无标题-4

|  |  |  |  |
| --- | --- | --- | --- |
| 绿盟下一代网络入侵防护系统  产品白皮书  【绿盟科技】 | | | |
| ■ 文档编号 | NSF-PROD-NIPS-产品白皮书-V1.0 | ■ 密级 | 完全公开 |
| ■ 版本编号 | V1.0 | ■ 日期 | 2014-06-01 |
| * 撰 写 人 | 唐伽佳 | ■ 批准人 |  |



|  |
| --- |
| © 2014 绿盟科技 |

|  |
| --- |
| ■ 版权声明 |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
| 2014-06-01 | V1.0 | 新建 | 唐伽佳 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 前言 1](#_Toc329673707)  [二. 攻防的新特点 1](#_Toc329673708)  [三. 绿盟下一代网络入侵防护系统 2](#_Toc329673709)  [3.1 体系结构 4](#_Toc329673710)  [3.2 主要功能 4](#_Toc329673711)  [3.3 产品特点 5](#_Toc329673712)  [3.3.1 全新的高性能软硬件架构 5](#_Toc329673713)  [3.3.2 用户身份识别与控制功能 5](#_Toc329673714)  [3.3.3 更精细的应用层安全控制 6](#_Toc329673715)  [3.3.4 基于用户身份的行为分析 6](#_Toc329673716)  [3.3.5 全面支持IPv6 6](#_Toc329673717)  [3.3.6 多种技术融合的入侵检测机制 6](#_Toc329673718)  [3.3.7 2~7层深度入侵防护能力 8](#_Toc329673719)  [3.3.8 先进的Web威胁抵御能力 9](#_Toc329673720)  [3.3.9 基于对象的虚拟系统 9](#_Toc329673721)  [3.3.10 基于应用的流量管理 10](#_Toc329673722)  [3.3.11 强大的管理能力 11](#_Toc329673723)  [3.3.12 完善的报表系统 11](#_Toc329673724)  [3.3.13 完备的高可用性 12](#_Toc329673725)  [3.3.14 丰富的响应方式 12](#_Toc329673726)  [3.3.15 高可靠的自身安全性 13](#_Toc329673727)  [3.4 解决方案 13](#_Toc329673728)  [3.4.1 多链路防护解决方案 13](#_Toc329673729)  [3.4.2 混合防护解决方案 14](#_Toc329673730)  [四. 结论 15](#_Toc329673731) |

|  |
| --- |
| 插图索引 |
| [图 3.1 绿盟网络入侵防护系统体系架构 4](#_Toc329673701)  [图 3.2 虚拟IPS功能实现示意图 10](#_Toc329673702)  [图 3.3 NSFOCUS NIPS多链路防护解决方案 14](#_Toc329673703)  [图 3.4 NSFOCUS NIPS混合防护解决方案 15](#_Toc329673704) |

1. 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，原有的安全检测和防护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，更有效地检测和防御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和防护的实践，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防护系统，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、防得住的下一代入侵防护解决方案，标志着国内入侵防护市场迈入一个新的时代。

1. 攻防的新特点

随着网络的发展，网络应用不断丰富以及Web 2.0应用快速向业务环境渗透，大量应用建立在HTTP等基础[协议](http://cisco.chinaitlab.com/List_11.html" \t "_blank)之上，或者随机产生端口号，或者采用SSL加密等方式来隐藏内容，应用层面临的恶意威胁越来越多。

* **应用层攻击**

互联网的快速发展，使得单位的网络应用已经开始变的复杂多样，应用复杂度提高，安全威胁向应用化、深层化转变，隐藏在应用中的攻击增多，越来越多的基于应用的攻击行为出现了，网络攻击也开始转向应用层。据Gartner统计：目前75%攻击转移到应用层。

* **恶意文件攻击**

系统运维者一般只关心操作系统、网络设备的安全问题，而很少在意文件的漏洞。近年来，通过恶意文件开展攻击比较普遍。将攻击代码埋设在Word、Excel、PDF及Flash等正常格式文件中，这类文件隐蔽性高、欺骗性强，只要用户访问这类文件，个人电脑就有遭到劫持的危险，从而威胁系统和网络的安全。

