内外网文件安全
交换及传输整体解决方案

目录

一、概述

在信息化社会中，由计算机技术和通信技术相结合所形成的计算机网络，已经成为反映信息社会特征最重要的基础设施。计算机网络在政治、军事、商业、交通、电信、广电等方面的作用日益增大，人类对计算机网络的依赖也日益增强。人们建立了各种各样完备的信息系统，使得人类社会上的一些机密和财富高度集中于计算机中，并通过网络计算机接收和处理消息，实现相互间的联系和对目标的管理与控制。以网络方式获得信息和信息交流已经成为现在信息社会的一个重要特征。随着网络的开放性、共享性及互联程度的扩大，特别是 Internet 的出现，网络的重要性也越来越大。同时，随着网络上各种各样新业务的兴起，比如电子商务、电子政务、网络银行、数字货币以及各种专用网的建设等等，使得网络安全问题显得越来越突出。因此网络安全成为了越来越多的企事业单位关心的问题。

数据安全主要有两大类：传输安全和存储安全。传输安全指在数据的生成、传输和访问过程中，确保数据的完整性、准确性及排他性，防止篡改和窃取。存储安全指在数据保存上确保完整、可靠和有效调用。

二、风险及需求分析

2.1 现状分析

目前绝大多数企业都在内部实施了内外网分离，互联网与内网隔离，生产网与办公网隔离，办公网与研发网隔离，以确保企事业单位信息安全。随着企事业单位的不断发展，不同工作区域及不同网段工作人员需要着广泛的文件交换。然而，随着文件交换的频繁度不断增加，安全威胁也随之越来越严重。企事业单位目前需要解决多处安全威胁，首先，解决文件交换过程中的病毒传染问题。由于文件在各种工作站、服务器间不断传输、交换，因此被病毒感染的问题往往会在企事业单位内部网络中快速传播与扩散，难以清除。其次，传统的文件交换方式依旧大量使用 U 盘进行拷贝，AutoRun 等 U 盘介质病毒也容易在企事业单位网内大量驻留和传播，手工清除工作量极大。最后，工作人员通过 FTP、文件共享等高风险方式通过公共网络和办公外网向内网传输文件，虽然采用了双网卡的方式进行工作，使企事业单位内网跟外网形成了不同网段的划分，但在没有安全防御措施的情况下，企事业单位的办公网仍然易遭受到黑客攻击与控制。

2.2 USB 移动介质风险分析

1）在网络还不像现在这么盛行的年代，可移动存储设备是传播病毒的重要方式。就是将恶意程序放在 U 盘，或者移动硬盘，甚至软盘中——在不同的 PC 交换数据的过程中，就可以达到传播病毒的作用。

2）同事间交换数据，大家的电脑都插一遍带毒 U 盘，自然就都感染上了。已经被感染的设备，再感染插入设备的新 U 盘，以此达到扩散的目的。

3）USB 的可访问性和可复制性，使它们更易于发生数据泄漏、丢失和病毒感染。

2.3 内外网文件传输风险分析

在企事业单位的日常业务中，存在大量需要在不同网络之间进行文件传递的场景。处在内网员工，需要将设计图纸、项目资料等文件发送给外网的用户。科技型企业，需要持续将从外部获取的大量数据导入到研发网，进行机器学习、数据挖掘等数据处理工作，比如传感器采集的数据、测试数据、网络服务收集的数据等。

因此，随着企事业单位业务系统的日益成熟，可控的跨网数据交换需求也越来越强烈。

目前，企业在解决跨网文件传输时，主要采取以下方式。

（1）通过移动硬盘在内外网间进行数据拷贝

频繁的使用移动硬盘，不仅动作繁琐，而且在文件传输的过程中有可能导致病毒的传播。

（2）通过 FTP 软件传播或者使用网络共享的方式内外网文件传输

使用此两种方式内外网文件传输，可能会出现文件传输中断问题，也无日志追踪记录。在传输过程中无法隔离病毒。

2.4 文件选择与过滤需求

基于规则的过滤器，对文件类型进行控制。只允许用户选择工作需要的文件格式文件进入工作区，并且文件进行深度检测，防止伪文件欺骗进入到系统。对于系统没有的文件格式，进入文件智能学习，选择需要的文件格式后缀。避免与业务无关的文件或伪造业务文件的病毒、木马文件进入企事业单位文件共享系统。同时，对交换到外部网络的文件格式进行限制，防止涉密文件泄露。

2.5 授权不清晰引发的问题

在企事业单位里，经常会有多人同用同一账号的问题，管理员与普通使用者授权不清晰往往导致诸多问题;

