绿盟企业安全中心

产品白皮书

目录

一. 安全管理的新需求和挑战

需求分析

随着企业对信息技术越加依赖，安全问题也越加凸显。从爆库门（用户信息泄露）到间谍门（企业数据窃取）再到棱镜门（数据窃听），时时刻刻提醒着我们在 IT 技术迅猛发展的同时，安全威胁也在不断地发生着演变，新生的威胁（如挂马、钓鱼、0Day、APT）正在不断涌现。安全威胁日趋常态化，直接导致安全防御设备的专业化和多元化，也给 IT 运维管理工作带来了困惑。

同时，IT 技术及攻防技术的不断演进，企业对信息安全技术人员的依赖日益加深，对技术人员的安全能力也有了更高的要求。这不仅加剧了技术人员的需求缺口，也增加了管理人员使用成本。企业在转变生产方式和业务拓展的大背景下，IT 运维和人员数量和人员成本的与日俱增，又使得企业预算捉襟见肘。

另外，主流企业的 IT 架构正在向“云计算”逐步演进，并希望通过“云计算”的方式解决企业遇到的各种安全和运维困境。越来越多的客户已经看到了这一点，但在实际的 IT 运维工作中又遇到一系列的协同和管理问题。综合以上问题，我们总结了以下突出特点：

- ✧ 部署量大，设备类型多，角色多，难以整体把控的特点
- ✧ 事后响应，难以快速发现和定位问题
- ✧ 人员和管理成本增加
- ✧ “云计算”导致设备“虚拟化”和“资源池”的特点
- ✧ 多系统，多平台协同运维的特点
- ✧ 运维工作面向终端用户开放的特点

面临的挑战

当前主流的 IT 管理系统主要面临着以下几种挑战：

1） 如何面对“云计算”对“运维管理”带来的挑战

Gartner 预测的未来 5 到 10 年，“云计算”将成为主流 IT 技术。如何对“云计算”环境下的设备进行统一监控，自主访问，分等级访问控制以及虚拟设备的整个生命周期管理，都日益成为企业统一管理系统面临的重大课题和挑战。

2） 如何面对多系统，多平台协同工作的挑战？

无论是传统企业环境中，还是在未来的“云计算”环境中，不可避免的存在一个或者多个业务系统并存的情况。 这些业务系统可能是网管、SOC 、SIEM 或者 CMDB 等。它们自身定位不同，并且负责着不同类型信息的收集、汇总以及展示。如何与这些相关业务系统协同运维，打破各自为战的“信息孤岛”是摆在企业面前的另一道障碍。

3） 如何保障业务平台系统的可用性？

业务系统的可用性体现在：对新兴的威胁防御以及资产维度上的威胁感知。

传统的 IT 管理系统强调对单个设备和性能的可用性管理，缺乏通过多设备联动，对复杂网络威胁攻击（APT 攻击）的检测和防护。同时，从设备监控视角出发，过渡地强调设备故障的及时诊断，已经不能够从根本上保障核心业务系统的可用性，更缺乏从核心资产维度的监控和分析。

如何应对挑战

客户需要一套全新的 IT 管理系统来应对传统网络和云计算所带来的所有挑战，该系统能够通过设备之间的联动，自动组合成威胁防御方案。它以资产为核心，兼具设备管理功能，对企业 IT 资产情况进行全方位的监控和告警，协助用户进行网络安全威胁的统一管理。能够对虚拟化安全产品进行全方位的监控和管理，确保虚拟设备启动，运行，销毁等整个生命周期管理。能够符合等级保护的基本要求。同时，这个系统应该是一个开放的平台，能够与客户的其他管理系统实现协同工作。

二. 绿盟科技企业安全中心产品

产品概述

绿盟科技推出的绿盟企业安全中心 V7.0 （以下简称 NSFOCUS ESPC）是总结多年攻防运维管理经验的结晶，并基于当前用户第一手需求而推出的绿盟自有产品的安全管理平台。是企业进行安全设备维护与安全运维管理的重要工具和伙伴。

