配置 IPS

主动保护网络安全

配置 IPS　主动保护网络安全

入侵防御系统(Intrusion Prevention System，IPS)是这段时间网络安全业内比较热门的一个词，这种既能及时发现又能实时阻断各种入侵行为的安全产品，自面世那天起，就受到各大安全厂商和用户的广泛关注。本指南将帮助你深入了解 IPS，并介绍专家对 IPS 未来的预测。

入侵防御的定义

本部分介绍入侵防御系统（IPS）的含义，以及与 IDS 的区别入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。和入侵检测系统（IDS）类似，入侵防御系统（IPS）监测网络流量。但是，因为攻击可能在攻击者获得访问后非常迅速地发生，入侵防御系统也有能力立即采取措施，根据的是网络管理员建立的一套规则。

- 入侵防御的定义
- 入侵检测和入侵防御的区别
- 奔向 IPS 安全 不要漫步
- 什么是‘自上而下’的 IPS 传感器搜索？

入侵防御技术和配置

当人们谈及安全和入侵防御时，会冒出许多术语，并且含义不明确，很容易会混淆。本部分将介绍入侵防御中的关键技术及其含义，并对如何配置 IPS 以及如何避免 IPS 误报问题提出建议。

- 如何限制 IPS 的假阳性？

- 采用 IPS 的最佳实践
- 网络边界入侵防御策略中的关键技术(一)
- 网络边界入侵防御策略中的关键技术(二)
- 企业应该配置网络入侵防御系统吗?

入侵防御的作用

除了杀毒工具，我们还有一种方法对抗恶意代码和僵尸网络攻击：入侵防御系统。多数基于网络的 IPS 有它们自己的特征库用于检测漏洞和攻击性数据流。其中一些更进一步。但是为应付日益增多的逐渐加强的攻击，必须保证 IPS 本身的特征数据库是最新的。

- 入侵防御系统可防御僵尸攻击吗？
- 网络 IPS 抵御蠕虫病毒

入侵防御的未来

我们看到，过去的几年中，网络入侵检测和防御领域出现了一些进步。那么入侵防御技术的发展将会有哪些障碍和促进因素呢？在未来将会发生什么样的变化呢？在这一部分中，专家们提出了各自的观点。

- 入侵防御技术的未来
- 下一代入侵防御技术：性能的连续性
- 下一代入侵防御技术：攻击之前
- 下一代入侵防御技术：攻击中
- 下一代入侵防御技术：攻击后
- 下一代入侵防御技术：集成系统

入侵防御知识测试

本部分提供了对你的入侵防御（IPS）知识的小测验。

- 入侵防御系统（IPS）知识快速测试
- 入侵防御系统（IPS）知识快速测试答案

入侵防御的定义

入侵防御是一种抢先的网络安全方法，可以用于识别潜在威胁并快速做出回应。和入侵检测系统（IDS）类似，入侵防御系统（IPS）监测网络流量。但是，因为攻击可能在攻击者获得访问后非常迅速地发生，入侵防御系统也有能力立即采取措施，根据的是网络管理员建立的一套规则。例如，IPS 可能会丢失它认为是恶意的数据包，并进一步阻挡来了那个 IP 地址或者端口的流量。同时，合法流量应该传输到接受人那里，而不会出现服务的明显中断或者延迟。

据 Top Layer Networks 公司的 Michael Reed 说，有效地入侵防御系统还应该执行更复杂的监控和分析，例如对流量样式和单独信息包的查看和回应。“检测机制可以包括地址匹配、HTTP 字符串和子链的匹配、普通的样式匹配、TCP 链接分析、信息包异常检测、流量异常监测和 TCP/UDP 端口匹配”。

广义上来讲，入侵防御系统可以说是包括用于阻止攻击者访问网络的任何产品或者做法，例如防火墙和杀毒软件。

（作者：searchsecurity.com　译者：Tina Guo 来源：TechTarget 中国）

入侵检测和入侵防御的区别

问：IDS 和 IPS 的相似之处和区别是什么？在网络上他们可以被用于发挥相同的作用吗？

答：实际上，入侵检测系统（IDS）和入侵防御系统（IPS）在技术上非常类似，但是他们在网络上的功能有些不同。

IPS 和 IDS 工具都是为监控网络活动的迹象和滥用而设计的。它们识别潜在的恶意流量的有以下两种基本策略：

- 特征检测系统有一个包含已知恶意活动的样本的数据库。它们观察通信的所有和样本匹配的网络流量。如果发生了匹配，就会触发警告。
- 异常检测系统监控网络，并在一段时间，即“培训时期”内创建正常行为模式。然后他们观察网络中背离标准的活动。如果差异太大，异常检测系统就会触发警告。

IPS 和 IDS 的差异在于他们处理警告的方式。单纯的 IDS 系统简单地通知管理有可疑行为的发生。在另一方面，IPS 系统可以阻止可疑流量近土网络。实际上，两种系统都关注故意目的行为。大部分的入侵检测产品都可以在 IPS 或者 IDS 模式中运行，这都取决于用户的结构。

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

奔向 IPS 安全 不要漫步

入侵检测系统（IDS）和入侵防御系统（IPS）在今天的安全市场中增长很快，——而且没有下滑的迹象。

每年全球的 IDS/IPS 产品收入在 2007 年增长迅猛。使用这样的工具在成功保护 Windows 安全中非常重要，而且如果你还没有采用现在就需要了。以下将讨论 IPS。

如果你不熟悉 IDS 和 IPS，他们都是跟踪访问网络的活动的系统。

IDS：神经

IDS 工具可以和你已经在边界配置的其它系统协同工作，这些系统包括防火墙和路由器，并在遇到可能导致入侵的恶意活动发生时向管理员报告。

IDS 技术是基于已经有二十年的监控 windows 系统和网络的概念的。现在很多强大的企业级的防火墙和路由产品至少都包括这些功能，可以在恶意事件在外部开始发生时可以向监控系统提出报告。

IPS：白细胞

IPS 工具可以更进一步，识别环境中潜在的不正当行为，这样就可以自主向其它系统发出指令切断攻击。这些系统和白细胞很相似，可以阻挡入侵的细菌、病毒等。

IPS 技术相对比较新，主要是因为这些工具的复杂的逻辑和通信需要做出及时的决定，并向最近才可用的平行的设备发出命令。

IPS 的采用是不是有越来越多的选择呢？我不认为是这样的——但是我们应该是。让我来传一点儿福音吧。

我们需要作更多的事情。IDS 可以提供有用的警告，但是他们很像 Tom Clancy novel 中给总统的信息：不明核弹头正在向华盛顿发射。然后你要做什么呢？你要匆忙的组建团队，很可能需要研究报告，并可以比 IDS 报告获得更多的信息、识别受影响的系统并阻挡攻击者。所有这些都必须在攻击者掩盖踪迹之前的最短的时间内发生，如果踪迹被掩盖了，你就不能了解他们接触过什么了。（如果你不确定攻击计算机上是否有破解器，假定存在：只有在提供有力的证据后才是犯罪的。）

IPS 可以节约很多精力，但是真正的优势是速度，就是它执行这些行为的速度。我不能想象有一天当安全泄漏在没有任何手动调查的时候就进行处理，但是我可以预测有一天当泄露在发生的几秒内被阻止，而且向紧急响应小组要求回应阻挡受影响的系统。

