IPS-7000 入侵防御系统

技术白皮书

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京安博通科技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，但北京安博通科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目　录

1 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。

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，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

入侵检测系统很好的弥补了防火墙的不足，通过部署入侵检测系统，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。

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。

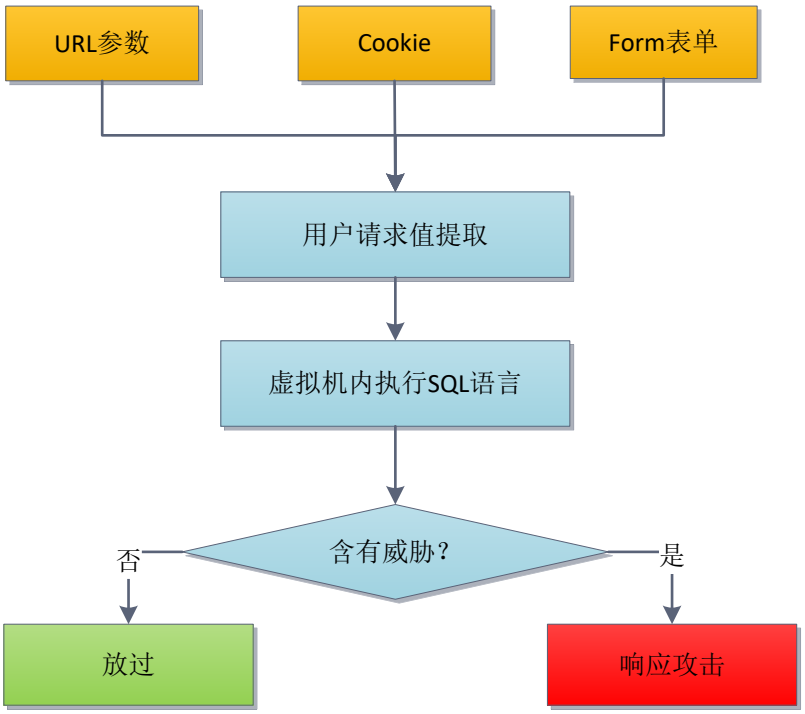
2 产品特点

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。

安博通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

安博通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。

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

安博通入侵检测系统提供了用户身份识别功能，安博通将下一代防火墙中的用户识别的理念引入到入侵检测系统当中，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。

安博通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

现有的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

安博通 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。安博通 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。

例如安博通 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 串将被提交给安博通 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。

安博通 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，安博通 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 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 2 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。

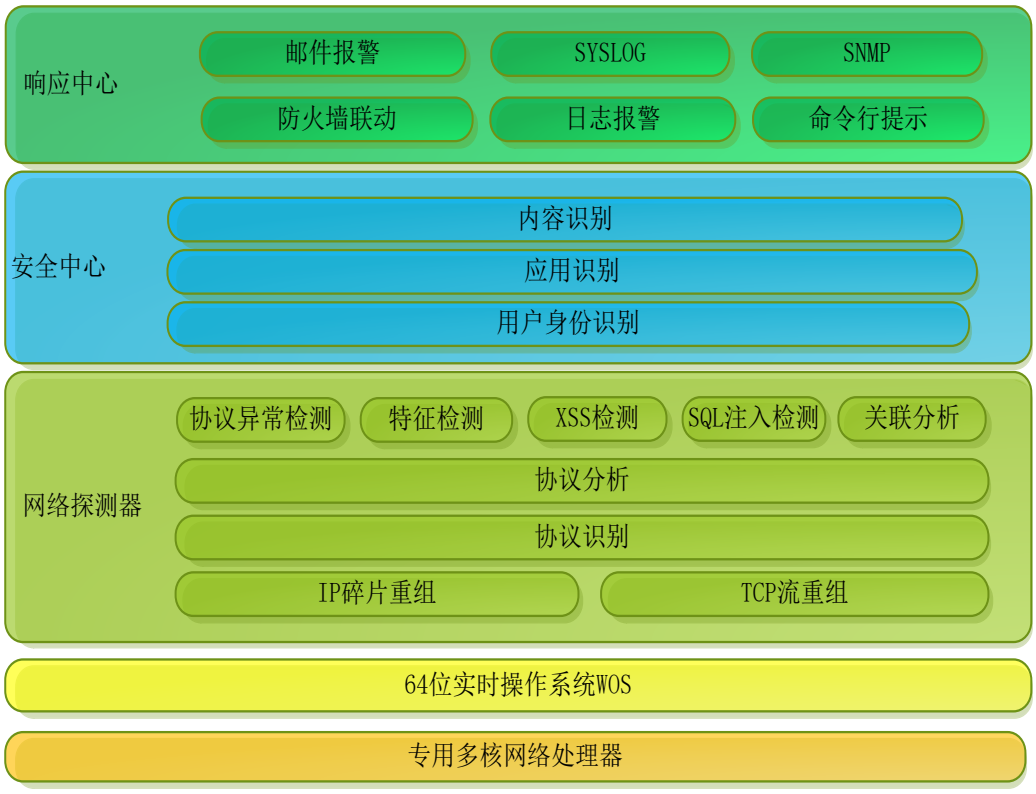
这个攻击是否流行。如果攻击针对的漏洞是几年前出现的，这样攻击的威胁成都就比较低。

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。安博通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。

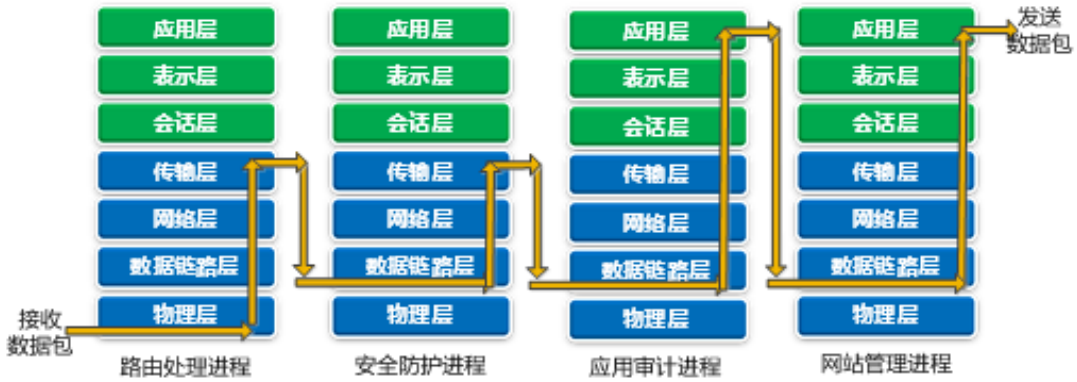
2.8 高性能多业务并行架构

IPS-7000 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 IPS-7000 产品的性能得到大幅度的提升。