* **用户身份攻击**

原有仅针对IP采用的安全防护方法已经不能适应当前系统网络攻防的发展，仅依赖 IP的防护手段无法准确识别用户身份，无法基于用户身份做细粒度的策略管理。

* **异常行为攻击**

对于传统的攻击行为，我们仅需关注恶意程序的样本提取并做分析，便可以掌握攻击者的动机及传播渠道，但对于以APT为代表的异常行为攻击以点概面的安全检测手段已显得不合时宜。这类攻击伪装成正常流量，没有特别大的数据包，地址和内容也没有可疑的不相配，所以一般不会触发警报。即利用合法身份掩护，实施非法行为。同时通过加密通道外传数据，面对这类攻击威胁，我们应当有一套更完善、更主动、更智能的安全防御体系。

* **安全防护的性能要求**

网络带宽增长迅速，网络正在从千兆走向万兆甚至更多。为应对这种变化，要求安全防护设备应有足够的性能和扩展性。

* **IPV6所带来的安全问题**

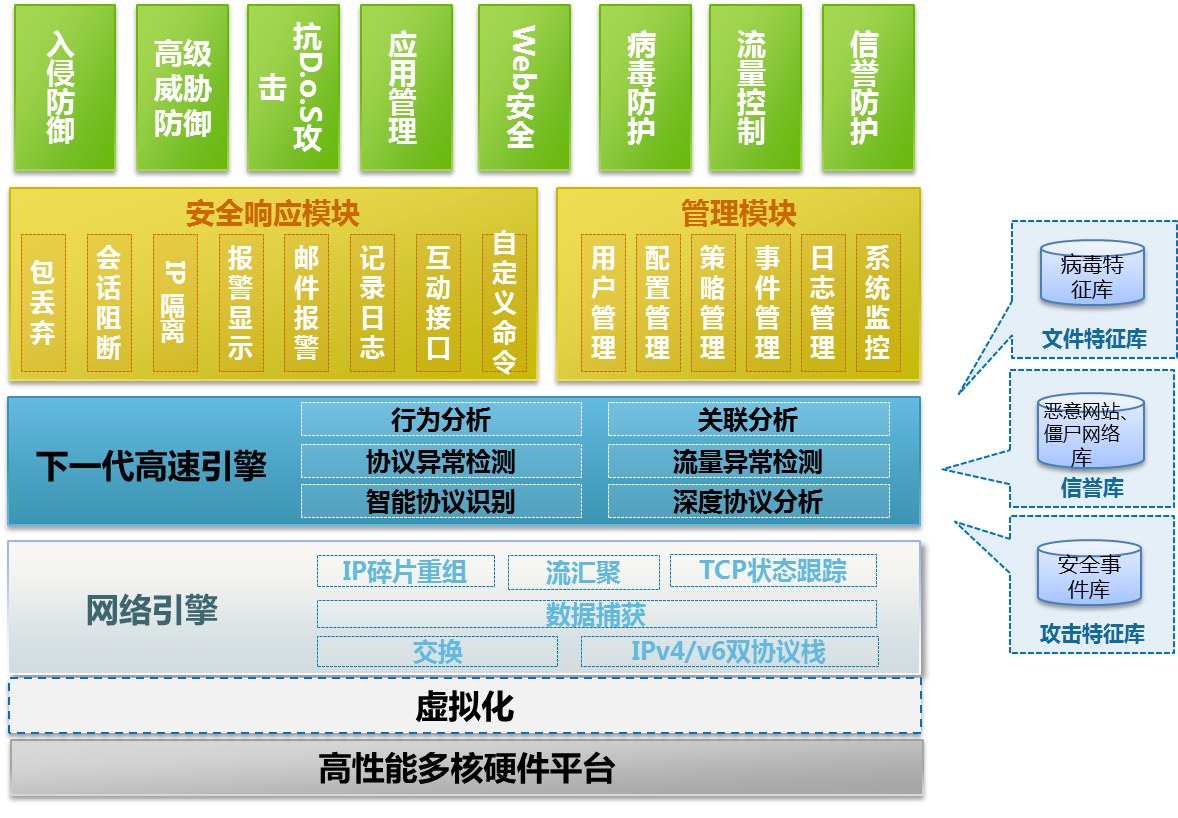
IPv6已是大势所趋，IPv6的使用会带来一些独特的安全难题，如何在保证业务[正常运营](http://www.chinabyte.com/keyword/正常运营/)的前提下安全平滑过渡以及保证安全防护在IPv4网络和IPv6网络上均实现无缝稳定地运行，是单位十分头疼的问题，

