360 入侵防御系统

白皮书

目录

1.产品概述

针对日趋复杂的应用安全威胁和混合型网络攻击，360 企业安全集团推出完善的安全防护方案。360 入侵防御系统（简称 360IPS）全线产品采用多核芯片，基于自主研发的、充分利用多核优势的 360SecOS 软件系统，采用多层次深度检测技术和多扫描引擎负载分担与备份技术，完全满足当前网络带宽和网络攻击泛滥、应用越来越复杂的趋势和需求。

360IPS 作为一种在线部署的产品，通过准确监测网络异常流量，自动应对各类攻击流量，及时将安全威胁阻隔在企业网络外部。入侵防御产品弥补了防火墙、入侵检测等产品的不足，提供动态的、深度的、主动的安全防御，为企业提供了一个全新的入侵防护解决方案。

2.产品特色

2.1. 实时主动的安全防御能力

360 入侵防御系统以在线的方式部署在客户网络的关键路径上，通过对数据流进行 2 到 7 层的深度分析，具有能精确、实时地识别和阻断病毒、木马、SQL 注入、跨站脚本攻击、DoS/DDoS、扫描等安全威胁，还具有防火墙、文件控制、URL 过滤、关键字过滤、P2P、IM 等网络滥用流量的识别和限制功能。

360 入侵防御系统检测引擎结合了异常检测与攻击特征数据库检测的技术，它同时也包含了深层数据包检查能力，除了检查第四层数据包外，更能深入检查到第七层的数据包内容，以阻挡恶意攻击的穿透，同时不影响正常程序的工作。

360 入侵防御系统的检测引擎提供多种检测模式来保证准确度，并且在不影响网络性能的状况下，提供客户最佳的保护；在 360 入侵防御系统上使用的检测方法包括：

- **状态模式检测（Stateful Detection）**

许多的攻击是试图推翻通讯协议状态。基于多年 TCP/IP 的研究，360 入侵防御系统开发了一个状态检查引擎来分析协议状态，并且防止畸形数据包攻击网络。

- **攻击特征数据库模式检测（Signature-based Detection）**

360 入侵防御系统检测与保护针对应用协议和脆弱系统的攻击，具有超过 4,000 多条的攻击特征数据库，这些攻击特征数据库是由深具网络安全经验的 360 企业安全集团安全研究团队开发制定。

- **缓冲区溢出检测（Buffer-overflow Detection）**

缓冲区溢出是一种黑客经常利用的通用技术，例如冲击波攻击就是利用微软的 RPC DCOM 漏洞感染网络上数百万的主机。360 入侵防御系统可以通过内置特征库阻挡缓冲区溢出攻击，阻止黑客取得非法的授权进入网络。

- **木马/后门检测（Trojan/Backdoor Detection）**

黑客使用木马和后门程序取得非法授权进入个人计算机或服务器。基于现有的木马和后门程序的技术，360 入侵防御系统可以通过内置特征库检测并防止木马和后门程序。

- **拒绝服务/分布式拒绝服务检测（DoS/DDoS Detection）**

黑客可以在不需要任何授权的情况下发送大量的数据包进入网络，这些流量可以是单一个数据包或是自动发送分布式拒绝服务攻击的工具所产生的攻击信号，一些蠕虫也可以发送大量的扫描讯号进入网络，360 入侵防御系统利用拒绝服务/分布式拒绝服务检测机制防止此类型的所有攻击。

- **访问控制检测（Access Control Detection）**

一些会造成敏感信息泄漏的网络行为是非常危险的，360 入侵防御系统利用攻击特征数据库来防止这些行为的发生，360 入侵防御系统也提供最大的灵活性，让客户可以定制专属的策略。此项功能可让客户自行制定网络第三层至第七层的防御策略。

- **Web 攻击检测（Web Attack Detection）**

Web 服务在全世界被广泛地使用，但是却发现相当多的弱点，利用这些弱点是相当容易的，信息可以通过因特网自由分享，为了防止黑客利用 Web 服务的弱点，360 入侵防御系统可以针对 Web 服务器的弱点进行保护。

