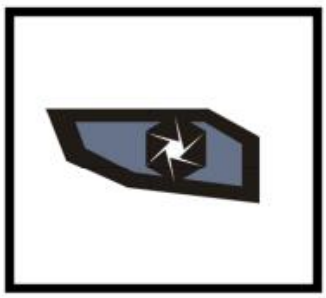
文档编号：**NSFD 101**

冰之眼入侵管理技术白皮书

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

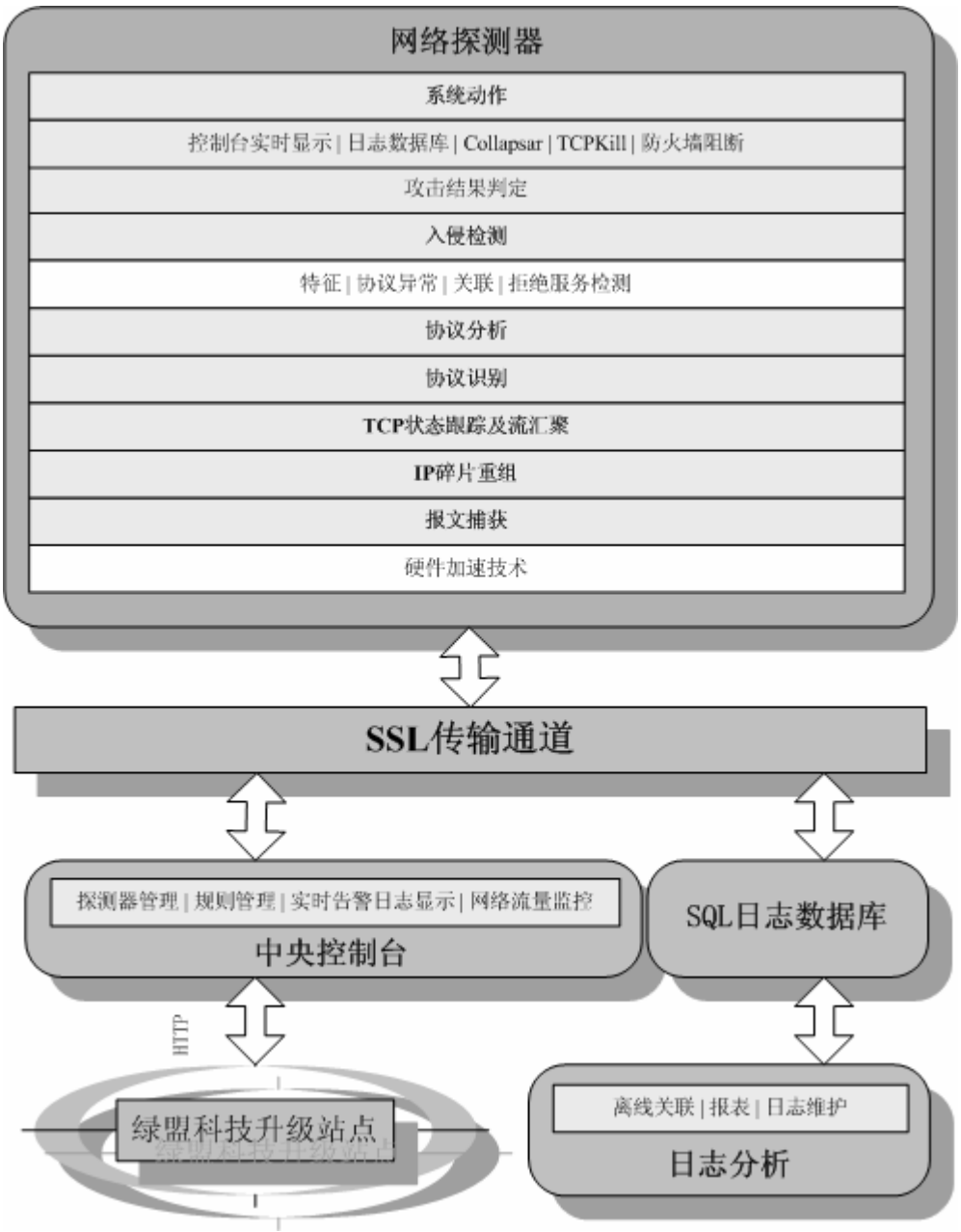
地址：广州市人民中路 555 号美国银行中心 1702

邮编：510180

电话：020-81301251，81301252

传真：020-81301251/52

一、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

二、产品特性

2.1 入侵管理

I 多层分布式集中监控

冰之眼控制台能够灵活部署在网络的任意节点，控制台支持任意层次级联部署与分布式部署。强有力的集中监控体系提供给管理员统管全局的能力，配合冰之眼新一代的探测引擎，管理员可以在最短的时间内对于入侵风险做出最快速的反应。

I 事件统计

作为新一代 **NIDS** 入侵管理观念体现，冰之眼控制台不再局限于以往事件日志高中低分类显示方式，而是转变为以各种实时事件统计为主。通过查看这些实时的数据，管理员从中获得当前网络的总体安全状态。控制台对于以下类别进行了统计计数：总的事件、归并后的事件、过滤的事件、攻击事件、网络监控事件、成功的攻击数、攻击成功率、失败的攻击数、攻击失败率、高风险攻击、中风险攻击、低风险攻击、各种蠕虫/**P2P** 事件等。

I 多样化日志分类

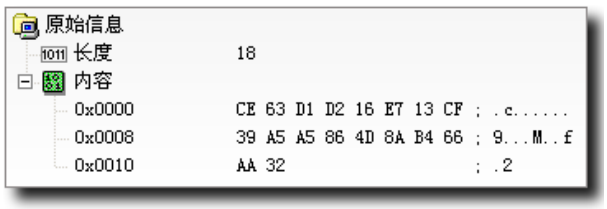
