中数国科网络入侵检测系统
产品白皮书

（中数国科集团）

■ **版权声明**

目录

一、概述

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。近年来，移动互联网、社交网络和云计算的兴起，更是更大的促进了互联网的发现。

伴随着网络的发展，也产生了各种各样的安全问题，网络中蠕虫、病毒及垃圾邮件肆意泛滥，木马无孔不入，DDoS 攻击越来越常见，黑客攻击行为几乎每时每刻都在发生。如何及时的、准确的发现违反安全策略的事件，并及时处理，是广大企业用户迫切需要解决的问题。

提到网络安全设备，大家都会想到防火墙。防火墙作为企业级安全保障体系的第一道防线，已经得到了非常广泛的应用，但是各式各样的攻击行为还是被不断的发现和报道，这就意味着有防火墙不是万能的。防火墙等访问控制设备没有能做到完全的协议分析，仅能实现较为低层的入侵检测，对应用层攻击等行为无法进行判断。

中数国科网络入侵检测系统（Intrusion Detection System）是对防火墙有益的补充，中数国科网络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。

中数国科网络入侵检测系统主要有以下特点：

事前警告：中数国科网络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，中数国科网络入侵检测系统可以及时发现、TCP Killer 等方式进行报警及动态防御；

事后取证：被入侵攻击后，中数国科网络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，而中数国科网络入侵检测系统提供动态防御，因此防火墙和中数国科网络入侵检测系统的结合，能够给网络带来全面的防御。对防火墙和中

数国科网络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，中数国科网络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

中数国科网络入侵检测系统很好的弥补了防火墙的不足，通过部署中数国科网络入侵检测系统，可以有效的监视交换机上的所有实时传输数据，专注的是全面检测、有效呈现中数国科网络入侵检测系统是作为安全监督管理工具存在，提供给用户全面的信息展现，为改善用户网络的风险控制环境提供决策依据。是整个网络体系中不可或缺的一部分。

中数国科网络入侵检测系统对缓冲区溢出、SQL 注入、暴力猜测、D.o.S 攻击、扫描探测、蠕虫病毒、木马后门等各类黑客攻击和恶意流量进行实时检测及报警，可运用发送邮件、SNMP trap 等方式进行动态防御。

二、产品特点

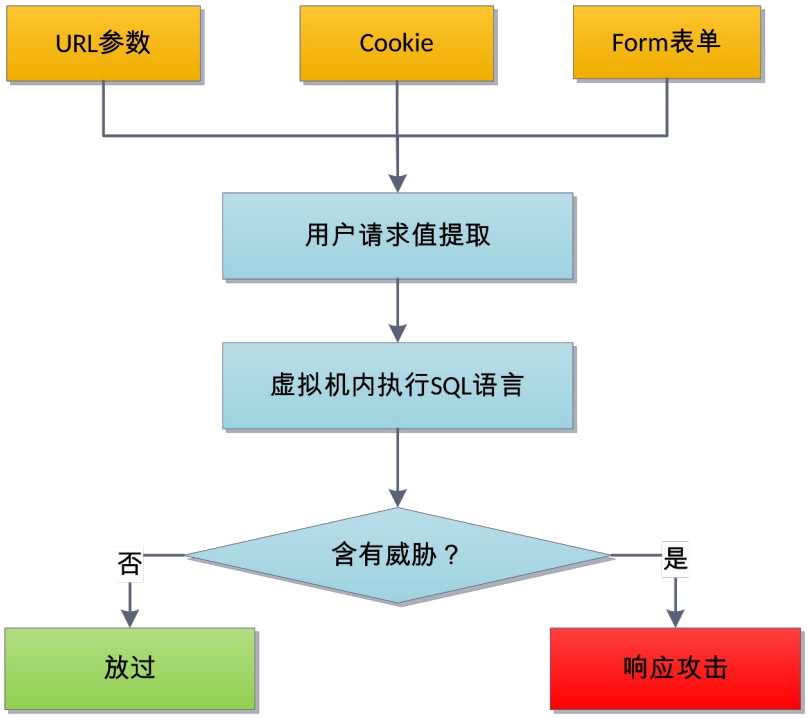
2.1 基于语义的 SQL 注入检测

利用现有应用程序，将(恶意)的 SQL 命令注入到后台数据库引擎执行的能力，这是 SQL 注入的标准释义。随着 B/S 模式被广泛的应用，用这种模式编写应用程序的程序员也越来越多，但由于开发人员的水平和经验参差不齐，相当一部分的开发人员在编写代码的时候，没有对用户的输入数据或者是页面中所携带的信息（如 Cookie）进行必要的合法性判断，导致了攻击者可以提交一段数据库查询代码，根据程序返回的结果，获得一些他想得到的数据。SQL 注入利用的是正常的 HTTP 服务端口，表面上看来和正常的 web 访问没有区别，隐蔽性极强，不易被发现。