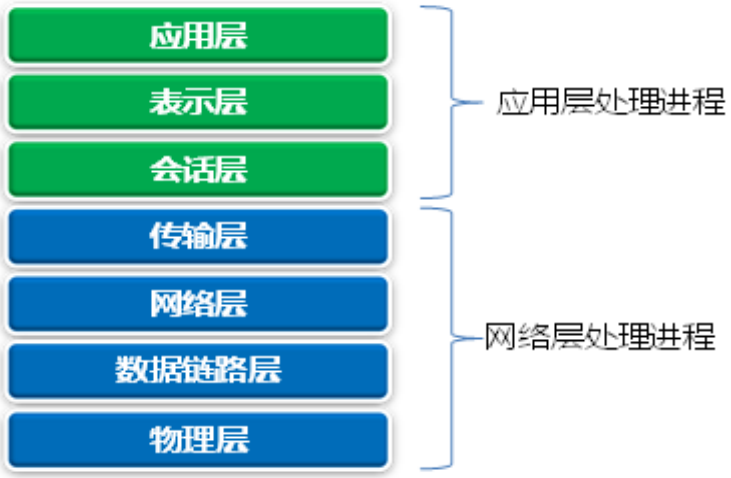


3 技术实现

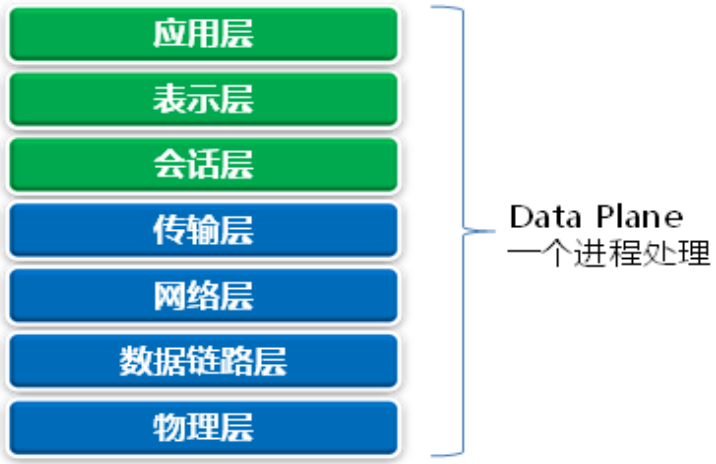
数据面传统的网关设备为了降低设计和开发难度，会将各个模块以进程的方式存在，数据包每通过一个模块都要重复对数据的解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



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。



IPS-7000 系列的 DP 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。



3.1 实时检测和过滤 Web 攻击

安博通 Web 应用防火墙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。

3.2 Web 访问检查和优化

安博通 Web 应用防火墙不但可以帮助用户进行 Web 安全防御，提高网站安全性，而且集成了网络爬虫识别和过滤、网站资源盗链防护、内容关键字过滤、HTTP 协议合规性和 URL 参数合规性检查等功能，可以帮助用户对网站的访问进行过滤和优化，提高网站运营的稳定性和服务质量。

3.3 病毒上传过滤

安博通 Web 应用防火墙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。

3.4 多种部署模式

安博通 Web 应用防火墙支持透明、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。

3.5 精细化的防护策略配置

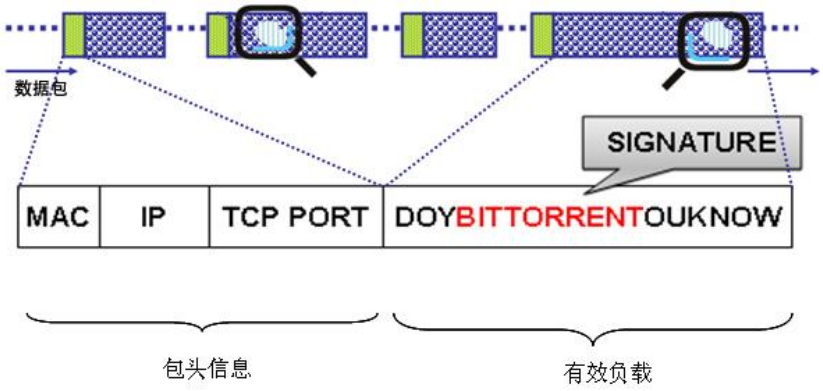
为了能够给不同的网站提供专业有针对性地安全防护，安博通 Web 应用防火墙提供了针对不同网站，甚至是不同 URL、Web 目录分别设置防护策略的功能。同时每一套防护策略都自成体系，可以进行菜单式的防护项目的组合和配置，形成针对每一个防护对象的独特策略模板。通过防护对象精细化和防护策略模板化的处理，用户可以方便、快捷的实现不同网站、不同 URL 的精准安全防护。

3.6 IPS 模块

IPS 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。IPS 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。



3.7 应用识别

3.7.1 应用识别概述

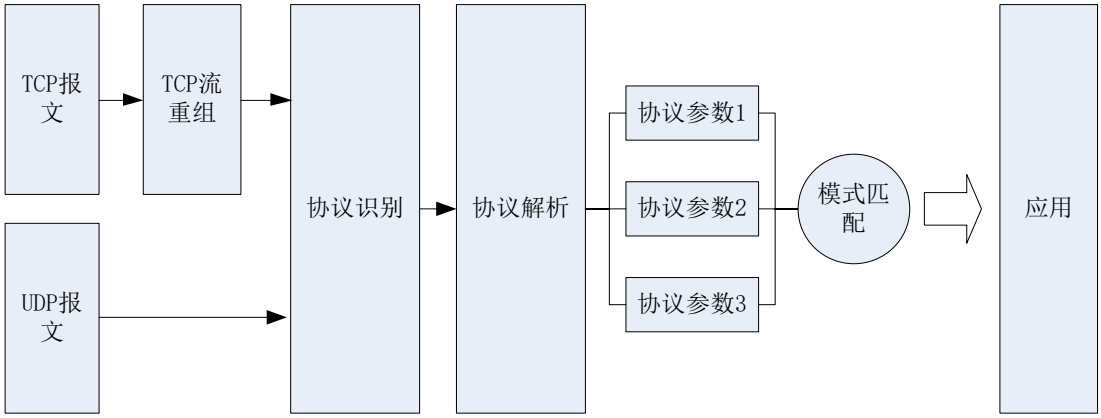
应用识别（Application identify)是 IPS-7000 系列的重要功能。借助于应用识别功能，可以准确识别网络上正在运行的应用，应用流量的准确识别不但可洞悉整个网络的运行情况，而且可针对具体需求做用户行为的准确管控，这在一定程度上既可保证业务流的高效运行也可预防由于内网机器受到攻击而生产的威胁，同时识别应用类型也是应用审计与应用流量控

