文档编号：**NSF-PROD-NIPS-V5-WH**

冰之眼网络入侵保护系统
产品白皮书

中联绿盟信息技术(北京)有限公司
NSFOCUS INFORMATION TECHNOLOGY CO.,LTD.

版权声明

商标信息

绿盟科技、**NSFOCUS**、冰之眼等是中联绿盟信息技术（北京）有限公司的商标。

第三方信息

Microsoft、**Windows**是美国**Microsoft Corporation**的在美国和其它国家注册的商标

目 录

图 表

前言

文档范围

本文主要介绍冰之眼网络入侵保护系统（以下简称冰之眼或**NIPS**）的必要性、产品特点、体系架构和部署方式等。

期望读者

期望了解本产品主要技术特性的用户、系统管理员、网络管理员等。本文假设您对下面的知识有一定的了解：

- 系统管理
- **Linux**和**Windows**操作系统
- **Internet** 协议

获得帮助

获取网络安全相关资料，可以访问绿盟科技网站：www.nsfocus.com

获取本产品最新的相关信息可以访问网址：

http://www.nsfocus.com/homepage/products/nips.htm

您也可以给我们的技术支持工程师发送电子邮件，Email地址是：

product@nsfocus.com

获取更详尽的绿盟科技网络安全专业服务信息、商务信息，您可通过如下方式和我们联系：

北京总部

地址：北京市海淀区北洼路 4 号益泰大厦 3 层

邮编：100089

电话：010-68438880

传真：010-68437328

Email：webadmin@nsfocus.com

上海分公司

地址：上海市南京西路 758 号博爱大厦 9 楼 A 座

邮编：200041

电话：021-62179591/92

传真：021-62176862

广州分公司

地址：广州市人民中路 555 号美国银行中心 1702

邮编：510180

电话：020-81301251，81301252

传真：020-81301251/52

沈阳分公司

地址：沈阳市和平区文化路 45 号机械大厦 901 室

邮编：110003

电话：024－83891274

传真：024-23998066

成都分公司

地址：成都市顺城大街冠城广场 8 楼 C 座

邮编：610017

电话：028-86528249

传真：028-86528248

一．前言

随着网络与信息技术的发展，尤其是互联网的的广泛普及和应用，网络正逐步改变着人类的生活和工作方式。越来越多的政府、企业组织建立了依赖于网络的业务信息系统，比如电子政务、电子商务、网上银行、网络办公等，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。

网络的发展和普及为我们的工作和生活提供了便利，但同时也带来了更多的安全隐患。近年来，企业所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其混合威胁的风险，如蠕虫、病毒、间谍软件、DDoS 攻击、垃圾邮件、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，给企业的信息网络造成严重的破坏。

能否及时发现并成功阻止网络黑客的入侵、保证计算机和网络系统的安全和正常运行便成为企业所面临的一个重要问题。

二．为什么需要入侵保护系统

说起网络安全，相信许多人已经不陌生了，因为大家可能都曾遇到过下面这些情况：

- 没及时安装新发布的一个安全补丁，结果服务器宕机，网络中断；
- 蠕虫病毒爆发，造成网络瘫痪，无法网上办公，邮件收不了，网页打不开；
- 有的员工使用 BT、电驴等 P2P 软件下载电影或 MP3，造成上网速度奇慢无比；
- 有的员工沉迷在 QQ 或 MSN 上聊天，或者玩反恐精英、传奇等网络游戏，或者看在线视频，不专心工作；
- 由于员工电脑被植入间谍软件，公司机密资料被窃；

根据调查数据显示，以上事件呈逐年上升趋势，给企业造成越来越大的直接和间接损失。对于上述威胁，传统的安全手段（如防火墙、入侵检测系统）都无法有效进行阻止。

2.1 防火墙的局限

绝大多数人在谈到网络安全时，首先会想到“防火墙”。防火墙得到了广泛的部署，企业一般采用防火墙作为安全保障体系的第一道防线，防御黑客攻击。但是，随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙已经无法满足企业的安全需要。传统防火墙的不足主要体现在以下几个方面：

- 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 Code Red 蠕虫等。
- 有些主动或被动的攻击行为是来自防火墙内部的，防火墙无法发现内部网络中的攻击行为。