传统的基于特征的 SQL 注入检测，首先抽取 SQL 注入过程中都会出现的特殊字符(例如:’ - #等)，抽取 SQL 注入过程经常会出现的 SQL 关键字(例如:’SELECT、UNION

等)作为检测 SQL 注入的依据。利用上述步骤中提取的特征构建 SQL 注入特征库，通过传统的模式匹配的方式进行检测。很显然这种方法有着极高的漏报和误报率，比如在 USER 字段提交 Select，将会被认作攻击行为。并且做了编码转换或函数转换或者是关键字跨域之后，攻击者很容易躲避机械地匹配字符串方式的检测。

中数国科网络入侵检测系统会首先构造一个可以执行各种 SQL 语句的虚拟执行环境，可以通过对输入的内容进语义分析，无论攻击者伪构造多么复杂，特殊的攻击内容。只要用户输入的内容中含有攻击的内容。就可以发现攻击。



2.2 灵活的安全策略管理

中数国科网络入侵检测系统采用基于策略的防护方式，内置了多种默认安全策略集，用户可以根据需要选择最适合自己需要的策略，以达到最佳防护效果。 用户即可以根据防护的类型不同而选择不同的事件集，即可以提高系统的性能，也可以减少误报的发生机率。比如用户需要防护的设备是 Linux 服务器，可以只选择 Linux 系统的策略集。同理，如果用户只要想防护 Web 攻击，可以只使用 Web 防护策略集。

中数国科网络入侵检测系统，可以根据安全类型、协议类型、系统、级别、事件来源

等多个方面来灵活的选择安全策略。同时对于不同的安全策略，可以自定义不同的防护级别，适用于各种不同的场景。

2.3 用户身份识别

中数国科网络入侵检测系统提供了用户身份识别功能，中数国科将下一代防火墙中的用户识别的理念引入到中数国科网络入侵检测系统当中，随着网络的不断发展以及 BYOD 的兴起，基于 IP 的管理越来越不能满足网络管理的要求，基于用户的身份识别将看不到的 IP 和真实的人联系起来。提供多种用户识别手段，方便管理员更好的发现威胁和攻击。

2.4 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。

中数国科网络入侵检测系统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。

2.5 基于流重组技术

现有的中数国科网络入侵检测系统产品中，决大部分产品属于单包过滤产品，他们的特点是拥有高性能的处理，却牺牲了攻击检测阻断的准确性。而在当前流行的网络攻击方式和种类是逐步向网络上层延伸，攻击行为常常掩藏在 7 层应用的数据流中，大量的攻击数据流都是封装在标准的应用协议数据流中，通过通用的端口，进行伪装，欺骗无法流重组和协议分析的 IDS 产品。而基于单个数据包检测的 IDS 产品更是无法有效抵御 TCP 流分段重叠的攻击，很多的攻击行为通过 TCP 流分段组合即可轻松穿透这种引擎，在受保护的

目标服务器上形成真正的攻击。犹如蒸馏水里混合了自来水，颜色都一样，简单的目视色差分析，并不能真正解决问题。在攻击检测的过程中,为了准确有效得检测出隐蔽在多个数据包中的攻击,必须进行 TCP 会话的还原,从而得到完整的攻击特征。

2.6 基于协议状态分析

中数国科 IDS 的协议分析技术，是对已知协议和 RFC 规范的深入理解，可准确、高效的识别各种已知攻击。同时根据系统协议分析的算法，sensor 拥有检测协议异常、协议误用的能力，彻底解决了以往基于模式匹配技术的 IDS 产品片面依赖攻击特征签名数量来检测攻击的弊端，极大的提高了检测的效率，扩大了检测的范围。中数国科 IDS 目前支持 Telnet、FTP、HTTP、SMTP、SNMP、DNS 等多达 30 种的主流应用层协议，遥遥领先于其他 IDS 品牌。

