IDS 入侵检测技术

IDS 入侵检测技术

入侵检测系统自从上个世纪 80 年代后期 90 年代早期就出现了，它是入侵检测系统是历时最久并最普及的技术。作为网络安全的入侵警报器，IDS 可以分为基于特征（Signature-based）的和基于异常（anomaly-based）的。基于特征的 IDS 的工作原理类似杀毒，查询和已知的恶意事件匹配的特征。基于异常的 IDS 查询网络协议、用户、流量行为模式或系统（核心）调用中的异常行为。

IDS 基础介绍

IDS 是网络安全的警报器。它是一个签名数据库，与已知的攻击相对应。然后，IDS 监测所有的网络流量，寻找任何能够与签名匹配的东西。入侵监测行为的实际所在是不断创建、维护和调整签名数据库。采用 Java 等任何高级的编程语言都可以编写 IDS，但是处于额外消耗的考虑，最好采用编译语言。

- 入侵检测基础
- 入侵检测 ABC
- 入侵监测系统应该采用 Java 编写吗？

IDS 的工作方式

入侵检测系统（IDS）通常是通过签名检测和异常检测实现的，旨在在黑客对你的网络造成实质破坏之前揪出黑客。他们可以是基于网络的，也可以是基于主机的。基于主机的 IDS 是安装在客户机上的，而基于网络的 IDS 是在网络上。

- 入侵检测系统的工作原理
- IDS：签名检测与异常检测比较

IDS 的应用

对于拥有错综复杂的网络的大公司，很自然的需要安装和设置这种检测系统以及防范系统。IDS 通常是较大规模网络安全结构的一部份，并且是随着防火墙一道安装的。如果要使用入侵检测系统，可以考虑两种不同的方式，根据你可以在这个项目中使用的时间和金融资源做出选择。

- 弥补边界安全和主机安全之间的漏洞
- 入侵测试对于企业网络安全必不可少吗？
- 中小企业如何实施 IDS？
- 为何需要分布式无线 IDS
- 入侵检测和防范：不仅仅是防火墙（一）
- 入侵检测和防范：不仅仅是防火墙（二）

IDS 选购建议

由于 IDS 已经是一项成熟的技术，不同厂商的产品在技术上差异不是很大。在选购产品时不会被产品评语、产品认证之类的检测结果所左右。如果时间充裕，我还是建议在你的模拟实验环境中测试这些产品。

- IDS（入侵检测系统）最佳选购建议

入侵检测基础

入侵检测系统（Intrusion-detection systems，IDS）是任何安全基本架构的关键组件这些硬件和/或硬件设备监控网络中的恶意行为，并向管理员报告进一步的调查。市场上有很多入侵检测系统，从为高带宽设计的专门的硬件（费用是上千美元）一直到绝对免费的基于软件的 IDS Snort。

实际上，有一种相对简单的分类法，可以用于区分大部分的入侵检测系统。它是 基于两个特征的——监控运算法则类型（特征或异常检测）和监控的环境（何网络或主机）。TechTarget 中国的特约专家将简要分别介绍种。

IDS 的监控运算法则明确了系统如何决定一种行为是良性还是恶性。两种最常见的法则类型如下：

- 异常检测首先在系统或网络上开发“正常”行为的基线，然后当异常行为发生时，使用这些基线进行检测。异常检测系统的主要优势在于他们可以在新类型的恶意行为发生时检测到。缺点是这种系统需要经过“教育”才能接受一种恶意行文作为基线的一部分，这是通过缓慢地把它引入监控环境，直到被接受为正常而实现的。
- 特征检测系统，另一方面，使用已知的攻击类型的基线。但他们检测到和这些类型符合的行为是，就会发出警告。特征检测系统的假警告（或者“假阳性”）率很低，但是需要不断地更新，保证可以检测到新型的攻击。

入侵检测系统可以根据检测的环境类型被进一步分为：

- 基于网络的系统监控整个网络中的恶意行为。他们可以检测到分散的攻击，但是可能会错过单个主机上的攻击，例如病毒感染。
- 基于主机的系统监控单个系统（虽然很多基于主机的系统体重中央监控方案）。他们可以检测恶意代码和其他可能影响系统而不影响网络的行为的攻击。