绿盟企业安全中心是绿盟科技拥有完全自主知识产权的产品，适用于安全设备维护、威胁管理以及“云计算”环境下的虚拟设备全生命周期管控等多种安全运维场景。

产品架构

如图所示，从技术的角度出发的展示管理系统架构。

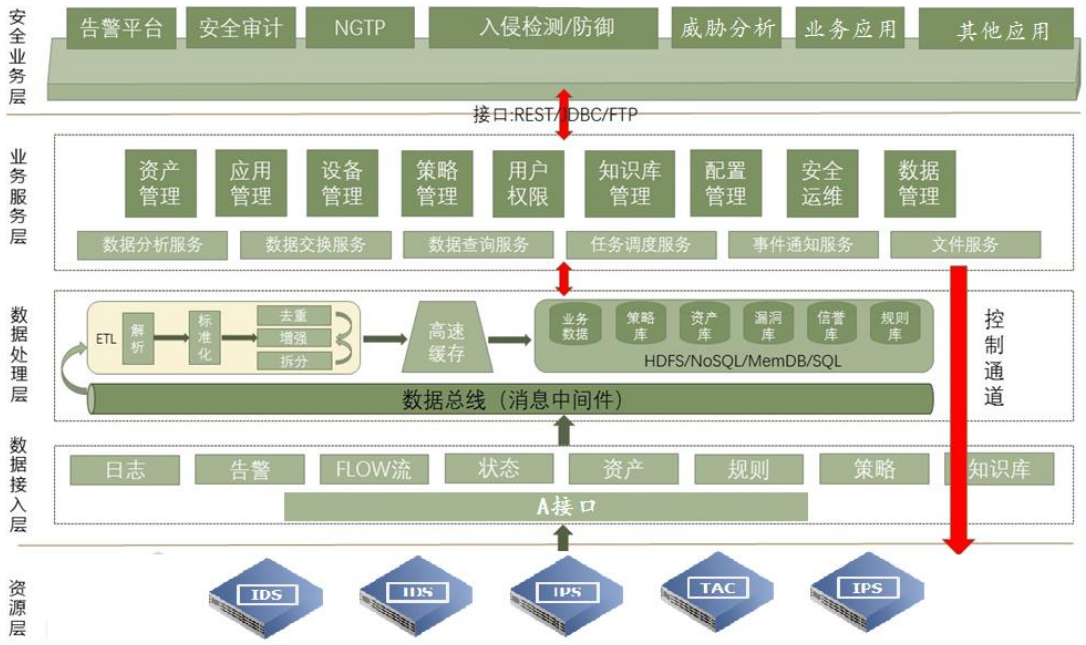

图 2.1 NSFOCUS ESPC 系统架构图

产品优势

业务模块插件化的特点

在传统产品中，业务模块与平台功能是多对多的关系，这样就导致某个业务模块的设计的更改会影响到平台的多个功能，也会导致不确定范围的其他业务模块的修改。随着业务模块的复杂程度和平台功能重用度的提高，管理这样结构的平台就会变得十分困难，尤其是用户个性化定制，往往“牵一发而动全身”导致工作量倍增和交付延期。

因此，NSFOCUS ESPC 采用全新的设计思想，将业务模块插件化处理，使业务模块与平台功能只能是一对一的关系，这样，业务模块的改善就不会造成其他模块或平台功能的调整，也就是将业务模块抽象并与平台功能实现分离，从而提高研发效率，降低企业维护成本。

安全管理集中化的特点

1） 安全事件集中收集和处理

通过 NSFOCUS ESPC 的部署，在所辖网络或者不同的业务支撑网络，只需网络可达即可建立安全信息采集点，通过私有安全通讯方式与绿盟入侵检测系统、绿盟入侵防

御系统、威胁分析系统等产品形成统一的集中安全管理方案，全面支持设备的各类操作，从而实现了针对整体的安全事件的集中收集和处理。

ESPC V7.0 可管理的设备一览表			
设备类型	设备安全定位	集中安全管理	日志备份与存储
NIDS	入侵监测	支持	支持
NIPS	入侵防御	支持	支持
TAC	未知威胁检测	支持	支持
NF	防火墙	支持	支持
SAS	安全审计系统	支持	支持
WAF	Web 应用防火墙	支持	支持
SAS-H	堡垒机	支持	支持

NSFOCUS ESPC 对绿盟科技自有产品的支持程度(1)

