第3章 入侵防御

3.1 入侵防御的基本概念

3.1.1 入侵防御的定义

入侵防御系统(Intrusion Prevention System,IPS)是指能够检测到攻击行为(包括已知攻击和未知攻击),并能够有效阻断攻击的硬件和软件系统。入侵防御系统在线检测网络和主机,发现攻击后能实施有效的阻断,防止攻击到达目标网络或主机。从技术上来说,入侵防御系统吸取并融合了防火墙和入侵检测技术,目的是为网络提供深层次的、有效的安全防护。

IPS技术可以深度感知并检测流经的数据流量,对恶意报文进行丢弃以阻断攻击,对滥用报文进行限流以保护网络带宽资源。对于部署在数据转发路径上的IPS,可以根据预先设定的安全策略,对流经的每份报文进行深度检测(如协议分析跟踪、特征匹配、流量统计分析、事件关联分析等),一旦发现隐藏其中的网络攻击,可以根据该攻击的威胁级别立即采取抵御措施,这些措施包括(按照处理力度)向管理中心告警、丢弃该报文、切断此次应用会话、切断此次TCP连接。

3.1.2 入侵防御的分类

入侵防御系统通常可分为3种:基于主机的入侵防御系统(Host-based IPS,HIPS)、基于网络的入侵防御系统(Network-based IPS,NIPS)和应用入侵防御系统(Application IPS,AIPS)。

1. 基于主机的入侵防御系统

HIPS是直接安装在受保护机器上的代理程序,检测并阻挡针对本机的威胁和攻击。它与操作系统内核紧密捆绑在一起,监视和窃听内核系统调用,阻挡攻击,并记录日志。同时,它还监视针对某一特殊应用的数据流和环境变化,如服务器的文件位置及系统配置文件的变化,保护应用程序免受目前系统特征库中还没有特征记录的攻击。进出这个特殊系统的通信和应用程序、操作系统的行为将被监视和检查,判断其是否存在攻击迹象。

HIPS不仅可以保护操作系统,还可以保护在其上运行的应用程序,如服务器等。当检测到攻击时,HIPS会在网络接口层阻断攻击,或者向操作系统发出指令,杀死攻击进程,停止进行的攻击行为。例如,通过禁止恶意程序的执行,可以防止缓冲区溢出攻击

(Buffer Overflow Attack),这些程序被攻击者植入到被侵入(Exploited)的地址空间。通过拦截和拒绝 IE 发出的写文件(Write File)命令,可以阻挡攻击者试图通过像 IE 这样的应用程序安装后门程序(Back Door)。

因为 HIPS 监听所有到受保护主机的请求,所以必需的前提是不能影响系统的性能,并且不会阻挡正常合法的通信。如果不能满足这些需求,不管它如何有效阻挡攻击,都不能部署在主机上。

HIPS 通过在主机服务器上安装软件代理程序,防止网络攻击入侵操作系统以及应用程序。基于主机的入侵防御能够保证服务器的安全弱点不被不法分子利用。奇安信公司的 Malware Defender、Cisco 公司的 Okena、NAI 公司的 McAfee Entercept 都属于这类产品,它们在防范红色代码和 Nimda 的攻击中起到了很好的防护作用。基于主机的入侵防护技术可以根据自定义的安全策略以及分析学习机制阻断对服务器、主机发起的恶意入侵。HIPS 可以阻断缓冲区溢出、改变登录口令、改写动态链接库以及其他试图从操作系统夺取控制权的入侵行为,整体提升主机的安全水平。

在技术上,HIPS 采用独特的服务器保护途径,利用由包过滤、状态检测和实时入侵检测组成的分层防护体系。这种体系能够在提供合理吞吐率的前提下,最大限度地保护服务器的敏感内容,既可以以软件形式嵌入到应用程序对操作系统的调用中,通过拦截针对操作系统的可疑调用,提供对主机的安全防护,也可以以更改操作系统内核程序的方式,提供比操作系统更加严谨的安全控制机制。

由于 HIPS 工作在受保护的主机服务器上,它不但能够利用特征和行为规则检测,阻止诸如缓冲区溢出之类的已知攻击,还能防范未知攻击,防止针对页面、应用和资源的未授权的非法访问。HIPS 与具体的主机服务器操作系统平台紧密相关,不同的平台需要不同的软件代理程序。

HIPS 具有如下优点。

(1) 软件直接安装在系统上,可以保护系统免受攻击,如阻断程序写文件、阻止用户权限的升级等。

(2) 当移动系统接入受保护网络时,保护特定主机免受攻击。蠕虫病毒主要是无线上网的笔记本式计算机带入受保护网络的。

(3) 保护系统免受本地攻击。能够物理(直接)访问系统的人,可以通过执行优盘、CD 或本地的程序发动本地攻击。这些攻击通常是为了把用户权限提升到超级用户(Root)或管理员(Administrator)权限,以攻击网络中的其他系统。

(4) 提供最后一道防线,免受其他安全工具检测的攻击。安装在目标受害者系统上的 HIPS 是安全人员防止系统受危及的最后一个防御点。

(5) 防止相同网段上的系统、设备受到内部攻击或滥用,NIPS 只能保护在不同网段间移动的数据,在同网段、系统间发动的攻击只能被 HIPS 检测到。

(6) 保护系统免受已加密的攻击,受保护系统正是加密数据流的终点。HIPS 等加密的数据在本机解密后,检查数据及其行为,或系统的活动。

(7) HIPS 独立于网络体系结构,允许需要保护的系统位于任何网络体系中,包括过时的或不常用的网络体系,如令牌环网(Token Ring)、FDDI 等。

2. 基于网络的入侵防御系统

网络入侵防御系统(NIPS)与受保护网段是串联部署的。受保护的网段与其他网络之间交互的数据流都必须通过 NIPS 设备。当数据包通过 NIPS 时,通信将被监视是否存在攻击。攻击的误报将导致合法的通信被阻断,也就是可能出现拒绝服务(DoS)的情况,因此,极高的精确性和高级别的性能对 NIPS 至关重要。高性能是合法通信通过 NIPS 时不会延迟的保障。当检测到攻击时,NIPS 丢弃或阻断含有攻击的数据,进而阻断攻击。

NIPS 兼有防火墙和反病毒等安全组件的特性,有时也被称为内嵌式 IDS 或网关式 IDS。NIPS 串联在网络的主干线上,至少需要两块网卡:一块连接内部网络;另一块连接外部网络,所有进出的数据包都要通过它。当数据包经过任何一块网卡时,NIPS 将把它们传递到检测引擎。在这一点上,IPS 的检测引擎同任何 IDS 一样,将确定此包是否包含威胁网络安全的特征。但是,与其他 IDS 不同的是,当检测到一个恶意的数据包时,IPS 不但发出警报,还会自动采取相应的措施,以最大可能地终止恶意入侵。

在技术上,NIPS 吸取了目前 NIDS 所有的成熟技术,包括特征匹配、协议分析和异常检测。特征匹配是应用最广泛的技术,具有准确率高、速度快的特点。基于状态的特征匹配不但检测攻击行为的特征,还要检查当前网络的会话状态,避免受到欺骗攻击。

协议分析是一种较新的入侵检测技术,它充分利用网络协议的高度有序性,并结合高速数据包捕捉和协议分析,快速检测某种攻击特征。协议分析正在逐渐进入成熟应用阶段。协议分析能够理解不同协议的工作原理,以此分析这些协议的数据包,寻找可疑或不正常的访问行为。协议分析不仅基于协议标准(如 RFC),还基于协议的具体实现,这是因为很多协议的实现偏离了协议标准。通过协议分析,NIPS 能够对插入(Insertion)与规避(Evasion)攻击进行检测。异常检测的误报率比较高,NIPS 不将其作为主要技术。

总的来说,NIPS 具有如下优点。

(1) 单个通信(流量)控制点可以保护许多位于 NIPS 之下的系统。这样,组织、企业就可以很快改变网络的规模,并且更加灵活地改变网络的体系结构。

(2) NIPS 设备像单个探测器(Sensor)一样易于部署,可以保护成百上千的系统。部署几个或几十个探测器比在成百上千的系统上安装软件省去许多的时间和精力。

(3) 提供一个更宽的视野,可以发现威胁情形,如扫描、探测、攻击基于非单一系统的设备。通过工作在网络层,NIPS 比 HIPS 具有更宽的发现威胁的视野。有了这个全局的战略性高度,更容易发现威胁环境,更容易采用安全管理,主动保护实时变化的网络环境。

