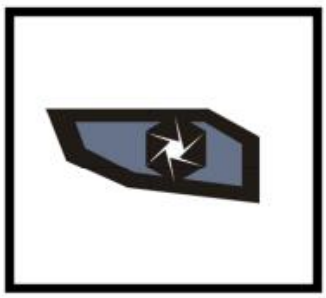
文档编号：**NSFD 102**

冰之眼入侵检测技术白皮书

V3.5



中联绿盟信息技术(北京)有限公司
NSFOCUS INFORMATION TECHNOLOGY CO.,LTD.

版权声明

商标信息

绿盟科技、**NSFOCUS**、冰之眼、**NIDS** 等是中联绿盟信息技术（北京）有限公司的商标。

第三方信息

Microsoft、**Windows** 是美国 **Microsoft Corporation** 的在美国和其它国家注册的商标

目录

前言

文档范围

本文主要介绍冰之眼网络入侵检测系统（以下简称冰之眼或 **NIDS**）的相关特性、技术架构和入侵检测技术的发展等。

期望读者

期望了解本产品主要技术特性的用户、系统管理员、网络管理员等。本文假设您对下面的知识有一定的了解：

- 系统管理
- **Linux** 和 **Windows** 操作系统
- **Internet** 协议

获得帮助

安全相关资料可以访问公司网站：www.nsfocus.com

本产品相关最新信息可以访问网址：

http://www.nsfocus.com/homepage/products/nids.htm

您也可以给我们的技术支持发电子邮件，Email 地址是：

product@nsfocus.com

获取更详尽的绿盟科技网络安全专业服务信息、商务信息，您可通过如下方式和我们联系：

北京总部

地址：北京市海淀区北洼路 4 号益泰大厦 5 层

邮编：100089

电话：010-68438880

传真：010-68437328

Email：webadmin@nsfocus.com

上海分公司

地址：上海市南京西路 758 号博爱大厦 9 楼 A 座

邮编：200041

电话：021-62179591/92

传真：021-62176862

广州分公司

地址：广州市人民中路 555 号美国银行中心 1702

邮编：510180

电话：020-81301251，81301252

传真：020-81301251/52

一、概述

1.1 为什么需要网络入侵检测系统

今天，越来越多的蠕虫、病毒、木马和黑客成功突破了防火墙的保护，很明显，我们需要网络入侵检测系统。绿盟科技的冰之眼网络入侵检测系统能够协助您：

- 检测来自数千种蠕虫、病毒、木马和黑客的威胁；
- 检测来自拒绝服务攻击的威胁；
- 检测您的网络因为各种 **IMS**（实时消息系统）、网络在线游戏导致的企业资源滥用；
- 检测 **P2P** 应用可能导致的企业重要机密信息泄漏和可能引发的版权相关的法律问题；
- 保障您的电子商务或电子政务系统 **7×24** 不间断运行；
- 提高企业整体的网络安全水平；
- 降低企业整体的安全费用以及对于网络安全领域人才的需求；
- 迅速定位网络故障，提高网络稳定运行时间。

1.2 常见的入侵检测技术

1、IP 碎片重组（IP Defragmentation）

入侵者将攻击报文拆分成 **IP** 碎片后发送，试图逃避 **NIDS** 的侦测。**IP** 碎片重组将这些碎片重新拼装后分析。由于不同的操作系统采用的重组方式不同，**NIDS** 必须针对所有的可能进行重组。

2、TCP 会话跟踪（TCP Session Track）

向服务器发送一个数据区包含 **cmd.exe** 的 **TCP** 报文不会给服务器带来任何危害，但却可能诱使 **NIDS** 发出一个攻击信息的误报。**NIDS** 将 **TCP** 特征检测建立在 **TCP** 会话的基础上，从而避免了此类误报，并提高了效率。

3、TCP 流汇聚（TCP Stream Reassembly）

入侵者将 **cmd.exe** 拆分为 **c**,**m**,**d**,.,**e**,**x**,**e** 七个 **TCP** 报文后发送，同样可以逃避 **NIDS** 的检测。**TCP** 流汇聚能够从多个 **TCP** 报文中检测出类似攻击行为。