例如中数国科 IDS 检测一个 http 的访问，第一步直接跳到数据帧的第 13 个字节，读取 2 个字节的协议标识。如果值是 0800，则说明这个以太网帧的数据域携带的是 IP 包，然后第二步跳到第 24 个字节处读取 1 字节的第四层协议标识，如果读取到的值是 06，则说明这个 IP 包的数据域携带的是 TCP 包，第三步跳到第 35 个字节处读取一对端口号。如果有一个端口号是 0080，则说明这个 TCP 帧的数据域携带的是 HTTP 包，第四步让解析器从第 55 个字节开始读取 URL。URL 串将被提交给中数国科 IDS 的 HTTP 解析器后，由 HTTP 解析器来分析它是否可能会做攻击行为。

中数国科 IDS 采用这种先进的检测技术，使它具有了明显的优势：

利用协议分析已知的通信协议，在处理数据帧和连接时更加迅速和有效准确，减少了误报的可能性。

能够关联数据包前后的内容，对孤立的数据包不进行检测，这和普通 IDS 检测所有数据包有着本质的区别。一方面因为这种检测机制的高效性降低了系统在网络探测中的资源开销，大幅度提高了检测性能，另一方面因为在命令字符串到达操作系统之前，模拟了它的执行，以确定它是否具有恶意，有效减少了误报。

它具有判别通信行为真实意图的能力，它不会受到像 URL 编码、干扰信息、IP 分片等中数国科网络入侵检测系统规避技术的影响。

当检测到的所有数据信息经过应用协议分析后，中数国科 IDS 将真实的应用数据与签名库进行攻击特征的匹配，因为我们知道特征匹配仍然是检测效率最高的和最准确的检测技术。只是这种匹配，与普通基于模式匹配的检测机制有着本质上的区别，它是在协议分析和还原以后真实有效的数据，这种真实可靠的有效数据的匹配，一方面提高了检测效率，另一方面，增强了检测攻击的准确度，减少了误报的概率。

2.7 工控协议深度解析

随着中国制造 2025 计划、互联网+和工业 4.0 的不断推进，工业互联网时代已经到来 IT 和 OT 已经深度融合，越来越多的工控设备接入到互联网，导致传统安全威胁可以迅速渗透到工业网络中，危害工控系统的正常运行。办公信息网与控制网络之间的威胁控制、工业互联网出口的安全防护已经成为当前工业网络安全整体方案中不可忽略的关键点。通过具备多种威胁防御的一体化安全网关产品，在第一时间发现来自外部的安全风险，感知核心设施的风险态势，构建纵深防御的工业网络安全体系成为重要的发展趋势。

中数国科入侵防御系统基于自主可控的操作系统和高性能硬件平台，采用访问控制、入侵防御、病毒过滤等融合的安全技术，重点监控工业网络中互联网边界、MES 层边界的网络流量，发现并阻断已知和未知的网络攻击行为，保护工业网络内部核心设施，从而构建可管、可信和可视的工业网络系统，为工业用户提供安全智能的边界安全防护方案。

入侵防御系统是集入侵检测、入侵防御产品于一体，依照安全策略对工业网络系统的运行状况进行监视，发现并阻断各种入侵攻击、异常流量、非法操作或异常行为的软硬件一体化设备。产品通过深入分析网络上捕获的数据包，结合特征库进行相应的行为匹配，实现入侵行为检测和防御、病毒恶意代码查杀、web 攻击防护、安全风险评估、安全威胁可视化等功能。部署中数国科网络入侵检测系统可以及时发现来自生产网外部或内部违反安全策略的行为及被攻击的迹象，通过告警提醒工业用户及时采取应对措施，最终达到保

障生产网络安全运行的目的。

2.8 智能关联分析

由于 IDS 可以监听网络内部的通讯，无论是内部主机直接的威胁还是从外到内的威胁，都可以及时报警，从而提醒网络管理员来处理存在的威胁。在大规模蠕虫爆发时，正是 IDS 的预警，使得管理员能及时采取行动，从而极大地避免了网络崩溃导致的危害。