(4) 保护非计算机类的网络设备。并非所有的攻击都是针对受 HIPS 保护的、运行操作系统的计算机。例如,路由器、防火墙、VPN 网关、打印机等,都是易受到攻击的,需要受到保护。

(5) 与平台无关。HIPS 对于所有网络中的系统不一定都适用,如保护不常用的操作系统或应用程序。而 NIPS 不一样,它可以保护所有设备,无论是操作系统,还是应用程序。

(6) 防止网络拒绝服务攻击(DoS)、分布式拒绝服务攻击(DDoS)、面向带宽的(Bandwidth-Oriented)攻击、同步洪水(SYN Flood)攻击等。攻击的一种形式是向网络发送大

量的洪水般的无关的通信，造成网络对授权的（合法的）用户不可用，或者网络性能大幅降低。NIPS 工作在网络层，可以保护系统免受这些类型的攻击。

3. 应用入侵防御系统

IPS 产品有一个特例，即应用入侵防御系统（Application Intrusion Prevention System，AIPS），它把基于主机的入侵防护扩展成为位于应用服务器之前的网络设备。AIPS 被设计成一种高性能的设备，配置在应用数据的网络链路上，以确保用户遵守设定好的安全策略，保护服务器的安全。

AIPS 可以把 HIPS 的功能延伸到驻留在应用服务器之前的网络设备。AIP（应用入侵防御）设备是部署在应用数据通路中的一种高性能设备，旨在确保用户遵守已确立的安全策略，保护应用环境的完整性。它会检查进出设备的应用流量，根据响应得出结论，从而尽量降低 IT 部门配置及管理更新的工作量。例如，某个应用的 HTML 表格索要信用卡号码，这样一来 AIPS 会核查提供的号码，以确保其不超过 15 位。提供号码过长会导致缓冲器溢出，而字母与数字混合的号码也会导致应用系统出错。AIPS 设备能够防止诸多入侵，其中包括 Cookie 篡改、SQL 代码嵌入、参数篡改、缓冲器溢出、强制浏览、畸形数据包、数据类型不匹配以及已知漏洞。

大多数企业一度认为，防火墙、内容扫描器和入侵检测系统（IDS）足以保护网络安全，但数量激增的因特网协议，如 HTTP、SSL、SMTP 以及用 Java 和 ActiveX 创建的活动代码致使许多面向因特网的应用系统容易受到攻击。AIPS 设备处在面向因特网的应用系统前，可以阻挡攻击进入应用系统或 Web 服务器。

AIP 是一种可以在一定程度上替代主机入侵预防系统的技术，作为 HIPS 产品外的另一种技术。AIP 设备是专门针对性能和应用级安全研制的专用设备。仅向 IT 部门报告已发现的威胁并不够，应用入侵预防更进一步，它可以防止已经被发现的攻击进入关键服务器。针对应用的大部分攻击是通过服务器端口 80（HTTP）或 443（SSL）进来的，因而 AIPS 多部署于面向 Web、依赖 HTTP 或 SSL 协议的应用系统中。

总的来说，AIPS 设备具有以下技术优势。

（1）易于管理。IT 部门不必安装和配置操作系统，就可以部署专用安全设备。操作系统和安全供应商提供的升级和补丁不需要相互协调，而且用于错误通路（Error Path）上的时间对应用性能的影响较小。最终用户只把 AIPS 设备插入机架、连接至网络、制定安全策略即可。

（2）加强应用错误诊断。IT 部门可以诊断任何应用服务器的错误，AIPS 不会产生副作用。如果把安全隔离在黑盒子里面，则有助于跟踪分析整个网络的错误及性能瓶颈。

（3）提高可伸缩性。AIPS 设备与负载均衡器放在一起，为许多下游应用服务器提供入侵预防功能。IT 部门可以按需要增添业务应用服务器，不必重新配置安全产品。

（4）AIPS 工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。

（5）AIPS 的实时检测与阻断功能很有可能出现在未来的交换机上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防护功能。

3.1.3 入侵检测与入侵防御的区别

通常 IPS 看起来和防火墙相似，并且具备防火墙的一些基本功能，但是防火墙阻止所有网络流量，除了某种原因能够通过，而 IPS 通过所有网络流量，除了某种原因被阻止。IPS 能够实现积极、主动地阻止入侵攻击行为对网络或系统造成危害，同时结合漏洞扫描、防火墙、IDS 等构成整体、深度的网络安全防护体系。

IPS 是位于防火墙和网络的设备之间的设备。如果检测到攻击，IPS 会在这种攻击扩散到网络的其他地方前阻止这个恶意的通信。而 IDS 只存在于网络外，起到报警的作用，而不是在网络前面起到防御的作用。IPS 检测攻击的方法也与 IDS 不同。一般来说，IPS 依靠对数据包的检测，它会检查入网的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包进入网络。从产品的价值方面和产品的应用方面讲，IPS 与 IDS 也有不同之处。

从产品价值角度讲，IDS 注重的是网络安全状况的监管。IPS 关注的是对入侵行为的控制。与防火墙类产品、入侵检测产品可以实施的安全策略不同，IPS 可以实施深层防御安全策略，即可以在应用层检测出攻击并予以阻断，这是防火墙做不到的，当然也是入侵检测产品做不到的。

从产品应用角度讲，为了达到可以全面检测网络安全状况的目的，IDS 需要部署在网络内部的中心点，需要能够观察到所有的网络数据。如果信息系统中包含多个逻辑隔离的子网，则需要在整个信息系统中实施分布部署，即每个子网部署一个入侵检测分析引擎，并统一进行引擎的策略管理以及事件分析，以达到掌控整个信息系统安全状况的目的。

而为了实现对外部攻击的防御，IPS 需要部署在网络的边界。这样，所有来自外部的数据必须串行通过 IPS，IPS 即可实时分析网络数据，发现攻击行为立即予以阻断，保证来自外部的攻击数据不能通过网络边界进入网络。

IDS 的核心价值在于通过对全网信息的分析，了解信息系统的安全状况，进而指导信息系统安全建设目标以及安全策略的确立和调整，而 IPS 的核心价值在于安全策略的实施，即对黑客行为的阻击；IDS 需要部署在网络内部，监控范围可以覆盖整个子网，包括来自外部的数据以及内部终端之间传输的数据，IPS 则必须部署在网络边界，抵御来自外部的入侵，对内部攻击行为无能为力。

IDS 是一种监控网络中未经授权行为的软件或设备。使用预先设置的规则，IDS 就可以检测端点配置，以便确定端点是否易受攻击，用户还可以记录网络上的行为，然后将其与已知的攻击或攻击模式进行比对。IPS 能够监测由僵尸网络、病毒、恶意代码以及有针对性的攻击引起的异常流量，还能够在破坏发生前采取保护网络的行动。许多网络攻击者会使用自动扫描探测互联网，对每个网络都进行漏洞探测记录供日后使用。这些攻击者对任何数据都感兴趣，如个人信息、财务记录等。

IPS 作为一种新型网络安全防护技术，它通过审计分析计算机网络或系统上的数据正确区分数据类型为正常或异常攻击，同时实时、主动响应和防御入侵攻击，从而保障了网络或系统安全。IPS 借鉴 IDS 的思想并在其基础上发展，因此两者既有共同之处，又存在区别。IPS 既可以像 IDS 对入侵攻击进行检测并报警响应，同时又能够主动阻止入侵

行为、自动切断攻击源。两者在功能上的差异，使得它们在网络中的部署情况不同。

IDS 主要是通过监视和发现网络中的攻击行为并发出报警的，采用旁路方式并联接入网络；而 IPS 不仅对网络中的攻击行为进行检测，同时要实时、动态响应并阻断攻击，才能保障内部受保护网络的安全，因此采用在线(In-Line)方式直接串联接入网络，图 3-1 给出了两者不同的网络拓扑结构。如果入侵攻击已通过防火墙的屏障，由于 IDS 处于网络中的旁路，即使能够检测并发出报警，也无法阻止已对内部网络造成的危害；IPS 因其直接串联在网络中，经过检测发现攻击时能够实时将恶意连接直接阻挡在外。显然，IPS 能够提供一个更加有效、深层次的安全防护。

