第4章 典型案例

4.1 企业网络入侵检测解决方案

4.1.1 应用背景及需求分析

1. 应用背景

随着互联网的发展，网络变得越来越复杂，也越来越难以保证安全。为了共享信息，实现流水线操作，各公司还将他们的网络向商业伙伴、供应商及其他外部人员开放，这些开放式网络比原来的网络更易遭到攻击。此外，他们还将内部网络连接到互联网（Internet），想从 Internet 的分类服务及广泛的信息中得到收益，以满足重要的商业目的，包括：

（1）让员工访问 Internet 资源。员工利用 Internet 中大量的信息和设施提高他们的工作效率。

（2）允许外部用户通过 Internet 访问内部网。企业需要向外部用户公开内部网络信息，包括客户、提供商和商业伙伴。

（3）将 Internet 作为商务基础。Internet 最吸引人的一个地方在于，与常规商业媒介相比，它能使各公司接触到的客户范围更广，数量更多。

虽然连入 Internet 有众多好处，但它将内部网络暴露给数以百万计的外部人员，大大增加了有效维护网络安全的难度。为此，技术提供商提出了多种安全解决方案，以帮助各公司的内部网免遭外部攻击，这些措施包括防火墙、操作系统安全机制（如身份确认和访问权限等级）及加密。但即使采用各种安全解决方案，黑客也总能设法攻破防线，而且网络为了适应不断变化的商业环境（如重组、兼并、合并等），不得不经常改动，这就使有效维护安全措施这一问题更加复杂。

近年来，全球重大安全事件频发，2013 年曝光的“棱镜门”事件、“RSA 后门”事件、2017 年爆发的新型“蠕虫式”勒索软件 WannaCry 等更是引起各界对信息安全的广泛关注。网络攻击从最初的自发式、分散式的攻击转向专业化的有组织行为，呈现出攻击工具专业化、目的商业化、行为组织化的特点。随着获利成为网络攻击活动的核心，许多信息网络漏洞和攻击工具被不法分子和组织商品化，以此牟取暴利，从而使信息安全威胁的范围加速扩散。个人信息及敏感信息泄露的信息安全事件，可能引发严重的网络诈骗、电信诈骗、财务勒索等犯罪案件，并最终导致严重的经济损失；政府机构、工业控制系统、互联网服务器遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫

痪，造成灾难性后果，严重危害国家经济安全和公共利益。全球整体网络安全形势不容乐观，国际间网络空间竞争形势日益紧张。

面对日益严峻的网络空间安全威胁，美国、德国、英国、法国等世界主要发达国家纷纷出台了国家网络安全战略，明确网络空间战略地位，并提出将采取包括外交、军事、经济等在内的多种手段保障网络空间安全。2011 年 4 月，美国发布了《网络空间可信身份国家战略》，首次将网络空间的身份管理上升到国家战略的高度，并着手构建网络身份生态系统。这一战略的出台表明美国已高度认识到网络身份安全在保障网络空间安全中的重要战略地位。从各国的战略规划的内容看，一方面政府希望通过顶层安全战略的制定引导本国安全产业的发展；另一方面，对网络空间的保护逐渐上升到和传统疆域保卫同等的地位，通过成立网络安全部队加速军队信息安全攻防的研发，积极应对未来有可能发生的网络战争。

随着我国不断完善网络安全保障措施，网络安全防护水平进一步提升。然而，信息技术创新发展伴随的安全威胁与传统安全问题相互交织，使得网络空间安全问题日益复杂隐蔽，面临的网络安全风险不断加大，各种网络攻击事件层出不穷，如图 4-1 所示，根据国家计算机网络应急技术处理协调中心（简称 CNCERT/CC）报告，网络安全事件依然持续不断爆发。国家互联网应急中心报告，2016 年，我国移动互联网恶意程序数量持续高速上涨且具有明显趋利性；来自境外的针对我国境内的网站攻击事件频繁发生；联网智能设备被恶意控制，并用于发起大流量分布式拒绝服务攻击的现象更加严重；网站数据和个人信息泄露带来的危害不断扩大；欺诈勒索软件在互联网上肆虐；具有国家背景黑客组织发动的 APT 攻击事件直接威胁了国家安全和稳定。

