

In the Boxing Ring

2025年5月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2025年5月的
In the **Boxing Ring**

本月我们讨论的主题是“加强网络安全：管理员最佳实践”。《Network Box最佳实践》总结了我们在保护客户网络方面超过二十年的经验，形成了一套指导方针。虽然最终的安全策略由客户自行决定，但通过实施这些最佳实践，他们可以显著降低遭受网络攻击的风险。在第2至第3页中，我们对这一主题进行了更详细的探讨，并重点介绍了每位网络管理员必须优先考虑的三项关键安全措施。

在第4页中，我们重点介绍了将在本季度 补丁星期二 发布的 Network Box 5 以及我们的云服务的更新与修复内容。

此外，Network Box 自豪地宣布，在2025年亚太史蒂夫奖中，我们荣获“网络安全解决方案创新”类别的金奖。同时，Network Box 香港也参加了在香港会议展览中心举办的 InnoEX 2025 展会。



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

本月摘要:

第2-3页 加强网络安全：管理员最佳实践

在本期的重点文章中，我们聚焦于三项最重要的 Network Box 网络安全最佳实践建议以加强网络安全：远程管理访问、有效的策略控制以及网络分段。近年来，我们所协助处理的每一起安全事件，其根本原因都涉及至少违反了这三项中的一项。

第4页 Network Box 5 新特性

本月 补丁星期二 将发布的 Network Box 5 及我们的云服务的功能更新与修复内容。

第5页 Network Box 亮点:

- Network Box 荣获2025年亚太史蒂夫奖金奖
- Network Box 香港
 - InnoEX 2025

加强网络安全： 管理员最佳实践

基于二十多年提供托管安全服务、调查安全事件以及协助客户保护其网络的经验，Network Box 将这些经验凝练成了一套简明的指导方针《最佳实践》。我们的安全工程师在为所管理的网络设计防御系统、处理策略变更请求，以及进行定期配置审查时，都会参考这些最佳实践。

<https://network-box.com/best-practices>

我们建议所有客户遵守这些最佳实践。虽然最终政策由客户自行决定，但我们致力于提供信息、警告，并指出当安全策略冲突时，可能会将网络暴露于常见的攻击向量和不必要的风险之下。

本月，我们重点关注每位网络管理员必须优先考虑的三项关键安全措施：远程管理访问、有效的策略控制和网络分段。近年来，我们所协助处理的每一起安全事件，其根本原因都涉及至少违反了这三项中的一项。

远程管理访问： 关闭开放的门

允许远程管理访问直接暴露在互联网上，就像是把安全设施的前门不上锁一样。当像安全外壳协议（SSH）、远程桌面协议（RDP）或虚拟网络计算（VNC）这样的服务暴露给公众互联网时，它们就成为了网络犯罪分子寻找漏洞并加以利用的目标。

攻击者通常使用暴力破解、凭证填充和未修补的软件漏洞进行攻击。更常见的情况是，开放远程管理访问会让你完全依赖于密码——实际上，这意味着只要一个用户犯了一个简单的错误（使用弱密码）或者未修补的漏洞被利用，你的网络就会受到威胁。

为了降低这些风险，管理员必须实施严格的访问控制。安全的虚拟私人网络（VPN）或软件定义广域网（SD-WAN）解决方案应该是唯一允许的远程访问网关，确保只有授权人员可以连接。多因素认证（MFA）通过要求除了密码之外的额外身份验证，增加了额外的安全层。此外，管理员应设置有效的防火墙策略，阻止所有未经明确允许的IP地址的远程管理访问，确保访问仅限于已知位置。最后，未使用的远程管理服务应完全禁用，以消除不必要的暴露。

