中数国科安全管理平台
产品白皮书

（中数国科集团）

【中数国科】

■ 文档编号	■ 密　　级
■ 版本编号	■ 日　　期
■ 撰 写 人	■ 批 准 人

■ 版权声明

目录

一、前言

经过十多年的信息化与网络安全建设，大多数企业和组织已经从安全的局部建设进入到了整体优化阶段。当前的客户更加关注全网的整体安全，强调从业务信息系统安全风险的角度，而非从单一安全威胁和防御机制的角度，去更加主动地管理网络安全。而要做好整体的网络安全管理工作就需要一套相应的安全管理体系。在这个体系中除了组织保障和流程保障以外，很重要的一点就是技术保障。网络安全管理平台就是一套配合企业和组织建设网络安全管理体系的技术支撑平台。

同时，随着《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）标准的发布和实施，对于网络安全管理中心提出了明确的要求，二级及以上级别的等保系统都需要建设网络安全管理中心。这使得网络安全管理平台成为企业和组织网络安全建设中的必选项。

目前，网络安全管理平台的需求主要源于客户管理层和执行层不同角色人员对于网络安全管理工作的切身需要。

对于管理层而言，高层领导、各业务主管领导和 IT 安全主管领导等都需要从各自的角度出发，对全网或相关业务信息系统的整体安全运行状况有一个直观的了解和清晰的掌控，能够获悉当前的安全态势、攻击分布、防护缺陷，掌握安全防御体系建设的水平和安全管理能力建设的水平。

对于执行层而言，安全管理员、运维工程师、安全分析员、应急响应人员等也都需要从各自的角度出发，对网络和业务信息系统实施有计划地、持续地监视、检测、审计、分析、评估、预警、响应和报告，并能够实现相互之间的协同工作。

大家共同面临着一系列问题需要回答：

- 如何实现分散的海量安全信息采集、分析、展示？
- 如何让将离散、抽象的网络安全数据关联起来，真正实现其价值？

- 如何获悉全网的整体安全态势？
- 如何保障业务信息系统的安全？
- 如何进行积极主动的网络安全管理？
- 如何整合各种网络安全防护设备和能力？
- 如何符合并体现等级保护及信息安全管理体系的要求？
- 如何建成网络安全管理的长效机制？

二、产品概述

中数国科网络安全管理平台（以下简称中数国科安管平台）是一套提供网络安全统一管理能力的专用硬件产品，该产品可以对各种网络设备、网络安全设备、主机等进行资产管理、运行状态监控、日志收集和存储、事件分析和告警、配置管理等操作，提供一整套网络安全一体化运维管理解决方案和能力，成为用户网络安全运维管理的技术抓手，帮助用户达到网络安全等级保护相关合规要求。

中数国科安管平台整体架构分为采集器、数据分析处理单元、业务功能单元三大部分。

产品架构图

采集器主要负责与外部的系统、设备进行对接，以指定的方式方法获取其资产、性能状态、日志、配置等信息，是网络安全管理平台的数据来源。

数据分析处理单元负责对采集的数据进行范式化、归一化处理，形成统一格式的数据然后根据业务逻辑的需要进行数据的实时和异步分析，完成关联、统计、分析、告警匹配等工作，产生业务功能单元所需要的各种结果数据，用以支撑上层业务应用。

业务功能单元是系统的交互界面，面向使用者提供各种数据查询、统计呈现、报表输出和系统配置管理功能，接受用户的操作请求，与数据分析处理单元进行交互，提取相应的结果数据进行呈现和反馈。

三、产品功能

3.1 资产管理

网络空间是一个虚拟的空间，它将设备、系统、应用、数据通过一定的规则联系在一起并进行信息交互及数据传递。网络空间中的这些元素被称之为“资产”，这些资产具有数量巨大、种类繁多、分布广泛、增长迅速、使用和调拨频繁等特点，导致资产管理方面堆积了大量的问题。同时资产也是一切网络攻击最终的落脚点，任何网络入侵和攻击都是以资产为载体或目标的，因此摸清资产家底是网络安全防护的基础工作，如果网络资产都是一本糊涂账，那么网络安全保障就是无源之水，无本之木。

中数国科安管平台提供全面的资产管理功能。同时还提供了以资产为中心，聚合资产基本信息、相关的单位信息、状态、性能、日志、配置、告警、工单等数据。分层次、多维度的进行资产情况的描述和画像，帮助用户全方面、立体化的去认识和理解一个资产在网络中全生命周期的变迁，建立完整的资产台账，做到资产底数清晰。

3.2 性能和可用性监测

为了最大限度地降低对被监控系统及其网络的影响性，中数国科安管平台采用SNMP、API 等多种网络协议实时监测。支持主流 IT 和 OT 资产，包括网络设备（交换机、路由器等）、网络安全设备（防火墙、入侵防御系统、网闸等）、主机服务器、虚拟化系统、数据库、中间件、应用系统等。提供细粒度的指标监测，包括设备名称、IP 信息、运行时间、接口信息、网络状态信息、网络流量信息、网络性能信息、CPU 使用率、内存使用率、存储空间使用情况等。

通过持续不断的监测和分析，对每一个设备、每一套应用系统的健康状况进行综合的评估和呈现，形成统一的运行监测结果，支撑日常的运维管理工作。

3.3 日志管理

为了满足相关法律法规对于日志持久化存储、集中化管理和审计的要求，中数国科安管平台提供了专门的日志管理功能模块。该功能可以通过 Syslog、WMI、SNMP Trap、JDBC、FTP、Agent、http/https、API、SMB、Kafka 等采集方式实时或周期性的采集和汇聚各种主流操作系统、网络设备、安全设备、Web 服务器、数据库、虚拟平台等异构日志，并且通过统一的范式化规则引擎将来自于不同数据源的异构日志进行范式化、归一化、标签化处理，形成规范、统一的格式化数据，进行集中的持久化统一存储和管理。