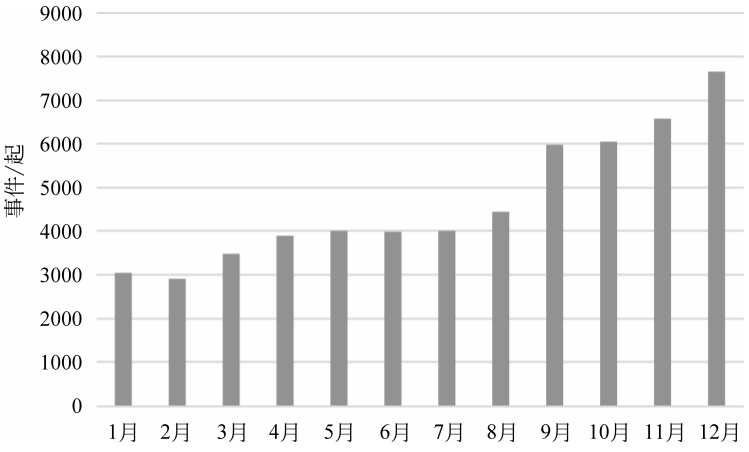

图 4-1　2016 年我国网络安全事件的发生情况

2. 需求分析

现在许多用户已经意识到这一点，使用了许多安全设施保护内部网络使其免遭外部攻击。实际上，由心怀不满的雇员或合作伙伴发起的内部攻击占网络入侵的很大一部分。据统计，80％的计算机犯罪来源于内部威胁。

因此需要一种独立于常规安全机制的安全解决方案——能够破获并中途拦截那些能

够攻破网络第一道防线的攻击。这种解决方案就是“入侵检测系统”，利用“入侵检测系统”连续监视网络通信情况，寻找已知的攻击模式，当它检测到一个未授权活动时，软件会以预定方式自动进行响应，报告攻击、记录该事件或是断开未授权连接。“入侵检测系统”能够与其他安全机制协同工作，提供真正有效的安全保障。

3. 对有效的攻击识别和响应的要求

要将网络安全保护得滴水不漏是不太可能的，即使是按照预先制定的安全策略保护网络，也是一项非常艰巨的任务。即使是被保护的很好的网络，也需要不断更新，以修补新出现的漏洞。保护网络是一项持久的任务，它包括保护、监视、测试，以及不断的改进。“入侵检测系统”必须满足许多要求，以提供有效的安全保障，主要有以下要求。

(1) 实时操作：攻击识别和响应软件必须能够实时检测、报告可疑攻击，并做出实时反应。那些仅能在事后记录事件、提供校验登记的软件效率是不高的。这种事后检查的软件就像是在盗贼们扬长而去之后才报警的防盗警铃。此外，许多攻击者在攻入时就擦掉了记录，所以仅扫描事件记录是检查不到攻击的。

(2) 可以升级：正如有新的计算机病毒不断涌现一样，黑客们总能找到新的方法侵入计算机系统，所以攻击识别和响应软件必须能够将已知的入侵模式和未授权活动不断增加到知识库中。

(3) 可运行在常用的网络操作系统上：软件必须支持现有的网络结构。也就是说，它必须支持现有的网络操作系统，如 Windows XP、Windows 7、Windows Server 2003/2008/2012。

(4) 易于配置：在无需牺牲效率的条件下，易于配置。攻击识别和响应软件应提供默认配置，管理员可以迅速安装并随着信息的积累对其不断优化。此外，软件还应提供样本配置，指导管理员安装系统。

(5) 易于改变安全策略：现在的商业环境是动态的，公司由于许多因素而不断变化，包括重组、合并和兼并。所以，安全策略也随之改变，为了保证有效性，攻击识别和响应软件应易于适应改变了的安全策略，这保证了安全策略在实际运行中和理论上一样有效。

(6) 不易察觉：该软件应该以不易被察觉的方式运行。也就是说，它不会降低网络性能。它对被授权用户是透明的，所以它不会影响生产率。此外，它不会引起入侵者的注意。

4.1.2 解决方案及分析

1. 解决方案

网神 SecIDS 3600 通过高效的模式匹配、异常检测、协议分析等技术手段，对用户网络链路的实时监控，期间发现大量的 DoS/DDoS、Web 攻击等异常行为攻击特征，设备能及时向管理员发出警告信息，根据用户实际环境监测统计分析，为管理员提供及时准确的网络行为分析数据，有助于针对性地对网络采取一些规避补救措施，保障了用户网络的安全及可靠性。

