In the Boxing Ring
2024年6月

Network Box 技术新闻

Mark Webb-Johnson
CTO,Network Box

欢迎阅读2024年6月份的 In the **Boxing Ring**

本月，我们将讨论 SSL/TLS 检测。据估计，互联网上 85% 的流量是加密的（其中很大一部分是 SSL/TLS 加密的），大约 70% 的恶意软件活动使用某种形式的加密。如果不对所有流量进行解密以进行检查和策略执行，则可能会带来相当大的安全风险。为了解决这个问题，Network Box 为 SSL/TLS 流量提供了不同级别的检查和策略执行。我们将在第 2 页至第 3 页详细讨论这些内容。

在第 4 页，我们重点介绍了本月的 "补丁星期二 "为 Network Box 5 和我们的云服务发布的一系列增强和修复功能。

另外，Network Box 很荣幸地宣布公司荣获由 Cybersecurity Insiders 颁发的三项网络安全卓越奖。此外，Network Box Hong Kong 与 FUJIFILM Business Innovation HK 合作举办了网络安全研讨会。在本月的科技焦点中，我们将重点介绍 Network Box SOC 服务。你知道吗，当你订阅 Network Box 时，你可以免费获得 SOC 服务。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2024

本月摘要:

SSL/TLS 检查

据估计，互联网上 85% 的流量是加密的，其中很大一部分是 SSL/TLS 加密流量。Google Chrome 浏览器 99% 的浏览时间都花在 HTTPS 网站上，Google 上 95% 的网站都使用 HTTPS。大约 70% 的恶意软件活动使用某种形式的加密。

不对所有流量进行解密以进行检查和策略执行显然是一个巨大的安全问题，但我们都必须认识到对所有 SSL/TLS 流量进行解密（中间人方式）的复杂性。

为了解决这个问题，Network Box 为 SSL/TLS 流量提供了不同级别的检查和策略执行，本文将详细介绍这些选项。

协议强制

由于有大量加密流量经标准连接端口如TCP/443 (https)、TCP/993 (imap4s)、TCP/955 (pop3s)等向外传送，恶意软件透过这些连接端口向外连接，试图逃避加密的情况屡见不鲜。 Network Box 可监察这些连接端口的流量，并检查这些流量，以确保其确实已被 SSL/TLS 加密。如果不是，则可配置策略规则进行适当的阻止和警报。不过，一些常见的应用程序（如 WhatsApp 等）也会尝试使用这些标准端口，但并不使用 SSL/TLS 协议，因此在执行此类策略时需要小心谨慎。

SSL/TLS 服务器名称指示 (SNI) 分类

多年来，SSL/TLS 客户端握手一直包含一个名为 SNI（服务器名称指示）的选项，如今几乎已被普遍使用。只有极少数应用程序（大多是自定义的、旧的或过时的）不提供该选项。SNI 包括要连接的服务器名称（如果服务器在同一 IP 地址或端口上托管多个不同的 SSL/TLS 服务，服务器就可以利用 SNI 提供适当的连接和证书）。如果启用了 SSL 检测，Network Box 就能看到这些 SNI 提示，并以与网站分类相同的方式对这些服务器名称进行分类。然后，就可以根据服务器名称或服务器类别来控制策略规则和进一步解码，而不是简单地根据 IP 地址进行控制。这种方法非常有用，启用简单，对网络的影响也最小。

SSL/TLS 卸载

如果要保护网络服务器（即我们的服务器，而不是客户端浏览器），则可以选择 SSL/TLS 卸载。在这种配置下，受保护服务器的 SSL/TLS 证书会放置在执行保护的 Network Box 装置上（通常是 WAF+）。这样，Network Box 就可以终结 SSL/TLS 连接、解密流量、检查、扫描和应用策略。由此产生的可接受流量可作为 HTTP 或 HTTPS 重新加密后传递给网络服务器。

SSL/TLS 中间人模式

最后一种最全面但最具侵入性的方法是完全的 SSL/TLS 中间人解密--用于保护网络或邮件客户端免受互联网上恶意服务器或内容的攻击。这种方法的主要问题是：(a) SSL/TLS 协议的设计从根本上就是为了防范这种技术；(b) 一些客户端应用程序（通常不是网络浏览器，而是在手机上运行的应用程序）使用证书锁定技术试图阻止这种技术。

实际上，只有一种方法可以实现这种方法。此方法是首先在 Network Box 上建立证书授权，并在所有受保护工作站的网络浏览器和操作系统上安装该证书授权证书。然后，当客户端浏览器访问 HTTPS 网站时，Network Box 设备可以检索远程证书，验证证书是否符合策略要求，如果符合，则使用 Network Box 证书授权重新签署证书。这样，从网络客户端到 Network Box 的流量会在设备上解密、检查、扫描、应用策略控制，如果可以接受，则重新加密后发送到远程网站。从远程网站返回的流量也会得到类似处理。

