天阗入侵检测与管理系统（V6.0）

系列化产品

网络入侵检测白皮书

（Intrusion Management System）

（适用型号：NS200/NS500/NS2200/NS2800）

启明星辰信息技术有限公司

2004.8

版权声明

启明星辰信息技术有限公司©2004 版权所有，保留一切权力。
未经启明星辰书面同意不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。本文档中的信息归启明星辰信息技术有限公司所有并受中国知识产权法和国际公约的保护。
“天阗”为启明星辰信息技术有限公司的注册商标，不得侵犯。

信息更新

本文档及其相关计算机软件程序（以下文中称为“文档”）仅用于为最终用户提供信息，并且随时可由启明星辰信息技术有限公司（下称“启明星辰”）更改或撤回。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778

免责条款

根据适用法律的许可范围，启明星辰按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，启明星辰都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使启明星辰明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。
本文档中所有引用产品的使用及本文档均受最终用户可适用的特许协议约束。

出版时间

本文档由启明星辰信息技术有限公司2004年8月制作出版。

目　录

第 1 章　前言 4
1.1 术语定义 4
1.2 入侵检测的地位 4
1.3 入侵技术和手段 5
第 2 章　天阗入侵检测技术 8
2.1 高性能报文捕获 8
2.2 基于状态的全面协议分析 9
2.3 树型规则和匹配算法 10
2.4 准确的特征分析和规范描述 11
第 3 章　产品介绍 12
3.1 关于天阗 12
3.2 产品组成 12
3.3 产品结构 13
3.4 产品型号 14
第 4 章　产品特性 15
4.1 完善的管理控制体系 15
4.2 全面的入侵检测能力 15
4.3 细致的检测策略配置 16
4.4 可扩展的事件响应和安全产品联动 17
4.5 多样的日志综合分析和报告输出 17
4.6 高度的自主安全保障 18
4.7 美观的界面设计和人性化功能操作 18
5.8 稳定的成熟产品应用 18
4.9 性能指标 19
第 5 章　服务支持 22

启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

第1章 前言

1.1 术语定义

入侵是对信息系统的非授权访问及（或）未经许可在信息系统中进行操作,威胁计算机或网络的安全机制（包括机密性、完整性、可用性）的行为。入侵可能是来自互联网的攻击者对系统的非法访问，也可能是系统的授权用户对未授权的内容进行非法访问。

入侵检测就是对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程。

入侵检测系统（英文简称 IDS：Intrusion Detection System）是从多种计算机系统及网络中收集信息，再通过这些信息分析入侵特征的网络安全系统。

1.2 入侵检测的地位

网络安全是一个动态的概念。网络的动态安全模型能够提供给用户更完整、更合理的安全机制，全网动态安全体系可由下面的公式概括：

网络安全(S) = 风险分析(A)+ 制定策略(P) + 系统防护(P) + 实时监测(D) + 实时响应(R) + 灾难恢复(R)

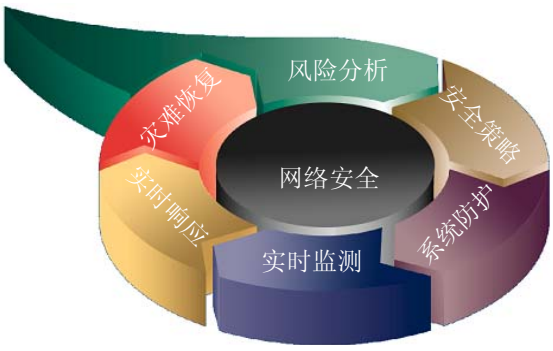


图 1-1：APPDRR 动态安全模型

即：网络安全是一个“APPDRR”的动态安全模型。然而，在这个安全模型中，并非各个部分的重要程度都是等同的。在安全策略的指导下，进行必要的系统防护有积极的意义，但是，无论网络防护得多么牢固，依旧不能说“网络是安全的”。因为随着技术的发展，任何防护措施都不能保证网络不出现新的安全事件，不被手段高超的人员成功入侵。在攻击与防

御的较量中，实时监测（D）是处在一个核心的地位。在实时监测中，入侵检测系统是目前最为主要的一个广泛应用的技术和管理手段。

相比较而言，入侵检测系统是动态安全模型中唯一一个全天候运行的系统。利用入侵检测系统可以了解网络的运行状况和发生的安全事件，并根据安全事件来调整安全策略和防护手段，同时改进实时响应和事后恢复的有效性，为定期的安全评估和分析提供依据，从而提高网络安全的整体水平。

因此，结合安全模型中的各个环节，入侵检测的作用概括起来就是如下四点：

- 从不知到有知
- 从被动到主动
- 从事后到事前
- 从预警到保障

1.3 入侵技术和手段

入侵技术和手段是不断发展的。从攻击者的角度说，入侵所需要的技术是复杂的，而应用的手段往往又表现得非常简单，如下图 1-1 所示。这种特点导致攻击现象越来越普遍，对网络和计算机的威胁也越来越突出。