IPS 并不完美，但是什么是呢？它是为你特定的网络设计定制的；它必须了解它是对什么发出指令的，它必须理解平常的流量类型，而且需要在不发生任何问题的定期当场更新。IPS 很昂贵，主要因为用于在电脑上持续不断的流量内部分析和检测样式的处理器电量不便宜，而且会造成假阳性。

IPS 不可能是万能药，但是泄露每天都会发生，而我们目前得解决方案也不会减少。我们需要可以提供下一步加强措施的 IPS。

（作者：Jonathan Hassell　译者：Tina Guo　来源：TechTarget 中国）

什么是‘自上而下’的 IPS 传感器搜索

问：IPS 传感器用“自上而下”的方式搜索特征文件是什么意思呢？

答：你可能对防火墙的“自上而下”的匹配方法比较熟悉。当防火墙遇到新的流量的时候，它就从规则的上部开始，检查每一条规则是否和流量匹配。当防火墙找到匹配的时候，它就执行某种行为并停止检查。即使流量和不止一条防火墙规则相匹配，它也只受最高等级的规则的影响：从上向下数的第一条。

IPS 传感器使用同样的方法：他们从列表的开始处理入侵特征，然后执行第一条匹配规则的特定行为。因此，每个公司都应该把 IPS 特征分类，这样最重要的特征就能处于最高的位置。这样，当信息包和很多条特征相匹配的时候，你就可以肯定是最高优先级的规则在执行 IPS 响应。把规则以这种方法分类相当简单。实际上，最简单的做法是以响应的严重程度排序：把所有“拒绝”规则放在列表的最前面，下面是“警告”规则。然后是“允许”规则。这样可以保证最强大的可用回应最先执行。

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

如何限制 IPS 的假阳性？

随着在全世界中，入侵检测系统（IPS）在企业数据中心和网络边界中越来越多的应用，假阳性的问题也凸现出来了。假阳性是这样一种警报：显示为系统上的恶意活动，但是在进一步的检测中证明是合法的网络流量或者行为。太多的假阳性会减少从系统中收到的数据的真正价值，而且随着网络攻击的增加会成为问题。以下从五个方法减少 IPS 的假阳性。

- **定义。**在把 IPS 应用到产品中之前，需要特别考虑网络中的正常使用模式中的定义、诊断和修复策略。造成过多假阳性报告的最大的单一作用因素是基线网络使用资料的无效率或者不恰当，而 IPS 用之监测异常活动。
- **慎重创建极限警报（threshold alarm）。**在最初的测试和展示阶段，要平均关注条件的相配、极限和触发，这样警告就不会在遇到较小的障碍或者异常活动的时候发出不必要的警告了。考虑一下，真正需要了解什么、网络上别人对你攻击的意义最大的部分是什么，然后再创建极限警告，使其只在你认为严重的事情发生时才会发出提醒。
- **考虑只在混合模式或者 bridge mode 下运行。**很多企业都选择混合模式或者 bridge mode，而不使用阻挡模式，来防止过多的假阳性问题阻止重要的合法传输。不运行阻挡模式仍然可以允许你阻挡简单的恶意流量类型，例如蠕虫，但是却在正常阶段把 IPS 设备的功能转变的更像入侵检测系统（IDS）。你可以总是打开阻挡模式，从而在你最需要的时候激活 IPS 的全面而详细的产品功能。
- **变更 IPS。**这可能是最坏的情况。基于简单的签名分析进行网络防御的 IPS 更可能发出错误警告。寻找这样的 IPS：包括连续稳定运算、基于 Windows 的时间比例限制（对于监测下班时间发生的攻击很有用处，而这些攻击可能在上班时间被分

析认为是合法流量）以及可以启发式的检测异常活动的特别的应用意识协议模式。

- **切记环境问题。**建立认为活动报告的人为环境。例如，Windows Media Player 播放的音频和视频是用户可以使用的合法过程，但是对于 IPS，WMP 中内置的端口扫描和发送机制非常类似于恶意端口扫描。需要对所接收到的事故报告创建人为的要素。

（作者：Jonathan Hassell 译者：Tina Guo 来源：TechTarget 中国）

网络边界入侵防御策略中的关键技术

当人们谈及安全和入侵防御时，会冒出许多术语，并且含义不明确时，很容易会混淆。在深入讨论入侵防御之前，我们先来定义几个术语。我不会试图对所有文章中涉及的每个术语提供确定的答案，但是我给出它们在边界入侵防御策略中的定义。

- ✓ **防病毒**
- ✓ **反间谍软件**
- ✓ **反垃圾邮件**
- ✓ **反网络钓鱼**
- ✓ **入侵检测与防御系统**
- ✓ **拒绝服务/分布式拒绝服务防御**
- ✓ **内容过滤**
- ✓ **应用程序控制与带宽管理**
- ✓ **法规限制**

防病毒

防病毒可能是边界安全中最常见的术语了，但是即使是这样一个简单的术语也有很多种定义。病毒、特洛伊木马程序、蠕虫病毒、以及恶意软件都是共同用于描述恶意（或许起初并非有害的）软件中的具体一种或另外一种形式的术语。例如，恶意软件的本质是和若虫不同的一种病毒。但是当我们说“防病毒”时，我们谈论的是检测是否存在这些有害软件中的任一种，并非仅仅是病毒本身。

病毒是一种可以感染其它应用程序的恶意软件。当这个应用程序由终端用户启动时，该病毒就被激活了，它既可以感染其它应用程序，也可以执行其罪恶的行为，比如随意删除你磁盘上的文件或者在你的 Web 浏览器上突然出现关于伟哥的广告。与病毒不同，蠕虫病毒既是独立的，又可以自动扩展；一旦感染了蠕虫病毒，人们将无法启动一个应用程序。特洛伊木马也是一种恶意软件，它可以伪装成一个合法的应用程序，但它不能扩展自己。

当然，黑客并不担心这些不同的分类——他们只是乐于使用特洛伊木马来携带一个蠕虫病毒的有效载荷，这个有效载荷也能像病毒一样传染应用程序。术语“混合威胁”通常就是用来描述这些混合病毒。

了解这些不同之处是非常重要的，理由是防病毒，尤其是在边界防病毒，可能拥有多种功能，可以在其生命周期内的不同时刻捕捉到不同类型的恶意软件。此外，你可能会在不同的环境中看到术语“防病毒”。

简单说来，防病毒技术在传输过程中查找恶意软件。最流行的恶意软件的自动扩展技术是通过电子邮件，这样的话扫描电子邮件中的恶意附件就是防病毒策略的重要组成部分。然而，恶意软件也可以留在 Web 站点上，边界防病毒扫描器也可以顺便检查 Web 数据流中的恶意软件。

这两项技术的问题在于它们不能保证从所见到的信息包重建病毒的有效载荷。加密的电子邮件和 Web 会议是一个问题，但是不标准端口上的 Web 信息流或者特定 Web 应用程序中的病毒也可能通过病毒扫描器。出于这个原因，边界的任何防病毒策略只能补充桌面上的防病毒程序。

第二个边界防病毒技术包括搜索病毒不当行为的标志。比如，著名的 Code Red 蠕虫病毒发送一个特殊的 URL，进而扩散到 IISWeb 服务器中。边界防病毒技术可以通过计算机的行为发现 Code Redf 感染的计算机。这项技术仅在感染发生以后，对识别恶意软件有用。然而，与了解到有人被病毒感染了相比，首先保护用户免于受到病毒感染的用处大不了多少。也有一些入侵防御工具专门用于寻找恶意软件的传播迹象，并可以使用该信息帮