4、协议分析（Protocol Analysis）

协议分析分为应用层协议解码与应用层状态跟踪两个部分。在 **HTTP** 协议的 **GET** 请求报文中，前者将请求拆解为各个域，然后进行相应的模式匹配。后者用于跟踪该请求的状态，从中可以判断出攻击是否成功。协议分析是几乎所有新一代入侵检测技术的基础。深入而细致的协议分析能够极大地提高检测的准确性，降低误报率。

5、特征检测（模式匹配）（Signature Detection）

将协议解码后的域值与事先精心提取的攻击特征（规则）进行匹配，从中发现潜在的攻击行为。基于特征（规则）的检测是一项传统而成熟的入侵检测技术，提供了很高的准确性与广泛性。

6、关联分析（Correlative）

实时的关联分析引擎能够发现基本 **NIDS** 引擎所不能发现的攻击事件，如口令猜测等，是基本引擎的一个重要的补充。

7、日志归并（Merger）

当前入侵检测系统面临的一个重要问题是如何将最有用的攻击信息快速地呈现在管理员面前，尽可能地减少或消除无用的信息。日志归并根据一系列事先制定的策略，将多条告警日志合并为一条，从而极大地减少了告警日志的数量。同时也可在一定程度上缓解 **NIDS** 遭受 **Flood** 的可能。

8、网络流量异常（Traffic Abnormity）

通过监控网络上流量的变化情况，可以获得当前网络的健康状况。分析长期的历史数据可以判断当前网络是否出现了某种问题。网络异常流量检测作为一项审计功能是入侵检测系统的一个组成部分。

1.3 新一代入侵检测技术

1.3.1 协议识别（Protocol Discover）

协议识别是新一代的网络安全产品的核心技术。今天，安全产品如防火墙、**NIDS**、**NIPS** 均是通过协议端口映射表（或类似技术）来判断流经的网络报文属于何种协议，然后递交给相应的协议分析引擎。但事实上，协议与端口是完全无关的两个概念。我们仅仅可以认为某个协议运行在一个相对固定的缺省端口，但是没有任何的法律限制该协议必须绑定在该端口。

l 标准协议运行在任意端口

HTTP 尽管通常运行在 **80** 端口，但实际环境中可以运行在任意端口，比如 **312** 端口。采用协议端口映射表技术的产品需要管理员必须预先知道这一点，通过管理员手动修改映射表，来驱动协议分析引擎认识捕获的通往 **312** 端口的 **HTTP** 报文。由于目前的网络具有的复杂性和动态性，管理员往往不可能知道所有的应用实际运行的端口，也不可能跟踪所有的端口变动，而黑客则可以通过扫描发现这些非标准端口，发动攻击。此时绕过了所有的安全设备，包括 **NIDS**。

l 数以千计的木马、后门

几乎所有的木马，后门运行在黑客指定的任意端口，管理员事先完全无法获知其端口号，也就无法修改映射表来驱动 **NIDS** 进行检测。事实上，目前传统的 **NIDS** 产品只能检测绑定在缺省固定端口的木马与后门。

l Smart Tunnel（智能隧道）技术的广泛应用

高速网络飞速普及的今天，**P2P**（点到点）应用（如各种 **P2P** 下载工具、**IP** 电话等）、**IMS**（实时消息系统 如 **MSN**、**Yahoo Pager**）、网络在线游戏等迅速普及。这些崭新的网络应用大部分使用了一种被称为 **Smart Tunnel**（智能隧道）的技术，该技术正是为了避开防火墙、**NIDS** 产品而诞生的。其特点是：服务端（或接收端）没有绑定任何固定的端口，客户端（或发起端）可以自行使用任意随机端口连接服务器。这些软件在带给人们各种便利的同时也带来了各种严重的问题。最为典型的是网络资源的滥用和公司资源的浪费。**P2P** 软件还有可

能带来严重的法律问题：公司内部的重要机密信息可能通过 **P2P** 技术穿透防火墙与 **NIDS** 的封锁隐蔽地传递到黑客手中。采用类似协议端口映射表技术的 **NIDS** 产品根本无法检测并防止此类事件的发生。