实时地将告警日志按各种条件进行分类有助于帮助管理员迅速地发现某些特定攻击。冰之眼控制台可以按多种标准动态地切换告警日志的分类。包括：攻击结果（成功－失败－可疑）、高中低风险、服务、攻击流行程度、攻击采用的技术手段、攻击源－目的－事件名称、攻击时间等。对于每条攻击日志可按事先的定义以不同的颜色高亮显示。

l 灵活的事件过滤系统

规则驱动的冰之眼事件过滤系统支持采用多种粒度过滤探测器所产生的告警日志，当前支持：攻击发生时间范围、事件名称、事件类别、所属服务、源网络范围、目的网络范围、触发探测器、攻击结果、事件动作等。管理员可以制定基于时间的攻击检测规则。如：控制探测器仅仅检测凌晨 **2~5** 点发生的失败的属于 **FTP** 协议的攻击事件。灵活的运用的此功能，可以控制冰之眼系统仅仅记录管理员关心的攻击告警事件，极大地减小了攻击告警的数量，降低了管理员的工作强度，提高了对于高风险攻击的反应速度。

l 攻击取样与取证

异常检测技术的发展成熟使得检测未知的攻击成为可能。由于未知攻击的特点，**NIDS** 事先没有其对应的详细描述与漏洞修复方法。冰之眼系统对于未知攻击自动的提取其样本（包括攻击现场与攻击原始报文），**NSFocus** 安全小组会在最短的时间内分析提取特征，提供详细的解决办法。同时，由于攻击样本的保存，使得调查取证成为可能。原始的攻击样本可以提交作为法律证物。同时，冰之眼具有如下特性使得管理员可以迅速定位入侵者位置：



（1）自动解析入侵者机器名/域名。

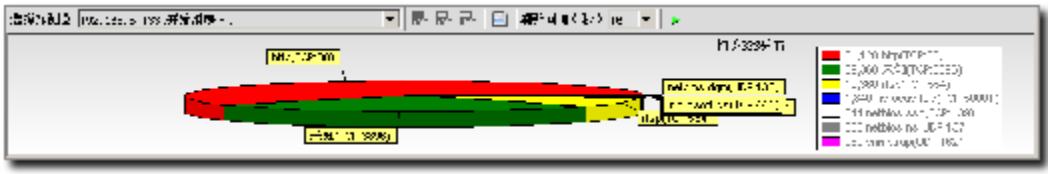
（2）自动获得入侵者所使用的机器型号。

如：来源：**192.168.5.20 jingdg (Dell Computer Corp.)**

l 探测器状态监控

对于运行中的探测器，冰之眼控制台 **24** 小时不间断地监控其健康情况，管理员可随时查看探测器的各种主要参数性能，包括：**CPU**、内存、剩余硬盘空间等。

