

In The Boxing Ring



IN THIS ISSUE

2.

NETWORK BOX Office 客户门户（用户界面）

Network Box 系统允许客户在全球、地区或国家层面管理一台或多台 Network Box。它将于本月正式上线。

2.

2008 年度 PC3 至尊品牌大奖

在 UTM 领域，我们被授予至尊品牌大奖。

3.

加密 SMTP 邮件

如果您对邮件通讯的隐私有所顾虑，请考虑使用加密 SMTP 或者客户端（加密）的解决方案。

3.

NETWORK BOX 入侵 侦测及防御系统

我们正处于开发一套全新的入侵侦测及防御系统的最后阶段。

4.

May 2009 FEATURES

我们最近公布的错误修复和增强性功能的部署情况。

Network Box 技术新闻

作者：**Mark Webb-Johnson**，首席技术官

致辞

欢迎您来到 2009 年 5 月版 'In The Boxing Ring'。

在这一版，我首先会和大家讲一讲 Network Box Office 客户门户。它的主要功能是可以让用户在国家、地区和全球等各种级别下管理一个或多个 Network Box。该系统计划于今年 5 月份的头两个星期正式上线，详情请见第 2 页。

在 2009 年 4 月的下旬，Network Box 被授予 UTM 类的 PC3 白金至尊品牌大奖，PC3 大奖也授予给了一些其它的全球性品牌。请转到第 2 页查看详细信息。

在第 3 页，我将提供有关 Network Box 对 SMTPS 和 STARTTLS 的支持情况，及讨论 SMTP 邮件加密——后者我建议我们所有的客户考虑，如果你还没有这样做的话。

我也将向您来介绍我们的入侵检测

和预防的新方法，其中包括四个解决方案，及我们即将进行系统全面发布的日期。

本月我们再次有非常多的一批关于 NBRS - 3.0 的重大改进。我们也有关于 my.network-box.com 管理界面的小的改动，以便更好的用来查询，报告和控制 Network Box 设备。

和以往一样，如果您有任何的反馈，意见或者建议，我们都欢迎您随时提出来。您也可以通过发送邮件到我们的邮件列表：nbhq@network-box.com 联系我们。或者当您下次在香港市区的话来随时来我公司办公室进行参观指导。

您也可以通过加入或订阅我们的安全响应 Twitter 和我们保持联系，网址是：

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
May 2009





NETWORK BOX Office 客户门户（用户界面）

我们的客户的组织架构可以是集中式、分布式或者个性化的（也包含三者之间的任意组合），Network Box 的全球化视野包括全球支持功能是客户非常关注的。

我们的分支机构和网络安全运维中心已经遍布全球。它们都会提供给我们的叫做 **Outbreak** 的集中管理系统相关回馈信息。

Network Box Outbreak 系统目前可以在每分钟处理大约 60,000 个安全事件（每秒钟处理 1000 个或者每天处理 8 千 6 百万个），一个名叫 **WOPR** 的大型电脑系统会实时的对这些安全事件进行实时动态地采集、整理和进行关联分析；测算出未来的安全趋势并且告知我们的网络安全工程师全球的安全威胁状况。

Network Box 客户门户为客户提供一个通向这个（和其他）内部系统的窗口。它提供 **Network Box** 设备在我们管理之下的实时状态，并允许同 **Network Box** 网络运维中心（**NOC**）进行正式双向的沟通，他们负责监测和配置 **Network Box** 设备和网络。系统提供下列主要的功能：

- * 概貌页面提供一个有着全球地图背景的包含 **BOX**、**VPN** 和管理链路连接状况的网络接入拓扑图。它提供一个客户所托管的网络安全的简单概貌。

- * 一个工单模块显示用户或者 **NOC** 创建的工单和它们的状态。这就为客户和 **NOC** 之间建立了一个重要的沟通渠道，它可以提供正式的问题事件跟踪，遵从服务级别协定，授权访问控制，变更和配置管理等（等）。这个模块也包括：

