领信网络入侵检测系统*技术白皮书* V7.0

LinkTrust™

IDS Family

SN:200301125

更体贴您的每一项安全需要

We know more …

Your security

安氏互联网安全系统（中国）有限公司

Information Security One (China) Ltd.

安氏互联网安全系统(中国)有限公司广州分公司
地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室　邮编：510630
总机：020-38731555、38732069、38730525 转 2013　传真：020-38730144
手机：13600056899　　网址：http://www.is-one.net

1）权利归属

本文档中的 LinkTrust™的所有权和运作权归安氏互联网安全系统（中国）有限公司（下称安氏公司），安氏公司提供的服务将完全按照其发布的版权声明以及相关的操作规则严格执行。LinkTrust™ 是安氏公司的商标。因 LinkTrust™所产生的一切知识产权归安氏公司,并受版权、商标、标签和其他财产所有权法律的保护。

2）其它产品说明

本文档中所提及的所有其他名称是各自所有者的品牌、 产品、商标或注册商标。

3）授权声明

任何组织和个人对安氏公司产品的拥有、使用以及复制都必须经过安氏公司书面的有效授权。

4）服务修订

安氏公司保留可能更改本文档中所包含的信息而不需预先知照用户的权利；如果该信息非从安氏公司接收，它们将有被更改或变更的可能，安氏公司不需对用户或第三方负责。

5）特别提示

用户对该信息的使用承担风险，并须在"原封不动"条件下使用。安氏公司对此不作任何类型的担保，不论是明确的或隐含的，包括商业性和某个特定目的适应性的保证。

6）有限责任

安氏公司仅就产品信息预先说明的范围承担责任，安氏公司对引起使用或传播的任何损害（包括直接的、间接的、偶然的、附加的、重要的或特殊的以及继起的损害）不负任何责任（即使已经建议安氏公司这些损害的可能性）。

7）管理

用户对信息和服务的使用是根据所有适用于安氏公司的国家法律、地方法律和国际法律标准的。

8）目的

本声明仅为文档信息的使用而发表，非为广告或产品背书目的。

9）服务

安氏公司在产品发布前完全检查过对 Internet 资源的链接和地址，但是 Internet 不断变化的性质使安氏公司不能保证资源内容的连续性或存在性。如有可能，将参考包含使用其他方法可获得信息的预备站点或关键词。

10）法律

上述条款要与中华人民共和国的法律解释相一致，用户和安氏公司一致同意遵循中国司法管辖之原则。如发生上述条款与中华人民共和国法律相抵触时，则这些条款将完全按照法律规定重新解释，而其他条款则依旧保持原法律效力和影响。

支持信息

如果希望得到关于 CyberWall 产品的报价、产品信息以及技术支持，请查阅公司网站：http://www.is-one.net。如果从 www 网站上仍然得不到你所需要的技术支持，请致电本公司技术支持部。

安氏互联网安全系统（中国）有限公司
Information Security One (China) Ltd.

安氏客服中心

北京：010-88083566-1600

上海：021-52396026-2100

广州：020-38731555-2013

目 录

安氏互联网安全系统(中国)有限公司广州分公司
地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室 邮编：510630
总机：020-38731555、38732069、38730525 转 2013 传真：020-38730144
手机：13600056899 网址：http://www.is-one.net

1 前言

网络与信息技术的发展，尤其是互联网的兴起正在改变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运作系统，宝贵的信息资源以数字的形式存在于网络上。互联网是开放的，这意味着任何人都可以在世界任何地点利用互联网访问与之相连的企业网络和信息资源，当然这种访问可能是授权的也可能是非授权的。访问者对企业网络的恶意或非恶意侵犯会给企业带来灾难性的后果，其损失是显而易见的且难以估量的，网络信息安全问题日益突出。随着网络应用范围的不断扩大，对网络的各类攻击与破坏也与日俱增，攻击的方法和手段层出不穷。有矛必有盾，一场破坏与反破坏的信息安全技术大战正在如火如荼地展开。网络安全防护手段多种多样，主要有：

- 入侵检测
- 防火墙
- 漏洞扫描与评估
- 认证与授权
- 密码与加密技术
- 防病毒
- 访问控制

这些技术有的偏重于静态防护、有的偏重于动态防护。任何一种技术都不能保证网络信息系统的足够安全。为了构建一个足够强健的网络安全防护体系，必须采用多种技术结合的方案。入侵检测系统是动态防护技术的核心，是必选的网络安全设备之一。

入侵检测是指：“通过对行为、安全日志或审计数据或其它网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图”(参见国标 GB/T18336)。换言之，入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。违反安全策略的行为有：入侵—非法用户的违规行为；滥用—合法用户的违规行为。

一个理想的入侵检测系统应具备以下特征：

- 在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击；
- 在入侵攻击过程中，能减少入侵攻击所造成的损失；
- 在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加入知识库内，以增强系统的防范能力。
- 在被入侵攻击发生前后，收集入侵攻击的相关信息，作为安全审计数据和法庭证据。

