NSFOCUS

绿盟下一代网络入侵检测系统

产品白皮书

目录

插图索引

一. 前言

随着网络与信息技术的发展，尤其是互联网的广泛普及和应用，网络正逐步改变着人类的生活和工作方式。业务对信息和网络的逐渐依赖对社会的各行各业产生了巨大深远的影响，信息安全的重要性也在不断提升。

近年来，网络信息系统所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其是基于应用的新型威胁，如隐藏在 HTTP 等基础协议之上的应用层攻击问题、web2.0 安全问题、木马后门、间谍软件、僵尸网络、DDoS 攻击、网络资源滥用（P2P 下载、IM 即时通讯、网游、视频）等，极大地困扰着用户，给单位的信息网络造成严重的破坏，严重影响了信息化的进一步发展。

未来几年，随着云计算、物联网、智慧城市、移动互联网和微博等新一代应用和技术在行业得到广泛应用，在促进应用创新的同时，也将带来严重的信息安全隐患。攻防的不断发展，安全威胁的不断进化，新应用、新技术的广泛使用，对原有的安全保障理念和模式也将带来巨大的冲击，原有的安全检测手段已经不能完全解决面临的安全问题。

如何在新旧技术交叠应用的变革过程中，更有效地检测系统网络面临的安全问题，已成为各方关注的重点。

基于对网络入侵检测的实践，以及攻防的深刻理解和研究，绿盟科技正式发布国内首款下一代入侵检测系统，开启了下一代安全之门。该产品采用了全新的检测防护模型，综合运用智能识别、环境感知和行为分析技术，为用户提供一份看得见、检得出的下一代入侵检测解决方案，标志着国内入侵检测市场迈入一个新的时代。

二. 为什么需要入侵检测系统

随着网络的普及，网络安全事件的发生离我们越来越近，我们可能遇到如下情况：

- 企业的网络系统被入侵了，造成服务器瘫痪，但不知道什么时候被入侵的；
- 客户抱怨企业的网页无法正常打开，检查发现是服务器被攻击了，但不知道遭受何种方式的攻击；
- 员工因为访问恶意站点，将后门、木马等威胁引入企业内网，造成敏感信息外泄，给企业造成巨大的损失，却无法找到问题根源；

- 企业网络拥塞，应用正常业务运转，却无法定位消耗带宽的应用类型；
- 企业网络瘫痪，检查出遭受蠕虫病毒攻击，但不知道如何清除并避免再次遭到攻击；
- 企业网络被入侵了，安全事件调查中缺乏证据。

根据调查数据显示，以上情况给网络管理员带来极大的困扰，也给企业带来了巨大的安全风险。如何及时的、准确的发现违反安全策略的事件，并及时处理，是广大用户迫切需要解决的问题。

2.1 防火墙的局限

众多的企业、组织与政府部门都在组建和发展自己的网络，为了保证网络资源的安全，企业一般采用防火墙作为安全保障体系的第一道防线，通过访问控制，防御黑客攻击，提供静态防御。

但是随着越来越多的系统本身漏洞以及应用系统的漏洞被发现，以及攻击者的入侵方式更加隐蔽，新的攻击方式层出不穷，所以单纯的依靠防火墙已经无法完全防御不断变化的入侵攻击的发生，部署了防火墙的安全保障体系还有进一步完善的需要。

传统的防火墙主要有以下的不足：

- 防火墙作为访问控制设备，无法检测或拦截嵌入到普通流量中的恶意攻击代码，比如针对 WEB 服务的注入攻击等。
- 防火墙无法发现内部网络中的攻击行为。

2.2 入侵检测系统的特点

入侵检测系统（Intrusion Detection System）是对防火墙有益的补充，入侵检测系统被认为是防火墙之后的第二道安全闸门，对网络进行检测，提供对内部攻击、外部攻击和误操作的实时监控，提供动态保护大大提高了网络的安全性。

入侵检测系统主要有以下特点：

- 事前警告：入侵检测系统能够在入侵攻击对网络系统造成危害前，及时检测到入侵攻击的发生，并进行报警；
- 事中防御：入侵攻击发生时，入侵检测系统可以通过与防火墙联动、TCP Killer 等方式进行报警及动态防御；
- 事后取证：被入侵攻击后，入侵检测系统可以提供详细的攻击信息，便于取证分析。

综上所述，防火墙提供静态防御，而入侵检测系统提供动态防御，因此防火墙和入侵检测系统的结合，能够给网络带来全面的防御。对防火墙和入侵检测系统的关系有一个经典的

比喻：防火墙相当于门卫，对于所有进出大门的人员进行检查，入侵检测系统相当于闭路监控系统，监控关键位置如财务、库房等地安全状况，仅有门卫是无法发现内部人员的非法行为，而闭路监控系统可以实时监控，发现异常情况及时报警，两者配合使用才能保证安全。

