安数云 DataCloudSec

安数云网络入侵防御系统

技术白皮书

北京安数云信息技术有限公司

二〇一七年三月

版权声明

免责条款

本文档依据现有版本制作，其内容如有更改，恕不另行通知。

北京安数云信息技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，北京安数云信息技术有限公司不对本文档中的遗漏或错误导致的损失承担责任。

目　　录

1 背景

随着计算机网络与信息化技术的快速发展，互联网得到了广泛的普及也应用，在日趋信息化的今天，互联网已经成为人们日常工作和生活不可或缺的一部分。作为信息和服务提供商的政府和企业为了满足人们日益增长的网络需求，都在构建和完善自己的互联网业务信息化系统。随之而来的网络信息安全问题，也逐渐得到政府和企业的高度重视。

随着互联网的不断发展，企业面临的安全威胁也在飞速增长。相比过去，网络攻击的方式、形式和攻击者都在发生着深刻变化。网络攻击从早期的随机性攻击，逐渐发展成以政治或经济利益为目的的攻击；攻击的方式也从单一的攻击，逐渐发展成通过蠕虫病毒、木马后门间谍软件、缓冲区溢出、垃圾邮件、SQL/XSS 注入、DOS/DDoS、僵尸网络等进行混合攻击；攻击者也从简单的个体攻击，逐渐发展成有组织的群体性攻击。随着网络攻击的发展，对政府和企业网络安全也提出了更高的要求。

另外，当前网络充斥着各种各样的网络应用，如网络游戏、网络多媒体、各种即时通信软件、P2P 资源上传下载软件等，这些应用软件过度消耗政府和企业的网络资源，对正常的业务服务造成严重破坏。

能否及时主动发现并防御这些网络入侵行为，保证政府和企业的网络安全及业务信息系统的正常运行，是政府和企业面临的一个非常重要的问题。

2 系统的必要性

网络入侵防御系统(IPS: Intrusion Prevention System)是串联在计算机网络中，能够监视网络通信过程中一些不正常网络行为或主动防御具有攻击性的网络行为的安全设备。网络入侵防御系统主要是对应用层数据进行深度解析，发现并阻断各种内部和外部网络的攻击行为。一般部署在防火墙和内部网络设备之间，是对防病毒软件和防火墙的有力补充。

网络入侵防御系统主要是对应用层数据进行深度检测和防御，对内部网络的

上网行为进行必要的管控，其必须具备如下功能：

1. 漏洞攻击防御
2. 蠕虫病毒攻击防御
3. 木马后门攻击防御
4. 缓冲区溢出攻击防御
5. SQL/XSS 攻击防御
6. DOS/DDoS 攻击防御
7. 上网行为识别和控制

- **防火墙的局限**

防火墙（Firewall）是一种位于内部网络与外部网络之间的网络安全系统，能够依照设定的规则，允许或限制传输的数据通过。在实际的应用中防火墙一般会部署在企业网络的入口位置，承担着企业网络安全的第一道防线。但是随着网络攻击方法和形式的不断发展，防火墙的局限性逐渐的突显了出来，主要包括以下方面：

1. 只能拦截不符合安全策略的数据报文，进行被动攻击防御。
2. 不能主动检测网络流量。
3. 不能发现并防御漏洞、蠕虫和木马等网络攻击行为。
4. 不能发现并防御内部网络发起的攻击行为。

- **入侵检测系统的不足**

入侵检测系统（Intrusion Detection System，简称“IDS”）是继防火墙之后，快速发展出来的一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。IDS 是一款主动防御设备，在一定程度上弥补了防火墙的一些功能缺陷，但随着攻击技术和手段的不断发展，IDS 也存在着一些不足之处，主要有如下表现：

1. 只能旁路部署，当其发现攻击行为时，只能发出告警，不能及时主动切断攻击进行有效的防御，在等待用户采取行动的过程中，攻击者的目的可能已经达成。
2. 只能用于事后审计，为用户提供安全决策依据。