1）普通用户和管理员账号共用可能存在文件被篡改和丢失等问题。

2）普通用户可以在管理员权限上进行系统配置，造成文件管理混乱。

再优秀的管理者也不可能做完所有的事情，因此，一个优秀的管理者必须学会授权，并且要避免因授权不当而带来的管理混乱。

面对授权不清晰引发的问题，我们要足够的重视，在一个理想的文件安全传输中，我们需要对普通使用者的权限或者是访问的权限进行精确的定位。

2.6 使用者的审计日志问题

各系统独立运行、维护和管理，所以各系统的审计也是相互独立的。每个网络设备，每个主机系统分别进行审计，安全事故发生后需要排查各系统的日志，但是往往日志找到了，也不能最终定位到行为人。

日志记录的好坏直接关系到系统出现问题时定位的速度。同时，我们可以通过对日志的观察和分析，提前发现系统可能的风险，避免线上事故的发生。对于运维人员来说，线上日志审计尤其重要，能够帮助我们第一时间发现线上问题并及时解决。

2.7 病毒隐患

目前的情况下，病毒主要通过以下 3 种途径进行传播：

1）通过不可移动的计算机硬件设备进行传播，这类病毒虽然极少，但破坏力却极强，目前尚没有较好的检测手段对付。

2）通过移动存储介质传播，包括软盘、光盘、U 盘和移动硬盘等，用户之间在互相拷贝文件的同时也造成了病毒的扩散。

3）通过计算机网络进行传播。计算机病毒附着在正常文件中通过网络进入一个又一个系统，其传播速度呈几何级数增长，是目前病毒传播的首要途径。

病毒的危害是非常大的，比如前些年出现的熊猫烧香的病毒，已经感染，会给企事业单位带来重大的损失。

三、文件传输安全解决方案

3.1 方案设计原则

3.1.1 先进性和成熟性

采用代表当前计算机发展趋势的先进技术和成熟的产品，确保该信息系统在 2 年内不落后，保证平台在技术上领先、成熟、稳定和可靠。

3.1.2 可靠性原则

整个网络系统必须具备高度的稳定性和可靠性，提供充分的可靠性服务。网络系统运行稳定、故障率低、容错性强，实现 7*24 小时正常工作。

3.1.3 最小影响原则

在方案设计及实施时，遵循对信息系统影响最小原则，尽可能地采用对网络、系统、应用影响最小的技术手段，对现有系统不产生干扰，保护现有系统。

3.1.4 安全性原则

1. 其主要通过以下几种方式进行文件病毒隔离。

1）USB 介质白名单及电脑 USB 接口的禁用。

2）文件白名单

3）深度检测

4）杀毒库

2. 通过 MD5 值进行校验文件在传输过程中的完整性。

3.2 解决方案概述

为避免文件传输安全威胁，对企事业单位文件交换安全应用的解决方案，从文件传输的源头---USB 移动介质文件管控，乃至文件上传、映射、摆渡至高密区。设计了三个不同应用场景的文件传输安全解决方案。

文件传输安全解决方案设计是为了使用者完全透明的文件上传、下载、共享以及交换的安全认证与权限管理服务，通过 USB 白名单、文件白名单、深度检测以及病毒库为服务器提供文件安全防护，完善的身份认证、文件读写权限控制、传输安全保护等完整的安全防御体系。

