安恒信息
DAS-security 安全中国

明御综合日志审计分析平台产品

V3.0.3

产品白皮书

文档版本：01

发布日期：2023-04-21

文档说明

产品名称		明御综合日志审计分析平台	
适用平台/版本			
拟制人		评审组	
发布人		备注	公开

修订记录

日期	修订版本	修改记录	修改人
2022-04-27	01	初次发布	
2023-04-21	02	修订-修改部分错别字	陈岳军

目 录

前言

概述

感谢选择安恒信息的网络安全产品。本手册对明御综合日志审计分析平台产品进行了简单介绍，主要包括背景信息、产品简介、产品功能、产品特点以及典型应用场景。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于期望了解明御综合日志审计分析平台产品的读者，包括网络安全工程师、运维技术售后工程师、运维技术售前工程师以及网络安全技术爱好者等。本文假设读者对以下领域的知识有一定了解：

- 日志分析
- 网络安全知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段
- 网络安全产品的原理及使用方法……

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310051

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1 背景信息

1.1 市场现状

随着政府、交通、电信、能源、金融、医疗等关键行业和企业信息化建设的大力推进，《网络安全法》及“等保 2.0”政策的正式实施，日志审计产品作为满足合规要求的重要产品，市场需求量快速增长。根据 CCID 报告显示，2019 年达到 11.5 亿元，增速为 27.8%，中国日志审计产品市场仍将保持高度增长的速度，预计 2022 年将达到 22.9 亿元。

1.2 风险挑战

随着现代数字化转型的快速发展，在云计算、大数据、IOT 的大趋势下，各种网络攻击、信息安全事故发生率也在不断攀升，攻击手法也逐渐向专业化和产业化的方向靠拢，如何保障信息系统的安全是所有单位和组织都关注的问题，日志作为系统运行和网络访问时产生的重要事件记录，对于排障有着天然优势，大量安全事件的发生都留有日志痕迹。当前，企业和组织在安全建设过程中已部署了大量的基础设施，但仍面临以下痛点：

- 海量繁杂-日志无法有效管理：日志来源不仅包括安全设备及各个系统，还包括各类传感器和移动客户端，每天产生巨大的日志量，且不同的日志格式纷繁复杂，无法进行统一管理。
- 信息孤岛-日志无法关联：各个设备独立分散、各自为政，日志无法进行关联以找到其中的关联共性。
- 大量误报-关键告警淹没：从各个设备上接收到的告警日志多种多样，其中不乏大量误报，致使关键告警被淹没。
- 多种界面-高成本低效率：排查安全事件时，需要登录一台台设备进行日志的查看与排错，多个界面的操作使得排查效率低，成本高，难以发现真正的安全威胁。

2 产品介绍

2.1 产品简介

明御®综合日志审计分析平台（简称 DAS-Logger）作为信息系统的综合性管理平台，通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营安全；明御®综合日志审计平台通过基于国际标准化的关联分析引擎，为客户提供全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，为客户提供真正可信赖的事件追责依据和业务运行的深度安全。同时提供集中化的统一管理平台，将所有的日志信息收集到平台中，实现信息资产的统一管理、监控资产的运行状况，协助用户全面审计信息系统整体安全状况。

明御®综合日志审计分析平台旨在实现网络资产安全状况的统一管理，使企业的利益受损风险降低，广泛适用于政府、金融、运营商、公安、电力能源、税务、工商、社保、交通、卫生、教育、电子商务及各企事业单位等。