l 网络流量监控



冰之眼探测器实时统计了当前网络中的各种报文流量发送到控制台，包括：当前协议分布图、总 **PPS**、总 **BPS**、**TCP** 会话数等。管理员通过观察这些实时数据，可以判断当前网络运行状况是否良好。

l 基于 XML 的开放式联动协议

冰之眼系统提供了 **Open Source** 的基于 **XML** 的开放式联动接口，任何安全产品可以基于此接口接收冰之眼系统的攻击告警。当前支持 **Windows** 系列、**Linux** 系列、***BSD** 系列、**SUN OS** 系列。

l 协议回放

冰之眼系统支持记录网络的通信报文，并解码回放。目前支持 **HTTP**、**SMTP**、**FTP**、**Telnet**、**POP3** 协议。

l 可信时间戳

为提高检测精度，冰之眼控制台与探测器内置了时钟同步机制，所有连接同一控制台的探测器均保持毫秒一级的精确度。同时，冰之眼探测器还提供了系统时区的修改，即使探测器安装在伦敦，控制台放置在北京也可准确无误地工作。

2.2 规则库管理

l 系统规则管理

系统规则编辑采用模板形式，支持组编辑修改。管理员可以快捷地修改整个组的规则属性，包括是否激活，以及各种系统动作等。当前支持分组标准为：高中低风险、服务、流行程度、技术手段、操作系统类型等。管理员可以在各分组间实时地切换。

l 用户自定义规则

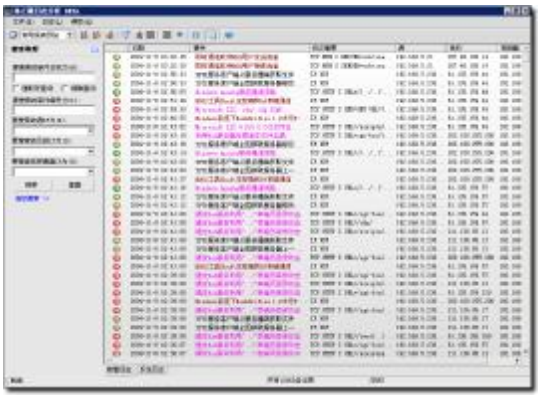
冰之眼控制台提供了强大的用户自定义规则系统，用户可以定义几乎所有的协议字段，并支持正则表达式。

l 攻击描述与修复方法

绿盟科技著名的 **NSFocus** 安全小组提供了对于每个攻击漏洞的详细描述，同时对应 **NSFocus ID**、**CVE ID**、**Bugtraq ID**，并提供了详细的修复方法及补丁下载地址。管理员在帮助页面内即可完成对于系统的补丁下载与升级。极大的提高了对于攻击的响应速度。

2.3 日志分析

l 报表



冰之眼控制台提供了详细、综合报表、自定义三种类型 **10** 多个类别的报表模板，支持生成：日、周、月、季度、年度综合报表。报表支持 **MS Word**、**Html**、**JPG** 格式导出。同时支持定时通过电子邮件发送报表至系统管理员。

- **零管理**

从实时升级系统到报表系统，从攻击告警到日志备份，冰之眼入侵检测系统完全支持零管理技术。所有管理员需要日常进行的操作均可由系统定时自动后台运行，极大地降低了维护费用与管理员的工作强度。