这种方法存在的问题可归纳如下：

- 有些手机应用程序使用证书锁定来专门限制它们将接受哪些证书颁发机构。Network Box 可以绕过这些应用程序（使用 SNI 或其他基于策略的方法），但这并不理想，而且可能会很麻烦。
- 为了得到保护，需要在所有工作站上安装 Network Box 证书管理机构证书。虽然有自动工具可以帮助完成这项工作，但可能会很繁琐。

其优点是，它能够提供最全面、最有效的 SSL/TLS 流量保护。它甚至超越了客户端工作站所提供的保护，通过对可接受的策略和站点提供集中策略控制。SSL/TLS 策略可以从工作站（用户通常单击“是”以绕过保护并获得他们想要的内容）移动到网关（可以应用可接受内容的集中策略）。

结论

那么，这四种方法哪种最好呢？答案当然是 "视情况而定"。在方便性和安全性之间，总会有一个权衡；这只是其中的一种情况。不过，我们可以提供一些总体指导和建议：

- 协议强制通常不是必需的，但建议在有敏感数据的更安全网络中使用。例如，在主要包含服务器的 DMZ 网络上启用此功能非常简单，对正常的日常运行影响不大，但在检测和防止数据外泄方面却非常有用。
- SSL/TLS SNI 分类实施简单，几乎没有缺点，一般都应启用。即使没有定义策略规则，启用它也能改进 SSL/TLS 流量事件的日志记录（不仅能记录 IP 地址，还能记录协议详情和远程服务器名称）。
- 应为所有受 WAF+ 保护的网络服务器和其他提供 SSL/TLS 保护服务的 DMZ 服务器（如 SMTP、 IMAP4、POP3 等）启用 SSL/TLS 卸载。同样，这也很容易实现，而且允许扫描和策略执行，缺点很少。
- 考虑到 SSL/TLS 中间人解密初始部署的难度，我们通常建议仅将其部署到包含 Linux、OSX 和 Windows 工作站和服务器的局域网和 DMZ 区段。通常不需要将其部署到包含手机的 WIFI 网络中（因为存在证书锁定、自定义应用程序等问题，而且此类加固设备的风险相对较低）。

我们希望本文中的信息对您有所帮助--无论是在解释该技术方面，还是在决定如何在您的网络中最好地使用该技术方面。如需更多建议和帮助，请随时与当地的 Network Box SOC 联系。

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

在 2024 年 6 月 4 日星期二，Network Box 将发布我们的"补丁星期二"增强和修复功能。各地区 SOC 将在未来七天内分阶段推出新功能。

Network Box 5 功能
2024 年 6 月

本月对于Network Box 5, 包括这些:

- 改进 IDS/IPS 中的事件关联。
- 将 Microsoft Azure 常用的 HTML 脚本列入白名单（附加到电子邮件时不再将此类脚本标记为可执行脚本）。
- 改进主机 ACL 中 IP 地址的更新。
- 扩展地区 SOC IP 地址范围，以支持台湾和菲律宾地区的 SOC 扩展。

在大多数情况下，上述更改不会影响正在运行的服务，也不需要重启设备。但在某些情况下（取决于配置），可能需要重新启动设备。如有必要，本地 SOC 将与您联系安排。

如果您需要有关上述任何方面的进一步信息，请联系当地的 SOC。他们将安排部署和联络。

Network Box HIGHLIGHTS

网络安全卓越奖 2024

Network Box 很荣幸地宣布，该公司在 "统一威胁管理"、"反恶意软件 "和 "网页内容过滤 "三个类别中赢得了 Cybersecurity Insiders's 2024 网络安全卓越奖。

"Network Box 的卓越成就证明了他们在网络安全领域对卓越、创新和领导力等核心原则的坚定承诺。"

Holger Schulze
Cybersecurity Insiders
CEO

LINK: https://network-box.com/awards

Network Box 香港 网络安全研讨会

Network Box 香港 与 FUJIFILM Business Innovation HK 合作，为中小型企业举办了一场网络安全研讨会。活动的主要议题是黑客为何针对小型企业。

Network Box 技术聚焦

你知道吗...

订购 Network Box 后，您可以免费获得 SOC 服务？

下面列出了 Network Box SOC 的一些主要功能及其提供的服务：

- 24x7x365 全天候监控和支持
- 全球威胁情报
- 实时安全更新
- 实时响应和支持
- 硬件监控和备份
- 集中登录和管理

以及更多...

有关 Network Box SOC 服务的更多详情，请访问:
https://network-box.com/securityresponse-soc

月刊主办 订阅

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

翻译：Jason Jiang