3 产品概述

北京安数云信息技术有限公司基于当前网络安全的严峻形势，推出了安数云网络入侵防御系统（简称安数云 IPS）。安数云 IPS 采用在线部署方式，能够实时检测和防御包括拒绝服务、缓冲区溢出、木马蠕虫、CMS、WEBSHELL 等 3000 多种网络攻击行为，第一时间将安全威胁阻隔在企业网络之外。安数云 IPS 有力的弥补了防火墙和入侵检测系统的不足，其能自主的进行深度检测和自动防御，而不只是简单的告警等待用户处理。因此，安数云 IPS 能有效保护用户的网络资源，使其免收各种外部攻击，全面保证业务系统的健康运行。

4 产品架构

安数云 IPS 采用多核架构，具有低功耗，高性能的特点，产品的体系架构主要包括以下内容：

(1)入侵防御系统引擎

入侵防御系统引擎主要是检测通过其的数据流量，按照内置的规则或算法发现攻击行为并进行相应的防御，同时记录相应的日志，便于查看或审计。

(2)WEB 管理界面

安数云 IPS 支持用户通过 WEB 的方式对设备进行管理。用户可以通过 WEB 查看或修改各种配置，查看或下载日志和报表等。

(3)升级站点

安数云 IPS 支持通过 WEB 手动导入的方式，升级系统特征规则库，以保证系统对热点事件的及时防护。

5 产品功能

安数云 IPS 高度融合了高安全性、高可靠性、高性能和高易用性等特性，同时具备深度入侵防御、上网行为管理能力，能够为用户提供攻击防御和上网行为

管理的完美体验。

5.1 DOS/DDoS 防御

- 支持 jolt2、ping of death、tear drop 等 DDOS 攻击防御。
- 支持 TCP、UDP、ICMP flood 攻击防御。
- 支持 TCP、UDP、ICMP 扫描防护。

5.2 WEB 安全

- 支持 WEB 内容关键字、URL 和文件传输过滤。

5.3 病毒过滤

- 支持基于数据流的查杀模式，实时阻断含有网络病毒的数据报文和连接。
- 支持 HTTP、FTP、SNMP、POP3、IMAP 等协议。

5.4 流量控制

- 支持以区域单位的总流量出/入限制。
- 支持以服务器为单位的总流量出/入限制。
- 支持限制单位时间内每台客户机连接服务器的 TCP、UDP、ICMP 连接的数目。
- 支持限制单位时间内服务器允许客户机 TCP、UDP、ICMP 连接的数目。
- 支持以具体网络应用（如：P2P 下载、网络多媒体）为单位的流量限制。

5.5 上网行为管理

- 支持即时通信软件、P2P 软件、网络游戏、证券软件、网络多媒体等应用的识别。
- 支持基于各种应用的精细化控制，可以对单个应用进行监视、透传、阻断和限速管理。

5.6 未知检测

- 支持针对未知病毒攻击的检测和识别。
- 支持基于 HTTP、SMTP、POP3、IMAP、FTP 协议的办公、压缩等文件过滤。

6 产品优势

安数云 IPS 采用高性能的多核处理器硬件平台，同时引入并行处理技术，为用户提供 2 到 7 层的网络安全防护。安数云 IPS 不仅具有强大的攻击防御能力，而且可以智能识别网络通信协议、上网行为并进行上网行为管理，下面将对安数云 IPS 产品的功能特色进行详细介绍。

6.1 强大的入侵检测能力

安数云 IPS 在协议解析的基础上，融合特征识别、流量异常检测、会话跟踪等多种技术手段，能够精确的发现各种网络入侵行为，并进行相应的防御，为客户提供深入全面的安全解决方案。

(1)安数云 IPS 拥有强大的 DOS/DDoS 攻击防御能力,其内置了各种 DOS/DDoS 的检测算法，能够防御 Jolt2、Land-Base、Tear Drop 等多种攻击行为，以及 SYN、UDP、ICMP 扫描行为。