由于防火墙具有以上一些缺陷，所以部署了防火墙的安全保障体系还有进一步完善的需要。

2.2 入侵检测系统的不足

入侵检测系统 IDS（ Intrusion Detection System）是近几年来发展起来的一类安全产品，它通过检测、分析网络中的数据流量，从中发现网络系统中是否有违反安全策略的行为和被攻击的迹象。它弥补了防火墙的某些缺陷，但随着网络技术的发展，IDS 受到新的挑战：

- IDS 旁路在网络上，当它检测出黑客入侵攻击时，攻击已到达目标造成损失。IDS 无法有效阻断攻击，比如蠕虫爆发造成企业网络瘫痪，IDS 无能为力。
- 蠕虫、病毒、DDoS 攻击、垃圾邮件等混合威胁越来越多，传播速度加快，留给人们响应的时间越来越短，使用户来不及对入侵做出响应，往往造成企业网络瘫痪，IDS 无法把攻击防御在企业网络之外。

我们看到，入侵检测系统 IDS 侧重网络监控，注重安全审计，适合对网络安全状态的了解。

2.3 入侵保护系统的特点

基于目前网络安全形势的严峻，入侵保护系统 IPS（Intrusion Prevention System）作为新一代安全防护产品应运而生。

入侵保护系统 IPS 提供一种主动的、实时的防护，其设计旨在对常规网络流量中的恶意数据包进行检测，阻止入侵活动，预先对攻击性的流量进行自动拦截，使它们无法造成损失，而不是简单地在监测到恶意流量的同时或之后发出警报。IPS 是通过直接串联到网络链路中而实现这一功能的，即 IPS 接收到外部数据流量时，如果检测到攻击企图，就会自动地将攻击包丢掉或采取措施将攻击源阻断，而不把攻击流量放进内部网络。

从 IPS 的工作原理来看，IPS 有几个主要的特点：

- 为企业网络提供“**虚拟补丁**”

IPS 预先、自动拦截黑客攻击、蠕虫、网络病毒、DDoS 等恶意流量，使攻击无法到达目的主机，这样即使没有及时安装最新的安全补丁，企业网络仍然不会受到损失。IPS 给企业提供了时间缓冲，在厂商就新漏洞提供补丁和更新之前确保企业的安全。

- 提供“**流量净化**”

目前企业网络遭受到越来越多的流量消耗类型的攻击方式，比如蠕虫、病毒造成网络瘫痪、BT、电驴等 P2P 下载造成网络带宽资源严重占用等。IPS 过滤正常流量中的恶意流量，为网络加速，还企业一个干净、可用的网络环境。

- 提供“**反间谍**”能力

企业机密数据被窃取，个人信息甚至银行账户被盗，令许多企业和个人蒙受重大损失。IPS 可以发现并阻断间谍软件的活动，保护企业机密。

入侵保护系统 IPS 的设计侧重访问控制，注重主动防御，而不仅仅是检测和日志记录，解决了入侵检测系统 IDS 的不足，为企业提供了一个全新的入侵保

护解决方案。

三．如何评价入侵保护系统

针对越来越多的蠕虫、病毒、间谍软件、垃圾邮件、DDoS 等混合威胁及黑客攻击，不仅需要有效检测到各种类型的攻击，更重要的是降低攻击的影响，从而保证业务系统的连续性和可用性。

一个完善的入侵保护系统 IPS 应该从四个方面考虑：

- 实时、主动的阻断攻击；
- 精确检测出恶意攻击流量；
- 从性能和架构上支持入口点部署，保障整体安全；
- 具备很强的扩展性和良好的可靠性；

基于以上四点，入侵保护系统 IPS 应具备以下特征：

- 支持在线模式部署，第一时间把攻击阻断在企业网络之外，同时也支持旁路模式部署，用于攻击检测。
- 准确识别攻击，避免影响正常的业务通讯。
- 满足高性能、高可靠性的要求，达到网络服务的质量保证。
- 提供灵活的部署方式保护现有投资。

