

中国电信 一站式安全服务



张百川 15339230081

陕西电信信息安全服务中心
www.safe365.cc

中国电信一站式安全服务

急客户所急，想客户所想！

—— 中国电信一站式安全服务

- 用户的困扰
- 服务介绍
 - 产品：“天御五行”可信网络行为管理系统
 - 服务

网站整体安全

安全事件监控

数字证书认证

- 应用案例解析
- 我们的优势

网络管理员的困扰

● 互联网行为不可控

行为管理

- 上班偷菜？
- 开心网
- QQ聊天
- 非法网站
- 求职
- 炒股
- 网络游戏

流量控制

- 在线视频
- 电影&电影下载
- P2P/迅雷/电驴

安全审计

- 百度贴吧
- 天涯论坛
- 门户发帖
- QQ空间
- 邮件安全
- 网站访问

“天御五行”可信网络行为管理系统

上网行为管理

- 上网人员控制
- 上网时间控制
- 网站分类访问控制
 - 800万URL库
 - 54个网址分类
- 应用协议控制
 - 110种应用协议（QQ、MSN、迅雷、电驴……）
- 搜索关键词控制

网络流量控制

- 静态流量控制
 - 人均流量控制
- 动态流量控制
 - 根据设定值自动调整
- 智能流量控制
 - 智能学习，自动分配
- 协议流量控制
 - 迅雷、电驴等……

网络安全审计

- URL访问审计
- 电子邮件审计
 - FoxMail、OutLook
 - 网易、搜狐……
- 网页发帖审计
 - 百度、QQ空间、天涯、猫扑……
- 报表统计
 - 人员、协议、网址、流量等的统计

典型应用·可信网络行为管理系统

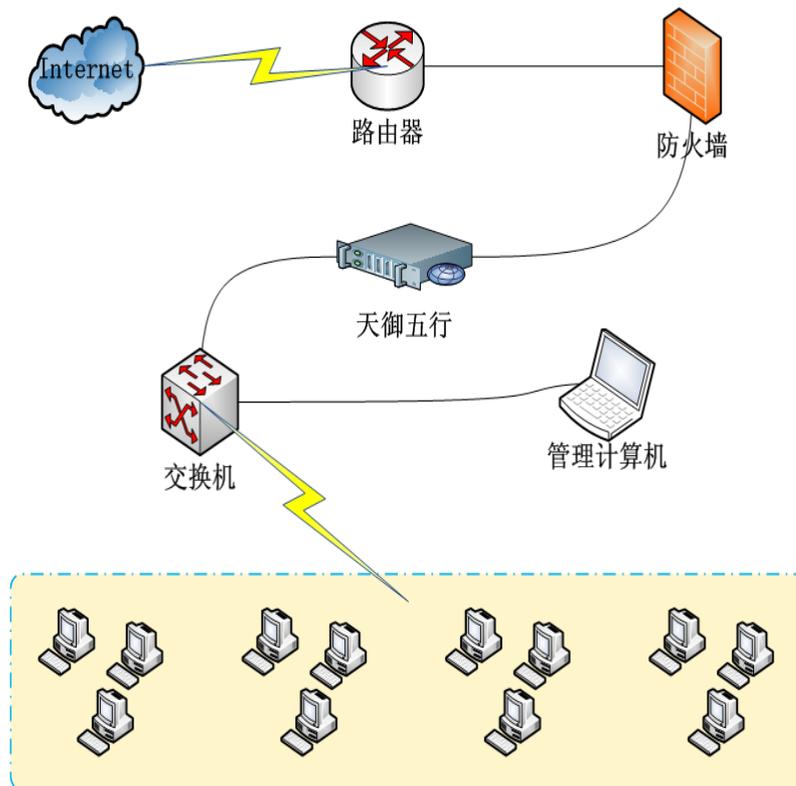
● 西安某企业

■ 存在问题

- ◆ 无序下载导致网速变慢
- ◆ 上班时间聊天、炒股、游戏
- ◆ 曾经因浏览非法网站被通报

■ 实现效果

- ◆ 自动流控，对持续5分钟流量大于2M的计算机自动限定到100K并保持30分钟，极大的提高了上网速度
- ◆ 封堵娱乐、炒股、电影等网站和应用，提高工作效率
- ◆ 通知：对邮件、URL审计，再无人浏览非法网站



网站维护人员的困扰

- 有硬件防火墙防护
- 有入侵检测系统检测入侵企图
- 还有正版的防病毒系统.....