助隔离那些受感染的系统。这些就是我们通常所知的“网络异常行为检测”（NBAD）系统。

反间谍软件

对你刚刚阅读的病毒方面的知识有了一定的了解以后，很容易就可以知道间谍软件（有时称为广告软件）是另一种恶意软件，并且采用相同的技术就可以检测到。间谍软件最普遍的传播方式是“隐蔽强迫下载”，在这种方式中，用户访问某个 Web 站点，并且作为一种副作用，将另外的软件下载在自己的计算机中。有时候，下载软件是在用户不知情的情况下进行的，或者 Web 站点可能试图故意迷惑用户，进而绕过浏览器的安全保护进行下载。用户甚至有意下载并安装间谍软件，通常是由于他们被欺骗性的宣传所误导，误认为该软件在某种程度上会提高他们的因特网技能。

至于原因最好留给阴谋论来解释，反间谍软件的处理方式通常与病毒不同。然而，寻找文件签名（尤其出现在网页中，比电子邮件信息中的更多）和异常行为的检测技术都与反间谍软件和防病毒技术有关。并且，与防病毒一样，桌面检测与防御策略必须增加一个边界防御。随着时间的推移，我们可以期待反间谍软件和防病毒软件将合并为一种工具，尽管现在市场上的风暴和骚乱已经导致许多企业不得不购买这两种工具，与这种日益严重的困境作斗争。

反垃圾邮件

与恶意软件检测相比，检测垃圾邮件难度要大得多，同时又要简单得多。因为任何大脑机能正常的人都可以产生出垃圾信息，新垃圾邮件的创造率相当高。同时，垃圾邮件只能通过电子邮件传播，所以改变这些信息流的方向，使之通过垃圾邮件过滤器，比捕获所有可能存在的病毒传播或者活跃的信息流要简单得多。

反垃圾邮件技术与防病毒技术的另一个不同之处是反垃圾邮件的警报误判（合法信息被标记为垃圾邮件或者垃圾邮件被标记为合法信息）率比防病毒软件要高得多。换句话说，更多的垃圾邮件（与病毒相比）通过，并且更多的信息（与病毒相比）被归类为垃圾

邮件。结果，反垃圾邮件特征，比如终端用户隔离以及单个用户灵敏度设置与白名单，通常决定着终端用户的满意程度。

反网络钓鱼

多种有害的或者恶意的邮件，网络钓鱼邮件可由与垃圾邮件相同的方法检测出来。在技术层面上，任何反垃圾邮件工具同时也可以是反网络钓鱼工具。在市场层面上，把这两种威胁合并到同一个产品上的理念是无法抵抗的，因此产生了大量专门处理这两种威胁的工具。

由于反间谍软件与防病毒软件有关，因此，反网络钓鱼是与反垃圾邮件联系在一起的。所有能够处理反垃圾邮件的工具同时也擅长于处理网络钓鱼攻击。

另一种基于网络行为的反网络钓鱼正在一些边界防护经销商中间流通。由于网络钓鱼电子邮件通常要求读者点击一个某个网页的链接，并提供了相关信息，理念是你可以帮助“受感染的用户”——他们受到网络钓鱼电子邮件欺骗，访问设有圈套的网址——通过采用 NBAD 系统捕获这些连接。结果是这种技术也是为标准的垃圾邮件服务的（因为用户被引导进入网站订购毒品、观看色情视频，以及购买股票），但是由于对用户的损害并不重大，一般不使用该技术。

现在，大量的边界入侵防御产品都在电子邮件中使用 URL，此外，终端用户点击 URL 来检测来袭的垃圾邮件/网络钓鱼邮件并输出反应情况。本质上来讲，虽然这与用于检测正在传播或正在攻击的恶意软件的技术是相同的，但是，它致力于一种具体任务：阻止用户回应任何网络钓鱼电子邮件。

入侵检测与防御系统

尽管这些产品家族听起来似乎应该有一定的联系，但是它们几乎没有类似之处。入侵检测系统（IDS）在网络中的一个或多个端点检测数据流，并就可疑或恶意的信息流提供警报和鉴定。IDS 的关键部分是警报系统，以及鉴定和输入意图的数据存储。

入侵防御系统是一个内嵌的设备，可以阻止恶意信息流。一些早期的 IPS 并不是内嵌的。它们可以检测到恶意信息流，然后减轻该信息流的影响；比如，可以采用 TCP 重置的方法进而淹没发送器和接收器，或者改变防火墙或路由器中的访问列表规则。然而，同时代的 IPS 看起来都一样：内嵌的信息流评估器寻找一些理由，丢掉信息包或者重置连接。由于 IPS 搜索恶意信息流，因此与 IDS 相比，它区别性更少，并且更为仔细。

比如，在网络中，IDS 可以检测到蠕虫病毒的在网络内部扩散，并且警戒这些企图。然而，IDS 可以按照对系统受到攻击的企图，攻击对企业的重要程度，或者按照特定攻击企图的漏洞进行分类。IPS 的复杂度并不相同。当 IPS 注意到一个明确的攻击企图时，就会简单地阻止这个攻击。受到攻击的系统是否存在漏洞、是否重要、甚至该系统是否存在，这些并不重要。IPS 可以安全地阻止明确的攻击企图。然而，IPS 一定不会阻止合法的信息流。因为 IDS 发出警报，而 IPS 阻止攻击，大多数 IPS 仅有几百个激活的特征（防止产生误报：将非法信息标记为合法信息），而 IDS 通常有成千个攻击特征。

并非每一个 IPS 都使用特征来确定攻击，并且甚至那些使用特征的 IPS 也可能会与其它技术相结合，帮助确定（并阻止）恶意信息流。NBAD 系统的范围与 IPS 功能有一部分是重叠的，这些产品尽管使用不同的技术，但通常被认为可以解决类似的问题。

拒绝服务/分布式拒绝服务防御

IPS 也是“以速率为基础的”，意味着它们寻找不正常的信息流。这些系统也是一 DoS 和 DDoS（拒绝服务攻击和分布式拒绝服务攻击）防御工具为标志的。基于速率的 IPS 可以与特徵式 IPS 相结合。然而，由于它们抵御不同类型的攻击，它们通常配置在网络的不同端口，并保护不同类型的系统。比如，以速率为基础的 IPS 最常用在大型网络服务器池或者大型电子邮件服务器的前端，而特征式 IPS 是直接配置在公司防火墙内部（或者作为企业防火墙的一部分），进而保护终端用户或者更多普通类型的服务器。

IPS 和 IDS 执行异常行为检测，或者寻找特殊的病毒或网络钓鱼行为，它们就会作为防病毒或反网络钓鱼工具而出售。尽管这是这些产品中非常有用的一方面，但重要的是你不能 IPS 或 IDS 座位一种反恶意软件或垃圾邮件的“第一道防线”。

内容过滤

内容过滤工具可以使用大量不同的技术，其目的都是为了实现同一个目标：限制来自公司电脑上的有害内容。通常情况下，内容过滤几乎都用于网络浏览文本，尽管这个想法可以用其它方法来扩展。大多数内容过滤使用分类阻止的方法。内容过滤器可以在网络 ULR 离开公司网络之前进行监测，并且与大型数据库进行区分比较。URL 可能作为未知返回来，或者可能适合于某个类别，比如“运动”或“赌博”。基于这种分类，网络管理者可能选择阻止信息流进入那些类型或者全部的网站，或者以一些其它更多的限制标准为基础，比如每天的时间或者用户认证信息。