- * 一个部署调查模块，用来跟踪在 **BOX** 的安装和部署期间的信息（包括必要的信息收集、使用在线协同工作工具）。

- * 一个资产模块，用来显示 **BOX** 的所有者信息及状态。这个模块也包括：

- * **BOX** 健康状态模块，它也嵌入全球监控系统（**GMS**），显示 **BOX**，网关和 **VPN** 的状态。

- * 许可证模块，显示合同信息，及服务级别协议 **SLA** 信息。

- * 负载模块，显示 **BOX** 的工作负载及趋势分析。

- * 一个用户管理模块，允许客户中的指定特权用户自己查看和维护 **Box Office** 的用户账号信息，而不需 **NOC** 的参与。这个模块允许客户更好地控制和管理支持全球部署的团队。

这个系统提供了一个简单、单一而强大的基于 **WEB** 的用户界面，它可以在国家、地区和全球等级别管理一台或多台 **Network Box**。

我们很高兴地宣布，该系统现定于 2009 年 5 月 12 号进行（全球）正式发布。



2008 年度 PC3 至尊品牌大奖

在 2009 年 4 月，**Network Box** 被授予统一威胁管理（**UTM**）类别的白金至尊品牌大奖。

Network Box 和它的一些主要竞争对手获得了 **PC3** 优质品牌奖 **UTM** 类的提名，并参与了竞争的过程。

处于技术发展最前沿，抵御日益增长的互联网威胁是一项非常艰难的工作，并且行业竞争非常激烈。然而，尽管其他的 **UTM** 类参选者是 **Network Box** 的竞争对手，大家都努力，以保持各种规模的企业客户免受日益扩大的数字安全威胁。

其中有不少相关的互联网安全部门也获得提名及获奖，包括我们的合作伙伴卡巴斯基防病毒软件，与提名者 **NOD32**，趋势科技和其他企业安全软件，其中包括 **Sophos** 公司，赛门铁克公司及其他机构。

其他奖项组包括快闪记忆体，科技教育和网上商店解决方案。进一步类别集中在互联网安全，移动硬盘，投影机和文件解决方案等等。

总体而言，共有 45 个奖项由两个团体通过两个类别颁发。获奖的还有三星电子，**Acronis**，卡巴斯基，索尼，华硕和许多其他知名品牌。主办机构在香港九龙塘的创新中心简短地举办了颁发仪式，但是很专业和正规。



加密 SMTP 邮件

由于标准的 SMTP 发送邮件时，并不使用加密或认证，所以您所传送的每封邮件都以明文文件被转发。针对这一问题，有邮件客户端解决方案（如 S/MIME 和 PGP）可以供采用。它们可以非常有效地解决这一问题，但需要终端用户的参与并且非常复杂。现在有一个更加好的方法可以提供基本的 SMTP 保护，它就是在邮件服务器/网关进行邮件加密。

为什么要这么做呢？答案主要是为了避免对你的通讯受到不必要的窃听。和 SMTP 协议类似的一个真实世界中的例子就是传递不密封信封口的公开信件：您的邮递员，前台工作人员，清洁员，或任何可以接触到这封信的人都可以打开和阅读，甚至修改它并继续传递。最终在你一点儿都未觉察的情况下，你的“私人”通讯被拦截了。如果您信任您的邮差（如：运营商），通讯的隐私或许并不那么重要，那么您不必担心保护您的 SMTP 邮件。

如果您担心这一点，那么你应该先开始考察使用加密的 SMTP 或一个客户端解决方案（如 S/MIME 和 PGP）。

Network Box 已花费一些时间增加对 SMTPS 和 STARTTLS 协议的支持，对象包括我们的传入（进站）和传出（出站）的 SMTP 网关。

在 2009 年 5 月份的星期二补丁更新中，我们将向 SMTP 软件中增加这种支持，而且我们将开始在 5 月中下旬对这一技术进行公开测试，预估会在 2009 年 6 月达到完全支持的目标。

该 SMTPS 和 STARTTLS 协议建立于 SMTP 和标准的 SSL/TLS 之上。因此，它们需在链接的服务器端使用加密证书（也提供可选的客户端加密选项）。