制的基础。

随着 P2P 应用的广泛流行和基于 Web 的应用的兴起，令传统的利用固定端口来区分应用类型的设备无能无力。应用识别功能把对报文的协议解析、深度内容检测以及关联分析结合起来，通过对大量实际环境中的流量的分析，总结出每种应用的流量模型，把对数据包的协议解析、深度内容检测和关系分析的结果综合起来，由决策引擎通过与流量模拟的匹配程度，智能的判定应用类型，相比传统的应用识别技术，还具有以下特点：

基于协议状态分析，IPS-7000 系列对已知协议和 RFC 规范的深入理解，可准确、高效的对各种协议进行解析。例如，对于一次 HTTP 访问，先由协议解析出访问的 URL、Host、User-Agent 等信息，再将解析出来的信息进行特征匹配，这样可以带来以下优点：

- 提高性能，不需要对整个报文进行模板匹配，可以提高应用识别的性能。
- 降低误识别率，因为进行模式匹配的字段由整个报文缩小为特定的协议参数，可使特征写的更加精确，减少误识别率。

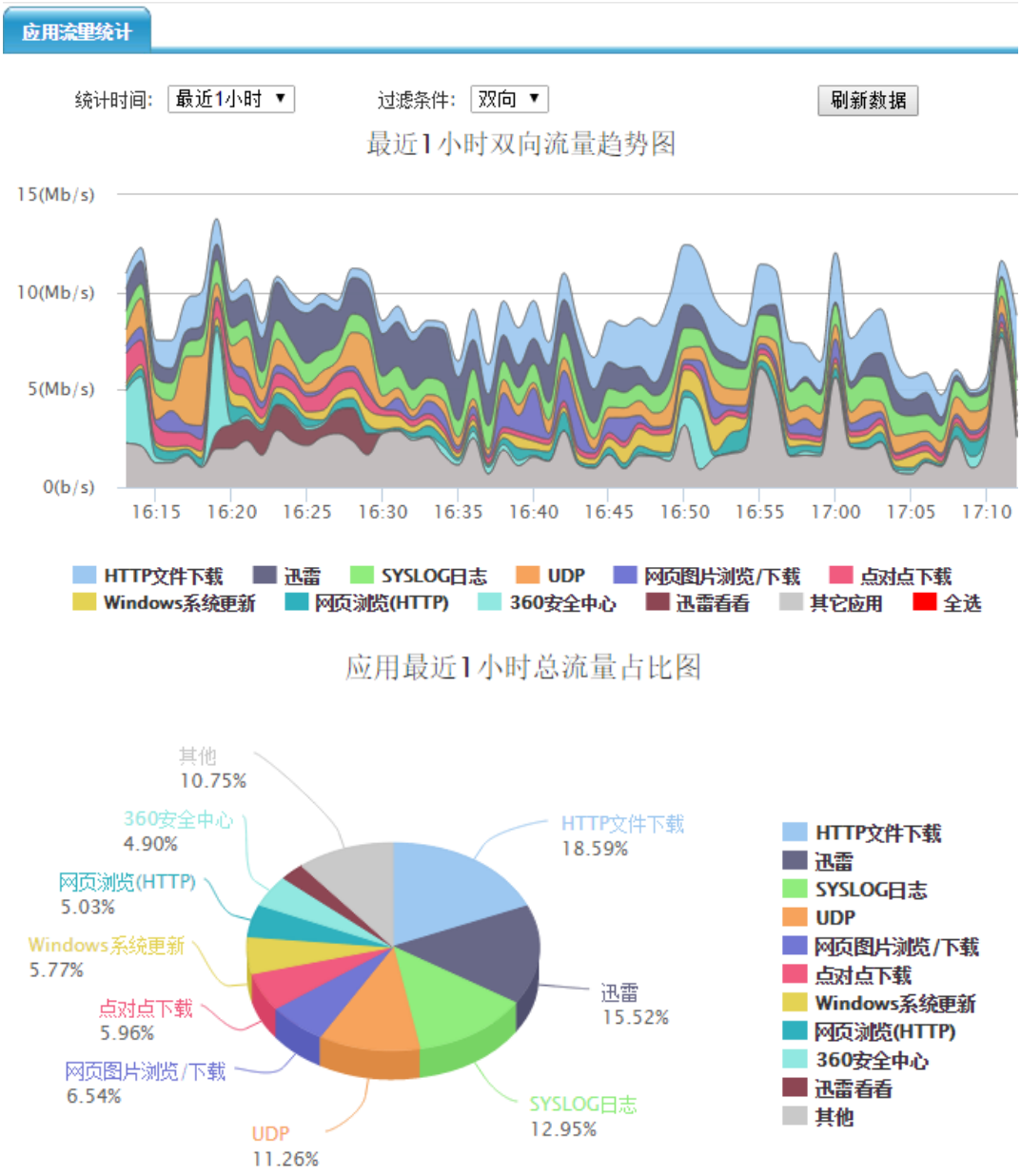


行为检测，不同的应用类型体现在会话连接或数据流上的状态各有不同；基于这一系列流量的行为特征，通过分析会话连接流的包长、连接速率、发送/接收的流量比例、包与包之间的间隔等信息来识别应用类型。

只有在准确识别应用协议的基础上，才能对应用做到深入、全面和准确地控制。不但可以准确、高效的识别出网络流量的应用类型，而且可以精准的识别出应用的行为。随着特征库的不断更新，支持的应用和行为在不断增加。网络中的应用日新月益，拥有强大的安全服务团队的支持，可以随时对网络中的新应用进行跟踪分析，持续的更新应用特征库。

