360 入侵检测系统

白皮书

目录

1.产品概述

网络安全是一个系统的概念，制定有效的安全策略或方案，是网络信息安全的首要目标。网络安全技术主要有，认证授权、数据加密、访问控制、安全审计等。入侵检测技术是安全审计中的核心技术之一，是网络安全防护的重要组成部分。因此通过入侵检测系统（缩写 IDS）设备检测网络中是否存在违反安全策略的行为和被攻击的迹象，也成为被人们普遍使用的网络安全产品。

入侵检测系统可以说是防火墙系统的合理补充和延伸，并且防火墙相当于第一道安全闸门，而入侵检测系统会在不影响网络部署的前提下，实时、动态地检测来自内部和外部的各种攻击，同时有效地弥补了防火墙所能无法检测到的攻击，进而与防火墙联动达到有效网络安全防护。

1.1 现今网络面临的难题

计算机网络的安全是一个国际化的问题，每年全球因计算机网络的安全系统被破坏而造成的经济损失达数百亿美元。进入新世纪之后，上述损失将达 2000 亿美元以上。

随着网络技术的发展，入侵的规模越来越大，入侵的手段与技术也不断发展变化，入侵的发起者和入侵的对象越来越趋于分布化，早期的网络安全产品，例如：防火墙，它作为网络边界的设备，只能抵挡外部来的入侵行为；自身存在的弱点也可能被攻破；对某些攻击保护很弱；即使通过防火墙的保护，合法使用者仍会非法地使用系统，甚至提升自己的权限；进而拒绝非法的连接请求，但是对于入侵者的攻击行为仍是一无所知，因此入侵就会很容易。这时企事业单位的网络安全性也受到了严峻考验：网络上的不法分子不断的寻找网络上的漏洞，企图潜入内部网络，一旦网络被攻破，一些机密的资料可能会被盗、网络可能会被破坏，给网络所属单位带来难以预测的损害。随着网络结构异常复杂，入侵检测系统体系结构也在随着网络安全需求而进化者，因此应用程序辨识、异常流量和攻击行为的检测、深层风险交互查询能力、全方位的系统管理均成为了新型入侵检测系统的标配。

1.2 采用的主流入侵检测技术

模式匹配技术是入侵检测技术领域中应用最为广泛的检测手段和机制之一，模式匹配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来发现，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。

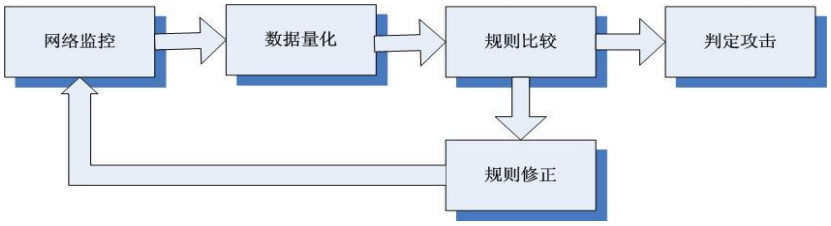
模式匹配技术有它自己的好处：比如只需收集相关的数据集合，显著减少系统负担，同时模式匹配技术经过多年发展已经相当成熟，使得检测准确率和效率都相当高，这也是模式匹配技术至今仍然存在并被使用的理由。当然，单纯的模式匹配技术也同样具有明显的不足：

- 如果对整个网络流量进行匹配，计算量非常大，系统有严重的性能问题。
- 只能使用固定的特征模式来检测入侵，对做过变形的攻击无法检测，因此容易被逃避检测。
- 特征库庞大，对攻击信号的真实含义和实际效果没有理解能力，因此，所有的变形都将成为攻击特征库里一个不同的特征，这就是模式匹配系统有一个庞大的特征库的原因所在。

因此，模式匹配的这种检测机制决定了它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。最为不足的是对任何企图绕开入侵检测的网络攻击欺骗无能为力，由此会产生大量的虚假报警，以至于淹没了真正的攻击检测。

第二种技术是异常行为检测，基于异常检测方法主要来源于这样的思想：任何人的正常行为都是有一定规律的，并且可以通过分析这些行为产生的日志信息总结出这些规律，通常需要定义为各种行为参数及其阀值的集合，用于描述正常行为范围。而入侵和滥用行为则通常和正常的行为存在严重的差异，通过检查出这些差异就可以检测出入侵。这样，我们就能够检测出非法的入侵行为甚至是通过未知攻击方法进行的入侵行为，此外不属于入侵的异常用户行为（滥用自己的权限）也能被检测到。