IDS 作为对网络攻击检测的产品，检测的全面性毫无疑问是其重要指标。而特征库是 IDS 的检测核心部分，因而很多时候检测的全面性被简化为特征库的数量，出现在招标要求或者产品的指标中。而另一个方面，同一个网络数据包，在有的网络环境下是威胁，而在有的网络环境下则是完全正常的行为，这样就只有将这样的行为都定义在默认的特征库中，因此通常情况下特征库中会出现“Ping”、“HTTP 连接”甚至“TCP 连接”这样的事件。

当前各种入侵检测产品产生的报警，往往都需要经过人工分析，才能筛选掉出重点关注事件。分析步骤一般如下：

对事件本身的性质进行判断。大多数 IDS 产品都能对 ping、tcp 连接等事件进行报警，一般情况下安全级别较低的报警不需要关注，如果有大量报警产生的话，确认一下是否是正常业务产生即可。

通过结合网络环境来判断。首先需要确定攻击对象和攻击者的性质、在网络中的位置比如 SNMP 查询这样的事件，需要确认源地址是否正常的网管软件，如果就是合法的网管软件在工作，这样的事件就不需要继续关注了，如果不是则需要确认是错误地配置了网管软件还是被控制来扫描了。而对于攻击对象需要确认漏洞是否真实存在。

这个攻击是否流行。如果攻击针对的漏洞是几年前出现的，这样攻击的威胁成都就比较低。

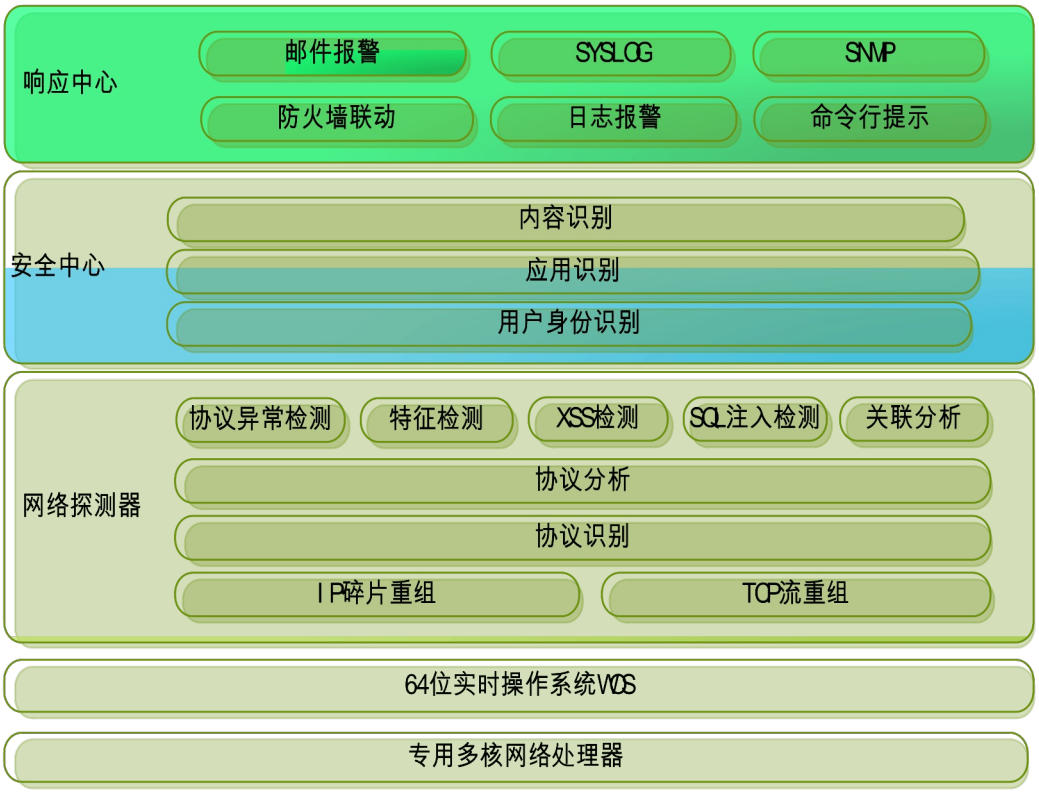
是否是特定关注，比如有些网络中不允许出现网络共享，因此如果出现针对网络共享的攻击必定需要仔细核实。

