绿盟日志审计系统

产品白皮书

目录

一. 日志审计需求和挑战

需求分析

日志审计主要来源于如下两方面的需求：

- 等保合规要求

目前国家的政策法规、行业标准等都明确对日志审计提出了要求，日志审计已成为企业满足合规内控要求所必须的功能。例如： 2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》中规定：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。《信息系统安全等级保护基本要求》中规定：二到四级需要对网络、主机、应用安全三部分进行日志审计，留存日志需符合法律法规规定。

- 业务需求

随着企业信息化的不断发展，公司信息化资产数量日趋增多、系统的关联性和复杂度不断增强，然而当前信息安全形势日益严峻，信息安全防护工作面临前所未有的困难和挑战。日志审计能够帮助用户更好监控和保障信息系统运行，及时识别针对信息系统的入侵攻击、内部违规等信息，同时日志审计能够为安全事件的事后分析、调查取证提供必要的信息。

面临的挑战

- 日志存储分散

  企业网络中的各种网络设备、安全设备、应用系统等分散在网络的不同位置，企业审计人员需登录不同设备控制台查看设备产生的日志、设备的状态。

- 日志数据量大

  企业网络中的各种安全设备、网络设备、应用系统等每天会产生大量的日志，企业审计人员很难通过人工的手段进行集中存储管理以及有效分析。

- 日志格式不统一

  企业网络中的各种网络设备、安全设备、应用系统等不同的设备类型产生的日志，其格式都不相同，企业审计人员需了解每种设备日志的格式才有可能去分析日志，日志分析成本很大。

如何应对挑战

基于如上分析，企业需要借助一个日志审计产品来满足等保合规要求，解决其面临的日志存储分散、日志数据量大、日志格式不统一等问题。该日志审计平台应具备如下的特性：

- 符合政策法规的规范性要求
- 可对分散的海量日志进行统一收集
- 可对不同格式的日志进行规范化的处理
- 可对日志进行集中存储、分析、审计和展示

二. 绿盟日志审计系统

产品概述

绿盟日志审计系统 (NSFOCUS LAS)是基于大数据架构的新一代日志审计系统，针对大量分散设备的异构日志进行集中采集、统一管理、存储、统计分析的一体化产品，可协助企业满足等保合规要求、高效统一管理资产日志并为安全事件的事后取证提供依据。

绿盟日志审计系统 (NSFOCUS LAS)包含日志采集、日志管理、资产管理、事件告警、统计管理、报表管理、系统管理以及用户管理等八大核心功能。

图 2.1 绿盟日志审计系统 (NSFOCUS LAS)系统功能示意图

绿盟日志审计系统 (NSFOCUS LAS)通过内置的日志采集功能可实时采集不同厂商的安全设备、网络设备、主机、操作系统以及各种应用系统产生的日志信息，然后经过统一的日志管理过程，如日志范式化处理等，将采集来的海量的异构的日志信息进行集中化的解析和存储，结合资产管理模块、事件告警模块的相关规则以及配置，形成事件告警信息，用户可基

于这些进行进行原始日志、范式化日志以及事件、告警等信息的查询，并可通过丰富灵活的日志报表功能进行可视化的查看，实现对日志的全生命周期管理。

产品架构

绿盟日志审计系统 (NSFOCUS LAS)系统层次分为资源层、采集管控层、大数据层、服务层以及业务层。通过对系统的分层设计，实现各层功能的松耦合对接。

资源层指绿盟日志审计系统 (NSFOCUS LAS)接入以及管理的资产、日志源，如常见的安全设备、网络设备、数据库、服务器、应用系统、主机等。采集层指海量异构数据的采集，通过各种协议将资源层对象的数据进行采集并高效范式化，并将数据传送数据层。数据层采用大数据存储、计算功能，为服务层提供相关的接口、引擎等功能。服务层是系统内的管理模块，实现系统功能的协调，管理系统的基本数据、支撑系统的核心功能。业务层，面向用户提供可视化的展现以及业务场景。

部署方式

单机部署

单机部署是一种简洁的系统部署模式，适用于大部分企业客户的网络环境。在单机部署场景中，用户仅需要一台绿盟日志审计系统 (NSFOCUS LAS)，其内置的日志采集器可以收集设备对象的日志信息并进行范式化处理、分析、集中存储等。用户可以通过浏览器登录日志审计系统的交互界面，并根据相应的权限进行各种管理操作。