1. 绿盟下一代网络入侵防护系统

针对日趋复杂的应用安全威胁和混合型网络攻击，绿盟科技提供了完善的安全防护方案。绿盟下一代网络入侵防护系统（以下简称“NSFOCUS NIPS”）是绿盟科技拥有完全自主知识产权的新一代安全产品，作为一种在线部署的产品，其设计目标旨在适应攻防的最新发展，准确监测网络异常流量，自动应对各层面安全隐患，第一时间将安全威胁阻隔在企业网络外部。这类产品弥补了防火墙、入侵检测等产品的不足，提供动态的、深度的、主动的安全防御。为应对新型攻击带来的威胁，从智能识别、环境感知、行为分析三方面加强了对应用协议、异常行为、恶意文件的检测和防护，为企业提供了一个看得见、检得出、防得住的全新入侵防护解决方案。

* 1. 体系结构

NSFOCUS NIPS的体系架构包括三个主要组件：网络引擎、管理模块、安全响应模块，方便各种网络环境的灵活部署和管理。

****

绿盟网络入侵防护系统体系架构

* 1. 主要功能

NSFOCUS NIPS是网络入侵防护系统同类产品中的精品典范，该产品高度融合高性能、高安全性、高可靠性和易操作性等特性，产品内置先进的信誉防护机制，同时具备深度入侵防护、高级威胁防护、精细流量控制等多项功能，能够为用户提供深度攻击防御的完美价值体验。

* **入侵防护**

实时、主动拦截黑客攻击、蠕虫、网络病毒、后门木马、D.o.S等恶意流量，保护企业信息系统和网络架构免受侵害，防止操作系统和应用程序损坏或宕机。

* **高级威胁防护**

高级威胁防护能够基于敏感数据的外泄、文件识别、服务器非法外联等异常行为检测，实现内网的高级威胁防护功能。

* **僵尸网络发现**

基于实时的信誉机制，结合企业级和全球信誉库，可有效检测恶意URI、僵尸网络，保护用户在访问被植入木马等恶意代码的网站地址时不受侵害，第一时间有效拦截Web威胁，并且能及时发现网络中可能出现的僵尸网络主机和C&C连接。

* **流量控制**

阻断一切非授权用户流量，管理合法网络资源的利用，有效保证关键应用全天候畅通无阻，通过保护关键应用带宽来不断提升企业IT产出率和收益率。

* **应用管理**

全面监测和管理IM即时通讯、P2P下载、网络游戏、在线视频，以及在线炒股等网络行为，协助企业辨识和限制非授权网络流量，更好地执行企业的安全策略。

* 1. 产品特点

NSFOCUS NIPS基于高性能硬件处理平台，为客户提供从网络层、到应用层，直至内容层的深度安全防御，以下将对NSFOCUS NIPS的产品功能特色进行逐一介绍。

* + 1. 全新的高性能软硬件架构

NSFOCUS NIPS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。

* + 1. 用户身份识别与控制功能

NSFOCUS NIPS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NIPS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 NIPS产品丰富的应用识别能力，可实现细粒度访问控制。

* + 1. 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 NIPS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。

* + 1. 基于用户身份的行为分析

系统中的用户根据各自的工作职责和个人爱好都会形成各自的行为习惯，这种行为习惯能够反应在日常的网络访问活动中。对这些网络访问活动进行分析并经过长时间地收敛，可以根据用户身份（Who）、地理位置/IP地址（Where）、业务系统/网络应用（Whom）、操作（What）、时间（When）、频次（How）等条件建立用户的正常网络访问模型。建立基于正常网络访问模型的单位网络“白环境”，当检测到网络中出现了违背白环境模型的异常行为时，则对其进行深入分析，以判断是否是攻击。

NSFOCUS NIPS在用户身份识别、应用识别的基础上，将用户身份、业务系统、地理位置、操作频次等多种与操作相关的网络环境信息进行关联分析，建立企业网络白环境，准确识别用户异常行为。