安氏公司的网络入侵检测系统－**LinkTrust™ IDS** 采用了新一代的入侵检测技术，包括基于状态的协议分析技术、开放灵活的行为描述代码、安全的嵌入式操作系统、先进的体系架构、丰富完善的各种功能，配合高性能专用硬件设备，是最先进的网络实时入侵检测系统。它以不引人注目的方式最大限度地、全天候地监控和分析企业网络的安全问题。捕获安全事件，给予适当的响应，阻止非法的入侵行为，保护企业的信息资产。

2 网络入侵检测技术

2.1 概述

基于网络的入侵检测系统传感器（NIDS）放置在需要保护的网段内，不间断地实时监控网络上各种数据包，对每个数据包或连接进行分析以发现异常行为或攻击企图并给予适当的及时响应。网络入侵检测技术、有时也称入侵发现技术，主要有三种：

- 模式匹配
- 异常检测
- 协议分析

模式匹配技术

模式匹配发现技术也称攻击特征检测技术，假定所有入侵行为和手段（及其变种）都能够表达为一种模式或特征，那么所有已知的入侵方法都可以用匹配的方法发现。模式发现的关键是如何表达入侵的模式，把真正的入侵与正常行为区分开来。模式发现的优点是对已知攻击的报警比较准确，局限是它只能发现已知的攻击，对未知的攻击无能为力，而且误报率

比较高。

异常检测技术

异常检测技术假定所有入侵行为都是与正常行为不同的。如果建立系统正常行为的轨迹，那么理论上可以把所有与正常轨迹不同的系统状态视为可疑企图。对于异常阀值与特征的选择是异常发现技术的关键。比如，通过流量统计分析将异常时间的异常网络流量视为可疑。异常发现技术的局限是并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。

协议分析技术

协议分析是目前最先进的检测技术，通过对数据包进行结构化协议分析来识别入侵企图和行为。协议分析是根据构造好的算法实现的，这种技术比模式匹配检测效率更高，并能对一些未知的攻击特征进行识别，具有一定的免疫功能。

监听

网络入侵检测数据收集和处理部件通常是一台专用主机，称为网络传感器。因为性能和安全的需求，现在的网络传感器多采用专用的设备实现（Appliance），它的一块网卡连接在被检测的网段上负责收集网络数据包，另一块网卡用于管理，其它模块负责分析和处理数据包。目前最先进的网络传感器技术通过编写高效的驱动程序、结合协议分析技术，已经达到100M 网络线速，甚至千兆网络上进行监听而不丢包的性能。