有一点很重要，市场上的每一种 IDS 都不能完美地这样划分。可以找到一些混合的系统，把这两种监控运算法则的特征结合起来和/或监控不止一种类型的环境。当策划一种 IDS 结构是，你应该努力在运算法则和监控环境中找到平衡。

(作者：Mike Chapple 译者：Tina Guo 来源：TT 中国)

入侵检测 ABC

问：有什么样的入侵检测系统？

答：入侵检测系统是历时最久并最普及的技术。入侵防御系统（IPS）比较新，产生的争论也很多。我将要讨论这两种工具都存在的子类。终于，一些防火墙厂商正在开始把这些技术合并到他们的产品中去。所有的这类产品应该有能力以某种方式向中央控制台报告，大量的这类产品也要实现中央管理。

入侵检测系统自从上个世纪 80 年代后期 90 年代早期就出现了，而且分为基于特征（Signature-based）的和基于异常（anomaly-based）的。基于特征的 IDS 的工作原理类似杀毒，查询和已知的恶意事件匹配的特征。基于异常的 IDS 查询网络协议、用户、流量行为模式或系统（核心）调用中的异常行为。他们进一步分为网络和基于主机的类型。现在的网络 IDS（NIDS）嗅探一个单独的网段，通常使用混合特征和流量和/或协议异常检测。基于主机的 IDS（HIDS）存在于独立的主机上，并监控系统记录，系统核心调用和/或不同的重要文件的改变的混合体。各种 IDS 的关键点是它只进行检测---这种事情已经发生过了。

入侵防御系统（IPS）和 IDS 的分类类似，也就是主机 IPS（HIPS）和网络 IPS（NIPS）。NIPS 通常是内联（本质上就是 smart bridge）这样它就可以阻止恶意流量通过网络。HIPS 可能阻止一个应用程序或一个线路的有问题的和危险的行为。这是 IPS 的重点---如果他们阻止了非恶意事物，他们可以突破这些事物。

最后，防火墙传统上很少在应用层上操作，除非应用代理已经大部分干预了协议遵从。他们习惯于执行流量策略，关于有什么问题，责任在谁，如何执行。防火墙厂商正要开始把 IDS 特征匹配和其他技术混合进他们的产品中，这样就有能力创建防火墙和 IPS 的结合体 。

所有的这些技术在假阳性（良性事件的警告）和假阴性（错失新的和以前不知道的事件）方面声名狼藉。异常检测和查找系统调用中的真实恶意事件是两种对抗后者的方式。正在调整的和“目标”IDS 是减少前者的方式。

（作者：JP Vossen　译者：Tina Guo 来源：TT 中国）

入侵监测系统应该采用 Java 编写吗？

问：入侵监测系统（IDS）可以采用 Java 编写吗？如果可以，采用 Java 会有什么危险？如果不行，最好采用哪种语言？

答：实际上，基于签名的入侵监测系统的功能非常简单。IDS 是一个签名数据库，与已知的攻击相对应。然后，IDS 监测所有的网络流量，寻找任何能够与签名匹配的东西。入侵监测行为的实际所在是不断创建、维护和调整签名数据库。

毫无疑问，采用 Java 等任何高级的编程语言都可以实现这项功能。然而，执行跨平台的 Java 代码所固有的额外消耗，可能对 IDS 而言不是很好的选择。采用编译语言可能会更好些。

也就是说，你要考虑好通过创建你自己的入侵监测系统，你希望完成哪些任务。维护签名数据库是件很困难的事，所以使用市场上已有的合格商业或者开源系统可能会简单一些。

（作者：Mike Chapple　译者：周姝嫣　来源：TT 中国）

入侵检测系统的工作原理

问：入侵检测系统如何工作

答：入侵检测系统（IDS）通常用于检测不正常行为，旨在在黑客对你的网络造成实质破坏之前揪出黑客。他们可以是基于网络的，也可以是基于主机的。基于主机的 IDS 是安装在客户机上的，而基于网络的 IDS 是在网络上。

IDS 工作方式可以是检测已知攻击信号，也可以检测反常行为。这些反常或异常行为增大堆栈，并在协议和应用层被检测到。他们可以有效地检测到诸如 Xmas tree 扫描，DNS 中毒和其他的恶意数据包。