2.2 产品架构

本产品主要由采集器、通信服务器、关联引擎及 Agent 组成。

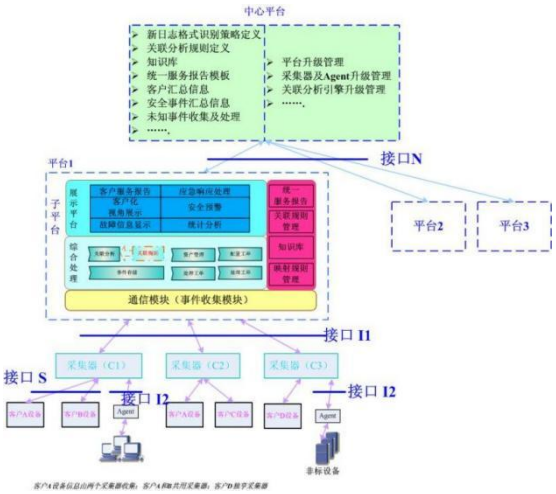

图 1-1 产品架构图

2.2.1 采集器

主要实现日志采集、日志解析与格式统一、日志预处理、完成日志向平台的传送等功能，被监控设备分为标准设备（支持 Syslog 或 SNMP trap）和非标设备（不支持 Syslog 和 SNMP trap）；采集器主要完成标准设备日志的收集功能。把采集的日志数据过滤并转化为统一定义的标准数据格式；完成日志压缩和归并。

2.2.2 通信服务器

通信服务器完成采集器与平台间的通信，将格式统一后的日志直接写入数据库并且同时提交给关联分析模块进行分析处理。通信服务器可以接收多个采集器的日志；在平台尚未支持统一日志格式时，能够根据要求，将定义的统一日志转换为所需要的日志格式。

2.2.3 关联引擎

对于整个综合日志安全管理平台收集到的事件种类多，数量大，为了更有效地对这些海量的事件进行分析和处理，确保第一时间对各种存在的安全问题采取措施，平台必须具有强大的事件处理和分析功能。目前对实践进行处理和分析最有效的方法就是做事件的关联。包括实时进行关联分析、跨设备关联分析、基于事件因果关系、事件安全要素、跨协议层、多层架构、时间回溯以及关联结果的回放等内容。

2.2.4 Agent

Agent 主要完成非标准设备（不支持 Syslog 和 SNMP trap）的安全日志采集，Agent 采集到日志信息后，通过 SYSLOG 日志发送给采集器。主要包括文件型 Agent、数据库型 Agent、Api 型 Agent 的开发工作，至少支持 windows 主机日志及性能采集；支持通过 SNMP Get 方式对主流安全设备、网络设备的性能数据采集；IIS、Apache web 服务器日志收集；Mysql、SQL server 数据库日志采集。

3 产品功能

3.1 日志信息接收

根据采集器的配置，日志信息接收模块可以监听在相应的端口上。收到相应的数据报文后，转换为相应的格式标准(SYSLOG 报文转换为字符串格式，SNMP TRAP 报文转换为 SNMP PDU 数据格式)，并且附加上来源地址信息。如果有必要，需要对收到的报文中文本信息进行正确的解码处理，保证不出现乱码现象。

3.2 日志信息解析

接收到的原始日志信息，经过解析规则的模式匹配，提取出直接信息和非直接信息，最终就得到了解析后的通用事件。日志信息解析模块启动的时候，需要首先进行规则库的加载，加载各种日志格式的解析、映射定义。加载完成后，才能进行日志的解析处理。当原始日志无法匹配规则库中任何一个规则时，就会生成一个未识别日志信息。用户收到未识别日志信息后，应该更新规则库，以支持这种日志格式。

3.3 日志信息标准化

完成解析后的通用事件，可以根据规则库，进行标准化处理。标准化主要是对解析后的日志，根据标准化的通用事件格式，对各个标准化字段，进行信息的直接映射、非直接映射处理。映射处理基于预先定义的标准。在本系统，标准基于对安全领域的技术、威胁、模式、以及网络层、应用层的抽象。标准化过程，也会进行字段的格式处理，如时间戳的 format、locale 的处理。经过映射处理后，就得到了最终的通用事件。

3.4 过滤处理

采集器为了消除不必要的日志事件，或者去掉不重要的日志事件，可以设定过滤规则。任何标准化完成后的通用事件，都会经过过滤规则匹配。当满足匹配后，此事件就会被过滤，直接过滤掉，不会进入后续模块进行处理。当不满足匹配，此事件就不会被过滤，直接进行后续模块处理。

3.5 聚合处理

采集器为了减少重复日志事件的数量，会在处理流程中，通过设定一个聚合周期、聚合规则，对于在聚合周期内，所有满足聚合规则的事件，进行聚合处理，得到聚合事件。聚合事件中的事件计数字段，会记录本次聚合的源事件的数量。聚合处理不会影响后续关联分析等处理。