四．绿盟科技网络入侵保护系统

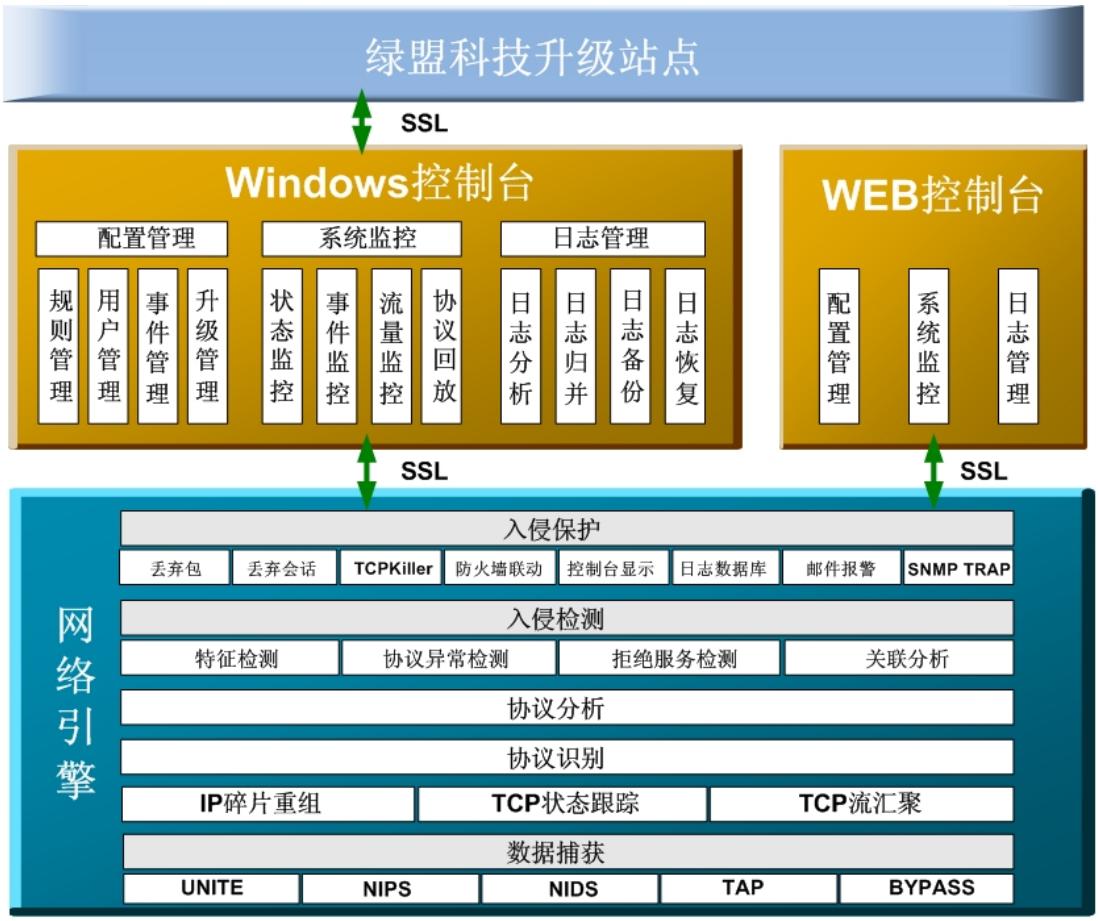
针对目前流行的蠕虫、病毒、间谍软件、垃圾邮件、DDoS 等黑客攻击，以及网络资源滥用（P2P 下载、IM 即时通讯、网游、视频……），绿盟科技提供了完善的安全防护方案。冰之眼网络入侵保护系统（ICEYE NIPS）是绿盟科技入侵保护解决方案的核心，作为自主知识产权的新一代安全产品，先进的体系架构集成领先的入侵保护技术，包括以全面深入的协议分析技术为基础，协议识别、协议异常检测、关联分析为核心的新一代入侵保护引擎，实时拦截数据流量中各

种类型的恶意攻击流量，把攻击防御在企业网络之外，保护企业的信息资产。

冰之眼网络入侵保护系统能够协助客户：

- 阻止来自外部或内部的蠕虫、病毒和黑客等的威胁，确保企业信息资产的安全。
- 阻止间谍软件的威胁，保护企业机密。
- 阻止企业员工因为各种 IM 即时通讯软件、网络在线游戏、P2P 下载、在线视频导致的企业网络资源滥用而影响正常工作，净化流量，为网络加速。
- 阻止 P2P 应用可能导致的企业重要机密信息泄漏和可能引发的与版权相关的法律问题。
- 实时保障企业网络系统 7x24 不间断运行，提高企业整体的网络安全水平。
- 智能、自动化的安全防御，降低企业整体的安全费用以及对于网络安全领域人才的需求。
- 高效、全面的流量分析、事件统计，能迅速定位网络故障，提高网络稳定运行时间。

