In the Boxing Ring
JAN 2025

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2025年1月的 In the **Boxing Ring**

新年快乐！本月，我们将探讨“刻板分类”（Pigeonholing）这一话题。作为一个物种，人类喜 欢对事物进行分类，因为将事物分解并 归类有助于更好地理解和处理——分而 治之。然而，有时候我们会走得太远， 开始不必要地对事物进行刻板分类。

在网络安全领域，起初我们只有防火墙，随后出现了UTM（统一威胁管理） 和NGFW（下一代防火墙）。如今，各种流行术语层出不穷——SIEM、 EDP、 EDR、XDR、MSSP、MDR、SASE、PaaS、 WAF、SOAR、SECaaS、SD-WAN、边缘安全等等，还有数十个小众术语纷纷加入战场。归根结底，这一切不过是营销噱头。在第2至3页中，我们将拨开这些术语和炒作的迷雾，直击保护您的真正关键所在。

在第 4 页中，我们重点介绍了本月“ 补丁星期二” 中针对 Network Box 5 和我们的云服务即将发布的一系列增强功能 和修复内容。

此外，Network Box 香港参与了由贸易通（Tradelink）举办的“网络安全360”活动，以及由互联网专业协会主办的“数字与质量发展论坛”。与此同时，Network Box 的 Michael Gazeley 在香港浸会大学商学院举办了一场网络安全研讨会。最后，Network Box 成为最新一期《今日银行业》的封面故事。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
January 2025

本月摘要:

Pigeonholing

人类天生喜欢对事物进行分类。这是我们基因的一部分。从远古时代起，我们就根据种族、 性别、宗教、部落及其他属性将自己区分开来，最常见的方式是划分为“ 他们”和“ 我们”。 随后，随着科学的出现，复杂的分类体系应运而生，如生物分类法（Taxonomy），最终发 展到图书馆领域的巅峰——杜威十进制分类法（Dewey Decimal Classification System）。这一切是可以理解的。在一个复杂的世界中， 分类有助于将事物分解、归类，达到“分而治 之”的目的。

但有时候，尤其是涉及商业利益时，我们往往会做得过火。不必要地将事物分类，通常是为了区分或获得竞争优势。

以防火墙为例。在早期，‘防火墙’一词的定义非常明确：一种可以配置以阻止特定网络流量的软件。就像建筑中的防火墙可以阻挡不需要的烟雾、热量或火焰一样，计算机防火墙用于阻止不需要的流量。早期的防火墙通常只能基于 IP 地址进行配置，但随着时间推移，其他配置条件也被加入（例如接口、UDP 或 TCP 协议端口、ICMP 请求类型、时间等）。

随后，出现了可以跟踪连接的状态防火墙（Stateful Firewall），能够在连接开始时进行阻止或允许，而不仅仅针对每个数据包进行处理。然而，无论可配置的阻止类型多么复杂，无论是状态防火墙还是无状态防火墙，这些统称仍然是‘防火墙’。

随后，市场上出现了一种新产品，具有检查连接内容、执行非常基础的签名模式匹配并基于此进行阻止的功能。其他公司也在做类似的事情（将杀毒系统与防火墙结合），但这里的不同之处在于营销团队介入并发明了一个新的分类——“统一威胁管理”（Unified Threat Management，简称 UTM）。营销的巧妙之处在于，如果你使用的是“防火墙”，那么那是过时的技术，你需要 UTM 才能实现真正的安全。好吧，人们大致能接受这一点——理解为 UTM 意味着将多个安全功能或服务结合到一个统一的设备中。

接着，另一位新成员登场。这次，提供了协议识别（再次通过流量的启发式/签名技术），于是一个新术语——“下一代防火墙”（Next Generation Firewall，简称 NGFW）应运而生。如果你在使用 UTM，那么那已经是过时的技术，你需要 NGFW 才能实现真正的安全。

你开始看出其中的规律了吗？

如今，我们已经拥有了大量的流行术语——SIEM、EDP、EDR、XDR、MSSP、MDR、SASE、PaaS 、WAF、SOAR、SECaaS、SD-WAN、边缘安全，以及 数十个其他小众术语。而这些，仅仅是关于保护的术 语。威胁本身已经从“病毒”演变为数十个更加细致和 交叉的术语，如 勒索软件、内核木马、特洛伊木马、蠕虫、投放器、零日漏洞、广告软件、网络钓鱼、键盘记录器，以及一个涵盖所有威胁的统称——“恶意软件（malware）”。