3.6 日志缓存

为了实现日志缓存的需求，需要对队列进行持久化处理。采集器日志缓存基于状态驱动。当队列的空闲状态较低时，超过最低阈值后，会触发回写模块，把内存队列中的事件持久化到设备磁盘系统上。当队列的空闲状态较高时，超过最高阈值后，会触发加载模块，把磁盘系统上持久化的数据，加载到内存队列中。

3.7 状态检测处理

为了实现状态检测处理，需要维护每个资产的状态信息。当收到设备的原始日志后，会更新此设备的事件计数、最后活跃时间等信息。当状态检测周期到达后，采集器会把每个设备的状态信息组装成心跳事件，上送给上层设备。

3.8 通信服务器的功能

通信服务器接收各个采集器上发的通用事件，汇总后进行存储。通信服务器处理收到的心跳事件，更新对应资产的心跳状态，并持久化心跳信息到数据库中。通信服务器处理配置同步请求。当用户或管理员在界面上新增、删除、修改了客户、资产、规则库后，通信服务器应该能够把这些改动同步到各个连接的采集器上。

3.9 关联引擎的功能

关联引擎从接收到的通用事件中，基于关联规则，发现关联事件。关联事件包括各个原始事件列表。关联引擎产生的关联事件，能够支持入库接口，进行持久化处理。关联引擎支持自定义的关联规则，支持规则的启用、禁用。

3.10 日志代理的功能

当某些设备无法主动发送 SYSLOG 日志、或者由于配置等原因(如不允许直接网络访问)的时候， 在目标对象主机上部署一个轻量级的 Agent 进程，用于主动抓取日志。Agent 采集到日志信息后，通过 SYSLOG 日志发送给采集器。Agent 支持以下的日志获取方式：

- 通过读取日志信息
- 通过 Windows 日志 API 接口获取日志信息
- 对系统可用性资源(如 CPU、内存、磁盘、任务)进行监控

4 产品特点

4.1 全面的智能收集功能

不断地连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控；可配置过滤和聚合功能可以消除无关数据，并且合并重复的设备日志，强大的数据压缩功能可节省昂贵的带宽。

4.2 标准化日志

各种安全事件日志(攻击、入侵、异常)、各种行为事件日志(内控、违规)、各种弱点扫描日志(弱点、漏洞)、各种状态监控日志(可用性、性能、状态)、安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类。

4.3 创新的日志解析能力

解析规则激活，仅当接收到对应的日志后，规则才会被激活，同时支持未识别日志水印处理，采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理，同时支持多种解析方法（如正则表达式、分隔符、MIB 信息映射配置等）；日志解析性能与接入的日志设备数量无关。

4.4 先进的关联算法

明御综合日志审计分析平台的关联分析引擎本系统的最大亮点之一。明御综合日志审计分析平台的关联引擎采取了 In-Memory 的设计，全内存运算方式保证了事件分析极高的效率和实时性，这和一般的日志审计产品通过 SQL 查询方式提供关联分析能力有巨大差别，无论在分析速度、分析维度、灵活性、IO 抗压能力方面都完全不可和明御综合日志审计分析平台的关联分析引擎比拟。

另外，在关联算法方面，明御综合日志审计分析平台有如下独到之处：

- 标准化之上的关联规则，适应性强
- 可定制性强，几乎可根据通用事件的任何字段进行关联
- 基于逻辑表达式，可以进行复杂关联
- 时序宽容，无惧乱序

4.5 可维护性及可扩展性

系统具有对自身的维护配置功能，如：系统参数设置、系统日志管理等。 硬件系统采用模块结构，保证

系统内存、CPU 及储存容量的扩展；硬件配置的升级不会引起软件的修改和开发；每个组件都可以横向扩展，通过增加设备满足业务需求。

4.6 采用通用的安全事件标准

明御综合日志审计分析平台系统根据多年的网络安全经验，总结出了通用标准的安全事件归一化格式和分类体系结构。明御综合日志审计分析平台可以以标准方式处理以下元素：

- 各种安全事件日志(攻击、入侵、异常)
- 各种行为事件日志(内控、违规)
- 各种弱点扫描日志(弱点、漏洞)
- 各种状态监控日志(可用性、性能、状态)
- 安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类