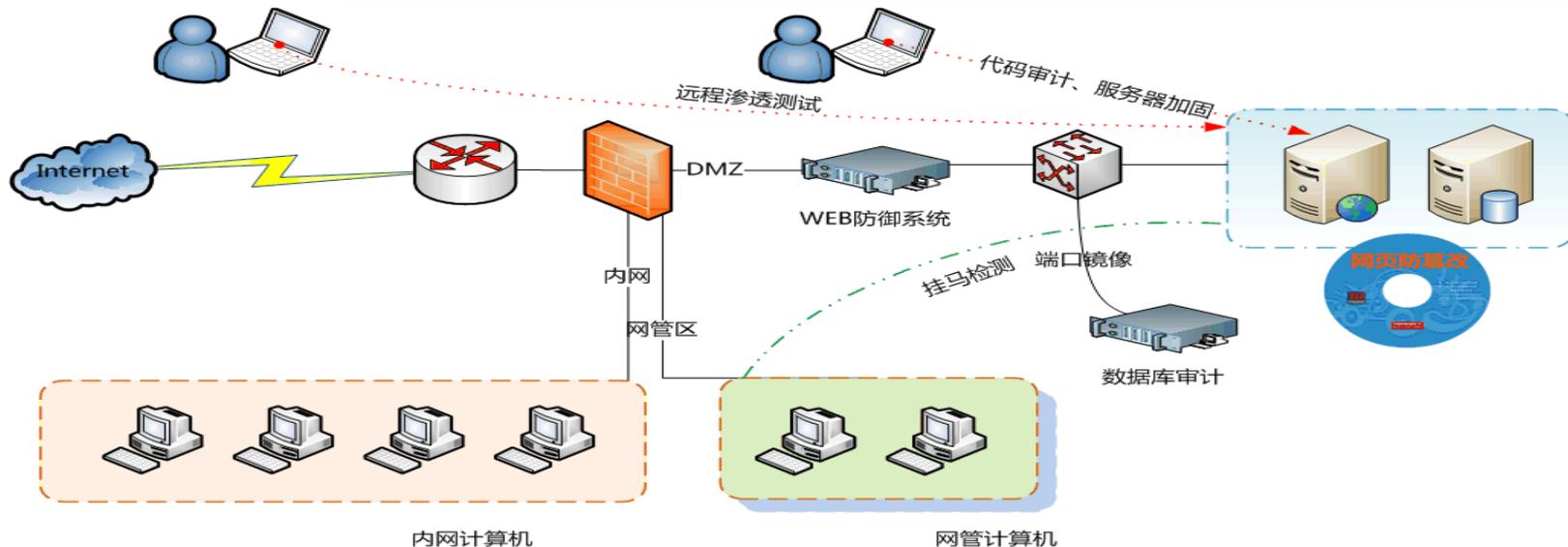
为什么又被攻击了! ?



抓狂啦!



网站整体安全解决方案



主机

主机层加固

抗黑客攻击

网页防篡改

网络

攻击阻断

WEB加速

流量清洗

数据

数据库评估

数据库加固

数据库审计

程序

木马检测

代码审计

渗透测试

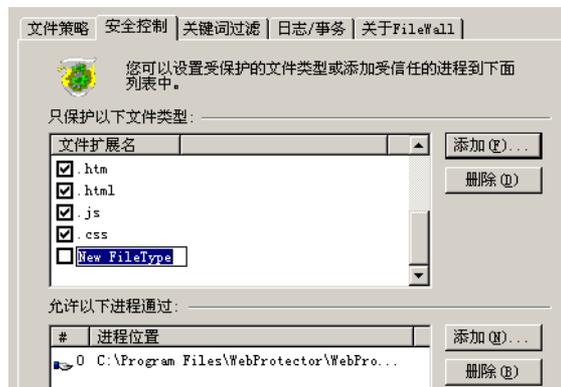
某政府机关

存在问题

- ◆ 网站多次被攻击
- ◆ 首页被篡改、挂马
- ◆ 网站访问缓慢

实现效果

- ◆ 通过WEB安全评估和加固实现代码、应用、系统安全
- ◆ 安装网页防篡改软件，实现主机层面的安全
- ◆ 部署WEB应用防火墙，实现网络层黑客攻击行为检测和阻断，如：跨站、注入攻击
- ◆ 实现了网页访问加速功能