三. 如何评价入侵检测系统

入侵检测系统具有实时检测、报警和动态响应等功能。是否能够很好地帮助网络管理员完成对网络状态的把握和安全的评价是入侵检测系统的基本标准。

入侵检测系统(IDS）应该从几个方面评价：

- 准确的、广泛的入侵检测能力
- 优异的产品性能
- 强大的管理能力
- 良好的自身安全性
- 丰富的响应功能

一个完善的入侵检测系统（IDS）应该具有以下特点：

- 实时报警，报警的准确率高，误报和漏报率低
- 不同性能的产品，能够满足不同网络的需求
- 操作简单，易于部署、管理
- 自身的安全性高，不易遭受攻击

四. 绿盟下一代网络入侵检测系统

针对目前流行的蠕虫、病毒、间谍软件、垃圾邮件、DDoS 等黑客攻击，以及网络资源滥用（P2P 下载、IM 即时通讯、网游、视频等），绿盟科技提供了完善的检测方案。绿盟下一代网络入侵检测系统（以下简称“NSFOCUS NIDS（N 系列）”）是绿盟科技拥有完全自主知识产权的安全产品，它是对防火墙的有效补充，实时检测网络流量，监控各种网络行为，对违反安全策略的流量给予及时报警和阻断，实现从事前警告、事中防护到事后取证的一体化解决方案。

4.1 体系架构

NSFOCUS NIDS（N 系列）的体系架构主要由安全引擎、安全管理模块及响应模块三个部分组成，方便各种网络环境的灵活部署和管理。

图 4.1 绿盟网络入侵检测系统体系架构

4.2 主要功能

NSFOCUS NIDS（N 系列）是网络入侵检测系统同类产品中的经典之作，该产品拥有业界其它产品无以比拟的高性能、高安全性、高可靠性和易操作性等特性，具备全面入侵检测、可靠的 Web 威胁检测、细粒度流量分析，以及全面用户上网行为监测等四大功能，为用户带来了极佳的安全体验。

◆ **入侵检测**

NSFOCUS NIDS（N 系列）对缓冲区溢出、SQL 注入、暴力猜测、D.o.S 攻击、扫描探测、蠕虫病毒、木马后门、间谍软件等各类黑客攻击和恶意流量进行实时检测及报警，并通过与防火墙联动、TCP Killer、发送邮件、安全中心显示、日志数据库记录、运行用户自定义命令等方式进行动态防御。

◆ **Web 安全**

基于互联网 Web 站点的挂马检测结果，结合 URL 信誉评价技术，在用户访问被植入木马等恶意代码的网站时，给予实时警告，并录入安全日志。

- **流量分析**

NSFOCUS NIDS（N 系列）能够统计出当前网络中的各种报文流量，协助管理员了解实时的网络流量性质和分布，以便及时做出调整，确保关键业务能够持续运转。

- **用户上网行为监测**

NSFOCUS NIDS（N 系列）系统对网络流量进行监测，对 P2P 下载、IM 即时通讯、网络游戏、网络流媒体等严重滥用网络资源的事件提供告警和记录。

4.3 产品特点

NSFOCUS NIDS（N 系列）基于高性能硬件处理平台，为用户提供全面、深入的黑客入侵行为检测，以下将对 NSFOCUS NIDS（N 系列）的产品功能特色进行逐一介绍。

4.3.1 全新的高性能软硬件架构

NSFOCUS NIDS（N 系列）采用了全新的硬件平台，全新底层转发模块、多核架构和新一代的全并行流检测引擎技术，新平台和新架构的引入，优化了产品的功能，使处理性能较原来有了大幅度提升。

同时大部分配置都是应用配置生效。增强了对客户业务的连续性支持。

4.3.2 用户身份识别与控制功能

NSFOCUS NIDS（N 系列）提供了用户身份识别与基于用户身份的访问控制功能，可以有效解决用户网内漫游带来的越权访问。传统 NIDS 产品基于 IP 地址进行访问控制，当非授权子网用户将终端接入到授权子网并配置为授权子网 IP 地址后即可访问和使用非授权的网络资源。结合 NSFOCUS NIDS（N 系列）产品丰富的应用识别能力，可实现细粒度访问控制。

4.3.3 更精细的应用层安全控制

基于应用的识别技术，是各种应用层安全防护的基础，目前各类新的应用层出不穷，如 QQ、MSN、文件共享、Web 服务、P2P 下载等，这些应用势必会带来新的、更复杂的安全风险。这些风险和应用本身密不可分，如果不结合应用来分析将无法抵御这些风险。