4.7 分布式设计

明御综合日志审计分析平台系统采取分布式设计，将系统分为采集器、通讯服务器、关联分析引擎和管理中心四个部分。四个部分可以分布式部署，也可以组合部署，最大程度上兼顾了系统的可扩展性和灵活性；另外基于 HTTPS 的通讯模式，使跨互联网部署成为了可能，异地监控不再需要昂贵的专线私网模式。可以适用于从大型电信级网络环境到寥寥数台设备的中小企业。

明御综合日志审计分析平台典型的部署模式如下：

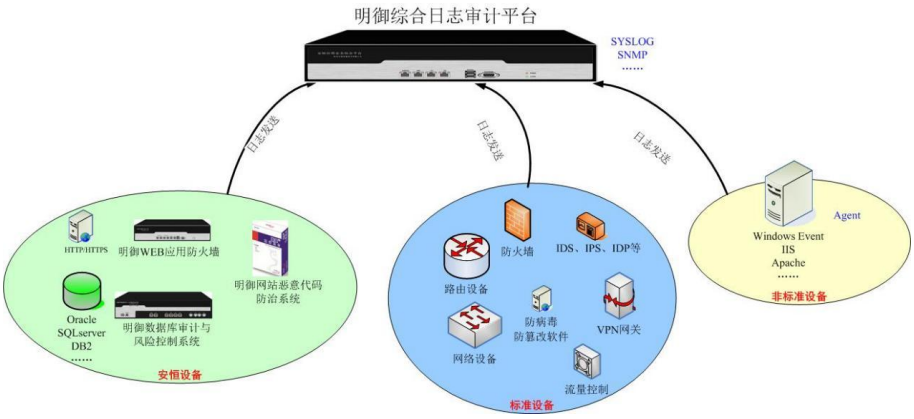

图 1-2 简单环境部署

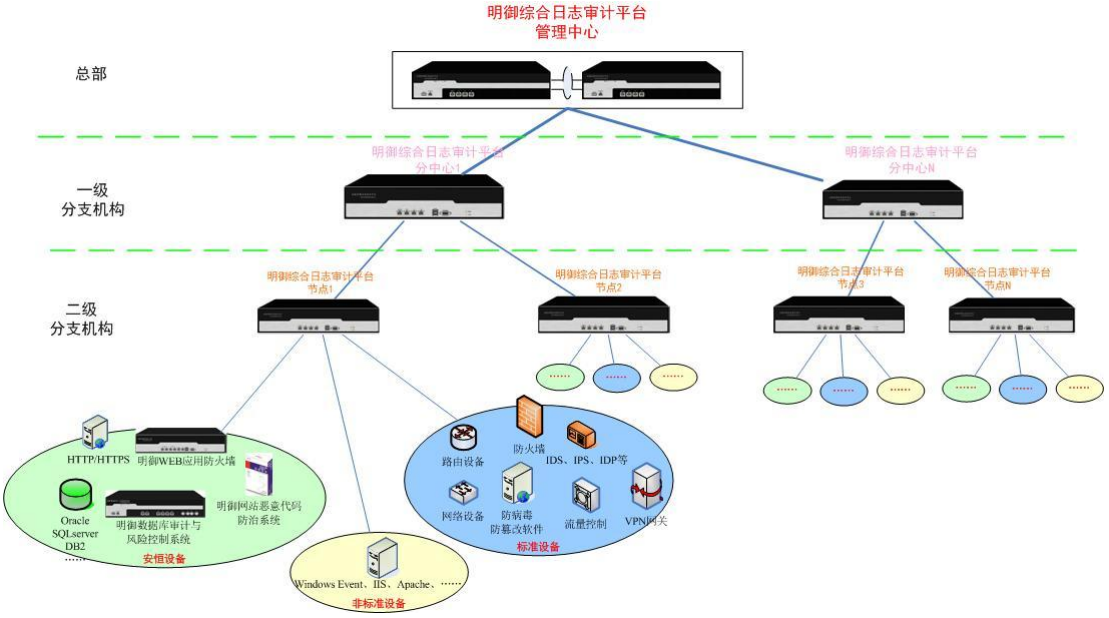

图 1-3 复杂环境部署

4.8 可配置的内容策略

明御综合日志审计分析平台系统采用了安全策略与基础系统分离的设计架构，将事件格式分析规则、关联分析规则、报警规则、综合报表规则等策略内容独立出来，变成可以独立演进、独立配置、独立升级的内容（称为 Content），由安恒经验丰富的专门团队根据多年安全经验专门定制开发，这种模式具有非常强的反馈速度和适应性。