从以上步骤可以看出人工分析事件的时候，需要结合多个维度的信息进行分析。中数

国科结合其多年产品研发经验和对大量客户使用过程的研究，将实现对报警的智能分析系统，抑制海量事件，突出展现重点关注事件，必将推动行业向智能化方法发展。

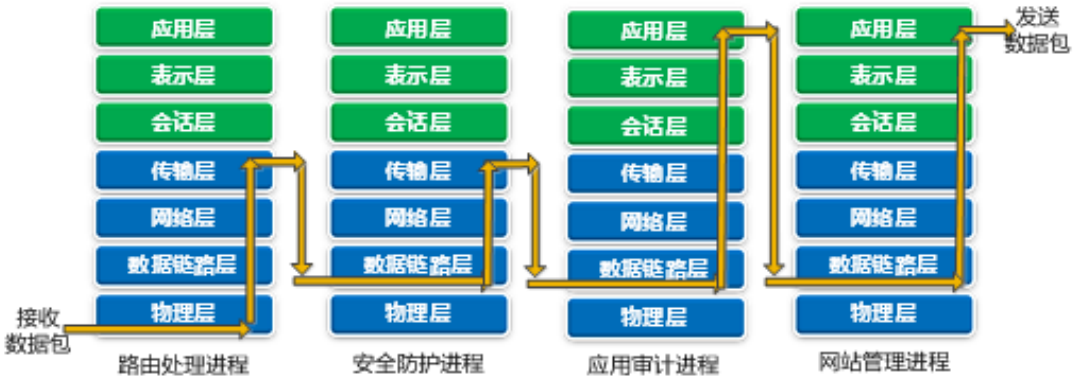
2.9 高性能多业务并行架构

产品采用最新最先进的多核硬件架构，在硬件架构上运行自主知识产权的安全 OS，高效的并行调度算法和内存管理机制提高了流量转发报文的性能。另外，将 CPU 处理的数据根据其特性分为 Data Plane（数据面）和 Control Plane（控制面）两类，简称 DP 和 CP。在多核系统一部分 CPU 专职 CP 工作，大部分 CPU 专职 DP 工作。这样就避免了因系统调度，导致设备转发性能降级或者无法响应管理操作等现象。具体 DP 和 CP 的 CPU 分布根据用户场景定义。在应用层安全方面通过数据”零拷贝“、多核并行控制、多线程应用代理等多项关键核心技术，使产品的性能得到大幅度的提升。

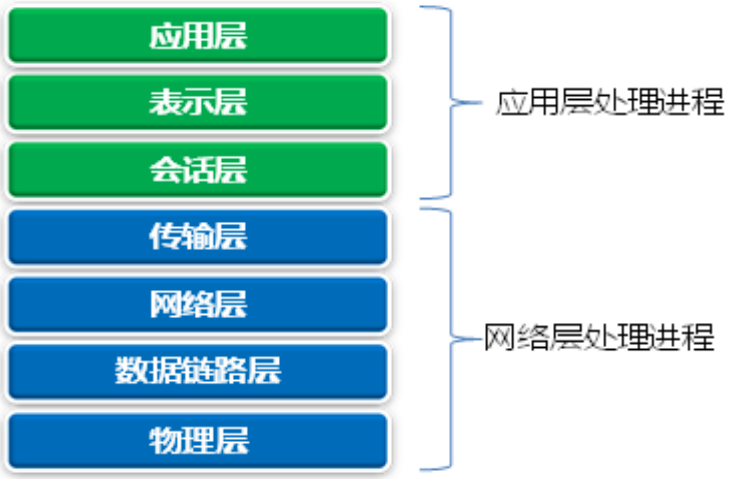


三、技术实现

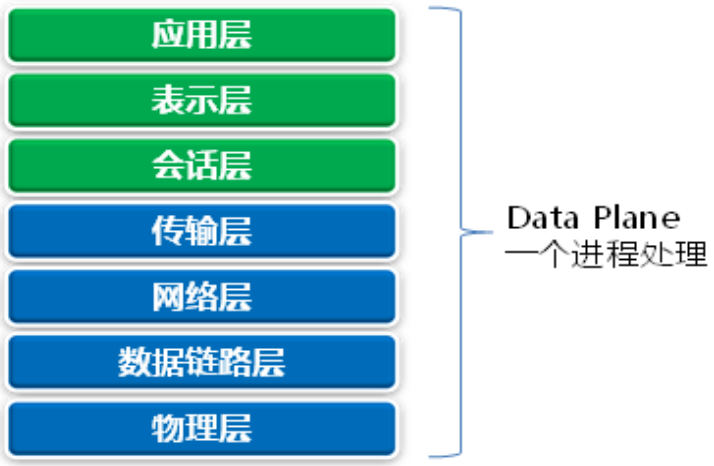
数据面传统的网关设备为了降低设计和开发难度，会将各个模块以进程的方式存在，数据包每通过一个模块都要重复对数据的解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