网神 SecIDS 3600 可以通过单机部署的方式部署在服务器上。单机部署方式即把管理控制台安装在一台功能较强大的计算机上。虽然集中式部署的计算能力可能不如分布式部署，但这种部署方式有利于管理，对于一般的中小企业很适用。这种模式适合于负载不是很重，设备较少的网络环境。

单机部署网络如图 4-2 所示，其显示的是最具代表性的单机部署网络拓扑结构。经过安全需求分析，用户一般比较关注的是服务器区和 Internet 出口这两个部分。那么，在这两个部分部署一套独立的入侵检测系统就能够满足安全需求。用户如果需要增加监控区域，只选择多端口的高端入侵检测设备即可满足需求。

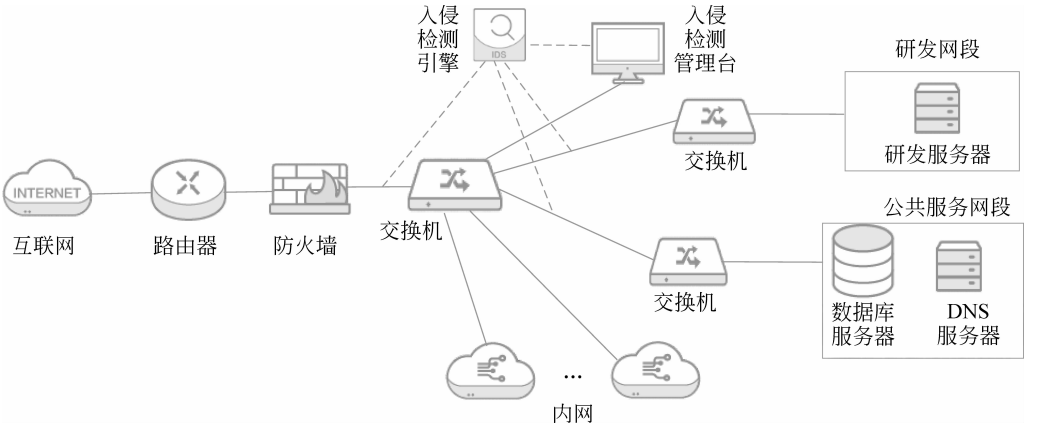

图 4-2　单机部署网络

2. 产品功能及特点

SecIDS 3600 入侵检测系统是基于网络安全技术和黑客技术多年研究的基础上开发的网络入侵检测系统。SecIDS 3600 入侵检测系统是一项创新性的网络威胁和流量分析系统，它综合了网络监控和入侵检测功能，能够实时监控网络传输，通过对高速网络上的数据包捕获，进行深入的协议分析，结合特征库进行相应的模式匹配，通过对以往的行为和事件的统计分析，自动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，帮助企业最大限度地保护公司内部的网络安全。

1）产品功能

（1）部署和管理功能。

提供中文化的管理界面；提供检测策略模板，并可针对不同的网络环境派生新的策略，方便用户根据实际情况制定适合企业自身环境的安全策略；支持安全事件数据库容量预警及异常处理功能，以防止因存储空间的不足导致的数据丢失。

（2）检测与报警能力。

提供对多种应用的检测能力，包括间谍木马、恶意软件、蠕虫病毒及 DDoS 等的多种攻击威胁检测；提供在线和本地的升级方式，平均升级周期不大于 1 周；产品提供多种抗逃避技术：具备 IP 碎片重组与 TCP 流重组功能、具备抗 HTTP 变形逃避功能等；报警信息提供关于攻击的详细内容：如 IP 地址、端口、时间和类型等常规信息；支持邮件、Syslog

等多种高级报警方式；提供对 IEEE 802.1q 封装数据包的解析及检测能力。

(3) 报表与日志审计。

入侵检测系统相关日志的导出；支持统计和查询报告的导出。

(4) 自身安全指标。

支持设备的带外管理，监听端口支持隐秘模式，无需 IP 地址和网络配置；支持 Console 配置界面管理；支持用户分角色管理。

2) 产品特点

(1) 配置简单、使用方便。

SecIDS 3600 入侵检测系统的平台经过专门优化及加固，使用更加安全、方便。用户经过简单配置，接电即可使用。

(2) 检测基于网络的攻击。

SecIDS 3600 网络传感器检查所有包的头部，从而发现恶意的和可疑的行动迹象。例如，许多来自 IP 地址的拒绝服务型(DOS)和碎片包型(Teardrop)的攻击只能在它们经过网络时检查包的头部才能发现。这种类型的攻击都可以在 SecIDS 3600 中通过实时监测网络数据包流而被发现。