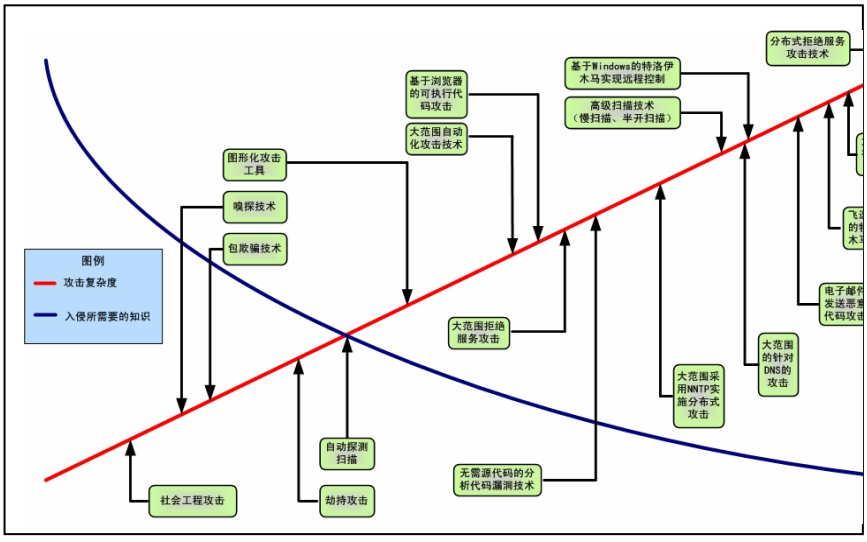


图 1-2 入侵技术和手段的关系图

启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

入侵过程一般可以概括为五个步骤或阶段，我们可以就入侵过程的五个阶段来分析其应用的技术和手段。需要注意的是，作为具体的攻击，不一定完全按此五个阶段进行。

■ **信息探测**

信息探测一般是入侵过程的开始，攻击者开始对网络内部或外部进行有意或无意的可攻击目标的搜寻，主要应用的技术包括：目标路由信息探测、目标主机操作系统探测、端口探测、帐户信息搜查、应用服务和应用软件信息探测以及目标系统已采取的防御措施查找等等。目前，攻击者采用的手段主要是扫描工具，如操作系统指纹鉴定工具、端口扫描工具等等。

■ **攻击尝试**

攻击者在进行信息探测后，获取了其需要的相关信息，也就确定了在其知识范畴内比较容易实现的攻击目标尝试对象，然后开始对目标主机的技术或管理漏洞进行深入分析和验证，这就意味着攻击尝试的进行。目前，攻击者常用的手段主要是漏洞校验和口令猜解，如：专用的 CGI 漏洞扫描工具、登录口令破解等等。

■ **权限提升**

攻击者在进行攻击尝试以后，如果成功也就意味着攻击者从原先没有权限的系统获取了一个访问权限，但这个权限可能是受限制的，于是攻击者就会采取各种措施，使得当前的权限得到提升，最理想的就是获得最高权限（如 Admin 或者 Root 权限），这样攻击者才能进行深入攻击。这个过程就是权限提升。目前，攻击者常用的手段主要是通过缓冲区溢出的攻击方式。

■ **深入攻击**

攻击者通过权限提升后，一般是控制了单台主机，从而独立的入侵过程基本完成。但是，攻击者也会考虑如何将留下的入侵痕迹消除，同时开辟一条新的路径便于日后再次进行更深入地攻击，因此，作为深入攻击的主要技术手段就有日志更改或替换、木马植入以及进行跳板攻击等等。木马的种类更是多种多样，近年来，木马程序结合病毒的自动传播来进行入侵植入更是屡见不鲜。

■ **拒绝服务**

如果目标主机的防范措施比较好，前面的攻击过程可能不起效果。作为部分恶意的攻击者还会采用拒绝服务的攻击方式，模拟正常的业务请求来阻塞目标主机对外提供服务的网络

带宽或消耗目标主机的系统资源，使正常的服务变得非常困难，严重的甚至导致目标主机宕机，从而达到攻击的效果。目前，拒绝服务工具成为非常流行的攻击手段，甚至结合木马程序发展成为分布式拒绝服务攻击，其攻击威力更大。

第2章 天阗入侵检测技术

2.1 高性能报文捕获

■ DMA 和零拷贝技术

IDS 作为保障信息安全的重要环节，一直发挥着重要作用。目前，由于网络自身的发展非常迅速，一般的网络局域网主干交换带宽速度由 10/100M 的网络发展到 1000M，给 IDS 带来了巨大的挑战。由于传统的入侵检测系统一般基于简单的模式匹配实现，在百兆满负荷的网络环境中工作已经相当吃力，而网络带宽成 10 倍的增加，如果不考虑其它条件，意味着要求 IDS 增加 10 倍的处理能力，因此网络的发展，提出了千兆或更高性能 IDS 的需求。而高性能入侵检测的一个重要瓶颈就在于高速的报文捕获和批量处理分析。