有的设备则将网络层处理与应用处理分别在两个进程上实现，这样就出现了数据包多次拷贝的情况，增加了内存访问次数，降低了系统性能。

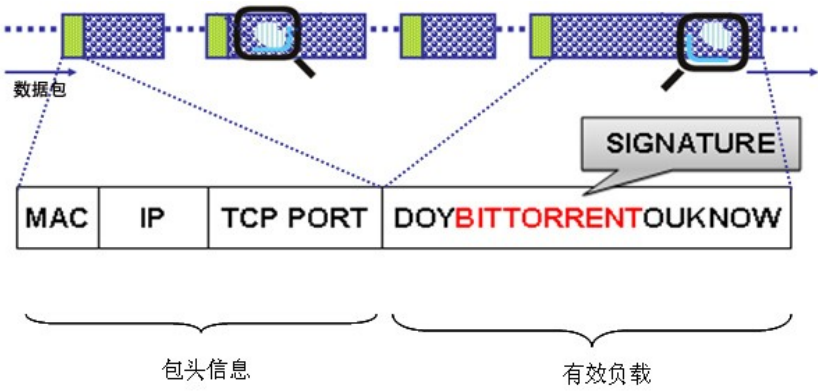


IDS3000 系列主要处理转发相关的工作，通过对数据包一次解析，按层次由对应模块处理，可以节省不同模块间重启解析数据包所消耗的资源，从而降低网络延迟。



IDS 其工作原理是检测数据包有效载荷，提取特征（如下图），然后与设备加载的攻击特征码进行比对，设备加载的特征码都是从已知通用应用协议或应用系统漏洞中提取出来的，专门针对这类通用漏洞的攻击防护，大部分能通过打补丁的方式解决。

然而，经业界众多专业厂商研究分析，目前攻击者大多采用的是针对网站代码内容的攻击手段，而不是采用传统特征库中已有的通用攻击手段。IDS 具备了针对已知通用应用协议或应用系统漏洞的防护，但对于目前普遍定制开发的 Web 站点系统，由于网站应用代码中的漏洞而带来的应用攻击，不能提供有效的防御，尤其是对一些逻辑关系复杂的应用攻击。



如果代码编写者对用户提交的数据未做适当的检查及验证，恶意攻击者可以利用 Web 页面中提交数据的表单构造访问后台数据库的 SQL 指令，从而能够非授权操作后台数据库，达到获取敏感信息、破坏数据库内容和结构、甚至利用数据库本身的扩展功能控制 Web 服

务器操作系统，如此不仅能够达到网页挂马，还可以构成对 Web 服务器的其他攻击，篡改网页内容更是轻而易举。

四、产品功能

4.1 多种部署模式

产品支持透明、旁路、桥模式、混合、双机冗余模式五种不同的部署方式，可以根据网站的实际情况进行灵活的组合和搭配。既适合单一网站的保护，也可以作为旁观者，进行网站风险检测和评估，还可以将分布于不同地理位置的多个网站进行聚合性的统一安全防护。

4.2 检测 Web 攻击

内置自主研发的深度 Web 内容过滤引擎，可以对 HTTP 请求的包头信息、URL、网页内容、Cookie、表单参数等多种元素进行实时的检测，发现和过滤其中的 Web 攻击行为。可检测和过滤 Web 攻击包括 SQL 注入、跨站脚本、跨站请求伪造、WebShell、命令行注入、弱口令、缓冲区溢、CC 攻击、针对 Cookie 劫持和篡改等多种 Web 攻击，全面覆盖 OWASP 公布的常见 Web 应用安全威胁。

4.3 病毒上传检测

产品内置病毒过滤引擎和实时更新的病毒特征库，可以对通过 HTTP 和 FTP 协议上传的文件进行病毒过滤和阻断，防止网站被恶意利用，成为病毒和木马传播的工具。

4.4 精细化的防护策略配置

为了能够给不同的网站提供专业有针对性地安全防护，产品提供了针对不同网站，甚至是不同 URL、Web 目录分别设置防护策略的功能。同时每一套防护策略都自成体系，可以进行菜单式的防护项目的组合和配置，形成针对每一个防护对象的独特策略模板。通过防护对象精细化和防护策略模板化的处理，用户可以方便、快捷的实现不同网站、不同 URL 的精准安全防护。

