In the Boxing Ring

Network Box 技術資訊

Mark Webb-Johnson, CTO Network Box

歡迎閱讀2013年4月刊的《In The Boxing Ring》

這個月，Network Box 研發部的 Nick Jones 將會繼續討論 Network Box 安全套接層(SSL)安全性原則。SSL 被 HTTPS 用來保護 web 流覽器和 web 應用間的資料通訊。但 SSL 自己也會有自己的設計和實現缺陷帶來的安全問題。在第 2-3 頁我們將討論詳細細節，以及 Network Box Anti-DDoS WAF+ SSL 協議升級如何解決這些問題。

我們自豪的宣佈 Network Box 贏得資本傑出企業成就獎 最佳網路安全提供商"。

另外，Network Box 韓國最近出席了在韓國國際展覽中心舉辦的 2013 eGISEC 博覽會和 2013 SECON 安全展覽會。

第 4 頁，是這個月對 NBRS-3.0 發佈的新特性和修復補丁的詳情。在可預見的未來幾年，我們將繼續 NBRS-3.0 的開發和支援工作，這一頁將讓您瞭解到我們核心產品的動態資訊。

Mark Webb-Johnson
CTO, Network Box Corporation
April 2013

您可以通過郵箱 (nbhq@network-box.com) 與我們總部取得聯繫，或者到我們的辦公地點親臨參觀指導。您還可以通過以下幾個對外網站對我們保持關注：

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

本 刊 概 要

HTTPS 是流覽器和 web 應用伺服器之間標準 HTTP 通訊協定的安全擴展。它規定了一系列加密技術，以及兩端應該遵守的約定。HTTPS 和它帶來的安全性一直是電子商務必不可少的要素，但近來安全專家也在鼓勵將 HTTPS 用於常規的 web 流覽。Google 最早啟動用 HTTPS 提供所有服務的戰略，為登錄用戶提供 HTTPS 安全版本的服務，從一般的搜索到地圖服務。

Nick Jones
Network Box研發部總監

Network Box 安全套接層安全性原則 (SSL Plus)第三篇

SSL 被 HTTPS 用來保護 web 流覽器和 web 應用伺服器之前的資料通訊。但 SSL 也會有自身設計和實現缺陷帶來的安全問題。為給 HTTPS 提供最高級別的安全，應用伺服器的 SSL 子系統必需保持最新。不幸的是 SSL 系統往往和作業系統捆綁在一些，使之面臨與作業系統同樣的更新維護問題：缺乏長期廠商支援或 web 應用軟體與有限可升級的作業系統間複雜的依賴關係。

Network Box 意識到維護 SSL 和作業系統軟體的複雜性，並開發了"**SSL 協定升級**"，並作為 Anti-DDoS WAF+系統的重要功能之一。

除作為 SSL 終結前端代替 WEB 應用伺服器處理 SSL 連接，Anti-DDoS WAF+能夠通過提供最新 SSL 協議實現來"**升級**"客戶的安全 web 配置。

Network Box 研發部團隊致力於保持 NBRS-5 SSL 子系統的維護更新，來防止針對已知漏洞的攻擊，如 BEAST 和 CRIME 攻擊。

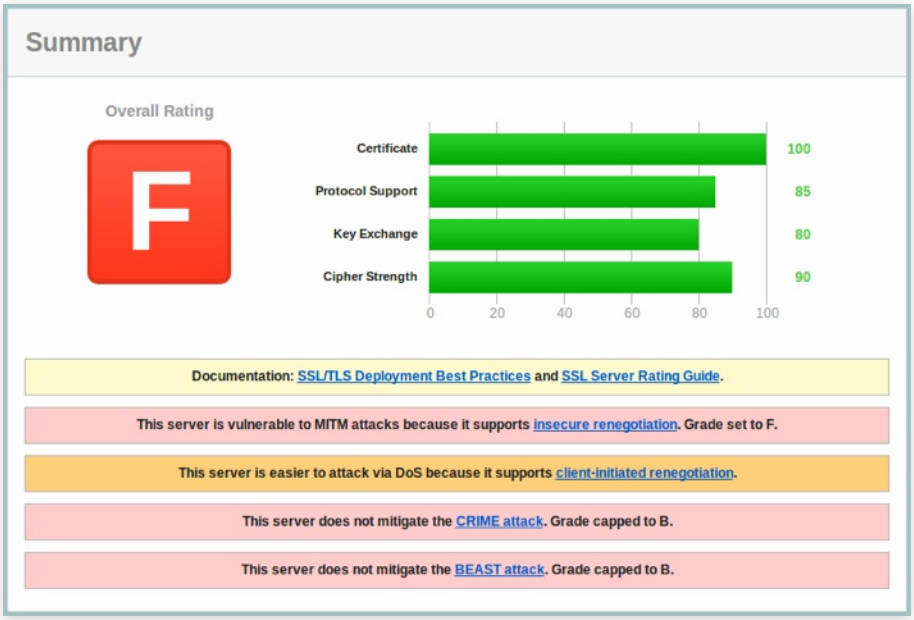
為證明有效性，Network Box 在一個客戶的網站中安裝了 SSL 終端子和 "協定升級"，經客戶的許可我們將在下文解讀此網站的安全分析結果。

將客戶域安全證書導入到 nbconfig 系統，並在已經用於保護客戶網站的 Anti-DDoS WAF+系統上啟用幾個簡單的配置，SSL 終端子和協定升級在**幾分鐘**內就生效了。