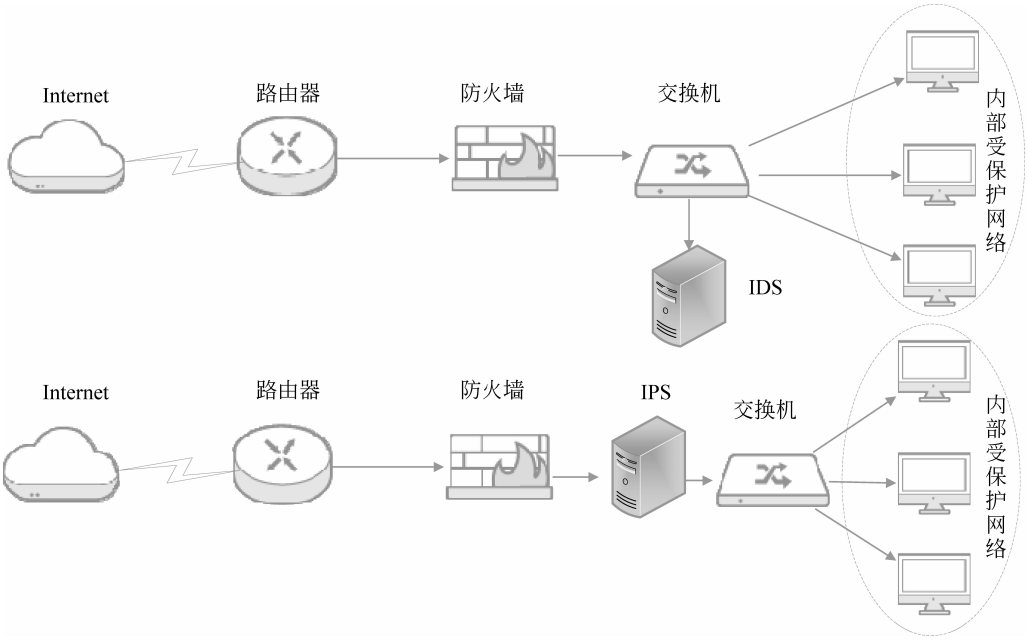

图 3-1　IDS 与 IPS 的区别

3.2　入侵防御系统的功能

IPS 是一种智能化的入侵检测和防御产品，它不但能检测入侵的发生，而且能通过一定的响应方式，实时中止入侵行为的发生和发展，实时保护信息系统不受实质性的攻击。IPS 使得 IDS 和防火墙走向统一。简单地理解，可认为 IPS 就是防火墙加上入侵检测系统，但并不是说 IPS 可以代替防火墙或入侵检测系统。防火墙是粒度比较粗的访问控制产品，它在基于 TCP/IP 的过滤方面效率高，而且在大多数情况下，可以提供网络地址转换、服务代理、流量统计等功能，甚至有的防火墙还能提供 VPN 功能。与防火墙相比，IPS 的功能比较单一，它只能串联在网络上(类似于网桥式防火墙)，对防火墙不能过滤的攻击进行过滤。这样，一个两级的过滤模式可以最大限度地保证系统安全。

一般来说，企业用户关注的是自己的网络能否避免被攻击，对于能检测到多少攻击并

不关注，但这并不是说入侵检测系统就没有用处，在一些专业的机构或对网络安全要求比较高的地方，入侵检测系统和其他审计跟踪产品结合，可以提供针对企业信息资源的全面的审计能力，对于攻击还原、入侵取证、异常事件识别、网络故障排除等都有很重要的作用。可以将入侵防御系统的主要功能总结为以下 15 个部分。

1. 实时监视和拦截攻击

实时主动地拦截黑客的攻击、蠕虫、网络病毒、木马、DoS 等恶意流量，保护企业信息系统和网络结构免受侵害，防止操作系统死机，应用程序损坏。

2. 虚拟补丁

基础系统漏洞主要是指操作系统的基本服务或主流服务软件的漏洞。正如只有特定纹路的钥匙才能打开一把锁，只有特定“特征”的攻击才能攻陷一个漏洞。采用基于漏洞存在检测技术的引擎，通过检测攻击的特征，才能有效地对抗经过特殊设计的躲避技术，做到零误报，从而达到给受保护的操作系统和服务软件安装虚拟补丁的效果。

3. 保护客户端

现在主流的攻击很多是面向客户端程序的，浏览器、可编辑文档、多媒体是重中之重，客户端防护的薄弱使大量的 PC 被黑客控制成僵尸，PC 上的重要信息也被窃取。引擎根据协议和文件格式做深入解析，可以检测被编码或压缩的内容，如 GZIP、UTF 等；解析过程中，自动跳过和威胁无关的部分，为用户提供浏览器及其插件的安全防护。

4. 协议异常检测

黑客通常利用网络上用于服务器设计中的漏洞对服务器进行攻击。通过向服务器发送非标准或者缓冲区溢出的通信数据，进而夺取服务器控制权或者造成服务器死机。协议解析引擎对网络报文进行深度协议分析，对那些违背 RFC 规定的行为，或者对明显过长的字段、明显不合理的协议交互顺序、异常的应用协议的各个参数等信息进行识别。协议异常检测包括 HTTP、SMTP、FTP、POP3、IMAP4、MSRPC 等 30 多种常用协议。同时，引擎把内容层面如 XML 页面和 PDF 文件等也看作协议，如果出现异常的文件结构，也会认为是一种协议异常，通过这种方法分析出潜藏在文件内容中的缓冲区异常攻击或者脚本攻击等入侵行为。

5. Web 应用防护

入侵防御系统产品采用积极的安全模式确保执行正确的应用行为，不靠攻击特征符或模式匹配技术就能识别正确的应用行为，并阻止任何背离了正确应用活动的恶意行为，能够在威胁达到终端前就采取拦截动作。网络智能防护的核心是一个多层次的安全引擎，分析威胁从网络到达最终用户计算机的整个过程，具备深层次的协议和隧道的分析能力，使得它能够在复杂的 Web 2.0 的交互中检测威胁。

6. 流量安全防护

入侵防御系统应该具备从网络层到应用层的 DDoS 攻击检测能力，可以在拒绝攻击发生或短时间内大规模爆发的病毒导致网络流量激增时，能自动发现并检测异常流量，提

醒管理员及时应对，保护路由器、交换机、VoIP 系统、DNS、Web 服务器等网络基础设施免受各种拒绝服务攻击，保证关键业务畅通。

7. 应用识别和控制

入侵防御系统能全面监测和管理即时通信(Instant Messenger，IM)、网络游戏、在线视频及在线炒股等网络行为，协助企业辨识和限制非授权网络行为，更好地执行企业的安全策略，保障员工的工作效率，采用细致带宽分配策略限制 P2P、在线视频、大文件下载等大量不良应用占用的带宽，保障办公自动化(Office Automation，OA)、企业资源计划(Enterprise Resource Planning，ERP)等办公应用获得足够的带宽支持，提升上网速度。

8. IPv6 及隧道检测

入侵防御系统同时支持 IPv6/IPv4 双栈的漏洞防护，支持 IPv6、IPv6 over IPv4、IPv6 和 IPv4 混合网络的应用层攻击防护，以及 DDoS 流量异常攻击防护，能够完全适应 IPv6 环境及过渡期网络环境。同时，系统还支持对 VLAN IEEE 802.1q、MPLS、IPSec 及 GRE(通用路由封装)等隧道的流量分析和处理，能够对流量进行识别并且解析出内层报文进行检测，从而适应各种复杂的网络。

9. 策略管理

防御入侵系统采用灵活的策略配置和管理方式，内置多种威胁防护策略模板，可适用于大多数用户的常见场景。各种功能的策略可以任意组合，可以对网络流量检测和控制进行细粒度的配置。