基于上述采集的各类异构日志数据中数国科安管平台利用关联分析、数据挖掘、数据建模等大数据技术，通过可灵活定义的关联分析规则驱动系统对发生在不同时间、不同空间、不同日志类型、不同应用场景的海量日志数据进行异步的分析、串联、挖掘，深挖日志数据的规律和内在联系。

3.4 资产配置

安管平台一个重要职能就是提供统一的管理途径，中数国科安管平台通过集成 HTTP、

HTTPS、SNMP、SSH 等多种远程管理方式，可以对中数国科自有的工业防火墙、网闸、光闸等网络安全设备进行远程的联动管理，实现其配置的查看或变更，同时也支持第三方网络安全设备管理的对接开发。

3.5 漏洞管理

中数国科安管平台通过集成第三方漏洞扫描设备，获取扫描结果和修复建议，使管理员可以及时掌握系统中存在的漏洞和弱点，并根据扫描结果和修复建议制定漏洞修复整改方案，从而全面提升整体安全性。

3.6 告警和工单

告警和工单是中数国科安管平台中的两种“处置行动”功能模块，与资产管理、日志管理、资产监测形成联动，可以对发现的异常和问题进行告警、响应处置等操作。

中数国科安管平台提供事件告警、工单管理两个方面的处置功能，系统内置告警引擎和告警服务，资产管理、日志管理、资产监测等环节可以通过调用告警引擎和告警服务，直接或间接的触发系统消息、邮件、短信等告警。告警信息可以转换为工单，下发到对应的单位或个人进行处理、反馈，并可以实时跟踪工单处理和响应的过程，形成网络安全管理流程的闭环。

3.7 数据报表

中数国科安管平台报表模块支持报表的订阅功能。系统开放所有数据，提供基础的图表模板，网络安全管理的不同角色人员可以根据自己的业务和管理需要将数据和图表进行组合，指定报表内容、报表格式、数据范围、图表形式、生成时间等，制作自己所需要的

日常数据报表，系统会根据配置要求定期生成相应的报表，并以电子邮件的形式投递，满足网络安全决策层、管理层、技术执行层不同的数据汇总需要。

3.8 安全知识库

中数国科安管平台提供开放的安全知识管理功能，包括安全知识、安全事件、漏洞、补丁等网络安全信息，辅助用户完成安全决策。用户可以在日常运维管理过程中不断丰富和完善知识库体系和内容。

四、关键技术

4.1 完善的数据采集与治理

采集网络空间中海量、异构、高速的日志数据。日志采集层支持分布式采集，提供分布式消息队列保证数据采集性能。

通过各种渠道和途径汇聚的海量数据存在以下问题：

- 不同业务数据的数据格式定义并不完全相同；
- 不同途径获取的数据存在重复、包含，甚至矛盾的情况；
- 非结构化数据中存在许多可用于关联分析的线索，但因其存储空间大、保存时间短，难以充分有效发挥作用；
- 海量数据中存在不少无法处理或者没有价值的垃圾数据，降低了整体数据的利用率。

针对以上情况需要进行数据预处理，即对数据进行规范化、归一化、去重、补全、过滤和归并等数据处理过程，提取其中有效的信息，剔除无用的数据。

数据的**清洗过滤**包括三个方面：

- 清洗：针对数据格式的不一致、数据输入错误、数据不完整等问题，支持对数据进行转换和加工。常用的数据转换组件有字段映射、数据过滤、数据清洗、数据替换、数据计算、数据验证、数据加解密、数据合并、数据拆分等；
- 修改：错误数据，产生原因是业务系统不够健全，在接收输入后没有进行判断直接写入后台数据库造成的，比如数值数据输成全角数字字符、字符串数据后面有一个回车、日期格式不正确、日期越界等；
- 删除：重复性数据。

对于安全事件数据清洗与过滤功能包括但不限于：

- 不属于大数据平台数据源中的数据；
- 重复数据；
- 噪音数据；
- 数据不完整或不合理性的数据；
- 低于业务需求的最低级别以下的数据。

对异构原始数据进行统一格式化处理，以满足大数据平台存储层数据格式定义的设计对于被标准化的数据应保存原始日志。

数据标准化的原则包括但不限于：

在保证基本扩展能力的基础上，根据每种类型数据的标准库规则，实现相关字段的标准化；

对于常用的字段，保证字段内容的一致性，消除不同威胁对于相似问题描述的不一致性，满足依赖于这些字段的规则的可移植性。未被标准化的数据应保存原始日志。可用于事后为该特定数据再定义标准化规则。

此外，日志审计系统再采集 UDP 数据包时，可不打开 UDP 端口实现使用 java 程序接手和处理 udp 数据。在数据链路层抓包，而 UDP 数据传输是一种“非面向连接的数据传输协议”，无需接收端设备打开相应端口，无需提前建立连接，只要网络可达，即可将数据传输