- **弱点扫描/探测检测（Vulnerability Scan/Probe Detection）**

为了得到信息和系统的漏洞，黑客会在网络上发送检查数据包来扫描系统，360 入侵防御系统可以检测出这些弱点扫描/探测的数据包，并提供最好的保护。

- **基于邮件的攻击检测（Mail-based Attack Detection）**

基于邮件的攻击在现在是很普通的，例如 W32/Mydoom 引起全世界几十亿的金融损失，360 入侵防御系统提供 SMTP 过滤功能及病毒数据库以防止病毒侵入邮件服务器。

- **蠕虫检测（Worm Detection）**

网络蠕虫会如此的令人讨厌是因为它能够迅速的繁殖，并因此引起全世界网络的异常甚至是瘫痪，360 入侵防御系统能够阻挡蠕虫的攻击，保障网络的安全与干净。

- **异常检测（Anomaly Detection）**
  - **协议异常检测（Protocol Anomaly Detection）**

360 企业安全集团安全团队研究与分析因特网的协议和标准，一般的因特网服务器遵循这些标准提供稳定的服务，黑客经常利用破坏这些标准协议的方式强迫进入，360 入侵防御系统检测并清除这些异常数据包，保障服务器免遭受这些未知数据包的攻击。

  - **流量异常检测（Traffic Anomaly Detection）**

当网络被攻击时，网络流量异常的增加是很正常的，依据多年网络攻击事件处理的经验，360 企业安全集团安全团队建立了最佳的规则，并将此统计分析方法整合进 360 入侵防御系统，提供最佳的检测与防御。

  - **扫描/探测检测（Scan/Probe Detection）**

主机计数是黑客了解网络拓朴与主机状态的一种方式，主机/端口扫描是黑客决定下一步攻击方式的重要因素，360 入侵防御系统会在黑客试图扫描时即检测并加以防御，隐藏黑客想要取得的信息并保障整个网络的安全。

  - **洪流检测（Flooding Detection）**

网络洪流攻击会造成服务器与网络设备许多不必要的负荷，有时这些攻击可以造成核心路由器的死机，使得网络系统完全瘫痪，360 入侵防御系统能够检测并阻挡此类的攻击事件，保护服务器及网络系统。

  - **拒绝服务/分布式拒绝服务检测（DoS/DDoS Detection）**

拒绝服务/分布式拒绝服务攻击是网络管理员的恶梦，360 入侵防御系统能分析网络流量来检测与阻挡拒绝服务/分布式拒绝服务的攻击。

- **其它领域的检测（Other Detection Scopes）**

360 入侵防御系统提供网络应用层检测技术控制多种网络行为：

- **实时聊天程序（Instant Messenger）**

360 入侵防御系统是一个网络第七层设备，能够检测出网络第七层应用层的不同行为，例如 QQ、MSN 的聊天、QQ、MSN 文件传输、QQ、MSN 电视会议等，它们不以某些特定端口提供服务，360 入侵防御系统能够针对不同的行为分别做出不同的处理。分开制定安全策略，使得 IT 经理能有效地管理他们的安全策略。

- **流媒体和在线下载程序（P2P）**

P2P 流媒体和在线下载程序会严重消耗网络带宽，并造成网络速度变慢，通过使用 P2P 在线下载程序也可能对外泄漏内部机密信息，360 入侵防御系统是一个网络第七层的设备，可以轻易的检测出迅雷、网际快车等各种 P2P 在线下载程序和 PPStream、QQLive 等流媒体应用程序，IT 经理能有效地通过 360 入侵防御系统管理他们的安全策略。

- **网页邮件/论坛（Web Mail/ Post）**

利用网页邮件服务器与论坛发出机密信息是非常容易的，通过 360 入侵防御系统，IT 经理可以轻松并有效地管理此类行为。

- **指定网站过滤**

360 入侵防御系统支持指定网站过滤功能，客户可以自定义建立 URL 白名单和黑名单。

- **垃圾邮件（SPAM）**

360 入侵防御系统能通过自定义关键字来进行垃圾邮件的过滤。

2.2. 优异的产品性能和自身安全性

360 入侵防御系统依赖先进的体系架构、高性能专用硬件，在实际网络环境部署中性能表现优异，具有线速的分析与处理能力。

360 入侵防御系统采用专门设计了安全、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、吞吐量；操作系统经过优化和安全性处理，保证系统的安全性和抗毁性。