NSFOCUS NIDS（N 系列）采用流检测技术对各类应用进行深入分析，搭建应用协议识别框架，准确识别大部分主流应用协议，可以对基于应用识别的应用进行精细粒度的管理，能够很好的对这些应用安全漏洞和利用这些漏洞的攻击进行检测和防御。

支持在 WEB 界面和安全中心上配置应用管理策略，可根据应用管理策略控制应用的使用，并支持在对象中搜索名称，提高了策略配置的效率和产品易用性。

4.3.4 全面精细的检测技术

◆ **业界领先的安全漏洞研究能力**

绿盟科技作为微软的 MAPP（Microsoft Active Protections Program）项目合作伙伴，可以在微软每月发布安全更新之前获得漏洞信息，为客户提供更及时有效的保护。

公司的安全研究部门 NSFocus 小组，已经独立发现了 40 多个 Microsoft、HP、CISCO、SUN、Juniper 等国际著名厂商的重大安全漏洞，保证了 NSFOCUS NIDS（N 系列）技术的领先和规则库的及时更新，在受到攻击以前就能够提供前瞻性的保护。

◆ **高品质攻击特征库**

覆盖广泛的攻击特征库携带超过 2000 条，由 NSFocus 安全小组精心提炼、经过时间考验的攻击特征，并通过国际最著名的安全漏洞库 CVE 严格的兼容性标准评审，获得最高级别的 CVE 兼容性认证（CVE Compatible）。

绿盟科技具有领先的漏洞预警能力，是目前国内唯一向国外（美国）出口入侵检测规则库的公司。绿盟科技每周定期提供攻击特征库的升级更新，在紧急情况下可提供即时更新。

◆ **全面深入的协议分析技术**

NSFOCUS NIDS（N 系列）全面深入的协议分析技术能够分析超过 100 种应用层协议，包括 HTTP、FTP、SMTP 等，极大地提高检测的准确性，降低误报率。

NSFOCUS NIDS（N 系列）通过分析网络报文中包含的协议特征，发现其所在协议，然后递交给相应的协议分析引擎进行处理，能够高速的、智能的、准确的检测出对运行在任意端口的应用层协议的攻击行为和标准协议运行在非标准端口行为，准确发现绑定在任意端口的各种木马、后门，对于运用了 Smart Tunnel 技术的软件也能准确地捕获分析。

NSFOCUS NIDS（N 系列）通过协议分析，发现任何违背 RFC 规定后，均视为协议异常。协议异常最为重要的作用是检测未知的溢出攻击与拒绝服务攻击，协议异常具有接近 100%的检测准确率和近乎零的误报率。

◆ **IP 碎片重组与 TCP 流汇聚**

NSFOCUS NIDS（N 系列）具有强大的 IP 碎片重组、TCP 流汇聚，以及数据流状态跟踪等能力，能够检测到黑客采用任意分片方式进行的攻击。

◆ **支持应用重组**

NSFOCUS NIDS（N 系列）可以记录网络的通信报文，并解码回放，目前支持 HTTP、SMTP、FTP、Telnet、POP3 等多种协议。

4.3.5 全面的 IPv6 支持

NSFOCUS NIDS（N 系列）基于 IPv4 和 IPv6 双协议栈的系统架构，能同时辨识 IPv4 和 IPv6 通讯流量。IPv6 环境下深度入侵检测技术和基于 IPv6 地址格式的安全策略，针对 IPv4 向 IPv6 的过渡，同时为 IPv4 与 IPv6 提供可靠的网络入侵检测服务。

4.3.6 可靠的 Web 威胁检测能力

越来越多的病毒、木马等恶意代码将基于 HTTP 方式传播，新一代的 Web 威胁具备混合性、渗透性和利益驱动性，成为当前增长最快的风险因素。员工对互联网的依赖性使得企业网络更容易受到攻击，导致用户信息受到危害，对公司数据资产和关键业务构成极大威胁。

NSFOCUS NIDS（N 系列）内置先进、可靠的 Web 信誉机制，采用独特的 Web 信誉评价技术，在用户访问被植入木马的页面时，给予及时报警，能够协助企业员工识别 Web 安全威胁，防止敏感信息外泄等安全事件的发生。

4.3.7 基于对象的虚拟系统

◆ **基于对象的策略管理系统**

NSFOCUS NIDS（N 系列）提供业界领先的基于对象的策略管理系统，完全统一的规则配置方式强大而灵活。NSFOCUS NIDS（N 系列）的所有策略（规则）配置都使用包括网络、服务、时间、事件等元素在内的预定义对象以及对象组完成，通过组的概念可以减少 NIDS 的规则数量，简化了产品的管理工作量。