一个以 IDS 为基础的良好的网络是 SNORT。它是免费的，而且可以在 Linux 和 Windows 上运行。建立起来的一个简单的方法是扫描一个端口，允许这个端口截获所有横跨网络节点的所有流量。在你的操作系统上安装 SNORT，使用“只接受”的网络线缆把它连接到网络的这一部分。一旦你配置了你的规则，就准备好了。

（作者： Michael Gregg 译者：Tina Guo 来源：TT 中国）

IDS：签名检测与异常检测比较

你在这个指南中将学到：签名和异常检测的优点和弱点以及这两种检测方法如何相互补充。

在购买入侵检测系统的过程中，一个决策的关键点通常是入侵检测系统采用签名还是异常检测引擎。最初厂商了解两种方法的优点并且把这两种方法都集成到入侵检测系统中。理解签名和异常检测这两种方法的优点和弱点揭示了它们是如何相互补充的。

签名检测

签名检测包括在网络通信中搜索一系列字节或者数据包队列以查找已知的恶意程序。这种检测方法的最大的好处是，如果你清楚你想要找出的网络行为，这种签名就很容易开发和理解。例如，你可以利用一个签名寻找在一个可利用的安全漏洞中的特定的字符串来检测利用特定的缓存溢出安全漏洞实施攻击的企图。这个由基于签名的入侵检测系统产生的事件能够传达什么导致了报警。模式匹配在现代系统上能够很快完成，因此对于确定的一套规则来说，进行这种检查所需要的计算能力是最小的。例如，如果你要保护的系统仅通过 DNS、ICMP 和 SMTP 通信，所有的其它签名都将被删除。

签名引擎也有自己的弱点。由于签名引擎仅检测已知的攻击，必须为每一种攻击制作一个签名，而且新的攻击还无法检测。由于签名通常是根据正常的表达和字符串设计的，因此，签名引擎还会出现不正确的检测结果。这两种机制只是在线路上传输的数据包中检测字符串。

虽然签名对于检测以固定方式实施的攻击很成功，但是对于人工制作的或者具有自我修正行为功能的蠕虫发起的多种形式的攻击的检测就有些力不从心。有些利用安全漏洞允许恶意用户把攻击隐藏在“nop 发生器”、负载编码器和加密数据通道的后面，使检测更加复杂。由于必须为每一种攻击的变体制作一个新的签名，而且随着规则的增加检测系统

的运行速度将减缓，因此，签名引擎检测这些变化的攻击的整体能力将受到影响。这就是大多数入侵检测系统都使用 2 路服务器至 8 路服务器并且配置许多 GB 网卡的原因。

实际上，基于签名的入侵检测系统可以归结为攻击者和入侵检测系统签名开发商之间的军备竞赛。这场竞赛的关键是签名编写和应用到入侵检测引擎中的速度。

异常检测

异常检测技术是以网络行为基准概念为中心的。这个基准是人们接受的网络行为的解释。任何不符合人们预先制定的或者接受的行为模式都会被异常检测引擎查出来。

网络行为基准不可分割的组成部分是异常检测引擎认真分析所有层的协议的能力。对于每一个被监视的协议来说，异常检测引擎必须具有解码和处理协议的能力，以便理解其目的和负载。这种协议分析一开始将耗费昂贵的计算机资源，但是，这种分析能够让异常检测引擎随着规则数量的增长进行调整，并且在检测到异常行为时很少发出错误的警报。

异常检测引擎的缺点是确定规则的困难。进行分析的每一个协议都必须要进行定义、执行和测试，以验证其准确性。不同的厂商执行不同的协议使规则的制定过程更加复杂。在网络上传输的客户协议没有很大的努力是不能进行分析的。因此，必须要建立异常网络行为的详细知识，并且把这些知识输入到异常检测引擎的内存中，以便正确地实施监测。另一方面，一旦建立一个协议和定义一个行为，异常检测引擎就可以更迅速和更方便地调整检测范围。这个速度要比签名检测引擎的速度快得多，因为异常检测引擎不需要为每一个攻击和潜在的变体制作一个签名。