2.3. 虚拟化、弹性化的管理方式

360 入侵防御系统提供虚拟 IPS 的弹性设置，用户可以利用一台 IPS 设备，依照实际的网络规划，把网络端口做不同的划分，成为虚拟的 IPS 设备来运行，每一个虚拟的 IPS 设备可以拥有独立的安全防御策略，这样运用可以大大增加 IPS 在大型网络架构中的使用弹性。

2.4. 高度容错能力

360 入侵防御系统支持失效开放（Fail bypass）机制，当出现软件故障、硬件故障、电源故障时，系统 bypass 电口自动切换到直通状态以保障网络可用性，避免单点故障，不会成为业务的阻断点。

360 入侵防御系统的工作模式灵活多样，支持 inline 主动防御、旁路检测方式，能够快速部署在各种网络环境中。

360 入侵防御系统支持通过链路冗余的双机热备份和负载均衡技术实现设备安全长时间稳定运行。

2.5. 全面的网络安全检测、控制与展示

360 入侵防御系统具有 DDOS 防护（防 CC 攻击）、漏洞防护、URL 过滤、关键词过滤、防病毒、流量管理、应用管控等众多网络安全方面的功能，能够为用户网络提供较为全面的网络安全防护功能。

360 入侵防御系统中包含了众多安全措施的报表信息，提供了流量统计和监控、入侵监控、应用排名、AV 排名、木马排名、URL 过滤排名和关键词过滤等众多报表信息，并且可以对历史日志的事件根据不同等级和类别进行查询。

在线实时网络攻击监测

360 入侵防御系统的在线实时网络攻击监测功能可依靠入侵攻击事件的威胁程度做分类监控，提供客户实时的警示，以便采取进一步措施，阻挡与防范各类的安全事件。

网络入侵攻击事件查询

360 入侵防御系统对于网络攻击的查询可以按不同攻击类型分为四大类，第一类为应用安全类，包括 web 关键字过滤，url 过滤，文件控制，web 邮箱过滤等信息。用户可以按时间段、日志类型及日志级别进行日志的查询、删除和导出；第二类为入侵防护类，此类查询是重要攻击事件的查询，可以针对服务器主机或网络攻击种类进行网络攻击事件查询；第三类则为垃圾邮件类，此类查询是防病毒及反垃圾邮件日志信息的查询。包括基于流量的防病毒，基于文件的防病毒，反垃圾邮件等。第四类则为 DDOS 防护日志，展示 DDOS 的防护信息。

客户可通过可视选项，选择所需要的不同防护日志信息，客户可透过这些日志信息，了解到内部哪些服务器主机经常受到哪些种类的攻击，而这些攻击源是由哪些 IP 地址发出，经由这些日志报表的协助，加强经常受到攻击的服务器主机本身的安全防护，并追踪攻击来源。

在线实时流量监测

360 入侵防御系统提供在线实时流量监测功能，360 入侵防御系统提供各种不同的数据包（TCP、UDP、ICMP、IGMP、ARP、IPX）流量变化的情形，用以协助客户观察整个网络流量有无异常状况发生。

系统事件查询

对于与 360 入侵防御系统系统本身相关的事件，包括远程登陆、设备设定更改等均会被记录起来，以保障系统本身的安全，及追查网络异常的状况。

3.技术优势

3.1. 控制层面与数据层面相分离的并行计算技术

360SecOS 系统被划分为控制平面（Control Plane）、数据平面（Data Plane）以及系统虚拟层，控制平面主要负责对系统管理、协议处理、数据转发进行控制；数据平面专门负责数据转发、安全过滤业务处理，TCP/IP 协议栈的 2、3、4 层均在数据平面进行处理，每个 CPU 核心均实现了 IPV4、IPV6、MPLS 引擎，可以并行处理