为了提高报文捕获的效率，通过修改网卡驱动程序，使用 DMA 和数据零拷贝技术零拷贝技术，大大提高了效率，如下图所示：

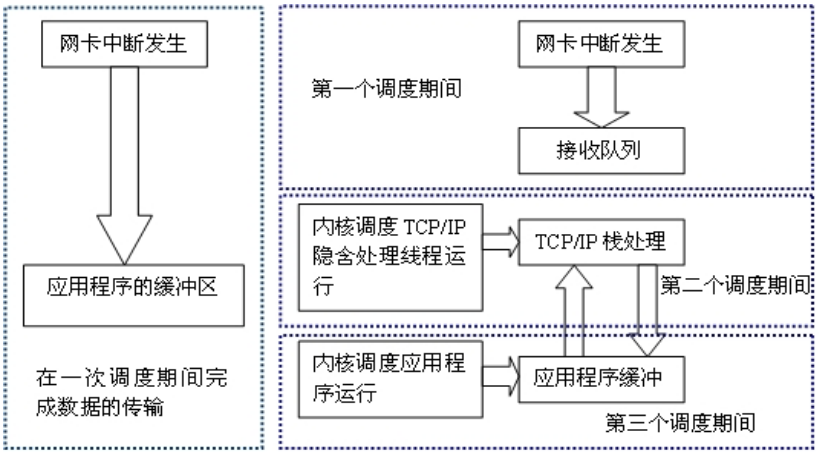


图 1：DMA 和数据零拷贝技术和传统入侵检测报文捕获技术的比较

零拷贝技术省略了 TCP/IP 堆栈的处理，直接将网卡通过 DMA 直接数据传输将报文数据传递到了 IDS 系统可以访问的空间，大大减少了传统方式中因为上下文切换和数据拷贝而带来的系统开销，使用了零拷贝技术之后，系统的捕包效率大大提高，测试结果是在能够在 1.4G 的 CPU 下，捕获 100 万/秒报文时，CPU 占用率还低于 10%。这种效率完全可以满足在千兆高速环境下入侵检测分析。

■ **支撑平台结构和系统优化**

对于整体结构的优化有助于进一步提高 IDS 系统引擎的速度。

- 并行处理

在双 CPU 并行处理机上，通过使用多线程，使得我们可以将多个报文同时进行处理，为了减少同步带来的代价，使用报文的预分析，然后根据预分析的结果进行任务分配，将一个报文的所有分析和匹配工作都交给一个工作线程去处理，多个线程可以同时并行处理多个报文。

- 使用汇编语言实现关键处理

通过使用汇编语言可以大大减少使用高级语言带来的冗余代码，在核心的关键处理上如模式集合的匹配上使用汇编语言实现能够大大提高效率。

- 优化内存分配算法

经过分析在 IDS 系统中，会大量的使用内存的分配和释放操作，如果，实现中都通过系统的分配释放函数来实现会大大影响系统的处理速度。通过使用简化而且合理的内存分配算法，能够使这部分的代价减少。

- 精简运行的操作系统

通过精简运行的操作系统，使用优化程序技术也是提高入侵检测的性能的必要条件，同时保证了入侵检测产品的自身安全性。

2.2 基于状态的全面协议分析

协议分析模块完成 IDS 系统引擎中主要的分析工作，对于一个报文在引擎的处理过程中，报文：分析：匹配＝1：1：N，这就是说一个报文需要经过一次分析，再和 N 条规则进行匹配之后产生事件。如果能够通过更准确的分析，减少匹配的工作，就能够最终提高整个 IDS 系统的处理效率。因此协议分析的准确性和效率对于整个系统的处理效率影响非常大。这部分包括两个大的方面：

■ 提高协议分析的速度

1．基于状态的协议分析

网络中通讯的报文一般都不是孤立的，而是在一系列的报文通讯之中的，也就是说

是有一定的报文前后上下文的。通过基于状态的协议分析，能够大大提高解析的准确度，同时对于不同报文采用不同的少量分析的方式，从而也提高了协议分析的速度。

2．运用多种算法进行解析

在报文的分析过程，采用多种算法来提高协议解析的速度，比如使用高速树型匹配算法、HASH 算法等等。

■ 提高协议分析的效果

采用两种方法提高协议解析的效果：直接产生协议分析中确定的事件和更深入的协议分析。

1．直接产生协议分析中确定的事件

通过在协议分析模块中直接产生事件，从而减少在匹配规则模块中规则集的规模，如：RFC 协议确定的事件和异常事件：如 FLOOD 攻击，从而提高整个报文的处理速度。

2．更深入的协议分析

更深入的协议解析提高了规则集中规则的匹配准确性，比如缩小一次字符串匹配在报文中搜索范围，从而节省时间，提高规则匹配的效率。

2.3 树型规则和匹配算法

前面已经提到，报文：分析：匹配＝1：1：N 的关系。一个报文需要跟多条规则进行比较，这需要大量的运算，占用许多的 CPU 时间。通过三个方法去提高其效率：协议规则子集、规则树和快速模式集合匹配。

1. 协议规则子集

协议规则子集是通过将规则集合中的规则按照其所属的协议分成许多小的子集，而一个报文只与其相关的协议规则子集中的规则进行匹配，从而大大减少实际一个报文进行匹配的规则数量，减少匹配时间。

2. 规则树

将线性规则匹配方式改造成为树型规则匹配方式，就必须构造规则树。通过规则树，我们可以很容易在匹配过程中淘汰掉不可能的规则，减少重复判断的次数，并实现将一个协议变量的多个取值放到一起（形成取值集合）进行判断，大大的提高了比较效率。