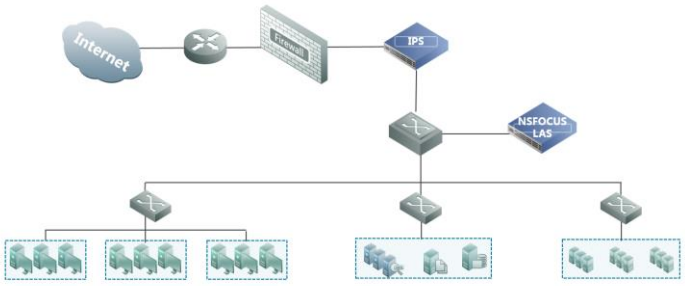

图 2.2 单点部署示意图

采集器分布式部署

采集器分布式部署是一种很经典的模式，是指将日志采集功能采用分布式部件进行部署的模式。适用于如下几种情况：

i. 管理节点规模较大且分散在物理网络中的多个位置。

ii. 被管理节点与绿盟日志审计系统(NSFOCUS LAS)不在同一个逻辑网络中，例如之间存在安全网关、防火墙、网闸隔离、或者有 NAT 地址转换。

iii. 被管理节点与绿盟日志审计系统(NSFOCUS LAS)所在网络是跨广域网链接的，且广域网接入的带宽容量有限。

在采集器分布式场景中，通过在被管理节点处就近部署分布式的日志采集器采集数据，日志采集器承担了日志采集范式化相关工作，支持日志过滤，可提升绿盟日志审计系统(NSFOCUS LAS)的处理能力。日志采集器在采集数据后通过压缩加密的方式传输给绿盟日志审计系统(NSFOCUS LAS)，可降低网络负载。此外，当被管理节点与绿盟日志审计系统(NSFOCUS LAS)不在同一个逻辑网络中（如有安全网关、防火墙、网闸隔离、或者有 NAT 地址转换）时可以通过部署分布式日志采集器节点进行中继。

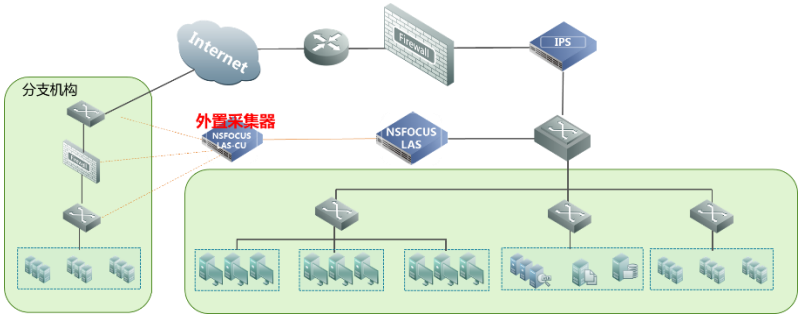

图 2.3 采集器分布式部署示意图

产品功能

绿盟日志审计系统 (NSFOCUS LAS)的功能如下：

日志管理功能

- 支持对安全设备、网络设备、主机设备、应用系统、中间件等的海量日志采集
- 支持异构日志的统一范式化处理
- 支持原始日志、范式化日志的存储，可自定义存储周期
- 支持丰富灵活的日志查询方式、便捷的日志分析操作
- 支持多种日志存储扩展方案
- 支持外置采集器
- 支持 IPv4、IPv6 部署以及日志采集

日志转发功能

- 支持原始日志、范式化日志的转发

事件告警

- 支持自定义事件规则、丰富的内置事件规则
- 支持事件的查询、统计、分析展示等
- 支持自定义事件告警规则以及告警通知方式

资产管理

- 支持对资产进行分组、增加、删除、修改、查询、备份回复等操作
- 支持资产下钻资产查看相关的日志、事件等信息

报表管理

- 支持丰富的内置报表以及灵活的自定义报表
- 支持实时报表、定时报表、周期性任务报表等方式
- 支持 html，pdf，word 格式的报表文件以及报表 logo 的灵活配置

产品优势

- 数据强化技术

  绿盟日志审计系统 (NSFOCUS LAS)根据绿盟科技对攻防研究的长期积累，提供一套简洁有效的日志统一分类，使用数据强化技术将日志快速标准化，并基于安全分析需要进行数据的过滤和强化，丢弃无法使用的噪音信息，提升日志查询和分析效率。

- 海量的日志处理能力

  绿盟日志审计系统 (NSFOCUS LAS)使用大数据技术，在并发内存处理机制方面能够带来数倍于其它采用磁盘访问方式的解决方案，借助离线计算引擎在小时级别内，即可完成对海量日志的处理。

- 灵活的扩展存储方案

  绿盟日志审计系统 (NSFOCUS LAS)提供了多种日志存储扩展方式，支持按需选择日志存储扩展方案，可支持《网络安全法》规定留存 6 个月日志的要求。

- 全面支持 IPv6 部署以及数据接入

  绿盟日志审计系统 (NSFOCUS LAS)支持 IPv6 的部署以及 IPv6 环境下的日志采集、分析以及检索查询。

产品价值

绿盟日志审计系统 (NSFOCUS LAS)可协助企业满足等保合规要求，如：2016 年 11 月 7 日发布，2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》、《信息系统安全等级保护基本要求》以及其他行业的合规性要求。

绿盟日志审计系统 (NSFOCUS LAS)可协助企业解决日志分散、种类繁多、数量巨大的问题，高效的收集日志、处理日志、分析提取日志时间，可提升企业的日常运维效率、变被动审计为主动告警。