SecIDS 3600 网络传感器可检查有效负载的内容，查找用于特定攻击的指令或语法。例如，通过检查数据包有效负载可以查到黑客软件，而正在寻找系统漏洞的攻击者毫无察觉。

(3) 实时检测和响应。

SecIDS 3600 可以在恶意及可疑的攻击发生的同时将其检测出来，并做出快速的通知和响应。实时通知时可根据预定义的参数做出快速反应，这些反应包括收集信息、计入数据库、将告警事件发往安全运行中心等。

(4) 对网络几乎没有影响。

SecIDS 3600 完全不会造成网络的时延。SecIDS 3600 网络传感器仅对网络数据流进行监控，复制需要的包，完全不会对包的传输造成延迟。唯一可能造成延迟的情况是网络传感器发出中断连接的数据包，当然受到影响的只有攻击者。

SecIDS 3600 增加的网络流量也微不足道。增加的网络流量取决于分布式配置的情况，主要因素取决于网络传感器向控制台传输数据的数量和频繁程度。

(5) 攻击者不易转移证据。

SecIDS 3600 使用正在发生的网络通信进行实时攻击的检测，所以攻击者无法转移证据。被捕捉的数据不仅包括攻击的方法，而且还包括攻击的源地址和目的地址。许多黑客都熟知审计记录，他们知道如何操纵这些文件掩盖他们的作案痕迹，但他们很难抹去被入侵检测系统实时记录下来的数据。

3) 产品优势

(1) 强大的分析检测能力。

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，并显著地提高系统的性能，能够适应日益复杂的网络环境。

(2) 基于状态的协议分析。

基于已知协议和 RFC 规范的深入理解，SecIDS 3600 入侵检测系统具有强大的检测协议异常、协议误用的能力，解决了以往基于单纯模式匹配技术的 IDS 产品片面依赖攻击特征签名数量检测攻击的弊端，提高了检测准确性和效率。SecIDS 3600 入侵检测系统目前支持 Telnet、FTP、HTTP、SMTP、DNS 等数十种主流应用层协议。

(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技术、应用层协议分析技术及多项反 IDS 逃避技术，支持在复杂的网络环境中部署，提供业界超低的误报率和漏报率。

(4) 丰富的事件响应方式。

针对不同类型数据包流量传递的过程，入侵检测系统可在发现攻击的当下通过已定义好的检测行为动作加以检测，系统提供事件记录、通过邮件警告、Syslog 报警等。

(5) 更直观的策略管理结构。

SecIDS 3600 入侵检测系统采用全新的策略管理结构，结合新的策略分类、策略派发、策略响应管理等功能，用户可以方便快捷地建立适用不同环境的攻击检测策略。

(6) 灵活的签名分类。

基于网络应用、风险级别和攻击类型等分类原则，用户可以更准确、快捷地查找到所关注的签名类别。

4.2 用户网络入侵防御解决方案

4.2.1 应用背景及需求分析

1. 应用背景

通过对大量用户网络的安全现状和已有的安全控制措施进行深入分析可知，很多用户网络中仍然存在着大量的安全隐患和风险，这些风险对用户网络的正常运行和业务的正常开展构成严重威胁，主要表现在以下 3 方面。

1) 操作系统和应用软件漏洞隐患

用户网络多由数量庞大、种类繁多的软件系统组成，有系统软件、数据库系统、应用软件等，尤其是存在于广大终端用户办公桌面上的各种应用软件不胜繁杂，每个软件系统都有不可避免的潜在的或已知的软件漏洞，每天软件开发者都在生产漏洞，每时每刻都可能有软件漏洞被发现、利用。无论哪一部分的漏洞被利用，都会给企业带来危害，轻者危及个别设备，重者漏洞成为攻击整个用户网络的跳板，危及整个用户网络安全，即使安全防护已经很完备的用户网络，也会因一个联网用户个人终端 PC 存在漏洞而丧失其整体安全防护能力。

2) 各种 DoS 和 DDoS 攻击带来的威胁

除了由于操作系统和网络协议存在漏洞和缺陷可能遭受攻击外，现在 IT 部门还面

临着 DoS 攻击和 DDoS 攻击的挑战。

DoS 和 DDoS 攻击会耗尽用户宝贵的网络和系统资源，使依赖计算机网络的正常业务无法进行，严重损害企业的声誉并造成极大的经济损失。

3）与工作无关的网络行为

权威调查机构 IDC 的统计表明：30%～40%工作时间内发生的企业员工网络访问行为与本职工作无关，如游戏、聊天、视频、P2P 下载等。另一项调查表明：1/3 的员工曾在上班时间玩计算机游戏。