◆ **虚拟系统（VIDS）**

NSFOCUS NIDS（N 系列）提供基于对象的虚拟系统（VIDS），针对不同的网络环境和安全需求，基于 IP 地址（组、段）、规则（组、集）、时间、动作等对象，制定不同的规则和响应方式，每个虚拟系统分别执行不同的规则集，实现面向不同对象、不同策略的智能化入侵检测。

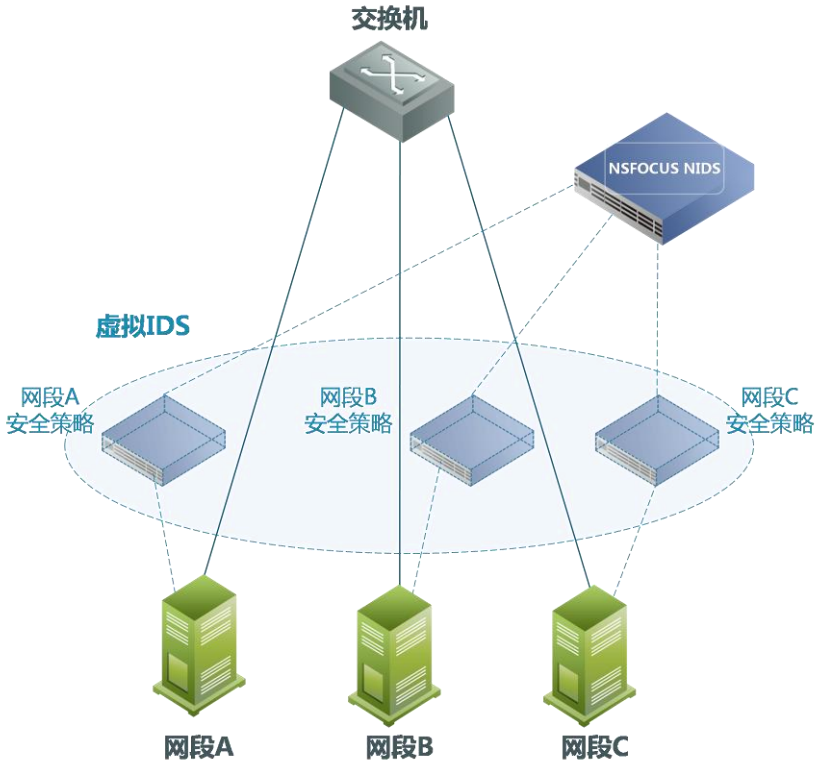

图 4.2　虚拟 IDS 功能实现示意图

4.3.8 细粒度的流量统计分析

NSFOCUS NIDS（N 系列）具有细粒度流量统计分析的功能，不是仅仅通过端口来判断协议进而统计流量，而是通过分析协议的内容后才进行统计，更精确可靠，同时能够基于 IP 地址、攻击事件、应用协议等条件产生详细的流量报表，可以通过编辑自定义统计指定协议流量的 TOP 排名，能够协助管理员了解当前网络带宽的使用状况，并及时做出响应。

4.3.9 全面的用户上网行为监测

NSFOCUS NIDS（N 系列）结合协议分析和会话关联等多种技术，综合分析应用软件特征和数据内容，能够智能识别和记录各种主流的 P2P 下载、IM 即时通信、在线视频、网络游戏和在线炒股等用户上网行为，以及加密型的 P2P 下载和 IM 即时通信。

通过对网络中各类应用所占用带宽情况的了解，能够让管理员清晰地识别出可能影响关键业务正常运转的流量，以便及时调整网络带宽管理策略。

4.3.10 可扩展的安全审计能力

NSFOCUS NIDS（N 系列）能够为用户提供可扩展的敏感信息审计方案，系统支持基于时间、用户、协议、内容等多种条件的组合审计策略，对邮件收发（WEBMAIL、SMTP、POP3）、文件上传下载（HTTP、FTP）、论坛、即时通讯等进行全面信息审计，提供实时告警、信息还原功能。系统同时支持基于关键字的信息审计，实现敏感信息的深度检测识别还原，对机密信息外泄、非法言论传播等行为的及时响应处理、事后追查取证提供有力支持。

4.3.11 强大的管理能力

◆ **灵活的 Web 管理方式**

NSFOCUS NIDS（N 系列）支持灵活的 Web 管理方式，适合在任何 IP 可达地点远程管理，支持 MS IE、Netscape、Firefox、Opera 等主路的浏览器，真正意义上实现了跨平台管理。