协议识别通过动态分析网络报文中包含的协议特征，发现其所在协议，然后递交给相应的协议分析引擎进行处理。具备了协议识别技术的 **NIDS** 产品，能够在完全不需要管理员参与的情况下，高速智能准确地检测出对于运行在任意端口的应用层协议的攻击行为，也可以准确发现绑定在任意端口的各种木马、后门，同时，对于运用了 **Smart Tunnel** 技术的软件也能准确地捕获分析。

1.3.2 协议异常检测（Protocol Abnormity）

基于特征检测（模式匹配）的 **NIDS** 产品可以精确地检测出已知的攻击。通过不断升级的特征库，**NIDS** 可以在第一时间检测到入侵者的攻击行为。但事实上，存在三个方面的因素导致协议异常的诞生：

（1）厂商从提取某个攻击特征到最终用户的 **NIDS** 产品升级需要一个时间间隔，在这个时间间隔内，基于特征检测的 **NIDS** 产品是无法检测到黑客的该攻击行为的。

（2）来自 **0-day** 或未公开 **exploit** 的隐蔽攻击即使是安全厂商往往也无法第一时间获得攻击特征，通常 **NIDS** 无法检测这类具有最高风险的攻击行为。

（3）**Internet** 上蠕虫在 **15** 分钟内席卷全球，即使是最优秀的厂商也不能够在这么短的时间内完成对其的发现和检测。

建立在协议分析基础上的 **NIDS** 产品，发现任何违背 **RFC** 规定后，均可视为协议异常。**协议异常最为重要的作用是检测未知的溢出攻击与拒绝服务攻击**。作为一项成熟的技术，协议异常具有接近 **100%**的检测准确率和近乎零的误报率。

1.3.3 攻击结果判定（Attack Result Detection）

对于管理员来说，从每天发生的成千上万次攻击中快速定位风险程度最高的攻击——成功的攻击是最为重要的事情。

通过对多种尖端检测技术的综合运用以及数千种攻击行为的全面深入分析，可以精确检测出几乎所有攻击的最终结果——成功还是失败。依据该结果，管理员可以迅速判断出具有最高风险的安全隐患，并在第一时间做出处理措施加以弥补。

较为简单的例子是针对 **HTTP** 的 **CGI** 请求攻击。通常服务器返回 **200 OK** 代表请求成功，**4xx** 为请求失败。**NIDS** 的协议分析引擎可以借此判断出该攻击的最终结果。