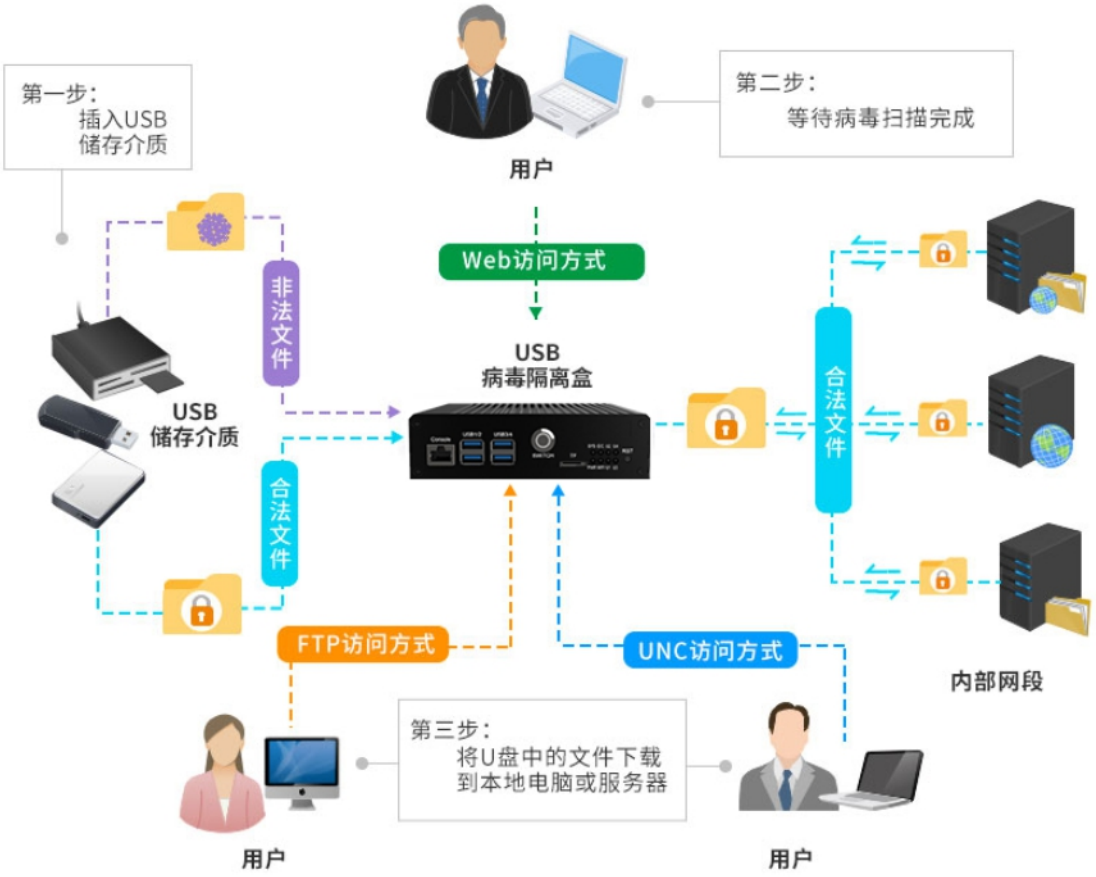
3.3 方案设置

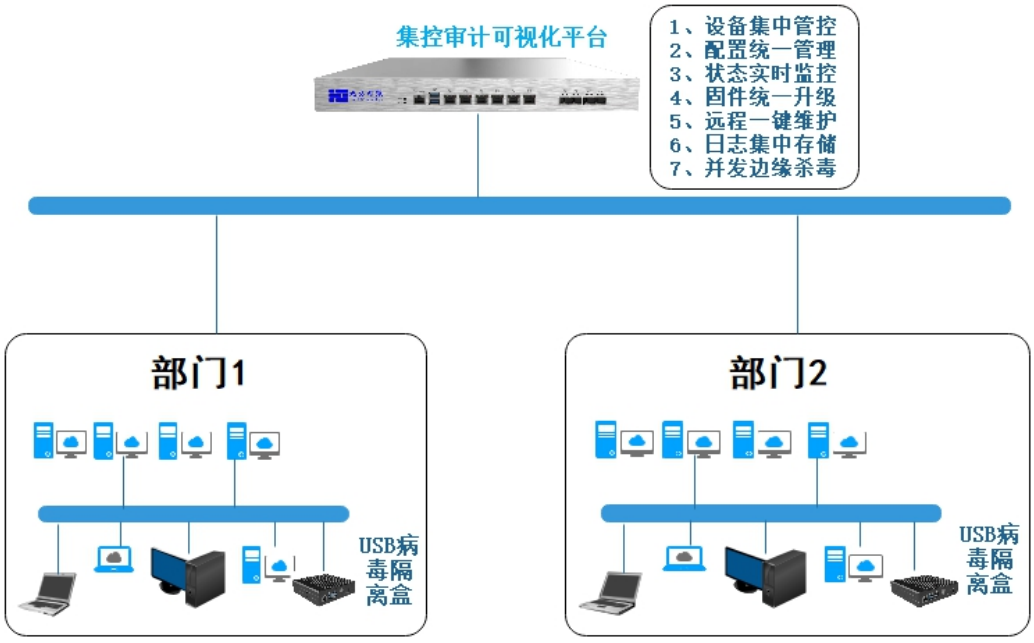
在不同的场景，企事业单位可以选择不同的设备进行文件安全管控。

3.3.1 USB 病毒隔离盒

USB 病毒隔离盒是一款专门针对 USB 存储器进行病毒隔离及查杀的产品，其通过控制 USB 移动存储介质的授权合法接入，对存储介质中的数据文件进行有效控制及实时查杀隔离并告警，并对上传下载的数据文件进行记录审计，能有效的防止 USB 移动存储器上的文件携带病毒进入内网，究根溯源，提高了内网的安全，避免出现安全事故。