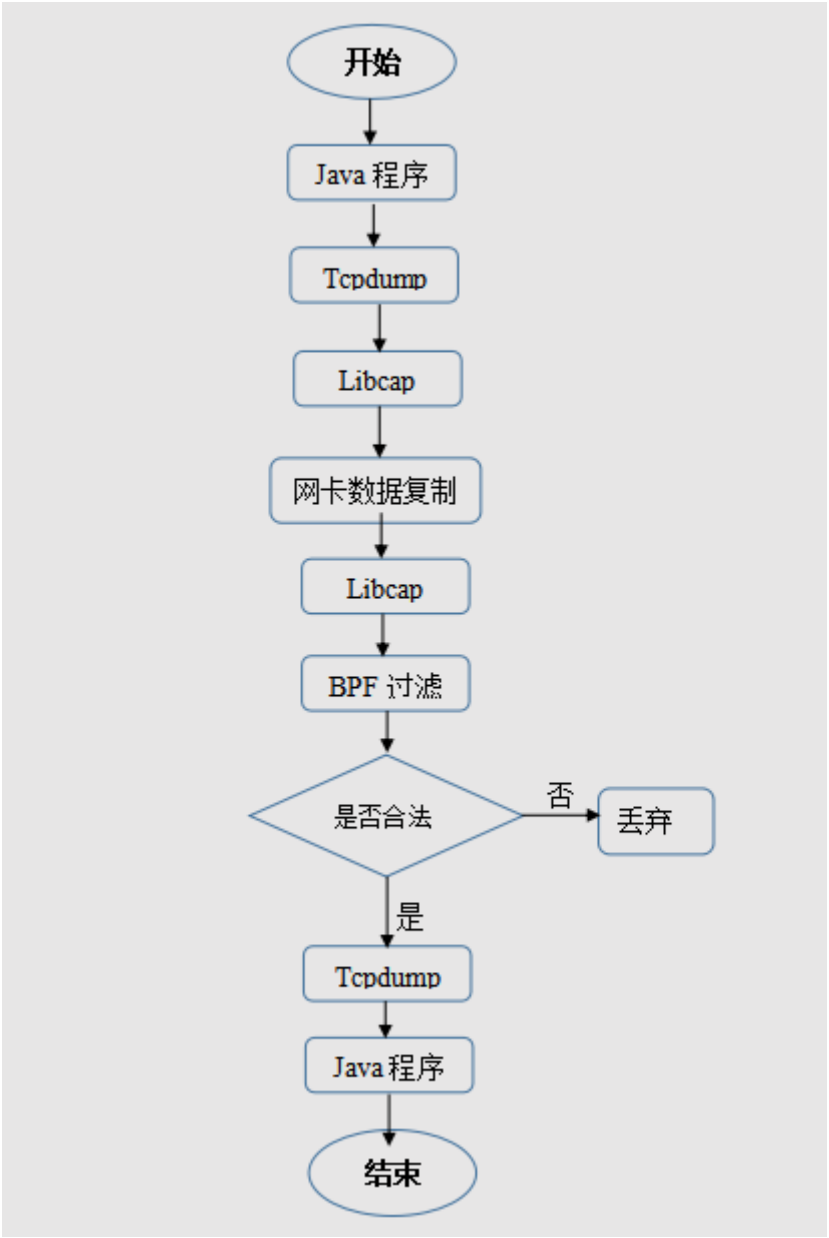
至目标设备的物理层（网卡），物理层在向“网络链路层”传输数据时，尚不考虑本机相应端口是否打开，此时数据就被复制到“BPF 过滤器”。

此技术方案优点：

无需打开相应的 UDP 端口，就能采集 udp 数据，从而增加系统的安全性,少开一个端口，就能增加一份安全。

直接从数据链路层抓取数据，而非从应用层采集数据，大大提高了数据采集效率。

利用 tcpdump 的分析结果，在其基础上进行二次分析，能够提高数据分析处理效率。



4.2 快速展示日志数据的方法（专利）

在日志采集过程中，不同类型的设备，所发出的日志格式千差万别，这给前端界面对他们的展现、查询等处理增加了难度。传统的做法是，给每一种类型的数据专门做定制的展现和查询页面，这种开发方式有以下弊端：

（1）极大的增加了前端程序开发的工作量和难度，有多少种数据类型，就需要开发多少种页面；

（2）由于前端页面的增加，前端页面的体积就会较大，浏览器页面加载及渲染速度就会变的缓慢，用户体验不佳；

（3）缺乏灵活度，在客户现场实际使用的过程中，遇到新的没有被支持的数据格式，是比较常见的，这样就定制开发新页面，开发及部署周期较漫长，极大的影响了客户的体验。

为此，日志审计系统采用一种快速展示页面的方法，通过创建一个数据分析处理页面组来分析和处理各种类型日志数据的特征，然后将他们的特征、数据逻辑关系自动存储在后台数据库中，前端页面在展现时，根据这种逻辑关系就能自动生成展现页面和查询页面，如果遇到新的未处理过的数据，只需要将他们的特征数据通过界面设置，之后对他们的前端处理，就能够自动生成，完全不需要再次进行前端开发。