(2)安数云 IPS 拥有完善的特征库，具有强大的特征检测系统。该系统采用快速高效的匹配算法，能够精确的检测出各种漏洞、缓冲区溢出、蠕虫木马、暴力破解、安全扫描等已知攻击行为。

(3)安数云拥有强大的安全事件研究团队,致力于研究国内外热点安全事件，并积极寻找修复方案，形成特征规则后，直接用于到安数云 IPS，及时提升产品的防御能力。

(4)安数云 IPS 拥有强大的特征规则库，目前已覆盖各种病毒、漏洞、蠕虫木马等规则，并在安全研究团队的努力下，一直在不断完善。

6.2 强大的上网行为识别能力

安数云 IPS 能够识别各种即时通信、P2P 软件、金融交易、网络游戏和网络多媒体等在内的多种用户上网行为，并能更好的协助用户了解当前网络的应用状况，发现网络中的各种异常流量，继而采取阻断、限速等控制手段，保证网络的畅通。

6.3 完善的 WEB 安全防护能力

安数云 IPS 不仅可以对 WEB 访问进行安全检测和防御，还可以阻断携带某些特征关键字、URL 的 WEB 请求，还可以结合敏感信息过滤功能对 WEB 内容和上传文件进行更精细的检查和防御。

安数云 IPS 支持用户手动添加关键字列表、URL 列表等，以满足客户对产品动态需求。

6.4 邮件协议过滤能力

随着计算机网络的发展，电子邮件在为人们提供便利的同时，随之而来的垃圾邮件也给人们带来了不少的麻烦。据统计，全球高达 80%的邮件都是垃圾邮件，由此可见垃圾邮件攻击已经严重影响到了人们的日常生活和工作。

安数云 IPS 可以根据邮件相关的各个字段进行过滤，包括主题、发件人、附件名、邮件大小、IP 地址或 SMTP 命令等，还可以结合敏感信息过滤功能对主题、正文、附件名、附件内容等进行更细化的检测和过滤，从而可以最大程度的改善和保护客户的电子邮件环境。

6.5 高效的病毒检测能力

安数云 IPS 具备高效的防病毒能力，采用基于特征扫描和启发式扫描技术的检测技术，能够检测针对 HTTP、FTP、SMTP、POP3、IMAP 等多种协议的蠕虫病毒、木马病毒、后门等多种病毒，并进行实时查杀。

6.6 多维度的流量控制

安数云 IPS 提供强大、灵活的流量管理功能，从多个纬度对客户的网络环境进行流量保护。安数云 IPS 支持以安全服务、主机、协议和网络应用为单位的多维度流量控制。从不同层面，灵活的保护客户的网络环境。

6.7 强大的防火墙能力

(1)支持访问控制

安数云 IPS 支持根据协议、网络接口、源/目的 IP、时间等元素，自定义访问控制规则。通过这些规则，可以帮助客户灵活的管控自身网络的流量出入规则。

(2)支持 NAT

安数云 IPS 支持源/目的、静态/动态地址转换功能，同时也支持多种网络转换方式，如一对一、一对多和多对一等方式。

(3)支持路由

安数云 IPS 支持静态路由和策略路由两种路由方式。其中策略路由能够根据网络接口、IP、端口等选择报文转发策略，尽可能满足客户的各种应用场景。

6.8 高可靠的业务保障能力

安数云 IPS 设备拥有支持热插拔的冗余双电源，避免当电源出现故障时，出现设备停止工作，造成攻击无法防御、甚至断网等严重后果。因此，冗余电源的存在，在一定程度上提高了 IPS 设备自身的可靠性。