10. 知识库和引擎升级

入侵防御系统可以及时升级，实时捕获最新的攻击、蠕虫病毒、木马等，提取威胁的签名，发现威胁的趋势，这样能够在最短的时间内获得最新的签名，及时升级检测引擎，从而具备防御 0-day 攻击的能力。签名库定期升级，特殊情况下可及时进行升级。为满足设备在各种应用环境下的灵活部署，支持多种升级方式。

11. 设备集中管理

随着设备的逐渐增多，安全管理的复杂性大大增加，设备的集中管理软件为用户提供设备集中配置管理功能，能够全面实现安全策略的配置和用户业务的管理，减轻用户的维护工作量，保障用户投资。集中管理软件采用 B/S 架构，在控制台通过浏览器进行访问，支持多用户同时操作，能适应复杂、大型网络的管理需求，采用图形化的配置、维护界面，可以通过直观的 Web 配置界面完成对大部分设备的业务配置。

软件的集中管理功能主要体现在设备管理、故障监控、策略管理、系统监控及日志和报表管理等几大方面。集中管理软件可自动识别设备类型和型号，同时对全网所有设备进行管理，完成设备的差异性适配，自动获取设备的实体数据，包括机框、单板、电源、风扇、端口、温度、CPU 占用率、内存占用率等。支持设备的单点配置，将设备内嵌的 Web 配置集成到集中管理软件界面，用户单机进行连接。

12. 故障监控

集中管理软件可以对网络中的异常运行情况进行实时监视，通过告警统计、定位、提

示、重定义、告警远程通知等手段，帮助网络管理员及时采取措施，恢复网络正常运行。同时，对管理员已经处理过的告警进行标识，便于区分。

系统提供告警信息浏览、告警查询功能，并且可以将常用查询条件保存为告警查询模板。针对大量的告警信息，系统支持按照设置的统计条件（如告警名称、告警级别、告警功能分类、告警时间、告警状态等）对告警信息进行统计，使用户可以快速了解告警发生的情况。

为了避免大量的冗余信息，集中管理软件上支持设置告警屏蔽功能，根据设置的屏蔽条件，可以对不重要的告警进行屏蔽，既不显示，也不保存。

13. 集中软件管理

集中管理软件需要从全局角度对所有设备实现集中管理、集中制定安全策略。当分支机构比较多时，可以采用统一的安全策略统一监控，避免下属机构各自制定安全策略，引发网络混乱。用户只需要一次性定义一条策略，然后将其部署到多台设备中。对于设备升级的场景，集中管理环境支持集中部署在线升级策略，并且可以进行全网设备的集中本地升级。

系统提供设备发现策略功能，可以将现有设备的配置用管理软件进行管理；提供策略部署成功、失败、审计不一致、设备命令变更的状态，对设备配置现状一目了然。

用户的管理域和权限管理相对于安全管理至关重要，入侵防御集中管理软件除了预置常用的管理员、操作员、审计用户组外，还支持用户根据实际情况创建自己需要的用户组并设置相应的管理和操作权限。根据用户的权限，在操作界面上，不可管理的设备和界面区域是不可见的，从而实现用户的分级管理，保证安全性。

14. 系统监控

入侵防御集中管理软件的系统管理功能是对管理软件本身的系统进行维护和管理，而不是对设备的管理。除了对软件自身的安全操作事件进行监控外，还包括日志管理、数据库管理、通信参数管理等内容。系统监控的功能需要能够监控系统或进程的启动/停止服务，进行通信模式设置，提供工具实现自身的进程、内存占用率、CPU 占用率、硬盘空间情况监控，一旦超出设置的阈值，即可产生告警。

为保证数据安全，应定期进行数据库备份。入侵防御系统的数据库备份管理系统提供统一的数据库备份和恢复工具，以减小网管维护数据库的难度。集中管理软件支持数据库的转储功能，转储数据库中的数据包括操作日志、安全日志、告警数据、事件数据及多种性能事件。用户可以选择启动手工转储，或者设置溢出转储或周期转储的方式。

15. 日志和报表

作为安全产品，日志和报表的展现具有重要的用户价值。通过日志和报表，用户可以及时掌握网络状况，对网络的流量和安全情况有整体的认识，能够对不正常的行为进行审计和分析，并且可以依据已知的信息对受保护的系统进行安全加固，以及对网络的安全策略不断调整优化。

入侵防御系统提供丰富的报表功能。预置的综合报表包含了大多数用户需要重点关注的信息内容，针对不同设备的网络流量、应用协议分布、漏洞和流量威胁发生的情况进

行分析，并结合图表呈现分析结果。除了预置的综合报表，系统还提供给用户灵活的制定报表的方式，可选择多个报表子项进行组合，定时生成日报表、周报表和年报表，并且可以用邮件方式发送给用户，生成可编辑的报表格式，用户可以根据需要对报表内容和格式进行再次编辑。

入侵防御系统提供多维的日志查询系统，用户可以根据不同的组合条件对日志进行过滤查询，便于在海量数据中寻找需要的关键信息。

3.3　入侵防御系统的原理与部署

3.3.1　入侵防御系统的原理

入侵防御系统的总体架构如图 3-2 所示。

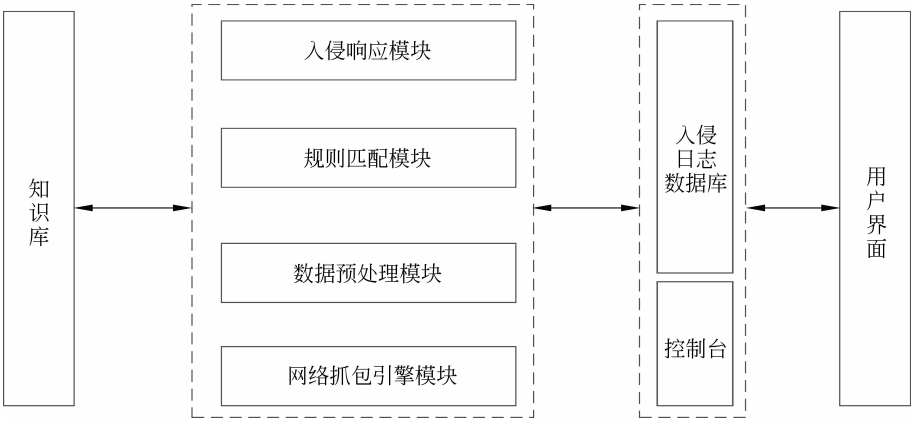

图 3-2　入侵防御系统的总体架构

1. 入侵响应模块

入侵响应模块可以在捕获到入侵事件之后及时做出处理，并将相应的信息反馈给入侵日志数据库和控制台。

2. 规则匹配模块

规则匹配模块是对数据预处理模块提交的数据运用匹配算法和知识库中的规则进行比较分析，从而判断是否有入侵行为。

3. 数据预处理模块

数据预处理模块主要是对数据报文进行协议解析及标准化，包括 IP 碎片重组、TCP 流重组、HTTP、Unicode、RPC、Telnet 解码等功能。经过数据预处理模块之后提取相关信息，并将处理后的报文交给规则匹配模块处理。

4. 网络抓包引擎模块

网络抓包引擎模块可捕获监听网络中的原始数据包，作为入侵防御系统分析的数据

来源。

5. 入侵日志数据库

入侵日志数据库负责对整个系统的工作过程进行数据收集、记录、统计分析和存储管理。

6. 控制台

控制台是引擎和外部指令交互的窗口，主要接收外部的指令执行相关操作。

7. 用户界面

用户界面是用户和入侵防御系统互动的直接窗口，界面提供可视化的威胁分析、系统状态显示、用户指令输入接口等功能，以 Web 方式提供给客户。

由于入侵检测大多只能进行网络安全监控，产生报警、日志等操作，已经不能满足网络安全的需要，因此在入侵检测系统的基础上提出了入侵防御系统。入侵防御系统用来识别针对计算机系统、网络系统或更广泛意义上的信息系统的非法攻击，包括检测外界非法入侵者的恶意攻击或试探，以及内部合法用户超越使用权限的非法行为等。入侵防御系统是入侵防御软件与硬件的结合。与其他安全产品不同的是，入侵防御系统需要更多的智能，它能对网络数据包进行协议分析，解析出包头信息和数据信息，并能实现 IP 碎片重整、TCP 的流重组等功能。通过对数据包内容进行检测过滤，从而发现网络攻击行为。入侵防御系统是对传统安全产品的合理补充，它能帮助系统对付网络攻击，扩展系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高信息安全基础结构的完整性。

