隧道进行传输，保障外出期间系统访问安全。



四川省质监局

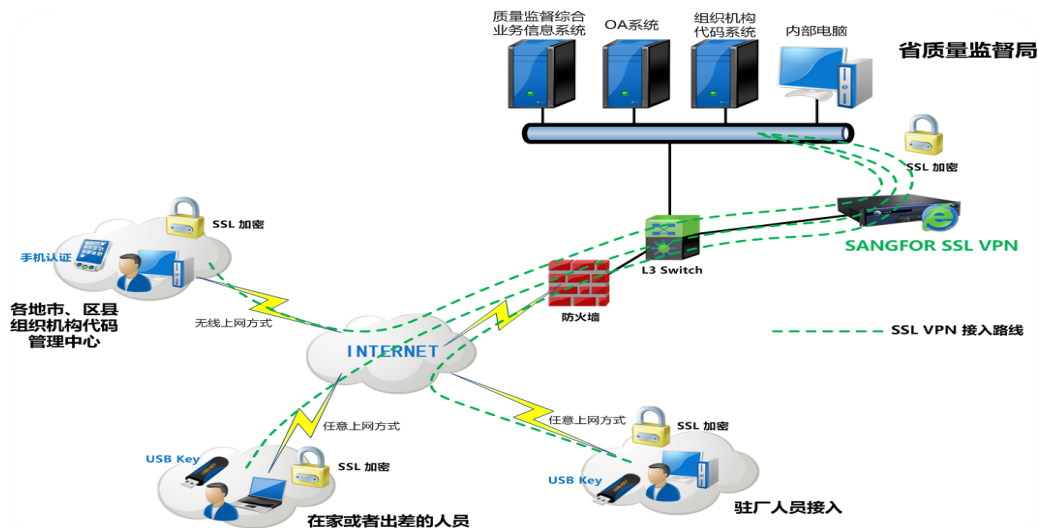
——专线备份及第三方运维人员安全接入

客户需求：

- ✓大量人员在家或者出差时候的远程访问
- ✓以IPSEC VPN为专线做备份
- ✓驻厂人员安全接入及统一运维

应用效果：

- ✓通过SANGFOR SSL VPN与四川省质量监督局网络结合，实现保密的数据交换，增强安全性。
- ✓不需要安装任何客户端，只要有浏览器即可快速访问到对应的应用系统，简单方便操作，维护成本低，实现了OA、组织机构代码系统、质量技术监督信息系统（CQS）接入的安全，全面提高访问速度，提高办公效率