4.1 体系架构



图表 1 绿盟科技网络入侵保护系统体系架构

冰之眼网络入侵保护系统的体系架构包括三个主要组件：控制台、网络引擎、升级站点，方便各种网络环境的灵活部署和管理。

4.2 产品特点

4.2.1 实时的主动防御

- 冰之眼网络入侵保护系统提供“虚拟补丁”，为企业提供了时间缓冲，在厂商就新漏洞提供补丁和更新之前确保企业的安全。
- 冰之眼 NIPS 提供准确和智能的检测和防护，以预防已知和未知攻击，使需要管理人员干预的程度最小化，有效减轻攻击报警处理的压力。

- 冰之眼 NIPS 与内置防火墙的完美集成提供了更高级的防护功能，同时还可获得更强的访问控制功能和灵活性，并降低总拥有成本。
- 冰之眼 NIPS 提供丰富的流量管理机制，可以基于规则、通断、时间、IP 地址等多种条件组合，灵活控制网络流量。
- 绿盟科技拥有著名的安全研究部门 NSFocus 小组，已经独立发现了 20 余个 Microsoft、HP、CISCO、SUN、Juniper 等国际著名厂商的重大安全漏洞，保证了冰之眼 NIPS 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。

4.2.2 准确的检测/防护

- 冰之眼 NIPS 全面深入的协议分析技术能够分析近 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。
- 冰之眼 NIPS 独有的协议识别技术能够识别近 100 种包括后门、木马、IM、网络游戏在内的应用层协议，不仅可以更有效的检测通过动态端口或者智能隧道等进行的恶意入侵，并且能更好的提高检测效率和准确率。
- 冰之眼 NIPS 出色的协议异常检测针对检测未知的溢出攻击与拒绝服务攻击，达到接近 100%的检测准确率和几乎为零的误报率。
- 冰之眼 NIPS 能够有效防御拒绝服务攻击 DoS，阻止攻击者消耗网络资源、中止服务。
- 覆盖广泛的攻击规则库带有超过 1800 条由 NSFocus 安全小组精心提炼、经过仔细检测与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）。

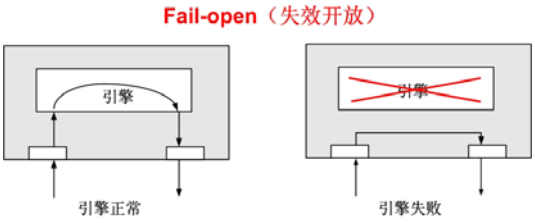
而且绿盟科技具有领先的漏洞预警能力，是目前国内唯一一个向国外（美国）出口入侵检测规则库的公司。绿盟科技每月平均提供四到五次升级更新，在紧急情况下可即时提供更新。

4.2.3 优异的产品性能

- 冰之眼 NIPS 专门设计了安全、可靠、高效的硬件运行平台。硬件平台采用严格的设计和工艺标准，保证了高可靠性；独特的硬件体系结构大大提升了处理能力、吞吐量；操作系统经过优化和安全性处理，保证系统的安全性和抗毁性。
- 冰之眼 NIPS 依赖先进的体系架构、高性能专用硬件，在实际网络环境部署中性能表现优异，具有线速的分析与处理能力。

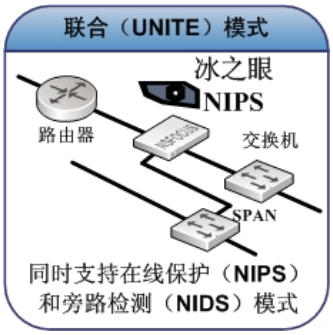
4.2.4 高可靠、可扩展

- 冰之眼 NIPS 支持失效开放（Fail-open）机制，当出现软件故障、硬件故障、电源故障时，系统自动切换到直通状态以保障网络可用性，避免单点故障。同时在国内首家支持内置的千兆硬件 BYPASS 功能（光纤口/以太口）。