系统部署拓扑图如下：


第一步：
插入USB
储存介质
用户
第二步：
等待病毒扫描完成
Web访问方式
非法文件
USB
储存介质
USB
病毒隔离盒
合法文件
合法文件
FTP访问方式
UNC访问方式
内部网段
第三步：
将U盘中的文件下载
到本地电脑或服务器
用户
用户

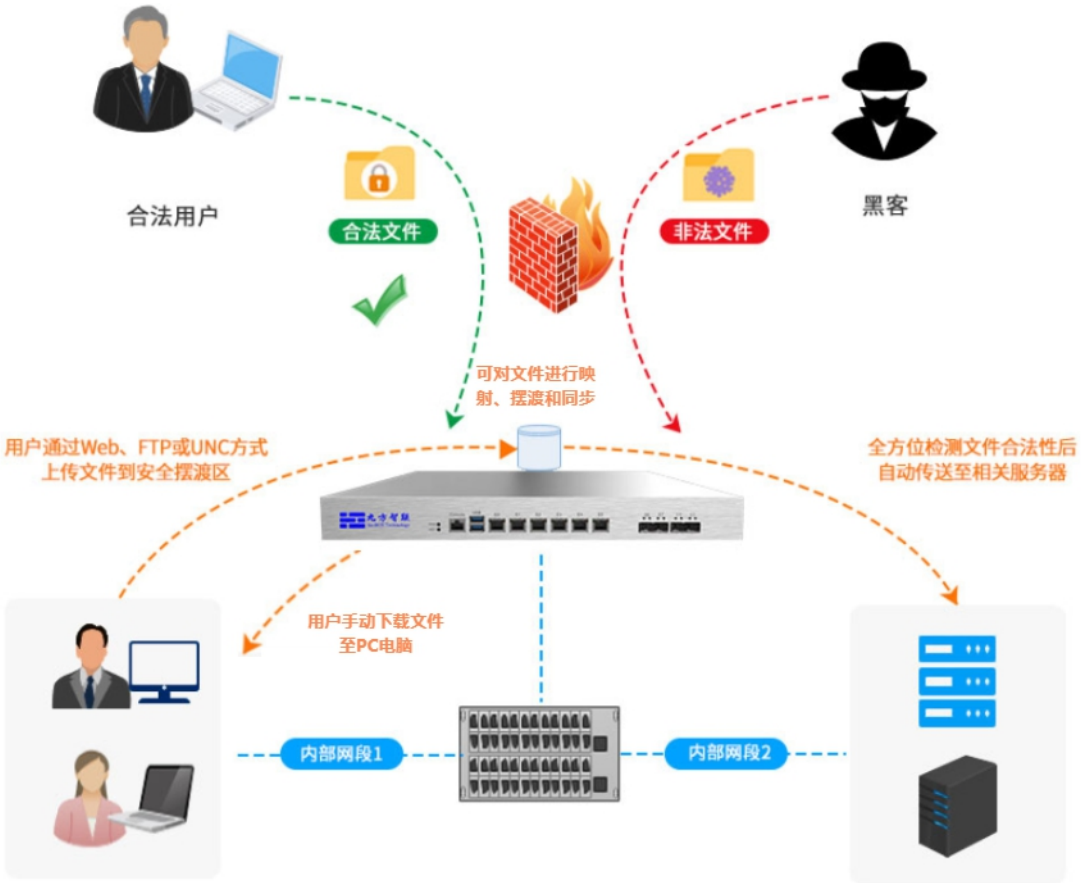

集控审计可视化平台
1、设备集中管控
2、配置统一管理
3、状态实时监控
4、固件统一升级
5、远程一键维护
6、日志集中存储
7、并发边缘杀毒
部门1
USB病毒隔离盒
部门2
USB病毒隔离盒

应用场景（带管理平台）

3.3.2 文件安全摆渡网关

"文件安全摆渡网关"是一款专门针对文件病毒检测的文件传输安全隔离产品，在很多应用场合又叫文件安全传输网关或上载摆渡网关。针对外来文件中可能存在的病毒，其先进行文件白名单的检查，然后通过病毒检测引擎的病毒查杀，最后再经过文件类型的深度检查，三层检查之后，才允许该文件在内部网络中传输，全面保障外来文件在内部网络的安全使用。文件病毒隔离网关支持直传、映射、摆渡、同步四种文件传输模式，在保障数据传输的同时，实现了数据资料的受控传输、格式检查、深度过滤、病毒查杀等安全功能，确保整个传输过程高速、安全、可控。