◆ **丰富的多级管理方式**

NSFOCUS NIDS（N 系列）支持三种管理模式：单级管理、多级管理、主辅管理，满足不同企业不同管理模式需要。

单级管理模式：安全中心直接管理网络探测器，一个安全中心可以管理多台网络探测器。

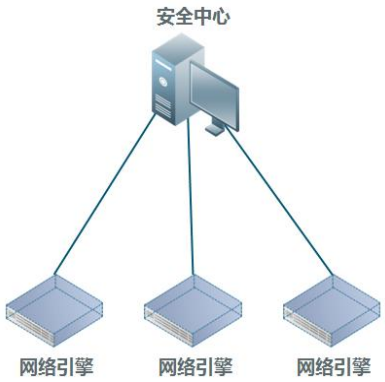

图 4.3 IDS 单级管理模式

主辅管理模式：网络探测器同时接受一个主安全中心和多个辅助安全中心管理。主安全中心可完全控制网络探测器；辅助安全中心只能接受网络探测器发送的日志信息，不能操作网络引擎。

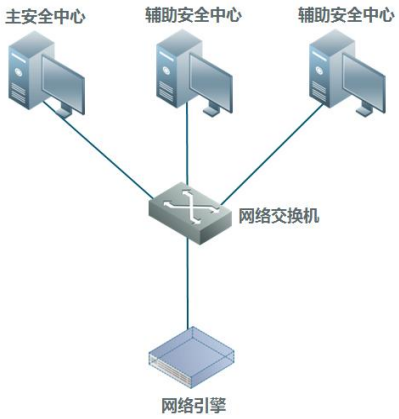

图 4.4 IDS 主辅管理模式

多级管理模式：安全中心支持任意层次的级联部署，实现多级管理。上级安全中心可以将最新的升级补丁、规则模板文件等统一发送到下级安全中心，保持整个系统的完整统一性；下级安全中心可以向上级安全中心传送日志信息。

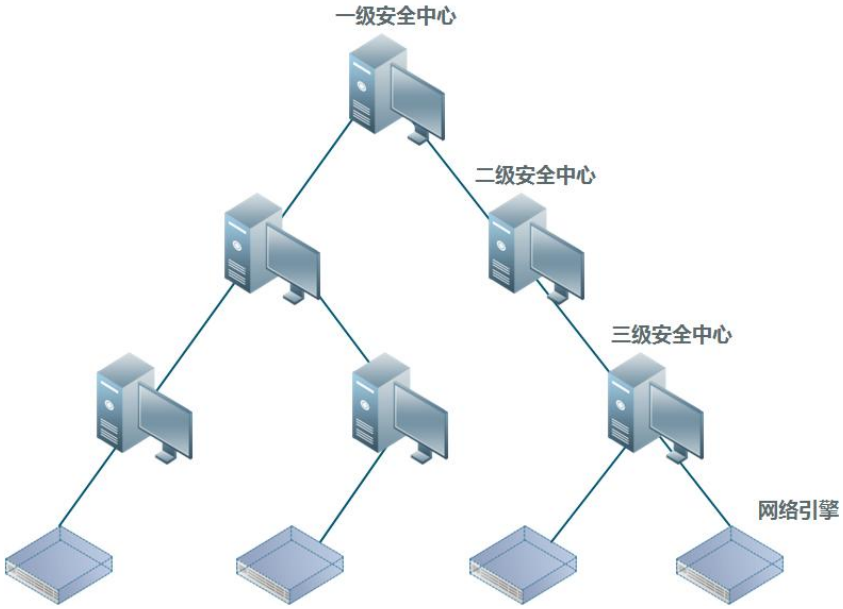

图 4.5 IDS 多级管理模式

◆ **带外管理（OOB）功能**

NSFOCUS NIDS（N 系列）提供带外管理（OOB）功能，解决远程应急管理的需求，减少用户运营成本、提高运营效率、减少宕机时间、提高服务质量。

◆ **升级管理**

NSFOCUS NIDS（N 系列）支持多种升级方式，包括实时在线升级、自动在线升级、离线升级，使 NIDS 提供最前沿的安全保障。

4.3.12 完善的报表系统

◆ **高品质的报表事件**

NSFOCUS NIDS（N 系列）事件过滤系统支持采用攻击发生时间范围、事件名称、事件类别、所属服务、源网络范围、目的网络范围、触发探测器、攻击结果、事件动作等多种粒度过滤探测器所产生的告警日志，仅记录相关的攻击告警事件，极大地减小了攻击告警的数量，提高了对于高风险攻击的反应速度。

◆ **多样化的综合报表**

NSFOCUS NIDS（N 系列）报表系统提供了详细的综合报表、自定义三种类型 10 多个类别的报表模板，支持生成：日、周、月、季度、年度综合报表。报表支持 MS Word、Html、JPG 格式导出。同时支持定时通过电子邮件发送报表至系统管理员。

◆ **强大的“零管理”**

从实时升级系统到报表系统，从攻击告警到日志备份，NSFOCUS NIDS（N 系列）完全支持零管理技术。所有管理员需要日常进行的操作均可由系统定时自动后台运行，极大地降低了维护费用与管理员的工作强度。