详细信息 2009/05/19 22:06:35

威胁: 跨站脚本攻击

URL地址: /jsp-examples/sessions/carts.jsp?submit=addItem-->>></SCRIPT></style></!t e></textarea><SCRIPT>alertString.fromCharCode(88,115,115,84,101,115,116)</SCRIPT>]

服务器IP: 192.168.10.21

服务器端口: 80

客户端IP: 192.168.10.8

客户端端口: 1687

客户端环境: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 3.0.04506.30)

标签(tag): WEB_ATTACK/XSS-1

动作: Access denied with code 403

攻击特征码: <script

触发规则: 查看

访问唯一编号: ShK8638AAAAAFvycalAAA6b

威胁	事件	客户端IP	服务器IP
高	跨站脚本攻击	192.168.10.8:1687	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1683	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1679	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1677	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1675	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1664	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1661	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1659	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1656	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1653	192.168.10.21:80
高	跨站脚本攻击	192.168.10.8:1649	192.168.10.21:80

WEB加速缓存配置

是否启用缓存

是否启用过期

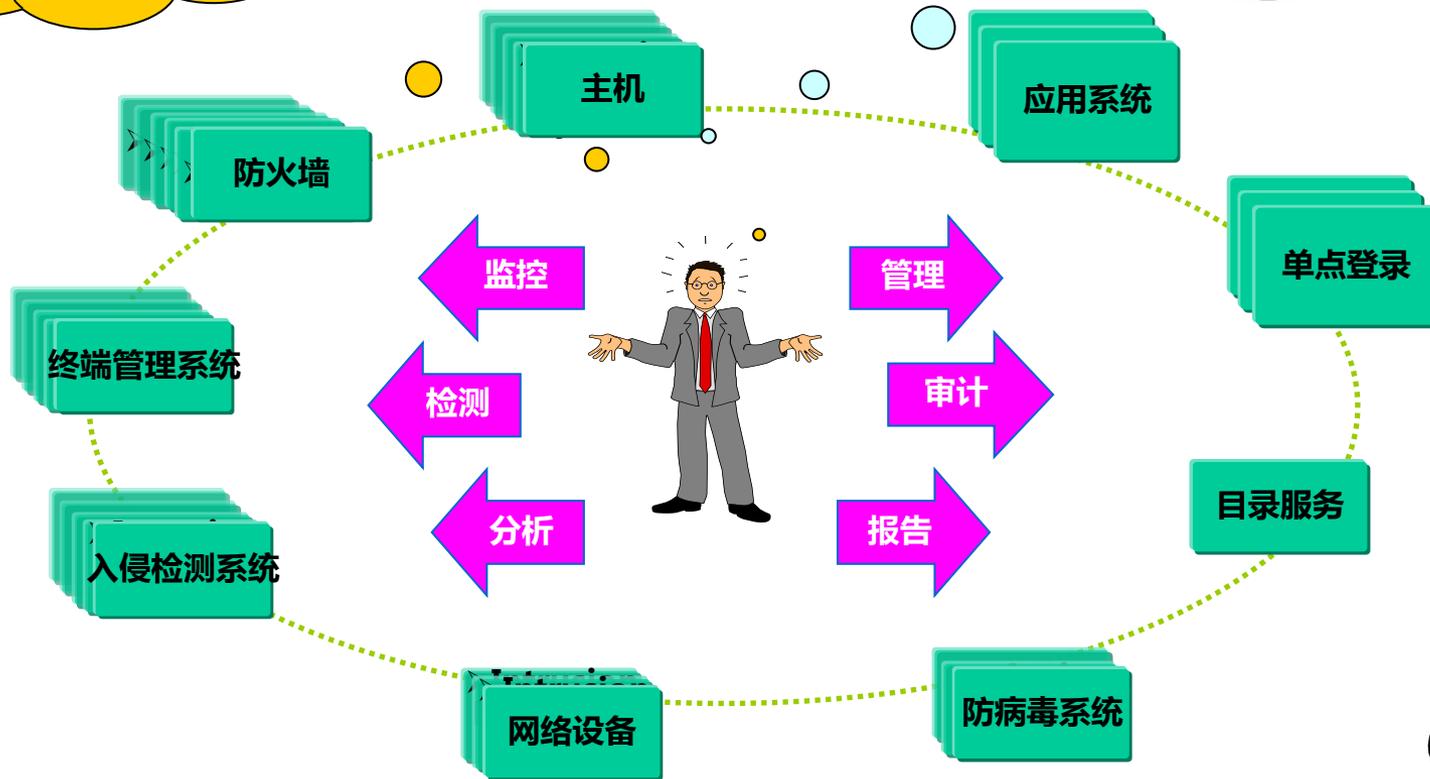
默认过期时间(秒)