3. 快速模式集合匹配

由于在一个报文的匹配中，最为耗时的匹配运算是在报文中匹配一个字符串模式，通过快速模式集合匹配算法来提高这部分匹配的效率。快速匹配意味着能够尽可能快的在一个正文串中查找到一个模式串的存在，这是通过提高匹配时移动模式的距离实现的；集合匹配意味着同时快速的对多个模式进行匹配。二者的结合就是在一个报文中快速的匹配多个模式。

2.4 准确的特征分析和规范描述

解决入侵检测的漏报和误报现象还依赖于准确的特征提取和描述，在天阗所应用的特征全面采用了如下两种特征分析方法和统一的规范化语言描述

- 基于漏洞机理的特征分析

利用漏洞机理的方法来提取和定义特征，可以实现检测和具体攻击工具的无关性，特别对于防止新型变种的攻击和攻击工具改造非常有效。

- 基于攻击过程的特征分析

攻击过程分析法则是完全站在攻击者的角度，破析完整的攻击过程，可以判断攻击是处在攻击尝试阶段还是已经攻击成功。

- VT++规范描述语言

天阗不论是那种分析方法，最后都是通过规范化的 VT++描述语言来进行统一定义。采用 VT++描述语言保证了特征的快速更新和供用户自主定义新的攻击特征以及用户关注的特殊行为，从而扩充检测内容和范围。

第3章 产品介绍

3.1 关于天阗

“天阗”入侵检测系列产品是启明星辰信息技术有限公司自行研制开发的入侵检测系统，是国内第一批在入侵检测方面获得国家公安部销售许可证的网络安全产品，同时天阗还通过了所有权威管理部门的测评和认证。

“天阗”入侵检测系列产品是一种动态的入侵检测与响应系统。它能够实时监控网络传输，自动检测可疑行为，及时发现来自网络外部或内部的攻击，并可以实时响应，切断攻击方的连接。天阗系统可以与防火墙紧密结合，弥补了防火墙的访问控制不严密的问题。其联机文档提供了丰富的事件说明及恢复措施，可以最大程度地为网络系统提供安全保障。

启明星辰坚信，不了解黑客技术的最新发展，就谈不上对黑客入侵的有效防范。为了了解黑客活动的前沿状况，把握黑客技术的动态发展，深化对黑客行为的本质分析，预防黑客的突然袭击并以最快速度判断黑客的最新攻击手段，启明星辰专门建立了积极防御实验室和CERT[1]小组，通过持续不断地研究、实践和积累，逐渐建立起一系列数据、信息和知识库作为公司产品、解决方案和专业服务的技术支撑，如黑客攻击特征库、系统漏洞库、系统补丁库和 IP 定位数据库等。启明星辰在入侵检测技术领域的成就受到了国家权威部门的肯定和认可，并成为 CNCERT[2]和 CNCVE[3]的承建单位，体现了启明星辰时刻与国际先进技术保持接轨的不凡实力。这些卓有成效的研究工作正是“天阗”入侵检测系统能够始终保持领先地位的最有力保障！

天阗系统强大的功能、简单的操作、友好的用户界面、全面的技术支持解除了您的后顾之忧，是您值得信赖的网络安全产品

3.2 产品组成

“天阗”网络型入侵检测系统（以下简称天阗 NIDS）独创性的将检测、管理配置、报

[1] CERT：Computer Emergency Response Team
[2] CNCERT：China National Computer Emergency Response Team，参考网址：www.cncert.org.cn
[3] CVE：Common Vulnerability Exposure，参考网址：www.cve.mitre.org

警显示以及日志分析四部分的功能可以实现分开部署，满足多人同时监测和分权限管理。

网络探测引擎：网络探测引擎采用专用硬件设备通过旁路方式接入检测网络。网络探测引擎全面侦听网上信息流，动态监视网络上流过的所有数据包，进行检测和实时分析，从而实时甚至提前发现非法或异常行为，并且执行告警、阻断等功能并记录相应的事件日志。

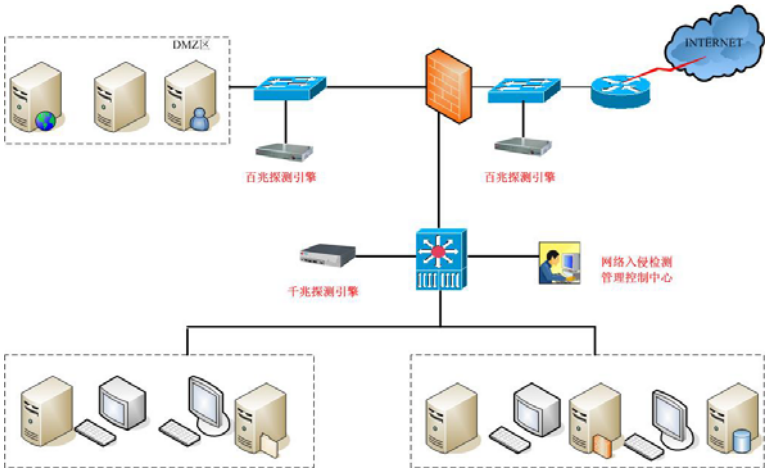
管理控制中心：控制中心面向用户，提供管理配置之用。控制中心是个高性能的管理系统，它能控制位于本地或远程的多个网络探测引擎的活动，集中制定和配置策略，提供统一的数据管理。管理控制中心可以被设置为主、子结构，主管理控制中心可以实时接收、转发子控制中心的告警信息，定时、分类提取子控制中心的日志信息，下发各种配置文件、策略供子控对其所属网络探测引擎进行配置。