5 典型应用场景

5.1 某市高校项目

5.1.1 场景描述

学校拥有多个网站及信息系统，包含多台服务器主机、防火墙、WAF、IDS、IPS 等等。已进行了初级的网络安全建设，未部署日志审计系统，未进行等保建设，需要进行等保 2.0 建设并通过等保检查。

5.1.2 典型部署方案

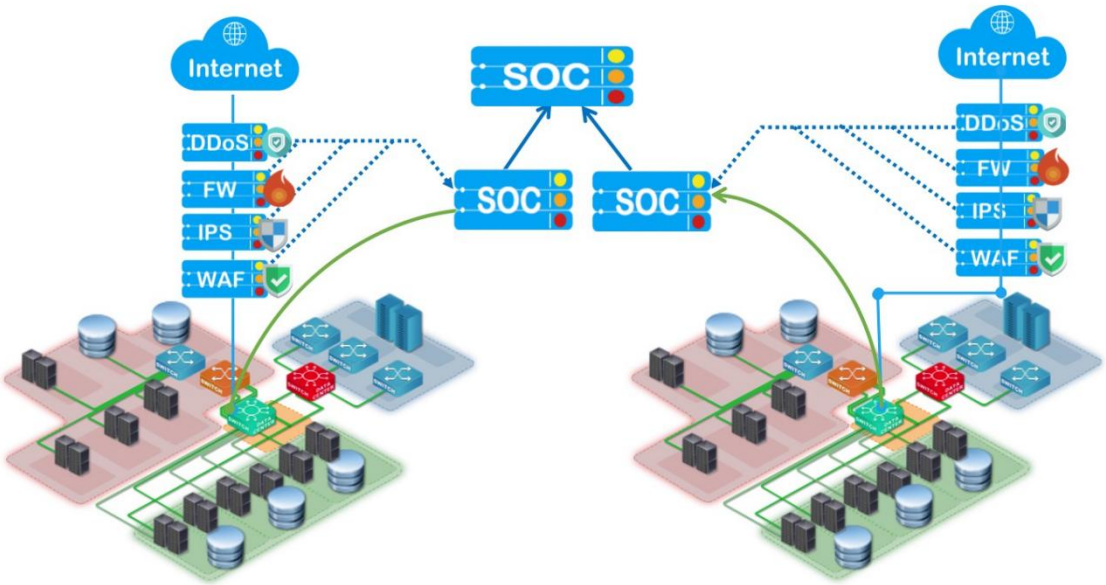

图 1-4 典型部署方案

5.1.3 客户收益

1、满足网安法和等保 2.0 的合规要求

2、帮助安全管理人员进行安全策略审计，发现违规行为

3、利用日志进行 IT 运维与故障排查；

4、通过关联分析帮助客户发现网络中的安全威胁与攻击。

5.2 某市公安项目

5.2.1 场景描述

客户已进行了较为完善的网络安全建设，网络中的日志数据量成指数级增长，原有的日志审计系统已无法满足当前不断爆发式增长的海量日志的审计和分析需求：

1、原有系统的存储容量较小，随着日志规模的扩大，原有系统无法满足网安法要求的日志保存 6 个月以上的要求

2、原有系统已经无法满足日益增长的日志统计报表的需求

3、原系统的关联分析功能不足，无法对新增 IT 安全设施和新业务日志进行审计，主要表现在日志字段无法扩展，对新业务属性无法识别和提取，从而影响审计能力

5.2.2 典型部署方案

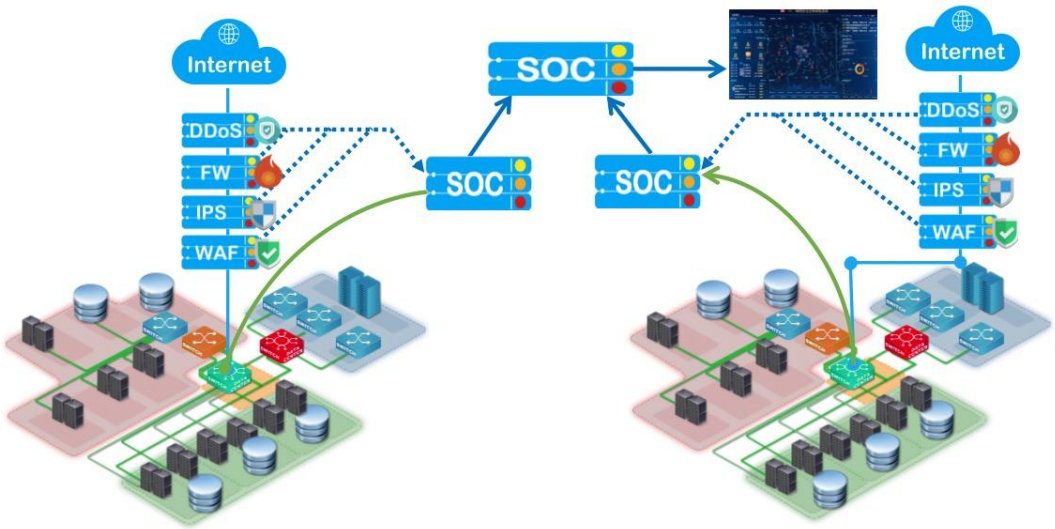