* + 1. 全面支持IPv6

双协议栈(dual stack)架构，支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。多种隧道模式的支持，确保IPv6过渡时代的网络通畅。IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略，为IPv6环境提供了有力的入侵防护能力。

NSFOCUS NIPS通过了IPv6 Ready 认证，

保证了在IPv6环境下的互联互通。

* + 1. 多种技术融合的入侵检测机制

NSFOCUS NIPS以全面深入的协议分析为基础，融合权威专家系统、智能协议识别、协议异常检测、流量异常检测、会话关联分析，以及状态防火墙等多种技术，为客户提供从网络层、应用层到内容层的深度安全防护。

* **智能协议识别和分析**

协议识别是新一代网络安全产品的核心技术。传统安全产品如防火墙，通过协议端口映射表（或类似技术）来判断流经的网络报文属于何种协议。

但是，事实上，协议与端口是完全无关的两个概念，我们仅仅可以认为某个协议运行在一个相对固定的缺省端口。包括木马、后门在内的恶意程序，以及基于Smart Tunnel（智能隧道）的P2P应用（如各种P2P下载工具、IP电话等），IMS（实时消息系统 如MSN、Yahoo Pager），网络在线游戏等应用都可以运行在任意一个指定的端口，从而逃避传统安全产品的检测和控制。

NSFOCUS NIPS采用独有的智能协议识别技术，通过动态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，能够在完全不需要管理员参与的情况下，高速、准确地检测出通过动态端口或者智能隧道实施的恶意入侵，可以准确发现绑定在任意端口的各种木马、后门，对于运用Smart Tunnel技术的软件也能准确捕获和分析。

NSFOCUS NIPS具备极高的检测准确率和极低的误报率，能够全面识别主流应用层协议。

* **基于特征分析的专家系统**

特征分析主要检测各类已知攻击，在全盘了解攻击特征后，制作出相应的攻击特征过滤器，对网络中传输的数据包进行高速匹配，确保能够准确、快速地检测到此类攻击。

NSFOCUS NIPS装载权威的专家知识库，提供高品质的攻击特征介绍和分析，基于高速、智能模式匹配方法，能够精确识别各种已知攻击，包括病毒、特洛伊木马、P2P应用、即时通讯等，并通过不断升级攻击特征，保证第一时间检测到攻击行为。

绿盟科技拥有的业界权威安全漏洞研究团队NSFocus小组，致力于分析来自于全球的各类攻击威胁，并努力找到各种漏洞的修补方案，形成解药，融于NSFOCUS NIPS攻击特征库，以保持产品持续、先进的攻击防护能力。

* **协议异常检测**

基于特征检测（模式匹配）的NIPS（N系列）产品可以精确地检测出已知的攻击。通过不断升级的特征库，NIPS（N系列）可以在第一时间检测到入侵者的攻击行为。但是，事实上，存在三个方面的因素导致协议异常的诞生。

* 厂商从提取某个攻击特征到最终用户的NIPS（N系列）产品升级需要一个时间间隔，在这个时间间隔内，基于特征检测的NIPS（N系列）产品是无法检测到黑客的该攻击行为的；
* 来自0-day或未公开exploit的隐蔽攻击即使是安全厂商往往也无法第一时间获得攻击特征，通常NIPS（N系列）无法检测这类具有最高风险的攻击行为；
* Internet上蠕虫在 15分钟内席卷全球，即使是最优秀的厂商也不能够在这么短的时间内完成对其的发现和检测。

协议异常检测是NSFOCUS NIPS应用的另外一项关键技术，以深度协议分析为核心的NSFOCUS NIPS，将发现的任何违背RFC规定的行为视为协议异常。协议异常最为重要的作用是检测检查特定应用执行缺陷（如：应用缓冲区溢出异常），或者违反特定协议规定的异常（如：RFC异常），从而发现未知的溢出攻击、零日攻击以及拒绝服务攻击。作为一项成熟的技术，协议异常检测技术使得NSFOCUS NIPS具有接近100%的检测准确率和几乎0的误报率。