好想你枣业

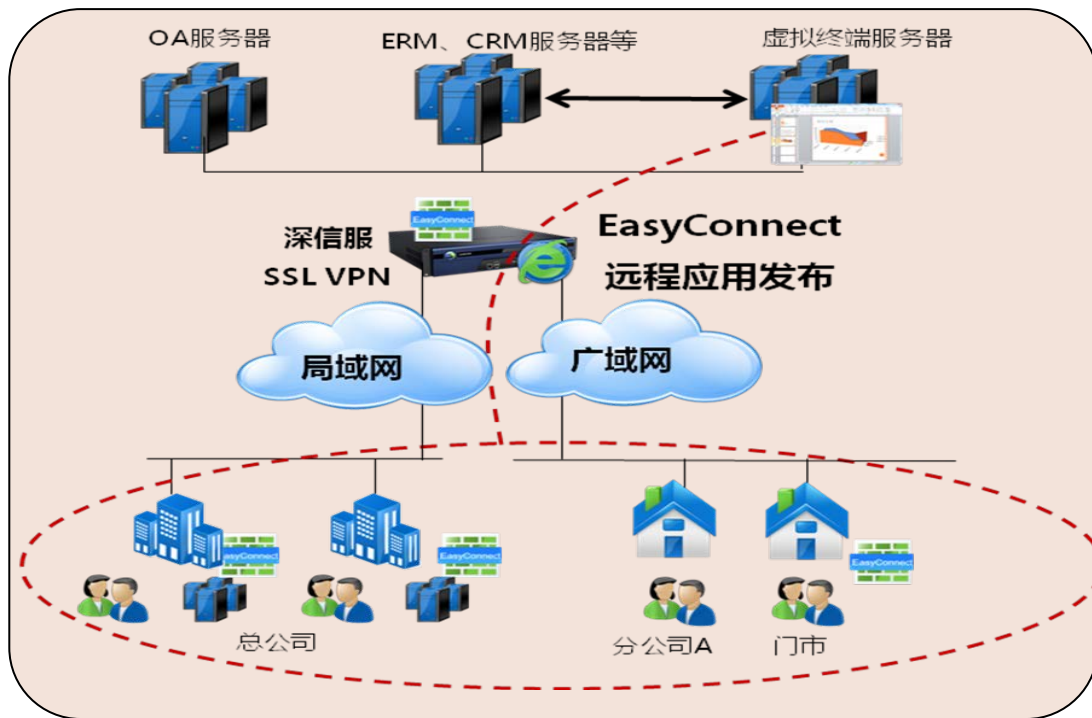
——PC端远程应用发布

客户需求：

- 1、全国店面过多，设备双边部署困难，需要单边部署
- 2、由于业务人员IT水平参差不齐，运维管理需要集中化
- 3、总部调整系统后，全球任何一个机构可以使用浏览器接入企业的服务器，使用最新的应用程序并获得最新信息。

应用效果：

- 1、只需要几个小时的时间，就快速实现ERP应用的部署，解决了应用兼容问题，大大减少总部运维工作量，提高了业务效率。
- 2、此外，对于大量传输数据的应用来说，还能明显提升150%的访问速度，大大加速了业务系统的访问。
- 3、对于今后扩张的店面，可以快速实现应用发布，并且无需任何定制直接在智能终端（ISO、安卓系统）上访问。



中国货运航空

——手持终端Easyconnect远程接入

客户需求：

- ✓ 运控部门主要访问货运公司相关的运营系统，以及马上要上线的航务系统，以便实时查看航班的运行状态。
- ✓ 部门领导在外面做业务洽谈时需要及时浏览和批复文件。
- ✓ 飞行员航空任务执行完毕后，在到达地方的休息室访问oa, foc, 以及飞行准备系统，实现高效便捷的移动办公。

应用效果：

- ✓ 在总部部署深信服VPN（EC）设备，后端搭建终端服务器。对于跨平台终端用户只需在appstore或安卓市场中下载深信服的EC客户端即可使用，实现系统安全接入



政府	金融	教育科研	能源电力	运营商	大企业
中华人民共和国最高人民法院	中国人民银行总行	中国科学院计算机网络信息中心	中国海洋石油	中国移动通信有限公司总部	中国远洋运输集团
中华人民共和国农业部信息中心	中国银行	浙江大学	中国国电集团	中国移动陕西省分公司	中国航天科技集团公司
中华人民共和国教育部考试中心	中国农业银行	中国人民大学	中国电力投资集团	中国移动四川省分公司	中国邮政集团
中华人民共和国卫生部卫生监督中心	中国银行	中山大学	中国华能集团	中国移动云南省分公司	中国电子信息产业集团
中国对外贸易中心	招商银行	电子科技大学	中国大唐集团	中国电信山东省分公司	中国邮电器材集团公司
中国民用航空总局	兴业银行	中国政法大学	中国华电集团	中国电信湖南省分公司	中国航空器材集团公司
中国妇幼保健中心	中国银联	中央广播电视大学	国家电网公司	中国电信四川省分公司	中国黄金集团公司
中国环境监测总站	中国人寿保险股份有限公司	中国传媒大学	中国南方电网	中国电信广西区分公司	中国葛洲坝集团股份有限公司
国家林业局森林病虫害防治总站	泰康人寿财产保险股份有限公司	华东理工大学	中国水电顾问集团	中国电信陕西省分公司	中国长江航运集团
国家药典委员会	新华人寿保险股份有限公司	吉林大学	广东省粤电集团有限公司	中国联通河北省分公司	招商局集团有限公司
中国残疾人联合会	华夏基金管理有限公司	华东交通大学	广西电网公司	中国联通辽宁省分公司	中国铝业公司



中国移动
China Mobile

谢谢!

中国移动内部资料，
未经允许不得复制、转发、传播。