异常检测引擎的另一个弱点是异常使用行为中的恶意行为不能够检测出来。例如，一种对有安全漏洞的服务器实施的目录遍历攻击行为，由于这种攻击是根据网络协议编写的攻击程序，并且不启动任何协议以外的行为、负载或者限制带宽的标志，因此这类攻击就检测不出来。

然而，异常检测在检测新的攻击方面比签名检测引擎有优势，能够检测到签名引擎中不存在的新的攻击，如果新的攻击有异常的网络行为的话。最好的例子是这种系统检测新的自动传播的蠕虫。当一台新的系统被蠕虫感染之后，这个蠕虫就会以非常快的、异常的速度查找网络中具有安全漏洞的计算机，从而导致违反 TCP 连接或者带宽规则的不正常的恶意通信。

你可以看到一种检测方式的优点正好可以弥补另一种检测方式的弱点。反之亦然。在购买入侵检测系统时，选择检测方式不再是选择这一种而不选择那一种的问题了。而应该全部选择。

（作者：James C. Foster 来源：TT 中国）

弥补边界安全和主机安全之间的漏洞

大多数机构都认识到信息安全的重要性，并且以充分的技术控制把资源用于信息安全计划中。在许多情况下，这种控制在网络接入控制（边界保护）和加强网络中的单个系统的保护（主机保护）方面是很严密的。现在，我们开始看到用基于网络的安全机制弥补这两个方面之间的漏洞的重要性。

在本文中，我们将研究你可以在企业中用来弥补这个安全漏洞的三种技术控制方法：入侵检测系统、蜜罐/蜜网以及暗网。这三种技术中的每一种技术都有从简单到复杂的应用。

入侵检测系统

入侵检测有两种基本的方法：

基于签名的入侵检测系统以与现代抗病毒技术相似的方式进行工作。它们不断地更新解释各种已知的恶意行为的攻击定义文件（签名）。然后，基于签名的入侵检测系统便扫描网络，查找与签名匹配的数据包，接下来就是向安全管理员报警。

基于异常状况的入侵检测系统以不同的原则工作。这种入侵检测系统通过不间断地监视网络了解“正常”网络活动的状况，然后向管理员报警任何不正常的状况。基于异常状况的入侵检测系统的优点在于它能够识别出以前出现过的攻击。遗憾的是，基于异常状况的入侵检测系统还不能成为信息安全的主流产品，它们的成熟程度还不可靠，不能用于生产网络中。

如果你要使用入侵检测系统，你可以考虑两种不同的方式，根据你可以在这个项目中使用的时间和金融资源做出选择。第一个选择是开源软件。Snort 入侵检测系统是 Snort.org 免费提供的软件，并且得到了信息安全团体的大力支持。如果不愿意耗费大量

的时间安装和运行 Snort 软件，你可以购买商业性的入侵检测软件。目前，思科和 Enterasys 等厂商提供了许多这样的产品。你还可以考虑 Sourcefire 公司提供的商业版本的 Snort 设备。

蜜罐和蜜网

蜜罐和蜜网是安全从业人员加强网络安全的另一个选择。不管你信不信，这些工具就是为了吸引恶意攻击者的。蜜罐设计成吸引黑客攻击的目标，对于观察和监视黑客的攻击行为和学习新的黑客工具和技术是非常有用的。从蜜罐系统中学到的知识可用来保护整个网络。

蜜网是用许多蜜罐系统组成的网络，一般都以不同的配置运行不同的操作系统和应用程序。许多学术团体都在研究一种所谓能够自我修复的蜜网。这些蜜网旨在吸引和监视恶意的行为，然后快速把网络恢复到原来的状态，等待应付未来的攻击。这可以节省许多网络管理时间。如果你要进一步了解有关建立蜜罐或者蜜网的信息，请咨询 Honeynet.org 网站的蜜网计划。

暗网

你在你的网络中可以使用的最简单的工具之一就是暗网。你要做的一切就是把不使用的 IP 地址空间放在一边，并把这些 IP 地址区域指定为暗网。接下来，配置你的入侵检测系统或者其它网络监视系统设备以便检测任何指向暗网地址的通信。由于在暗网中没有运行合法的系统，你可以安全地推测任何指向暗网 IP 地址的通信都是恶意系统或者配置错误的系统所为。暗网对于检测你的网络中的系统是非常有用的。它可以检测出你的网络中的电脑是否受到蠕虫或者恶意软件的感染，正在随机地向你的网络地址传播。