综合信息显示：它能显示详细的入侵告警信息(如入侵者的 IP 地址、攻击特征)，对事件的响应提供在线帮助。

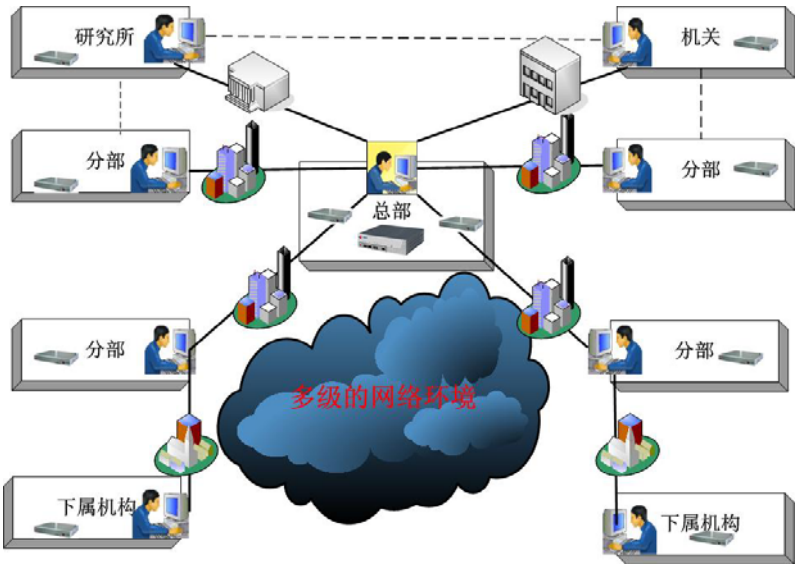
日志分析中心：将历史的报警信息进行分类提取，提供了多种分析手段和模版，可以产生用户所需要的独特的统计性和分析性的管理报表

3.3 产品结构

1、单级管理下的分布式检测部署



2、多级管理下的分布式检测部署



3.4 产品型号

产品型号	NS200	NS500	NS2200	NS2800
多级管理	无	支持	无	支持
网络环境	百兆	百兆	千兆	千兆
检测网路	一路	两路	一路	两路
检测能力	100Mbps	200Mbps	1000Mbps	2000Mbps

第4章 产品特性

4.1 完善的管理控制体系

■ 多层分级管理

天阗的管理控制中心可灵活设置成与行政业务管理流程紧密结合的集中监控、多层管理的分级体系。通过策略下发机制，使上级部门能够统一全网的安全防护策略；通过信息上传机制，使上级部门能够及时了解和监控全网的安全状态；

■ 灵活的更新和版本升级

天阗支持手动和自动的特征更新和版本升级，也可以在分级管理体系下由主控统一来完成。天阗的探测引擎同时支持通过 USB 口进行升级。

■ 全局预警

在天阗的多层分级管理体系下，可以实现把单点发生的的重要事件自动预警到其它管理区域，使得各级管理员对于可能发生的重要安全事件具有提前的预警提示。

利用全局预警通道，各级管理员也可以发送交互信息，交流对安全事件的处理经验。

■ 严格的产品权限划分

天阗通过最严格的国际 CC3 测评，可以设定多种分类权限供不同的人员人员使用，支持更为严格多鉴别的身份认证方式。同时在产品部署上支持事件监测、事件分析以及管理配置分布部署，从物理角度保证管理安全。

■ 可扩展到入侵管理

天阗入侵检测全面支持入侵管理，实现多种安全产品的统一管理和协同关联

4.2 全面的入侵检测能力

■ 多种技术结合防止漏报

- 天阗采用引擎高速捕包技术保证满负荷的报文捕获；
- 天阗采用的高速树型匹配技术实现了一次匹配多个规则的模式，检测效率得以成倍的量级提高；

- 天阗采用了 IP 碎片重组、TCP 流重组以及特殊应用编码解析等多种方式，应对躲避 IDS 检测的手法，如：WHISKER、FRAGROUTE 等攻击方式；
- 天阗拥有了业界最为全面和更新速度最快特征库，能够对通用的攻击方法和最新的流行攻击手段进行报警；
- 采用预制漏洞机理分析方法定义特征，对未知攻击方式和变种攻击也能及时报警；
- 采用行为关联分析技术，可以发现基于组合行为的复杂攻击

■ 多种措施降低误报

- 基于状态的协议分析和协议规则树，保证特征匹配的位置准确性；
- 基于攻击过程的分析方法定义特征，可以识别攻击的状态，提供不同级别的事件报警信息；
- 通过支持入侵管理，可以结合漏洞扫描结果和入侵验证来校验攻击是否成功、失败。