网络数据包；系统虚拟层主要为控制平面和数据平面提供统一的系统服务接口，包括内存管理、时钟管理、任务管理、中断管理、文件系统管理、设备管理等；底层驱动负责各种设备的初始化、寄存器设置和控制以及报文收发控制等。

软件平台充分利用多核硬件架构以达到高性能的主要技术：

(1). 数据平面并行处理数据报文。

(2). 采用巧妙的数据分流技术，使得数据报文被均衡的分配到并行处理器。

(3). 尽量避免发送出去的报文乱序，如果乱序，由数据平面的保序模块处理后再发送出去以保证设备发送到网络的报文是有序的，以免影响整个网络和一些网络应用程序的正常运行。

(4). 实现流引擎转发和处理，同时提供快速转发路径，流转发确保安全防护得到保证，快速转发确保处理高性能。

(5). 利用芯片本身的加密引擎或者硬件加速设备，实现高速加解密或者深度内容过滤，如防病毒、反垃圾邮件等。

(6). 数据平面支持二次分发，当系统发现某个 CPU 负荷太重的时候将启动二次分发机制，把部分报文分发到负荷较轻的 CPU 上继续处理。

3.2. 丰富且全面的入侵检测技术

常见的网络入侵通常采用下面几种技术：漏洞攻击、木马植入、间谍软件和蠕虫传播，360IPS 综合运用多种技术来做到有效检测并及时阻断入侵事件的发生。

流量学习

入侵行为一般都会与正常流量或报文特征存在一定的差异，但同样入侵手法并非一成不变，网络黑客会根据情况不断的变化攻击入侵手法从而试图绕过安全设备的检测和阻断。360IPS，可以针对正常网络的行为特征进行学习，从而产生历史数据，一旦有异常出现，则能够立即启动相应的安全策略比如告警、阻断、回探等方式进行。

特征比对

特征比对是当前入侵防护最常用的技术，是当前比较有效和高效的检测方法。360企业安全集团拥有完备的特征库，客户可以选择在线实时更新或离线更新。

通常特征比对非常耗费设备性能，随着特征规则中的通配符数量的上升，IPS 产

品的性能将受到严重的挑战。360IPS 充分利用多核并行计算的优势，设计多个扫描引擎并行进行特征比对，使得设备整体性能达到非常可观的级别。

流分类与检测

一般的，入侵检测有数据两种数据检测技术：基于文件的检测和基于流的检测。

通常情况下，基于单个报文实施特征检测就可以应付大部分的入侵行为，但是比较狡猾的入侵行为往往将特征分散在不同的报文中，这样基于单包的检测则会失效，这时候就得要求入侵防护系统缓存报文并重组成文件实施检测。这种技术的优点是检测准确率较高，缺点是入侵防护系统往往由于性能不足、实时性较差而成为网络中的瓶颈。

而基流特征的检测，克服基于文件检测的实时性较差和基于单包检测的准确性较差的缺陷。360IPS 结合自身 ACL 的高效分流技术和 Session 的状态跟踪技术，通过跨包检测、关联分析和“零”缓存技术，在基于流的检测方面取得很好的效果。

抗 DDoS 攻击技术

360IPS 采用独创的多核并行计算算法和智能防护算法，对攻击行为进行智能分析，动态形成攻击特征库，可有效防护 SYN Flood、UDP Flood、ICMP Flood 等二十多种攻击，保障正常业务不受影响。

360IPS 的抗 DDoS 功能模块采用如下多种防护技术：

- 特征识别：通过分析网络流量特征，与特征库比对扫描，可以有效识别常用的攻击。
- 反探校验：在识别和判断是否是攻击的时候，可以验证源地址和连接的有效性，防止伪造源地址和连接的攻击。
- 状态监测：支持简单包过滤、状态包过滤和动态包过滤，可以分别选用，根据五元组信息进行访问控制。
- 智能学习：360 入侵防御系统的防护采用多种算法，除了传统的统计丢包算法，还通过智能学习、关联分析等算法使得 SYN Flood/UDP Flood 等具有良好效果。检查通信过程是否符合 TCP/IP 协议的完整性，并对 HTTP、DNS、P2P 等协议进行深度分析，支持对 SYN/SYN ACK/ACK Flood 攻击、HTTP Get Flood 攻击、DNS Query Flood 攻击、CC 攻击的防护，支持 BT、电驴等 P2P 协议的