（作者：Mike Chapple　来源：TT 中国）

入侵测试对于企业网络安全必不可少吗？

问：入侵测试在企业网络安全战略中应该扮演多大的角色？

答：入侵测试能够提供有关你的安全防御状态的有价值的信息。但是，入侵测试太昂贵。要让入侵测试具有可信性，这种测试通常必须由一个独立的外部公司实施。如果你使用内部人员进行入侵测试并且发现了安全漏洞，你会听到这样的批评，说这些测试人员肯定利用了他们的内部信息和基础设施知识，企图提高安全预算。另一方面，如果测试显示一切正常，你会受到这样的批评，说测试进行得不全面。这肯定是我曾经看见的一个第 22 条军规！

由于入侵测试成本很高，我经常建议成熟的安全计划考虑这个问题。如果你目前正在建立一个安全基础设施并且缺少一些主要的产品，你可以把投资首先用于入侵测试。否则，入侵测试只能找到你已经知道的安全漏洞。另一方面，如果你使用入侵测试来评估全面实施的基础设施，你可能会得到有关潜在弱点的有价值的内部情况。

（作者：Mike Chapple　来源：TT 中国）

中小企业如何实施 IDS？

问：在现实生活中，经费不足的中小企业往往无力实施 IDS（入侵检测系统）。对于数目众多的中小企业，你是否有一个成本合算的实用建议？

答：对中、小型企业来说，首先应该做一个总体安全评估。你的数据和业务流程面临怎样的威胁？你更关心来自互联网的威胁还是来自内部的？研究表明 60%到 80%的攻击来自内部。

众所周知，对中、小型企业来说，首先应该确保在互联网接口上安装有防火墙，最好是经过正式检测的，完成过滤和网络地址转换（NAT）功能。如果还能提供基于代理的服务就更好了。

接下来，使用某些入侵检测的产品。思科的 IDS 产品性能优良（曾叫 NetRanger）。你可以在网络中的许多位置配置传感器（防火墙之前，防火墙之后，DMZ 中等等），并且通过中央控制台进行管理。基于主机的入侵检测同样有效。ZoneAlarm Pro 是解决资金短缺问题的好选择。同时使用这两种产品效果更佳。

至于文件校验和其他类似技术，TripWire 是用于提供这些服务的工具之一。尽管 TripWire 有商业版本，仍然可以免费下载可用的较老版本（仍然非常有效，用于 Unix 系统）。

如果你负担不起这里所建议的所有方法，你仍然有许多免费或花费很少的选择。不过，你需要从另一面来考虑这个问题。如果你的网络遭到较严重的入侵，你将遭受多大的损失？你愿意将相当于损失的百分之几的费用用于保护你的网络？把这笔花费当作保险费吧。

（作者：Stephen Mencik　译者：Shirley　来源：TT 中国）

为何需要分布式无线 IDS

让我们面对现实。现有的无线局域网（WLAN）技术价格便宜，并且几乎任何人都可以轻松地设置。更糟糕的是，它可以安装在任何地方，甚至在未经您同意的情况下，也能安装在您的企业局域网内。任何储存专有数据或敏感数据的网络，包括大多数商业和/或政府网络，都应该安装分布式无线入侵检测系统（IDS）。通常说来，使用无线网络的网络策略非常严格；许多用户一般会忽略了策略，而试图寻找可以使其工作更有效率的方法。WLAN 技术拥有更高的效率和灵活性，这就使得用户极大地提高了生产力。