4.5 IDS 自定义规则

如果有些攻击是客户网络环境中特有的或者出现新的漏洞还未提供升级库，安全管理员可以使用自定义规则功能，自己写签名进行防护。自定义规则检测是基于流检测的，支持多种协议字段，其中包括 IP、UDP、TCP、FTP、HTTP、ICMP、POP3、SMTP 协议。对于字符串字段，一般都支持正则和非正则匹配的方式。一个规则中可以配置多个检测条件，各个条件之间可以是与、或的关系；

4.6 WEB 防护引擎

针对 WEB 网站进行防护的安全引擎，实现对整个网站全面的防护，采用领先的安全检测技术。

WEB 防护引擎能有效抵御各种注入式攻击，包括 SQL 注入、系统命令注入、LDAP 注入、SSI 注入、邮件注入、请求体 PHP 注入等攻击；对于常见的 XSS 攻击的防护结合基于语义分析和攻击指纹两种方式，相比传统只基于攻击指纹的检测方法，检测准确率更高，误报率更低，防逃避能力更强；为了检测出恶意攻击者对 WEB 站点的扫描行为，WEB 防护引擎支持多种检测方式，多种扫描方式，同时也具备检测恶意爬虫的能力，其中包括 Acunetix、Appscan、Nessus、Sqlmap、Arachni、Netsparke、Webinspect、绿盟

极光等。其它的防护还包括会话劫持检测、木马检测等。

WEB 防护引擎里面还集成了一些高级防护功能，精确访问控制的自定义规则功能、防盗链、CSRF 攻击检测、CC 攻击防护、应用隐藏、防篡改。这些高级防护能够对 WEB 站点资源进行保护、防止 HTTP FLOOD 攻击、内容防泄漏等。

4.7 工控安全

中数国科网络入侵检测系统融合工控协议引擎，可以在互联网与工业网络之间做协议深度解析和识别，结合传统入侵防御和工控解析引擎优势，对不同网络协议进行区分处理，满足网络安全合规要求。

通过自主研发的深度数据包解析引擎，产品能够检测出 100+种的常见工业协议识别，同时支持 Modbus、OPC、S7、Enternet/IP（CIP）、DNP3、ICE104、Profinet 等主流工控协议的深度报文解析，可以协议报文中的有效内容特征、负载和可用匹配信息，如恶意软件、具体指令和应用程序类型，对工控协议特征做到实时解析和精准的识别。

■ 支持主流 100+工控协议识别。

■ 支持 Modbus、OPC、S7、CIP、DNP3、ICE104、Profinet 等 7 类工控协议深度解析。

■ Modbus 支持源目 IP、功能码、起始地址、结束地址控制。

■ CIP 支持源目 IP、对象、服务控制。

■ S7 支持源目 IP、功能码、寄存器区、DB 区区号、点类型、起始地址、结束地址控制。

■ OPC 支持动态端口识别，支持源目 IP、接口名、方法名控制。

■ DNP3 支持动态端口识别，支持源目 IP 功能码、对象组号、变体号控制。

■ Profinet 支持源目 IP、接口名、方法名、Block Typ 控制。

■ ICE104 支持源目 IP、类型标识、起始公共地址、结束公共地址、起始信息体地址、结束信息体地址。

■ 支持白名单自动学习功能，可以设定学习源目 IP、学习时间、学习时长等属性。

■ 支持学习模式、控制模式、告警模式。

4.8 应用审计

应用审计，是通过对数据包的深入解析，获取应用的行为及操作内容。通过用户配置的关键字进行匹配。达到对互联网访问的行为控制和内容控制的目的。其依附于安全策略，减少了数据包的过滤范围，并有针对性（针对用户、应用）的进行审计和记录。

应用审计是基于应用+行为+动作+关键字的四维匹配条件，可以实现精细化的控制。可以实现允许查看微博，但是不允许发微博的精细化控制。

4.9 URL 审计

URL 策略，是通过 URL 分类库，对网站访问进行过滤。让用户通过网站分类的选择，轻松控制网站访问。同样，URL 过滤也依附于安全策略。可以减少了数据包的过滤范围，并记录访问网站及 URL。