(1)本文所示产品功能规格变动恕不同步更新，具体详情请咨询绿盟科技分支机构业务人员。

2） 安全策略集中配置和管理

策略管理是安全管理平台不可缺少的功能之一，通过安全策略配置管理平台可以进一步完善整个网络的安全策略管理体系建设，为安全运维管理人员提供统一的安全策略，为各项安全工作的开展提供技术指导。

配置管理是对安全设备进行运行参数配置，主要针对网络边界设备等。通过 NSFOCUS ESPC 可将安全资源配置集中备份，以便日后设备初始化后进行恢复或对比。主要包括：备份和恢复管理等。

3） 安全报告集中展示

NSFOCUS ESPC 的报表系统具备全面、灵活、个性化三个特点，可以帮助用户更好地汇报安全运维工作、制定安全运维的工作计划。

NSFOCUS ESPC 的报表系统内容丰富，涵盖了每一类设备、每一台设备上所有不同类型的告警事件。报表还可以对告警事件按照用户指定的要求进行统计分析，为用户展现各类事件的发展趋势和统计结果。

NSFOCUS ESPC 可以实现自动化报表，可通过筛选自定义报表内容，自动完成日报、周报、月报、季报、半年报和年报，协助用户完成汇报工作。NSFOCUS ESPC 也通过手动定制方式即时生成报表，并根据报表内容，制定下一步的工作计划。

NSFOCUS ESPC 还具备个性化功能，用户可以自定义报表的标题和创建人，使报告可以广泛用于各种场景。

4） **级联部署和分级管理**

NSFOCUS ESPC 可以通过级联部署和授权管理功能建立“分级管理-集中监管”的安全管理体系。当前您的业务不断扩展，需要由专人负责分支机构网络安全时，可通过 NSFOCUS ESPC 级联功能将各分支 ESPC 与总部 ESPC 进行级联对接。由总部安全管理人员对分支安全运维人员进行授权，并在总部对分支安全运维情况进行统一监管。

主要功能

◆ 威胁管理

NSFOCUS ESPC 可以接入绿盟科技自有的入侵检测与防御系统、威胁分析系统等威胁检测与防护类产品，可实现对恶意嗅探、DDoS 类攻击、应用攻击、病毒文件、蠕虫、获取权限类攻击、可疑网络活动等行为的集中告警，安全运维人员可以通过告警筛选、告警分析完成对威胁的监视、分析、诊断工作。

◆ 资产管理

NSFOCUS ESPC 建立了一套完整的多维度资产管理系统，可从资产维度对企业网络内部的存在的威胁进行统计和分析。帮助运维人员洞悉企业内部 IT 基础设施的情况，包括：资产 IP 地址、名称、开放的协议端口和应用。

◆ 设备管理

NSFOCUS ESPC 可以对绿盟科技的入侵检测与防御系统、威胁分析系统等设备进行统一的集中管理，可以帮助企业安全运维人员对设备进行统一的维护和管理。NSFOCUS ESPC 可以对安全设备的各类指标进行监测，集中展示安全产品的运行状态，帮助安全运维人员及时发现和诊断故障。

◆ 集中授权

NSFOCUS ESPC 可以对绿盟科技的虚拟化下一代防火墙系统、虚拟化远程安全评估系统等虚拟化设备进行统一的授权管理。可帮助企业的安全运维人员对绿盟科技虚拟化设备进行统一的维护和授权管理。

◆ 信誉库

系统提供开放的知识管理功能，内置了部分的云端信誉知识，包含：URL 信誉，IP 信誉，C&C 信誉和文件信誉。同时也允许用户在使用过程中不断丰富和完善本地信誉。

◆ 权限管理

NSFOCUS ESPC 不仅提供三权分立的设计，内置系统管理员、用户管理员和审计管理员、安全员。还能够基于角色的权限管理机制，对所有用户的权限通过角色来分配。

◆ 系统管理

系统具有丰富的自身配置管理功能，包括自身配置、系统运行参数监控等。系统具有自身运行监控与告警、系统日志记录，存储，备份等功能。

◆ 应用管理

绿盟“云计算”商城主要面向有安全管理需求的企业和机构，通过专业的云端应用程序，为企业提供从云端到企业的一条龙式的“安全服务”。企业用户登录 NSFOCUS ESPC 后，通过“应用管理”模块就可以第一时间与绿盟“云计算”商城连接，按需采购符合企业发展的应用程序。