实际上，一些内容过滤器着眼于捕获那些没有经过合理分类的信息流，并将其返回，进而试图分析这些内容。它的长度已经非常长了。举例来说，试图分析图片内容的产品已经上市，其特殊目的是为了阻止色情图片。

内容过滤并不是一个特别可靠的技术，并且一般不能阻止有特定用户下载不合适的信息。然而，它通常用于这样的环境中：需要某种过滤（比如初等学校），或者一些技术实施支持固定的安全或使用策略（比如在一个面向客户的零售设置中）。

应用程序控制与带宽管理

内容过滤对网络浏览的作用，和应用程序控制和带宽管理对所有其它类型的应用程序的作用是一样的。这两种技术都是用于阻止或者控制某种特定的网络使用类型的。应用程序控制通常是高级防火墙的一部分，而带宽管理则是集成到防火墙和其它基础体系设备里的，比如路由器，或者通过独立的设备便可处理。

与内容过滤相似，应用程序控制通常用于这样的环境中：技术实施必须带有一项规定的使用策略。比如，如果某个公司想要禁止使用 Skype 公司的 voice-over-IP，应用程序控制就可以用于执行这个禁止令。

法规限制

从广义的范畴来讲，法规限制的概念是范围足够大，包括其所有条款。然而，边界的大多数法规控制可以分为三个字类：泄漏防护、审计和日志记录、以及流程稽核。

泄漏防护最难配置。泄漏防护工具借用了 IDS 的技术，通过在边界进行检测，试图监控和管理流出企业之外的敏感信息流。依靠调节体制，这个范围可以从受保护的个人信息（比如个人健康资料）到公司的敏感财务数据。

审计与日志记录工具是比较被动的，旨在帮助企业遵守审计访问的要求（比如公司的财务信息）或者保持长期的记录（比如企业外部的所有即时通讯信息流）。

流程稽核工具在确保企业外部连接遵循符合适用调节体制的策略方面更加活跃。最常见的例子就是对敏感信息加密。比如，一个流程稽核工具可以观测医院和保险公司之间的电子邮件通信，也可以阻止任何没有加密的通信，或者访问并对其按照策略的要求进行加密。

（作者： Joel Snyder 译者：李娜娜 来源：TechTarget 中国）

企业应该配置网络入侵防御系统吗?

三年多以前，我在大型学术网络上见证了试验性配置入侵防御系统（IPS）的情形。我们正在讨论的技术是一个顶级经销商（该经销商今天仍然存在）力荐的产品。该产品已经做了大量的销售广告，许诺消除所有的网络威胁，并且多年来首次使安全分析家高枕无忧。

那么启动该系统后发生了什么情况呢？正如你所预料到的，在 15 分钟内，它就崩溃了了，在一个未过滤的网络连接上，被试图推行经销商所谓“最佳方式”的 IPS 信号所淹没。执行失败并与其它组织的同事交流以后，我们发现，显而易见，那时的企业还没有完全准备好配置 IPS（或者，更好的说法是：IPS 技术还不够成熟！）。

三年过去了，换了一些销售代表以后，还是那些经销商正忙于敲我们的门、打电话、承诺 IPS 市场已经“成熟”了，是时候再给这项技术一次机会了。今天的 IPS 设备能跟上高速网络连接，并且进程规则数据库变得更有效率。我不能确定技术本身是否已经成熟；但实际上，它并没有发生很大的变化。

入侵防御系统是入侵监测系统的一个基本扩展；它们可以监测到对网络的攻击，并且一旦监测到，可以准确阻止其到达目的地。这与入侵检测系统（IDS）形成对比，IDS 允许攻击通过并随后提醒管理员。当然，不同的经销商已经加上了一些铃声和口哨声，比如 IPS 与网络设备交互的能力（防火墙、转换器等），这些功能可以在网络中的不同点实施执行准入控制决定。多年来，经销商已经添加了监测暂漏头角技术性攻击的能力，比如那些反 VoIP 系统或 IPv6 网络。

然而，一个成功的 IPS 产品归结到底是一个高质量的监测引擎和平稳的用户界面。核心技术与第一版 Snort 有惊人的类似度。Snort 是一种流行的开源入侵检测系统，10 年前，Sourcefire 公司的创始者 Martin Roesch 向世界介绍了该系统。

尽管如此，我的确相信在过去三年间入侵防御系统的使用和采用已经发生了显著的变化。然而，标志性变化不在于新添加的特色，而是经销商和安全专业人士在配置和维护 IPS 时所采用的最佳方式。

这里有一些关于最佳方式的简单总结，您可以遵循以下几条，以成功实施 IPS：

- ✧ 在“监控”模式下运行 IPS，直到确定系统的配置合理。在企业网络中采用经销商授权的默认策略，简单地将其调为免除格式，进而配置 IPS，这种做法是一个巨大的错误。（如果你忘记了这么做的理由，请重新阅读这篇文章的前两段！）在监控模式下配置设备更为安全，监控模式与 IDS 的运行方式相同。仔细观察，直到它正确地执行你企业的安全策略，让您满意为止。

仔细检查任何一个警告，留心误报检测信号，并且切记一旦你在这些任何一个规则中启用积极反应，那么这些连接确实会受到阻挡。这里关键的一步是：调试阶段投入大量的时间分析 IPS 警报。简单地数出误报数目是远远不够的。深入研究它们：如果两个误报就已经阻止了你的电子商务应用程序与销售数据库相连接，会怎么样呢？保全自己，谨防犯下导致职业生涯结束的错误。

- ✧ 保持“块”模式规则的数量在一个微小、精确的设置状态。最为成功的 IPS 配置使用了一种混合的 IDS/IPS 方法。只需要设置与极高信用率有关的规则便可，以阻止信息流横穿网络。比如，如果 IPS 检测出某个网外系统使用 SSH 探测器系统地搜索了你的地址空间，你绝对想要阻止该通道。过去几年间，经销商也已经对这种忠告熟悉起来。现在，大多数经销商推荐“块”规则的一小核心组，同时将其余的保留在典型的 IDS 警戒模式。这是一种谨慎的态度，能够显著提高你成功配置 IPS 的可能性。
- ✧ 考虑使用应急开放设备。IPS 的另一个缺点是为了在“块”模式中运行，设备在物理上必须是内嵌的。正如任何网络工程师告诉你的，内嵌设备的数量越少越好。在网络中增加单点故障是存在的一个问题，此外，当出现一些尚未找出原因的问题时，这就为其他任何人提供了指责安全小组的机会。

阻止这些问题发生的方法之一是在 IPS 上使用应急开放技术。这样，如果设备失去作用，它就像一根直铜线，不会导致整个网络中断。如果预算允许的话，也可以考虑将备用 IPS 设备配置为高可用性模式。

总之，毋庸置疑，IPS 市场在过去三年中已经变得成熟了。这些变化不仅仅体现在技术本身之中，而且体现在其配置和操作方式上。现在，经过恰当的管理，IPS 设备在企业安全构架中可以起到重大作用。

（作者：Mike Chapple　译者：李娜娜 来源：TechTarget 中国）

入侵防御系统可防御僵尸攻击吗？

问：入侵防御系统（IPS）是防御僵尸攻击的最好方法吗？在企业环境中有没有其他方法可以用于防御这些威胁？

答：网络入侵防御系统提供了对僵尸网络的防御，但只是一部分。很多现代的 IPS 系统都有流行僵尸网络控制流量的特征库，当僵尸网络想要获得攻击者的命令行的时候，系统就会发出警告。其他的 IPS 系统可以更加深入，可以阻止僵尸网络控制他们检测到的流量。但是应该注意网络 IPS 只有大部分流行的僵尸网络的特征库，而不是所有，所以需要进一步的防御。