Emule、BT 等 P2P 应用和 MSN、QQ 等即时通信软件在很多网络中被不加控制地使用，使大量宝贵的带宽资源被业务无关流量消耗。这些行为无疑会浪费网络资源、降低劳动生产率、增加企业运营成本支出，并有可能因为不良的网络访问行为导致企业信息系统被入侵和机密资料被窃，引起法律责任和诉讼风险。

2. 需求分析

根据上面的安全威胁分析，需要采取相应措施消除这些安全隐患。因此，安全需求可以归纳为以下 3 方面。

（1）加强网络边界的安全防护手段，准确检测入侵行为，并能够实时阻断攻击。

（2）防御来自外部的攻击和病毒传播。

（3）加强网络带宽管控及上网行为管理。

4.2.2 解决方案及分析

1. 解决方案

网神 SecIPS 3600 入侵防御系统基于先进的体系架构和深度协议分析技术，结合协议异常检测、状态检测、关联分析等手段，针对蠕虫、间谍软件、垃圾邮件、DDoS/DoS 攻击、网络资源滥用等危害网络安全的行为，采取主动防御措施，实时阻断网络流量中的恶意攻击，确保信息网络的运行安全。

1）针对应用程序防护

SecIPS 3600 入侵防御系统提供扩展至用户端、服务器及第 2～7 层的网络型攻击防护，如防御蠕虫与木马程序。利用深层检测应用层数据包的技术，SecIPS 3600 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，轻易穿透防火墙。SecIPS 3600 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，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 SecIPS 3600 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。

2）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。网神 SecIPS 3600 入侵防御系统的网络架构防护机制提供了一系列网络漏洞过滤器，以保护网络设备免于遭受攻击。

3）针对性能保护

针对性能保护用于保护网络带宽及主机性能，免于被非法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，如点对点文档共享应用或实时通信软件将会快速耗尽网络的带宽，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。

2. 方案部署方式

1）部署拓扑

网神 SecIPS 3600 部署方式如图 4-3 所示，显示的是最具代表性的部署网络拓扑结构。经过安全需求分析，用户一般比较关注的是内网边界、数据中心、服务器区，可以在这些区域部署独立的入侵防御系统。用户如果需要增加监控区域，只选择多端口的高端入侵检测设备即可满足需求。