图 1-5 典型部署方案

5.2.3 客户收益

1、能够把所有重要资产的大量运行日志信息进行收集、解析并存储；

2、能够把所有重要资产的日志信息进行关联分析，并在可视化图上直观的呈现出来；

3、能够实时的将解析及分析后的日志转发给态势感知平台。

5.3 某市银行项目

5.3.1 场景描述

已初步构建起了一套较为完善的安全检测和防御技术体系，但随着信息建设的快速发展，仍有以下痛点：

1、全面的日志采集：需要将接入网络基础设施、安全系统和设备、网站系统范围内的安全日志及主机系统日志，统一采集日志，进行集中的管理与分析。

2、日志规范化：需要对采集到的各种设备日志进行归一化处理，提取审计记录完整信息，为后续审计与分析提供依据。

3、关联分析及审计需求：对于发生在多个设备上的事件痕迹进行关联分析，形成一个完整的事件分析。

4、通过安全事件告警，达到将网络中的各类事件以告警的方式进行分类分级展示，并提供告警抑制机制，消除重复告警，提高工作效率。

5.3.2 典型部署方案

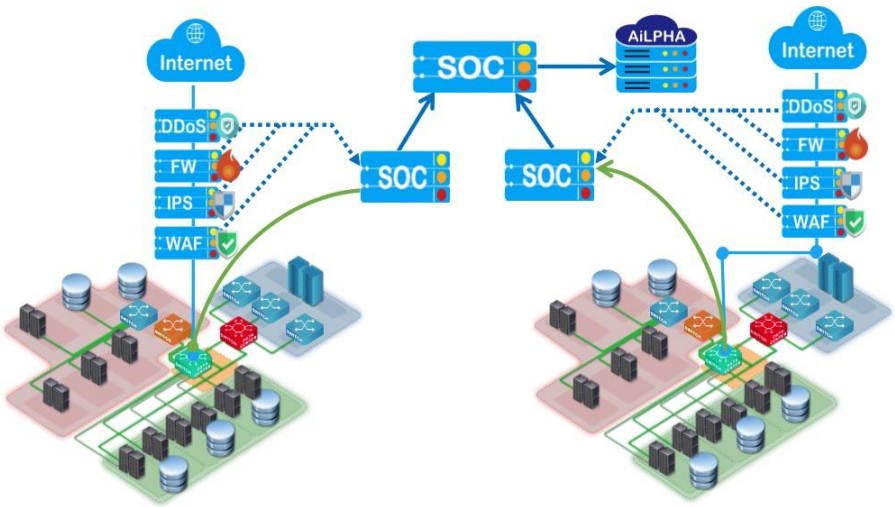

图 1-6 典型部署方案

5.3.3 客户收益

1、能够将所有重要资产的大量运行日志信息进行分散的收集、解析、存储并查询；

2、能够把所有重要资产的日志信息进行关联分析，并在可视化图上直观的呈现出来；

3、同时总行对总部的所有设备进行日志采集、存储、分析和查询，实现日志留存和分析。