主机 IPS 是另一层的防御。这些工具限定了在系统上运行的不同应用，阻止他们和基本内核的交互作用。但是有些僵尸网络可以把自己安装到合法应用的内部，用以 u 破坏系统，并可能可以躲避主机 IPS 的检测。

所以，除了网络 IPS 和主机 IPS，还应该确保你已经配置了杀毒软件、反间谍软件和主机防火墙。通过操作这些前面的工具，你可以大幅降低企业环境中僵尸网络的威胁。

（作者：Ed Skoudis　译者：Tina Guo 来源：TechTarget 中国）

网络 IPS 抵御蠕虫病毒

除了脆弱的杀毒工具，我们还有一种以网络为中心的方法对抗恶意代码：基于网络的入侵防御系统（network-based intrusion prevention system，以下简称基于网络 IPS）。尽管基于网络的 IPS 用于对付洪水攻击（thwarting denial-of-service），保护系统不受威胁已有数年时间，但用于阻止蠕虫病毒的传播只是最近于开始流行。

这一技术的的主要思路是：一个组织在其网络的关键网络结点(strategic point)部署基于网络的 IPS，实际上形成了自动的阻击点用于检测和阻止攻击。比较典型的情况下，这些工具在线运行（inline），监测通过的网络数据流，将这些数据与已知的攻击代码进行特征匹配，截留恶意代码。另一些工具不在线运行，而是监测 LAN 中的数据流，向网络中注入消息阻断攻击并阻止恶意代码的进一步传播。不同于基于网络的 IDS（IDS 主要功能是发现恶意代码、发出预警），基于网络的 IPS 不仅发现恶意代码、发出预警，还会自动做出反应：阻断通信或是重置连接。

当一台主机受到蠕虫病毒的感染时，运行于其上被控制的系统会开始自动地搜索其他易受攻击的主机。当这些数据流到达时，基于网络的 IPS 工具可以自动地发现它们，并且抑制这种搜索和传播病毒的数据流，以防止在 IPS 另一侧的系统受到感染，或是做为同一 LAN 上其他系统的 IPS 防止这些系统受到感染。值得注意的是，只有这些基于网络的 IPS 接收到数据流才能阻止恶意代码的传播。如果仅仅在整个企业网络中部署少量的监测点，它们确实可以防止病毒在网络上的传播，但也会留下一些真空区域易受攻击。

一些成熟产品，如 ForeScout 公司的 WormScout、TippingPoint 公司的 UnityOne、Top Layer 公司的 Attack Mitigator、McAfee 公司的 IntruShield（即以前的 IntruVert）和 ISS Proventia，都属于这一类产品。也有一款开源且免费的基于网络的 IPS 产品 snort_inline，它建立在 Snort IDS 之上，由 Rob McMillen 在 Honeynet 工程中进行维护。

读者可能会想：这些不就是防火墙支持的功能吗？当今的大多数防火墙检查数据包和协议，根据端口和服务的设置确定是否传送这些数据包。但是这些防火墙没有特征匹配功能用于检测漏洞、恶意代码或流量激增。换句话讲，防火墙只是检查服务和端口，并不检查是否具有攻击的特征和行为。IPS 检查后者。

尽管如此，基于网络的 IPS 这一分类在防火墙是否也算做其中之一这一问题上，有一些模糊不清。随着防火墙中内建了越来越多的技术识别实际的攻击代码，防火墙与基于网络的 IPS 的之间的区别在逐渐减少。实际上，Check Point 公司产品 Application Intelligence 的功能和 Juniper Network 公司产品(NetScreen) Deep Inspection 的技术都是防火墙的扩展，它们试图对已知的攻击进行特征匹配并且阻止这些攻击，修补很多蠕虫病毒使用的常见漏洞。这些使用了相应功能的防火墙，构成了一种形式的基于网络的 IPS。不远的将来还会出现更多的具有 IPS 相似功能的防火墙，让我们拭目以待。

多数基于网络的 IPS 有它们自己的特征库用于检测漏洞和攻击性数据流。其中一些更进一步，它们监测网络流量(traffic load)，用于与已有的正常流量对比。比如 TippingPoint 提供了一种称为 Statistical Anomaly Control 的功能，这一功能监测不同协议的流量并与预期的基准流量进行比较。当网络流量超过基准流量时，基于网络的 IPS 会减小数据流或阻断它。举例来说，考虑感染 Nachi 病毒后产生的 ICMP(互联网控制信息协议)数据流，当寻找新主机进行攻击时，如同洪水一样发送 ping 数据包。TippingPoint 的内置智能认为 100Mbps 的数据数对于 ping 数据流极为不正常，并决定阻断这一数据流，这一过程完全不需要任何人工的干预。

当检测到蠕虫病毒攻击时，基于网络的 IPS 设备可以以多种方式自动地采取行动，但是，用户需要仔细地配置设备做出何种方式的反应。大多数的工具都有对应于不同处理方法的选项，这些不同的处理方法包括减小流量以保留一部分带宽、用 TCP Reset 重置连接或是发送 ICMP Host Unreachable（无法访问主机）消息、或是简单的丢掉与蠕虫病毒相关的数据流以阻止其传播。仅仅减小流量导致一个典型的问题，一些机器可能仍会被感染。重置连接或是由这些工具发送无法访问主机信息可能会导致更多的攻击，这将占用用户最需要的所有的带宽。数以千计被蠕虫病毒感染的系统寻找新猎物产生巨大的网络流

量，用户的网络在这样的重压之下喘息，而不能用基于网络的 IPS 自身产生的重置数据包化解这一问题，这种情况非常糟糕。另外，精心设计的蠕虫病毒还可能忽略这些重置数据包而继续传播。由于这一原因，彻底地阻止与蠕虫病毒有关的网络数据流通常是基于网络的 IPS 最有效最安全的设置方法。这样，阻止了蠕虫病毒的传播，也保留了网络带宽。

此外，为防误报而开始阻止合法数据流，应确保基于网络的 IPS 配置为立即提醒紧急情况处理团队中的工作人员。他们可以人为的确认是否为攻击，可以允许被错误地阻止的合法数据流，或是当发生感染时启动一个清理的过程

如果部署这一技术，也不要放弃或是减弱其他的防御措施。我曾经有一个顾客，由于他们部署了一个新款的基于网络的 IPS，而计划降低他们服务器上设置的安全等级并去掉与边界路由器之间的 ACL。在线或是在 LAN 中的基于网络的 IPS 需对攻击进行实时的判断。要满足这样苛刻的性能要求，特征数据库及基于网络的 IPS 的适用性往往不如基于网络的 IDS 和基于主机的 IPS 全面。

由于它具有实时监测的能力，基于网络的 IPS 做出误判而带来的损失也较显著。不同于由紧急事件处理团队做出的误判（这可能是 IDS 引起的错误），或是只阻止了从一台主机发出的动作（这可能是基于主机的 IPS 发出的错误警告），基于网络的 IPS 做出的误判可能会严重到禁用一个网段，或是整个的网络连接，这取决于客户的网络结构。记住这一点，基于网络的 IPS 不是防火墙或是基于主机的安全设置的替代品。将基于网络的 IPS 应视为现在防御系统基础上额外的一层防御，并保证其他的防御措施（传统的防火墙、IDS 产品、杀毒工具和文件完整性检查工具）升级到最新。