当然，很多时候也存在一些“酷因素”。

请回答如下问题：

你的企业有关于 WLAN 技术的书面策略吗？

你是如何落实和执行该策略的？

你是否知道已经有未经授权的 WLAN 技术安装在你的企业中？

无线系统是庞大的。如果你不积极地寻找无线技术，你的网络安全就可能存在巨大的缺口，而你却从来不知道。如果在企业没有认识到或认同的情况下，通过无线技术绕过你的防火墙和其它外围防御，那么你的这些技术就形同虚设。通常，插入局域网的恶意访问点是不安全的，并且为网络提供一个开放后门——绕过所有周边安全防护——类似于工作站的电话调制解调器。恶意访问点通常是低成本消费产品，同时拥有最低限度的安全性，安装时采用众所周知的默认设置，这使得它们很容易成为攻击对象。在插入局域网时使用特定网络，形成无线黑客容易攻击的目标。（特定网络是在点对点模式下，单个客户之间采用无线相互连接的网络，与 windows 系统中的工作组类似。）除了操作系统(OS)被锁定，或者一个基于主机的防火墙（如果安装了的话），几乎没有安全性可言。考虑到大

部分新的笔记本电脑都装有无线网卡，那么在未来大约一年内，特定网络的威胁将大大增加。

在因特网上哈瓦那容易获得无线扫描软件。所谓的“战争司机”只是在网络周围闲逛，扫描那些开放或者容易进入的无线网络，谨防黑客攻击；或者仅采用免费的因特网服务。无线技术解放了劳动力并提高了生产力，但如果配置不合适的话，它将成为你的致命弱点。

考虑到服务集标识符（SSID），SSID 可以将 Windows 中与域类似的无线网络分隔开。接入点传送穿过无线介质的 SSID，进而使得客户可以找到它们。这正是战争司机扫描软件轻而易举地找到无线网络的方式。

那么，企业该如何保证其无线网络的隐藏状态，使其免于被不定期的战争司机检测到？

将其构建到大多数企业级别的无线接入点就可以关闭 SSID 传播。不定期的战争司机将不能找到无线网络；不幸的是，一个有经验的黑客仍然能够找到 SSID，有了 SSID 进而找到无线网络。这只需要更多的努力便可实现。这就构成了目标性攻击，正是基于此，企业需要构建无线安全体系结构。这些目标性攻击可能来自于黑客，他们为了证明其技能；也可能来自于竞争者，他们为了寻求竞争优势。

安全地运行无线局域网不是没有可能的，但是这需要计划和测试。构建到现有无线接入点的安全级别还不足以保证企业网络的安全。虚拟专用网（VPN）技术和恰当的结构体系都必须为无线网络提供一个令人满意的安全级别。

随着无线产品以极高的速率增加，许多公司开发了创新的软件和硬件解决方案，已经接近了向盘片的发展。这种解决方案之一就是分布式无线 IDS，它能够从某个单一地址、全天候的对整个全程企业（包括多个地点的多个建筑物）进行检控。分布式无线 IDS 提供了一种贯彻和执行书面无线策略的方法，以及实时警报管理员有入侵行为或者非法使用无线技术。对一些管理员尽力保护其网络上的敏感数据，这方面的信息对于他们而言是

无价的。设置详细的策略，并与现有可用/不可用的无线操作程序相匹配，这就会实时提醒管理员整个公司的访问冲突。

现有的无线局域网大大受益于分布式无线 IDS。比如，它可以处理许多管理任务，保存使用记录、吞吐量、与之有联系的站点数量和连接到哪个接入点、性能统计、以及除入侵检测之外的更多内容。管理员在保护敏感或私有数据的同时，可以很容易地管理整个全程无线结构体系。利益远大于成本。

无线技术通过捷径出现了。重要的是提高企业的意识，使其认识到可能有人秘密使用无线技术。管理员可能会忽略无线技术或者在实施安全策略前有前摄心理。无论一个企业是否运行无线局域网，重要的是要了解无线技术对任何储存有敏感或私有数据的网络所产生的影响。

(作者：Derek Krein　译者：李娜娜　来源：TT 中国)

入侵检测和防范：不仅仅是防火墙（一）

入侵检测系统(Intrusion Detection System，IDS)以及它们的近亲---入侵防御系统(Intrusion Prevention System，IPS)是网络安全的入侵警报器。我们知道，防火墙只能阻止通信量，而一个 IDS 能够检测出恶意通信量(如果存在恶意通信的话)，然后向系统管理员或者 IT 安全人员发出警报。而 IPS 则不仅仅能察觉恶意入侵，还能试图对其修复。