4.3.13 丰富的响应方式

◆ NSFOCUS NIDS（N 系列）具有良好的可扩展性，仅仅通过数字证书就能很方便、快捷地从 IDS 升级到 IPS，为用户未来的产品使用提供更广阔的空间。

◆ NSFOCUS NIDS（N 系列）可以与流行的主流防火墙产品（绿盟安全网关、Checkpoint FW、Netscreen、天融信、卫士通龙马、东软、迈普等）进行联动阻断入侵者。

◆ NSFOCUS NIDS（N 系列）具有 TCP KILLER 功能，能够实时地切断基于 TCP 协议的攻击行为。

◆ NSFOCUS NIDS（N 系列）支持通过发送邮件、安全中心显示、日志数据库记录、运行用户自定义命令等响应方式及时报警。

◆ NSFOCUS NIDS（N 系列）提供了基于 XML 的开放式 IDBP（Intrusion Detection and Block Protocol）联动接口，任何安全产品可以基于此接口与 NSFOCUS NIDS（N 系列）联动。

◆ NSFOCUS NIDS（N 系列）支持 CEF 通用事件格式，支持与 ArcSight 的无缝融合。

- NSFOCUS NIDS（N 系列）提供标准 snmp trap（V1、V2、V3）和 syslog 接口，可接受第三方管理平台的集中事件管理。

4.3.14 高可靠的自身安全性

- NSFOCUS NIDS（N 系列）采用安全、可靠的硬件平台，全内置封闭式结构，配置完全自主知识产权的专用系统，经过优化和安全性处理，稳定可靠。系统内各组件通过强加密的 SSL 安全通道进行通讯防止窃听，确保了整个系统的安全性和抗毁性。
- NSFOCUS NIDS（N 系列）具有更强的高可用性，设备支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，提高设备可用性。
- NSFOCUS NIDS（N 系列）监听网口无需设置 IP 地址，避免了被扫描和攻击。
- NSFOCUS NIDS（N 系列）的网络探测器与安全中心在网络完全断开的情况下，探测器仍然会将检测到的事件在探测器本地保存，等网络恢复正常自动地同步到绿盟安全中心，提供日志缓存。

4.4 解决方案

绿盟科技提供一整套的入侵检测解决方案，实现从企业网络核心至边缘及分支机构的全面检测。NSFOCUS NIDS（N 系列）的部署方式灵活多样，能够快速部署在几乎所有的网络环境中，满足不同企业不同管理模式需要。

4.4.1 小型网络之精细管理方案

针对小型网络，绿盟网络入侵检测解决方案提供虚拟 IDS 精细管理方案，通过基于对象的策略管理，NSFOCUS NIDS（N 系列）针对不同部门/网段，制定不同的规则和响应方式，每个虚拟系统分别执行不同的安全策略，实现面向不同对象、实现不同策略的智能化、精细化的入侵检测。如下图所示：