配置出站邮件，使其支持 SMTPS（或 STARTTLS）非常简单。该 Network Box 可配置为在“随机加密”模式（这样它就可以自动检测，看服务器是否支持 STARTTLS，如果不行就切换到 SSL/TLS，进而自动加密所有这些服务器的流量）。Network Box 也可以配置成只针对指定的网域或服务器应用 SMTPS。

配置进站邮件支持 SMTPS（或 STARTTLS）需要在 Network Box 上安装一个 SSL 证书。这些证书可以在线购买，并且可以很简单地取得它。通常情况下，您购买的证书将包括您的发布 DNS MX 记录的名称（因为协议会使用这些名称来验证服务器是谁及是否属实），人们通常会按每年一次支付费用。

该 Network Box 能坐在一个加密的 SMTP 连接的中间。这样，加密邮件可以通过网络传送到 Network Box，接着邮件被解密和扫描以发现恶意/垃圾邮件及执行公司政策，然后被重新加密，最后传递给目标服务器。

加密 SMTP 协议（SMTPS 和 STARTTLS）并不适合每一个人。但是，他们会为那些需要这种保护水平的客户提供有效的 SMTP 协议的保护支持。该协议是标准化的，而且有非常好的互操作性。



NETWORK BOX 入侵侦测及防御系统

一段时间以来，Network Box 提供的 IDP 系统是其可管理 UTM+ 韧体（固件）的一部分。这是一个非常

轻量级的，高速的服务，专门提供针对网络蠕虫，缓冲区溢出和其他此类攻击的零延迟保护。

我们正处于开发一套全新的入侵侦测及防御系统的最后阶段。这套新办法，将提供四种运行模式（1 个旧的和 3 个新的）：

。目前 NBIDS 系统 - 轻量级，零延时，非常快的高性能。

。新 NBIDPS 引擎，使用全面流和协议解码。能够运行在混杂模式（使用交换机的监听口，或集线器），只需使用很少的 IP 地址，并有三种模式：

。被动入侵检测系统 - 报警和记录相关流量，旁路方式部署获取数据流——方便执行政策和发放更具攻击性的规则。

。积极的入侵检测系统 - 报警和记录相关流量，侧路方式部署获取数据流，它可以使用积极的方式中断连接会话。

。串联的 IPS - 报警和记录相关流量，数据流将穿透经过系统；好处是可以减少流量。

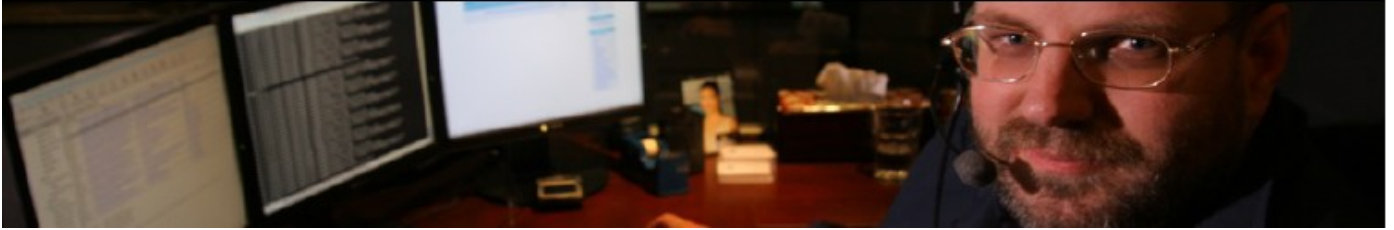
上述几种模式可以结合起来，以适应客户的需求，鉴于性价比的限制，我们通过灵活地部署达到尽可能高的保护水平。

新引擎的签名按照行业标准的 Snort 格式，并可以按全球，按 NOC，按每个客户等不同层面来建立自己的规则。在每个设备的基础上也可以按需要定义所需的签名和独特的配置。每个规则有一个记录和检索帮助页，以帮助进行报告和分析之目的。我们目前的新系统已经有超过 10000 个签名。