三. 典型部署

部署方式

单级部署

单级部署是指仅部署一个管理中心的模式。此时，在网络中就部署一个管理中心程序，所有的用户都登录到该管理中心进行访问，通过系统权限设置来区分不同的管理职责。

在单级部署模式下，又分为单机部署和集群部署。

单机部署

单级单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分企业客户的网络环境。在单机部署场景中，用户仅需在一台服务器上部署 NSFOCUS ESPC 系统。之后，管理中心可以收集设备对象的日志和性能信息。用户可以通过浏览器登录系统的交互界面，并根据相应的权限进行各种管理操作。

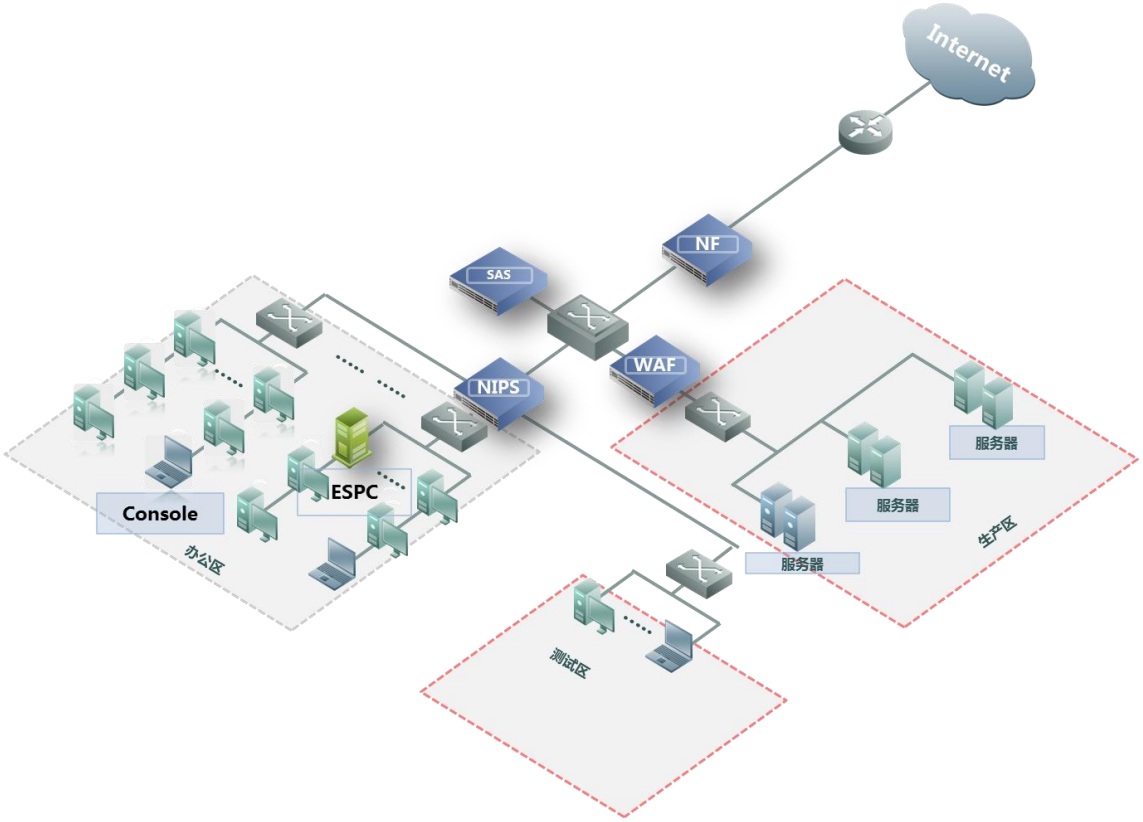

图 3.1 单级单机部署模式

集群部署（可选）

集群部署是指将 ESPC 的功能模块采用多地，按照分组的运行的方式进行部署的模式。一般地，当需要在分散在物理网络中进行较大规模的节点部署时，此时，大量的性能、日志数据通过网络汇总到管理中心，会给管理中心造成一定的性能影响。通过在将 NSFOCUS ESPC 功能模块分组运行于不同物理主机的方式，可以大大降低系统负载。通过这种部署方式，将一部分信息预处理的工作压力分散到了分布式主机上，保障了业务的可用性。