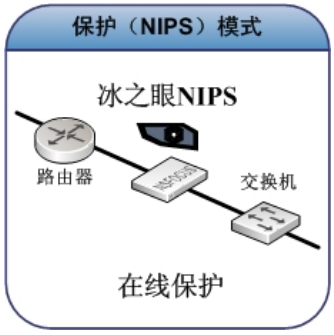


- 冰之眼 NIPS 支持双机热备 HA，不仅支持 Active-Standby（主从热备），还支持 Active-Active（对等热备），提供高可用性保障。

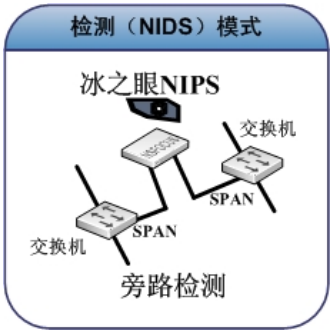
- 冰之眼 NIPS 的工作模式灵活多样，支持五种模式：联合（UNITE）、保护（NIPS）、检测（NIDS）、分接（TAP） 、直通（BYPASS），能够快速部署在几乎所有的网络环境中。当用户网络结构改变时，可根据用户变化后的安全需求调整部署方式，继续使用，从而保护用户投资。



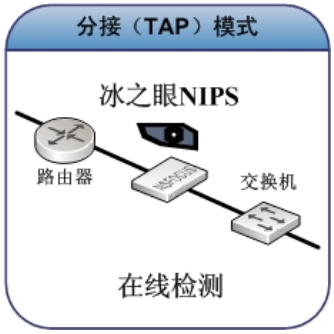
联合（UNITE）模式：这是冰之眼 NIPS 出厂的缺省模式，同时支持 NIPS 和 NIDS 两种模式。冰之眼 NIPS 的两个网络端口以一进一出的方式，串联在网络链路上，形成 NIPS 模式，通过实时拦截恶意流量来防止网络攻击；另外的网络端口连接到集线器端口或交换机的 SPAN 端口上，形成 NIDS 模式，对网络中的数据流量进行入侵检测。在联合（UNITE）模式中，NIPS 和 NIDS 共同运行，既对进出数据流量进行入侵防护，也对其他网段提供入侵检测，节约客户投资。



保护（NIPS）模式：冰之眼 NIPS 的两个网络端口以一进一出的方式，串联在网络链路上。数据流量经过 NIPS 时，NIPS 对数据流进行深入全面的检测，对发现的恶意攻击流量实时阻断。实时的主动防御使得冰之眼 NIPS 能够快速阻止来自蠕虫、病毒、间谍软件和黑客的威胁，把攻击防御在企业网络之外。

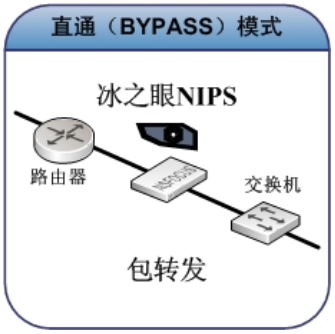


检测（NIDS）模式：冰之眼 NIPS 的网络端口连接到集线器端口或交换机的 SPAN 端口上，实际上就是纯粹意义上的入侵检测系统 NIDS。冰之眼 NIPS 以旁路的方式，对网络中的数据流量进行入侵检测，对攻击提供响应措施，如与防火墙联动、TCP Killer 等。



分接（TAP）模式：冰之眼 NIPS 的两个网络端口以一进一出的方式，串联在网络链路上。数据流量经过 NIPS 时，NIPS 对数据流仅仅检测，但不阻断。这种模式解决如下问题：1、全双工的监听；2、快速部署；3、交换机不支持双向镜像。

直通（BYPASS）模式：冰之眼 NIPS 的两个网络端口以一进一出的方式，串联在网络链路上。数据流量经过 NIPS 时，NIPS 旁路引擎，直接包转发，不做检测和阻断。这种模式主要用于网络调试，排除引擎故障。



- 冰之眼 NIPS 提供丰富的响应方式，包括主动响应（丢弃数据包、丢弃连接会话）、被动响应（与防火墙联动、TCP Killer、发送邮件、控制台显示、日志数据库记录、打印机输出、运行用户自定义命令、写入 XML 文件、snmp trap），用户可自定义，满足各种需要。
- 冰之眼 NIPS 运行在特别定制的操作系统上，在提供给网络引擎强健的性能与稳定性的同时，本身具备了超强的安全性。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。

4.2.5 强大的管理能力

- 冰之眼 NIPS 同时支持 B/S 和 C/S 模式，用户不需要安装任何客户端即可管理冰之眼网络引擎。
- 从实时升级系统到报表系统，从攻击告警到日志备份，冰之眼 NIPS 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。