* **流量异常检测**

流量异常检测主要通过学习和调整特定网络环境下的“正常流量”值，来发现非预期的异常流量。一旦正常流量被设定为基准（baseline），NSFOCUS NIPS会将网络中传输的数据包与这个基准作比较，如果实际网络流量统计结果与基准达到一定的偏离，则产生警报。在内置流量建模机制的同时，NSFOCUS NIPS还提供可调整的门限阀值，供网管员针对具体环境做进一步调整，避免因为单纯的流量过大而产生误报。

流量异常检测和过滤机制使得NSFOCUS NIPS可以有效抵御分布式拒绝服务攻击(DDOS)、未知的蠕虫、流氓流量和其他零日攻击。

* + 1. 2~7层深度入侵防护能力
* **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 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。

* **高品质攻击特征库**

覆盖广泛的攻击特征库携带超过3000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。

* **广泛精细的攻击检测和防御能力**

NSFOCUS NIPS主动防御已知和未知攻击，实时阻断各种黑客攻击，如缓冲区溢出、SQL注入、暴力猜测、拒绝服务、扫描探测、非授权访问、蠕虫病毒、僵尸网络等，广泛精细的应用防护帮助客户避免安全损失。

NSFOCUS NIPS同时具备全面阻止木马后门、广告软件、间谍软件等恶意程序下载和扩散的功能，有助于企业降低IT成本、防止潜在的隐私侵犯和保护机密信息。

* **IP碎片重组与TCP流汇聚**

NSFOCUS NIPS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。

* **虚拟补丁**

NSFOCUS NIPS提供“虚拟补丁”功能，在紧急漏洞出现而系统仍不具备有效补丁解决方案时，为客户提供实时防御，增强了客户应对突发威胁的能力，在厂商就新漏洞提供补丁和更新之前确保企业信息系统的安全。

* **强大的D.o.S攻击防护能力**

NSFOCUS NIPS能够全面抵御ICMP Flood、UDP Flood、ACK Flood等常见的D.o.S攻击，阻挡或限制未经授权的应用程序触发的带宽消耗，极大限度地减轻D.o.S攻击对网络带来的危害。

* **应用客户端的漏洞防护能力**

内置最新的基于应用客户端的漏洞防护规则，绿盟攻防研究团队对客户端易受漏洞攻击的应用进行了长期的跟踪和研究，积累了大量的经验成果，并转化为产品规则，有力提升了产品的内网入侵防护能力。

* + 1. 先进的Web威胁抵御能力

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 NIPS内置先进、可靠的Web信誉机制，采用独特的Web信誉评价技术和URL过滤技术，在用户访问被植入木马的页面时，给予及时报警和阻断，能够有效抵御Web安全威胁渗入企业内网，防止潜在的隐私侵犯，保护企业机密信息。

* + 1. 基于应用的流量管理

NSFOCUS NIPS提供强大、灵活的流量管理功能，采用全局维度（协议/端口）、局部维度（源/目的IP地址、用户、网段）、时间维度（时间）、流量纬度（带宽）等流量控制四元组，实现基于内容、面向对象的流量保护策略。

NSFOCUS NIPS智能识别并分类各类应用后，通过流量许可和优先级控制，阻断一切非授权用户流量，管理合法网络资源的利用，使得网络中不同类型的流量具有更合理的比例和分布，并结合最小带宽保证，及最大带宽和会话限制，有效保证关键应用全天候畅通无阻。

* + 1. 部署极其简便
* **零配置上线**

零配置上线，即设备出厂状态下不用做任何配置，联通一对网口即可上线工作并能取得理想的防护效果。

* **简便的策略管理**

客户的网络拓扑环境和资产防护类型千差万别，如何能根据自己网络应用情况简单配置各种入侵防护策略，并能取得最好的防护效果是客户面临的一个比较大的问题。

NSFOCUS NIPS内置了多种高效的规则模板，便于用户依照不同的网络环境有选择的使用，以达到策略管理的最简化和防护效果的最大化。例如，系统缺省规则模板根据防护的资产类型有WEB服务器模板、Windows服务器模板、UNIX服务器模板，通用服务器模板。用户可通过自身网络的资产防护对象来选择使用，并且还可以通过系统提供的多种自定义方式建立个性的防护模板，最终达到更好的防护效果。