■ 多种机制限制滥报

- 天阗内置了状态检测机制，可以识别和处理类似“STICK”等的反 IDS 攻击，有效地避免了事件风暴的产生；
- 天阗提供了多种统计合并技术，可以对同一事件采用合并上报，减少报警量。

■ 自定义入侵检测规则

天阗提供了规范化的 VT++语言和向导定义模式，帮助用户自定义检测模式，扩充检测范围。

4.3 细致的检测策略配置

■ 天阗提供多种不同分类方式的系统策略集，可以针对不同环境、不同应用以及关注目标选取最合适的检测策略。

■ 天阗提供向导方式、已有策略集之间逻辑操作和在系统策略集上衍生等多种方式，方便用户自定义最佳使用的检测策略集，并支持策略集的导入和导出。

■ 天阗提供了灵活的策略编辑方式，确保用户在最短的时间内调整自己所需要的策

略。

4.4 可扩展的事件响应和安全产品联动

天阗具有丰富的可扩展事件响应方式， 包括

- 屏幕显示
- 日志记录
- TCP KILLER 阻断
- 支持邮件方式远程报警、声音以及自定义程序报警
- 支持向网管发送 SNMP TRAP 信息

天阗通过自有 VIP[4]协议族，可以充分实现和第三方安全产品以及网络设备的策略响应联动。

- 防火墙联动:通过对天阗的联动通讯标准的支持，防火墙业界主流的 20 家以上的产品可以实现和天阗的联动，对攻击行为进行阻断。
- 交换机联动：天阗可以和港湾公司的交换机联动，根据策略制定动态关闭相应的交换机端口，可以防止蠕虫类事件的攻击扩散

4.5 多样的日志综合分析和报告输出

天阗分别为管理人员和入侵检测分析员提供了不同类型的日志分析和报告输出

天阗为管理人员提供了常用的周期性统计报表类型模版，管理人员可以直接利用，得出管理性的安全的结论。管理性统计分析报表可以导出为多种格式输出，并设置邮件定时发送报告功能。

天阗为入侵检测分析员提供了多种缺省分析模版，根据这些模版可以获得多种分类的事件日志信息和统计排名，入侵检测分析员在这个基础上可以采用渐进、迭代的方法产生分析方案，形成多个模版之间的具有关联性的分析报告。对于特定的分析方案可以保存为方案文件，供下次再分析时使用。

[4] VIP：Venus Interaction Protocol，启明星辰专有的通用联动协议。

4.6 高度的自主安全保障

堡垒最容易从内部攻破，因此安全产品要保证自身的安全性尤其重要。天阗采取了多种先进措施保障自己的安全，并通过了国家 EAL3 级安全评测.

- 控制中心与所探测网段可以实现隔离部署，保证控制中心的自身安全管理；
- 控制中心与探测引擎通信加密，探测器和控制中心互相认证，防止欺骗，防止日志、策略在传输过程中被篡改；
- 探测引擎检测网口无 IP 地址，入侵者无法对消失在网络中的目标进行扫描和攻击，这样在网络中实现自身隐藏及带外管理；管理网口不开放额外连接端口，提高自身的隐藏性；
- 探测引擎操作系统内核重新编译，并经过了特别的优化，不采用通用的 TCP/IP 堆栈，避免通用 TCP/IP 堆栈的缺陷导致的安全漏洞。

4.7 美观的界面设计和人性化功能操作

天阗在界面设计和功能充分考虑的整体美观性布局和用户操作习惯方便性，主要表现在：

- 采用图形化拓扑结构显示产品组件之间的管理控制关系；
- 采用可定制的分窗口和事件树，分类显示报警信息；
- 采用连续性的曲线图表方式，显示流量统计和事件的趋势变化；
- 提供可定位的联机手册和具有详细的攻击、漏洞解释的安全信息手册，帮助用户参阅功能使用和事件查询；

5.8 稳定的成熟产品应用

天阗产品从投入商业化生产以来，销售数量始终占据国内 IDS 市场前两名。已投入用户使用的产品数以千套计，并且在国内唯一拥有单用户部署数量超过百套的成功案例。

天阗的用户类型覆盖了国内最广泛的行业用户群体，销售领域遍及政府、金融、电信、

交通、能源、教育、企业等部门和行业，共 200 多家；天阗的用户地域分布包含了全国各省、直辖市以及各省的中小型城市。

天阗的应用给用户的网络安全提供了可靠的保障。根据针对天阗的用户调查结果，80%的用户及时发现了各类入侵行为（黑客入侵、拒绝服务、蠕虫泛滥、内部的可疑行为等），50%的用户发现了系统的脆弱性问题（如系统漏洞、弱口令等），还有一部分用户使用天阗大大加强了内部网络运行状况的管理（对通信内容管理、流量监测、访问控制监测等）。