复杂的例子来自 **0-day** 的未公开溢出攻击。多种检测方式的综合运用可以最终检测出该攻击的成功与否。

攻击结果判定是新一代 NIDS 技术的显著标志。

1.3.4 拒绝服务检测（Denial of Service Detection）

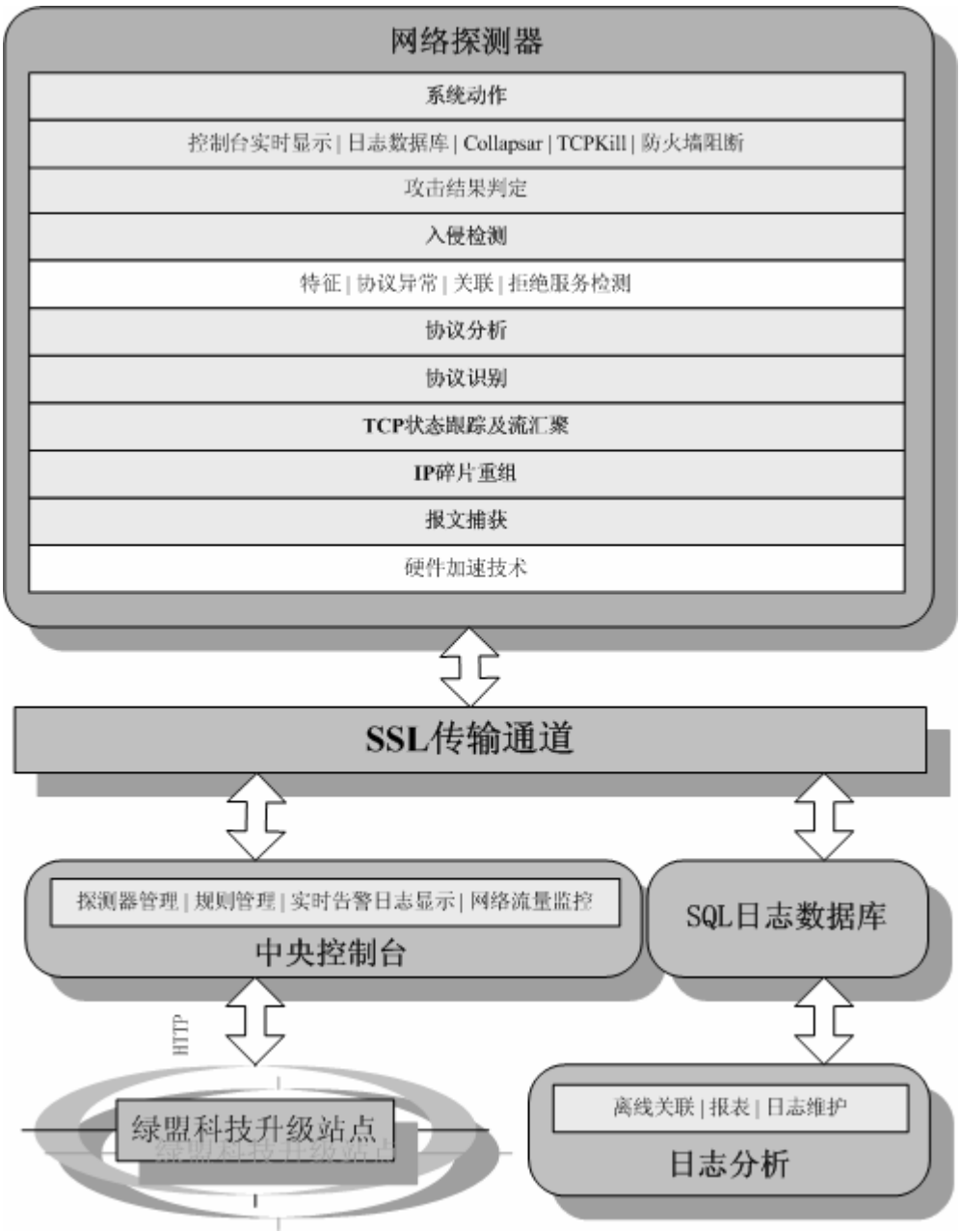
基于 **TCP/IP** 协议缺陷的拒绝服务攻击（**DoS** 或 **DDoS**）至今仍对互联网造成巨大的威胁。如何精确检测并保护运行关键任务的电子商务或电子政务系统远离拒绝服务的威胁，是一项复杂具有挑战性的工作。常见的拒绝服务检测与保护技术如系统优化、路由器优化、负载均衡、防火墙等并不能完全彻底地解决此类问题。绿盟科技抗拒绝服务专利 **Collapsar™**技术可以完美而彻底地检测并阻止来自拒绝服务的威胁，保障您的电子商务或电子政务系统 **7×24** 得以不间断运行。

1.3.5 基于硬件的 GIGAbit 线速入侵检测

性能是 **NIDS** 产品不可回避的一个问题。作为网络安全产品，**NIDS** 应该在任何极端情况下检测出所有的攻击行为。**GIGAbit** 线速是其最好的保证。新一代

的硬件加速技术能够保证 **NIDS** 产品高速稳定可靠地工作在各种复杂的网络环境下。

二、产品架构


网络探测器
系统动作
控制台实时显示 | 日志数据库 | Collapsar | TCPKill | 防火墙阻断
攻击结果判定
入侵检测
特征 | 协议异常 | 关联 | 拒绝服务检测
协议分析
协议识别
TCP状态跟踪及流汇聚
IP碎片重组
报文捕获
硬件加速技术
SSL传输通道
探测器管理 | 规则管理 | 实时告警日志显示 | 网络流量监控
中央控制台
SQL日志数据库
HTTP
绿盟科技升级站点
离线关联 | 报表 | 日志维护
日志分析