识别、阻断和限制。

- 连接限制：支持对具体 IP 的并发连接和新建连接限制，可根据五元组限制并发连接总数和新建连接速率限制，可防止大规模攻击和蠕虫扩散的发生。
- 流量控制：通过内置的 QoS 硬件引擎，支持最大带宽、保证带宽、优先级，从而有效的实施网络资源的合理分配。

3.3. 高效的检测引擎体系结构

1) 零拷贝技术

直接存储器访问（DMA）是一种不需要处理器参与的传输，在系统存储器和外设之间进行传输数据块的技术。 DMA 不仅减轻系统处理单元的工作，而且以比处理器的读取和写入速率高得多的速率传输数据。360 入侵防御系统采用的 Scatter-Gather DMA 增强了这种技术，提供从一个非连续的存储器块到另一个存储器，采用通过一系列较小的连续数据块传输的方法进行数据传输。数据包以 Scatter-and-Gather 方式主动通过千兆网卡 DMA 进入内存后就不再拷贝，有效地减少内存存取次数。

2) 核心层优化

所有报文的解析与比对都由核心层（Kernel）进行，完全不用通过核心层与应用层之多余的转换，因此不用进行内存拷贝，从而有效地减少内存存取次数。

3) 实时特征比对

360 入侵防御系统采用的特征比对引擎能直接比对特征码格式，相对于一般只对报文内容进行文字搜索的作法，引擎同时整合了第四层的特征内容，减少了处理器额外比对并且有效降低误判，实现线速对比。

4.典型应用

4.1. 部署 IPS 的两个阶段

为了让 IPS 能准确无误的保护您的网络，部署 IPS 设备应该按照以下的两个阶段

进行：

第一阶段：IPS 以监测模式工作，只检测攻击并告警，不进行阻断

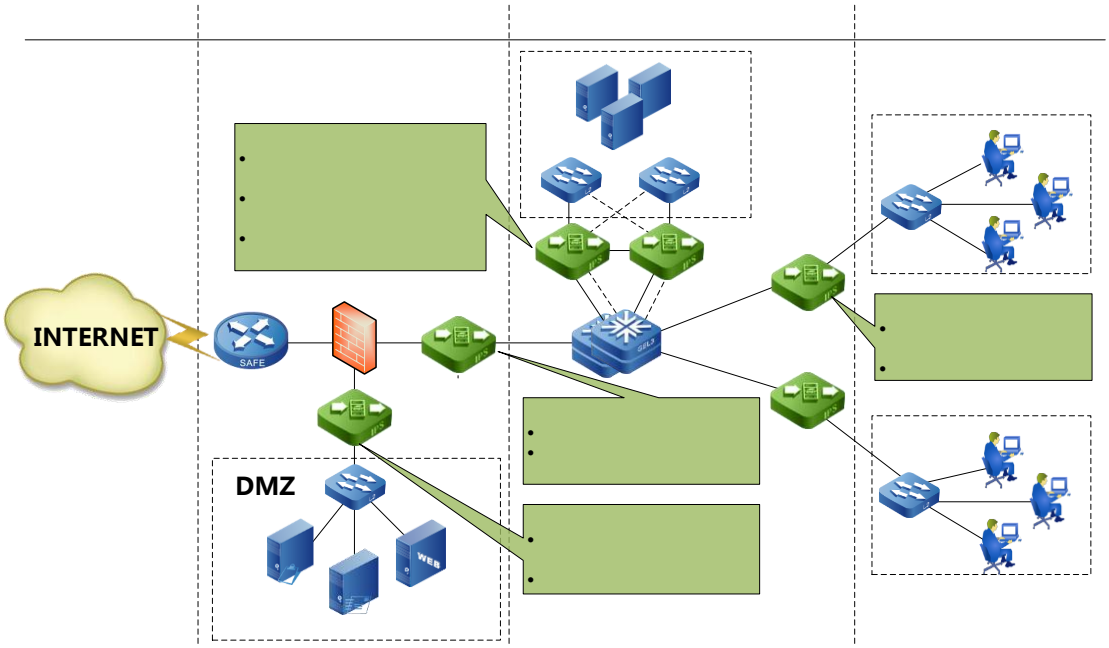
首先，将 IPS 的工作模式设置为 IPS 监视模式，在该模式下，IPS 的检测引擎将根据安全策略对网络中通过的数据进行检测，如果用户设置了对攻击数据包的阻断功能，IPS 会产生相应的阻断报警，但是不会采取任何阻断或流量控制操作。这种模式主要用于首次部署时对用户网络环境的学习与策略优化阶段，根据检测到的网络中可能出现的攻击行为，对攻击签名特征库和阈值等参数做出调整，减少 IPS 产生误报的可能性。