在启用缓存后，如果禁用过期来判定缓存文件是否过期。可

安全主管的困扰

人力？技能？成本？

要是能有一种既省钱有有效的
统一管理手段就好了！



安全事件监控解决方案

MSS (Managed Security Service)

从远端的安全运营中心 (MSSP) 监控、管理企业的IT安全信息、资产和流程

MSS扩展服务

通过安全管理服务为基础，为客户提供安全产品选型、集成等服务。

安全设备的监控与管理

防火墙、IPS的监控与管理

- 1、防火墙监控与管理
- 2、主机入侵与防护
- 3、网络入侵与防护

IDS的监控与管理

- 1、网络入侵检测
- 2、无线入侵检测
- 3、主机入侵检测

应用安全服务

- 1、邮件防病毒
- 2、防垃圾邮件
- 3、防毒网关管理

防DDOS攻击服务

弱点和智能管理服务

企业安全弱点管理

- 弱点扫描
- 渗透测试
- 安全告警

安全智能服务

- 安全信息管理
- 安全事件管理
- 安全符合性管理
- 安全专家建议
- 报告服务

其他扩展服务

日志管理、集中存储服务

其它，如SSL VPN、认证等服务
安全产品集成服务
现场服务

MSSP是MSS服务的基础和前提

典型应用·安全事件监控

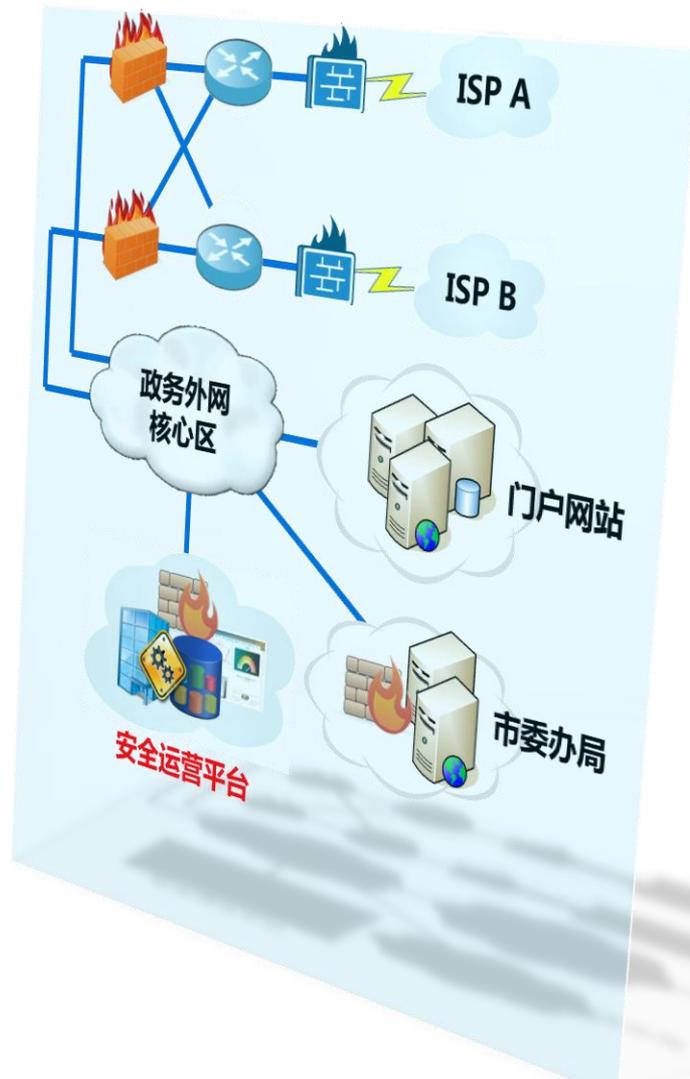
● 某电子政务网

■ 存在问题

- ◆ 无法实时监测路由器、交换机、防火墙、入侵检测、数据库等的运行状态

■ 实现效果

- ◆ 生成网络拓扑，运行状态一目了然
- ◆ 中国电信7×24小时安全监控，网络攻击实时监测，安全事件10分钟通知用户
- ◆ 设备运行状况尽收眼底，防患安全事件于未然
- ◆ 极大提升了政务网安全性