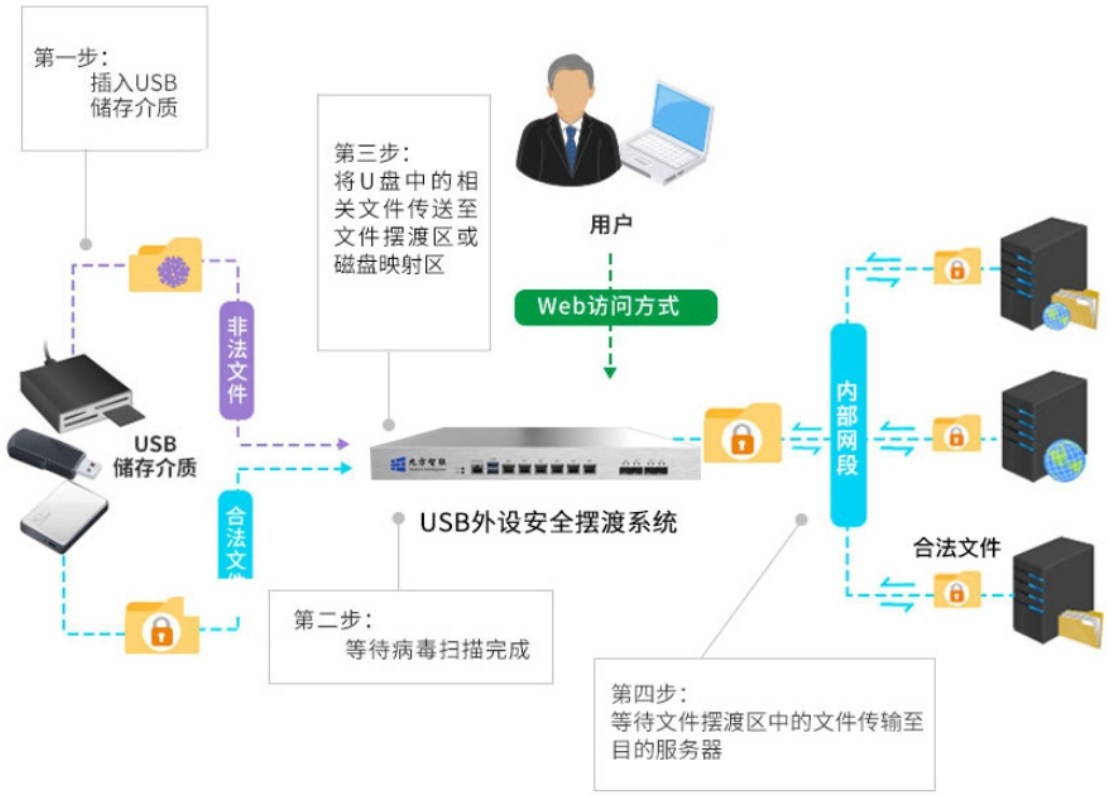
系统部署拓扑图如下：



3.3.3 USB 外设安全摆渡系统

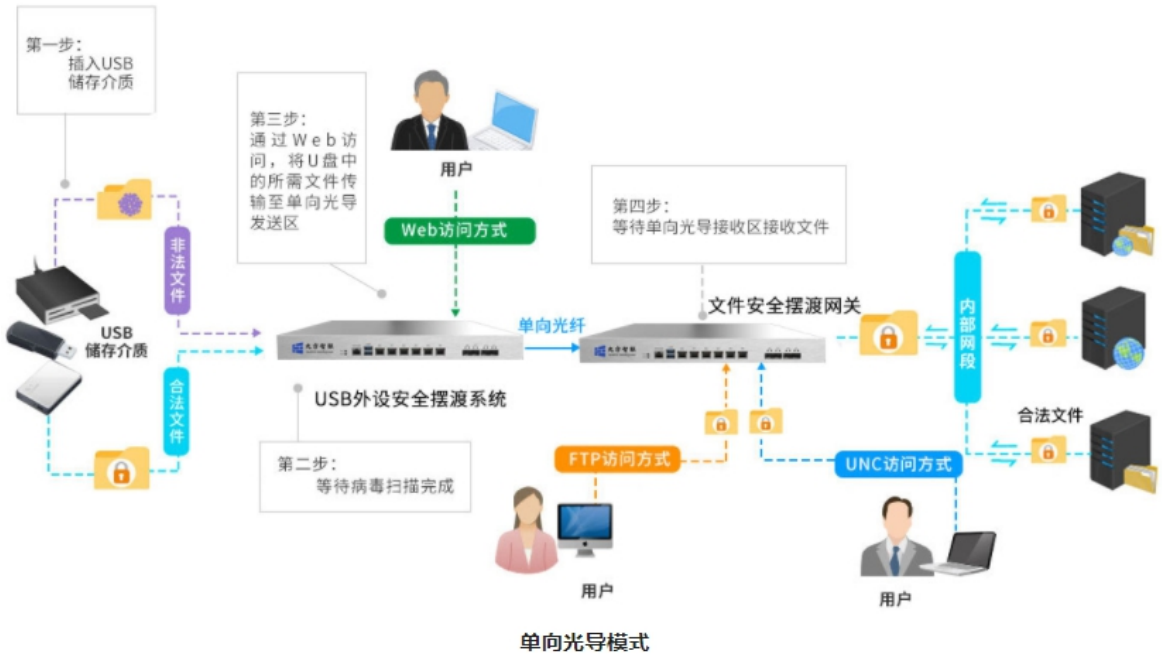
USB 外设安全摆渡系统是一款带有病毒防护及深度检测并能进行文件自动摆渡及单向光导传输功能的文件摆渡产品。其可以通过白名单来授权外来的 USB 移动存储介质的的有效接入，并对相关文件进行深度检测和病毒查杀，从而防范病毒文件在办公内网的的传播。系统部署拓扑图如下：

① 文件摆渡模式：



文件摆渡模式

② 单向光导模式：



单向光导模式

3.4 产品的主要功能模块

3.4.1 权限分配

所有产品为用户提供了三种不一样的用户，特定人员可以使用该特定人员应该使用的权限。三种不同权限的用户 admin、audit 和 user 分别对于管理员、审计员和普通用户。admin 权限用户可以对系统设置文件白名单、USB 白名单、深度检测、普通用户文件上传下载和删除权限分配、系统配置等诸多功能。审计员可以查看用户操作日志和文件行踪。普通用户只能在管理员分配的规则下进行设备操作。

3.4.2 访问控制

使用 IP 黑白名单来控制访问设备。设置白名单后，非白名单 IP 地址禁止访问设备，黑名单 IP 地址禁止访问设备。访问控制策略是保护系统安全性的重要环节，制定良好的访问策略能够更好的提高系统的安全性。

3.4.3 病毒隔离

病毒隔离主要使用以下几种方式实现：

1）USB 白名单

对接入的 USB 移动介质进行管控，需要使用的 USB 移动介质进行添加 USB 白名单，非 USB 白名单移动介质禁止读取。设备 WEB 登录界面工具栏有一个电脑端 USB 接口禁用工具，一次启动后无需电脑再次启动工具。

2）文件白名单

对经常使用的文件类型后缀进行设置文件白名单，非文件白名单文件禁止传输。

3）深度检测

基于文件内容的深度检测算法，根据文件类型和格式进行深度检查，不简单停留在后继检测，能准确快速的识别病毒伪装文件，避免危险文件通过。

4）病毒库

计算机病毒正在不断的推陈出新，其中包括一些独特的新型病毒暂时无法按照常规的的类型进行分类。所以携带的病毒库需要 24 小时不间断更新，及时更新病毒库，查杀新型病毒、变异病毒。

