区域智慧隔离安全解决方案

华为技术有限公司

HUAWEI

企业网络访问的安全风险

随着网络应用的丰富，给人们带来无尽方便的同时，其安全风险也变得更加严重和复杂。单台计算机安全事故引起的损害可能传播到其他计算机和网络，引起大范围的信息系统瘫痪；缺乏安全控制机制和对网络安全规范认识不足，各类安全风险正日益加剧。企业网络访问的安全风险来自以下两个方面：

其一，来自访问互联网的风险：企业内网由于工作必须与互联网相连，而互联网自身的开放性、自由性等特点，含有机密信息的企业内网会被入侵者列入其攻击目标。调查显示，今年上半年，我国遇到过病毒或木马攻击的网民达到2.17亿，其中中毒的计算机有40%以上是办公用途。内网一台计算机中毒后，其他计算机、服务器均有遭遇病毒感染的可能，导致内部业务系统瘫痪，给企业带来严重经济利益；对政府部门来说，可能引发机密信息泄露。

其二，来自企业内网互访的风险：根据加利福尼亚州旧金山的计算机安全协会(CSI)的观点，大约60%到80%的网络滥用事件起源于内部网络，在企业网络中，任何一台计算机的安全状态都将直接影响到整个网络的安全。员工安全意识薄弱，企业安全策略难以实施，网络病毒泛滥；网络资源的不合理使用，行为规范难以管控，工作效率下降；各种外设滥用，高密区数据访问缺乏管控，信息泄漏频繁等问题极大的困扰企业高层管理人员和IT部门。

内网安全管理的现状和挑战

为应对上述安全风险，客户会采用网络隔离的方式，从网络层隔离互联网和内网，以及内网的高密区和低密区，保护内网安全的同时，保障机密信息不被泄漏。

网络隔离分为物理隔离和逻辑隔离两种。常用的物理隔离是通过网闸、双硬盘、两套主机、网络隔离卡等方式来实现，这往往需要花重金和大力气部署隔离产品，建设成本高、周期长，运维管理工作量也成倍增加，用户体验差，由于工作需要网络之间需要交换信息，而物理隔离完全禁止了数据的交换和传输，影响工作效率。常用的逻辑隔离是安全隔离网关或者防火墙，但只要是包转发，就存在基于包的安全漏洞，存在对包的攻击。

因此，如何有效地将网络区域安全逻辑隔离，同时保证用户操作简便，工作效率提升，是企业IT部门最为关注的问题。

华为区域智慧隔离安全解决方案概述

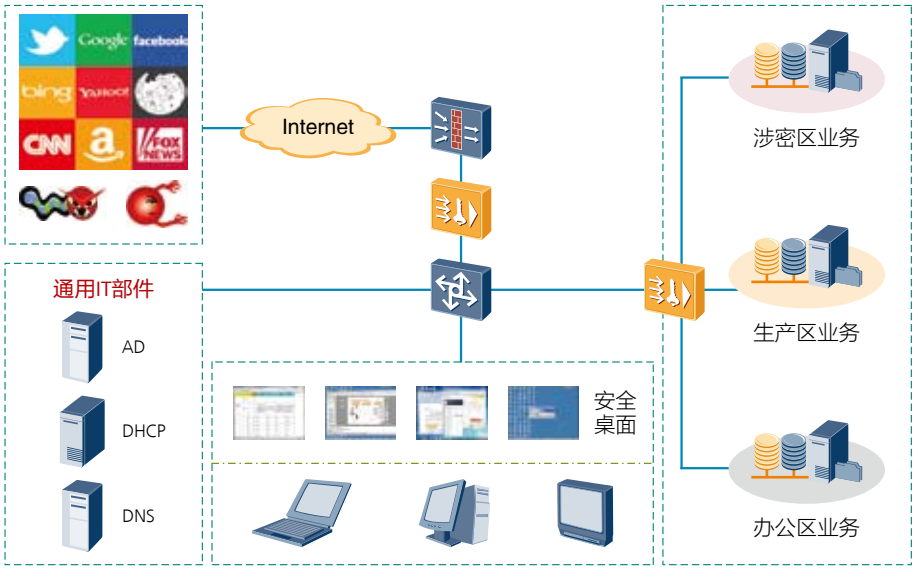

图1 华为区域智慧隔离解决方案架构

华为推出的智慧隔离安全解决方案弥补了网络区域隔离现状的不足，通过领先的“安全沙箱”技术为不同区域的网络访问提供了安全的逻辑隔离方法，使用户能够在一台计算机上，同时建立多个逻辑隔离空间（互联网安全桌面、业务安全桌面、涉密区安全桌面），在每个安全桌面中进行不同的网络访问，安全桌面内的操作通过安全策略得到控制，安全桌面退出后数据自动清除。有效地阻止病毒、木马对企业内网的攻击；可靠地防止涉密区机密数据有意泄漏（外设、截屏、二次跳转）和无意泄漏（病毒、木马攻击、忘锁屏）。同时，华为区域智慧隔离安全解决方案提供了安全的跨区域文件传输方法，支持指纹级的文件审计，保证文件传输安全可控，提高工作效率。