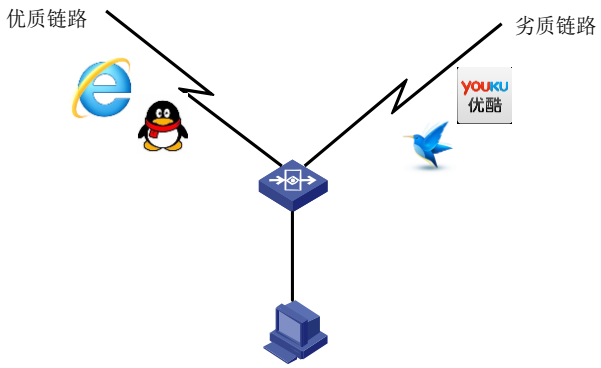
3.7.2 应用流量统计

借助于强大的应用识别，用户可以通过应用流量统计查看到网络中的应用流量组成，准确了解网络的使用情况。



3.7.3 应用路由

IPS-7000 系列通过配置策略路由，可以实现基于应用的路由选择。在用户有多条链路的情况下，不同的应用分别使用不同的线路，使办公、游戏等重要应用的流量使用链路状态较好的线路，使 P2P、视频等流量走链路状态较差的线路，帮助用户合理的分配链路资源，即保证重要业务的使用，也不影响 P2P、视频等的使用。



IPS-7000 系列的应用路由功能是不是基于端口，而基于应用来实现的，当发现某种应用的流量的时候，会把对应的 IP + 端口信息缓存在系统中，相同的 IP + 端口再次新建会话的会话，会命中相应的缓存，从而实现应用路由的功能。

3.7.4 基于应用的流量管理

IPS-7000 系列可以实现基于应用的带宽分配，帮忙用户更好的限制 P2P、视频等占用带宽比较高的业务，保障重要业务的运行。

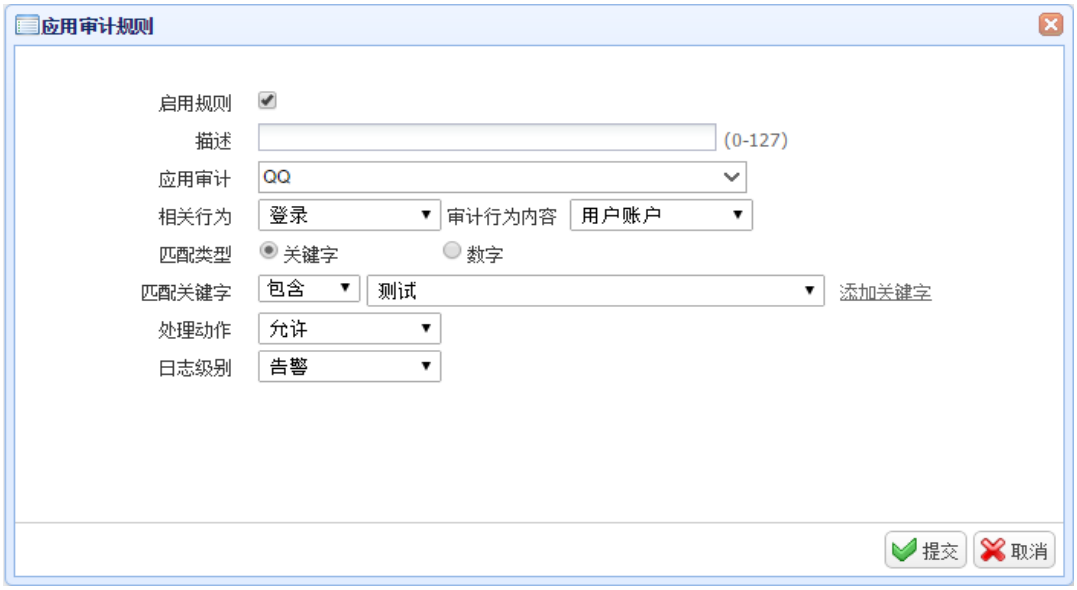
3.8 应用策略

应用策略分为应用审计和 URL 审计两部分。

3.8.1 应用审计

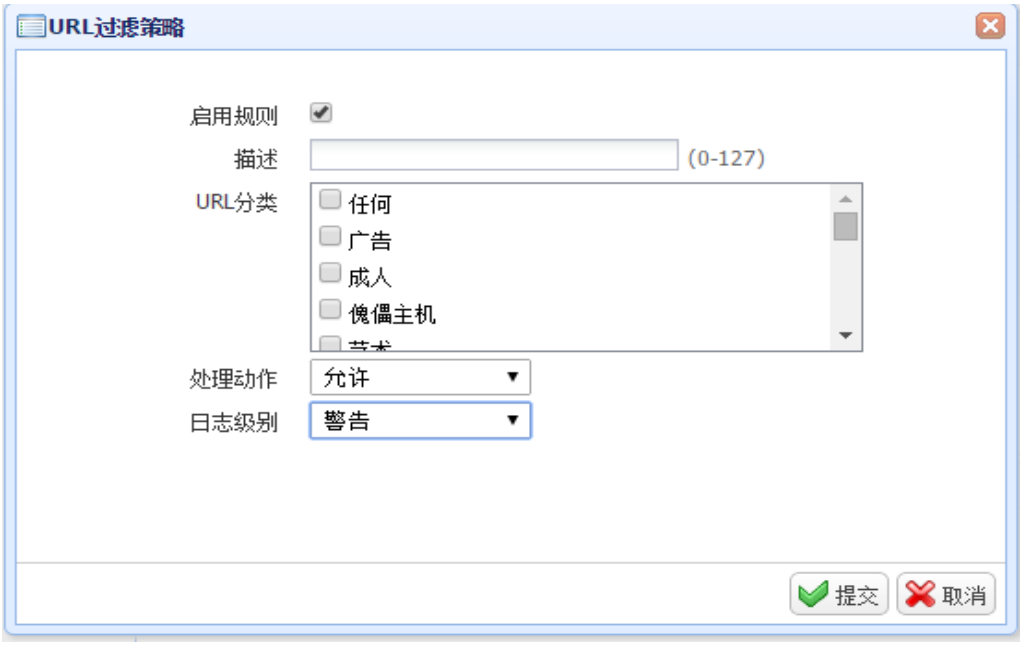
应用审计，是通过对数据包的深入解析，获取应用的行为及操作内容。通过用户配置的关键字进行匹配。达到对互联网访问的行为控制和内容控制的目的。其依附于安全策略，减少了数据包的过滤范围，并有针对性（针对用户、应用）的进行审计和记录。