安数云 IPS 支持软件和硬件两种 BYPASS 方案。其中，硬件 BYPASS 包括外置 BYPASS 设备和设备板卡自身 BYPASS 两种方案。当系统在运行过程中出现软件故障后，系统会自动开启软件 BYPASS 功能，自动构建一条通路，使流量能够正常通过设备，避免网络中断的情况发生；当安数云 IPS 设备断电或出现故障时，设备会自动启动硬件 BYPASS 功能或外置 BYPASS 自动启动，保证流量的正常传输。

安数云 IPS 支持主主和主备模式两种双击热备技术，在设备出现宕机或硬件故障时，能够自动完成主备切换，完全可以实现链路的高可用性。

6.9 可视化报表功能

安数云 IPS 提供了可视化的实时报表功能，可以根据攻击、应用、流量、病毒等多个维度进行细粒度统计和做趋势图展示。通过这些图表，客户可以很轻松的了解当前网络的安全状态。

安数云 IPS 还提供了详细的安全报表功能，系统支持生成各种周期的综合安全报表，报表以 PDF 格式导出。

安数云 IPS 支持按照日志级别记录日志，自动忽略设定级别以下的日志，不仅极大的减少了攻击告警的数量，而且提高了对于高风险攻击事件的反应速度。

6.10 丰富的响应方式

安数云 IPS 提供了通过、丢弃、丢弃会话、阻断等响应方式，并可以通过本地、邮件和 syslog 的方式进行告警。安数云 IPS 还提供了标准的 SNMP TRAP（V1、V2、V3）和 syslog 接口，既可以向第三方平台发送日志报告，也可以接收第三方的管理。

7 产品部署

由于企业结构和业务系统的特殊性，使得网络结构都不尽相同，安数云 IPS 提供了串联、路由和旁路等多种接入方式，无需改变用户的网络结构，即可达到防御外来网络入侵和对办公区域终端上网行为进行管控的目的。

7.1 典型部署

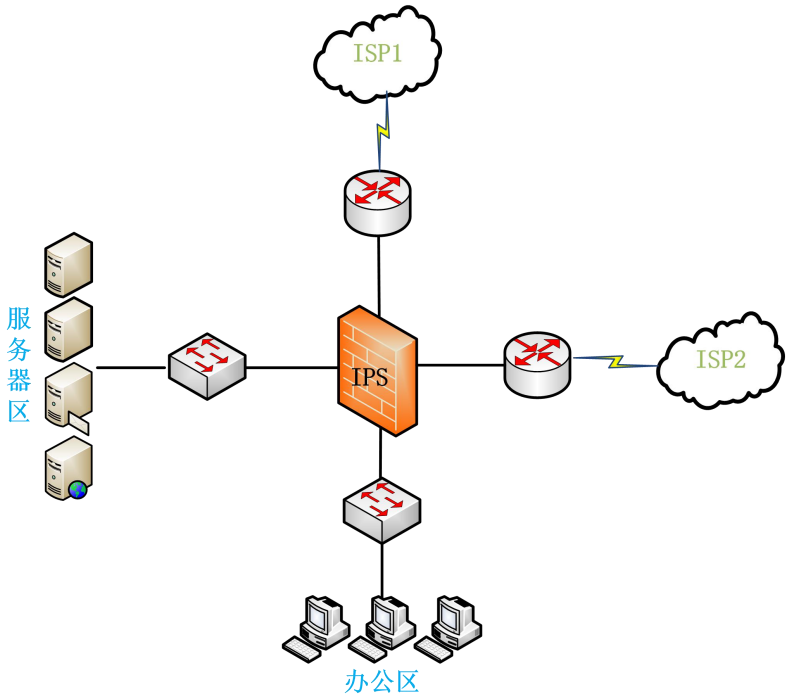
将安数云 IPS 部署在网络接口处，该部署模式既支持单条链路接入，也支持多条链路同时接入。具体链路接入方式需根据用户的实际网络环境进行选择。