入侵防御系统相对入侵检测系统而言，更倾向于提供主动的防护。它直接嵌入到网络流量中，通过一个网络接口接收来自外部系统的流量。若经过检查确认不含有异常活动或可疑内容，再通过另外一个网络接口将它传递到内部系统中。这样，有问题的数据包以及所有来自同一数据流的后续数据包，都会被 IPS 彻底清除掉。

入侵防御系统指不但能检测入侵的发生，而且能通过一定的响应方式实时中止入侵行为的发生和发展，实时保护信息系统不受实质性攻击的一种智能化的安全体系。它是一种主动的、积极的入侵防范及阻止系统，其设计旨在预先对入侵活动和攻击性网络流量进行检测和拦截，避免其造成任何损失，而不是简单地在恶意流量传送时或传送后才发出警报。它部署在网络的进出口处，当它检测到攻击企图后，它会自动将攻击包丢掉或采取措施将攻击源阻断。入侵防御系统的工作原理如图 3-3 所示。

入侵防御系统实时检查和阻止入侵的原理在于入侵检测系统拥有数量众多的过滤器，能够防止各种攻击。当新的攻击手段被发现后，入侵防御系统就会创建一个新的过滤器。入侵防御系统数据包处理引擎是专业化定制的集成电路，可以深层次地检查数据包的内容。如果有攻击者利用 Layer2（介质访问控制）～Layer7（应用）的漏洞发起攻击，入侵防御系统能够从数据流中检查出这些攻击并加以阻止。传统的防火墙只能对 Layer3（网络层）或 Layer4（传输层）进行检查，不能检查应用层的内容。防火墙的包过滤技术不会针对每个字节进行检查，因而无法发现攻击活动，而入侵防御系统可以做到逐字节地检查数据包。所有流经入侵防御系统的数据包都会被分类，分类的依据是数据包中的包头

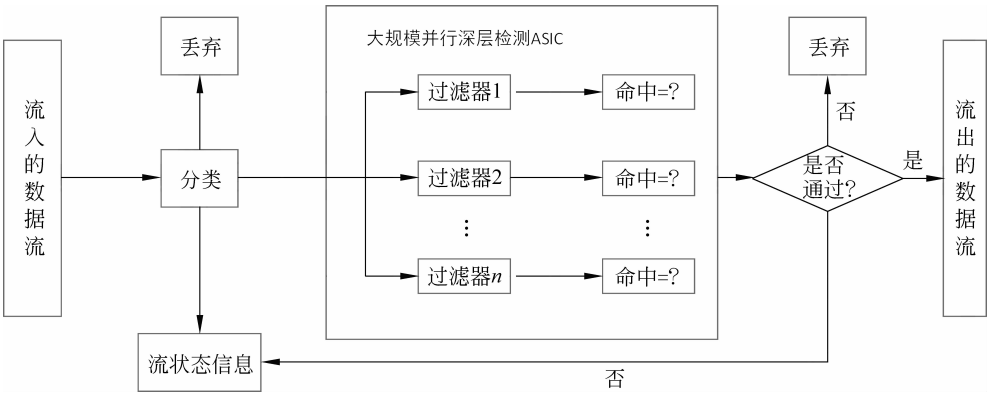

图 3-3　入侵防御系统的工作原理

信息，如源 IP 地址和目的 IP 地址、端口号和应用域。每种过滤器负责分析对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包会被丢弃，被怀疑的数据包需要接受进一步检查。

针对不同的攻击行为，入侵防御系统需要不同的过滤器。每种过滤器都设有相应的过滤规则，为确保准确性，这一规则定义十分广泛。在对传输内容进行分类时，过滤引擎还需要参照数据包的信息参数，将其解析至一个有意义的域中进行上下文分析，以提高过滤的准确性。

过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可确保数据包能不断地快速通过系统。这种硬件加速技术对于入侵防御系统具有重要意义，因为传统的软件解决方案必须串行进行过滤检查，会导致系统的性能大打折扣。

入侵防御系统虽然在某些方面和防火墙有相似之处，但它却是一种将审计和访问控制相融合的安全技术。普遍采用的防火墙技术是基于七层网络协议层第三层的路由访问控制，是串联在网络中的。入侵检测系统则通过并联在网络中进行网络监控和审核跟踪评估系统面临的危险，而且一方面采用与防火墙类似的过滤技术，也是串联在网络中的，但是它不仅工作在网络层，还可以提供网络模型从第三层到第七层的细粒度深层防御，因此能够实现比防火墙更细粒度的访问控制。另一方面，采用基于对应用层数据内容与数据行为进行分析的检测技术，其中行为分析技术与传统的基于异常行为特征库的匹配检测方法不同，同时检测正常与异常两类行为，并且不仅检测单包的行为，更重要的是检测基于流的行为系统，实现了将传统的两大网络安全技术-访问控制技术和分析检测技术统一在一个完整的系统里，形成了一个密切联系的紧耦合系统，避免了与防火墙联动解决安全问题时产生的通信效率低，自身安全性差的问题，从而可以实现对网络流量进行实时放行或拦截控制，将传统的静态访问控制发展为动态的访问控制，并可以实现更高的效率和更高的安全性。系统将访问控制和分析检测功能紧耦合在一个系统里，在实践上实现了动态网络安全模型的防护、检测和响应的有机统一，进一步提高了网络防护的智能性和主动性。

3.3.2 入侵防御系统的部署

IPS主要用于一些重要服务器的入侵威胁防护，如用它保护OA系统、EPR系统、数据库、FTP服务器、Web网站等。IPS在部署时应该首先保护重要设备，而不是先保护所有的设备。当然，如果是小型办公网络，也可以部署在网络前端用它保护所有服务器和办公终端。

IPS有两种部署方式：串联与并联。

IPS串联部署：

（1）针对所有传输数据可以实时监控，并可以立即阻断各种隐蔽攻击，如SQL注入、旁路注入、脚本攻击、反向连接木马、蠕虫病毒等。

（2）串联的IPS还具有内网管理功能，对上网行为进行管理，如禁止QQ、MSN等网上聊天软件，禁止或限制网上看电影，禁止或限制P2P下载，禁止或限制在线游戏等。

（3）串联的IPS一旦死机，采用硬件Bypass功能立即开启网络全通功能，才不会影响网络使用，不会造成网络中断。

IPS并联部署：

（1）设备不会对网络传输形成瓶颈，一旦设备死机，不会中断网络。

（2）可以监控网络传输的所有数据，并分析数据、安全审计。

3.4 入侵防御系统的关键技术

入侵防御系统是能够识别对计算机或者网络资源的恶意企图和行为，并对这些网络提供实时的入侵检测，以及采取相应防护的一种积极主动的入侵防护。入侵防御系统需要搜集网络上的数据流量信息，并根据这些信息进行统计、识别。再基于这些统计、识别的内容采取相应的识别手段。目前，基于统计和识别网络上异常流量的技术手段有基于特征的异常检测和基于行为的异常检测。

1. 基于特征的异常检测

基于特征的异常检测是根据已经定义好的攻击特征表述，对网络上的数据流量信息进行分析，当收集的信息与该攻击特征描述相符时，则认为发生了入侵行为。这一检测假设入侵者活动可以用某种模式特征表示，系统的目标是检测主体活动是否符合这种模式特征。该方法的一大优点是：只需收集相关的数据集合并依据具体特征库进行判断，显著减少了系统负担，且技术已相当成熟。它与病毒防火墙采用的方法类似，检测准确率和效率都相当高。但是，该方法存在的弱点在于，与具体系统依赖性太强，系统移植性不好，且不能检测到从未出现过的黑客攻击手段，需要不断升级，以对付新出现的入侵手段。如果可以定义所有的不可接受行为，那么每种能够与之匹配的行为都会引起告警。收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录匹配时，系统就认为这种行为是入侵。这种检测模型虽然误报率低，但是漏报率高。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且特征库必