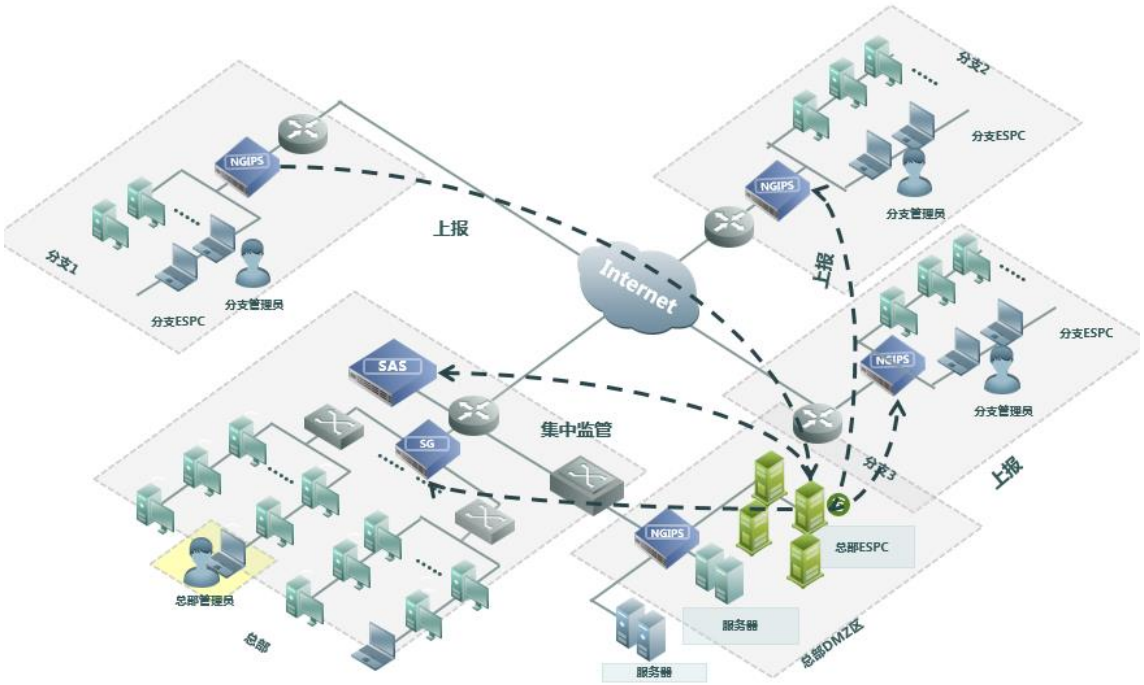

图 3.2 集群部署模式

多级部署

多级部署是指部署多个管理中心，并构建起一个总中心连接若干个分中心的部署模式。此时，在网络中就部署了多个管理中心部件，各个分中心的管理员通过浏览器登录各自的分中心对所辖网络进行安全管理，总中心的管理员则通过浏览器登录总管理中心进行全网的统一管理、集中展现，并可以监督各个分中心的管理工作。该部署模式用于具有分支机构或者垂直管理下属机构的单位，以适应多级管理的体制需要。