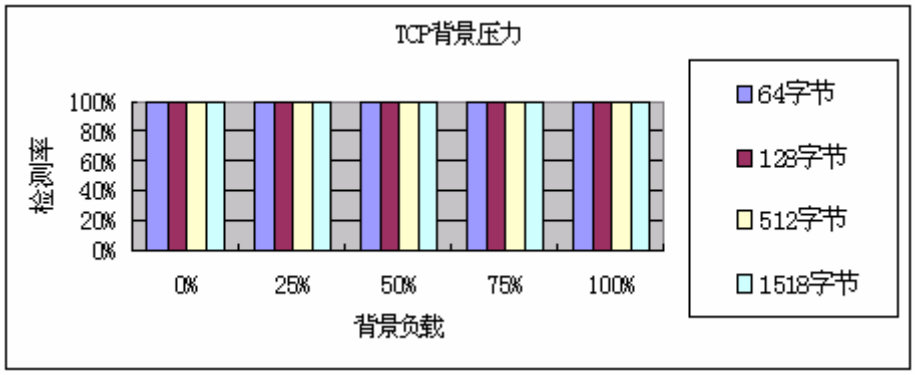
天阗的用户调查结果表明，天阗产品的客户满意度达到 90%以上，客户对于天阗产品安全服务（安装调试、排错、升级、应急响应等）的满意率达到 99%以上。

通过广泛的用户群体，在天阗的应用部署方面积累大量的实际经验，推动着天阗向着成熟化、客户化、国际化的全面发展。

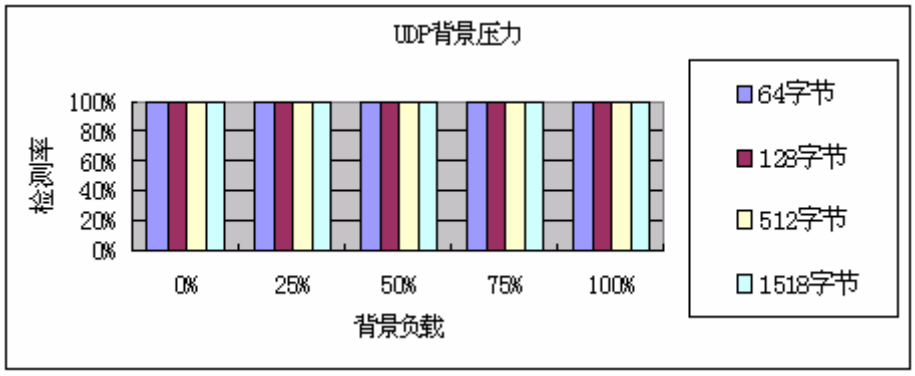
4.9 性能指标

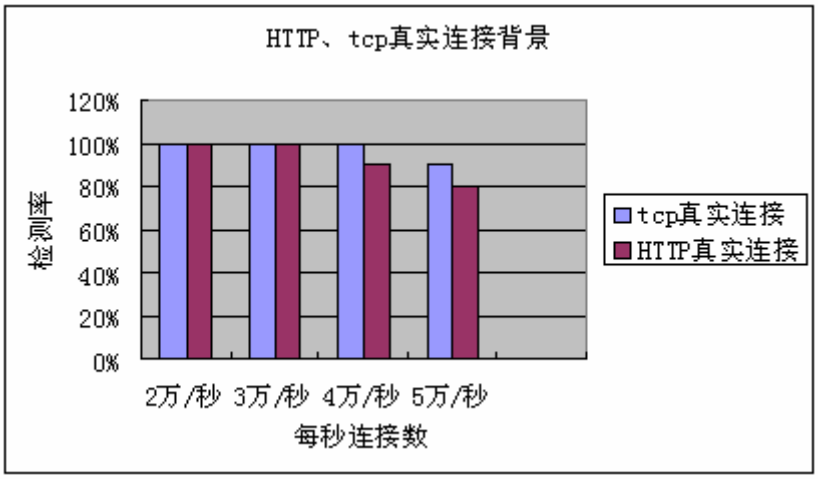
攻击特征流采用统一的 100 种标准的不同攻击样本，目标机器配置多种网络服务。网络背景流量采用专用发包设备来制造，以 0 背景流量为基准，测试入侵检测系统在不同的流量环境（包长）和不同连接背景下的检测能力。