- **离线关联分析与归并**

区别于探测器进行的实时的关联分析与归并，离线关联分析能够发现某些较长时间范围内的攻击特征。离线归并能够减小攻击告警的数量，提高管理员对于攻击的响应速度。

- **日志备份与恢复**

冰之眼日志系统支持定时自动日志备份与清除，完全不需要管理员的参与，极大地减小了管理员的工作量。

- **XML 支持**

日志支持 **XML** 格式导出以便进行二次分析。

- **支持 Microsoft SQLServer2000 系列大型数据库（包括对应的 MSDE 产品）**

2.4 升级与技术支持

- **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冰之眼规则库中。

- **升级方式**

冰之眼入侵检测系统支持实时控制台在线升级、**SSH** 远程升级。

- **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。

2.5 自身安全性

l 多权限多用户

冰之眼控制台身份验证系统采用独立于操作系统的多权限多用户系统。管理权限与审计权限独立，支持生成审计报表。

l SSL 传输

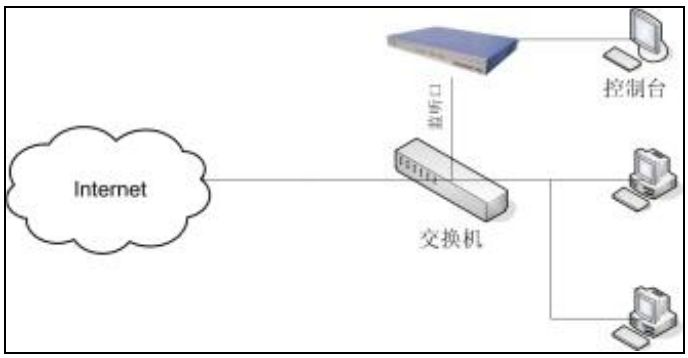
冰之眼探测引擎与控制台间采用强加密的 **SSL** 加密传输告警日志与控制命令。完全避免了可能存在的嗅探行为。

l 第三方软件

在冰之眼系统中使用了部分第三方软件，如 **Microsoft SQL Server2000** 系列。这些软件系统可能引入新的安全隐患。冰之眼软件光盘中附带了这些第三方软件的最新安全升级补丁，可以避免因此导致的安全隐患。

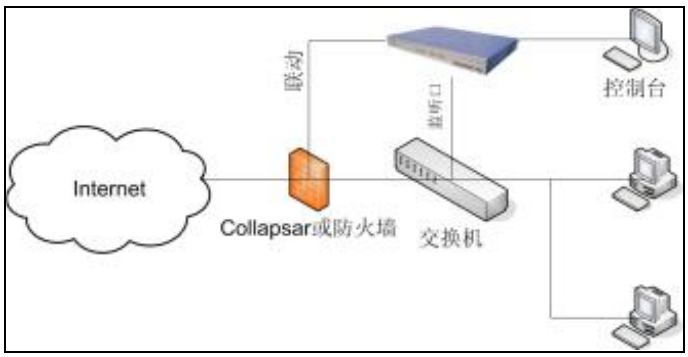
2.6 实施部署

l 典型



冰之眼探测器需要捕获所有进出的网络报文。可通过设置交换机的监听口达到此目的。值得注意的是某些老的交换机型号不支持设置监听口，购买时请先确定。需要监听多个网段时，将多个网段分别接到不同的探测器监听口上即可。

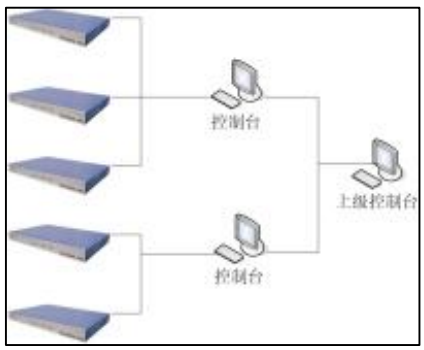
l 与 Collapsar、防火墙联动



冰之眼 **NIDS** 与绿盟科技 **Collapsar** 产品或防火墙产品进行联动可以切断攻击来源，将入侵者屏蔽在被保护网络之外。

l 多层分布式

冰之眼系统具有非常灵活的部署方式。在需要按照行政级别部署冰之眼控制台时，可以采用此类方式。控制台支持任意层次的级联部署，上级控制台可以将最新的最新升级补丁，规则模板文件，探测器配置文件等统一发送到下级控制台，保持整个系统的完整同一性。



l 其它

如果您的交换机不支持设置监听口，可以选用 **TAP**、**HUB** 等其它方式安装。具体方法请联系绿盟科技的工程人员。