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。



3.8.2 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。



3.9 访问控制和审计

现代的网络应用发展已经从以前单一的功能，向着多功能的方向发展。比如 QQ，以前只是作为一种通信工具，传输消息，现在 QQ 可以传文件、发微博、购物、发邮件等等；丰富的应用功能让企业管理者对内部资料泄密和员工工作效率下降大伤脑筋。IPS-7000 系列提供以访问控制、事后审计、用户轨迹三大功能。核心思想是帮助 IT 管理员使整个网络易

用、安全。IT 管理员可以从用户、设备、应用、行为等多个视角来管理分析网络。

3.10 精细化访问控制

随着 WEB2.0 技术的蓬勃发展和动态端口的新应用层次不穷，使得传统网关产品采用五元组的访问控制方式早已变得力不从心，而 IPS-7000 的出现让访问控制变得简单，基于 7 元组以及时间的访问控制策略，能有效的控制自然人、应用的访问控制。在该访问策略中，还可以对应用行为和内容进行控制，比如控制 QQ 传文件但不控制 QQ 收发消息；过滤关键字，防止涉密信息通过邮件泄密等等。

3.11 链路负载均衡

随着带宽成本的下降及业务需求，企业通常存在两个或两个以上的网络出口，多出口提升了网络出口稳定性同时又带来了多链路带宽利用率低、多链路带宽差异大、各运营商网络质量差异、内网应用对带宽需求差异等问题；以上诸多问题只需通过 IPS-7000 提供的链路负载均衡即可迎刃而解。具体实现主要基于以下几点：

- 实时多链路监测：

实时监测每条出口链路的逻辑连通性，即使端口处于 UP 状态，但可能由于远端故障导致的检测报文超时，IPS-7000 同样会执行链路切换的动作，以保证网络连接的可用性，实现多条链路的冗余备份。

- 基于权重流量分担：

IPS-7000提供了基于优先级和权重的多链路流量分担算法以满足不同应用场景的需求，从而达到高效的利用出口链路带宽的目的。

- 运营商智能选路：

内置电信、联通、移动和教育网地址库，可以智能的依据目的 IP 运营商属性来决定流量走向，将属于该运营商的访问自动的指向该运营商的链路，实现“南北互通”。

- 智能应用路由：

IPS-7000 内置超过 1400 种以上的应用识别能力，将网络中各种应用进行准确分类和精细识别，让不同的应用分别使用不同的出口线路，保证重要业务不中断。

- DNS 透明代理：

通过透明代理技术，完成对客户 dns 流量的无感知代理，从而保证客户的 dns 请求得到最快，最稳定的响应，大幅度提升客户的上网感受。

3.12 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。

3.13 成熟稳定的数据库

审计功能每秒钟会产生数以千计的审计记录。为了使这些审计记录能被快速的统计，浏览，就需要使用数据库。目前我们使用的是比较成熟的 PostgreSQL 数据库。但是对于审计功能，记录量过于庞大，将这些记录放入同一个表格中显然不便于后续处理。所以，对于每个审计，我们每天创建一个表格。当天的数据会存放到对应的表格中，每天 0 点，会自动切换要入库的表格。

这些表格会在系统启动时创建，创建时为了便于切换，将当天的表格和第二天的表格一起创建。以后每 5 分钟检查一次，如果表格不存在或者需要创建新的表格（时间已经过了 0 点，需要创建第二天的表格），就创建对应的表格。大量的统计数据入库，对于磁盘的压力也是巨大的。如果不及时清理，有可能造成磁盘耗尽，新的数据无法入库。系统对磁盘使用率一个上限和一个下限，每 1 分钟检查一次磁盘使用率。如果磁盘使用超过上限，系统开始删除数据库中最先创建的表格，一直删除至磁盘使用率小于使用率下限。

所有的审计记录都被输入到的指定的文件中。系统每一秒检查一次这些文件，将其中的记录批量导入到相应的数据库表格中。然后清空文件，方便下一次记录。

3.14 集中管理和数据分析系统

安博通集中管理和数据分析系统是提供对 IPS-7000 的集中监控、配置和升级，并且对上报的安全相关信息收集存储，通过数据发掘提供详尽灵活的统计图、报表，从而辅助管理员进行安全信息审计。利用集中管理和数据分析系统，管理员可以高效地管理各 IPS-7000 设备，全面掌握网络的整体安全状况。

3.14.1 设备集中管理

安博通集中管理和数据分析系统可以作为 IPS-7000 大规模部署的集中管理平台，能够支持大规模的并发量。系统每隔 5 分钟就对这几千个网络节点进行轮巡，并且可以根据不同的轮巡时间对网络设备进行分组监测，这样就大大降低系统的并发监测数量，提升系统的性能。

3.14.2 策略统一下发

安博通集中管理和数据分析系统具有策略统一下发能力，帮助管理员脱离苦海，集中新建七元组策略批量下发到每一台设备，对于政府、运营商、金融、电力和大型企业等分支结构众多的客户，可以极大的降低运维人员的工作量，帮助客户实现高效率管理运维。

3.14.3 采用高性能数据存储和查询

安博通集中管理和数据分析系统采用高性能数据仓库，此数据仓库是一款基于网格技术的列式数据库。简单易用，快速安装部署，使用中无需复杂操作，能大幅度减少管理工作；在应对 50TB 甚至更多数据量进行多并发复杂查询时，更能够显示出令人惊叹的速度。

安博通集中管理和数据分析系统支持 TB 级原始数据量的高性能查询，大数据量查询性能强劲、稳定：查询性能高，如百万、千万、亿级记录数条件下，同等的 SELECT 查询语句，速度比 MyISAM、InnoDB 等普通的 MySQL 存储引擎快 5 ~ 60 倍。高效查询主要依赖特殊设计的存储结构对查询的优化，帮助用户快速定位网络问题，查询各种条件的审计检索。高数据压缩比，能够帮助用户节省存储成本，支持普通 X86 服务器，无需专用硬件设备和存储，在某实验局没有采用集中管理和数据分析系统前日志存储 1 个月产生 500G 数据，而采用安博通集中管理和数据分析系统后，数据 1 个月存储减少至 60 多 G，这样大大节省了用户的存储硬件成本。