异常检测技术的检测流程：



异常检测技术具有的特点：

- 异常检测系统的效率取决于合法用户行为定义的完备性和监控的频率大小。因为不需要对每种入侵行为进行定义，因此能有效检测未知的入侵。

- 系统能针对用户行为的改变进行自我调整和优化，但随着检测模型的逐步精确，异常检测会消耗更多的系统资源。

- 漏报率低，误报率高

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。

当然要使用异常检测还面临着几个问题：

- 用户的行为有一定规律性，但选择哪些数据来表现这些规律的行为仍然存在一些问题。

- 如何有效表示这些正常行为，使用什么方法反映正常行为，如何能学习到用户的新正常行为存在问题。

- 规律的学习过程时间到底为多少，用户行为的时效性等问题。

第三种是协议分析技术，这是目前最先进的检测技术，是在传统模式匹配技术基础之上发展起来的一种新的入侵检测技术。它主要是针对网络攻击行为中攻击者企图躲避 IDS 的检测，对攻击数据包做一些变形，它充分利用了网络协议的高度有序性，并结合了高速数据包捕捉、协议分析和命令解析，来快速检测某个攻击特征是否存在，从而逃避 IDS 的检测而开发设计的。它最大的特点是将捕获的数据包从网络层一直送达应用层，将真实数据还原出来，然后将还原出来的数据再与规则库进行匹配，因此它能够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。协议分析大大减少了计算量，即使

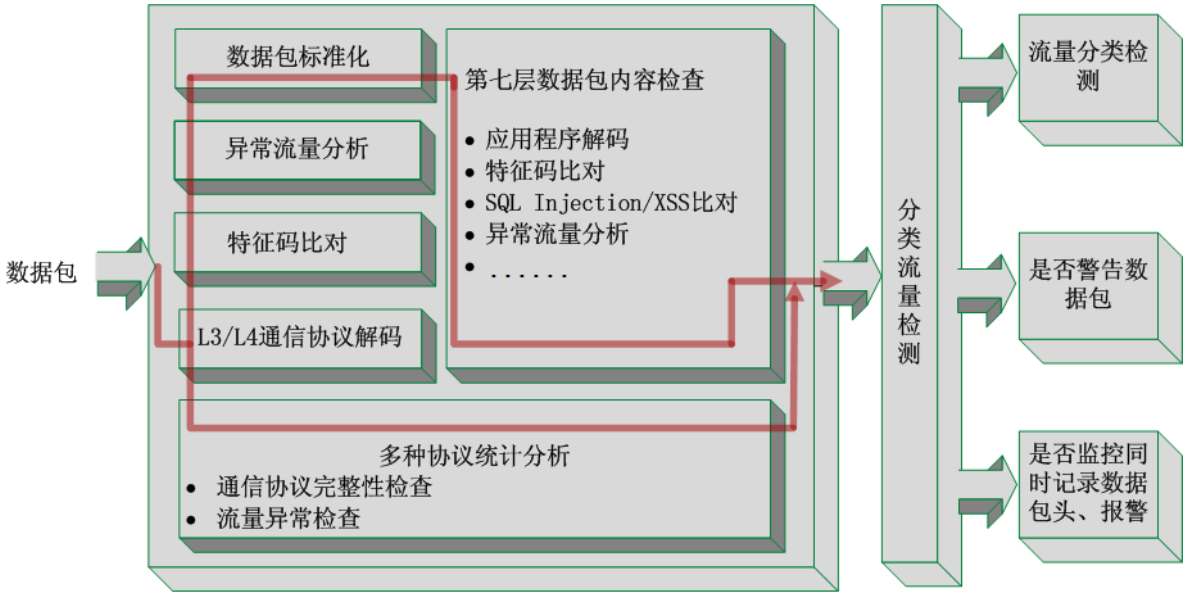
在高负载的高速网络上，也能逐个分析所有的数据包。采用协议分析技术的 IDS 能够理解不同协议的原理，由此分析这些协议的流量，来寻找可疑的或不正常行为。对每一种协议，分析不仅仅基于协议标准，还基于协议的具体实现，因为很多协议的实现偏离了协议标准。协议分析技术观察并验证所有的流量，当流量不是期望值时，IDS 就发出告警。协议分析具有寻找任何偏离标准或期望值的行为的能力，因此能够检测到已知和未知攻击方法。

同时，状态协议分析技术就是在常规协议分析技术的基础上，加入状态特性分析，即不仅仅检测单一的连接请求或响应，而是将一个会话的所有流量作为一个整体来考虑。有些网络攻击行为仅靠检测单一的连接请求或响应是检测不到的，因为攻击行为包含在多个请求中，此时状态协议分析技术就是 IDS 技术的首选。同时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。