3.4.4 磁盘映射、文件摆渡和文件同步

磁盘映射：主要用来映射服务器的共享文件夹目录内容，用来对文件的上传、下载和删除等不同操作。（文件安全摆渡网关和 USB 外设安全摆渡摆渡系统使用）

文件摆渡：把需要传输的文件摆渡到目的服务器共享文件夹。文件摆渡后，设备上的摆渡文件和目录自动消失。（文件安全摆渡网关和 USB 外设安全摆渡摆渡系统使用）

文件同步：低密区服务器共享文件夹的文件同步到高密区共享文件夹去。

3.4.5 操作审计

操作审计管理主要审计操作人员的帐号使用情况。在设备的访问日志记录采用不同的帐号、不同的 IP 地址标识后，操作审计能更好地对操作人员的完整使用过程进行追踪。

系统通过系统自身的用户认证系统、用户授权系统，以及访问控制等详细记录整个会话过程中用户的全部行为日志。还可以将产生的日志传送给第三方。

对于生成的日志支持丰富的查询和操作：

- 支持按用户名方式进行查询

  通过对用户名进行查询，可以发现该用户的所有行为。

- 支持按登录地址方式进行查询

  通过对特定 IP 地址进行查询，可以发现该地址在设备上进行的所有操作。

- 支持按照登录时间进行查询

  通过对登录时间或操作时间进行查询，可以发现特定时间内，用户对其进行过的所有操作。

- 支持用户对文件的操作进行查询

  可以通过对文件传输方向和文件名进行查询。

- 支持对日志的下载和删除处理

3.4.6 备份配置

管理员可以配置备份文件，不小心设置配置出错时，可对系统进行恢复配置。

3.4.7 集审平台

通过集控管理多个设备，实现了高效集控管理。通过对多个设备的文件白名单管理、USB 移动介质白名单管理、用户权限、文件病毒报警、设备固件统一升级、设备日志、设备维护、设备证书等多个集控管理，实现了一平台-多管控的高效工作理念。

3.5 集控审计可视化管理平台设计理念

要解决核心资源的访问安全问题，我们首先从管理模式上进行分析。管理模式是首要因

素，管理是从一个很高的高度，综合考虑整体的情况，然后制定出相应的解决策略，最后落实到技术实现上。管理解决的是面的问题，技术解决的是点的问题，管理的模式决定了管理的高度。我们认为随着应用的发展，设备越来越多，维护人员也越来越多，我们必须由分散的管理模式逐步转变为集中的管理模式。

只有集中才能够实现统一管理，也只有集中才能把复杂问题简单化，集中管理是运维管理思想发展的必然趋势，也是唯一的选择。集中管理包括：

◆ 集中账号管理

在平台上统一设置账号，设置不同用户的文件上传、下载和删除权限，统一下发用户到各个设备中去。

◆ 集中文件安全策略管理

细粒度的白名单授权策略，针对不同的使用情况，管控各个设备的文件白名单、USB白名单、深度检测和统一病毒防护。

◆ 集中认证管理

集控审计可视化管理平台提供了多种认证方式，包括：本地认证、证书认证、哈希算法和国密算法认证。使集控审计更为安全可靠。

◆ 集中操作审计

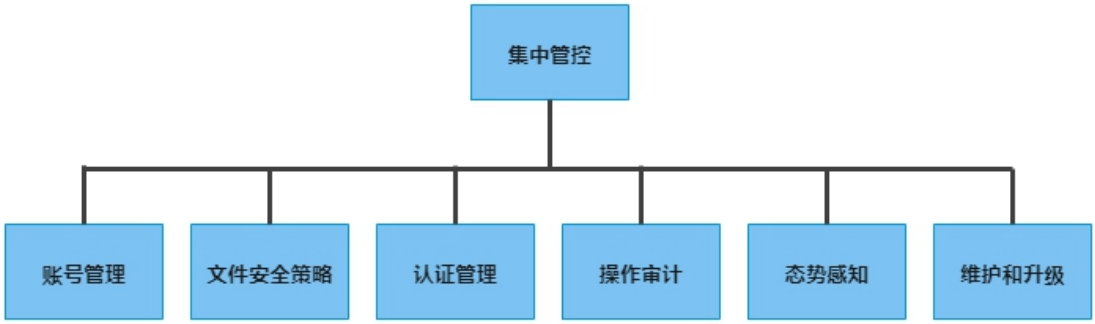
基于唯一身份标识，全程审计用户对从登录到退出的操作行为，使得事后的审计和责任的定位有了可靠有力的根据。