你头晕了吗？

归根结底，这些都是营销噱头。问问街头的普通人，他们认为自己需要什么才能确保网络安全，他们会回答： 防火墙 ，而这个回答离真相也不会太远。

我们（这个行业）非常清楚，保护一个组织所需的措施，实际上是一个相对简单的三步过程：

1. 选择一个框架（如 NIST、CIS、PCI DSS、ISO 27001/27002、CMMC 或其他任何框架）。
2. 实施一个符合该框架的技术平台。
3. 以符合该框架的方式监控和管理平台。

要么自己做，要么将其外包给托管安全服务提供商。但请记住，尽管过去 25 年间很多事情发生了变化，但许多基本原则依然未变，且网络安全的核心问题仍然是：80% 的攻击成功是因为没有部署防止这些攻击的技术，另外 20% 的攻击成功则是由于平台的故障未被检测到或配置错误。

因此，在新的一年 **2025** 年，让我们决心摒弃那些狭隘的营销竞争性流行术语。我们将新平台命名为 **Network Box X** （这样你可以根据需要替换**“X”**以适应任何最新的流行术语）。让我们都认识到，我们需要一个网络安全平台来保护我们的组织，并以符合标准化安全框架的方式进行部署、监控和管理。其实，事情真的是如此简单。

Network Box 5

NEXT GENERATION MANAGED SECURITY

2025年1月7日星期二，Network Box 将发布本月的补丁星期二增强功能和修复内容。各地区的安全运营中心（SOC）将在接下来的 14 天内分阶段进行新功能的部署。

Network Box 5 新特性
2025年1月

本季度，针对 Network Box 5，更新内容包括：

- 对证书授权错误报告的小修复
- 改进了 SOC 系统，用于将配置变更请求归因到匹配的工单
- 改进了管理员门户网络接口设置
- 更新了区域 SOC IP 地址分配
- 停用 networkbox@network-box.com 邮箱地址
- 对 SOC 配置和设备维护系统进行多项改进

关于 networkbox@network-box.com 邮箱地址的弃用，我们已经使用该地址一段时间了。然而，随着电子邮件的不断演变，以及 DKIM和 SPF 等电子邮件安全功能的重要性日益凸显，以这种方式使用我们的全球 @network-box.com 域变得越来越困难。因此，本月我们的区域 SOC 将迁移报告邮件，使其来自各自的域或客户特定的邮箱地址。这一变更应能提高报告邮件的发送可靠性（特别是当报告的目的地是 Microsoft 365、GMAIL 等大型电子邮件服务提供商时）。

在大多数情况下，上述更改不应影响正在运行的服务或需要设备重启。然而，在某些情况下（取决于配置），可能需要进行设备重启。如果有必要，您的本地 SOC 将联系您安排相关事宜。

如果您需要了解上述任何内容的进一步信息，请联系您的本地 SOC。他们将负责安排部署和沟通。

Network Box HIGHLIGHTS

Network Box 香港
iProA Event

Network Boxx 香港参与了由互联网专业协会（**iProA**）主办的一场活动。该活动在香港生产力促进局举行，主题为“数字与质量发展论坛：开创新优势，共创未来”。

Network Box 香港
香港浸会大学网络安全研讨会

Network Box 董事总经理 Michael Gazeley 在香港浸会大学商学院的金融科技大师班（FinTech Masterclass）上发表了一场网络安全演讲。

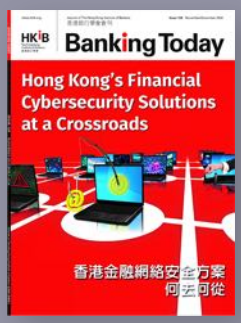
月刊主办	订阅
Mark Webb-Johnson 主编	Network Box CNNOC cnnoc@network-box.cn
Michael Gazeley **Kevin Hla** 产品支持	或者上门到: 深圳市福田区深南大道 竹子林求是大厦西座 920
Network Box HQ **Network Box USA** 贡献者	+86 (755) 3336 1581 www.network-box.cn

翻译：James 校对：Jason

Network Box 香港
网络安全 360 活动

Network Box 与贸易通（Tradelink）合作举办了Cybersecurity 360 活动，该活动在朗廷酒店举行。活动期间，贸易通首席运营官（COO）郑炜光（Andrew Cheng）发表了精彩的演讲，分析了最新的网络安全趋势，展示了各种网络攻击，并为企业提供了保护数字资产的实用策略。他还重点介绍了贸易通如何利用 Network Box 的托管网络安全服务，在过去 20 多年中实现保护、业务连续性和关键绩效指标（KPI）报告。

Network Box 媒体报道



《今日银行业》

第 139 期
2024 年 11-12 月
封面故事:
香港的金融网络安全解决方案正处于十字路口

链接: https://tinyurl.com/4xkpz6ts