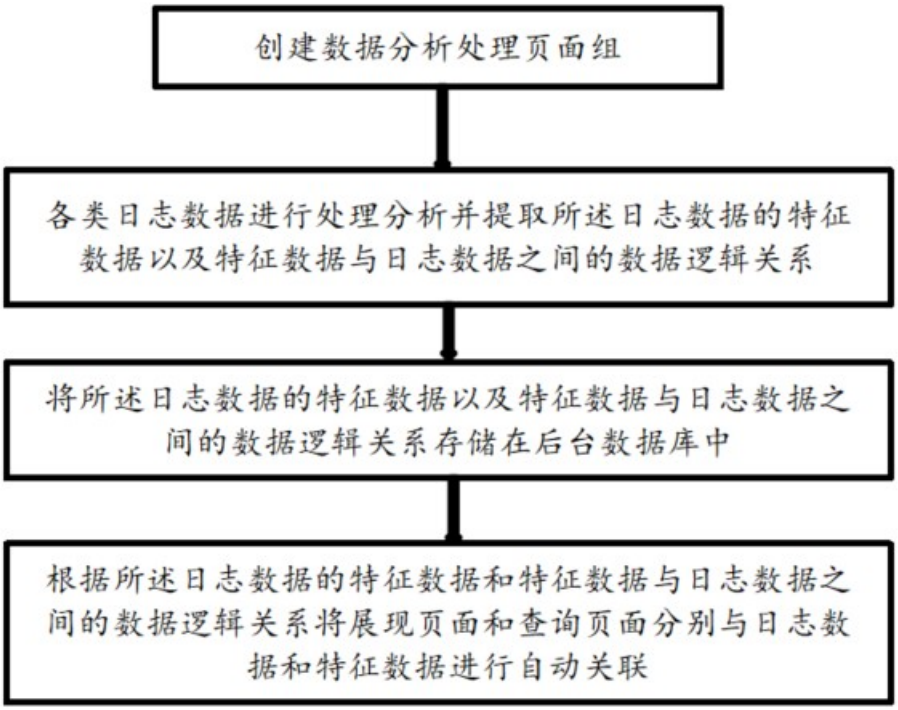
通过使用此技术，日志审计系统取得了如下有益的技术效果：

1、减少前端工作量：页面的数据展示都通过后端数据库存储的逻辑关系自动生成 ，不需要每种日志开发一个页面；

2、减少了前端页面的体积，提高了浏览器的加载及渲染速度；

3、灵活便捷：遇到新的数据，只需要进行简单的页面设置，就能够完成对新数据的支持，甚至经过简单培训，用户自己都可以完成配置，极大的增加了用户好的体验；

4、减少了售后支持的工作量和难度，降低售后支持的成本。



4.3 基于大数据技术的日志数据存储

数据存储层将采集的日志数据根据数据处理的需要保存在相应的数据库中。

数据存储层支持不同类型的大数据的存储，这些数据包括结构化和非结构化数据，关系型和非关系型数据，实时数据和历史数据。服务于后续的监测分析，系统使用多种数据存储技术，使用非关系型数据库 ElasticSearch 存储采集数据，使用非关系型数据库 Redis 存储缓存数据。

ElasticSearch 是一个基于 Lucene 的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于 RESTful web 接口。可作为 Restful API 标准的可扩展和高可用的实时数据分析的全文搜索工具使用。分布式实时文件存储，可将每一个字段存入索引，使其可以被检索到。实时分析的分布式搜索引擎，分布式：索引分拆成多个分片，每个分片可有零个或多个副本。集群中的每个数据节点都可承载一个或多个分片，并且协调和处理各种

操作；可以扩展到上百台服务器，处理 PB 级别的结构化或非结构化数据。

日志审计系统具备快速自定义的各种形式搜索，而不局限于固定几种的字段，系统可以自由选择搜索策略，保存搜索策略，可以指定字段及条件进行搜索，同时支持字段组合搜索。系统支持普通搜索、高级搜索两种方式，通过即时查询，立即产生搜索结果，操作简洁易用。

Redis 数据库是非关系型数据库，将数据存储在缓存中，读取速度快是其最大的优点。日志审计系统在 Django 中需要引入第三方扩展 django-redis 来使用。redis 适用于存储使用频繁的数据，这样减少访问数据库的次数，提高了运行效率。

4.4 基于分布式架构的日志关联分析

分析计算提供计算模型和计算方法。分析方法包括关联分析、数理统计分析、数据挖掘等。其中日志审计关联分析方法包含：基于规则的关联分析、基于统计的关联分析、基于行为的关联分析、数量统计分析等。

- **基于统计的关联分析**

基于规则的关联分析是指将可疑的安全活动场景（例如某潜在安全攻击行为的一系列安全事件序列）加以预先定义，系统能够使用定义好的关联性规则表达式，对收集到的安全事件进行检查，确定该事件是否和特定的规则匹配。基于规则的关联分析即可用于识别单个安全事件的场景，也可用于识别多个安全事件组成的场景。

在基于规则的关联分析过程中，安全专家制定规则形成规则库；规则驱动关联引擎分析安全事件，形成关联事件。规则采用如下产生式规则形式：

IF　条件　THEN 结果

其中，条件为安全别事件中某些属性的限制条件，即规则的激活条件，具有检测事实

存在与否、比较事实、根据标志检验事实等功能。条件可以由单个检测属性组成，也可以由多个检测属性组成，且各属性用逻辑符号 OR、AND、NOT 来表示多属性的逻辑关系。结果是新证据的断言或某个用户行为的可疑度，具有产生一条高优先级关联威胁的功能。

- **基于统计的关联分析**

统计关联是指在给定的时间范围内，发生符合某种条件的威胁次数超过设定值而产生报警的过程。统计关联主要是针对系统中的事件计数，通过定义门限值，统计在一定时间间隔内事件发生次数。如果系统发生事件超出了正常设定的门限值，就认为系统出了异常。

在统计关联分析过程中，首先定义一些大的安全事件类别，对每个类别的事件设定一个合理的阀值，将出现的事件先归类，然后进行缓存和计数，当在某一段时间内，计数达到该阀值，可以产生一个级别更高的关联事件。

基于统计关联的关联模型如下：

在基于统计的关联分析过程中，统计关联引擎统计固定时间长度中安全事件数量是否达到统计阀值 N，如果超过 N，生成关联威胁。

- **数量统计分析**

数量统计分析是指采用统计学方法，对各类威胁的状态、频次、发生周期等数据量化特征进行计算、得出威胁数据的分布状况、主要特征、时间序列的趋势性、是否存在异常值、威胁汇总结果等内容，威胁统计分析结果可直接用于威胁性质的判定、解释和决策。

- **基于行为的关联分析**

基于行为的关联分析用于在海量告警数据中发现攻击活动背后逻辑，发现其攻击步骤与预测其下一步攻击行为。

网络入侵行为通常是一系列的攻击，或者是组合式攻击，这些攻击都不是孤立的，而是表现为不同的阶段，前一阶段为后一阶段作准备，也就是攻击之间存在某种因果关联关系。因此，要对安全监控告警信息进行处理，以进行全局性分析。