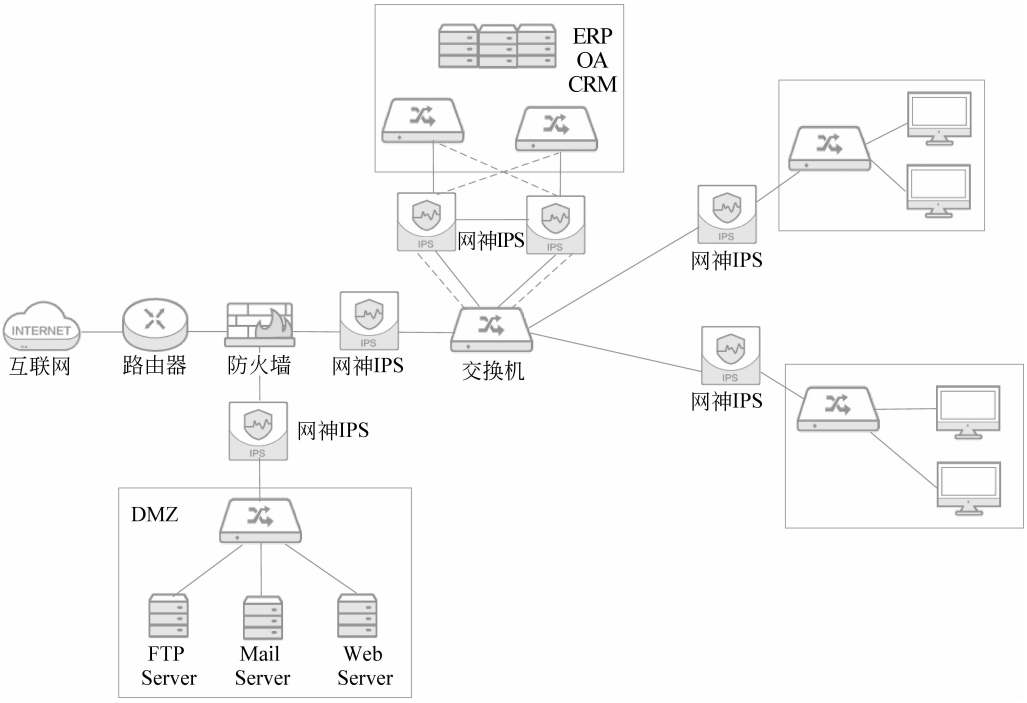

图 4-3　网神 SecIPS 3600 部署方式

2）系统优化调整

为了让 IPS 能准确无误地保护网络，部署 IPS 设备应该按照以下两个阶段进行。

（1）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。

(2) 第二阶段，IPS 以 Inline 模式工作，全面检测，全面防护。

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，这时就可以开启 IPS 的防御功能，进入阻断攻击、全面防御的阶段。

3. 产品优势

1) 新一代的检测分析技术

SecIPS 3600 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 4 层数据包外，更能深入检查到第 7 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。

SecIPS 3600 的检测引擎提供多种检测模式保证准确度，并且在不影响网络性能的状况下，提供客户最佳的保护。在 SecIPS 3600 上使用的检测方法包括：

(1) 状态模式检测(Stateful Detection)。

许多攻击是试图推翻通信协议状态。基于多年 TCP/IP 的研究，SecIPS 3600 开发了一个状态检查引擎分析协议状态，并且防止 malformed 数据包攻击网络。

(2) 攻击特征数据库模式检测(Signature-Based Detection)。

SecIPS 3600 检测针对应用协议和脆弱系统的攻击，具有超过 2600 条的攻击特征数据库，这些攻击特征数据库由深具网络安全经验的安全服务团队开发制定。

(3) 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技术，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。SecIPS 3600 可以通过内置特征库阻挡缓冲区溢出攻击，阻止黑客取得非法授权进入网络。

(4) 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，SecIPS 3600 可以通过内置特征库检测并防止木马和后门程序。

(5) 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数据包进入网络，这些流量可以是单一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扫描信号进入网络，SecIPS 3600 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。

(6) 访问控制检测(Access Control Detection)。

一些会造成敏感信息泄露的网络行为是非常危险的，SecIPS 3600 利用攻击特征数据库防止这些行为发生。SecIPS 3600 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 3～7 层的防御策略。

(7) Web 攻击检测(Web Attack Detection)。

Web 服务虽然在全世界被广泛使用，但是却被发现有很多弱点，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，SecIPS 3600 可以针对 Web 服务器的弱点进行保护。

(8) 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，SecIPS 3600 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。

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

基于邮件的攻击现在非常普遍，如 W32/Mydoom 引起全世界几十亿的金融损失，SecIPS 3600 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。

(10) 蠕虫检测(Worm Detection)。

网络蠕虫能够迅速繁殖，并引起全世界网络的异常，甚至瘫痪。SecIPS 3600 能够阻挡蠕虫的攻击，保障网络的安全与干净。

(11) 协议异常检测(Protocol Anomaly Detection)与流量异常检测(Traffic Anomaly Detection)。

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都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入侵系统，SecIPS 3600 检测并清除这些异常数据包，保障服务器免遭这些未知数据包的攻击。

当网络被攻击时，网络流量异常增加是很正常的。依据多年网络攻击事件处理的经验，安全团队建立了最佳的规则，并将此统计分析方法整合进 SecIPS 3600，提供最佳的检测与防御。

2) 优异的产品性能

SecIPS3600 入侵防御系统专门设计了安全、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。

SecIPS3600 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。

SecIPS 3600 入侵防御系统支持应用保护、网络架构保护和性能保护，彻底防护各种网络攻击行为：间谍软件/木马、蠕虫、DoS 和 DDoS 以及各种入侵行为。

3) 高可用性

SecIPS 3600 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。

SecIPS 3600 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。

4) 对攻击事件的取证能力

网络入侵防御系统除需要能检测辨别出各种网络入侵攻击，保护网络及服务器主机的安全外，还需要提供完整的取证信息，提供客户追查黑客攻击的来源，这些信息需包括入侵攻击的数据包种类、来源 IP 地址、攻击的时间等信息。

SecIPS 3600 可提供客户最完整的攻击事件记录信息，这些信息包括黑客攻击的目标