- 冰之眼 NIPS 支持三种管理模式：单级管理、主辅管理、多级管理，满足不同企业不同管理模式需要。

  单级管理模式：控制台直接管理网络引擎，一个控制台可以管理多台网络引擎。适合小型企业，用于局域网络。

  主辅管理模式：网络引擎同时接受一个主控制台和多个辅控制台的管理。主控制台可以完全控制网络引擎；辅控制台只能接受网络引擎发送的日志信息，不能操作网络引擎。适合大型企业或者有分权管理需求的用户。

  多级管理模式：控制台支持任意层次的级联部署，实现多级管理。上级控制台可以将最新的升级补丁、规则模板文件等统一发送到下级控制台，保持整个系统的完整统一性；下级控制台可以通过配置过滤器，使上级控制台只接收它关心的信息。适合跨广域网的大型企业用户。
- 实时在线升级、自动在线升级、离线升级、串口升级、SSH 远程升级，冰之眼 NIPS 支持多种升级方式，使 NIPS 提供最前沿的安全保障。
- 全中文界面、中文报表，符合中国人操作习惯，而中文规则库对每个漏洞都有详细描述，并提供了详细的解决方案及补丁下载地址。
- 控制台提供体验模式，模拟的数据动态显示，有利于用户学习掌握。

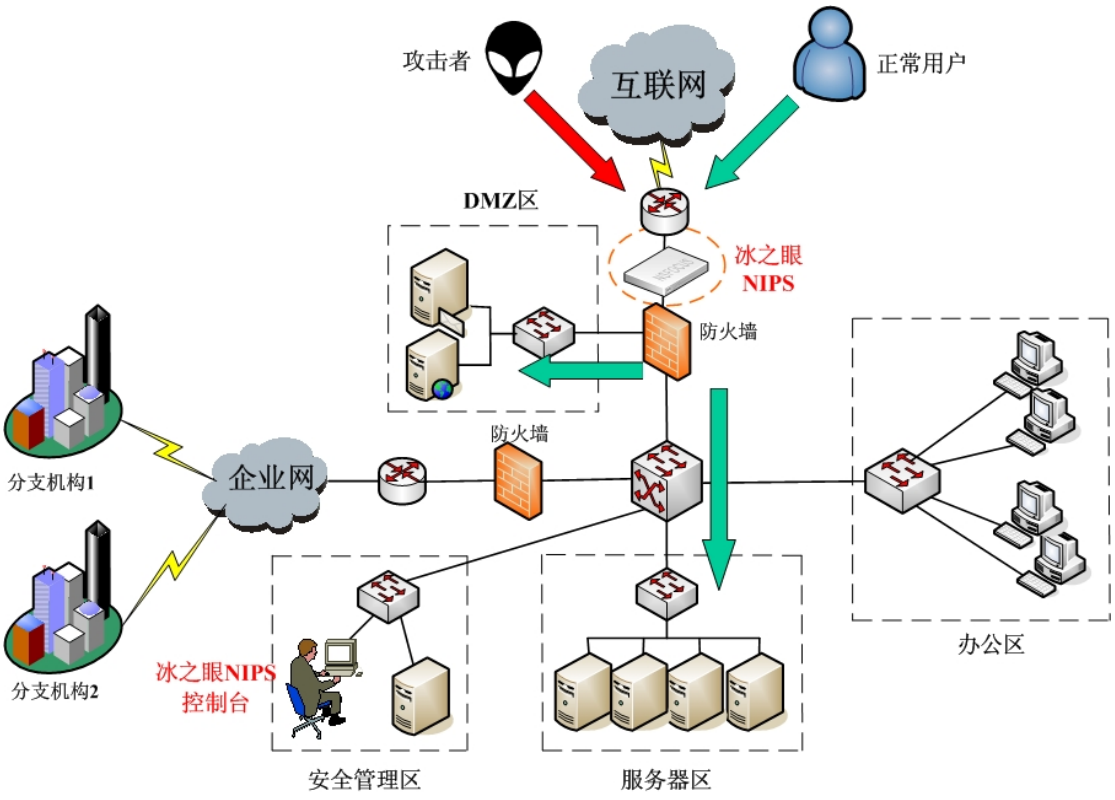
4.3 部署方式

绿盟科技提供一整套的入侵保护解决方案，具有良好可扩展性的冰之眼网络入侵保护系统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，实现从企业网络核心至边缘及分支机构的全面保护，适用于不同环境不同企业的安全需求。