大量的入侵案例表明入侵通常分为 4 个阶段：收集目标系统信息、进入系统、提升权限、放置后门和清理日志。例如黑客准备攻击一个网络，首先其可能会发动 IPSweep 攻击，来确定网络中的哪些主机可以被访问的，接着发动 Portscan 攻击可以发现感兴趣的那些主机向外提供了一些什么服务；然后再发动 Sadmind Ping 攻击，看看这台服务器上是否存在 Sadmind 漏洞，若存在，就可以利用这个漏洞发动 SadmindBOF 缓冲区溢出攻击，使攻击者非法获得授权的访问权限（如一般合法用户的权限或 root 权限）或得到一定权限的 shell；进一步利用已经得到的访问权限，在服务器上放置木马，留下后门等。在这个黑客的攻击过程中， IDS 等告警设备可能在每个阶段都产生了一系列报警，然而它却无法知道这些报警之间的关系，也就是说无法揭示深层次的攻击策略。

对于上面提到的问题，可以通过行为关联的方法来解决。行为关联分析就是要找出报警信息之间的这些关系，对于存在关联关系的告警信息就要提取出攻击步骤和策略，从而化简告警信息，提供给管理员更加直观的、深层次的信息。

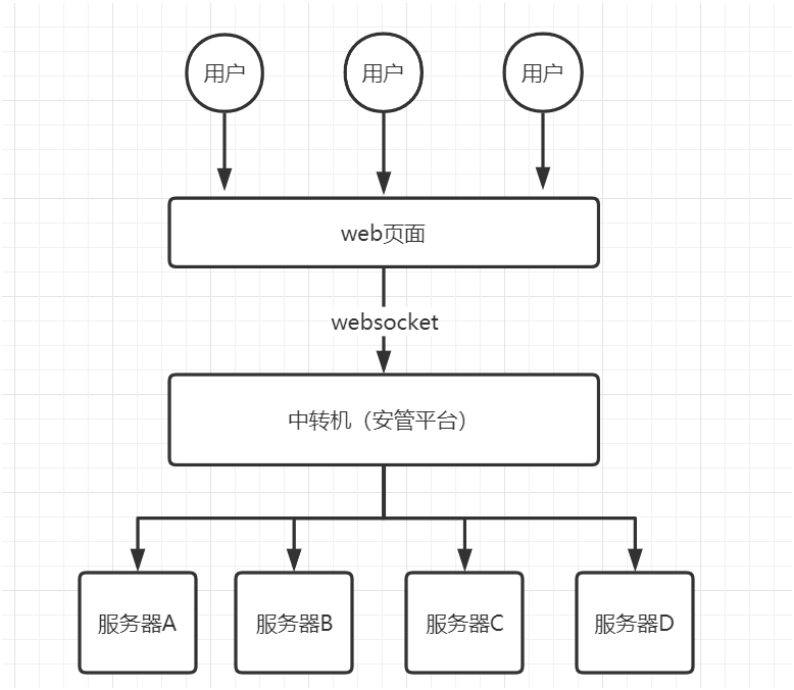
4.5 通过 Web 页面连接 ssh 服务器实现设备集中管理

安管平台采用通过 web 页面连接 ssh 服务器方式其他安全设备的集中管理功能。

通过开发浏览器插件或者第三方 js 工具来实现，开发难度大，第三方工具也会带来安全隐患。而 web 端直接和其他服务器连接，也容易带来安全隐患。同时在在用户现场，都

会安装防火墙等安全设备，而 web 端的 ip 地址一般不固定，这种情况会为防火墙的规则配置带来难度，因此，日志审计系统通过通过 web 页面通过 ssh 连接其他服务器，进行维护和管理。

原理流程如下图所示；用户想对其他服务器进行操作时，首先通过中转机和其他服务器连接，然后 web 页面通过加密的 websocket 协议和中转机连接，从而间接实现通过 web 页面和其他服务器连接，进行运维管理服务。



技术方案优势；

- 无需将被维护的服务器的登录用户名和密码传递至 web 页面，从而不会泄露重要信息。
- 无需第三方插件，开发难度减少，也减少了第三方工具带来的安全隐患。
- 采用基于 ssl 的 websocket 协议和中转机通讯，有效防止信息泄露，保证数据安全。

- 只需通过一台中转机就可以实现与其他所有服务器建立连接，给防火墙等安全设备的规则配置带来便利，增加了实际应用的可行性。

4.6 使用 NFS 与快照技术（Snapshot）对日志数据进行迁移与备份

通过使用 NFS，用户和程序可以像访问本地文件一样访问远端系统上的文件，使得每个计算机的节点能够像使用本地资源一样方便地使用网上资源。换言之，NFS 可用于不同类型计算机、操作系统、网络架构和传输协议运行环境中的网络文件远程访问和共享。

日志审计系统用到的 NFS 的工作原理是使用客户端/服务器架构，由一个客户端程序和服务器程序组成。服务器程序向其他计算机提供对文件系统的访问，其过程称为输出。NFS 客户端程序对共享文件系统进行访问时，把它们从 NFS 服务器中“输送”出来。文件通常以块为单位进行传输。其大小是 8KB（虽然它可能会将操作分成更小尺寸的分片）。NFS 传输协议用于服务器和客户机之间文件访问和共享的通信，从而使客户机远程地访问保存在存储设备上的日志数据。

传统上一直采用数据复制、备份、恢复等技术来保护重要的数据信息，定期对数据进行备份或复制。由于数据备份过程会影响应用性能，并且非常耗时，因此数据备份通常被安排在系统负载较轻时进行(如夜间)。另外，为了节省存储空间，通常结合全量和增量备份技术。显然，这种数据备份方式存在一个显著的不足，即备份窗口问题。在数据备份期间，企业业务需要暂时停止对外提供服务。随着企业数据量和数据增长速度的加快，这个窗口可能会要求越来越长，这对于关键性业务系统来说是无法接受的。降低数据保护的代价，提高数据保护过程中的应用感知能力，逐步成为客户的核心诉求，因此需要将数据备份窗口尽可能地缩小，甚至缩小为零。而数据快照(Snapshot)技术，就是为了满足这样的需求而