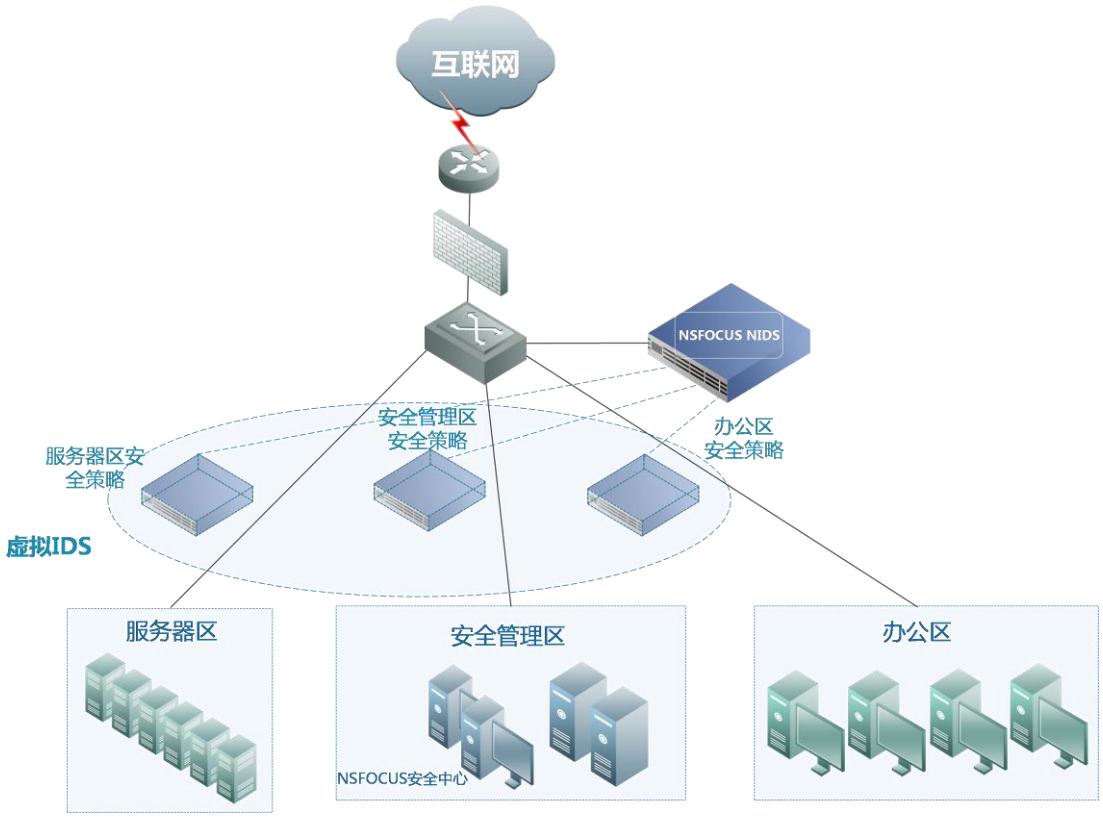

图 4.6　小型网络 IDS 精细管理部署方案

4.4.2 中型网络之集中管理方案

针对中型网络，绿盟网络入侵检测解决方案提供集中管理方案，通过将 NSFOCUS NIDS（N 系列）部署在多个关键网段（如安全管理区、DMZ 区、服务器区及办公区）实现多处监控。利用绿盟安全中心集中管理多台网络探测器，便于安全信息的集中管理，以便实时掌握全网的安全状况。如下图所示：

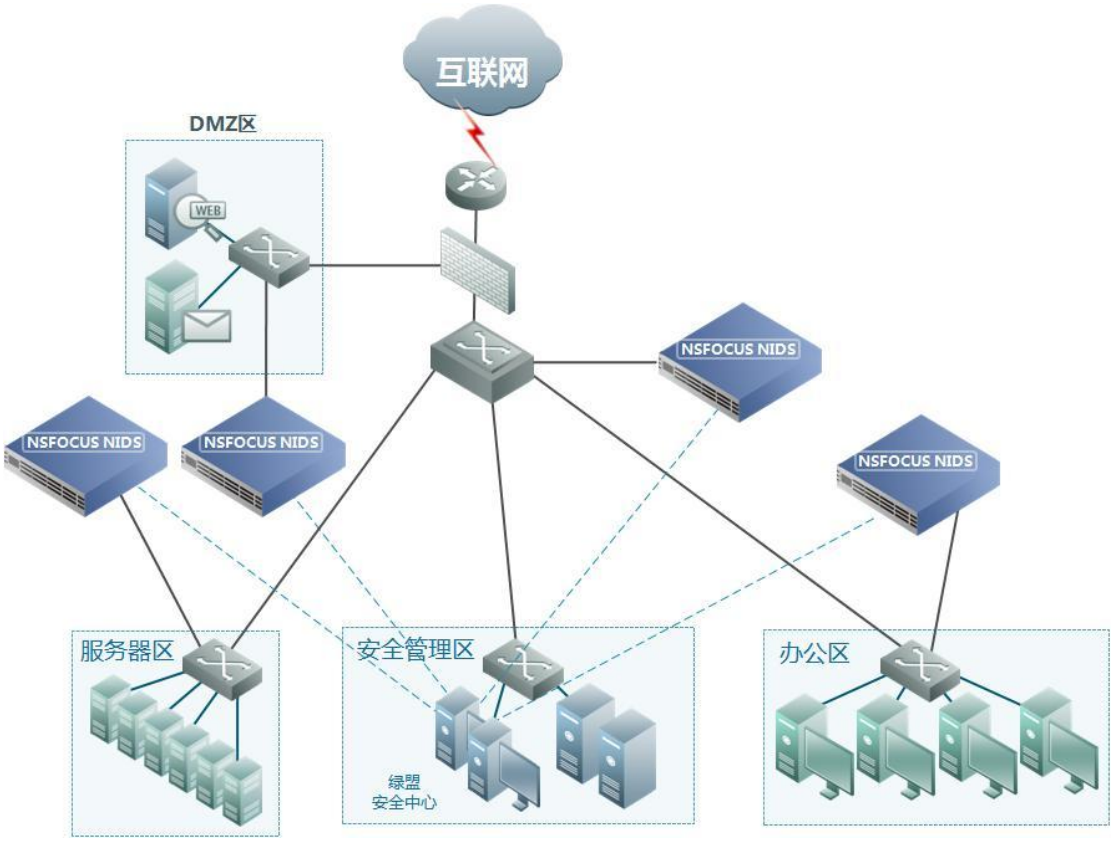

图 4.7　中型网络 IDS 集中管理部署方案

4.4.3 大型网络之分级管理方案

对于跨广域网的大型企业用户，其网络机构相对复杂，不仅有总部，全国各地还有分支机构，总部及下属各分支机构都建有自己的局域网络。用户租用 ISP 的专线建立自己覆盖全国的企业专网，各分支机构通过企业专网与总部建立业务信息交换。因此其对整个网络的管理比较重视，需要保证总部和各分支机构的安全策略的统一性。