须不断更新。该方法是目前主流的实现手段，安全模型比较容易建立。

2. 基于行为的异常检测

基于行为的异常检测的前提是入侵活动发生时，其行为活动与正常的网络活动存在异常，因此根据这个理论须建立一个正常活动行为的模型，当发生的行为与该模型规律相反时，则认为是入侵活动。若可以定义每项可接受的行为，则每项不可接受的行为就应该是入侵。首先总结正常操作应具有的特征用户轮廓，当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型虽然漏报率低，但误报率高。因为不需要对每种入侵行为进行定义，所以能有效检测未知的入侵。用户行为表现为可预测的、一致的系统使用模式，而入侵者活动异常于正常用户的活动。根据这一理念建立用户正常活动的“行为模型”。进行检测时，将使用者的行为或资源使用状况与“行为模型”相比较，从而判断该活动是否是入侵行为。例如，事先定义一组系统“正常”情况的阈值，如利用率、内存利用率、特定类型的网络连接数、访问文件或目录次数、不成功注册次数等，这类数据可人为定义，也可通过观察系统并用统计的办法得出，然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。异常检测与系统相对无关，通用性较强，它甚至有可能检测出以前未出现过的攻击方法。异常检测的关键在于如何建立“行为模型”以及如何设计检测算法降低过高的误检率，因为不可能对整个系统内的所有用户行为进行全面的描述，况且每个用户的行为是经常改变的，尤其在用户数目众多或工作目的经常改变的环境中。该方法能检测出未知攻击，但基于行为的异常检测模型难以建立，需要有相关经验的人制定，这是未来发展的一个方向。

3.4.1　原始数据包分析

入侵防御系统一般是作为一个独立的个体部署在被保护网络的出入口位置上，它使用原始的网络数据报文作为攻击分析的数据源。

入侵防御系统在线连接在需要检测的网络链路中，对接口上接收到的网络数据包，首先分析链路层、网络层、传输层和应用层协议，根据不同的协议类型检测特征值，同时判断是否为异常协议类型。然后将每个数据包与模式匹配规则库中的规则或建立好的安全模式进行匹配，判断该数据包是否为攻击数据包，如果该数据包是攻击数据包，则丢弃该数据包，否则进行 IP 分片重组（重组后进行更深层次的检测），同时转发该数据包。

不同的协议类型匹配不同的检测特征或者安全模型，也就意味着入侵防御系统中会包含不同类型的过滤器，通过层层过滤进行攻击检测，并加以阻止。因此，入侵防御系统首先需要做的就是对数据包进行解析。数据包解析基本过程如图 3-4 所示。

接收数据包时，通过网卡驱动程序收集网络上的数据包。数据收取上来后，进入入侵防御系统的解码器，解码器首先根据以太网首部中的上层协议字段确定该数据包的有效负载，确定获得的是 IP、ARP，还是 RARP 数据包，然后交给相应的协议解码器进行下一层解码。

以 IP 数据包为例，IP 解码器解析 IP 首部内容，确定从首部中获得的上层协议是 TCP、UDP、ICMP，还是 IGMP。然后再根据不同的协议选择解码器。如果是 TCP，则解

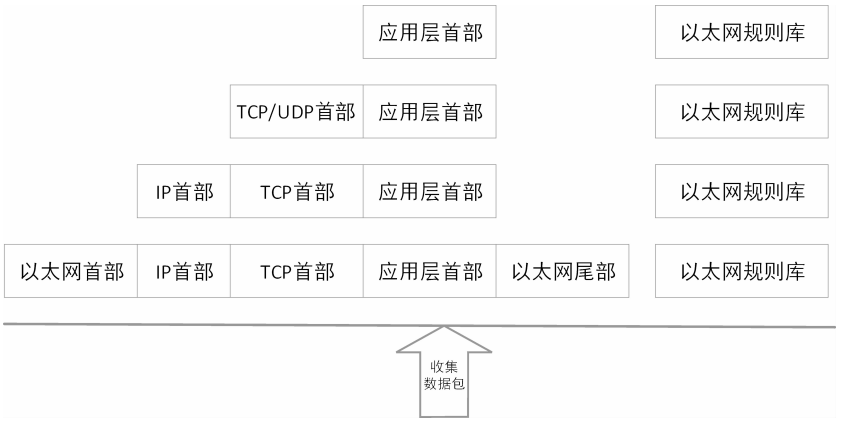

图 3-4　数据包解析基本过程

析 TCP 首部内容，并根据 TCP 首部中端口、协议识别等，确定应用层数据是什么协议，再解析应用层协议的数据。

进行解析的同时，也会根据不同的协议选择不同的规则库和安全模型，对这些数据包进行过滤，确定该数据包是否阻断或者转发。

解析数据包时，由于以太网中数据的最大长度是确定的，所以 IP 数据包会进行分片，并且大部分应用使用 TCP 或者 UDP 进行传输时，会将数据分为多个数据包，而且由于网络传输时路径延时等原因，数据包到达的时间可能不一致，因此入侵防御系统还需要按照待定顺序对数据包的内容进行重组，还原应用层数据。

3.4.2　IP 分片重组技术

IP 分片是网络上传输 IP 报文的一种技术手段。IP 在传输数据包时，将数据报文分成若干个分片进行传输，并且在目标系统中进行重组，这一过程称为分片。

IP 首部报文长度字段是 16 位，因此可以支持 IP 数据包传输的最大长度是 65536B，但是每种物理网络都会规定链路层数据帧的最大长度，称为链路层最大传输单元(Maximum Transmission Unit，MTU)。任何时候 IP 层接收到一份要发送的 IP 数据包时，都要判断向本地哪个接口发送数据(选路)，并查询该接口获得其 MTU。IP 把 MTU 与数据包长度进行比较，如果需要，则进行分片。分片可以发生在原始发送端主机上，也可以发生在中间路由器上。IP 报文长度不能超过 1500B，UDP 不能超过 1472B，TCP 不能超过 1460B。例如，应用进程将 1473B 应用字段交给 UDP 处理，UDP 加上 8B 的 UDP 报头后，交给 IP 层处理，IP 层在转发之前，发现该报文长度超出转发接口的 MTU，因此需要分片，分为两个 IP 分组。IP 数据报示意图如图 3-5 所示。

IP 首部中与分片相关的字段如下。

标识(Identification)字段占 16 位，是一个计数器，用来产生数据包的标识。一个 IP 地址每发送一个 IP 报文时标志位是上一个报文标志位加一，来自同一个 IP 报文的分片具有相同的 ID。

标志(Flag)占 32 位，目前只有前两位有意义。标志字段的最低位是 MF(More Frag-

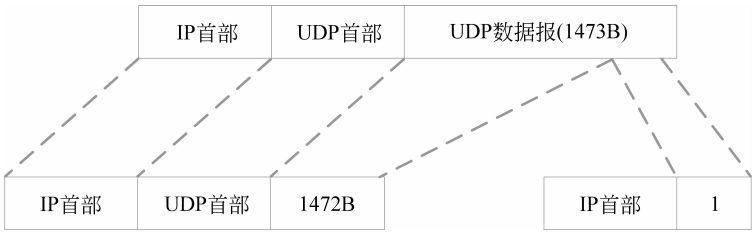

图 3-5　IP 数据报示意图

ment)。MF＝1 表示后面“还有分片”,MF＝0 表示最后一个分片。标志字段中间的一位是 DF(Don't Fragment),只有当 DF＝0 时,才允许分片。

偏移位占 12 位,偏移位的作用是指出较长的分组分片后某片在原分组中的相对位置,片偏移以 8B 为偏移单位。

IP 分片示意图如图 3-6 所示。对于长度超过 1500B 的 IP 报文,IP 层会将其分片分成若干长度不超过 1500B 的 IP 报文(分片)传递。从源报文的 UDP 头部开始将源报文数据段以 1480B 为单位依次分片,直到最后不足 1480B 时为最后一个分片。每个分片的段偏移为该片第一个 8B 在源 IP 报文数据段中以 8B 为单位的偏移。这些分片中只有第一个分片具有源报文的 UDP 头部,其余报文的 IP 数据字段为源报文的用户数据。所有分片 IP 头部和源 IP 报文一样。