三、产品特性

3.1 入侵检测

l 覆盖广泛的攻击特征库

冰之眼入侵检测系统携带了超过 **1800** 条经过仔细检测与时间考验的攻击特征，由著名的 **NSFocus** 安全小组精心提炼而成。针对每个攻击均附有详细描述和解决办法，对应 **NSFocus ID**、**CVE ID**、**Bugtraq ID**，管理员直接点击里面的安全补丁 **URL** 连接可以直接将系统升级到最新版本，免除遭受第二波的攻击。

l IP 碎片重组与 TCP 流汇聚

冰之眼入侵检测系统具有完美的 **IP** 碎片重组与 **TCP** 流汇聚能力，能够检测到黑客采用任意分片方式进行的攻击。

l 协议识别

冰之眼入侵检测系统能够准确识别超过 **100** 种的应用层协议、木马、后门、**P2P** 应用、**IMS** 系统、网络在线游戏等。

l 协议分析

冰之眼入侵检测系统深入分析了接近 **100** 种的应用层协议，包括 **HTTP**、**FTP**、**SMTP**……

l 攻击结果判定

冰之眼入侵检测系统能够准确判断包括扫描，溢出在内的绝大多数攻击行为的最终结果。

l 协议异常检测

冰之眼入侵检测系统具备了强有力的协议异常分析引擎，能够准确发现几乎 **100%**的未知溢出攻击与 **0-day Exploit**。

l 拒绝服务检测

冰之眼入侵检测系统采用绿盟科技的 **Collapsar™**专利技术，能够准确检测 **SYN Flood**、**ICMP Flood**、**Connection Flood**、**Null Stream Flood** 等多种拒绝服务攻击。配合绿盟科技的 **Collapsar™**产品，能够进行有效的防御保护。

3.2 性能

- **GIGAbit 线速（Wire-Speed）**

冰之眼入侵检测系统在全部检测功能、全部规则集打开的情况下具有 **GIGAbit** 线速的分析能力。

- **多监听口**

冰之眼入侵检测系统根据型号可以配置多个硬件监听口。监听口完全支持即插即用，用户在增加监听的网段时仅仅需要购买独立的硬件监听模块插上即可完成升级，而不需要购买单独的探测器引擎。极大地保障了用户的投资，降低了使用维护成本。

3.3 入侵保护

- **Collapsar™**

冰之眼入侵检测系统与绿盟科技的 **Collapsar™**产品联动能够最大限度地保护您的网络免除拒绝服务带来的危害。

- **TCP Killer**

冰之眼入侵检测系统能够实时地切断基于 **TCP** 协议的攻击行为。

- **防火墙阻断**

冰之眼入侵检测系统可以与超过 **10** 种的防火墙产品进行联动阻断入侵者。如 **Checkpoint FW-1**、**Netscreen**、天网、天融信、卫士通龙马等。

3.4 探测器管理

- **冰之眼控制台**

冰之眼控制台可灵活部署在网络的各个角落。管理员通过控制台可以查看到实时的攻击告警日志，并可修改探测器端加载的攻击特征规则库。

l 其它方式

包括串口（**RS232**）、远程 **SSH**。其中串口支持中/英文两种语言，可实时切换。

3.5 升级与技术支持

l 实时在线升级

冰之眼入侵检测系统所有部件包括攻击规则库与探测器引擎均可实时自动在线升级。**NSFocus** 安全小组 **24** 小时不间断地跟踪最新的安全信息，在第一时间提炼出攻击特征加入到冰之眼规则库中。

l 升级方式

冰之眼入侵检测系统支持实时在线升级、**SSH** 远程升级。

l 更新周期

绿盟科技承诺：日常升级至少每 **7** 天一次，重大安全问题升级在全球首次发现后三个工作日内完成。

3.6 自身安全

l 特别定制的操作系统

在提供给探测器无与伦比性能与稳定性的同时，本身具备了超强的安全性。

l SSL 传输

冰之眼探测引擎与控制台间采用强加密的 **SSL** 加密传输告警日志与控制命令。完全避免了可能存在的嗅探行为。

l 实时日志归并

冰之眼归并引擎由规则驱动，可以执行任意粒度的日志归并动作，完全避免类似 **Stick** 的 **Anti-NIDS**。

l 多点备份

冰之眼探测引擎可以将攻击告警日志实时发送到多个冰之眼控制台或日志数据库保存。

l 日志缓存

在冰之眼探测引擎与控制台的网络完全断开的情况下，探测引擎仍然会将检测到的攻击行为在探测器本地保存，等到网络恢复正常自动地同步到冰之眼控制台或日志数据库。