您的业务系统安全吗？

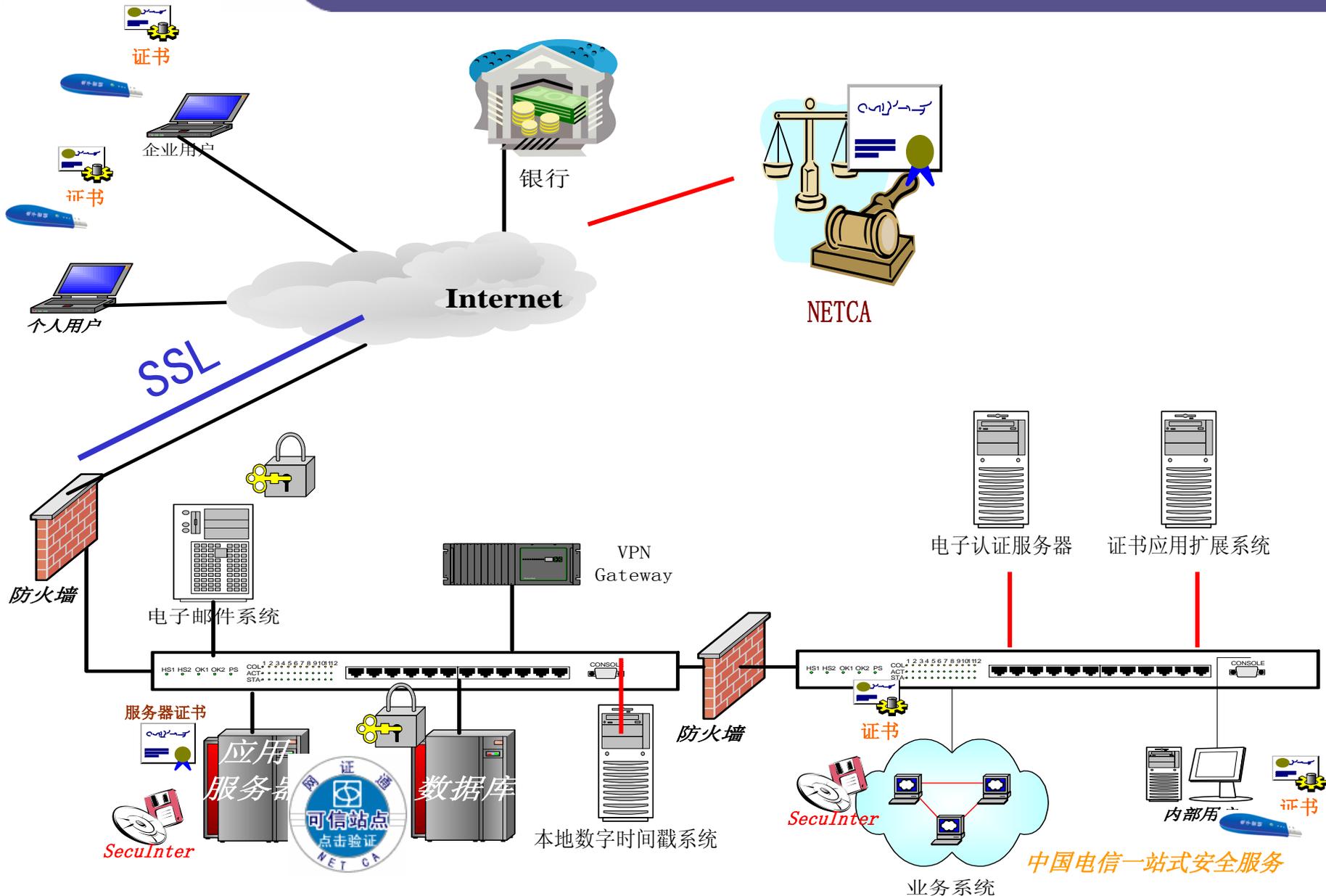
● 常见业务系统

- 办公系统、电子招投标、企业资源管理系统、电子病历管理系统、电子邮件系统.....

● 自身脆弱性和面临的威胁、风险

- 用户名和密码登录不安全
- 信息明文传输容易被截获
- 到手的红头文件无法确认是否被修改
- 无法确认邮件的真实发送人
- 无法控制电子邮件的接收人
- 网上提交的表单无法作为法律证据
- 远程接入安全性控制
- 各个业务系统用户管理各自为政，管理混乱

数字证书认证解决方案



典型应用·数字证书认证

● 某企业

■ 存在问题

- ◆ 出现过有人登陆办公系统冒充领导的情况
- ◆ 担心远程接入（VPN）的用户名和密码泄露
- ◆ 电子邮件安全堪忧
- ◆ 欲增强财务系统的安全性

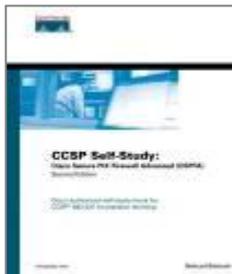
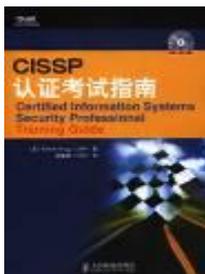
■ 实现效果

- ◆ 通过USB KEY形式的数字证书实现业务系统安全性
- ◆ 远程用户必须通过硬件的USB KEY才能登录内网
- ◆ 电子邮件签名、加密



我们的优势

- 本地化的专业服务队伍：陕西电信信息安全服务中心
- 5×8 或 7×24 的技术支持
- 遍布全省的：省、市、区县全方位的技术支持
- 高素质的人才：信息安全相关专业博士/硕士