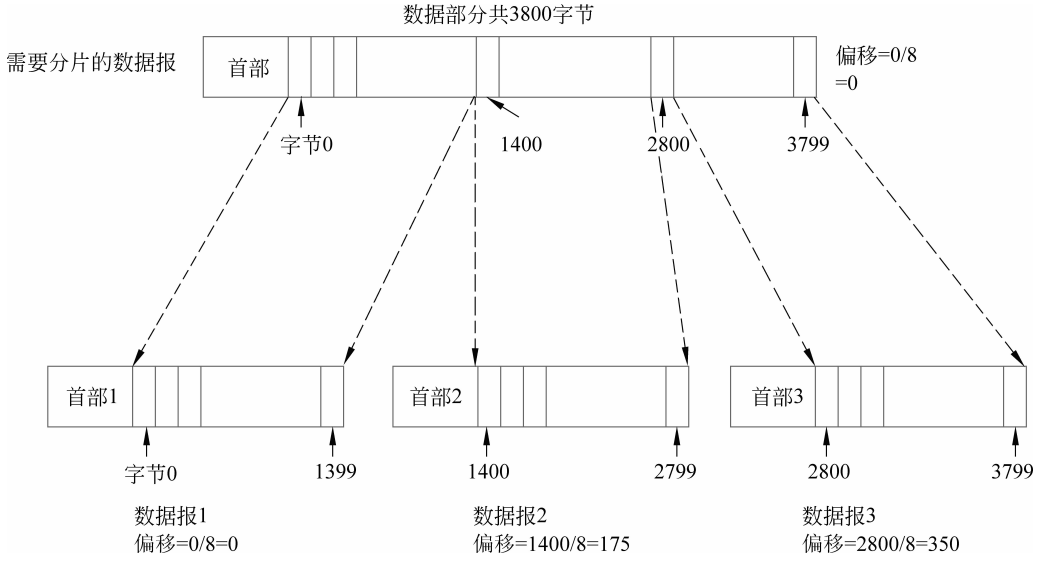

图 3-6　IP 分片示意图

攻击者通过分片的方式,将带有攻击内容的数据包分片后进行传输,通过不同的路由选择等方式可以达到绕过的效果。分片增加了入侵防御系统的检测难度,是目前攻击者绕过攻击的普通手段。攻击者利用 IP 分片的原理,往往会使用分片数据包转发工具(如 Fragroute),将攻击请求分成若干 IP 分片包发送给目标主机;目标主机接收到分片包后,进行分片重组还原出真正的请求。分片攻击包括分片覆盖、分片重写、分片超时和针对网

络拓扑的分片技术等。

所以，入侵防御系统需要在内存中缓存分片，模拟目标主机对网络上传输的分片包进行重组，还原出真正的请求内容，然后再进行分析，具体流程如图 3-7 所示。

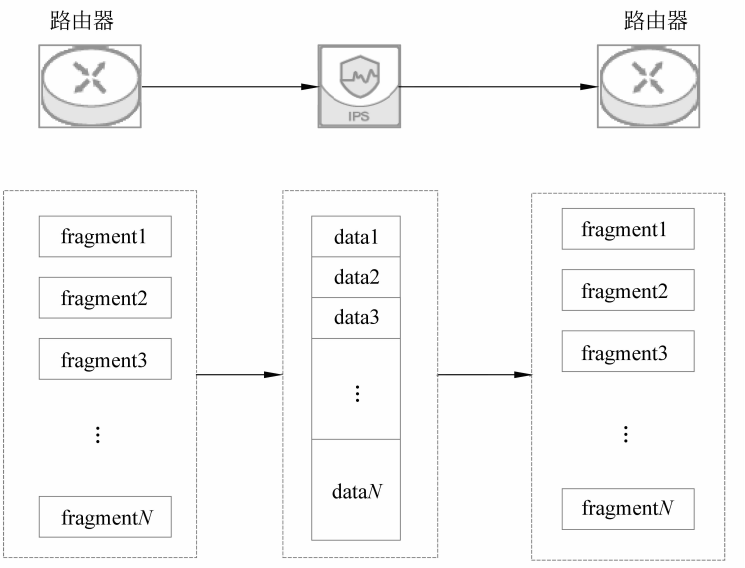

图 3-7　IPS 分片重组示意图

进行重组时，其重组原理和分片相反。如果一个包的段偏移为 0，而 Flag 字段不为 1，那么该报文一定不是来自一个分片。

对于接收到的无序分片，来自同一个包的分片具有相同的源 IP 及 ID 号。

当收到的标志位为 0 的分片时，说明这是最后一个分片。根据最后一个分片的段偏移可以知道在源报文中最后一个分片以前含有的数据长度，再加上最后一个分片的数据长度即为源 IP 报文数据部分的长度。如果接收到的所有分片的数据长度等于源 IP 报文数据部分的长度，就说明所有的分片都已经到达了，此时即可按照段偏移量重新组包，

校验到达包时，除第一个分片外，其余分片没有 UDP 头部，因此，对于每一个分片的校验是不方便的，可以再重组所有的分片，之后构建 UDP 伪头部校验。

由于 TCP 是面向连接的可靠传输协议，发送端 TCP 会将过大的数据采用按序流式方式以多个包形式发送，每发送一个包后，接收到接收端的确认信息后再发送下一个包，所发送的 TCP 包用户数据不超过 1460B，接收端 TCP 收到所有数据后进行重组，因此 TCP 数据不会在 IP 层重组。

3.4.3　TCP 状态检测技术

TCP 是基于状态的传输层协议，提供面向连接的、可靠的字节流服务。面向连接意味着两个使用 TCP 的应用在彼此交换数据前必须建立一个 TCP 连接，这一过程与打电话相似，先拨号振铃，等待对方摘机说“喂”，然后才说明身份。无论哪一方向另一方发送数据，首先都必须在双方之间建立一条连接，进行三次握手。

入侵防御系统会对 TCP 的连接状态进行检测和监控，不同的状态可能存在不同的攻击方式，同时还会对应用内容进行数据采集和特征检测。TCP 建立连接和关闭的状态变化如图 3-8 所示。

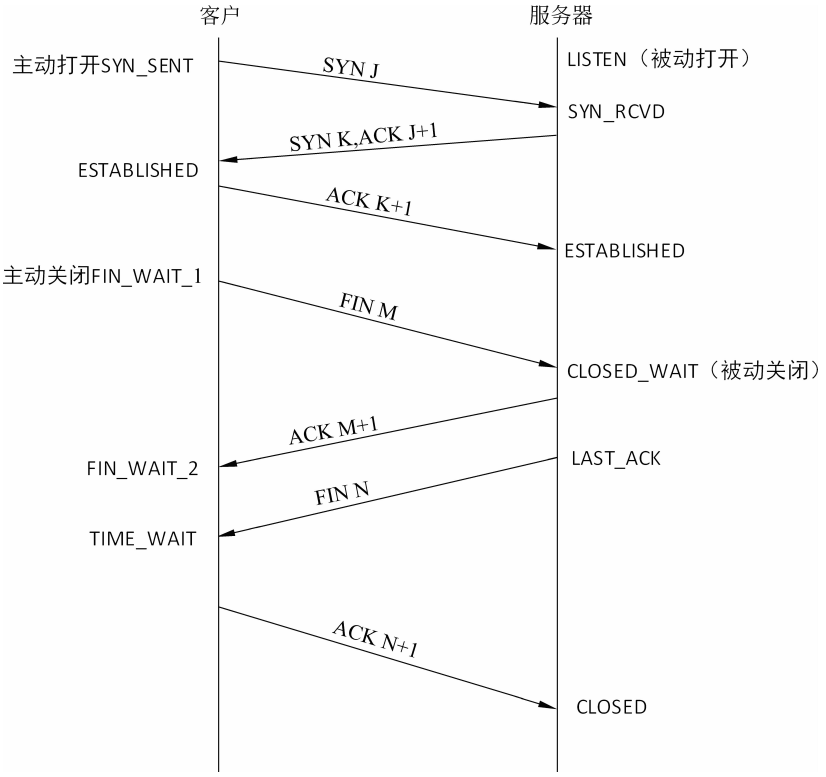

图 3-8　TCP 建立连接和关闭的状态变化

图 3-8 中包含 TCP 三次握手的过程，以及入侵防御系统采集 TCP 传输的数据内容的过程，采集数据包时，会对这些内容进行重组。图 3-8 中，TCP 一共有 10 种状态，分别为：