百兆引擎的性能指标如下：

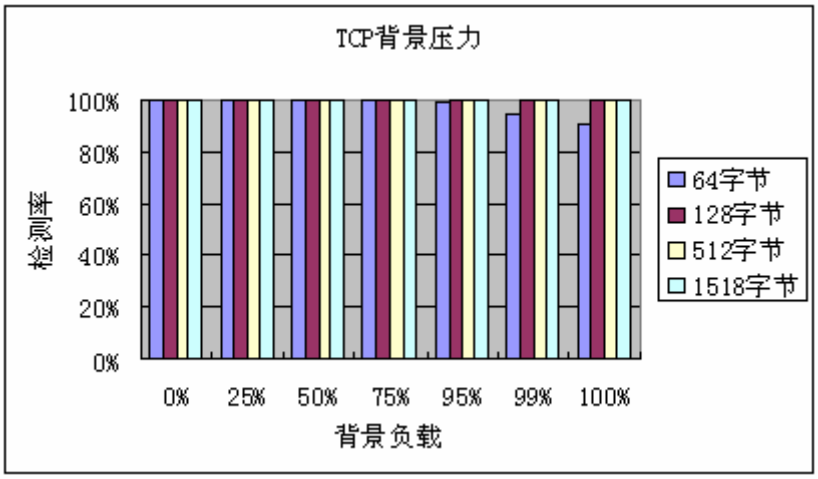


启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn

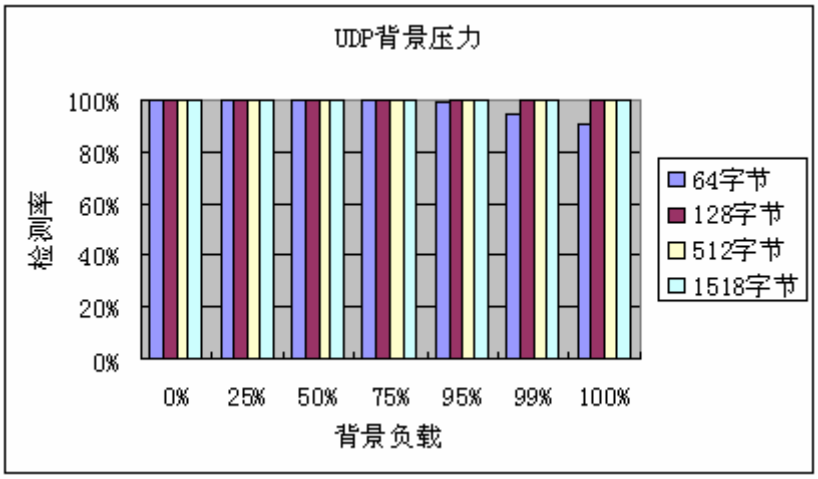


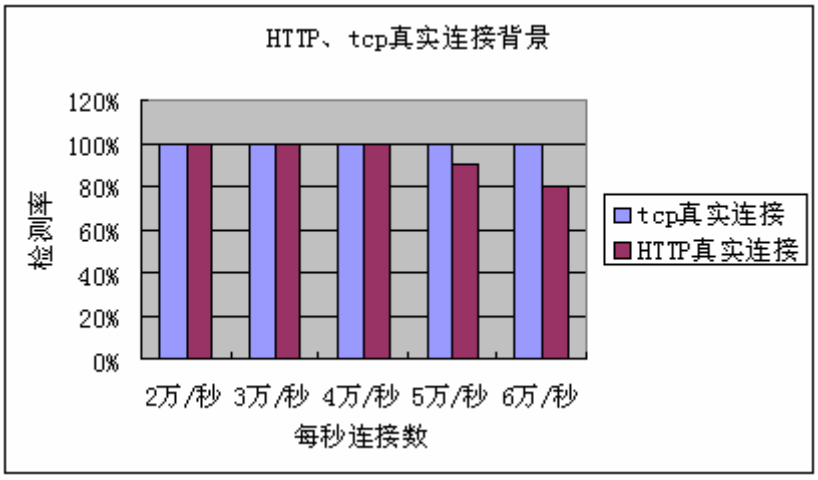


千兆引擎的性能指标如下：



启明星辰信息技术有限公司
地址：北京市海淀区中关村南大街 12 号 188 信箱
电话：010-62149966
传真：010-62146778
网址：www.venustech.com.cn


UDP背景压力
100%
80%
60%
40%
20%
0%
丢包率
0%
25%
50%
75%
95%
99%
100%
背景负载
64字节
128字节
512字节
1518字节


HTTP、tcp真实连接背景
120%
100%
80%
60%
40%
20%
0%
丢包率
2万/秒
3万/秒
4万/秒
5万/秒
6万/秒
每秒连接数
tcp真实连接
HTTP真实连接

第5章 服务支持

北京启明星辰信息技术有限公司

地址：北京市海淀区中关村南大街 12 号 188 信箱

邮编：100081

Tel：010-62149966

Fax：010-62146778

E-MAIL：venus@venustech.com.cn

启明星辰信息技术有限公司武汉分公司

地址：武汉市武珞路 717 号兆富国际大厦 3005 室

邮编：430072

电话：027-87862885

传真：027-87862896

E-Mail：wuhan@venustech.com.cn

上海启明星辰信息技术有限公司

地址：上海市浦东张江高科技园区松涛路 563 号海外创新楼 A 座 6 层

邮编：201203

电话：021-50801133

传真：021-50803515

E-MAIL：shanghai@venustech.com.cn

启明星辰信息技术有限公司重庆分公司

地址：重庆市高新区科园一路 200 号渝高广场 C 座 15－1 号

邮编：400039

电话：023-89099838

传真：023-89099500

E-Mail：chongqing@venustech.com.cn

启明星辰信息技术有限公司深圳分公司

地址：深圳市福田区深南中路 2 号新闻大厦十四层

邮编：518027

电话：0755-25951188

传真：0755-25951088

E-MAIL：shenzhen@venustech.com.cn

启明星辰信息技术有限公司沈阳分公司

地址：沈阳市和平区文化路 19 号金科大厦 910 室

邮编：110004

电话：024-23898819；024-23898858

传真：024－23898922

E-Mail：shenyang@venustech.com.cn

售后统一支持热线：800－810－6038

Web 网址：http://www.venustech.com.cn