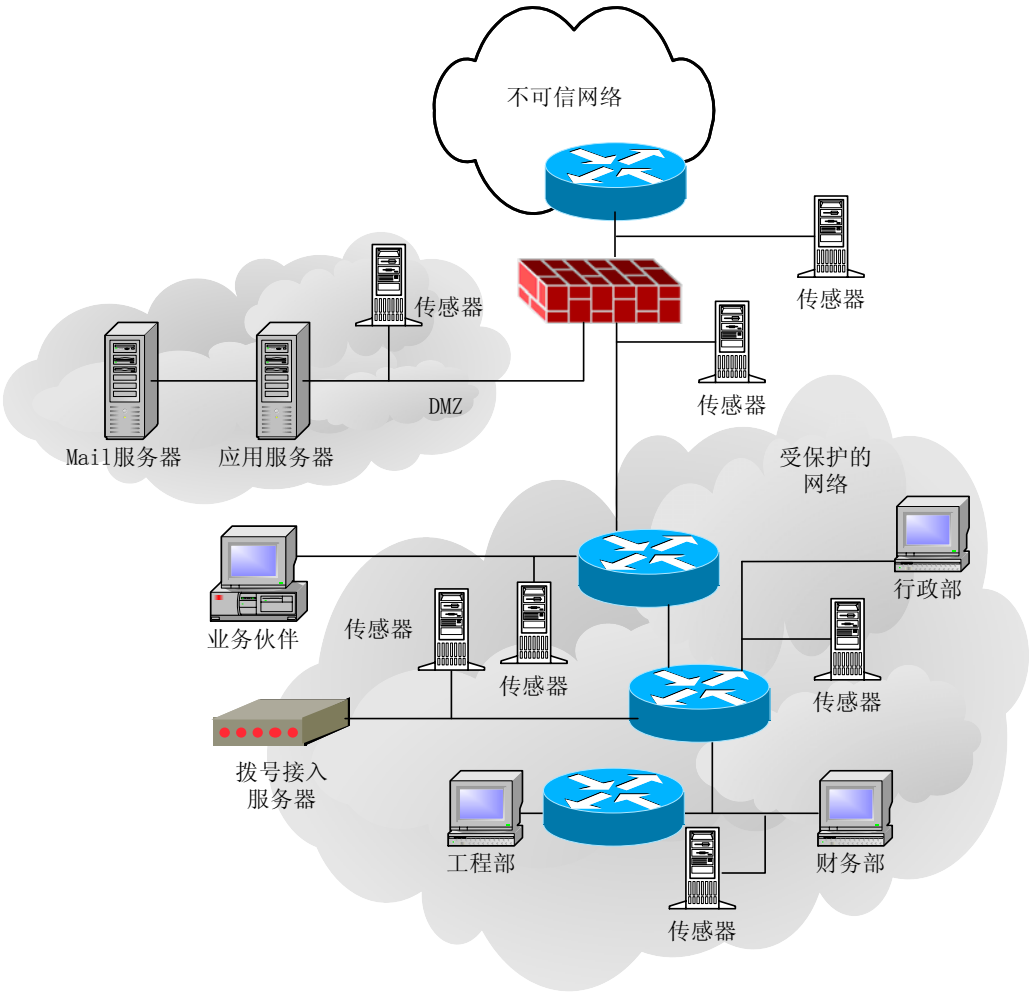
部署方式

在共享式网络中部署非常简单，监听网卡连接到需检测的网段中即可，网卡收集网络中的所有数据包进行分析和处理，其优点是不影响网络结构和正常通信。

在交换式网络中情况比较复杂，通常有三种收集数据的方式。一种方式是网络接口卡与交互设备的监控端口连接，通过交换设备的 Span/Mirror 功能将流向各端口的数据包复制一份给监控端口，入侵检测传感器从监控端口获取数据包进行分析和处理。第二种方式是在网络中增加一台集线器改变网络拓扑结构，通过集线器（共享式监听方式）获取数据包。例如，如果一个交换机端口连接到一个连接在 Internet 的路由器上，就可以在路由器和交换机之间

插入一个小集线器。第三种方式是入侵检测传感器通过一种 TAP（分路器）设备对交换式网络中的数据包进行分析和处理。

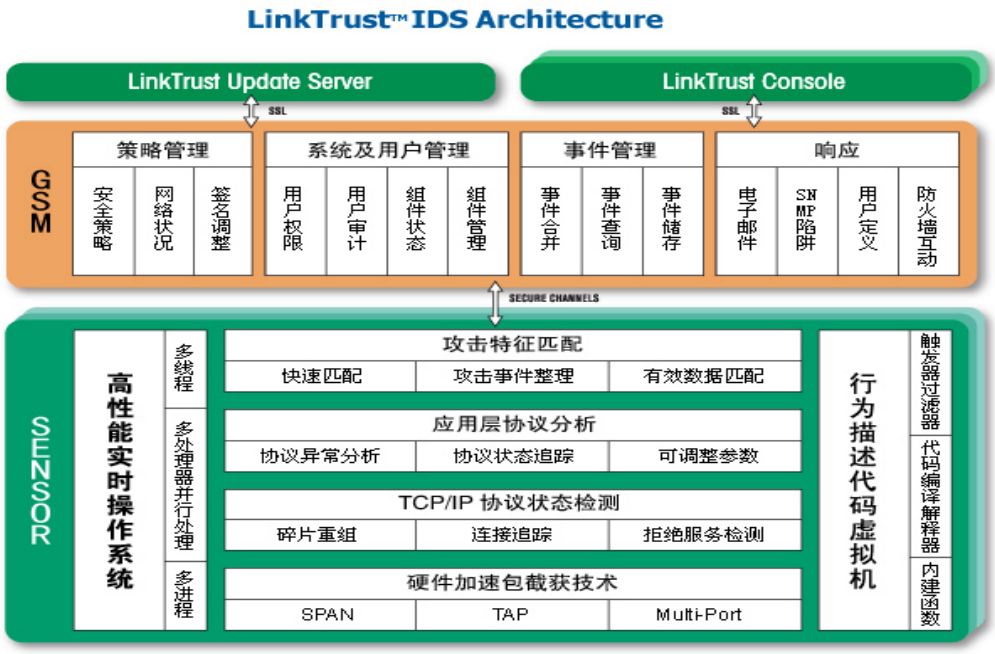
传感器可以被放置在企业网络中的任何可能存在安全隐患的网段。在这些网段中，根据网络流量和监控数据的需要来决定部署不同型号的传感器。如下图所示：



2.2 LinkTrust™ IDS使用的入侵检测技术

LinkTrust™ IDS的核心检测技术是新一代的协议分析技术。该技术结合了硬件加速信息包捕捉技术、基于状态的应用层协议分析技术和开放的行为描述代码描述技术来探测攻击。这三大技术构成了**LinkTrust™ IDS**所有解决方案的基础，它显著地提高了入侵检测系统的性能，能够适应高速的千兆网络环境。