CLOSED：表示关闭状态(初始状态)。

LISTEN：该状态表示服务器端的某个 SOCKET 处于监听状态，可以接受连接。

SYN_SENT：这个状态与 SYN_RCVD 遥相呼应，当客户端 SOCKET 执行 CONNECT 连接时，它首先发送 SYN 报文，随即进入到 SYN_SENT 状态，并等待服务端的发送三次握手中的第 2 个报文。SYN_SENT 状态表示客户端已发送 SYN 报文。

SYN_RCVD：该状态表示接收到 SYN 报文，正常情况下，这个状态是服务器端的 SOCKET 在建立 TCP 连接时的三次握手会话过程中的一个中间状态，很短暂。此种状态下，当收到客户端的 ACK 报文后，会进入到 ESTABLISHED 状态。

ESTABLISHED：表示连接已经建立。

FIN_WAIT_1：FIN_WAIT_1 和 FIN_WAIT_2 状态的真正含义都是等待对方的 FIN 报文。区别是，FIN_WAIT_1 状态是当 SOCKET 在 ESTABLISHED 状态时，想主动关闭连接，向对方发送了 FIN 报文，此时该 SOCKET 进入到 FIN_WAIT_1 状态。FIN

_WAIT_2 状态是当对方回应 ACK 后，该 SOCKET 进入到 FIN_WAIT_2 状态，正常情况下，对方应马上回应 ACK 报文，所以 FIN_WAIT_1 状态一般较难见到，而 FIN_WAIT_2 状态可用 netstat 看到。

FIN_WAIT_2：主动关闭链接的一方，发出 FIN 收到 ACK 后进入该状态，通常称为半连接或半关闭状态。该状态下的 SOCKET 只能接收数据，不能发送数据。

TIME_WAIT：表示收到了对方的 FIN 报文，并发送出了 ACK 报文，等待两个报文最大生存时间(Maximum Segment Lifetime，MSL)后即可回到 CLOSED 可用状态。如果在 FIN_WAIT_1 状态下，收到对方同时带 FIN 标志和 ACK 标志的报文时，可以直接进入 TIME_WAIT 状态，无须经过 FIN_WAIT_2 状态。

CLOSE_WAIT：此种状态表示在等待关闭。当对方关闭一个 SOCKET 后发送 FIN 报文，系统会回应一个 ACK 报文给对方，此时则进入到 CLOSE_WAIT 状态。查看是否还有数据发送给对方，如果没有，则可以关闭这个 SOCKET，发送 FIN 报文给对方，即关闭连接。所以，在 CLOSE_WAIT 状态下需要关闭连接。

LAST_ACK：该状态是被动关闭一方在发送 FIN 报文后，最后等待对方的 ACK 报文。收到 ACK 报文后，即可进入到 CLOSED 可用状态。

下面对 TCP 连接建立和关闭的状态变化进行介绍。

1. 建立 TCP 连接

在 TCP/IP 中，由于 TCP 提供可靠的连接服务，于是采用有保障的三次握手创建一个 TCP 连接。三次握手的具体过程如下。

(1) 客户端发送一个带 SYN 标志的 TCP 报文(报文 1)到服务器，表示希望和服务器建立一个 TCP 连接。

(2) 服务器发送一个带有 ACK 标志和 SYN 标志的 TCP 报文(报文 2)给客户端，ACK 用于对报文 1 进行回应，SYN 用于询问客户端是否准备好进行数据传输。

(3) 客户端发送一个带有 ACK 标志的 TCP 报文(报文 3)，作为对报文 2 的回应。

至此，一个 TCP 连接建立完成。

2. 断开 TCP 连接

由于 TCP 连接是全双工的，因此每个方向都必须单独进行关闭。原则是主动关闭的一方(如已经传输完所有数据等原因)发送一个 FIN 报文表示需要终止这个方向的连接，接收到一个 FIN 意味着这个方向不再有数据传输，但是另一个方向依旧能够发送数据，直到另一个方向也发送 FIN 报文。四次挥手的具体过程如下。

(1) 客户端发送一个 FIN 报文(报文 4)给服务器，表示将关闭客户端到服务器的连接。

(2) 服务器接收到报文 4 后，发送一个 ACK 报文(报文 5)给客户端，序号为报文 4 的序号加 1。

(3) 服务器发送一个 FIN 报文(报文 6)给客户端，表示自己也将关闭服务器端的连接。

(4) 客户端接收到报文 6 后，发回一个 ACK 报文(报文 7)给服务器，序号为报文 6 的序号加 1。

至此，一个 TCP 连接就关闭了。

其中，状态从 ESTABLISHED(三次握手)之后到四次挥手完成，中间会对正反向流量的数据包进行采集，并对其进行重组，同时监控 TCP 的状态，不同的状态可能包含不同的攻击特征，因此，当 TCP 的某个状态发生时，需要对其进行检测。

例如，一些攻击者不进行三次握手。序列号不正确的报文发送给入侵防御系统(SYN Flood 攻击，攻击者伪造一定量的客户端，对服务器发起 TCP 连接，服务器收到 SYN 报文后，会回复 SYN+ACK，此时攻击者不回应 ACK 报文，由于三次握手没有正常建立，在一定时间内，服务器将会等待客户端的 ACK 回应报文，等待期间需要占用系统资源，当数量达到一定量时，就会导致后续的请求不能得到正常回应，从而占用系统资源)，这些报文带有攻击特征，甚至有可能有多个攻击特征，所以入侵防御系统在匹配这些数据包的信息时，就会频繁进行告警，降低了系统的性能并产生误报。通过对 TCP 状态的检测，没有经过三次握手的报文属于非法报文，可以直接丢弃，无须进入特征的模式匹配，这样可以完全避免因单包匹配造成的误报并提升效率。

基于状态检测的 TCP 数据采集及检测如图 3-9 所示。

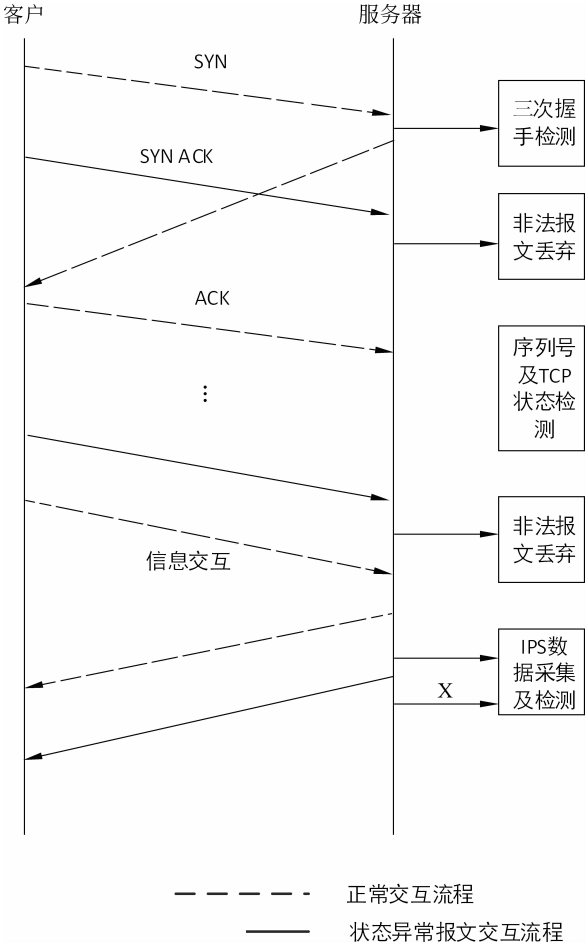

图 3-9　基于状态检测的 TCP 数据采集及检测