出现的数据保护技术。

快照是指关于指定数据集合的一个完全可用拷贝，该拷贝包括相应数据在某个时间点（拷贝开始的时间点）的映像。快照可以是其所表示的数据的一个副本，也可以是数据的一个复制品。从更具体的技术细节来讲，快照是指向保存在存储设备中的数据的引用标记或指针。日志审计系统使用 Snapshot 快照首先将原有的内容读取出来，写到另一位置处（为快照保留的存储空间，此文中我们称为快照空间），然后再将数据写入到存储设备中。而下次针对这一位置的写操作将不再执行复制操作，从 COW 的执行过程我们可以知道，这种实现方式在第一次写入某个存储位置时需要完成一个读操作（读原位置的数据），两个写操作（写原位置与写快照空间），如果写入频繁，那么这种方式将非常消耗 IO 时间。因此可推断，如果预计某个卷上的 I/O 多数以读操作为主，写操作较少，这种方式的快照实现技术是一个较理想的选择，因为快照的完成需要较少的时间。

五、产品亮点

5.1 “四位一体”的全方位网络安全管理手段

中数国科安管平台汇集资产管理、资产性能和可用性监测、日志管理、资产配置四个方面的功能，全面覆盖网络安全日常管理工作的需要，帮助用户实现目标清晰、状态准确实时、日志集中持久存储管理、统一配置管理的网络安全防护目标。

5.2 全面满足等级保护合规要求

安全管理中心是等级保护 2.0 中重点强化的环节，对于二级及以上等保系统是必备的网络元素之一。中数国科安管平台全面的满足等级保护技术标准中对于安全管理中心在资源管理和监测、安全事件管理、风险管理、设备策略管理、审计管理、自身安全性等方面的

要求。

5.3 完善的网络安全运维管理闭环

中数国科安管平台在“事前”监测资产状态、日志数据采集和大数据分析，及时预警响应，在“事中”进行安全事件告警响应，并通过下发工单责任到人进行处置和整改，在“事后”支持数据报表导出，以便统计和复盘。通过“事前”预警、“事中”处置、“事后”统计的管理手段形成完善的网络安全运维管理闭环。

5.4 基于海量日志特征的实时关联分析

中数国科安管平台内置海量日志事件动作库与关联分析规则，通过日志特征条件自定义日志事件策略形成动作库，作为关联规则的基础元素，可被重复使用，支持将异构日志进行实时解析与事件匹配。

支持针对 Windows、Linux/Unix、网络设备、安全设备、数据库、Web 服务器、虚拟平台等数据源产生的日志事件进行多维度的关联分析，通过建立异常行为分析模型与系统潜在危害分析模型，将网络系统中的登录、访问、操作、攻击威胁、异常情况等事件进行关联匹配，形成关联分析事件，并支持生成告警。