- 深厚的信息安全技术背景和实践积累：软件、网络、金融、芯片
- 专业的咨询服务方法和项目管理能力：PMP
- 领先的个人资质和从业资历：CISA/CISSP/CISP/CISM/ISO27001 LA/ITIL
- 优秀的业务整合能力：技术方案、管理理念和方法、最佳实践
- 值得信赖和肯定的职业道德、工作热情和专业精神
- 中国电信北京研究院等专业研究机构的技术支撑



客户群体 & 营销策略

- 终端数量 > 50 的光纤客户
- 新增的光纤用户（捆绑）
- 产品组合（如做网站安全送网站）



为用户指定不同套餐服务

套餐名称\定制服务	购买	租用
可信网络行为管理	○	○
网站安全	○	○
安全事件监控	○	○
数字证书认证	○	○



用户根据需求选择相应套餐服务

用户



中国电信一站式安全服务



根据套餐内容为用户提供相应的软件、硬件以及人工服务。

资料获取

- 宣传彩页

- 会场获取

- 电子资料

- www.safe365.cc

- 电话支持

- 029-87899001

- 邮件支持

- tech@safe365.cc



中国电信
CHINA TELECOM

2010年上海世博会全球合作伙伴
Global Partner of Expo 2010 Shanghai China

Thank You !

使命促就责任 安全成就价值

张百川 15339230081