我們使用此客戶啟用 Network Box Anti-DDoS WAF+ "SSL 協定升級"之前的 HTTPS 服務作為這次示範的對照。

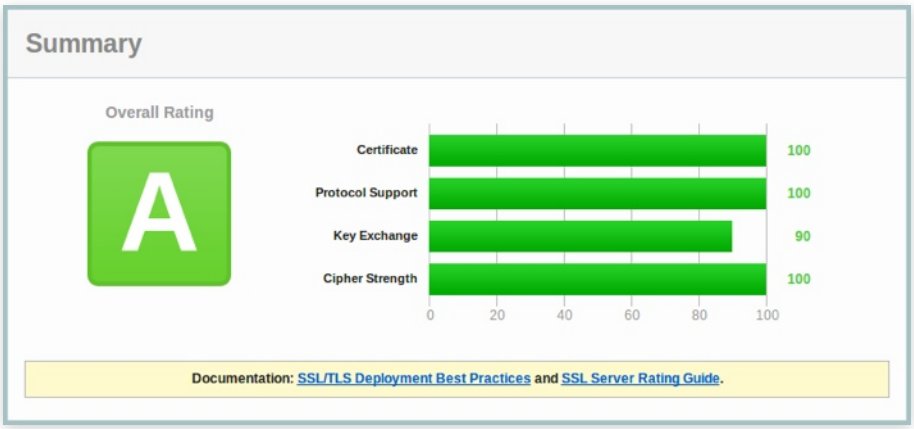
使用著名的 Qualys SSL Labs 分析工具（ https://www.ssllabs.com ），我們可以測試 Network Box Anti-DDoS WAF+ "SSL 協議升級"和原始標準的 HTTPS 的不同。

首先是原始 HTTPS web 服務的分析結果：



我們可以看到，SSL Labs 發現了使用客戶 web 應用伺服器內建的終端子時 SSL 執行的諸多問題。其中一些問題是因為作業系統 SSL 軟體太老，如 BEAST 攻擊漏洞和不安全的重協商，另一些則是因為 web 應用伺服器自身 SSL 配置問題。一些設置問題管理員可通過改變配置來改善，如加密演算法，另一些如 SSL 壓縮（可導致 DRIME 攻擊漏洞）則不能。

我們接下來看 Anti DDoS WAF+ 協議升級作為 SSL 終端子時的分析結果：



A 級！令人滿意的結果。通過在 NSRS-5 上使用最新的 SSL 軟體，和 "SSL 協定升級"優秀的可配置性，使我們成功將客戶網站在數分鐘內從脆弱的 SSL 安全實現升級到 A 級 SSL 配置。

注意：Key Exchange 中的 90 分是因為客戶提供的是 2048 位元的證書，如果使用建議的 4096 位元的證書這個分數將會是 100.

結論：

跟上 SSL 世界的變化並保持網站 SSL 配置的更新對網站管理人員來說是個艱難的任務，因為 SSL 軟體常常是緊密的嵌入在 web 應用伺服器和作業系統中的。Network Box，通過 Anti DDoS WAF+ SSL Protocol Upgrade 不但從徹底免除了 web 應用伺服器 SSL 加密的責任和負擔，更大大降低了管理和維護的複雜性。

保持 SSL 方案的最新對 web 伺服器自身來說是非常困難，甚至是不可能的，Network Box Anti-DDoS WAF+ SSL Protocol Upgrade 則可以為客戶提供 A 級的 SSL 公共服務配置方案。

Network Box 通過 ISO 9001 / ISO 20000 / ISO 27001 認證的安全操作中心

2013年 4 月 新特性

在2013年 4 月2日的星期二這一天，Network Box將發佈這次的Patch Tuesday的補丁包，各區域NOC將會在此之後的7天內安排這些新的功能的發佈和更新工作。這個月的更新補丁包包括：

- 各種內部NOC系統的改進
- 發佈 Box Office 中 NBRS-5.0 合約和許可支援
- 修訂 Kaspersky 防病毒引擎提高在高負荷下的穩定性
- 一系列針對Box Office和支援系統的（主要是內部）功能增強

在多數情況下，以上的修改並不會影響到正在運行的服務，也不需要硬體重啓。但在某些情況下（取決於具體配置），可能需要重啓設備。必要時您當地的區域 NOC 將會與您取得聯繫。

如果您還需要要關於這些的更多的資訊，請與您當地的區域NOC取得聯繫。他們將會進行相關的諮詢和安排。

Network Box 韓國
eGISEC 2013 和 SECON 2013

2013 年 3 月 6-8 日，首爾

Network Box 韓國出席了在韓國國際展覽中心舉辦的 2013 第二屆電子政務資訊安全博覽會（eGISEC）和 2013 SECON 安全展覽會。由公共管理和安全部和韓國資訊安全局(KISA)舉辦，超過 50 家公司展出了最新的安全技術。

資本雜誌
2013 傑出企業成就獎

2013 年 3 月 11 日，Network Box 贏得第 13 屆資本傑出企業成就獎"最佳網路安全提供商"。

MARCH 2013 NUMBERS

關鍵指標	數據	與上月差比
PUSH Updates	381	-8.0
Signatures Released	478,943	-27.4
Firewall Blocks (/box)	904,985	-6.1
IDP Blocks (/box)	106,943	-1.0
Spams (/box)	14,511	+32.9
Malware (/box)	905	+164.6
URL Blocks (/box)	196,054	+14.4
URL Visits (/box)	3,930,517	-0.6

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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