而且，为应付日益增多的逐渐加强的攻击，必须保证基于网络的 IPS 本身的特征数据库是最新的。需要自动的定期更新数据库，或是根据服务商发布数据库的周期每天手动更新数据库。仔细的切换这些工具也非常关键，以保证它们能辩认正常的网络数据流，并能区分攻击数据流（译者注：特征数据库中的数据包含大量恶意代码的特征，与攻击代码的部分代码段可能很相像，可能产生误判）。

最后，如果你还没有使用基于网络的 IPS，请关注一下这一技术。它可以提供一个有益的用于防御层。如果你还没有做好准备购买，但希望更熟悉这种工具的功能，可以在实验室或是运行非关键任务的服务器前端尝试运行一个 snort inline。然后决定是不是部署这一技术。

（作者： Ed Skoudis 译者：陈志辉 来源：TechTarget 中国）

入侵防御技术的未来

如果说分而治之对于解决问题是一个成功的策略，那么入侵防御仍然在分化阶段。大多数网络使用防火墙，许多使用 IDS，它们都有防病毒和反垃圾邮件的软件，并且一些网络使用 IPS。但是却没有一个经销商将这些技术结合成一个整体并进行管理，进而使得使用更简单。

提出更多全程的术语，大多数网络管理者在其网络上拥有大量的各种高效控制端口，不论是外围还是核心。然而，正如任何一个工程师告诉你的，仅有控制端口的网络并不等同于一个受控网络。受控网络需要测量端口、控制端口和反馈回路，以保证所有的端口均在限度里运行。当然，数据网络不同于石油管道网络——除此之外，在很多方面它们相似。我们处在可以控制的安全体制之中，但是我们不知道需要控制什么，以及为何要控制。

防火墙中关于统一威胁管理（UTM）意见之一似乎可以更好的进行综合管理，答案并不是将各种功能集中在一个盒子里。在小型网络中，单一的 UTM 防火墙是仅有的一个防御端口，单个管理端口的优点很突出。然而，当 UTM 经销商出于安全都在努力创建各站代办处时，他们会乐意承认 UTM 防火墙并没有涵盖所有的基线。如果你的 UTM 防火墙有一个病毒扫描器，那么是否意味着在桌面上你就不需要防病毒软件了呢？UTM 防火墙也可以退一步解决问题：当然，你现在可以管理一个单独的端口，但是如果你有两个端口怎么办啊？

必备知识

带有许多分布式控制点的网络能够各行其责，原因之一就是：过去，我们几乎不需要网络本身的知识。但是今天，大多数网络由数量巨大的一两条指令进行了大量设计，并且这种趋势仍在继续。观察带有 10 Gbit 端口的小型配线柜交换器在未来 12 个月中的增长情况，你就会得出进一步的证据。

构建一个十倍或者百倍于需求容量的大型网络比构建一个满足需求的网络要容易得多。网络经销商已经全心全意地跟上了这一潮流，并且提供了数量可观的经济鼓励。在他们心中，当一个 10/100/1000 交换器仅售几百美元时，谁会在配线间里安装一个 48 个端口、10/100 的交换器呢？

随着网络设备的价格大幅度下降，我们趋向于买许多快捷、便宜的硬件，而不安装和多需要测量和管理的工具。由于诸如交换器和路由器之类的基本设备组件之间的价格存在差距，以及越来越成熟的管理与控制产品的不断增加，比如 IDS 和安全信息管理（SIM），这种趋势将会继续下去。人类的时间观受到如下因素的影响：一个自动的交换器需要花费 1000 美元，网络管理人员需要花时间来安装，但是该交换器运行的时候几乎不需要任何费用。这样价格差距会更大。将 IDS 安装到网络中，并且你需要每周花几个小时来保证设备可以良好使用。这是一个巨大的代价。结果是产生了“黑箱”网络：网络有大量的连接点，看不到其运行情况。

构建这些黑箱网络的结果是它们大部分时间运行良好——除了它们运行不好的时候。当不必要的网络中断变得更加频繁时，网络中断的后果越来越来越严重。IT 性能以及甚至因特网的连通性更紧密地与关键操作结合在一起，对坚若磐石的网络性能的需求也变得极为重要。如果你将 CRM 外包到 SalesForce.com 中，但是又无法进入网站，你将如何销售？如果你转向一个无纸传输信息的物资需求计划（MRP）系统，当一堆材料出现在装载码头时，该系统又无法利用，你该怎么办呢？

这依赖于网络，也就意味着需要一定的知识，尤其是网络方面的知识。了解我们的网络内部的具体情况，我们就可以预防或阻止问题，并且当问题出现时，可以更快地解决问题。

你可能知道的太多

当我说你需要网络方面的知识，我并不是指全部的知识。很容易陷入这样一种陷阱：花费整天、每天的时间来查看你网络上一些毫无意义的安全和性能数据。任何网络知识、控制和可见性的投资都必须考虑其对公司的价值。获得太多的信息很容易。实际上，这种

情况很普遍。我们的每一个控制点通常几乎都是测量点，并且如果你简单地开启日志记录或统计资料，你将很快被数据所淹没。

将数据转变为有用的信息是一项相当艰巨的任务。我们今天现有的所有数据处理产品通常都要么范围过于偏大，要么范围狭小。比如，SIM 系统看起来不错，但是大多数的设计目的仅仅是用于处理防火墙和 IDS 的日志，几乎很少处理相关的网络流量数据。这些 SIM 规模更大，花费几十万美元，需要大量连续的人力资源进行检测，需要巨大的投资来解答最基本最简单的问题：这个网络健康吗？安全吗？我们是否需要增加性能？如果需要什么时候进行？

这是现在不令人满意的情形：大多数网络的构建和管理都是以黑箱进行的，在使用中很少或者没有监控和管理能力。虽然一些网络拥有它们所需要的所有监控，但是安装却需要大量的花销和高额的连续操作成本。此外，一个更多的花费已经用于安装了一些检测工具，但是由于这些工具不能满足 IT 工作人员的要求，或者因为这些工具需要花很长时间，因此它们从未得到使用。

未来的解决方法

今天，安全专家提供了一些构建黑箱网络的选择。在这样一个预算紧张以及安全与网络小组之间没完没了的紧张局势的时代中，仅仅大型企业可以负担得起购买产品和员工的开销，因为这些工具需要提供真正的网络可见性。这将随着时间而改变。越来越多的安全产品和网络信息经销商都开始考虑开发优良的产品，增长的网络和安全可见性带来一系列优点，而新开发的产品可以利用这些优点进而达到合理需求和运行费用之间的平衡。今天的关键之处是合理安置网络和安全的结构体系，并充分利用市场上的这些新产品。

确定了目标以后，考虑下面的策略为将来做好准备的同时提供临时的缓解方法。

1. 大多数安全控制点都有能力为外部设备提供日志。然而，诸如交换器和路由器之类的网络控制点的性能通常较差。将企业的安全和体系结构方面的信息结合起来，这一点很重要，进而可以创建一个有效的安全策略。确保你与网络小组共同工

作，将新的设备指引成为“安全报告兼容”形式。对于交换器，可能和 SNMP 性能端口的统计资料以及转发表一样简单；而对于路由器而言，流量分析资料和 NAT 表格就变得极为重要。这可能需要一些压力，因为制造一种可以传递流量统计资料的路由器会增加成本。