◆ 在线维护和统一升级

可通过平台去访问各个设备，统一升级设备，不再需要一对一复杂化运营维护设备。

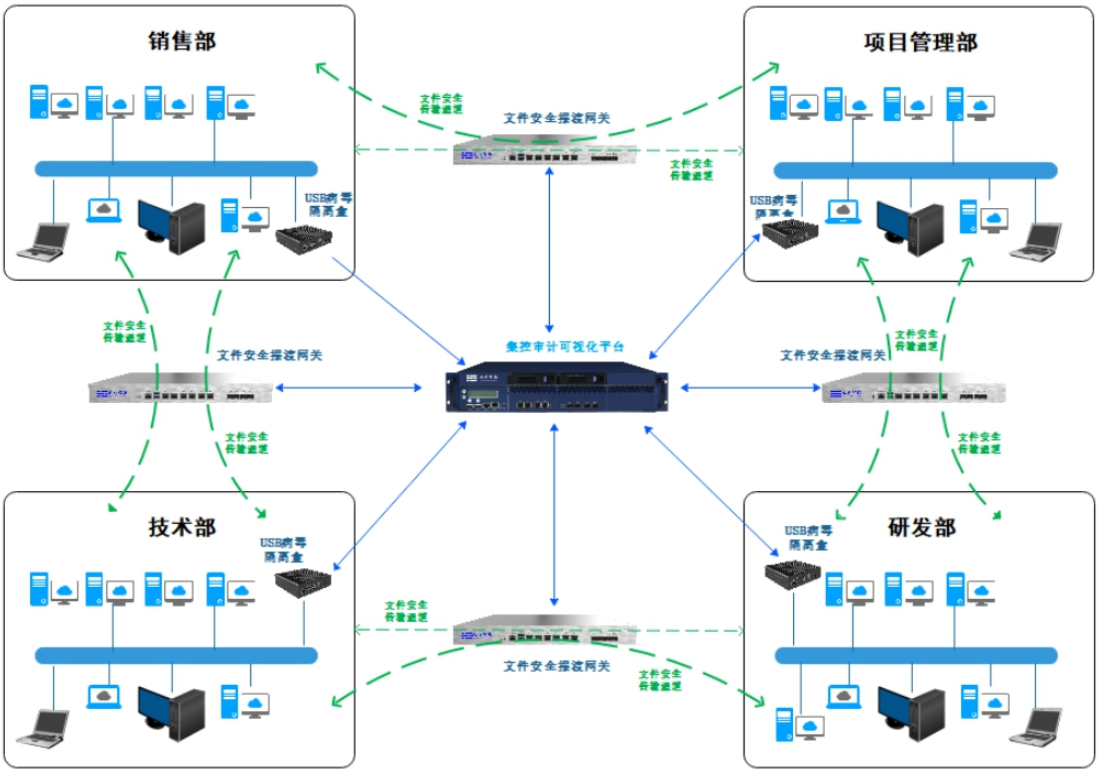
◆ 态势感知

对用户的登录、文件上传下载删除、设备接入和离线、文件智能学习、病毒报警和设备系统情况进行态势感知，发生事件实时感知。



集中管控框架

设备部署拓扑图：



四、文件安全交换及传输解决方案带来的价值

4.1 实现文件安全传输

以往的文件传输方式主要是 U 盘拷贝、FTP 服务器和 windows 下的文件共享文件夹等方式进行文件传输，在以上的传输方式中，无法在传输的过程中隔离病毒或查杀病毒。而通过九方智联文件安全传输设备，可以有效的杜绝了病毒文件传播，从源头上阻止了病毒的传播，在保障数据传输的同时，实现了数据资料的受控传输、格式检查、深度过滤、病毒查杀等安全功能，确保整个传输过程高速、安全、可控。

4.2 实现用户权限划分，避免文件拷贝和丢失

使用不同的权限划分，将管理员、审计员和普通用户区分来，管理员指定普通用户可以下载的文件类型和文件的上传、下载和删除等不同操作。

4.3 日志审计追踪，满足安全规范要求

审计员可通过 WEB 方式看到用户操作日志审计，对用户的行为全程进行记录，发生问题时有效快速追踪和定位。

4.4 方便灵活，可拓展性

不需要安装客户端，用户可以通过 WEB、FTP、UNC 方式进行登录使用设备。文件交互，使用统一的设备，实现同一内容在不同工作区域的工作人员实现文件数据交互。

4.5 实现集中管理，文件安全策略，减轻管理压力

1）实现统一的授权管理

各应用系统分别管理所属的资源，并为本系统的用户分配权限，若没有集中统一的资源授权管理平台，授权管理任务随着用户数量及应用系统数量的增加越来越重，系统的安全性也无法得到充分保证。集控审计可视化管理平台实现统一的授权管理，对所有被管应用系统的授权信息进行标准化的管理，减轻管理员的管理工作，提升系统安全性。

2）实现统一的文件安全策略

每新增一个用户或是设置文件白名单等不同操作时，没有集控平台下，运维人员需要一对一的运维设备，工作量必将很繁琐。集审平台有效的解决的这一问题，将统一的文件安全策略统一的下发到选择设备中去，大大的减少了不必要的工作量。

五、总结

内外网文件安全交换及传输整体解决方案及其相关产品可以对政府机关、企事业单位内外网文件文件安全交互提供强有力的安全保障，对于发现的病毒文件能实时告警与阻断，在发现问题时能够更快追溯并解决问题，对系统运维操作过程中的问题和责任，准确进行定位、取证和举证，对不合规的相关操作从技术上建立信息安全的重要防线。