LinkTrust™ IDS采用了如下的先进入侵检测技术：



LinkTrust™ IDS所使用的新一代入侵检测技术为客户带来许多好处，包括：

- **显著地提高性能：**协议分析技术充分利用通信协议结构，与模式匹配系统使用简单匹配相比，可以更快更有效的处理数据包和连接。
- **提高准确度：**协议分析技术比一个非智能模式匹配的IDS系统有少得多的错误倾向和错误诊断。**LinkTrust IDS™**将命令解析（语法分析）技术与协议分析技术相结合，来模拟一个命令串的执行，从而在通信流到达操作系统或应用之前决定该通信流是否是恶意的。
- **基于状态的分析：**当协议分析引擎评估一个信息包时，它考虑信息包是否处在一个已经建立的连接上，同时综合判断各个包前后关系，前面有什么、下一步可能发生什么，而模式匹配系统只能独立的看待每一个信息包。
- **灵活高效的行为描述代码：**允许用户根据自己的需要自创建几乎任意的新的特征签名，配置为最适合自己的入侵检测系统。
- **反躲避：**由于协议分析引擎能够判断一个通信会话实际内容及含义，它们不太容易受到黑客IDS躲避技术的影响，这些技术包括被动的目标系统指纹识别技术、目标应

用程序指纹识别技术，URL编码和IP碎片等。

- **资源消耗：**协议分析技术的高效性使网络传感器系统资源消耗大幅度降低，相反地，模式匹配技术则是非常消耗系统资源的。

2.3 LinkTrust™ IDS产品特点

LinkTrust™ IDS 采用基于状态的协议分析技术，结合模式匹配、异常统计来检测网络误用行为和异常活动。它采用专门定制的硬件平台，能够在高负载的千兆网络上提供高水平的性能；同时使用专用的操作系统，配合刻录在 CD－ROM 上的传感器程序进行引导，从而提供了最大可能的自身安全。

LinkTrust™ IDS 主要有以下特点：

- **领先的入侵检测技术**

LinkTrust™ IDS 以智能的状态协议分析技术为主，结合模式匹配技术。状态协议分析技术基于对已知协议结构的了解，通过分析数据包的结构和连接状态，检测可疑连接和事件，极大地提高了检测效率和准确性。不仅能准确识别所有的已知攻击，还可以识别未知攻击，并使采用 IDS 躲避技术的攻击手段彻底失效。

- **高性能**

LinkTrust™ IDS 采用高效的入侵检测引擎，综合使用虚机解释器、多进程、多线程技术，配合专门设计的高性能的硬件专用平台，能处理高达两千兆的网络流量。

- **行为描述代码**

用户可以非常方便地使用安氏提供的“行为描述代码”自创建新的特征签名，扩展攻击签名库,扩大检测范围，个性化入侵检测系统。

- **重组**

LinkTrust™ IDS 不仅能对 IP 分片进行重组分析而且能够进行 TCP 数据流的重组，从而提高产品的检测准确度。

- **分布式结构**

LinkTrust™ IDS 采用先进的多层分布式体系结构，包括控制台、事件收集器、传感器，这种结构能够更好地保证整个系统的可扩展性和可靠性，也带来了更多灵活性和更可伸缩性，适应各种规模的企业网络的安全和管理需要。

■ **全面检测**

LinkTrust™ IDS 检测准确率高，能识别一千多种攻击特征，如：预攻击探测,拒绝服务攻击,，针对各种服务漏洞的攻击，针对 Windows 和 Unix 网络的攻击，网络连接事件等。强大的“行为描述代码”可支持任意自定义安全事件。同时安氏公司也不断为用户提供扩充攻击特征库，用户可通过安氏网站随时更新。

■ **高可靠性**

LinkTrust™ IDS 是软件与硬件紧密结合的一体化专用硬件设备，安氏公司专门设计了安全、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；操作系统经过优化和安全处理，保证系统的安全性和抗毁性。

■ **高安全性**

LinkTrust™ IDS 运行在经优化和加固的嵌入式操作系统上，操作系统上不需要的服务、进程和驱动等都被裁减以保证安全和性能，软件和系统存放在 CD-ROM 上防止篡改。系统内各组件通过加密的安全通道进行通讯防止窃听。

■ **高可用性**

LinkTrust™ IDS 的所有组件都支持 HA 冗余配置，保证不漏掉任何的攻击。

■ **低误报率**

LinkTrust™ IDS 采用状态协议分析技术，同时允许用户灵活地调节签名的参数和创建新的签名，大大降低了误报率，提高了检测的准确性。

■ **隐秘部署**

LinkTrust™ IDS 支持安全的部署模式—隐秘配置。系统安装两块网卡，其中一块网卡不配置 IP 地址用于监听，攻击者察觉不到它的存在；另一块通过安全网络与控制台连接。

■ **灵活响应**

LinkTrust™ IDS 提供了丰富的响应方式，如：向控制台发出警告，发提示性的电子邮件，向网络管理平台发出 SNMP 消息，自动终止攻击，重新配置防火墙，执行一个用户自定义响应程序等。