2. 了解什么类型的数据对你来说是有用的。当一些糟糕的情况发生，你是否需要报警呢？那种情况下，过滤 IDS 和 IPS 日志中重要事件的产品可能很容易启动，而且一些工具将漏洞分析信息与攻击警报结合起来，这些工具用处更大。你是不是在寻找鉴定信息来跟踪问题和非法闯入者？SIM 设备和 IDS 的“超级控制台”可以帮助提供相关信息，研究问题时，这些信息可以分离重要信息与相关信息。采用今天可用的集中单点解决方案工具，可以获得经验，因为这有助于发现你在未来需要什么。
3. 最安全的产品，比如 IPS 和病毒扫描器，在入侵防御中是主动的。然而，比较被动的工具，比如异常行为检测系统和 IDS 可以提供真实安全可见性所需要的多余数据。即使你现在没有这些工具，计划一下你会将它们配置在什么地方，并确定你设计网络是为了这些所有可见的设备。偶尔检查一些开源 IDS 传感器，即使你不经常查看这些结果，它们会给你更多的信心，你可以在合适的点收集到合适的数据。
4. 在你的企业内部构建网络与安全小组之间的沟通桥梁。大多数企业在这两种职责的分工上采用了非常生硬的方法。最终，随着网络安全成为网络本身的核心功能和需求时，这种分工会消失。由于难以区分外围安全与核心安全，网络与安全状态信息的可见性同时将是任何监控系统的一种假设。现在关系更为紧密，你就可以确定企业网络持续的建设和升级可以满足这些可见性的要求。

（作者：Joel Snyder　译者：李娜娜 来源：TechTarget 中国）

下一代入侵防御技术：性能的连续性

我们看到，过去的几年中，网络入侵检测和防御领域出现了一些进步。这些进步大部分建立在增加数据传输和增强事件侦测能力的基础上。比如，大多数特征数据库已进行了扩展，考虑了所适用的协议。当然，这也导致了一个技术发展趋势，即实现实时反应（如阻止攻击），尽管相对于人工事后启动的校正措施这一技术应用还较少。然而，如果人们需要，尚难以确定这一技术能否在更大的程度上发挥作用。

入侵检测与防御技术面临的巨大挑战是，这些技术只能在一个表示入侵进行过程的时间线（timeline）的一个结点上发挥作用。由于多种原因，理解这一时间线是非常重要的。市场上充斥着一系列自封的、包罗万象的策略、使用须知、配置方案、补丁、漏洞、威胁和某某管理技术和功能，理解这一时间线有助于从这一混乱的局面中厘清它们的位置。也可以帮助企业建立一个全面的监测和反应过程。它也是下一代入侵防护的关键---一个集成了不同模块功能的系统，并且使用最佳加强措施。

时间线本身是一个相对明了的概念。它包括三个主要部分：攻击之前、攻击之时和攻击之后。简要地说，攻击之前的工作是尽量少得暴露弱点；攻击之时的工作是处理已被攻被和正在被攻击的防御弱点；攻击之后的工作主要是扩展检测（extended detection，例如事后检测）和修复、清理。

坦白地说，一些攻击的性质使得时间线的划分模糊不清。比如，强度弱且缓慢、多阶段的攻击是否有一个确切的攻击时刻这类问题是有争议的。相反，它们可视为由多个攻击事件组成，如果没有检查到，会逐渐积累为一个更严重的可识别的攻击。这些细微的差别在本系列文章的第二篇进行详细讨论。在这里，关键的问题是，在一个攻击的不同阶段可以应用不同的技术和子过程，通过实现一个有效应对每个阶段的解决方案，可达到挫败入侵的最好效果。因而，非常有必要对每个阶段进行深入的考查。。

（作者：Martin Roesch　译者：陈志辉 来源：TechTarget 中国）

下一代入侵防御技术：攻击之前

从宏观角度看，配置管理（configuration management）可能是描述与这一阶段有关的活动的最好术语，虽然这一状态也可以称为漏洞管理（vulnerability management）。不论如何称呼，按我们划分时间线的目的，攻击之前的阶段可以从逻辑上分为两个分离的时间段。

为了完成对计算机环境的适当配置，通常在进攻之前相对较长的时间（比如，几周或是几天）对系统的安全性进行评估。这就需要查明已建立措施的缺陷和漏洞，这两种都可能是软件编码的错误，也可能是配置的错误。可以应用各种各样的扫描技术，检查到的问题随后要进行处理，比较典型的是打补丁，重新配置受影响的设备或是重新配置上游的安全设施。

很明显，这些都是具有积极意义的预防性措施。它们构成了通常的方案。这种方法建立在周期性的快照基础之上，这种技术在应用的数量方面不断的减少，因为发现一个漏洞到利用该漏洞进行攻击之间间隔的时间在持续地缩短。相反，下一代入侵防御技术正在定义的一个特征是显著减小评估周期的能力，理想的情况是在某种程度上提供一些永远在线的、被动式的扫描功能，与按指令进行的、有较强针对性的主动扫描功能配合。

攻击之前的第二个部分指一个潜在的攻击正要发起实际进攻的那个时间。这是传统的访问控制工具发挥作用的领域，比如防火墙和具有 ACL（access control list,访问控制列表）的路由器，它们可以用例行措施阻止一个迫在眉睫的攻击，这是它们配置参数中包含的规则。虽然这一方法并不足以抵抗攻击，这些工具在使问题域变得更加容易管理方面还是非常有效的。下面第三部分会谈到，也存在更为动态的使用这些工具缓解攻击的潜力。

在下面的部分我们仔细地考查与攻击之时和攻击之后这两个阶段有关的技术和过程。

（作者：Martin Roesch　译者：陈志辉 来源：TechTarget 中国）

下一代入侵防御技术：攻击中

本系列文章的前几篇讲到充分地分析入侵防御问题需要考虑整个的攻击过程。前面文章将连续的攻击过程分为三个不同的阶段：利用漏洞进行攻击之前、攻击之时和攻击之后，并且随后非常详细地描述了与第一阶段相关的过程和技术。本篇着重分析余下的两个阶段，为进一步讨论下一代入侵防御技术的必要条件打下基础。

攻击的种类是多种多种的，在一定程度上难以准确地界定整个攻击时间线上的这一部分。有些攻击可能以短时间内（例如，小于 1 秒）的几个数据包的形式出现，立即就可以识别出。而另一些攻击可能具有间歇活动的特征，跨跃一段很长的时间（例如，几个小时，几天，甚至是几周），甚至，除非收集到大量的事件记录并且进行集中分析才能确认为攻击。所以，尽管每一攻击都有个确定的开始，但当发生攻击时并不总能识别出这一开始时间点。

为简单起见，从现在开始我们仅仅关注一个攻击刚开始的初始时间和实时系统在攻击开始后识别到攻击的这一段时间，换句话说，真实的时间零点再加上其后的一个很小的时间间隔（例如，小于一两秒钟）。从技术的角度讲，这是当前入侵和防御技术的现状。

这些技术在过去的几年中已应用到很大的范围中，没有必要用过多笔墨在这一问题上进行详细描述。做为两种先驱产品，入侵检测技术被动地监测业务数据流以发现可疑的行为和与进攻有关的特征。大部分的入侵检测产品依赖于额外的响应机制；相反，典型的入侵防御设备在线安装，主动地参与数据传输，因而可以直接对检测到的攻击做出反应（比如，在本地设备中阻击攻击）。