1.3 系统核心引擎运行流程

在深入分析用户信息安全需求之后，360 公司推出 360 入侵检测系统系列产品。360 入侵检测系统提供强大的网络安全检测性能，能够精确地检测您的网络遭受最新式的各种网络攻击，可以为企事业单位网络提供完善的网络安全保障，预防来自外部及内部网络的攻击及不法分子的入侵和破坏。

下图为 360 入侵检测系统核心引擎的运行流程，简要描述了 360 入侵检测系统处理数据包的方式和步骤。



360 入侵检测系统核心引擎运行流程图

2.产品特色

2.1 强大的分析检测能力

360 入侵检测系统采用了先进的入侵检测技术体系，基于状态的应用层协议分析技术，使系统能够准确快速地检测各种攻击行为，并显著地提高了系统的性能，能够适应日益复杂的网络环境。

2.2 全面的检测范围

360 入侵检测系统可对常见端口扫描攻击、木马后门、拒绝服务攻击、蠕虫、木马、缓冲溢出、Ping 攻击、远程服务攻击、邮件服务器攻击、远程登陆攻击、SQL 注入攻击、CGI 访问攻击、IIS 服务器攻击、p2p、IM、网络游戏以及其他违规行为等进行实时检测告警。

2.3 超低的误报率和漏报率

采用 TCP/IP 数据重组技术、应用程序识别技术、完整的应用层状态追踪、应用层协议分析技术及多项反 IDS 逃避技术，提供业界超低的误报率和漏报率。

2.4 更直观的策略管理结构

360 入侵检测系统采用了全新的策略管理结构，结合新的资源对象、策略对象、策略派发、响应管理等功能，用户可以方便快捷的建立适用不同环境的攻击检测策略。

2.5 细致详尽的全方位安全可视化

360 入侵检测系统是基于 360SecOS 的多级立体全方位可扩展的流可视框架，开发出多种详尽的流实时可视功能。360 入侵检测系统提供基于接口的流量统计、基于应用的流量统计、基于 p2p 的流量统计；支持应用识别分布及各应用具体分布情况；支持抗攻击事件、IDS 事件、内容过滤事件等统计和报表。支持根据时间、IP、应用、事件类别、攻击类型等要素查询和定制报表，并可导出。提供多种统计方式，如显示接口 IN/OUT 流量图、显示接口 IN/OUT 最活跃的 10 个内部 IP/外部 IP、Top10 应用分布图等。可对接口流量/应用/协议的异常状态进行告警，并以 Email 或 syslog 等方式通知管理员。

2.6 基于全局理念的安全指导指数

360 入侵检测系统通过提供各种详细复杂的安全状态、流量统计和流可视，辅以一定算法和关联、综合分析，提炼出网络环境中的网络安全指数、应用安全指数以及应用安全等级等指导、警示性数据，从总体评估网络的风险情况，为安全管理提供参考。

3.技术优势

3.1 硬件加速包截获技术

在整个体系架构中，360 入侵检测系统在底层采用了硬件加速包截获技术，结合新的芯片处理设备，大幅度提高了监听网卡的抓包能力，保证了信息收集的完整，即使在大流量负载情况下也能确保不丢包。

3.2 基于状态的协议分析技术

360 入侵检测系统的协议分析技术，通过对已知协议和 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，360 入侵检测系统拥有检测协议异常、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。360 入侵检测系统目前支持 Telnet、FTP、HTTP、SMTP、SNMP、DNS 等多达数十种的主流应用层协议。

基于状态的协议分析技术是在已知通信协议上做进一步的深入处理。它能够根据数据包中通信协议的状态而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，引擎将数据包解析、还原，将真实的应用数据与签名库进行攻击特征的匹配，能够辨别通信行为真实意图的能力，而不会受到像 URL 编码、干扰信息、IP 分片、变换端口等入侵检测系统规避技术的影响，增强了检测攻击的准确度，减少了误报的概率。

3.3 应用层协议分析

当 TCP/IP 协议状态检测后，再将数据包送到应用层，在应用层，采用了完整的应用层协议分析技术。360 入侵检测系统协议分析技术是一种新型的入侵检测技术，它充分利用了网络协议的高度有序性，使系统在每一层上都沿着协议栈向上解码，因此可以使用所有当前已知的协议信息，来排除所有不属于这一个协议结构的攻击。