针对大型企业用户，绿盟网络入侵检测解决方案提供分级管理方案，在各级网络上部署 NSFOCUS NIDS（N 系列）的多级安全中心，上级安全中心对下级安全中心进行统一管理，上级安全中心可以将最新的最新升级补丁、规则模板文件、探测器配置文件等统一发送到下级安全中心，保持整个系统的安全策略的完整统一性。如下图所示：

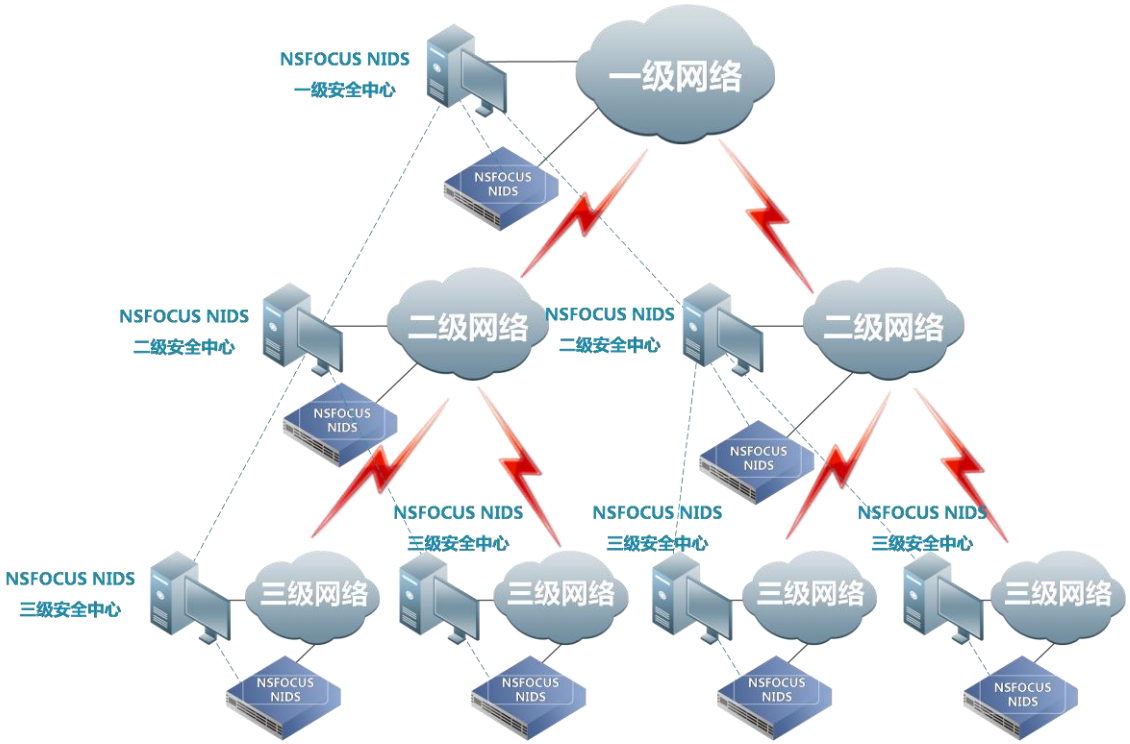

图 4.8　大型网络 IDS 分级管理部署方案

五. 结论

随着安全漏洞不断被发现，黑客的技巧和破坏能力不断提高，网络受到越来越多的攻击。每天成千上万的蠕虫、病毒、木马在网络上传播，阻塞甚至中断网络；BT、电驴等 P2P 下载软件轻易的占据 100%的企业网络上行下行带宽；员工沉浸在 QQ、MSN 等聊天或反恐精英、传奇等网络游戏中不能自拔，从而影响了正常的工作。这些新型的混合威胁越来越给企业造成巨大的损失，而对于上述威胁，传统防火墙、入侵检测系统和防病毒系统都无法有效地检测和阻止。

为了弥补目前安全设备（防火墙、入侵检测等）对攻击防护能力的不足，我们需要利用入侵检测技术，实时监控网络资源，不仅仅能够精确识别应用等各层面攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断，真正做到看得见、检得出、防得住。