4.3.1 边界防护部署

互联网的迅速发展，改变了人们的工作和生活方式，使企业越来越依赖互联网，大量业务应用通过互联网运行，然而互联网的开放性造成其安全性很差，大量的蠕虫、病毒、间谍软件、DDoS、垃圾邮件等在互联网上泛滥，而且攻击手段在不断增加，因此企业网络的互联网出入口承受着巨大的安全压力。

针对来自外部的攻击，绿盟入侵保护解决方案提供在线防御的部署模式，通过冰之眼网络入侵保护系统 NIPS“串联”在互联网出入口，实时拦截数据流量中各种类型的恶意攻击流量，把攻击防御在企业网络之外，保护企业的信息资产。如下图所示：



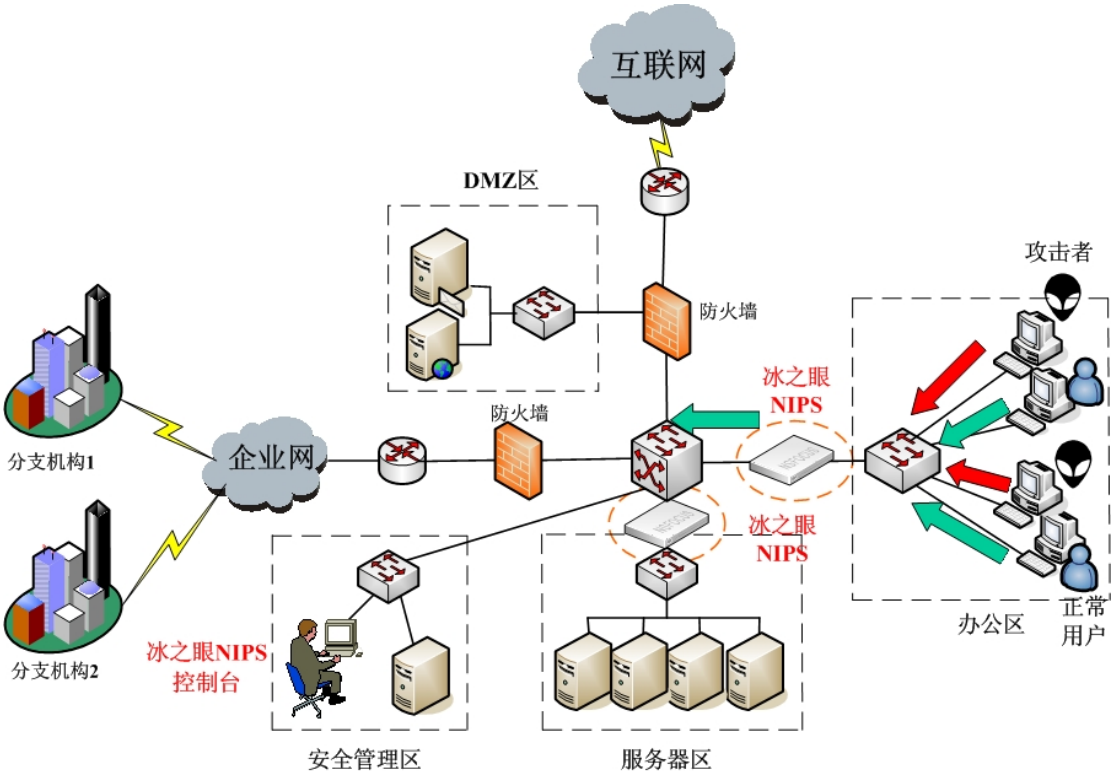
图表 2 边界防护部署方式

4.3.2 重点防护部署

由于安全技能和安全意识存在差异，企业员工可能无意识的通过互联网络将恶意代码下载到内部网络执行，甚至将 Internet 上的蠕虫、病毒、间谍软件传播

进入内部网络，阻塞甚至中断网络，而 BT、电驴等 P2P 下载软件轻易的占据 100%的企业网络带宽，这都对企业网络的安全带来严重威胁。

针对来自内部的攻击，绿盟入侵保护解决方案提供在线防御的部署模式，通过冰之眼网络入侵保护系统 NIPS“串联”在办公区出入口、重要服务器区出入口，实时拦截数据流量中各种类型的恶意攻击流量，把办公区内的蠕虫、病毒、间谍软件等混合攻击过滤掉，防止影响企业网络的整体安全运行，保护关键服务器等企业重要信息资产。如下图所示：