这些高效的系统策略模板的建立方式和技术原理：

* 高级规则动作判定算法保证了规则防护和分类的有效性。

规则配置文件中会以标签形式新增四个标签分别是规则类型、可靠度、攻防相关事件类型、策略模板类型，其中会根据可靠度和事件类型标签生成策略模板中各个规则动作（即阻断和告警），规则配置文件采用了多重判断和算法叠加的方式进行自动生成。

* 规则自动加权算法保证规则的可靠性。

独创的绿盟规则加权分类算法，通过加权机制，依照不同的分类属性，特征匹配度综合判断规则的可靠性并附值，以不同的权值再次进行规则分类和分组保证了规则的可靠性。

* + 1. 强大的管理能力
* **灵活的Web管理方式**

NSFOCUS NIPS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 NIPS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引擎，一个安全中心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安全中心和多个辅助安全中心的管理。主安全中心可以完全控制网络引擎；辅助安全中心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：**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；下级安全中心可以通过配置过滤器，使上级安全中心只接收它关心的信息。适合跨广域网的大型企业用户。

* **带外管理（OOB）功能**

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

* **升级管理**

NSFOCUS NIPS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NIPS（N系列）提供最前沿的安全保障。

* + 1. 完善的报表系统
* **高品质的报表事件**

NSFOCUS NIPS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 NIPS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 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。

* + 1. 完备的高可用性
* **丰富的HA部署能力**

NSFOCUS NIPS具备基于会话、配置等信息同步的HA部署能力，支持A/A和A/S两种部署方式，在出现设备宕机、端口失效等故障时，能够完成主机和备机的即时切换，确保关键应用的持续正常运转。

* **完整的BYPASS解决方案**

IPS作为一种在线串联部署设备，首先要确保客户业务数据畅通,而完备的BYPASS解决方案保证了设备出现故障时基础网络依然畅通，确保了客户基础业务数据不受影响。

NSFOCUS NIPS的BYPASS特性由以下三部分组成，由此形成一套完整的BYPASS解决方案：

* 提供硬件BYPASS功能，IPS在出现硬件故障或意外事故时（意外掉电、意外重启、硬件宕机等），数据会自动切到BYPASS转发，保证了业务的连续性。
* 提供软件BYPASS功能，系统软件故障时，自动实现旁路保护，避免网络中断等事故的发生。软件BYPASS工作流程描述：

系统内置安全和数通引擎，通过心跳交互，当数通引擎检测到安全引擎更新心跳超时后，不会再将包交给安全引擎进行处理，而是将等待安全引擎处理队列中的包和新收到的包直接进行转发，以保障网络畅通。



* 支持外置BYPASS硬件设备部署，如光BYPASS交换机等，扩展形成完整的BYPASS解决方案。
* **过载保护能力**

当IPS部署环境流量超过设备安全引擎所能承受最大处理能力时，为保障客户网络畅通所采用的一种保护措施。它的作用是尽量降低网络延时，减少因安全引擎性能问题造成的网络丢包。



* **冗余电源支持**

NSFOCUS NIPS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。

* + 1. 丰富的响应方式

NSFOCUS NIPS提供丰富的响应方式，包括：丢弃数据包、阻断会话、IP隔离、邮件报警、短信报警、安全中心显示、日志数据库记录、运行用户自定义命令等，同时提供标准snmp trap（V1、V2、V3）和syslog接口，可接受第三方管理平台的安全事件集中监控、报告和管理。支持CEF通用事件格式，能够与ArcSight无缝融合。