对于拥有错综复杂的网络的大公司，很自然的需要安装和设置这种检测系统以及防范系统。IDS 和 IPS 通常是较大规模网络安全结构的一部份，并且是随着防火墙一道安装的。

但是对于只有小型网络和若干 IT 工作人员的中小型企业(SMB)来说，IDS 可能显得有点奢侈。而且，还需要有工作人员能全天全周侯待命以监控 IDS。然而，中小型企业光有防火墙来实施保护是不够的。

这里有两种使用 IDS 和 IPS 的低预算方案，中小型企业可以考虑尝试。你可以使用适合较小公司小型网络的产品，或者也可以利用外包商们专为中小型企业提供的检测和预警服务。

但在你做任何决定之前，请先考虑一下评测 IDS 或者 IPS 的基本标准：你的网络的规模和范围，需要保护的数据和基础设施的类型，以及 IDS 将如何融入你现有的事故应对策略。

网络的规模和范围：你的网络的规模和范围是很重要的，因为 IDS 就像任何其他网络中的应用程序，可能影响网络性能。IDS 只是一种安全硬件，和你的防火墙以及病毒、垃圾邮件、内容管理过滤器一样。对于一个极小的网络来说，它会是一个很大的负担。如果是这样的话，具有良好处理能力的防火墙，会比完备的 IDS 更好控制。记住，防火墙能阻

止不必要的通信量，但并不总会记录它。IDS 记录不必要的通信量，但不一定能阻止它，除非还有 IPS。所以防火墙和 IDS 就像是硬币的正反面，功能互补?

另外，最近有很多产品结合了 IDS、防火墙、过滤以及其他功能，成为一种全能便利的应用软件。当中小型企业在考虑为小型网络购买一个价廉物美的设备时，可以考虑考虑这种产品。

数据和基础设施类型：中小型企业绝不能单单依赖 IDS 来实施保护。IDS 应该是一个多层防御系统的一部份，这个防御系统还应包括防火墙、安全进入管理、和桌面服务器硬件硬化。

另外，要想真正有效实施保护，入侵检测系统必须被安装在防火墙的两边以及内网和外网的通信量流入的网关处。IDS 并不是独立工作。它需要检测从各方来的通信量，无论是来自内部的还是外部的。把不同网段的检测结果进行比较，那么就能确定攻击的来源或者试图入侵的恶意程序了。内部攻击相当普遍，而且可以被确定，例如通过 IDS 对内部(而不是外部)网段可疑活动的检测。

为了让 IDS 融入你当前的应对策略，应当对你的服务器上存储的东西进行详细的风险分析：

1. 是可能导致客户身份暴露或者对你公司提起诉讼的重要客户信息吗?还是不仅仅关乎个人利益的人口和销售数据呢?

2. 你的服务器存储了私人公司信息或者计划吗?

3. 你的服务器存储了包括工资税和社会安全号码的员工信息吗?

如果数据风险不高，那么简单的防火墙就足以防止入侵。据说，黑客经常先闯入较低保护的系统作为后门，然后进入关键系统。低风险系统和存有高风险数据的服务器是隔离的吗?在安装 IDS 时，不仅要考虑数据风险级别，也要考虑系统结构和低风险到高风险的可进入性。

审查系统时，要检查它如何发送警报和发给谁。如果你的 IT 店只有一个人，那这个人能够应付得了没完没了的事故警报吗?而且其中很多可能是假警报。应该发送电子邮件吗?IDS 系统还会产生大量日志数据，大多数起不到任何作用。评测数据---及时处理以检测出真正的入侵---确实不容易。这种情况下，可以考虑使用那些可以帮助审查警报数据，并且能从黑客例行试探网络的普通无用数据找出真正入侵的产品。

（作者：Joel Dubin　来源：TT 中国）

入侵检测和防范：不仅仅是防火墙（二）

IDS 方案

这里有两个有趣的为中小型企业设计的应用软件，它们分别来自 iPolicy Networks Private 有限公司和 TriGeo 网络安全公司。

iPolicy 3.0 版，发布于去年 12 月，使用了被称之为 Real-Time Vulnerability Correlation (RVC)的程序。IPolicy 的 RVC 利用的是来自 Nessus 的数据(Nessus 是 Tenable 网络安全公司的一种流行的扫描工具)以及 eEye 公司的 Retina，Retina 可以将实时威胁信息与 Common Vulnerabilities and Exposures 和 BugTraq(两个 IT 安全界中有名的漏洞数据库)中的数据进行比较。用户可以根据资产的价值和风险级别来调整 iPolicy，RVC 然后通过资产的价值来确定威胁程度，并从它的 IDS 和 IPS 处发出警报。IPolicy 还包括抗滤过性病毒保护;它还可以监控因特网协议语音传输网络、即时信息和其它点对点式的通信(即使它使用的是非标准端口或者忙碌端口)。