3.14.4 深层次数据挖据分析

安博通集中管理和数据分析系统采用了先进的数据挖掘分析技术，从收集到的大量数据当中进行深层的数据挖掘及分析，该子系统由日志代理、日志审计中心、日志数据库、审计系统管理器、日志分析中心五个部分组成。日志代理负责收集区域内各种操作系统、网络安全设备、应用程序的日志信息，过滤后发送给日志审计中心处理。日志审计中心负责接受区域内日志代理和各种安全设备、系统转发的日志信息，集中保存在日志数据库，日志分析中心负责对日志数据进行深度挖掘。

日志数据的深度分析工作主要由日志分析中心来完成。日志分析中心首先通过 ETL 处理，利用专用的数据抽取工具，将日志数据按照定义的规则，通过复杂的抽取、转换、清洗及聚合，最后装载至数据仓库 DW 中，生成满足多维分析的数据仓库数据，即事实表和维表。通过 OLAP 多维分析技术和 BI 前端展现工具，提供针对日志数据仓库的日常查询、统计报表、OLAP 分析、数据挖掘、KPI 统计分析和监控告警等决策分析功能，并将结果通过 WEB/GUI 方式展现给用户。

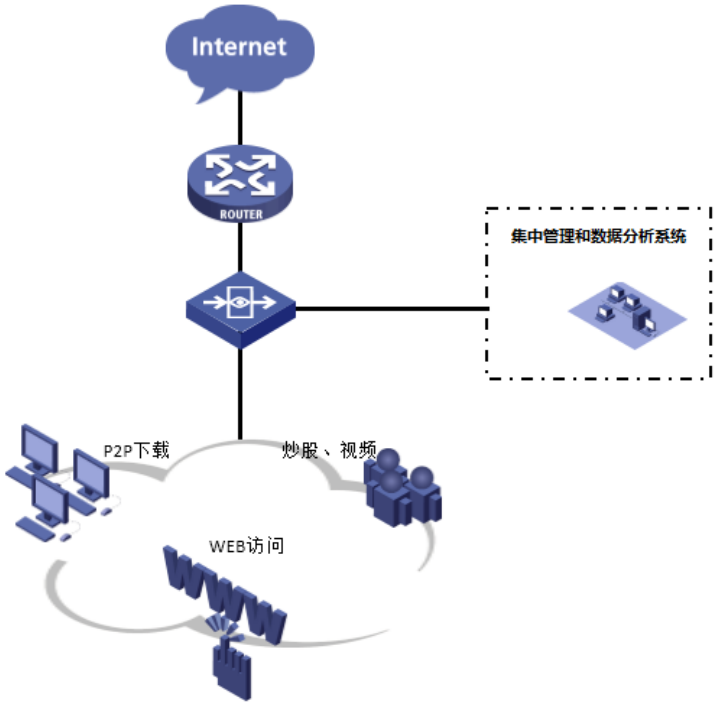
数据仓库是在企业管理和决策中面向主题的、集成的、与时间相关的、不可修改的数据集合。与其他数据库应用不同的是数据仓库更像一种过程，对分布在企业内部各处的业务数据的集合、加工和分析的过程。

数据仓库中包含 ETL、数据模型、信息展现等主要关键技术。ETL 是数据抽取（Extract）、清洗（Cleaning）、转换（Transform）、装载（Load）的过程。它是构建数据仓库的重要一环，用户从数据源抽取出所需的数据，经过数据清洗,最终按照预先定义好的数据仓库模型，将数据加载到数据仓库中去。数据模型的重要性在于对数据做标准化定义，实现统一的编码、统一的分类和组织。标准化定义的内容包括：标准代码统一、业务术语统一。ETL 依照模型进行初始加载、增量加载、缓慢增长维、慢速变化维、事实表加载等数据集成，并根据业务需求制定相应的加载策略、刷新策略、汇总策略、维护策略。