■ **简单易用**

LinkTrust™ IDS 安装简单，升级方便，查询灵活，并能生成适合各级管理任意需要的

多种格式的报告。

3 产品简介

3.1 体系结构

LinkTrust™ IDS 是三层分布式结构，由控制台（console）、事件收集器（EC）、传感器（sensor）组成。有以下两种部署方式：

- **简单部署**

控制台和事件收集器同时安装在一台机器上，而传感器单独安装。

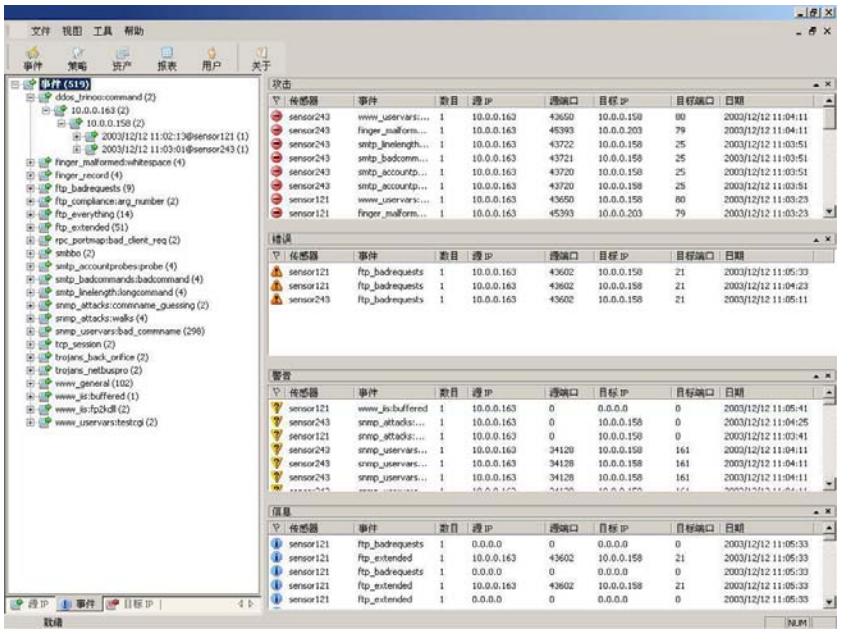
- **分布式部署**

由控制台、事件收集器、传感器组成，分别安装的不同的机器上，其中事件收集器是分布式部署的关键。

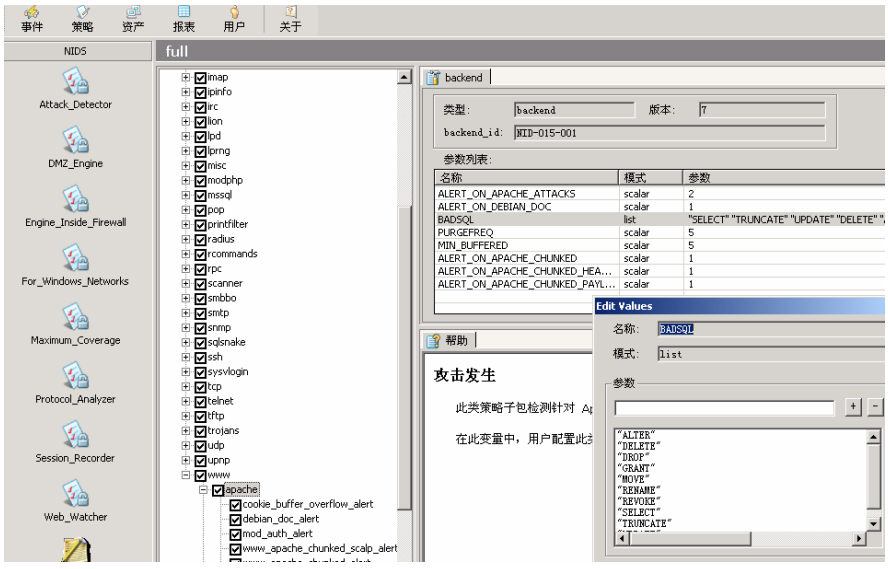
3.2 控制台

控制台是一个基于 Windows 的应用程序，控制台提供图形界面来进行数据查询、查看警报并配置传感器。一个控制台可以管理多个传感器。控制台有很好的访问控制机制，不同的管理员被授予不同级别的访问权限，允许或禁止查询、警报及配置等访问。控制台、事件收集器和传感器之间的所有通信都进行了安全加密。