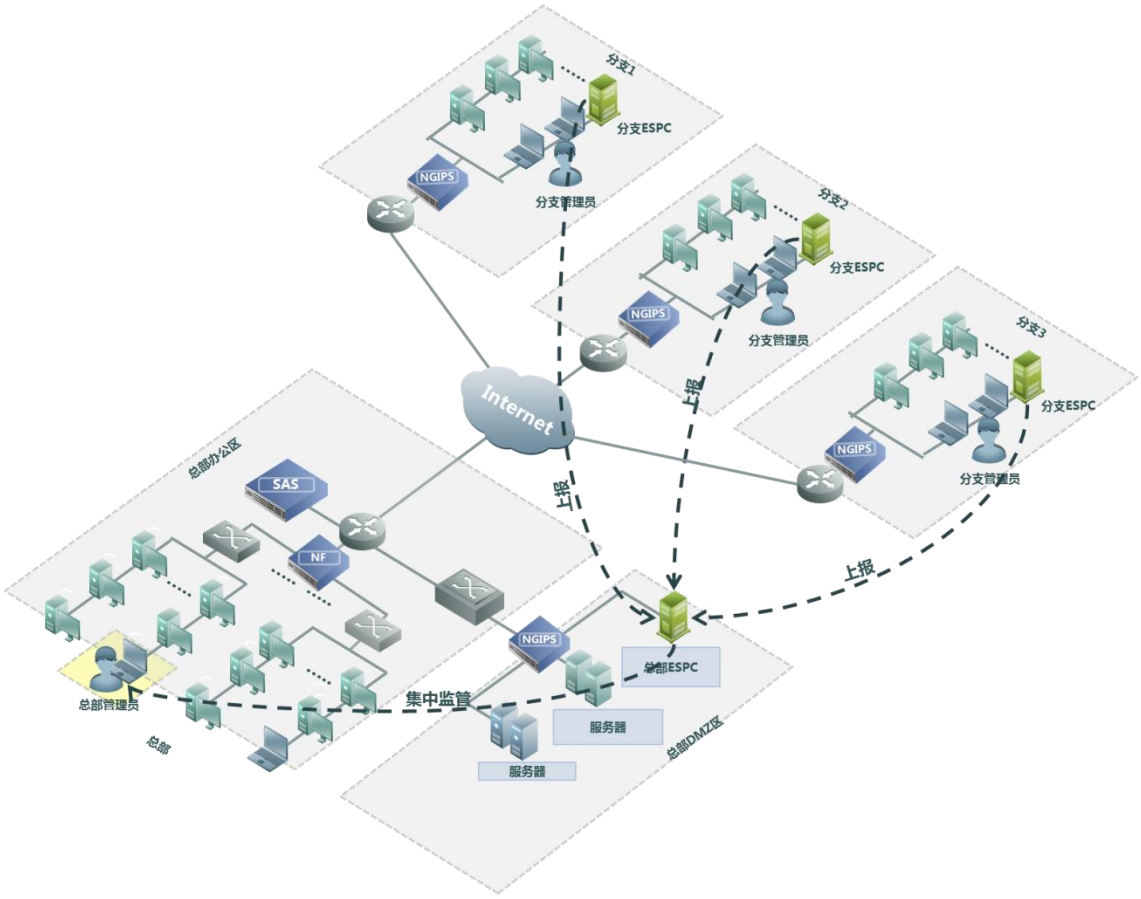

图 3.3 多级部署模式

运行环境

NSFOCUS ESPC 的运行环境：

平台	支持的操作系统	系统需求
Linux	64 位操作系统： - Red hat Enterprise Linux 6.5 - Cent OS 6.5	- Intel 酷睿 8 核 CPU，3.4GHz 以上 - 推荐 16GB 以上内存 - 1TB 以上磁盘空间

客户端环境要求：

用户通过浏览器即可访问管理中心。系统推荐使用微软 IE11，Google Chrome 或者 Mozilla Firefox 最新版本浏览器。浏览器所在 PC 的内存推荐 4GB。

四. 结论

在安全威胁和 IT 环境不断发展变化的今天，安全设备的集中管理已经成为大部分企业的刚性需求。我们应该对安全设备的集中管理有着清晰的认识，它在本质上还是针对人和技术的管理工具，当前阶段还没有一种工具可以完全替代人做自动化运维。如同狙击手对抗一样，拥有先进的狙击枪和伪装是取得胜利的必要条件之一，但拥有全面的对抗技能和知识是左右结局的关键。安全设备的集中管理和其他安全设备一样是防御者的工具，就和黑客有 nmap、nc、metasploit 等渗透所用的工具一样，是我们保护我们企业资产的必要工具和手段，是战胜黑客的先决条件。

一款适合我们的集中管理系统首先应该能够尽量覆盖我们安全运维的所有场景，能够帮我们监视安全威胁，能够帮我们下发安全策略，能帮我们对安全运维的结果进行审计。其次，集中管理系统应该具有良好的灵活性和可扩展性，能可持续地、连贯地使用，不会影响新产品或新版本的安全设备可用性，不会使我们安全管理模式受到牵制和羁绊，不会因安全管理的覆盖面难以扩展导致业务安全性面临挑战或更大的风险。