4 典型组网应用

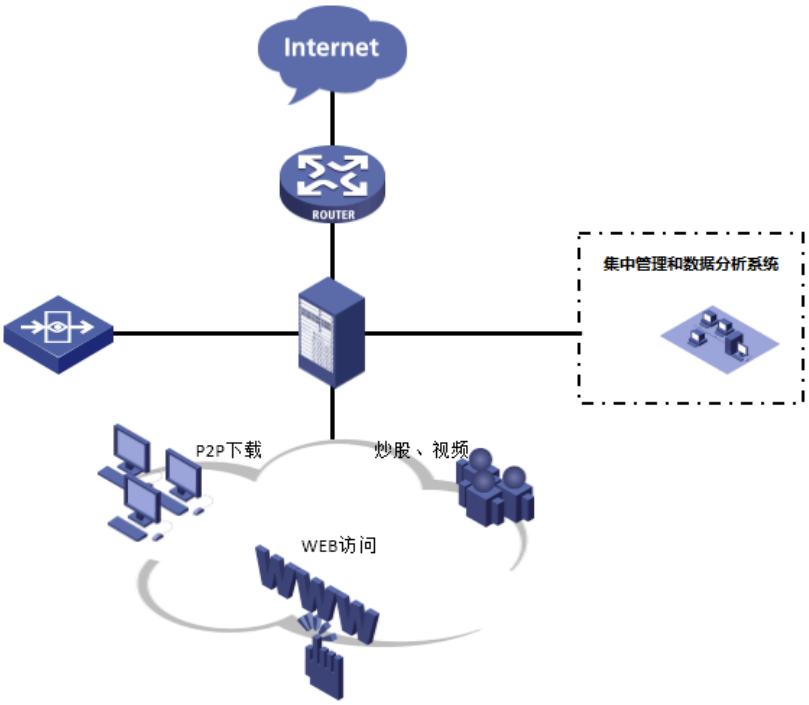
4.1 在线部署

- 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；



4.2 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；


Internet
ROUTER
集中管理和数据分析系统
P2P下载
炒股、视频
WEB访问

5 功能列表

分类	功能	详细指标
首页	系统信息	显示当前设备的：软件 SN；主机名称；产品型号；系统版本；系统时间； 运行时间；当前会话数；URL 版本；APP 版本；IPS 版本；AV 版本
	实时流量图	默认显示当前系统的整机实时流量，可以设置显示不同接口的实时流量
	系统资源	显示系统内存资源使用情况 ;显示系统 CPU 资源使用情况
	接口状态	显示当前系统 link 的接口信息
	应用流量排名	默认显示当前系统 TOP 20 的应用实时流量情况
	IP 排名	默认显示当前系统 TOP 20 的 IP 实时流量情况
	网络层攻击日志	显示当前系统最新的网络攻击日志
	入侵检测日志	显示当前系统最新的入侵防护日志
	病毒防护日志	显示当前系统最新的病毒防护日志
接口状态	接口状态	显示当前设备的接口相关状态：接口列表；接口链路状态；接口属性；接口工作速率 接口工作模式；接口 IP 地址；接口 Ipv6 地址；接口接收速率 ;接口发送速率 ;接口收包总数；接口发包总数。
日志管理	威胁日志	显示系统当前威胁日志，支持查询
	病毒防护日志	显示系统当前病毒防护日志，支持查询
	网络安全日志	显示系统当前网络安全日志，支持查询
	配置日志	显示系统当前配置日志，支持查询
	系统日志	显示系统当前系统事件日志，支持查询
	网站访问日志	显示系统当前的网站访问日志；恶意 URL 日志。基于硬盘显示
	应用审计日志	显示系统当前的审计日志包含：IM；社区；搜索；邮件；文件传输；娱乐股票；其他。基于硬盘显示
系统监控	会话统计	显示当前系统基于源地址的 session 实时统计状态，支持查询和会话过滤
	会话监控	显示当前系统实时的 session 情况，支持查询
	会话限制阻断	显示当前系统阻断的会话情况，支持查询
	黑名单记录	显示当前系统的黑名单记录。
	防共享监控	显示当前系统的防共享监控情况，支持查询和针对特定地址的操作
系统策略	IPv4 策略	支持策略增删改查、启用/禁用、移动

		支持策略匹配次数清零
		支持修改默认策略动作：允许/拒绝
		六元组策略匹配条件：、应用、源地址、源接口、目的地址、目的接口、服务
		支持基于时间表的策略配置
		支持应用选择过滤
		支持基于应用的应用类型组选择
		支持策略动作为：允许、拒绝
		基于策略的长连接（老化时间）
		支持动作为拒绝的策略进行日志记录
	IPv6 策略	支持策略增删改查、启用/禁用、移动
		支持策略匹配次数清零
		支持修改默认策略动作：允许/拒绝
		支持基于任意的 7 元组策略
		支持基于时间表的策略配置
		支持策略动作为：允许、拒绝
		支持动作为拒绝的策略进行日志记录
	地址转化策略	支持源地址转化
		支持目的地址转换
		支持一对一地址转换
		支持地址池资源配置
		支持 ALG 协议过 NAT，支持情况 :H.323、SIP、FTP、TFTP、PPTP
		所有地址转换策略支持，增删改查、移动
	解密策略	支持基于策略的 ssl 解密功能
		支持基于预定义 https 域名对象的 ssl 解密功能
		支持基于自定义 https 域名对象的 ssl 解密功能
		支持基于特定 https 域名对象的排除解密功能
		支持基于 ssl 加密邮箱的解密功能
		支持基于特定 IP 地址排除的解密策略
	广告插入	支持基于本地广告的 http 插入功能
		支持基于第三方广告的 http 插入功能
安全防护	入侵防护	支持基于源、目的、规则集的入侵检测。
		支持 5 种自定义动作
		支持软件 bypass（CPU and 内存高于 70%）
		可记录攻击日志和报警。
		支持系统规则库手动、自动升级。
		系统定义超过 3000 条规则，包含 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game。
		支持常见文本类 WAF 规则
		支持常见攻击防护类 WAF 规则
	防病毒	支持 HTTP，FTP，POP3，SMTP，IMAP 协议

		的病毒查杀
		查杀邮件正文/附件、网页及下载文件中包含的病毒
		支持 300 万余种病毒的查杀，病毒库定期与及时更新
		支持启发式扫描查杀未知病毒
		支持 ZIP/RAR 等压缩文件的病毒查杀
		压缩：默认 5 层，最大 20 层
		支持 TAR 等多种打包文件的病毒查杀
	网络安全-防 ARP 攻击	支持基于接口的 ARP 欺骗防护功能
		支持系统实时 ARP 表的系统查看，以及实时的 IP-MAC 绑定功能
		支持系统 IP 和 MAC 的绑定功能，以及新建和删除功能
		支持 ARP flood 防护功能
		支持基于接口的 ARP 学习控制功能
	网络安全-攻击防护	IPv4 安全防护支持 :ping of death ;land-base；tear-drop；tcp flag；winnuke；smurf；IP 选项；IP spoof；joit2.
		IPv6 安全防护支持：winnuke；land-base;tcp flag；fraggle；IP spoof
		支持基于接口的扫描攻击防御
	网络安全-FLOOD 攻击防护	支持基于目的 IP 的 flood 防护 :syn flood ;udp flood；icmp flood；dns flood
		支持基于接口的 flood 防护功能：syn flood；udp flood；icmp flood；dns flood
	网络安全-黑名单	支持系统黑名单的手工创建和删除
		支持系统自动生成对应 IP 地址的黑名单
对象管理	应用	显示预定义分类，支持 18 个分类
		显示分类下应用的属性：中英文名称、平台、风险级别、流行度、描述
		支持基于应用，应用组的增删改查
	关键字	增删改查，支持批量删除
	URL	支持基于特定恶意 URL 的排除
		预定义 56 类的 URL 列表
		支持 URL 的管理员自定义
		URL 支持管理员的增删改查
	地址	支持基于网段，地址段，主机的地址对象创建
		支持基于地址对象的地址组创建
		支持基于域名地址地址对象
		支持基于 IPv4 地址和 IPv6 地址的对象创建
		支持地址对象，地址组对象批量的删除
	服务	系统内设常用的 89 种预定义服务

		支持基于 tcp、udp、源端口、目的端口、icmp 以及其他协议的服务自定义
		支持基于服务对象的服务组对象创建
		支持服务对象，服务组对象的批量删除
	时间	增删改查，支持批量删除
		内置任何时间条目：any
		日计划、周计划、月计划
		计时器
	本地证书	支持内置 CA，为其他设备或移动用户签发证书。
		支持本地 CA 根证书、根私钥的更新。
		支持在线 CRL 列表。
接口管理	物理接口	启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型：静态（支持主从）
		DHCP 下发 DNS
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		协商模式：自动、强制（可设置双工和速率）
		工作模式：路由模式、桥模式
		MTU，修改范围 1280-1500
	子接口	子接口管理（增删改查）
		子接口 ID：1-4094
		启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	桥接口	桥接口管理（增删改查）
		桥接口 ID：0-255
		启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	聚合接口	聚合接口管理（增删改查）
		聚合接口 ID：0-255
		启用/关闭