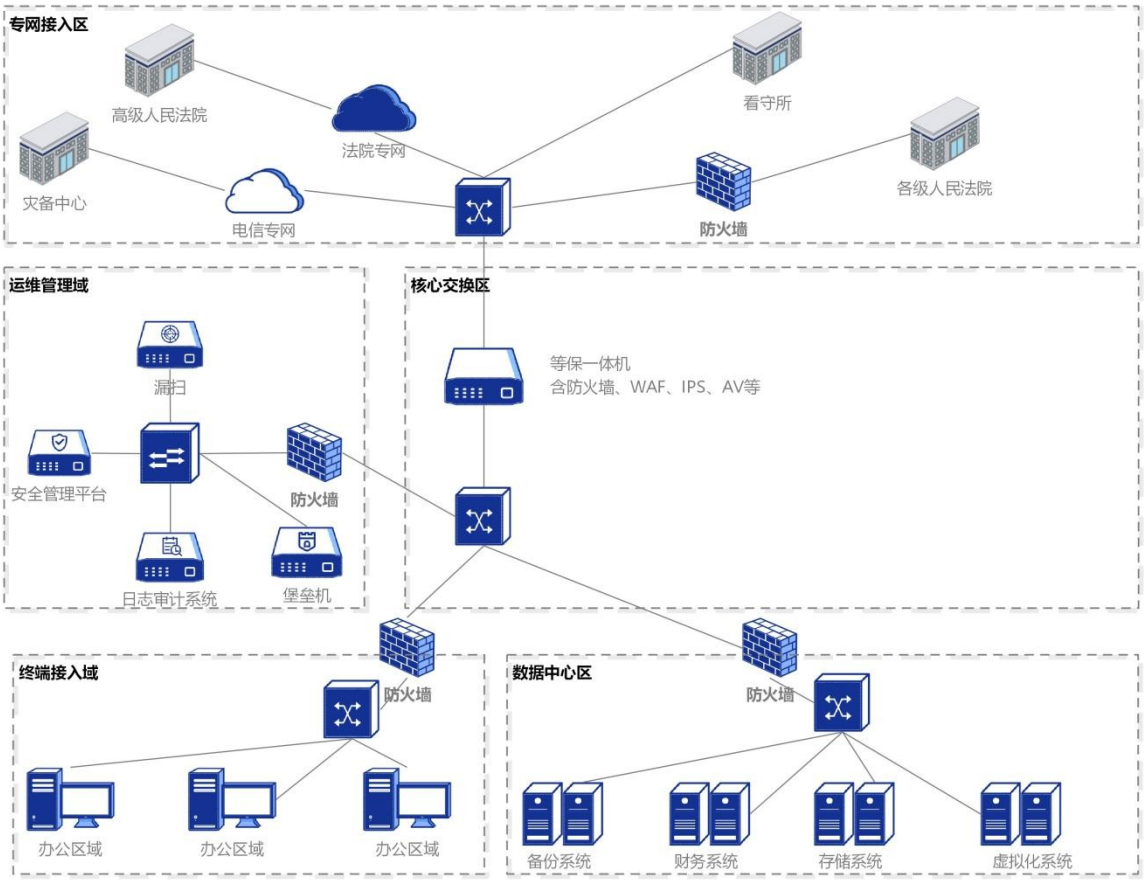
5.5 全面的日志采集能力

中数国科安管平台支持采用 Syslog、WMI、SNMP Trap、JDBC、FTP、Agent、HTTP/HTTPS、API、Kafka 方式，实现对各种主流操作系统、网络设备、安全设备、Web 服务器、数据库、虚拟平台等异构日志的采集，适用于传统网络，也适用于工业网络的日志收集与审计。

六、应用场景

6.1 法院行业场景

需求：法院业务专网属高度机密网络，如果遭受攻击、病毒、入侵造成数丢失、泄漏将会对社会造成不可弥补的损失。根据《网络安全法》、《人民法院非涉密重要信息系统安全等级保护定级工作指导意见》、《人民法院信息安全保障总体建设方案》、《信息系统等级保护基本要求》的相关要求，需通过安全建设，满足等保的相关要求。



方案拓扑图

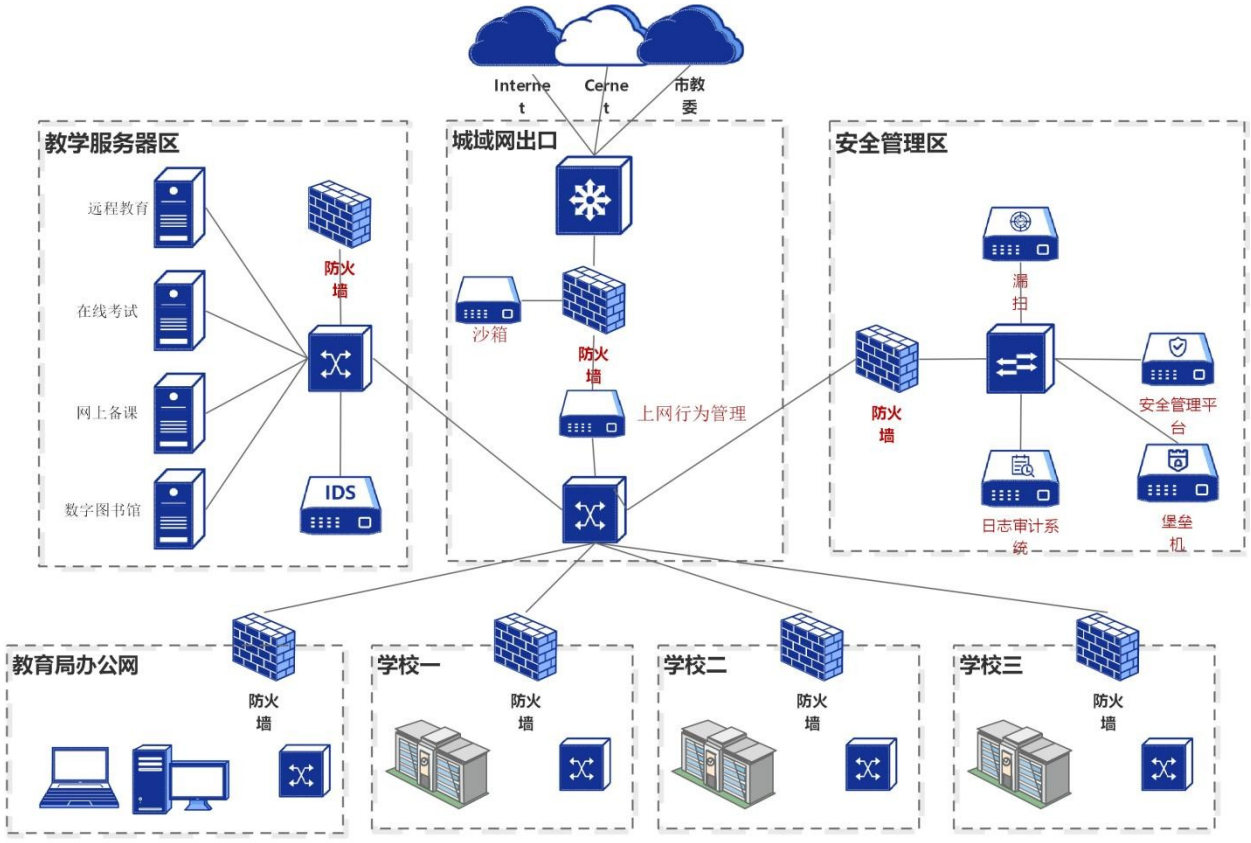
解决方案：如上图所示：

运维安全域部分：部署防火墙设备，做到管理区边界隔离；部署堡垒机，运维权限集

中管理，运维行为全程审计；部署漏洞扫描系统，及时发现网络设备漏洞；部署日志审计系统，记录和查询网络安全日志，符合国家网络安全法和公安部 151 号令要求；部署**中数国科安全管理平台**，对网络设备进行统计监控与管理。

6.2 教育行业场景

需求：计算机网络技术和管理信息化的发展，使我国的普通教育逐步进入新时代，数字化校园成为未来的发展方向，普通教育实现管理网络化、教育手段现代化。伴随高校网络规模的扩大，稳定的校园网络和计算机系统成为重要的基础设施，计算机病毒、黑客、系统漏洞等网络不安全因素对数字化校园建设存在严重威胁。根据《网络安全法》、《教育信息化“十三五”规划》、《信息系统等级保护基本要求》的相关要求，需通过安全建设，满足等保的相关要求。