有效的策略控制： 在每个层级强制执行安全性

薄弱的安全策略或不一致的执行可能会创造出攻击者可以轻易利用的漏洞。差的密码管理、过度的权限或未记录管理员操作是常见的疏忽，这些疏忽可能导致安全漏洞。例如，使用默认凭证如admin/admin，攻击者便能立即访问关键系统。组织必须采取积极的措施来实施和执行强有力的安全策略。应强制要求密码复杂性，迫使管理员使用强大、独特且定期更新的密码。基于角色的访问控制（RBAC）确保用户仅能获得执行其职责所需的权限，从而降低权限过高的账户成为攻击向量的风险。定期进行安全审计有助于发现策略漏洞，管理员可以相应调整控制措施。此外，记录和监控访问尝试有助于团队在发生事件之前发现可疑活动。

网络隔离： 在威胁传播之前进行遏制

平坦的网络架构，其中所有设备可以自由通信，为攻击者创造了理想的环境。一旦敌方成功进入网络，横向移动变得轻而易举，使他们能够轻松访问敏感系统，几乎没有任何阻力。缺乏网络分段可能会将小规模的安全事件转变为全面的安全漏洞。

适当的网络分段通过将关键资源与普通用户隔离开来，有效地降低了这些风险。使用虚拟局域网（VLAN）和防火墙来定义严格的通信策略，确保只有网络区域之间必要的交互被允许。管理员应定期审查各分段之间的流量规则，确保移除不必要的连接。



组织通过实施这些最佳实践，可以显著降低其遭受网络威胁的风险。安全性不是一次性的努力，而是一个持续的过程，需要保持警惕、适应变化并不断改进。网络管理员在保护数字资产方面发挥着至关重要的作用，通过应用这些原则，他们可以加强防御，保护网络免受不断变化的威胁。

通过定期的外部视图扫描和策略审查，Network Box 力求提供信息、警告，并指出当策略冲突时，可能会将网络暴露于常见的攻击向量和不必要的风险之中。但最终，由您——客户，决定策略。

Network Box

5

NEXT GENERATION MANAGED SECURITY

2025年5月6日星期二，Network Box 将发布本月的补丁星期二更新，包含一系列增强和修复功能。各地区的SOC将分阶段在接下来的14天内进行新功能的推广。

Network Box 5 新特性 2025年5月

本季度，Network Box 5 的更新包括以下内容：

- 地图显示性能增强，并切换至新的基础地图提供商。
- VPN会话报告布局改进。
- IPSEC NAT-T稳定性提升。
- 对HTTP代理中服务器端事件（Server Side Events）的额外支持。
- 增强对POP3邮件中的AUTH SASL身份验证的支持。
- 修复事件关联警报邮件的问题。



在大多数情况下，以上变更不会影响正在运行的服务，也不需要重启设备。然而，在某些情况下（根据配置不同），可能需要重启设备。如果需要，您的本地SOC将与您联系并安排相关操作。

如果您需要以上内容的进一步信息，请联系您的本地SOC。他们将负责安排部署和协调工作。

Network Box HIGHLIGHTS



Network Box 荣获 2025年亚太史蒂夫奖金奖



Network Box 荣获第12届亚太史蒂夫奖 (Asia-Pacific Stevie Awards) “网络安全解决方案创新” 类别的金奖。这个奖项体现了我们在推动先进网络安全解决方案方面的坚定承诺。并巩固了Network

Box 作为行业创新者的地位。Network Box 很荣幸能够与IBM、塔塔咨询服务公司 (Tata Consultancy Services)、思科系统 (Cisco Systems) 和新加坡电信 (Singtel) 等全球知名企业一同获得认可，在竞争激烈的领域中脱颖而出。

“我们非常荣幸能够与全球一些最受尊敬的创新者一起获得这份金史蒂夫奖。这一崇高的认可是对我们团队不懈努力的见证，并激励我们不断推动网络安全解决方案的演变。”

--Michael Gazeley
Network Box 管理总监

Network Box 香港 InnoEX 2025

Network Box 香港参加了2025年InnoEX展会，展会在香港会议展览中心举行。在为期四天的展会上，参观者了解了Network Box获奖的安全技术和托管服务。此外，Managing Director Michael Gazeley 还向香港恒生大学的师生做了演讲，讨论了人工智能时代的新兴网络安全挑战和应对策略。



月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

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

+86 (755) 3336 1581
www.network-box.cn