4.10 全面的安全能力

支持跨站脚本(XSS)、注入式攻击。包括 SQL 注入，命令注入 ，Cookie 注入等。跨站请求伪造等应用攻击行为。

支持恶意扫描防护，可以屏蔽 Web 扫描器的检测，如： Web Vulnerability Scanner 及 IBM-App Scan，有效阻止攻击者利用扫描器进行更换 Web 网站主页，盗取管理员密码，破坏整个网站数据等攻击，具备抗 CC 控制和通道防护能力。

4.11 资产识别和风险评估

如果看不到，则无法提供保护。深入了解网络设备、应用、用户、操作系统和文件等利用这些信息能更好地了解网络行为，识别违规操作，并评估入侵风险。

采用主动扫描和监控主机流量的方式识别网络中的资产信息，能够识别出网络中的设备类型，包括 PC、交换机、打印机等；能够识别设备的操作系统、使用的浏览器、杀毒软件、开启的应用服务；能够帮助安全管理人员掌握内网的资产情况，识别潜在风险。

根据产生的日志信息，多维度分析资产风险。包括是否受到 IDS 攻击、是否下载了病毒文件、是否存在弱密码，是否往外传输文件等。以确认资产的风险情况，对存在风险的资产发出告警，可以帮助安全管理人员及时调整安全策略。

4.12 服务器非法外联和外联自学习

服务器非法外联用于对特定条件下服务器的外联行为进行识别。可以通过设定允许服务器外联的地址、允许通过的协议及端口来定义服务器的正常外联行为。手工定义的正常外联行为之外的所有外联行为全部作为非法外联，将会按照服务器异常防护策略的设定进行处理。

服务器外联具备自学习功能。配置服务器外联学习之后，设备将对配置学习服务器主动发起的外联数据进行获取，并从获取到的主动外联数据中学习服务器开放的端口及其提供的服务信息。学习完成后设备将通过服务器自学习结果判定服务器的所有网络行为，可以判断哪些外联行为是正常的，哪些是异常的。对于正常外联行为可以直接加入非法外联策略白名单。

五、典型组网应用

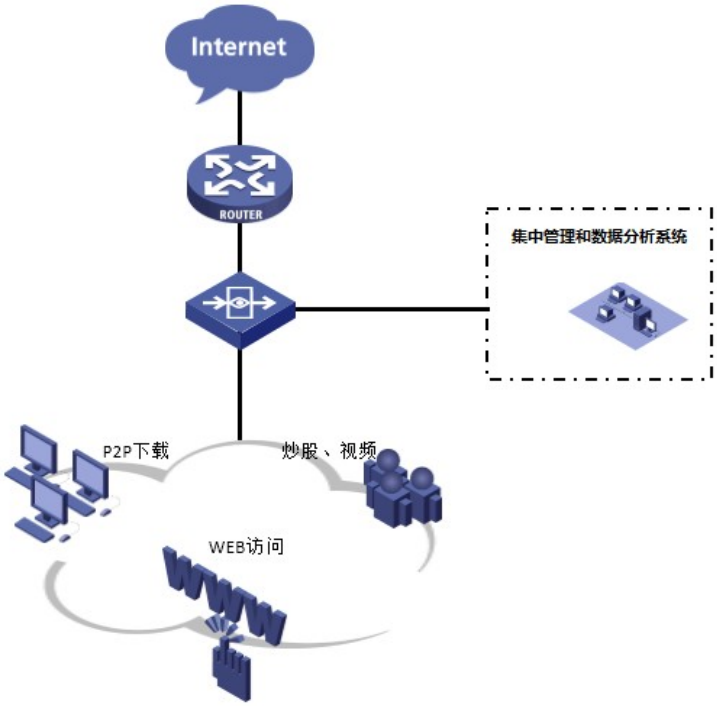
5.1 在线部署

■ 适用于大中型企业用户，以透明方式在线部署于网络出口；无需改变网络拓扑；

■ 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽；

■ 对用户上网行为进行分析与审计；

■ 支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理；



5.2 旁挂部署

■ 适用于大中型企业用户，以旁挂方式部署于核心设备旁；不影响网络结构，

部署简单；

■对用户网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等的流量、行为进行分析及审计；

■支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理；