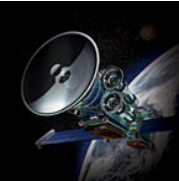
新的引擎提供了一个更强大的规则语言，及更好的流和协议解码支持。这是好的消息，但是它也会影响性能。该解决方案提供四种运作模式，以用来在保护水平（和延迟）和性能取得平衡。可以将不同的接口设定运行在不同的模式下（例如，在内部网络接口部署积极的入侵检测系统，在外网接口部署串联的 IPS）。或者，我们可以简单地对所有流量使用同一个模式运行。

日志记录将合并到我们的 NOC 的统计资料/报告/监测系统，以及定期的 PDF 报告和 my.network-box.com 管理界面。

这将是我们将提供的一个不用另外花钱的增值服务，所有 NBRS-3.0 FW+（或以上）的客户都可以享用，也将成为我们持续不断地服务和监测性能的一部分，当然是在性能允许的情况下。我们估计将于 2009 年 5 月下旬开始公开的测试，正式的发布会在 6、7 月份。



May 2009 Features



2009年5月5日的星期二补丁，我们将为 NBR3-3.0 系统发布大量的错误修复和改进工作。这些变化包括如下：

- 将在 2009 年 5 月 12 日进行全球发布的 Network Box Office 客户门户。
- 改进了 NOC 进行系统维护，诊断和控制的功能——包括更好地对 NOC 及客户更改配置进行集中审计的制度（如防垃圾邮件白名单 / 黑名单的制定）。
- 新的健康状态监督和检查，针对 DNS 服务器以及谷歌安全浏览，新功能会定期检查这些系统和报警（通过全球监控系统）发现的问题。
- 支持 SMTPS 和 STARTTLS 议定书我们存储转发 SMTP 代理。
- 支持 NBIDPS 和定期报告有关 IDPS 的警告。
- 关于 my.network-box.com 管理界面的一些小改动。

上述变化将不会对正在运行的服务产生任何影响，也不需要设备重新启动，所以不会造成任何设备运作的重大中断事故。您当地的网络安全运维中心 NOC 将以分阶段的方式进行新功能的推出。

如果您需要关于任何上述情况的进一步的资料，请联系您当地的网络安全运维中心 NOC，他们将会安排补丁的安装部署及在必要时同您联络。

May Hint

Network Box 利用行业标准协议和服务为您提供各种实时信息。我建议充分利用它以便及早了解全球范围内的安全事件，以及 Network Box 正在帮您做什么。通过这样您可以随时做到更好的准备。

您可以随时通过我们的网站或 my.network-box.com 主页看到新闻故事。但是，您是否知道您可以通过您的浏览器 / RSS 阅读器得到这些新闻的 RSS 种子？请访问：<http://www.network-box.com/aboutus/news/feed> 来订阅我们的简易信息聚合种子吧。

我们也提供更快的最尖端的新闻，提示和警示，请跟随我们的安全反应 RSS 种子
<http://twitter.com/networkboxhq> 或
<http://tinyurl.com/c49s7v>。

结束语

感谢您的支持 Network Box，并继续将您的网络安全托付给我们进行管理服务。我希望这份通讯月刊对您有用。如果您有任何建议，我们都非常欢迎，您可以向当地的 NOC 或客户经理反映；如果您有其它需求，也请别犹豫，马上与我们联系，寻求协助。

Mark Webb-Johnson
 CTO, Network Box Corporation
 May 2009

MAY 2009 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	1,213	-12.5
Signatures Released	2,083,850	-14.0
Firewall Blocks (/box)	618,154	+8.8
IDP Blocks (/box)	139,060	+12.8
Spams (/box)	35,025	+18.5
Malware (/box)	1,340	+63.2
URL Blocks (/box)	59,193	+9.8
URL Visits (/box)	2,611,502	+3.0

NEWSLETTER STAFF

Mark Webb-Johnson
 Editor

Pauline Chiu
 Michael Gazeley
 Jason Law

Production Support

Network Box Australia
 Network Box Hong Kong
 Network Box UK
 Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
 or via mail at:

Network Box
 Corporation

16th Floor, Metro Loft,
 38 Kwai Hei Street,
 Kwai Chung, Hong Kong
 Tel: +852 2736-2078
 Fax: +852 2736-2778
www.network-box.com