* + 1. 高可靠的自身安全性
* **安全可靠的系统平台**

NSFOCUS NIPS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。

* **用户权限分级管理**

NSFOCUS NIPS安全中心身份验证系统采用独立于操作系统的权限管理系统，管理权限与审计权限独立，提供对系统使用情况的全面监管和审计。

* **实时日志归并**

NSFOCUS NIPS归并引擎由规则驱动，可以执行任意粒度的日志归并动作，完全避免Stick此类Anti-NIPS（N系列）攻击。

* **多点备份**

NSFOCUS NIPS的探测引擎可以将攻击告警日志，实时发送到多个绿盟安全中心或日志数据库保存，避免因为数据损坏或丢失而导致系统不可用的事故发生。

* 1. 解决方案

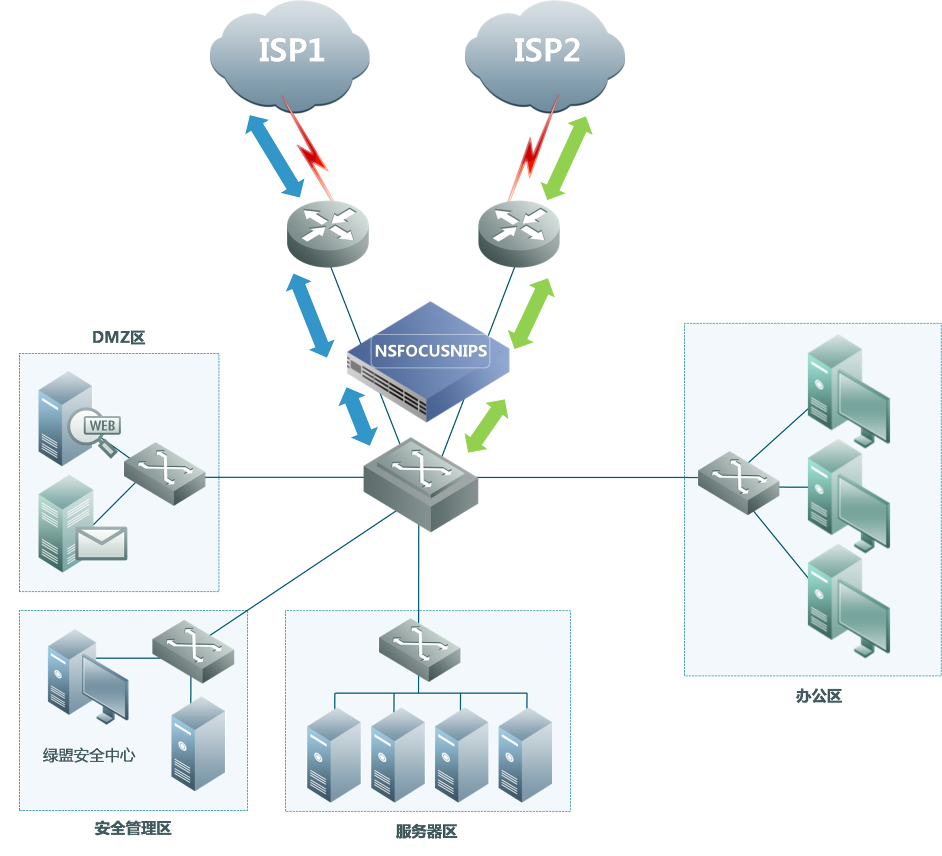
绿盟科技提供一系列完整的入侵防护解决方案，实现从企业网络核心至边缘，以及分支机构的全面保护，适用于不同环境的多种安全防护需求。

* + 1. 多链路防护解决方案

目前，很多企业为了保证网络带宽资源的充足和网络冗余，网络出口采用多链路连接方式，连接到两个或更多ISP服务商。

针对这种连接方式，绿盟科技入侵防护系统提供多链路防护的解决方案，在网络出口处部署一台绿盟网络入侵防护系统，采用多路NIPS（N系列）的部署方式：

1. NSFOCUS NIPS支持多路NIPS（N系列）部署，每路NIPS（N系列）单独防护一个ISP接入链路，一台NSFOCUS NIPS可以同时防护多条链路，节约客户投资；
2. NSFOCUS NIPS的各路NIPS（N系列）是相互独立的，彼此之间没有数据交换，互不干扰，保证了各链路流量的自身安全；
3. NSFOCUS NIPS实时监测各种流量，提供从网络层、应用层到内容层的深度安全防护。