安数云 IPS 在接入多条链路时，各链路之间不进行任何数据交换，彼此相互独立，互不影响，从而可以保证各条链路的相对安全。

安数云 IPS 实时检测各种流量，可以对办公区域的各种上网行为进行管控，

保证办公区域的网络畅通；也可以防御外网的各种攻击，保证办公网络和服务器的安全。

当前很多企业为了保证网络带宽的充足和网络冗余，网络出口一般都采用多链路连接的方式，本节以多链路为例，以图片的方式展示 IPS 的部署方式如下。

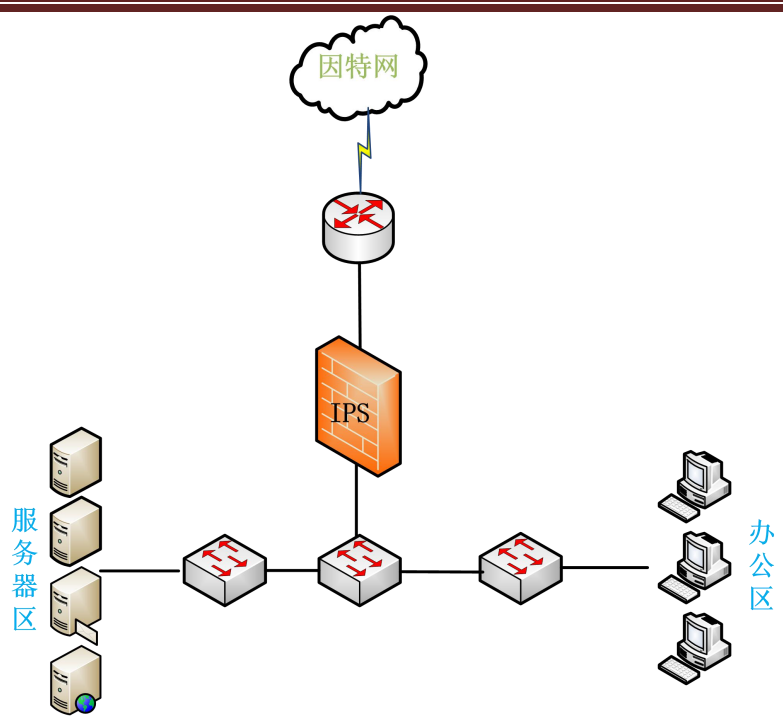


7.2 交换防护部署

企业内部网络可能会根据工作地点或部门的不通，将内部网络划分成多个网段，各个网段都与核心交换机连接，进行数据通信。如何保证企业内部各个网段的网络安全，往往是网络管理员比较关心的问题。

针对上述需求，安数云 IPS 提供了交换防护的部署模式。在该模式下，安数云 IPS 类似于一台交换机，一个接口与外网进行数据交互，使用其他接口与内网的不同网段进行连接。安数云 IPS 会根据报文所属的网段，将报文从该网段对应的接口上发出，保证报文能够正确传输。

安数云 IPS 实时检测各网段的各种流量，可以对各种上网行为进行管控，保证各个网段的网络畅通；也可以防御外网的各种攻击，保证内部网络的安全。部署方式如下图所示。



7.3 路由部署

很多企业在网络边界的敏感区域串联了很多安全设备，造成网络边界的故障率升高，为了降低整个网络的安全威胁，很多企业不希望将 IPS 设备串联到自身的网络环境中，但是又希望 IPS 能对网络进行安全防御。