另外在此模式下，用户可以观察 IPS 设备的加入会不会对原有的网络应用产生影响，以确保 IPS 的性能能够满足原有网络应用的需求。

第二阶段：IPS 以阻断模式工作，全面检测，全面防护

在经过第一阶段的学习、调整和适应后，已经可以确认 IPS 能够以监视方式正常运行，并且不会阻断正常合法的网络数据包，这时候就可以开启 IPS 的防御功能，进入阻断攻击、全面防御的阶段。

4.2. 完整的部署带来无处不在的防护能力



结合上图中的综合部署方案，我们能够清晰的看到 360 入侵防御系统所带来的防护效应。

■针对应用程序防护

360 入侵防御系统提供扩展至用户端、服务器、及第二至第七层的网络型攻击防护，如：蠕虫与木马程序。利用深层检测应用层数据包的技术，360 入侵防御系统可以分辨出合法与有害的封包内容。最新型的攻击可以透过伪装成合法应用的技术，轻易的穿透防火墙。而 360 入侵防御系统运用重组 TCP 流量以检视应用层数据包内容的方式，以辨识合法与恶意的数据流。大部分的入侵防御系统都是针对已知的攻击进行防御，然而 360 入侵防御系统运用漏洞基础的过滤机制，可以防范所有已知与未知形式的攻击。

■针对网络架构防护

路由器、交换器、DNS 服务器以及防火墙都是有可能被攻击的网络设备，如果这些网络设备被攻击导致停机，那么所有企业中的关键应用程序也会随之停摆。而 360 入侵防御系统的网络架构防护机制提供了一系列的网络漏洞过滤器以保护网络设备免于遭受攻击。

■针对性能保护

是用来保护网络带宽及主机性能，免于被非法的应用程序占用正常的网络性能。如果网络链路拥塞，那么重要的应用程序数据将无法在网络上传输。非商用的应用程序，如点对点文档共享 (P2P)应用或实时通讯软件 (IM) 将会快速的耗尽网络的带宽，通过对具体应用的有效控制，能够从根本上缓解因上述问题的涌现给网络链路带来的压力。

5.客户价值

洞悉威胁全面防护

系统内置超过 4000 条攻击事件特征库，可以实时检测防护各种入侵攻击及违规行为。辅以应用特征库、病毒特征库，全面检测网络各种形式的威胁并实时予以响应。

精细控制与误报避免

根据业务需要，不同网络接口可以配置不同的安全策略和响应方式，方便管理员灵活规划设计。同时，依托于 360 公司强大的安全分析团队以及系统内置的精准特征

库，确保不误杀关键业务。

业务连续保证

内置软硬件 bypass 机制，即使系统发生故障也不会影响业务系统的正常工作，保障业务永续开展。

业务平滑扩容

随着业务的增长，用户网络环境愈发复杂，该产品可以横向扩容，多台产品组成系统集群，最大化节约总拥有成本。