3.4 成熟的流检测技术，提升性能和准确性

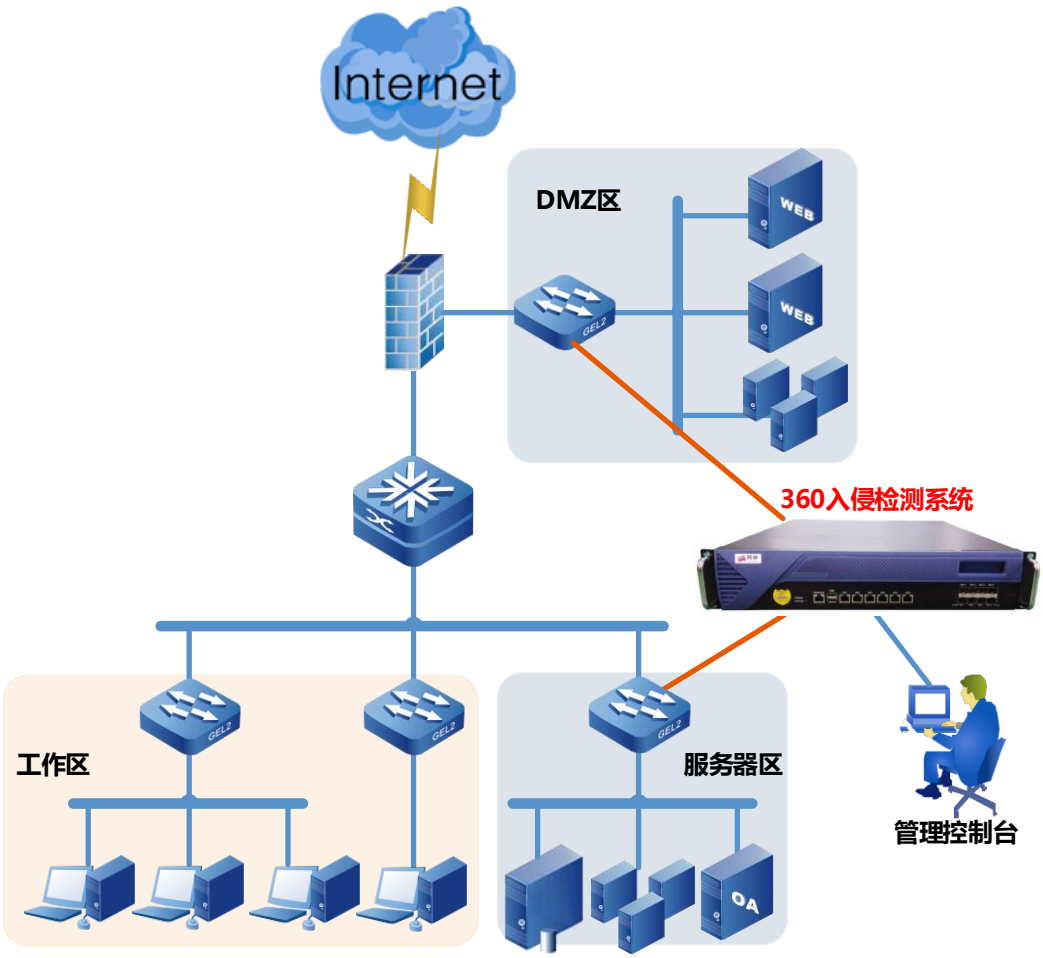
360 入侵检测系统采用的流检测技术综合运用了 ACL 高效分流技术和会话状态跟踪技术，结合跨包检测、关联分析和“零”缓存等技术，大幅提升了报文检测的准确性和处理性能。一举克服了传统的 IDS 基于文件检测的实时性差和基于单包检测的准确性差的技术缺陷。

3.5 深度数据分析

入侵检测系统的数据分析是发现可疑攻击行为的重要过程，360 入侵检测系统采用了深度数据分析技术，通过多次的数据查询和统计操作，用户可以从大量的事件告警中快速准确的找到所需要的数据。

4.典型应用

360 入侵检测系统产品探测器通常部署在网络关键链路（外网出口链路、主要服务器群访问链路、其他关键链路）的旁路位置，对网络流量进行实时采集并进行深度分析，将发现的攻击或威胁进行记录并实时报警，用户可以随时对用户网络目前正在发生或是可能构成潜在威胁的安全事件进行调用查看、分析和确认。



5.客户价值

全面检测与响应

系统内置超过 4000 条的攻击事件特征库，实时检测各种入侵攻击及违规行为，并通过邮件、Syslog 等多种响应方式通知管理员采取进一步的防护措施，也可通过会话重置功能进行实时阻断。

精准识别

依托 360 公司强大的安全分析团队以及系统内置的精准特征库，做到不漏报、不误报，节约管理员处置成本。

风险可视

依靠系统提供的多维度事件分析技术，全面掌握网络内的各种威胁和风险，及时调整安全策略或借助其他措施予以及时应对。

行业监管合规

产品通过公安部、保密局等多个权威机构的认证测评，可以满足等级保护、分级保护等行业标准的要求，增强用户的合规能力。