TriGeo 的 Security Information Manager(安全信息管理器)因它的实时日志分析而出名，而且它像 iPolicy 一样能分析实况数据和网络行为以实行更细致入微的入侵检测。该产品能够把日志信息聚集合计成一个单一的实用报告。而不是从头至尾过滤多重日志，在通常情况下，TriGeo 把每个时间排列整齐，那么，你的 IT 人员只需要扫一眼，便知道该采取何种行动。

中小型企业还可以通过外包给那些专门从事入侵监控和事故应对的公司来实施保护。有三种厂商向中小型企业提供这种服务：位于亚特兰大的互联网安全系统公司(Internet Security Systems Inc.)，位于加州 Redwood Shores 的 Qualys 公司和位于加州 Cupertino 的 Symantec 公司。这些公司都有专门的工作人员，他们都是事故应对和处理入

侵方面的专家。不需要使用硬件 IDS，这些公司可以从他们的操作中心对中小型企业系统进行远程扫描和管理网络。

同样提供 IDS 应用软件的 ISS 公司，利用的是来自它的 X-Force 安全情报服务中心的信息，并且有一个门户网站，为客户提供实时更新。Qualys 是先根据资产的价值和风险分级，然后根据级别进行监测。Symantec 的 DeepSight 威胁管理系统能够通过分析公司系统的特定区域来检测攻击。

Symantec 同时也是 Sourcefire 公司的一个安全管理服务供应商合作伙伴，Sourcefire 公司是 Snort 的生产公司---著名的开源 IDS 软件。Snort 也可以作为一个不需要外包支持的独立产品，是一个可靠的受欢迎 IDS，中小型企业可以考虑使用 Snort。

由于安全威胁已经混合在一起，从硬件到网络和软件，所以需要入侵检测来实施保护。入侵检测已经成为一个较大的安全保护的一部份，还包括防火墙和漏洞管理，网络接入控制和端点安全。IDS 应当仅被视为中小型企业 IT 安全计划的一部份，不是全部。

（作者：Joel Dubin　来源：TT 中国）

IDS（入侵检测系统）最佳选购建议

问：我们公司正在准备购买 IDS 设备，并且已经挑定了几个品牌。你能给我们提供一些关于这些产品的资料以便我们来最终确定选购选择哪家的产品吗?我们知道这些 IDS 产品有许多相似的特性，我们应该如何依据标准检查程序并争取到合理的价钱呢?

答：正如我曾经在购买安全产品指南中提到的，拥有多种选择在采购安全产品过程中是十分重要的。由于 IDS 已经是一项成熟的技术，不同厂商的产品在技术上差异不是很大。事实上如果你只关心 IDS 产品的性能，你也许更应该关注开源工具 Snort。它通常被认为是评价 IDS 的三项重要标准之一，而且价格是免费的。

一般而言，我在选购产品时不会被产品评语、产品认证之类的检测结果所左右。这些资源无疑可以帮助安全专家去了解产品，在一定层面上对产品做出比较，但是这些并无法代替安装并测试产品是否可以满足特殊组织的工作要求。

在这种情况下，如果时间充裕，我还是建议实施这些产品在你的模拟实验环境中。除非经过测试，否则人们很难知道一个产品是否可以满足特定环境的工作需要。检测中你可能会发现用户操作使用你并不适应，升级更新过于烦琐以及其他一些麻烦。这一切都要经过测试，否则一切都很难说。

一旦你选定了在你的公司使用何种 IDS 设备，便要开始商讨价钱。切记在讨价还价前一定要确定你所选购的机器是可以使用于你的环境要求的。

（作者：Mike Rothman　来源：TT 中国）