典型应用场景

互联网安全访问

图2 互联网安全访问部署图

在企业内网和互联网边界部署SVN网关，用户通过网关认证后将自动安装客户端软件。然后即可启动安全桌面，通过安全桌面访问互联网，确保来自互联网的内容仅仅在安全桌面环境中，病毒、木马不能传播到办公网络设备上，在安全桌面可以设置智能运行的应用程序，有效防止员工进行与工作无关的网络访问，提高工作效率。用户在互联网下载的任何数据都可以设置经过安全审核才能上传到服务器或者拷贝到真实桌面，且保存下来的数据都会进行指纹级的审计，保证来自互联网的数据安全可控。

内网区域安全访问

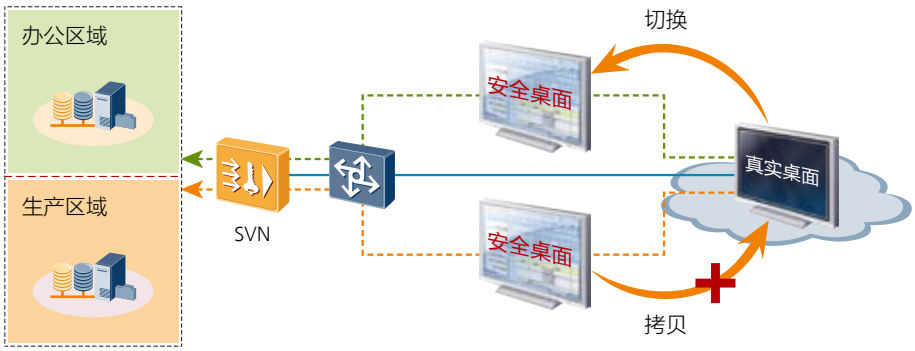

图2 互联网安全访问部署图

在企业内网各区域边界部署SVN网关，用户连接网络后将自动安装客户端软件。用户可以启用多个安全桌面，通过不同的安全桌面访问不同内网区域，有效实现内网各区域的安全逻辑隔离，保证来自高机密区（生产区）数据仅仅在安全桌面空间中，不能传播到其他办公网络设备上；低机密区（办公区）存在安全风险的个别终端不会影响整个内网安全；在安全桌面中各种外设设备如：USB口、COM口、打印机都有严格的控制，有效阻止通过外设或者移动存储设备泄漏机密信息；同时，安全桌面中可以阻止截屏、二次跳转等恶意泄密行为；另外，安全桌面退出后数据无痕清除，防止机密数据存储用户终端带来的数据泄漏风险。

方案亮点

完备的区域隔离，一机多用，降低投资成本

- **领先的安全沙箱：**将内网和互联网安全隔离，有效防止病毒、木马对内网的攻击，配置只能运行的进程名单，防止员工运行与工作无关的应用，提高工作效率；
- **专业的多实例技术：**一个物理桌面内同时创建多个安全桌面，不同的安全桌面访问不同的业务，一机多用，大幅度降低投资成本；

领先的数据防泄漏机制，数据安全无忧

- **完备的文件访问隔离：**在安全桌面中只允许用户操作真实桌面指定的文件夹和目录，跨区域获取的数据文件重定向加密存储在虚拟空间中，退出安全桌面后无痕化清除；
- **外设及网络访问控制：**可以设置禁止安全桌面内访问外设及网络传输；
- **高强度透明加解密：**在安全桌面内产生的数据都将被加密保存，采用强度最高的AES256加密算法，加密密钥动态生成，保存在SVN网关中，周期更新；
- **防截屏、防粘贴板拷贝：**通过屏蔽截屏、虚拟化粘贴板等措施，防止机密数据泄漏；

专业的跨区域传输控制，数据传输无忧

- **文件内容扫描：**跨区域数据传输和安全桌面与真实桌面的数据导入导出都支持按关键字进行内容监控；
- **指纹级操作审计：**用户文件的操作都会被详细的记录，管理员可根据记录定期审计用户行为，回溯用户的非授权操作；

部署便捷，用户体验好，降低管理成本

- **便捷部署：**只需在网络区域边界部署SVN网关、客户端可自动安装，极低的部署成本和运维成本；
- **桌面自启动：**安全桌面可以设置开机自启动、退出安全桌面注销或者关闭计算机；
- **多桌面切换：**用户可在终端屏幕上方浮动的导航条上进行多屏幕切换、操作方便；

华为技术有限公司

深圳市龙岗区坂田华为基地

电话: (0755) 28780808

邮编: 518129

版本号: M3-035027-20121203-C-1.0

www.huawei.com