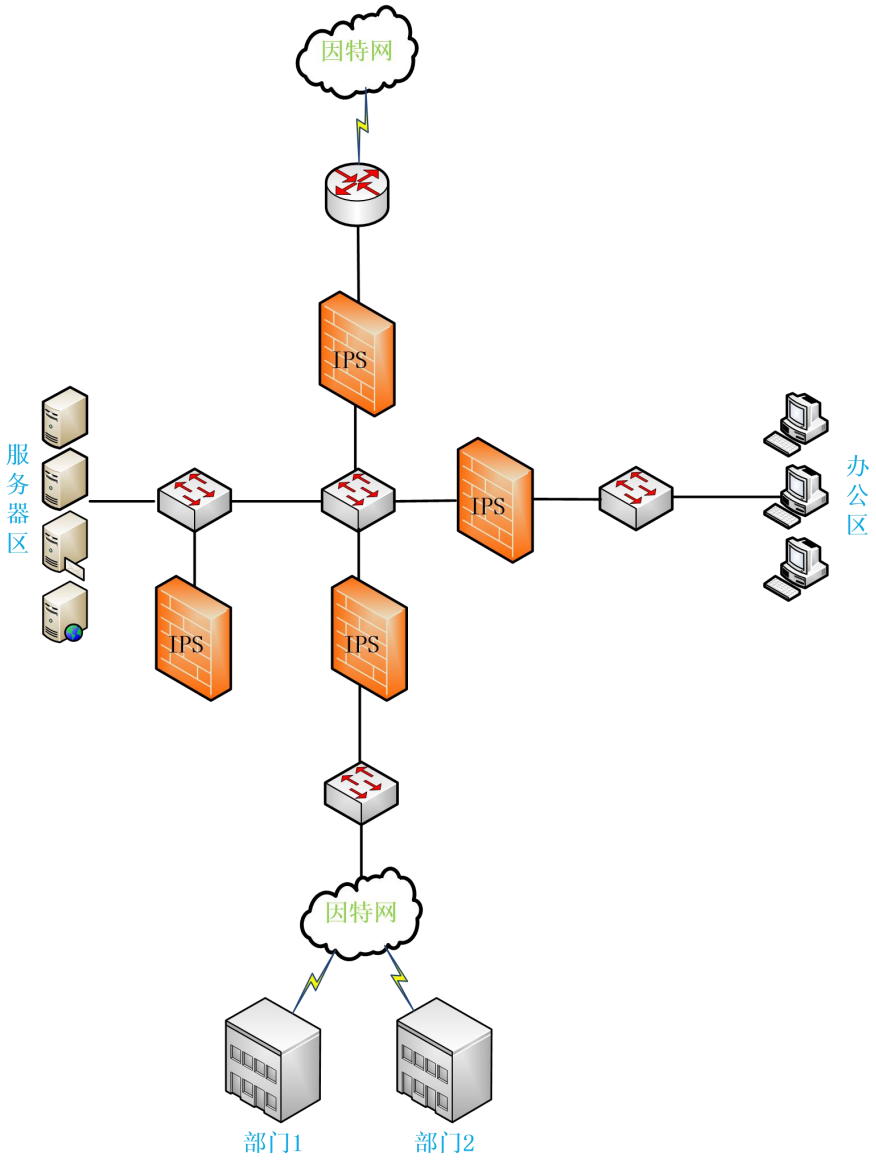
针对这一需求，安数云 IPS 提供了路由部署模式，通过配置静态路由和策略路由的方式，既可以将流量导入到 IPS 进行安全防护，又不会影响内外网的正常通信。部署方式与串联部署相同，唯一不同的是 IPS 会作为路由器与对端路由器进行通信。

7.4 混合部署

大型企业的网络规模一般都比较大，而且网络结构也比较复杂，此时企业既需要保护敏感区域的安全，又需要保护内部网络的安全。

针对这一需求，安数云 IPS 提供了混合部署方案，在企业网的边界采用路由部署模式部署安数云 IPS 设备，对边界流量进行网络入侵检测和防御。在企业网内部网段之间或与分支机构网络联通位置，采用串联模式部署安数云 IPS 设备，

实现安全区域划分和控制。在企业内部服务器区采用旁路部署的方式部署安数云 IPS 设备，相当于部署一台入侵检测设备，对服务器进行安全检测，并及时告警。部署方式如下图所示。



8 服务支持

详情请访问：http://www.datacloudsec.com。

欲购买及试用此产品，请联系销售代表。

北京安数云信息技术有限公司。

服务电话：010-62928890。

技术支持邮箱：service@datacloudsec.com。