		IPv4 地址类型：静态（支持主从）、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	旁路接口	所有物理接口支持旁路部署
	loopback 接口	支持生成、配置 loopback 接口。（命令行支持）
		支持基于 loopback（或指定 IP）接口地址的管理（设备管理等）（命令行支持）
	TCP MSS 调整	支持根据业务类型智能调整
		命令行支持接口 TCP MSS 手工调整, 支持全局设置和 VPN 单独配置
路由管理	路由表	显示设备路由信息
	高级路由属性	支持非对称路由
		命令行下支持强制源进源出
	静态路由	增删改查
		支持基于路由权重的多链路负载均衡
		支持路由优先级
		支持 VRF 配置
	策略路由	增删改查、移动
		5 元组策略路由+时间
		基于用户的策略路由
		基于应用的策略路由
		支持基于路由权重的多链路负载均衡
	ISP 路由	内置电信、联通 ISP 信息
		支持自定义 ISP 信息
		增删改查
	RIP	支持 v1、v2
		支持缺省路由发布和路由重发布
		支持接口下发送版本和接收版本的设置
		支持认证方式：字符、MD5、不需要认证
	OSPF	支持缺省路由发布、路由重发布
		支持 OSPF 网络区域信息的增删改查
		支持接口下相关配置
		支持认证方式：字符、MD5、不需要认证
高级网络	DHCP	DHCP 服务器
		DHCP 中继代理
		网络配置：网关、子网、开始结束 IP 地址
		租约：无限、有限时长
		高级属性：DNS 支持 2 个，Wins 支持 2 个，域

		支持排除地址
		支持 IP-MAC 绑定
		显示 IP 地址和 MAC 地址及开始时间、结束时间
		清除条目
	DNS 代理	支持基于系统的全局 DNS 透明代理功能
		dns 服务器支持基于每条链路的配置
		DNS 链路服务器之间支持权重和优先级两种配置算法
		支持全局的静态域名配置
		支持全局的特定域名特定 dns 服务器的解析
		支持 dns 全局的缓存功能，注缓存功能和基于权重的算法互斥
	IPv6 网络	IPv6 路由通告
		IPv6 静态路由、OSPFv3
		支持用户和应用均为任意的 7 元组策略
		扩展报文头的逐跳报文的处理、分片报文等的处理
		隧道支持：手工隧道，6to4 隧道，ISATAP
		Nat64
		防畸形报文攻击
	链路负载均衡	基于七元组的链路负载均衡策略
		基于域名的负载均衡策略
		基于接口，接口组的负载均衡策略
		基于直连网段和特定网段的负载均衡排除
		负载均衡接口支持 pppoe，dhcp，聚合链路，物理接口，等三层接口
		基于 ICMP 的接口探测机制
		支持基于源地址 hash 的链路负载均衡
		支持基于优先级的链路负载均衡
	服务器质量管理	支持 ping 地址监控条目
		支持 tcpsyn 地址监控条目
		支持 dns 地址监控条目
		支持接口类型：物理接口，子接口，桥接口，聚合接口，隧道接口
		支持多个地址探测从属组关系
		分为严格模式和非严格模式（严格模式即所有探测条目均成功组状态才成功，非严格模式探测条目间为独立状态）
		支持对探测组描述
		支持探测路由以确保路由有效性
		支持静态路由或 ISP 路由联动
		支持与接口状态联动

		支持与 HA 联动
		可对地址探测失效、恢复有日志记录
	每 IP 会话限制	显示限制信息
		IP 会话限制内容 :IP 地址、连接数、会话限制、每秒新建、每秒新建限制、限制阻断统计、引用地址对象名
		支持查询过滤和全部显示
基本配置	权限管理	管理员账号的增删改查
		只读管理员查看配置权限（审计员）
		登录认证方式支持本地认证、Radius 服务器认证、LDAP 服务器认证
		密码复杂度 :必须包括数字, 英文和字符, 6-63 个字符
		每帐号可绑定 3 个 IPv4 地址或子网
		支持管理员在线监控和强制下线
		支持管理员黑名单，阻断用户可监控，可解锁
	产品授权	许可证：系统版本；app；url；IPS 库，av 库
	产品升级	系统升级手动、自动、升级历史
		支持断点续传
		动态库升级（应用、URL、IPS、AV）
	高可用性配置	支持配置同步
		支持流同步
		支持特征库同步
		支持接口状态监控
		支持抢占模式
		支持备机可管理
		支持 AGG 口作为心跳口，提高心跳口可靠性
		支持 HA 状态监控
		支持主主模式和主备模式
系统设定	时间设定	手工设置时间
		NTP 同步
		设备间同步时间（通过 NTP 保持一致）
	DNS 设定	手工设置系统的 DNS 服务器
		dns 代理功能可以使用系统的 dns 服务器解析
	邮件管理设定	支持设定邮件服务器
		支持设定需要发送邮件的多个账号
		支持 IPS，AV，DDOS，系统资源的邮件告警
		支持邮件设定的增删改
	日志管理设定	syslog 日志配置日志服务器：地址和端口（3 组）
		日志过滤本地认日志记录开关、日志服务器日志级别开关
		设备映射表设备映射表流量、上网行为、系统

		管理
	引擎管理	支持系统三种应用识别模式的设置：智能模式；快速模式；关闭引擎
	SNMP 管理	SNMP 代理
		版本：v1、v2、v3
		trap 版本：v1、v2 Notification、v2Inform
		trap 地址
		CPU、内存
		增删改查
		认证方式：None、MD5、SHA
		支持跨三层 IP MAC 绑定
	系统会话设置	支持系统各种会话以及各种会话状态的时间设置
	系统服务管理	支持命令行管理端口的漂移
		支持界面管理端口的漂移
		最大登录重试次数 1-60 次，默认为 5 次
		登录失败阻断间隔 1-3600 秒，默认为 1 分钟
		页面超时时间 1-480 分，默认为 10 分钟
		在线管理员 1-20 个，默认为 20 个
系统维护	系统重启	恢复出厂配置
		系统重启
	配置维护	配置文件导入导出
		双备份配置
	信息收集	设置方式：手动搜集和自动收集
		收集内容操作：下载、查看、删除
	抓包工具	支持按照过滤条件抓取数据报文
		支持将报文下载到本地保存查看