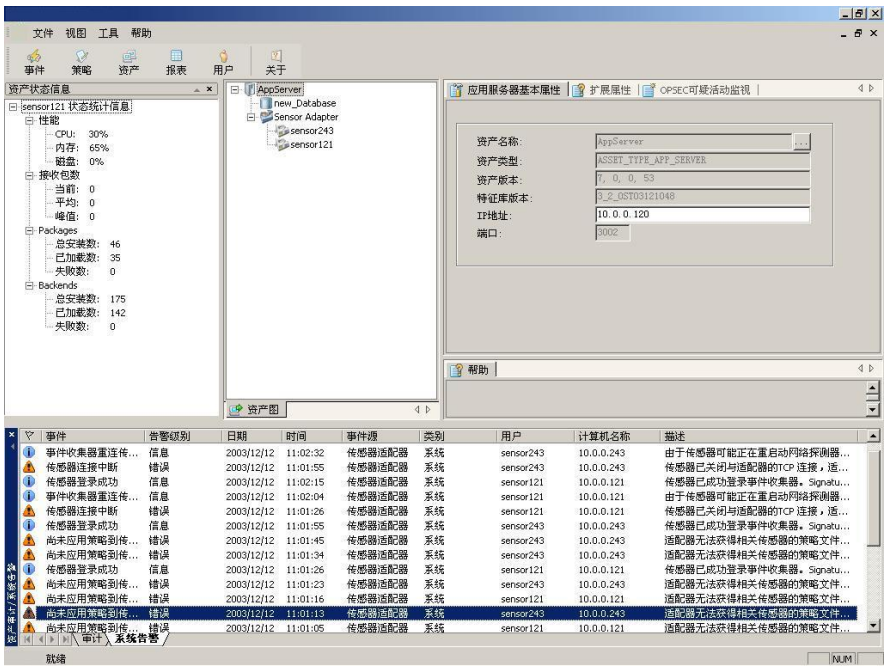
1. 强大事件分析和显示窗口



2. 灵活的策略配置和参数调整



3. 直观的资产控制



3.3 事件收集器

一个大型分布式应用中，用户希望能够通过单个控制台完全管理多个传感器，允许从一个中央点分发安全策略，或者把多个传感器上的数据合并到一个报告中去。用户可以通过安装一个事件收集器来实现集中管理，事件收集器实际上负责管理传感器及其数据。

远程传感器可以有同样配置，如同样的策略和警报。每个传感器也可以被独立进行配置，从而在需要的时候激活不同的策略。例如，既可以在所有传感器上邮件策略包内激活“邮件信息名单”策略，也可以只在部分传感器上激活该策略。

传感器上一些配置是独有的，例如用于监控的网络接口、系统级变量、以及访问控制信息。例如，如果每个传感器都在监控一个不同的网络，每个传感器的配置在事件收集器上设定。

在一个多层应用中，通常用管理员界面来访问策略，但其实是由事件收集器来进行实际管理的，并从传感器上收集数据集中处理。不同组件之间的所有通信都进行了安全加密。

3.4 传感器

传感器的基本功能是捕获网络数据包，并利用策略及签名对数据进一步分析和判断，当发现可疑的事件时触发传感器发送警报。

操作系统和 IDS 程序存储在可引导的 CD－ROM 中来确保它抗篡改，传感器设备包含一个大硬盘作为事件数据的存储空间，如存储所有的证据数据和警报。

管理员可使用控制台来查询数据，生成报告，或查看传感器的状态。传感器上另外有一些后台程序负责管理数据和系统。例如，空间管理程序管理磁盘空间，而访问控制程序管理对数据、警报和配置进行的访问。

3.4.1 分析器

分析器结合了应用层协议分析和基于签名的分析，数据流和单个数据包都被检查，破碎的数据包被重组，并对会话进行记录以便进行进一步检查。这保证了能够有效探测出分散到多个包中的攻击。

正如 IDS 工业增长的趋势一样，**LinkTrust™ IDS** 签名并不仅仅依赖于简单的模式匹配——它们同时还维护许多基于网络协议的协议状态。这种方式极大的降低了误报率，减少了受迷惑技术攻击威胁的机会，并提供了异常检测的要素。

例如，在很多情况下，基于事先未知漏洞的攻击可以被异常检测技术成功发现。基于状态的结构还可以通过配置，使其只对产生重要威胁的事件发出警报（例如，一个 IIS 攻击发向一台 Apache 服务器时，便不需产生警报），从而提高了正确性和性能。

可以提供多种签名，并由安氏的快速响应团队对其不断进行充实。新的签名将会被尽快放置到安氏的安全站点上，客户可以通过邮件来了解攻击的细节以及相关信息。一个安全的下载程序允许管理员通过事件收集器快速获得签名，并向网络中所有的传感器分发新的签名。如果没有安装事件收集器，新的签名必须从控制台分别发送到每个传感器上。

注意：由于安全事件是使用行为描述代码来定义的，用户和管理员可以在需要时修改内置的“签名”或创建新的签名。这使得 **LinkTrust™ IDS** 成为市场上最具扩展性的入侵检测系统。

3.4.2 策略

攻击签名被存储在称为策略的逻辑组中。例如，传感器中的“拒绝服务探测策略”包含多个签名策略，来观察拒绝网络服务的不同方法。签名还可以共享行为描述代码，这样在多个签名需要处理同种数据时，便可帮助消除冗余处理过程。每个策略都包括几个不同的部件：签名、共享行为描述代码和配置文件