当然，实现任何水平的自动应对都需要具有高精度的检测。过多的阻止非攻击性数据流最终都会降低生产率。因而，这一问题是以上两种类型的入侵管理产品共同的发展方

向。多种产品中附加的协议异常和基于漏洞的特征检验是这方面的两种常见的例子。然而，在检测精度方面，总是存在改进的余地。

比如，大多数的产品只关注流经它的数据流。使用这种操作方式，它们忽略了与潜在目标或是在网络环境中的主机相关的信息。恰当的收集并使用这类信息，可以提高自动化处理的水平，在准确性和性能两方面都有一个显著的提高。

同时，在当今存在不断变化的威胁的环境中，期望一种单一的产品截获所有的攻击是不现实的。然而，并不排除这样的方法，从其他已受过攻击的产品中采集信息，用以支持对未来攻击的自动阻止。。

（作者：Martin Roesch　译者：陈志辉 来源：TechTarget 中国）

下一代入侵防御技术：攻击后

正如攻击之前一样，细分攻击之后这个阶段也很有用，然而此时的分割原则是功能和目的，而不是时间顺序。

第一个子部分包括对攻击时检测活动的扩展，主要是相关检验。比如，网络异常行为检测（network behavior anomaly detector，NBAD）使用统计相关的方法为不同类型的事件建立基于速率的阈值。当然，安全事件 / 安全信息管理系统（security event/security information managerment system）是一个更明显的例子。这些工具提供了对从大范围的网络设备中收集事件进行相关检验的机会，这些检验有潜力发现从不同路径发起的攻击或是在相对较长的时间内进行的攻击。

第二个子部分的重点在流程方面，而不在技术方面。总体上来讲，可称为紧急事件响应，目标是包括评判和校正措施。基本上，这是受到一次成功的攻击后所要做的处理，理想的情况上，还应涉及到采取措施以防再次被攻击。

到此为止，对攻击时间线进行了全部说明。本系列的最后一篇描述下一代入侵防御技术的着眼点，该系统沿着时间线对功能进行了集成，致于于提供了个真正的自我防御环境。

（作者：Martin Roesch　译者：陈志辉 来源：TechTarget 中国）

下一代入侵防御技术：集成系统

本系列前几篇文章介绍了攻击的时间线的概念，提出下一代入侵防御系统需要在全部范围内考虑与主要阶段有关的技术和过程，主要阶段即攻击之前、攻击之时和攻击之后。

当然，已有证据表明，安全市场已认识到这种需要。起初只关注时间线的一段的各种各样的厂商已开始提供适用更多的子阶段甚至所有不同阶段的产品。还有一些厂商试图通过互补的伙伴关系达到类似的效果。不管哪种情况，结果只是数据的松耦合或是不同部分的集成。真正的下一代入侵防御系统所需要是在领域和深度方面更充分的集成。理想情况下，一个阶段中的组件应为其他每个阶段中的组件提供有用信息。要实现这样的目标，实现系统集成最少要考虑以下几点：

- 攻击之前阶段进行评估的结果依赖于对系统进行检查的深度，最少可以建立敏锐地发现特定威胁能力，最多可以最终形成对已知弱点的描述。在任一种情况中，这些评估结果都用来自动地协调入侵检测和入侵阻止产品，产生更少的误报，更多的可靠响应动作，甚至更好的性能和功能（比如，对与正在保护的系统不相关的信息不进行检测可以达到这一点）。更进一步，这种协调可以是动态的，因而更加有益，但前提是这些评估是连续的，而不是建立在并不经常进行的快照基础上。
- 类似地，正是这些评估得到的信息可以用于支持攻击之后阶段的工具。特别地，安全事件管理系统 / 安全信息管理系统(SEM / SIM)可以使用这些信息增强它们相关检测的准确性，以及判断所发现目标优先级的准确性。
- 考虑这一流程的逆过程，不管部署了什么其他的安全机制，多种用于攻击之后阶段的产品，比如 NBAD，SEM / SIM 和评判工具，不可避免地会发现一定数目的隐藏着的攻击。将这些攻击信息反馈给入侵检测和防御工具有助于防止再次受到同样攻击。同时，发现这些成功的攻击可以指出先前没有关闭的漏洞，将这些信息反馈给用于攻击之前阶段的评估工具，可以使它们发现哪一个其他系统易受攻击并

采取相应的措施。然而，这两种情况中的难题是适当的打包并表达反馈信息，以便于其他工具可以自动的使用它们。

- 最后，还需要传统的访问控制工具的参与。这些工具不为其他组件提供任何信息，但当遇到时间线任何一端的工具发出的简要信息时，这些工具无疑会更加有效。

显然，集成度达到上述要求非常重要，因为它形成了一个更为有效的解决方案——这一方案中整体功能大于各部分功能的简单和。在局部上，有效性的增强对已实现的额外的自动层有贡献。总之，非常明显，当今快速变化的蠕虫和病毒使得建立在单独的手工操作之上的防御不再有效，更不用提更为普通的情况，普通的情况中由于漏洞管理和威胁管理流程之间存在间隙，还会同时有决策时间和反应时间。

但是，即使实现了自动化，自动化处理也要屈从于或是依赖于更多的重要的先决条件。具体地讲，建立一个环境，在成功部署下一代入侵防御技术的过程的意义是不可低估的。全面的及时的关于受到保护的特定环境的信息是重要组成部分，会从根本上提高系统的有效性。它提供了更好的侦测和确定相关事件的精度，同时通过减少误报便利于实现更好地自动化的处理。没有这样的环境，其他的加强措施仅仅能在交流信息的层而上使阻止系统更为有效。

一个完整的想法必须要包括恰当的术语。以上介绍的下一代入侵防御系统可以简单的称为威胁防范系统或是威胁和漏洞管理系统。出于这种原因，任何描述这一领域特征的术语都可用来指代它。这些说法的区别归结为语法方面的区别，大部分是由于视角的不同。本质的特征是最主要的区别（比如，范围，内容和集成方式），这些方面应当成为致力于在信息安全领域取得更为有效成果的厂商关注的重点。

（作者：Martin Roesch　译者：陈志辉 来源：TechTarget 中国）

入侵防御系统（IPS）知识快速测试

1.)在《如何限制 IPS 的假阳性？》中，作者 Jonathan Hassell 推荐以两种模式之一运行 IPS，来减少假阳性。在哪种模式下 IPS 可能产生大量的假阳性？

a. 混合模式

b. 桥接模式

c. 阻止模式

答案见下页

2.)IPS 和 IDS 的区别是什么？

a. IPS 可以检测网络攻击，但是不能发出警告

b. IPS 可以检测网络攻击并发布警告

c. IPS 可以通过阻止流量并重新连接来回应网络攻击

d. IPS 是在线的并可以监控流量

答案见下页

3.)在安全策略的重要组成部分中，与 IDS 相比，IPS 的主要优势在哪里？

a.产生日志的数量

b. 攻击减少的速度

c. 较低的价格

d. 假阳性的减少量

答案见下页

4.)IPS 可以采用下面哪一种检测机制？

a. 信息包异常检测

b. 普通模式匹配

c. TCp 连接分析

d. 上面都可以

答案见下页

5.）下列哪个属于可以最好的描述系统和网络的状态分析概念，怎么处理其中的错误才是最合适的呢？

a. 回应的比例

b. 被动的防御

c. 主动防御

d. 上面都不对

答案见下页

入侵防御系统（IPS）知识快速测试答案

1.）c. 阻止模式

2.）c. IPS 可以通过阻止流量并重新连接来回应网络攻击

3.）b. 攻击减少的速度

4.）d. 上面都可以

5.）c. 主动防御。