方案拓扑图

解决方案：如上图所示：

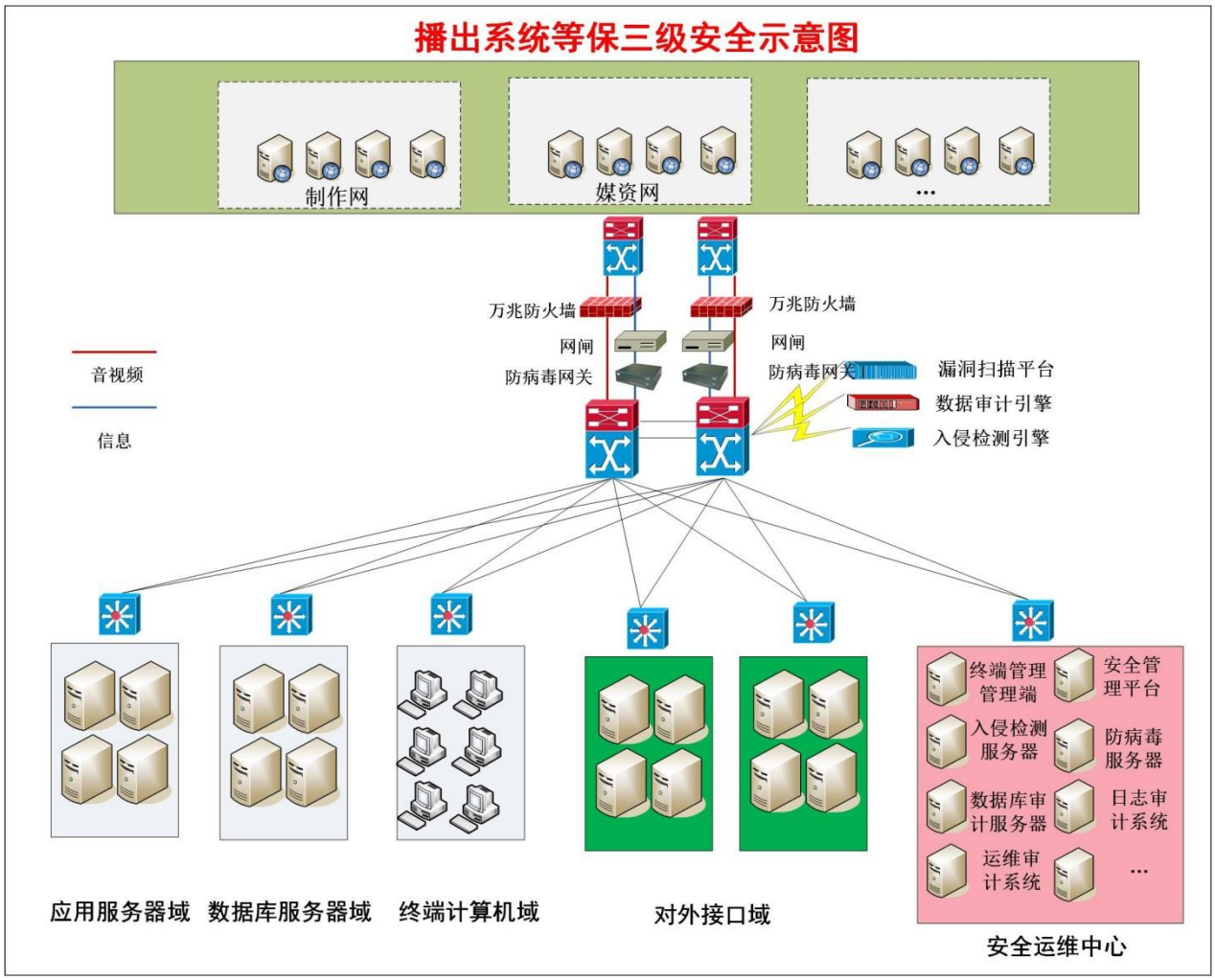
城域网出口：出口布置防火墙，提供访问控制功能；部署上网行为管理，对教育城域网师生的上网行为进行管控审计；部署沙箱，对未知文件进行识别，发现防火墙等设备没有识别的未知威胁，保证城域网安全。

数据中心：部署防火墙设备，做到数据中心边界的访问控制；部署 IDS 设备，有效检测针对信息系统的各种攻击，如病毒、木马等。

安全管理区：部署防火墙设备，做到管理区边界隔离；部署堡垒机，运维权限集中管理，运维行为全程审计；部署漏洞扫描系统，及时发现校园网络设备漏洞；部署日志审计系统，记录和查询校园网络安全日志，符合国家网络安全法要求；部署**中数国科安全管理平台**，对网络设备进行统计监控与管理。

6.3 广电行业

需求：作为信息技术与广电行业技术相结合的产物，网络安全工作的重要性日益彰显，广电总局于 2011 年发布了《广播电视安全播出管理规定》（总局令第 62 号），明确提出要开展信息系统等级保护工作。



案例拓扑图

解决方案：如上图所示：

在系统边界部署防火墙，对进入系统的数据包进行细粒度的访问控制。部署隔离网闸与单向网闸（单向网络隔离与交换系统），实现相关系统内、外的安全隔离和文件的安全摆渡；在相关系统边界部署 IDS 系统，对进入相关系统的入侵行为进行监控，并将告警信息发送至安全管理中心；部署日志审计系统、堡垒机，对相关系统接入交换机、服务器、安全设备的运行状况、用户行为等重要事件进行安全审计。部署**中数国科安全管理平台**，对网络设备进行统计监控与管理。

方案根据国标与广电总局行标等级保护标准的要求，帮助用户从全局视角进行网络安全相关的运维支持和安全服务，进一步提高电视中心信息安全管理和运维的能力，同时满

足用户对信息安全系统的审计合规需求。