3.4.3 行为描述代码

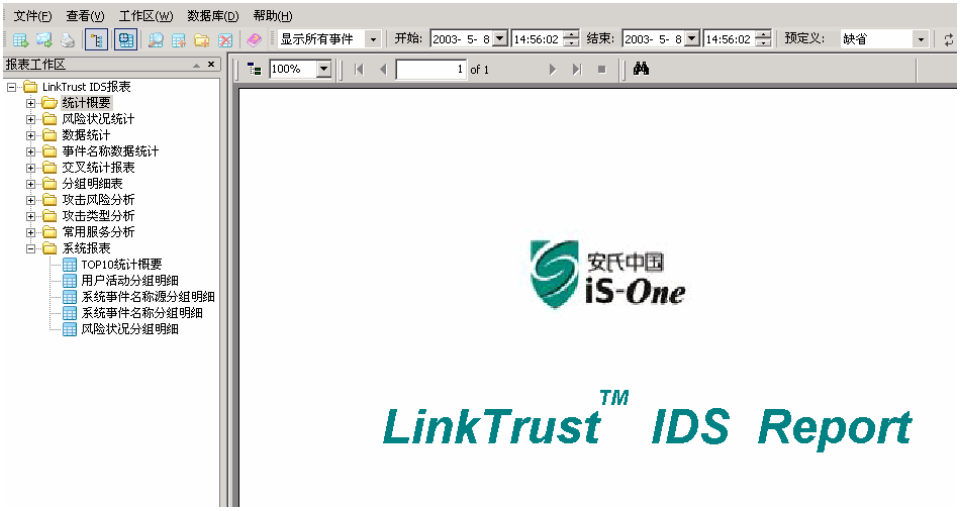
LinkTrust™ IDS 使用一种独特、高效的“行为描述代码”创建签名，“行为描述代码”触发传感器开始收集事件的数据。例如，如果一个数据包有一个 UDP 包头，UDP 策略的行为描述代码便开始收集数据。行为描述代码同时还告诉传感器该如何处理数据，行为描述代码中提供的功能告诉传感器记录什么类型的数据，并将该数据传递到记录器上。例如，Pingflood 策略告诉传感器来追踪源和目的 IP 地址、所发送的包数，及最后一个包之后总共的时间。所有的这些信息都发送到记录器上去。

行为描述代码的其他功能告诉传感器什么数据可作为警报发送。例如，Pingflood 策略包含行为描述代码，并告诉传感器引擎：在某时间，如果向某特定 IP 地址发送了超过一定量的 ping 包，便需向管理员发送警报。

3.5 报告

LinkTrust™ IDS 记录的除了基本的警报信息，还包括连接细节、URL 请求、FTP 请求、邮件信息等等。这允许管理员：

- 查看单个事件或寻找统计趋势
- 检查某些可能是误用网络服务的主机上的信息流
- 通过搜索信息流类型的变化，来搜索导致网络瓶颈的可能原因
- 检查单个连接的细节



使用 **LinkTrust™ IDS** 管理员界面，可根据某个签名搜集的任何数据对查询进行过滤，如数据类型、IP 地址、端口和时间。可保存查询详述以便再次使用。

查询提供对传感器系统所搜集数据进行实时查看——一旦信息写入传感器的磁盘上，便可供查询。控制台为查询结果提供几种不同类型的格式，从基于文本的列表到条形图和饼图。

同时能够提供所报告的漏洞的细节，包括该如何进行调整的信息。

3.6 产品型号

LinkTrust™ IDS *ND-100SE* 可以监测高达 90 Mbps 的流量，并且适用于中小企业的网络环境。在 10/100M 网络接口的支持下，同时支持监控 50 万个连接。

LinkTrust™ IDS *ND -100HP* 可以监测高达 100 Mbps 的速度，配置在多种网络环境中提供保护，在业务繁忙的 100M 网络环境，同时支持监控 80 万个连接。

LinkTrust™ IDS *ND -200* 可以监测高达 200 Mbps 的速度，配置在多种网络环境中提供保护，提供 2 个 100M 监听端口，可以同时监控 DMZ 和公司内部的网络。同时支持监控 100 万个连接。

LinkTrust™ IDS *ND -Giga* 通过提供定制的 ASIC 硬件加速器，提供高达的 1Gbps 速度的杰出性能，传感器提供一个 1000M 的监控端口，具有保护线速的千兆子网的能力。同时支持监控 120 万个连接。

LinkTrust™ IDS *ND -GigaHA* 通过提供定制的 ASIC 硬件加速器，提供高达 2Gbps 速度的杰出性能，传感器提供两个 1000M 的监控端口，具有保护线速的千兆连接和多个局部应用的千兆子网。并且能实现两个监控网卡之间实时切换。