图表 3 重点防护部署方式

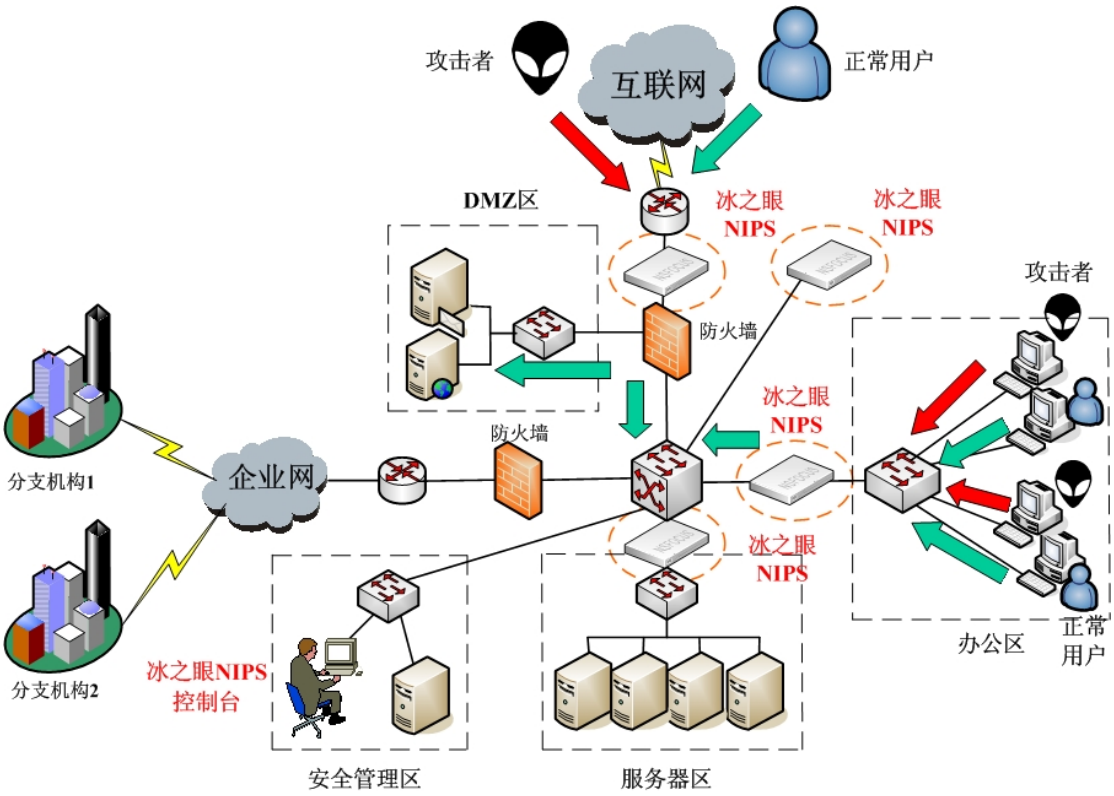
4.3.3 混合防护部署

面对复杂多变的安全形势，企业不仅需要有效的攻击防御，还需要全面的安全监控。

针对来自外部和内部的攻击，绿盟入侵保护解决方案提供在线防御的部署模式，通过冰之眼网络入侵保护系统 NIPS“串联”在关键网络链路上，实时拦截数据流量中各种类型的恶意攻击流量，保护企业的重要信息资产。

同时也可以把冰之眼网络入侵保护系统 NIPS 以“旁路”方式部署在企业网络的重要部位，相当于入侵检测系统，监测、分析企业网络内部的安全状况，保护企业安全。

两种部署方式的相互配合提高企业网络整体安全水平。如下图所示：



图表 4 混合防护部署方式

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、垃圾邮件在网络上传播，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、传奇等网游中不能自拔，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，我们需要一种新的工具用于保护业务系统不受黑客攻击的影响。这种工具不仅仅能够精确识别各种黑客攻击，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。

绿盟科技的冰之眼网络入侵保护系统提供了业界领先的实时、主动的防护能力，通过新一代的入侵保护技术，绿盟的产品和技术能够有效的阻断攻击，保证合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。