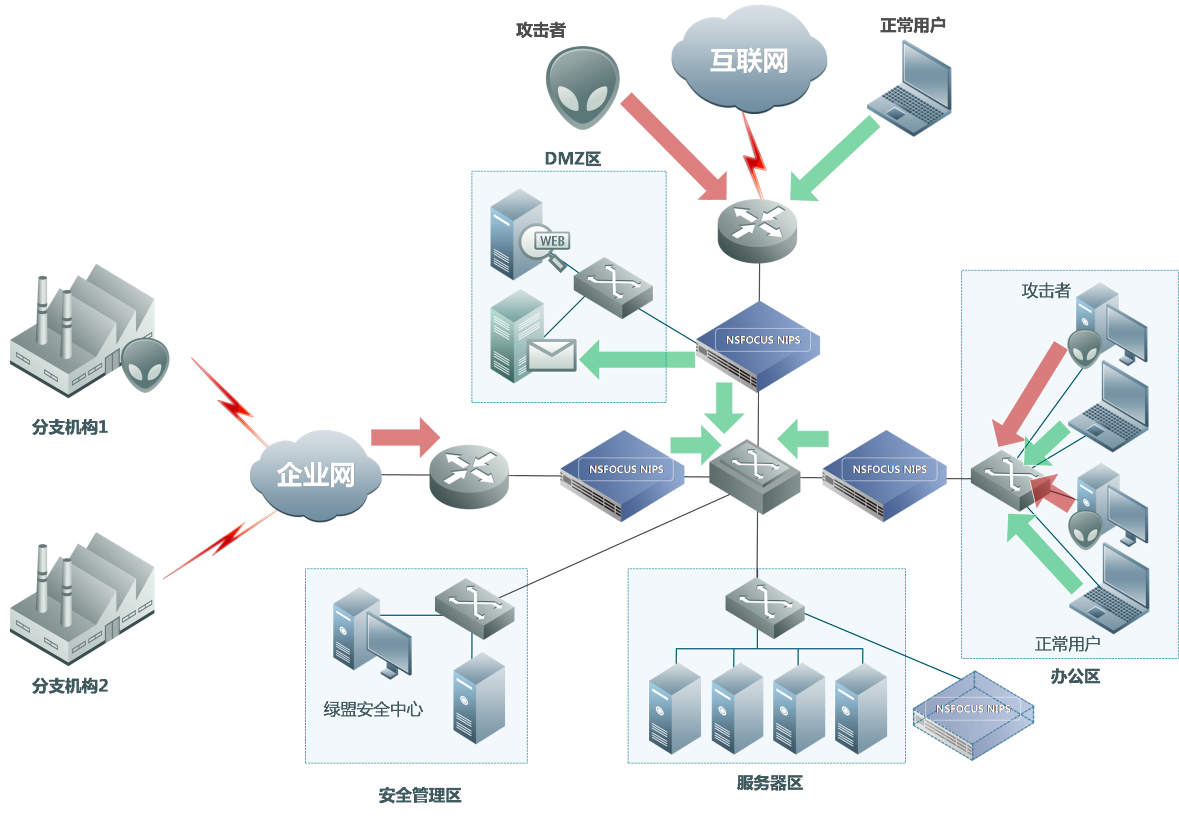
NSFOCUS NIPS多链路防护解决方案

* + 1. 混合防护解决方案

大型企业的网络规模很大，结构相对复杂，不仅有总部，还有各地的分支机构，既要保护网络边界的安全，同时又要保护企业内网的安全。

针对大型企业网络特点，绿盟科技网络入侵防护系统提供混合防护的解决方案：

1. 在总部互联网出入口处在线部署NSFOCUS NIPS，实现路由防护，提供互联网的从网络层、应用层到内容层的深度安全防护；
2. 在总部内部网段之间以及与分支机构网络之间在线部署NSFOCUS NIPS，提供透明接入的、独立多路NIPS（N系列）一进一出的、交换式NIPS（N系列）多进多出的全方位、立体式的安全防护体系，实现内网的安全区域划分和控制；
3. 在企业服务器区旁路部署NSFOCUS NIPS，相当于入侵检测系统，监测、分析服务器区的安全状况，保护服务器安全；
4. 通过一个绿盟安全中心，实现对全网NIPS（N系列）设备的集中管理、安全信息的集中分析和处理，有效解决企业面临的安全问题，提高投资回报率。



NSFOCUS NIPS混合防护解决方案

1. 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。

绿盟网络入侵防护系统提供了业界领先的实时、主动的防护能力，通过新一代的入侵防护技术，绿盟科技的产品和技术能够有效的阻断包括应用层面的各层面攻击，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。