4 硬件规格

4.1 ND-100 SE

- 1 C4 processor
- 1 Gbytes RAM.
- 1 x 80 GB HD
- 2 x 10/100 Ethernet NICs
- Up to 100Mbps

4.2 ND-100 HP

- 1 Pentium IV processor
- 1.5 Gbytes RAM.
- 1 x 80 GB HD
- 2 x 10/100 Ethernet NICs
- Up to 100Mbps

4.3 ND-200

- 2 Pentium III Tulatin processors
- 2 Gbytes RAM.
- 1 x 80 GB HD
- 3 10/100 Ethernet NICs （monitor two network segment）
- Up to 200Mbps

4.4 ND-Giga

- 2 Pentium III Tulatin processors
- 3 Gbytes RAM
- 1 x 80 GB HD
- 2 10/100 Ethernet NICs
- Single Gigabit Ethernet NIC (multimode fiber)
- Up to 1000Mbps

4.5 ND-Giga-HA

- 2 Pentium III Tulatin processors
- 4 Gbytes RAM
- 1 x 80 GB HD
- 2 10/100 Ethernet NICs
- Dual Gigabit Ethernet NIC (multimode fiber)
- Up to 2000Mbps

5 技术支持

安氏中国为 **LinkTrust™ IDS** 提供专业的、完善的售前、售后技术支持服务。

安氏中国作为专业的网络安全公司，提供出色的入侵检测产品，并致力于成为广大用户的安全合作伙伴和顾问。安氏中国通过提供完善的、多元化的技术服务，竭诚为广大用户服务，满足用户不同程度的需要，最大限度地保障用户的信息安全。

任何购买安氏中国网络安全产品的用户，都能够享受安氏中国全面周到的产品技术服务。

为了保证购买安氏中国安全产品的用户能够更好地使用安氏中国产品，建议用户配套采用安氏中国提供产品技术服务。

5.1 安氏中国的承诺

- 产品到货期承诺 —— 保证在合同交货日期内，安氏中国产品到货
- 公安部销售许可证承诺 —— 保证产品拥有中华人民共和国公安部颁发的销售许可证
- Y2K 承诺 —— 安氏中国保证自己的产品不存在计算机两千年问题
- 正版承诺 —— 保证向用户提供正版的安氏中国产品
- 中文手册承诺 —— 安氏中国将为用户提供完全中文的产品手册和其它文档

5.1.1 技术支持服务承诺

- 请求渠道畅通承诺 —— 安氏中国承诺用户可以通过热线电话、热线手机、电子邮件、传真等方式，将用户的技术支持服务要求有效地传达到安氏中国的客户服务中心和技术支持中心
- 现场服务响应时间承诺 —— 如果用户所在城市有安氏中国的分公司或者办事机构，安氏中国工程师将立即出发赶赴用户现场；如果用户所在城市没有安氏中国的分公司或者办公机构，安氏中国工程师将在有飞机、火车、汽车等交通条件下，选择实际可能的最快方式到达用户现场
- 问题解决承诺 —— 安氏中国技术支持工程师将及时、准确地回答用户提出的问题。对于一般技术问题，做到当时解决；对于无法立即答复的问题，做到 4 个工

作日内给予响应；对于无法解答的问题，安氏中国工程师将对用户提出的问题备案，在寻求到解决方案后通知用户

- 技术支持体系承诺 —— 安氏中国技术支持拥有有效的支撑体系，面对用户的技术支持人员背后有多种层次的支持，包括当地的技术支持中心以及设在北京的总技术支持中心
- 安氏中国将为用户提供一年时间的免费硬件维修服务

5.1.2 产品升级服务承诺

- 及时升级承诺 —— 安氏中国承诺在产品的升级版本发布的 3 天内，向用户发出产品升级通知。如果没有收到用户的确认信息，安氏中国将每周试图联络 1 次，直到用户收到升级通知并给予确认。如果联系到用户，对于需要递送介质的用户，升级的产品介质将在联系到的 1 周内寄出或送出。
- 最新安全消息承诺 —— 安氏中国将把用户主要联系人员的邮件地址添加到用户升级邮件列表中，定期向用户发布产品最新动态、产品升级内容、最新安全信息、最新黑客攻击手法警告等，最大限度地保证用户的网络安全，使用户紧跟安全技术的发展。

其他信息：

如果您想了解更多关于**LinkTrust™ IDS**入侵保护系统的信息请连接安氏公司的网站：

http://www.is-one.net

6 附录：联系方式

北京公司总部

北京东长安街 1 号东方广场办公楼 W3 座 1208 室　　邮编：100738

电话：010-85181101　　传真：010-85184777

安氏实验室

北京市海淀区三里河路 15 号中建大厦 A 座 8 层　　邮编：100037

电话：010-88083566　　传真：010-88083172

广州分公司

地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室　　邮编：510630

总机：020-38731555、38732069、38730525 转 2013

手机：13600056899　　传真：020-38730144